МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Н.Г. Парватов

ВВЕДЕНИЕ В МАТЕМАТИКУ

Учебное пособие

Томск
Издательский Дом Томского государственного университета
2019

УДК: 512
ББК: 22.144
П18

Парватов Н.Г.

П18 Введение в математику : учебное пособие. – Томск : Издательский Дом ТГУ, 2019. – 350 с.

ISBN 978-5-94621-833-7

Книга призвана помочь начинающим в изучении математики. В ней последовательно рассматривается ряд базовых разделов математики, в том числе изучаются элементы теории множеств, числовые системы, алгебраические структуры, метрические пространства. Данный материал должен составить основу для дальнейшего изучения алгебры, геометрии, топологии и разнообразных специализированных дисциплин.

УДК: 512
ББК: 22.144

Рецензенты:
доктор физико-математических наук, доцент, профессор кафедры алгебры,
А.Р. Чехлов;
доктор физико-математических наук, доцент, профессор кафедры системного анализа
и математического моделирования, *С.Э. Воробейчиков.*

ISBN 978-5-94621-833-7

© Парватов Н.Г., 2019
© Томский государственный университет, 2019

Содержание

Часть I. Множества, отношения и функции ... **7**

Глава 1. Множества и отношения ... 8
1. Множество ... 8
2. Отношения и отображения ... 9
3. Отношение порядка ... 15

Глава 2. Аксиомы теории множеств ... 21
1. Система Цермело-Френкеля ... 21
2. Аксиомы Гёделя-Бернайса ... 24
3. Универсумы ... 25

Глава 3. Натуральный ряд ... 26
1. Аксиомы Пеано ... 26
2. Конечное множество и число элементов ... 27
3. Принцип индукции ... 28
4. Больше-меньше ... 29
5. Фундированное множество ... 31

Глава 4. Мощность множества ... 34
1. Равномощность ... 34
2. Сравнение множеств по мощностям ... 35
3. Счётное множество ... 36
4. Несчётное множество ... 37
5. Операции над мощностями ... 38

Глава 5. Вполне упорядоченное множество ... 39
1. Теорема Цермело и лемма Цорна ... 39
2. Порядковый тип ... 41
3. Свойства бесконечных мощностей ... 43

Глава 6. Подстановки ... 45
1. Умножение подстановок ... 45
2. Разложение на циклы ... 45
3. Транспозиции и декремент ... 48
4. Инверсии и транспозиции соседних элементов ... 49
5. Чётные подстановки ... 50

Глава 7. Комбинаторные числа ... 52
1. Основные комбинаторные принципы ... 52
2. Размещения и сочетания ... 52
3. Биномиальная формула и обращение ... 54
4. Мультимножества ... 56
5. Полиномиальная формула ... 57
6. Числа Стирлинга и числа Белла ... 59
7. Формула включений и исключений ... 62

Часть II. Целые числа, матрицы и многочлены ... **65**

Глава 8. Целые числа ... 66
1. Построение целых чисел ... 66

2. Деление с остатком ... 67
3. Алгоритм Евклида ... 68
4. Простые числа ... 70
5. Классы вычетов ... 71
6. Целые т-адические числа ... 73
Глава 9. Алгебраические структуры ... 75
1. Алгебраическая операция ... 75
2. Коммутативность и ассоциативность ... 75
3. Полугруппа, моноид, группа ... 77
4. Кольцо ... 80
5. Гомоморфизмы колец ... 81
6. Кольцо целых т-адических чисел* ... 82
7. Целостное кольцо и поле ... 84
8. Поле частных целостного кольца ... 85
9. Кольцо частных, локализация* ... 87
10. Характеристика кольца ... 88
Глава 10. Степенные ряды ... 90
1. Степенные ряды и ряды Лорана ... 90
2. Дифференцирование рядов ... 91
3. Алгебраические операции над рядами ... 93
4. Экспоненцирование и логарифмирование ... 94
5. Биномиальная формула ... 95
Глава 11. Многочлены ... 98
1. Многочлены и рациональные выражения ... 98
2. Деление с остатком ... 99
3. Алгоритм Евклида ... 99
4. Разложение на неприводимые множители ... 100
5. Классы вычетов многочленов ... 101
6. Присоединение корня ... 102
7. Разложение на простейшие дроби ... 105
8. Линейные рекуррентные последовательности ... 107
Глава 12. Корни многочленов ... 110
1. Теорема Безу и схема Горнера ... 110
2. Кратные корни ... 111
3. Интерполяция ... 112
4. Производная и формула Тейлора ... 113
5. Производная и кратные корни ... 114
6. Производная и кратные множители ... 115
7. Полиномиальные функции над целостным кольцом ... 116
Глава 13. Матрицы ... 119
1. Операции над матрицами ... 119
2. Элементарные матрицы ... 122
3. Ступенчатая матрица ... 123
4. Система линейных уравнений ... 125
5. Линейная зависимость* ... 126
6. Определитель ... 128

7. Разложение определителя по строке ... 131
8. Формулы Крамера ... 132
9. Характеристический многочлен* ... 133

Глава 14. Свободные модули и векторные пространства ... 134
1. Модуль и алгебра ... 134
2. Линейные отображения ... 136
3. Свободный модуль и векторное пространство ... 138
4. Координаты вектора ... 142
5. Матрица линейного отображения ... 144
6. Инвариантность размерности ... 145
7. Теорема Гамильтона-Кэли ... 146

Глава 15. Симметрические многочлены и результант ... 153
1. Многочлены нескольких переменных ... 153
2. Теорема Гаусса о симметрических многочленах ... 155
3. Симметрические функции корней ... 159
4. Результант двух многочленов ... 160
5. Результант как симметрическая функция корней ... 164

Часть III. Действительные и комплексные числа ... 166

Глава 16. Действительные числа ... 167
1. Упорядоченное кольцо ... 167
2. Аксиома Архимеда и систематические дроби ... 169
3. Систематические и обыкновенные дроби ... 170
4. Аксиома Кантора ... 172
5. Аксиома Дедекинда ... 174
6. Фундаментальные последовательности ... 175
7. Поле действительных чисел ... 178

Глава 17. Корни вещественных многочленов ... 182
1. Непрерывность и теорема Вейерштрасса ... 182
2. Корни и степени ... 183
3. Локализация корней и последовательность Штурма ... 185
4. Стандартная последовательность Штурма ... 186

Глава 18. Комплексные числа и кватернионы ... 188
1. Комплексные числа ... 188
2. Основная теорема Алгебры ... 193
3. Кватернионы ... 196

Глава 19. Метрические и нормированные пространства ... 204
1. Метрические пространства ... 204
2. Топология метрического пространства ... 208
3. Последовательности и полнота ... 211
4. Непрерывность ... 213
5. Пополнения ... 216
6. Теорема Островского ... 219

Глава 20. Евклидовы и эрмитовы пространства ... 221
1. Евклидово пространство ... 221
2. Матрица Грама и объём параллелепипеда ... 225

3. Изометрии евклидова пространства ... 229
4. Эрмитово пространство ... 230

Часть IV. Кольца и модули ... 234

Глава 21. Кольцо ... 235
1. Идеал кольца ... 235
2. Фактор-кольцо ... 237
3. Теоремы об изоморфизмах ... 239
4. Прямые суммы ... 242

Глава 22. Теория делимости ... 247
1. Простые и неприводимые элементы ... 247
2. Область с однозначным разложением ... 249
3. Нётерово кольцо ... 252
4. Разложение в кольце многочленов ... 254

Глава 23. Поля ... 260
1. Определение и основные конструкции ... 260
2. Степень расширения ... 261
3. Алгебраические и конечные расширения ... 262
4. Простое расширение ... 263
5. Поле разложения ... 266
6. Теорема о примитивном элементе ... 268
7. Задача Чирнгауза ... 269
8. Конечные поля ... 270

Глава 24. Модуль над кольцом ... 276
1. Подмодуль ... 276
2. Фактор-модуль ... 277
3. Теоремы об изоморфизмах ... 279
4. Прямые произведения и суммы ... 280
5. Двойственный модуль* ... 285
6. Билинейные формы ... 290
7. Матрицы и билинейные формы ... 293
8. Точные последовательности* ... 297

Глава 25. Модуль над областью главных идеалов ... 301
1. Векторное пространство и ранг матрицы ... 301
2. Каноническая форма Смита ... 303
3. Свободный модуль над областью главных идеалов ... 306
4. Конечно-порождённый модуль над ОГИ ... 308
5. Нормальные формы матриц ... 311

Глава 26. Алгебраические числа ... 318
1. Целые элементы расширения колец ... 318
2. Норма и след ... 322
3. Дискриминант числового поля ... 328
4. Дедекиндово кольцо ... 334
5. Группа классов идеалов ... 340
6. Простые числа в расширении ... 345

Рекомендуемая литература ... 349

Часть I

Множества, отношения и функции

ГЛАВА 1

Множества и отношения

В главе рассматриваются множества, отношения и функции.

1. Множество

В понимании множества будем исходить из формулировок Кантора и Дедекинда. В дальнейшем это понятие будет уточнено.

Георг Кантор следующим образом объяснял, что такое множество: «под множеством мы будем понимать объединение в единое целое M вполне различаемых объектов m нашего восприятия или мысли (называемых элементами множества M)».

Рихард Дедекинд писал так: «множество S полностью определено только тогда, когда относительно всякой вещи известно, является ли она элементом множества S или нет».

При неправильном использовании понятия множества возникают так называемые парадоксы. Приведём в качестве примера парадокс Рассела и пару его переформулировок.

Парадокс Рассела. Назовём обычным множество, которое не содержит себя в качестве элемента. Вопрос: обычным или необычным является множество всех обычных множеств.

Переформулировка. Брадобрей бреет тех и только тех, кто не бреется сам. Вопрос: бреет ли он себя?

Ещё одна переформулировка. Прилагательное назовём самоприменимым, если оно обладает тем свойством, которое выражает. Например, таким является прилагательное «двадцатиоднобуквенное». Вопрос: самоприменимо ли прилагательное «несамоприменимое».

Принято считать, что для избавления от парадоксов следует регламентировать процесс построения новых множеств. Это выполнено в ряде аксиоматических теорий, которые будут рассмотрены позднее. До тех пор будем строить свои рассуждения на наивной основе, но придерживаясь определённой осторожности. Отметим ряд свойств.

∘ *Множество полностью определяется своими элементами.*

Пишут $m \in M$, если m является элементом множества M.

Чтобы задать множество, нужно объяснить каким-то образом, какие объекты являются его элементами. В ряде случаев это можно сделать,

перечислив явно его элементы или указав их свойство. Множество, составленное из элементов $a, b, c, \ldots$, обозначается

$$\{a, b, c, \ldots\}.$$

Следующим образом

$$\{x|P(x)\}$$

определяется множество, элементами которого являются все объекты со свойством P. Вопрос о том, какие свойства выделяют множество, а какие — нет, не прост, как показывает парадокс Рассела.

∘ *Существует множество без элементов.*

Оно называется *пустым* и обозначается $\emptyset$.

Множество A называется *подмножеством* или *частью* множества B, если каждый элемент из множества A принадлежит множеству B. В этом случае пишут $A \subseteq B$.

∘ *Для любого множества A существует множество, элементами которого являются всевозможные подмножества множества A.*

Оно обозначается $\mathcal{P}(A)$.

Удобно считать, что выполняется ещё одно свойство.

∘ *Существует универсальное множество, частью которого является любое множество, возникающее в нашем рассмотрении.*

2. Отношения и отображения

Опишем ряд конструкций, связанных с множествами.

Операции над множествами. Пусть A и B — множества. Их *объединение* $A \cup B$ состоит из элементов, принадлежащих хотя бы одному из них; их *пересечение* $A \cap B$ состоит из элементов, принадлежащих им обоим; их *разность* $A \setminus B$ состоит из элементов, принадлежащих множеству A и не принадлежащих B; их *симметрическая разность* $A \Delta B$ состоит из элементов, принадлежащих в точности одному из них.

Дополнением множества A называется множество $A' = \{c|c \notin A\}$. Отметим далее ряд свойств введённых операций над множествами.

Законы коммутативности:

∘ $A \cap B = B \cap A$,

∘ $A \cup B = B \cup A$

∘ $A \Delta B = B \Delta A$.

Законы ассоциативности:

∘ $A \cap (B \cap C) = (A \cap B) \cap C$.

∘ $A \cup (B \cup C) = (A \cup B) \cup C$,

$\circ$ $A\Delta(B\Delta C) = (A\Delta B)\Delta C$.

Законы дистрибутивности:

$\circ$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

$\circ$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

$\circ$ $A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C)$.

Законы поглощения:

$\circ$ $A \cup (A \cap B) = A$,

$\circ$ $A \cap (A \cup B) = A$.

Законы де Моргана:

$\circ$ $(A \cup B)' = A' \cap B'$,

$\circ$ $(A \cap B)' = A' \cup B'$.

Закон второго дополнения:

$\circ$ $A'' = A$.

Упражнение. Докажите перечисленные свойства.

Наборы. Выберем пару элементов a, b из соответствующих множеств A, B и образуем новый объект, который назовём *упорядоченной парой* этих элементов и обозначим (a, b). Будем считать две упорядоченные пары равными, если у них первые компоненты совпадают и вторые компоненты совпадают. Множество всех таких упорядоченных пар называется *декартовым произведением* множеств A, B и обозначается $A \times B$.

Аналогично, если имеются множества $A_1, \ldots, A_n$, то выбор элементов $a_1, \ldots, a_n$ из соответствующих множеств определяет *упорядоченный набор* $(a_1, \ldots, a_n)$ этих элементов. Число n называется длиной набора. Два набора одной длины равны, если их компоненты, стоящие в одной позиции, совпадают. Множество всех таких наборов обозначается $A_1 \times \ldots \times A_n$ и называется *декартовым произведением* множеств $A_1, \ldots, A_n$. Если все эти множества совпадают с множеством A, то декартово произведение обозначается A^n и называется n-ой *декартовой степенью* множества A.

Отношения. Подмножество $\alpha \subseteq A \times B$ называется *отношением* на паре множеств A, B. Вместо $(a, b) \in \alpha$ также пишут

$$a\alpha b \text{ или } \alpha(a, b)$$

и говорят, что пара (a, b) удовлетворяет отношению α, или элемент a находится в отношении α к элементу b. Отношение $\alpha^{-1} \subseteq B \times A$, такое, что

$$(b, a) \in \alpha^{-1} \Leftrightarrow (a, b) \in \alpha,$$

называется *обратным* для α. *Произведением* отношений $\alpha \subseteq A \times B$ и $\beta \subseteq B \times C$ называется отношение $\alpha\beta \subseteq A \times C$, определяемое условием

$$(a, c) \in \alpha\beta \;\Leftrightarrow\; (a, b) \in \alpha \text{ и } (b, c) \in \beta \text{ для некоторого } b \text{ из } B.$$

Произведение $\alpha\beta$ обозначается также $\beta \circ \alpha$ и называется тогда *композицией* отношений β, α. Как видно, композиция от произведения отличается лишь порядком записи сомножителей.

Отметим, что

- $(\alpha^{-1})^{-1} = \alpha$;
- $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$;
- $\alpha(\beta \cup \gamma) = \alpha\beta \cup \alpha\gamma$.

Записанные равенства выполняются, если произведения в них корректны.

Упражнение. Докажите эти соотношения.

Отображения. Отношение $\alpha \subseteq A \times B$ называется *отображением* или *функцией* из множества A в множество B, если для любого элемента a из A существует ровно один элемент b в B, такой, что $(a, b) \in \alpha$. В этом случае говорят, что задано отображение (или функция)

$$\alpha : A \to B$$

с *областью определения* A и *областью значений* B, а множество

$$\operatorname{im}\alpha = \{b | (a, b) \in \alpha \text{ для некоторого } a\}$$

называют *образом* отображения α. Элемент b, о котором говорится в определении, называется *образом элемента* a. Он обозначается обычно αa или $a\alpha$, но может обозначаться как a^α, α_a и т. д. Запись

$$\alpha : a \mapsto b$$

означает, что элемент b является образом элемента a при отображении α. В этой ситуации также говорят, что функция α отображает элемент a на элемент b.

Отображение α называют *инъективным* или *вложением*, если различные элементы из множества A имеют различные образы. Оно называется *сюръективным* или *наложением*, если $\operatorname{im}\alpha = B$. Для инъективных и сюръективных отображений используются соответствующие обозначения

$$A \hookrightarrow B, A \twoheadrightarrow B.$$

Отображение, являющееся одновременно инъективным и сюръективным, называется *биективным* или *обратимым*. Отметим пару свойств.

∘ Произведение отображений

$$\alpha : A \to B, x \mapsto x\alpha$$
$$\beta : B \to C, x \mapsto x\beta$$

является отображением

$$\alpha\beta : A \to C, x \mapsto (x\alpha)\beta.$$

Оно инъективно, если отображения α, β инъективны; и сюръективно, если эти отображения сюръективны. □

∘ Отображение $\alpha : A \to B$ тогда и только тогда биективно, когда обратное отношение α^{-1} является отображением $\alpha^{-1} : B \to A$. В этом случае имеют место равенства

$$\alpha\alpha^{-1} = \mathrm{id}_A, \alpha^{-1}\alpha = \mathrm{id}_B,$$

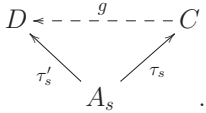
где $\mathrm{id}_A, \mathrm{id}_B$ — тождественные отображения на соответствующих множествах, отображающие каждый элемент на себя. □

При использовании произведения и композиции удобно по-разному писать аргументы: слева при использовании произведения и справа для композиции. Соотношения из первого свойства можно было бы записать в такой форме:

$$\alpha : x \mapsto \alpha x, \beta : x \mapsto \beta x, \beta \circ \alpha : x \mapsto \beta(\alpha x).$$

Упражнения.

∘ Объединение непересекающихся множеств A_1, A_2 называется их *прямой суммой* и обозначается $A_1 \sqcup A_2$. Докажите, что прямая сумма обладает следующим универсальным свойством: биекция $C \to A_1 \sqcup A_2$ существует тогда и только тогда, когда существуют отображения $\tau_s : A_s \to C$, где $s = 1, 2$, и для любого множества D и любых отображений $\tau'_s : A_s \to D$, где $s = 1, 2$, существует отображение $g : C \to D$, такое, что коммутативны диаграммы

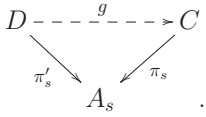


.

Коммутативность в подобных случаях означает, что все композиции, вычисляемые по стрелкам и имеющие общие начала и концы, совпадают.

∘ Докажите универсальное свойство декартова произведения: биекция $C \to A_1 \times A_2$ существует тогда и только тогда, когда существуют отображения $\pi_s : C \to A_s$, где $s = 1, 2$, и для любого множества D и

любых отображений $\pi'_s : D \to A_s$, где $s = 1, 2$, существует отображение $g : D \to C$, такое, что коммутативны диаграммы



∘ Сравните между собой приведённые выше диаграммы.

Двойственное отображение*. Пусть D — фиксированное множество. Обозначим через D^A множество всех отображениий из A в D. Для отображения $f : A \to B$ отображение

$$f^* : D^B \to D^A, f^* : \alpha \mapsto f^*(\alpha), \text{ где } f^*(\alpha) = \alpha \circ f,$$

назовём *двойственным*. Имеет место следующее свойство.

∘ Пусть заданы отображения

$$f : A \to B, g : B \to C.$$

Тогда для двойственных отображений

$$f^* : D^B \to D^A, g^* : D^C \to D^B$$

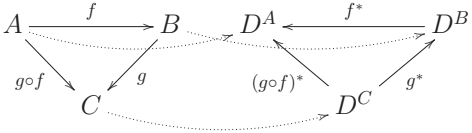
выполняется равенство:

$$(g \circ f)^* = f^* \circ g^*.$$

Доказательство. Для любого отображения $\beta : C \to D$ имеем:

$$(g \circ f)^*(\beta) = \beta \circ g \circ f = f^*(g^*(\beta)) = (f^* \circ g^*)(\beta). \square$$

Данное свойство можно проиллюстрировать диаграммой.



Произведения. Пусть T — произвольное множество и для каждого его элемента s задано некоторое множество A_s. В этой ситуации говорят, что задан набор

$$(A_s | s \in T)$$

множеств A_s, индексированных элементами s из T. Объединением этих множеств называется множество

$$\cup_s A_s = \{a | a \in A_s \text{ для некоторого } s \text{ из } T\}.$$

Отображение

$$f : T \to \cup_s A_s, s \mapsto f_s, \text{ где } f_s \in A_s,$$

называется *функцией выбора* из множеств A_s, а также *набором* элементов f_s, выбранных из множеств A_s. Оно может обозначаться как

$$(f_s | f_s \in A_s, s \in T).$$

Множество всех таких наборов обозначается

$$\prod_s A_s$$

и называется *произведением* множеств A_s. Если все множества A_s совпадают с множеством A, то их произведение состоит из всевозможных функций $f : T \to A$ и обозначается тогда A^T. Удобно считать

$$\prod_s A_s = A_1 \times \ldots \times A_n \text{ и } A^T = A^n$$

для множества T, состоящего из чисел $1, \ldots, n$.

Разбиения и эквивалентности. Система непустых подмножеств множества A называется его *разбиением*, если каждый элемент множества содержится ровно в одном из подмножеств, принадлежащих этой системе. Иными словами, подмножества не пересекаются и их объединение совпадает с A. Подмножества, принадлежащие разбиению, называются его *классами* или *блоками*.

Отношение $\alpha \subseteq A^2$ называется *бинарным отношением* на множестве A и называется *эквивалентностью*, если выполнены условия:

(рефлексивность) $a \alpha a$;

(транзитивность) $a \alpha c$, если $a \alpha b$ и $b \alpha c$;

(симметричность) $a \alpha b$, если $b \alpha a$;

для любых элементов a, b, c из множества A.

Укажем связь между разбиениями и эквивалентностями. Пусть α — эквивалентность, заданная на множестве A. Для прозвольного элемента a из A положим

$$[a]_\alpha = \{x | x \in A, a \alpha x\}.$$

Это множество называется *классом эквивалентности* α элемента a. Множество всех таких классов называется *фактор-множеством* множества A по эквивалентности α и обозначается A/α. Имеет место следующее свойство.

∘ Существуют взаимно обратные биекции:

$$\mathrm{Eq}(A) \to \mathrm{Part}(A), \alpha \mapsto A/\alpha,$$
$$\mathrm{Part}(A) \to \mathrm{Eq}(A), P \mapsto \varepsilon(P),$$

где $\varepsilon(P)$ — отношение «принадлежать одному классу из P». □

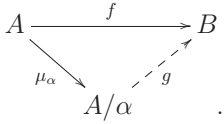
Эквивалентности и отображения. Установим связь между эквивалентностями и отображениями. Для любого отображения $f : A \to B$ отношение ff^{-1} называется его *ядром*. Это отношение является эквивалентностью на множестве A. Ему удовлетворяют пары элементов с одинаковыми образами при отображении f. Для эквивалентности α, заданной на множестве A, отображение

$$\mu_\alpha : A \to A/\alpha, a \mapsto [a]_\alpha,$$

называется *каноническим* отображением с ядром α. Отметим свойство.

$\circ$ Пусть $f : A \to B$ — отображение с ядром α. Тогда существует единственное отображение $g : A/\alpha \to B$, такое, что $f = \mu_\alpha g$. Отображение g инъективно. $\square$

Данное свойство иллюстрирует диаграмма



.

3. Отношение порядка

В данном разделе рассматривается отношение порядка.

Порядок. Бинарное отношение $\leqslant$ на множестве A называется *частичным порядком*, или просто — *порядком*, а множество A, рассматриваемое с этим отношением, называется (частично) *упорядоченным*, если выполнены условия:

(рефлексивность) $a \leqslant a$;

(транзитивность) $a \leqslant c$, если $a \leqslant b$ и $b \leqslant c$;

(антисимметричность) $a = b$, если $a \leqslant b$ и $b \leqslant a$;

для любых элементов a, b, c из множества A. Порядок называется *линейным*, если дополнительно выполненяется условие

(линейность) $a \leqslant b$ или $b \leqslant a$.

Отношение $<$, определённое условием

$$a < b \qquad \Leftrightarrow \qquad a \leqslant b \text{ и } a \neq b,$$

называется *строгим порядком*, связанным с отношением порядка $\leqslant$. Строгий порядок обладает свойством транзитивности, также для него выполняется условие

(иррефлесивность) $a \not< a$.

Каждое из этих двух отношений полностью определяют второе. Рассмотрим далее ряд конструкций частично упорядоченных множеств.

∘ Всякое подмножество частично упорядоченного множества упорядочено индуцированным порядком, при котором элементы сравниваются так же как в исходном множестве. Обычно для индуцированных порядков не вводят новых обозначений.

∘ Отношение, обратное порядку, также является порядком. Обратный порядок называется также *двойственным*. Для отношения $\leqslant$ двойственный (обратный) порядок обозначается $\geqslant$.

∘ Декартово произведении упорядоченых множеств A, B можно упорядочить покомпонентно, считая

$$(a_1, b_1) \leqslant (a_2, b_2) \;\Leftrightarrow\; a_1 \leqslant a_2 \text{ и } b_1 \leqslant b_2.$$

∘ Декартово произведение упорядоченых множеств A, B можно упорядочить *лексикографически*, или *словарно*, считая

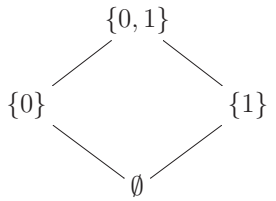
$$(a_1, b_1) < (a_2, b_2) \;\Leftrightarrow\; a_1 < a_2 \text{ или } (a_1 = a_2 \text{ и } b_1 < b_2).$$

Словарное упорядочение сохраняет линейность исходных порядков.

Диаграмма Хассе. В упорядоченном множестве элемент b *покрывает* элемент a, если $a < b$ и не существует элемента c, такого, что $a < c < b$. В этом случае элементы a, b называются *соседними*. Элемент b называют *минимальным*, если не существует элемента c, такого, что $c < b$. Двойственным образом определяются максимальные элементы.

Конечное частично упорядоченное множество изображается графически *диаграммой Хассе*. В ней элементы множества располагаются по ярусам. Ярусы линейно упорядочены и большие элементы располагаются на больших ярусах. В диаграмме проводятся рёбра (линии) между соседними элементами.

Диаграмма Хассе может быть построена следующим образом: на первый ярус запишем все минимальные элементы, на второй — минимальные среди оставшихся и т. д.; когда все элементы будут исчерпаны, проведём рёбра. Ниже приводится диаграмма подмножеств множества из двух элементов, упорядоченных включением.



Упражнение. В конечном частично упорядоченном множестве *высотой* элемента a назовём наибольшее значение n, такое что существует

цепочка

$$a_0 < a_1 < \ldots < a_n = a.$$

Проверьте, что при построении диаграммы частично упорядоченного множества указанным выше способом номер яруса произвольного элемента на единицу больше высоты.

Изоморфизм упорядоченных множеств. *Изоморфизмом* между частично упорядоченными множествами A, B называется взаимно-однозначное соответствие

$$A \to B, x \mapsto x',$$

такое, что

$$x \leqslant y \;\Leftrightarrow\; y' \leqslant y'$$

для любых x, y из A. Частично упорядоченные множества, между которыми существует изоморфизм, называются *изоморфными*. Если мы изучаем отношения порядка, определённые между элементами некоторых множеств, и не интересуемся природой их элементов, то изоморфные частично упорядоченные множества можно не различать, считая их копиями. Диаграммы Хассе у изоморфных множеств отличаются только обозначениями вершин. Рассмотрим далее ряд примеров изоморфных частично упорядоченных множеств.

∘ Пусть A — произвольное множество. Рассмотрим множество $\mathcal{P}(A)$ всех его подмножеств, упорядоченное отношением включения, и множество 2^A всех функций $A \to \{0,1\}$, где

$$\alpha \leqslant \beta \quad\Leftrightarrow\quad \alpha(a) \leqslant \beta(a) \text{ для всех } a \in A.$$

Имеет место изоморфизм упорядоченных множеств:

$$\chi : \mathcal{P}(A) \to 2^A, \chi : B \mapsto \chi_B, \text{ где } \chi_B(a) = 1 \;\Leftrightarrow\; a \in B.$$

∘ Пусть множество A содержит n элементов $a_1, \ldots, a_n$ и множество $\{0,1\}^n$ двоичных наборов длины n упорядочено покомпонентно. Существует следующий изоморфизм упорядоченных множеств:

$$\varphi : \{0,1\}^n \to \mathcal{P}(A), \varphi : x \to \{a_i | x_i = 1\}.$$

∘ Имеется изоморфизм между частично упорядоченными множествами $\{0,1\}^n$ и 2^A, совпадающий с произведением отображений φ и χ. Определите его явно.

∘ Упорядочим множество $\mathrm{Part}(A)$ всех разбиений множества A, считая

$$P_1 \leqslant P_2 \quad\Leftrightarrow\quad [a]_1 \subseteq [a]_2 \text{ для любого } a \in A,$$

где $[a]_i$ — класс разбиения P_i, содержащий элемент a. Имеется изоморфизм:

$$\mathrm{Eq}(A) \to \mathrm{Part}(A), \alpha \mapsto A/\alpha,$$

где эквивалентности на A упорядочены включением.

Упражнения.

∘ Проверьте, что (корректное) произведение изоморфизмов является изоморфизмом, как и отображение, обратное изоморфизму.

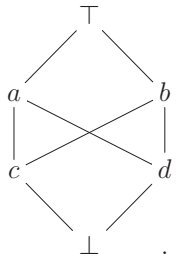
∘ Убедитесь, что рассмотренные выше отображения являются изоморфизмами, укажите обратные изоморфизмы, проиллюстрируйте рассуждения диаграммами.

Полная решётка. В частично упорядоченном множестве P элемент b называется *верхней гранью* (под)множества A, если для любого элемента a из A выполняется неравенство $a \leqslant b$. Обозначим через $\bigtriangledown A$ множество всех верхних граней множества A. Если элемент b принадлежит множеству A и является его верхней гранью, то он называется *наибольшим* элементом этого множества; такой элемент единствен, если существует. Наибольший элемент всего множества P обозначается $\top$ (когда существует).

Двойственным образом определяется нижняя грань множества A, множество $\bigtriangleup A$ всех его нижних граней и наименьший элемент множества A. Наименьший элемент всего множества P обозначается $\bot$.

Наименьшая из верхних граней множества A обозначается $\sup A$, если существует, и называется тогда его *точной верхней гранью*. Двойственным образом, *точная нижняя грань* множества A — это элемент $\inf A$, являющийся наибольшей из нижних граней этого множества.

Рассмотрим частично упорядоченное множество с диаграммой



.

Здесь $\bigtriangleup\{a,b\} = \{c,d,\bot\}$ и $\bigtriangledown\{a,b\} = \{\top\}$, $\sup\{a,b\} = \top$ и элемента $\inf\{a,b\}$ не существует. Отметим далее пару свойств.

∘ *Пусть a — элемент подмножества A, выбранного в частично упорядоченном множестве P. Тогда следующие условия равносильны.*

(I) *Элемент a — наибольший в A.*

(II) *В P имеет место равенство $a = \sup A$.*

Доказательство. Пусть a — наибольший элемент множества A. Тогда a является верхней гранью этого множества и для любой верхней грани b

верно $a \leqslant b$, поскольку $a \in A$. Таким образом, элемент a является точной верхней гранью для A. Обратно, пусть $a = \sup A$. Тогда a является верхней гранью множества A по определению точной верхней грани и является наибольшим элементом множества A, так как принадлежит ему. □

∘ *Если какой-то из элементов* $\inf \emptyset$, $\sup P$ *и* $\top$ *существует, то все эти элементы существуют и совпадают.*

Доказательство. Это свойство следует из предыдущего. □

Частично упорядоченное множество, удовлетворяющее условиям следующей теоремы, называется *полной решёткой*.

Теорема (о полной решётке). *Для частично упорядоченного множества* P *следующие условия равносильны.*

(I) *В* P *всякое подмножество имеет точную верхнюю грань.*

(II) *В* P *всякое подмножество имеет точную нижнюю грань.*

Доказательство. Пусть выполняется первое условие. Тогда для любого подмножества $A \subseteq P$ имеется элемент $\sup \triangle A$. Он является наименьшим элементом множества $\bigtriangledown \triangle A$. В частности, он является нижней гранью этого множества и тогда в силу включения $A \subseteq \bigtriangledown \triangle A$ является нижней гранью A, то есть принадлежит множеству $\triangle A$; тогда он является в этом множестве наибольшим элементом в силу свойства, доказанного выше. Таким образом, имеет место равенство $\sup \triangle A = \inf A$. Следовательно, выполняется второе условие. Из второго условия первое следует двойственным образом. □

Рассмотрим следующие примеры.

∘ Множество $\mathcal{P}(A)$ с отношением включения является полной решёткой, где точные нижние грани совпадают с пересечениями и точные верхние грани совпадают с объединениями.

∘ Множество $\mathrm{Eq}(A)$ с отношением включения является полной решёткой, где точные нижние грани совпадают с пересечениями. Очевидно, изоморфное упорядоченное множество $\mathrm{Part}(A)$ также является полной решёткой.

Упражнение. Что представляют собой точные нижние и верхние грани в полных решётках $\mathrm{Eq}(A)$ и $\mathrm{Part}(A)$?

Решётка. Частично упорядоченное множество P, в котором любые два элемента имеют точную нижнюю и точную верхнюю грани, называется *решёткой*. В этом случае определены бинарные операции

$$\wedge : P^2 \to P, (x, y) \mapsto x \wedge y = \inf\{x, y\},$$

$$\vee : P^2 \to P, (x, y) \mapsto x \vee y = \sup\{x, y\},$$

которые называются операциями решётки P. Решётка однозначно определяется своими операциями, так как верна

Теорема. *В решётке для любых элементов a, b, c выполняются следующие условия:*

(0) $a \leqslant b \Leftrightarrow a = a \wedge b \Leftrightarrow b = a \vee b$;

(1, идемпотентность) $a \wedge a = a, a \vee a = a$;

(2, коммутативность) $a \wedge b = b \wedge a, a \vee b = b \vee a$;

(3, ассоциативность) $a \wedge (b \wedge c) = (a \wedge b) \wedge c, a \vee (b \vee c) = (a \vee b) \vee c$;

(4, поглощение) $a \wedge (a \vee b) = a, a \vee (a \wedge b) = a$.

Обратно, если в некотором множестве заданы операции $\vee, \wedge$ и для любых элементов a, b, c выполняются условия (1–4), то существует упорядочение этого множества, для которого выполняется условие (0). Такое частично упорядоченное множество является решёткой с операциями $\vee, \wedge$.

Доказательство. Первая часть проверяется не сложно. Докажем вторую. Предположим, условия (1–4) выполнены. Заметим, что упорядочение корректно определено условием (0). Действительно, если $a = a \wedge b$, то $a \vee b = (a \wedge b) \vee b = b$ в силу коммутативности и поглощения. Аналогично проверяется обратная импликация. Проверим, что $a \vee b = \sup\{a, b\}$. Для этого заметим, что элемент $a \vee b$ является верхней гранью для элементов a, b в силу первых трёх свойств. Для любой их верхней грани c выполняется $c \vee a \vee b = c \vee b = c$, откуда $a \vee b \leqslant c$ и $a \vee b$ — наименьшая верхняя грань этих элементов. Аналогично проверяется равенство $a \wedge b = \inf\{a, b\}$. □

Теорема. *В решётке следующие условия равносильны.*

(I) *Выполняется тождество $a \vee (b \wedge c) \approx (a \vee b) \wedge (a \vee c)$.*

(II) *Выполняется тождество $a \wedge (b \vee c) \approx (a \wedge b) \vee (a \wedge c)$.*

□

Решётка, в которой выполняются условия этой теоремы, называется *дистрибутивной*.

ГЛАВА 2

Аксиомы теории множеств

В этой главе рассматриваются аксиомы теории множеств, относящиеся к аксиоматическим теориям Цермело-Френкеля и Гёделя-Бернайса.

1. Система Цермело-Френкеля

Объектами данной аксиоматической теории являются множества, которые рассматриваются с отношениями принадлежности $\in$ и равенства $=$; в частности, элементы множеств — тоже множества. Перечислим аксиомы Цермело и Френкеля; средствами математической логики им можно придать абсолютно строгий вид.

ZF1. Аксиома экстенсиональности. Два множества равны, если они содержат одни и те же элементы.

ZF2. Аксиома существования. Существует пустое множество.

ZF3. Аксиома пары. Для любых множеств x, y существует множество $\{x, y\}$, единственными элементами которого являются x, y.

ZF4. Аксиома объединения. Для любого множества x существует множество $\cup x$, элементами которого являются элементы множеств, принадлежащих x.

ZF5. Аксиома бесконечности. Существует множество ω, такое, что

$$\emptyset \in \omega, \text{ и}$$
$$x \cup \{x\} \in \omega, \text{ если } x \in \omega.$$

ZF6. Аксиома подстановки для свойства F. Пусть для любого множества x существует единственное множество y, такое, что пара (x, y) обладает свойством F (будем писать $F(x, y)$ в этом случае). Тогда для любого множества z существует множество

$$\{y | F(x, y) \text{ для некоторого } x \in z\}.$$

ZF7. Аксиома степени. Для любого множества x существует множество $\mathcal{P}(x)$ всех его подмножеств.

ZF8. Аксиома выбора. Для любого непустого множества x, такого, что $\emptyset \notin x$, существует «функция выбора» $g : x \to \cup x$, такая, что $g(y) \in y$ для любого множества $y \in x$.

ZF9. Аксиома регулярности. В любом непустом множестве есть элемент, не содержащий в качестве элемента элементов этого множества.

Прокомментируем записанные аксиомы.

∘ С использованием логического языка аксиома эктенсиональности записывается так:

$$\forall x \forall y (\forall z ((z \in x \to z \in y) \wedge (z \in y \to z \in x)) \to x = y).$$

Остальные аксиомы не станем записывать подобным образом.

∘ Пустое множество единственно в силу аксиомы эктенсиональности.

∘ При помощи аксиомы существования и аксиомы пары можно строить множества, содержащие один или два элемента.

В частности, для любого множества x существует одноэлементное множество $\{x\} = \{x, x\}$, единственным элементом которого является x. Из пустого множества $\emptyset$ получаем одноэлементные множества

$$\{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots$$

и двухэлементные множества, например, такие

$$\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}\}, \dots.$$

С использованием аксиомы пары для любых двух множеств x, y можно определить их *упорядоченную пару по Куратовскому*

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

На основании этого можно определить упорядоченные наборы как

$$(x, y, z) = ((x, y), z), (x, y, x, w) = ((x, y, x), w), \dots$$

или

$$(x, y, z) = (x, (y, z)), (x, y, x, w) = (x, (y, x, w)), \dots;$$

возможны и другие варианты.

∘ На основании аксиомы объединения из любых множеств $x, y, z, w, \dots$ можно составить конечные множества

$$\{x, y, z\} = \cup\{\{x\}, \{y, z\}\},$$

$$\{x, y, z, w\} = \cup\{\{x, y, x\}, \{w\}\}, \dots$$

и дать ещё одно альтернативное определение упорядоченных наборов:

$$(x, y, z) = \{\{x\}, \{x, y\}, \{x, y, z\}\},$$

$$(x, y, z, w) = \{\{x\}, \{x, y\}, \{x, y, z\}, \{x, y, z, w\}\}, \dots.$$

∘ Аксиома бесконечности говорит о существовании множества ω, включающего «натуральный ряд» элементов

$$\emptyset,\ \{\emptyset\},\ \{\emptyset, \{\emptyset\}\},\ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},\ \dots.$$

∘ В аксиоме подстановки под свойством понимется некоторое логическое условие. Аксиома формулируется для каждого свойства F, представляющего интерес. Таким образом, здесь речь идёт о схеме аксиом, содержащей бесконечное множество аксиом. Аксиома утверждает, что образ функции является множеством. Обычно можно обойтись следующей более слабой аксиомой.

ZF6'. Аксиома выделения для свойства P. Для любого множества z существует множество

$$\{y|y \in z \text{ и } P(y)\}.$$

Здесь P — некоторое заданное логическое условие (свойство), истинное или ложное для каждого множества y; мы пишем $P(y)$, если оно истинно для y.

Эта аксиома также формулируется для каждого свойства, представляющего интерес. Она говорит о том, что в любом множестве можно выделить подмножество, состоящее из элементов с заданным свойством.

∘ С использованием аксиомы степени декартово произведение может быть определено как

$$a \times b =$$

$$\{z|z \in \mathcal{P}(\mathcal{P}(a \cup b)) \text{ и } z = \{\{x\}, \{x, y\}\} \text{ для некоторых } x \in a, y \in b\}.$$

По-аналогии можно определить декартово произведение нескольких множеств. С использованием декартовых произведений можно определить функцию.

∘ Аксиома выбора позволяет осуществить выбор элементов в непустых множествах и составить из этих элементов множество. Это можно сделать, даже когда нет свойства, определяющего функцию выбора.

∘ Аксиома регулярности запрещает существование бесконечной цепочки множеств $x, y, z \ldots$, таких, что

$$\ldots \in z \in y \in x.$$

Упражнения.

∘ Как выполнить объединение заданных двух множеств?

∘ Проверьте свойства упорядоченных наборов.

∘ Проверьте, что следующие ситуации невозможны:

$$x \in x, \quad x \in y \in x, \quad x \in y \in z \in x, \quad \ldots.$$

2. Аксиомы Гёделя-Бернайса

Ещё одна широко известная система аксиом принадлежит Гёделю и Бернайсу. Объектами данной аксиоматической теории являются классы, рассматриваемые с бинарными отношениями принадлежности $\in$ и равенства $=$. Множеством называется класс, который является элементом другого класса. Идея класса принадлежит фон Нейману. Перечислим конспективно аксиомы Гёделя и Бернайса, следуя книге П. Дж. Коэна «Теория множеств и континуум-гипотеза».

GB1. Аксиома экстенсиональности для классов. Два класса равны, если содержат одни и те же элементы.

GB2. Аксиома существования. Существует пустое множество.

GB3. Аксиома пары. Для любых множеств x, y существует множество $\{x, y\}$, единственными элементами которого являются x, y.

GB4. Аксиома объединения. Для любого множества x существует множество $\cup x$, элементами которого являются элементы множеств, принадлежащих x.

GB5. Аксиома бесконечности. Существует множество ω, такое, что $\emptyset \in \omega$ и $x \cup \{x\} \in \omega$, если $x \in \omega$.

GB6. Аксиома подстановки для классов. Пусть F — класс и для любого множества x существует единственное множество y, такое, что упорядоченная пара (x, y) принадлежит классу F. Тогда для любого множества z существует множество

$$\{y | (x, y) \in F \text{ для некоторого } x \in z\}.$$

GB7. Аксиома степени. Для любого множества x существует множество $\mathcal{P}(x)$ всех его подмножеств.

GB8. Аксиома выбора для классов. Существует класс, содержащий пару (x, y) для любого непустого множества y и некоторого единственного элемента $x \in y$.

GB9. Аксиома регулярности для классов. В непустом классе есть элемент, не содержащий в качестве элемента элементов этого класса.

GB10. Аксиома пересечения. Для любых двух классов существует их пересечение.

GB11. Аксиома дополнения. Для любого класса существует его дополнение.

GB12. Существует класс, элементами которого являются всевозможные упорядоченные пары (x, y), где $x \in y$ и y — произвольное множество.

GB13. Для любого класса X существует класс

$$\{y|y \text{ — множество и } (x,y) \in X \text{ для некоторого множества } x\},$$

GB14. Для любого класса X существует класс

$$\{(x,y)|y \in X \text{ и } x \text{ — множество }\}.$$

GB15. Для любого класса X существует класс $\{(x,y)|(y,x) \in X\}$.

GB16. Для любого класса X существует класс $\{(y,z,x)|(x,y,z) \in X\}$.

GB17. Для любого класса X существует класс $\{(x,z,y)|(x,y,z) \in X\}$.

Система аксиом Гёделя и Бернайса получается следующим образом. Аксиомы экстенсиональности, выделения, выбора и регулярности формулируются для классов, остальные аксиомы системы Цермело и Френкеля остаются без изменений. При этом схема аксиом выделения заменяется одной аксиомой, но добавляются аксиомы 10–17, необходимые для построения классов, задающих свойства. В результате получается конечная система аксиом.

Теорема (Мостовский). *Всякая теорема теории Цермело-Френкеля является теоремой теории Гёделя-Бернайса. Обратно, каждая теорема теории Гёделя-Бернайса, в которой фигурируют только множества, является теоремой теории Цермело-Френкеля.* □

3. Универсумы

Множество U назовём *универсумом*, если

$$\omega \in U, A \subseteq U, \mathcal{P}(A) \in U, \cup A \in U, f(A) \in U$$

для любого множества $A \in U$ и любого отображения $f : A \to U$.

Существование универсумов не гарантировано в аксиоматических теориях Цермело-Френкеля и Гёделя-Бернайса. В связи с этим, имеет смысл добавить к этим теориям следующую аксиому.

Аксиома универсума. Существует хотя бы один универсум.

ГЛАВА 3

Натуральный ряд

В главе определяется числовая система натуральных чисел.

1. Аксиомы Пеано

Натуральные числа используется для указания количеств и нумерации. Выделим характерные свойства ряда натуральных чисел.

1. Для любого натурального числа n существует непосредственно следующее за ним натуральное число n^+.

2. У различных натуральных чисел непосредственно следующие различаются.

3. Существует единственное натуральное число, обозначим его через 0, которое не является непосредственно следующим ни для какого натурального числа.

4. Принцип индукции. Множество M содержит все натуральные числа, если оно содержит 0 и для любого натурального числа n верна импликация:

$$n \in M \to n^+ \in M.$$

Перечисленные условия называются аксиомами Пеано.

Заметим, что формулировка последней аксиомы включает в себя понятие «множество». Это означает, что аксиоматическая теория для натуральных чисел должна включать в себя аксиомы для множеств.

Любое множество, для элементов которого выполняются перечисленные выше свойства натуральных чисел, договоримся называть *натуральным рядом* и его элементы будем называть *натуральными числами*. Далее натуральный ряд обозначается $\mathbb{N}$.

Упражнение. Единствен ли натуральный ряд с точностью до обозначений? Единственность в данном случае означает, что между двумя натуральными рядами существует биекция φ, согласованная с отношением следования так, что:

$$\varphi(0) = 0, \varphi(n^+) = \varphi(n)^+.$$

Замечание. Натуральное число n будем называть *предшествующим* числу n^+. В силу второй аксиомы у натурального числа не может быть двух предшествующих. А в силу третьей аксиомы у любого отличного

от нуля натурального числа n имеется единственное предшествующее, обозначим его n^-.

2. Конечное множество и число элементов

Как выразить формально, что множество A содержит n элементов? Это удобно сделать на основе следующего определения. Множество B натуральных чисел назовём *начальным отрезком*, если вместе с любым отличным от нуля числом оно содержит непосредственно предшествующее ему, иными словами для любого натурального числа n выполняется импликация

$$n \in B \to n^- \in B.$$

Начальный отрезок, отличный от всего множества натуральных чисел, называется *собственным*. Например, собственными начальными отрезками натурального ряда

$$0, 1, 2, \ldots$$

являются множества

$$\emptyset, \{0\}, \{0, 1\}, \{0, 1, 2\}, \ldots.$$

Отметим следующие свойства.

∘ *Для любого собственного начального отрезка B существует натуральное число n, такое, что*

$$n \notin B, n^- \in B.$$

(Назовём такое n мощностью начального отрезка B.)

Доказательство. Иначе для некоторого собственного начального отрезка B и любого натурального числа n верна импликация

$$n^- \in B \to n \in B,$$

откуда с использованием принципа индукции получаем $B = \mathbb{N}$. □

∘ *Для любого натурального числа n существует единственный начальный отрезок мощности n. Он обозначается $[\mathbb{N}, n)$.*

Доказательство. Пусть M — множество всех натуральных чисел n, для которых существует единственный начальный отрезок мощности n. По-индукции проверяется, что множество M состоит из всех натуральных чисел. Единственный начальный начальный отрезок нулевой мощности это пустое множество, поэтому множество M содержит 0. Предположим, число n принадлежит множеству M, то есть существует единственный начальный отрезок мощности n. Добавим к нему число n, получим начальный отрезок мощности n^+. С другой стороны, удаление числа n из начального отрезка мощности n^+ приводит к начальному отрезку

мощности n. Следовательно, начальный отрезок мощности n^+ единствен. $\square$

$\circ$ *Не существует биекции между собственными начальными отрезками различной мощности. В частности, мощность любого собственного начального отрезка определена однозначно.*

Доказательство. Для любого натурального числа n не существует биекции между начальным отрезком мощности n и начальным отрезком иной мощности. Докажем это индукцие по n. Это так при $n = 0$. Предположим, что это верно для некоторого значения n. Представим, что существует биекция между начальными отрезками мощностей n^+, m^+. Можно считать без ограничения общности, что эта биекция n отображает на m. Но тогда она определяет также биекцию между начальными отрезками мощностей n, m. В силу предположения индукции $n = m$. Свойство доказано. $\square$

Теперь можно сделать следующее определение. Будем говорить, что A — конечное n-элементное множество, если оно отображается биективно на начальный отрезок $[\mathbb{N}, n)$. В этом случае число n будем обозначать через $|A|$ и называть *числом элементов* или *мощностью* множества A. Мощность определена корректно в силу свойств, указанных выше.

Это определение отражает следующее наблюдение: когда мы считаем или нумеруем элементы конечного множества, фактически мы устанавливаем биекцию с начальным отрезком натурального ряда.

Упражнение. Определите сумму и прозведение двух натуральных чисел как мощность некоторого множества. Проверьте корректность сделанного определения и перечисленные далее свойства, имеющие место для любых натуральных чисел a, b, c.

(Коммутативность.) $a + b = b + a, ab = ba$.

(Ассоциативность.) $a + (b + c) = (a + b) + c, a \cdot bc = ab \cdot c$.

(Дистрибутивность.) $a(b + c) = ab + ac$.

(Свойства нуля.) $a + 0 = a, a \cdot 0 = 0$.

(Свойства единицы.) $a \cdot 1 = a$.

(Сокращение.) $a + b = a + c \to b = c, (a \cdot b = a \cdot c \wedge a \neq 0) \to b = c$.

3. Принцип индукции

Принцип индукции (содержащийся в четвёртой аксиоме) используется для доказательства того, что некоторым свойством P обладают все натуральные числа. Чтобы это сделать, достаточно проверить, что свойством обладает 0, то есть $P(0)$ верно, и для любого натурального n выполняется

импликация

$$P(n) \to P(n^+).$$

Принцип индукции используется также для определения функций вида $f : \mathbb{N} \to A$. Для того, чтобы некоторые условия однозначно определяли такую функцию достаточно, чтобы значение $f(0)$ было определено однозначно и для любого натурального n из того, что значение $f(n)$ однозначно определено должно следовать, что $f(n^+)$ также однозначно определено.

Пример. Функция «факторал» определяется условиями

$$0! = 1,$$
$$n^+! = n! \cdot n^+.$$

Возможность индуктивных определений обосновывает следующая

Теорема. *Пусть A — произвольное множество. Для любой функции $g : A \to A$ и любого элемента a из множества A существует единственная функция $f : \mathbb{N} \to A$, такая, что $f(0) = a$ и $f(m^+) = g(f(m))$ для всех натуральных m.*

Доказательство. Можно убедиться, что для любого натурального n существует единственная функция $f_n : [\mathbb{N}, n^+) \to A$, обладающая свойствами, аналогичными свойствам функции f. Функции f_n согласованы между собой — принимают одинаковые значения на одинаковых элементах области определения. Тогда $f = \cup_n f_n$. □

Упражнение.

∘ Проведите данное рассуждение подробно.

∘ Определите по-индукции операции сложения и умножения натуральных чисел и докажите основные свойства этих операций.

4. Больше-меньше

Отношение $\leqslant$ в множестве натуральных чисел определяется следующим образом:

$$a \leqslant b \Leftrightarrow b = a + c \text{ для некоторого } c.$$

Это отношение является линейным порядком.

Упражнение. Проверьте свойства линейного порядка. Для этого полезно доказать, что для любых натуральных чисел n, m верно:

$$m < n, \text{ если } m \in [\mathbb{N}, n),$$
$$m \geqslant n, \text{ если } m \notin [\mathbb{N}, n).$$

Отметим следующие свойства.

(1. Вторая форма индукциии.) Множество M содержит все натуральные числа, если для любого натурального числа n верна импликация

$$[\mathbb{N}, n) \subseteq M \to n \in M.$$

(2. Условие минимальности.) Любое непустое множество натуральных чисел содержит наименьший элемент.

(3. Условие обрыва убывающих цепей.) Не существует бесконечной строго убывающей последовательности натуральных чисел $a_0, a_1, \ldots$, где

$$a_0 > a_1 > \ldots.$$

Иначе: бесконечная убывающая последовательность натуральных чисел $a_0, a_1, \ldots$, таких, что

$$a_0 \geqslant a_1 \geqslant \ldots$$

стабилизируется, так что начиная с некоторого номера n выполняются равенства

$$a_n = a_{n+1} = \ldots.$$

Упражнение. Перечисленные свойства равносильны между собой в предположении выполнения первых трёх аксиом Пеано.

Принцип индукции во второй форме также используется для доказательств и определений. В соответствии с этим, некоторое свойство P выполняется для всех натуральных чисел, если оно выполняется для произвольного натурального числа n в предположении, что оно имеет место для всех чисел отрезка $[\mathbb{N}, n)$. Для того чтобы функция $f : \mathbb{N} \to A$ была однозначно определена, нужно, чтобы для любого натурального n значение $f(n)$ было определено однозначно в предположении, что однозначно определены значения $f(m)$ для всех m из отрезка $[\mathbb{N}, n)$. Корректность таких определений опирается на следующую теорему.

Теорема. *Для любой системы функций $g_n : A^n \to A$, где $n \in \mathbb{N}$, существует единственная функция $f : \mathbb{N} \to A$, такая, что*

$$f(n) = g_n(f(0), \ldots, f(n-1))$$

для всех натуральных n. $\square$

Упражнение. Докажите теорему и следующие утверждения.

$\circ$ Деление с остатком. Для любых натуральных чисел n, k, где $k \neq 0$, существуют и определены однозначно натуральные числа q, r, такие, что

$$n = q \cdot k + r, r < k.$$

Эти числа называются частным и остатком при делении n на k, остаток также обозначается $n \mod k$.

∘ Пусть $k \geqslant 2$. Для любого натурального a существует единственный набор чисел $a_0, a_1, \ldots$, принадлежащих множеству $\{0, 1, 2\}$ и таких, что

$$a = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + \ldots.$$

∘ Для любого натурального a существует единственный набор чисел $a_0, a_1, \ldots$, таких, что $0 \leqslant a_n \leqslant n + 1$ для любого n и

$$a = a_0 \cdot 1! + a_1 \cdot 2! + a_2 \cdot 3! + \ldots.$$

∘ Пусть $k \geqslant 2$. Для любого натурального a существует единственный набор чисел $a_0, a_1, \ldots$, таких, что $0 \leqslant a_n \leqslant k - 1$ для любого n и

$$a = a_0 \cdot k^0 + a_1 \cdot k^1 + a_2 \cdot k^2 + \ldots.$$

Значения a_n называется n-м разрядом числа a в системе счисления по основанию k (в k-ичной системе счисления).

∘ Запишите формулы для вычисления разрядов суммы и произведения в k-ичной системе счисления.

5. Фундированное множество

Пусть множество A частично упорядочено отношением $\leqslant$. Для любого его элемента a положим

$$[A, a) = \{x | x \in A, x < a\}.$$

Имеет место

Теорема (об индукции). *Следующие условия равносильны.*

(1. Условие минимальности.) *В множестве A всякое непустое подмножество содержит минимальный элемент (относительно индуцированного упорядочения).*

(2. Условие обрыва убывающих цепей.) *В множестве A не существует бесконечной строго убывающей последовательности элементов.*

(3. Принцип индукции.) *Множество M включает множество A, если для любого элемента $a \in A$ верна импликация:*

$$[A, a) \subseteq M \to a \in M.$$

Доказательство. Докажем ряд импликаций.

$(1 \to 2)$ Из первого условия следует второе.

Действительно, если в A имеется бесконечная строго убывающая последовательность, то множество её элементов, очевидно, не имеет минимального элемента.

$(2 \to 1)$ Из второго условия следует первое.

Если подмножество B в множестве A не имеет минимального элемента, то мы можем выбрать в B бесконечную строго убывающую последовательность элементов a_k, где элемент a_0 произвольный и для любого натурального n элемент a_{n+1} строго меньше элемента a_n.

$(1 \to 3)$ Из первого условия следует третье.

Пусть выполняется первое условие. Предположим, что для множества M и любого элемента a из A верна импликация, записанная в третьем условии. Тогда множество M совпадает с A, так как иначе разность $A \setminus M$ является непустым множеством без минимального элемента. Таким образом, выполняется третье условие.

$(3 \to 1)$ Из третьего условия следует первое.

Пусть выполнено третье условие и подмножество $B \subseteq A$ без минимального элемента. Тогда по-индукции можно доказать, что множество $M = B \setminus A$ совпадает с A и, таким образом, B пусто. Этим доказывается, что из третьего условия следует первое. $\square$

Частично упорядоченное множество, для которого выполняются условия этой теоремы, называется *фундированным*. Фундированное линейно упорядоченное множество называется *вполне* или *полностью упорядоченным*; соответствующий порядок называется *полным*. Имеет место

Следствие. *Частично упорядоченное множество фундировано, если и только если каждая его цепь вполне упорядочена (индуцированным упорядочением).*

Доказательство. Необходимость следует по условию минимальности, достаточность — по условию обрыва убывающих цепей.

Примеры.

$\circ$ Словарно упорядоченное произведение $A \times B$ фундированных множеств A, B фундированно. Действительно, рассмотрим убывающую последовательность

$$(a_0 b_0) \geqslant (a_1 b_1) \geqslant (a_3 b_3) \geqslant \dots .$$

Ясно, что последовательность первых компонент убывает:

$$a_0 \geqslant a_1 \geqslant a_2 \geqslant \dots .$$

Так как множество A фундированное, эта последовательность стабилизируется, то есть

$$a_m = a_{m+1} = a_{m+2} = \dots$$

для некоторого натурального m. Ясно, что последовательность вторых компонент убывает с номера m:

$$b_m \geqslant b_{m+1} \geqslant b_{m+2} \geqslant \dots .$$

Эта последовательность также должна стабилизироваться. Но тогда и исходная последовательность пар стабилизируется. □

∘ В частности, множества $\mathbb{N}^2, \mathbb{N}^3, \ldots$ вполне упорядочены словарным упорядочением.

Упражнение. Пусть имеется двоичный набор. Найдём в нём пару рядом стоящих чисел 01 и заменим набором $10\ldots0$ произвольной длины. Докажите, что подобные действия невозможно совершать бесконечно долго. Эта задача — из книги Н. К. Верещагина и А. Шеня «Начала теории множеств».

Теорема. *Пусть A — фундированное множество и для любого его элемента a задана функция $g_a : Y^{[A,a)} \to Y$. Тогда существует единственная функция $f : A \to Y$, такая, что для всех a из A выполняется равенство $f(a) = g_a(f_{[A,a)})$.*

Напомним, что $Y^{[A,a)}$ — это множество всех функций $h : [A, a) \to Y$. Через $f_{[A,a)}$ выше обозначено ограничение $f \cap ([A, a) \times Y)$.

ГЛАВА 4

Мощность множества

В главе изучается отношение равномощности и отношение «меньше или равно» для мощностей. Определяются счётные и несчётные множества. Вводятся операции над мощностями.

1. Равномощность

Будем говорить, что множества A, B равномощны, или имеют одну мощность, если между ними существует биекция. Договоримся писать $|A| = |B|$ в этом случае. Отношение равномощности определено корректно и является эквивалентностью на любом множестве множеств.

Слово «мощность» можно употреблять как словесную конструкцию, заменяющую более длинное объяснение. Вместе с тем, можно рассматривать мощности как самостоятельные объекты, сопоставленные множествам. В этом случае мощности называются обычно *кардинальными числами*. Скажем, в аксиоматической теории Гёделя и Бернайса кардинальными числами можно считать классы равномощных множеств. Если в каждом классе выбрать по представителю, то эти представители могут считаться кардинальными числами в аксиоматической теории Цемело и Френкеля.

Примеры.

∘ Множества $\mathcal{P}(A)$ и 2^A равномощны, так как существует биекция

$$\mathcal{P}(A) \to 2^A, B \mapsto \chi_B, \text{ где } \chi_B(a) = 1 \Leftrightarrow a \in B.$$

Здесь $a \in A$ и $B \subseteq A$.

∘ Множества $\mathrm{Eq}(A)$ и $\mathrm{Part}(A)$ равномощны, так как имеется биекция

$$\mathrm{Eq}(A) \to \mathrm{Part}(A), \alpha \mapsto A/\alpha.$$

∘ Множества натуральных и чётных натуральных чисел равномощны в силу биекции

$$\mathbb{N} \to 2\mathbb{N}, x \mapsto 2x.$$

Упражнения. Докажите следующие утверждения.

∘ Конечное множество не равномощно собственной части.

∘ Пусть A — произвольное множество. Функция

$$\alpha : \mathbb{N} \to A, \alpha : n \mapsto \alpha_n$$

называется (бесконечной) последовательностью элементов множества A. Обычно последовательность записывается как

$$\alpha = \alpha_0\alpha_1\dots.$$

Множество всех таких последовательностей обозначается $A^{\mathbb{N}}$.

Докажите, что множества $[\mathbb{N},2)^{\mathbb{N}}$ и $[\mathbb{N},4)^{\mathbb{N}}$ равномощны.

∘ Множества $[\mathbb{N},2)^{\mathbb{N}}$ и $[\mathbb{N},3)^{\mathbb{N}}$ равномощны.

2. Сравнение множеств по мощностям

Говорят «мощность множества A меньше или равна мощности множества B» и пишут $|A| \leqslant |B|$, если множество A равномощно части множества B. Отношение «меньше или равно» (для мощностей) определено корректно (проверьте).

Теорема Кантора-Бернштейна. *Отношение «меньше или равно» антисимметрично для мощностей.*

Иными словами, для любых множеств A, B верно:

$$|A| = |B|, \text{ если } |A| \leqslant |B| \text{ и } |B| \leqslant |A|.$$

Доказательство. Пусть имеются инъективные отображения

$$f : A \to B, g : B \to A.$$

Рассмотрим последовательность:

$$\dots x_k \mapsto x_{k+1} \mapsto x_{k+2} \mapsto \dots.$$

Здесь элементы взяты из чередующихся множеств A, B и стрелки суть чередующиеся отображения f, g. Для любого элемента этой последовательности элементы, стоящие левее, назовём его предшественниками. Заметим, что для любого элемента множество его предшественников определено однозначно. Тогда множества A, B распадаются на непересекающиеся подмножества:

$$A = A_0 \sqcup A_1 \sqcup A_\infty, B = B_0 \sqcup B_1 \sqcup B_\infty,$$

где индексами $0, 1, \infty$ отмечены подмножества, состоящие из элементов с чётным, нечётным и бесконечным числом предшественников. Легко понять, что функция

$$h : A \to B, h : a \mapsto \begin{cases} f(a) & \text{для } a \in A_0 \sqcup A_\infty, \\ g^{-1}(a) & \text{для } a \in A_1; \end{cases}$$

определена корректно и является биекцией. □

Упражнение. Множества $[\mathbb{N},k)^{\mathbb{N}}$, где $k \geqslant 2$, равномощны.

3. Счётное множество

Множество, равномощное множеству натуральных чисел, называется *счётным*. Иными словами, для счётного множества A существует биекция $\alpha : A \to \mathbb{N}$, которая элементам множества сопоставляет натуральные номера, а также биекция $\beta : \mathbb{N} \to A$, которая выдаёт элемент по номеру.

Теорема (о счётных множествах). *Верны утверждения.*

(I) *Подмножество счётного множества конечное или счётное.*

(II) *Бесконечное множество содержит счётное подмножество.*

(III) *Счётное объединение счётных множеств счётное.*

Доказательство. Докажем первое утверждение. Достаточно доказать, что бесконечное подмножество $A \subseteq \mathbb{N}$ счётное. Для этого рассмотрим последовательность элементов a_k, определённых по индукции для любого натурального номера k так, что элемент a_k — минимальный в множестве $A \setminus \{a_0, \ldots, a_{k-1}\}$. Данная последовательность содержит все элементы из A и функция

$$\mathbb{N} \to A, k \to a_k$$

является биекцией. Следовательно множество A счётное. Таким образом, первое утверждение доказано.

Докажем второе утверждение. Пусть B — бесконечное множество. Определим последовательность элементов b_k, где, для любого натурального номера k, b_k — произвольный элемент в множестве $B \setminus \{b_0, \ldots, b_{k-1}\}$. Тогда образ функции

$$\mathbb{N} \to B, k \to b_k,$$

является счётным подмножеством в B и второе утверждение доказано.

Пусть для каждого натурального n задано счётное множество A_n, состоящее из элементов $a_{n0}, a_{n1}, \ldots$. Элементы этих множеств запишем в таблицу

$$a_{00}, a_{01}, a_{02}, \ldots$$
$$a_{10}, a_{11}, a_{12}, \ldots$$
$$a_{20}, a_{21}, a_{22}, \ldots.$$

Выписывая элементы на диагоналях, получаем последовательность

$$a_{00}, a_{01}, a_{10}, a_{02}, a_{11}, a_{20}, \ldots.$$

Каждому элементу сопоставим номер его первого вхождения в эту последовательность. Тем самым установлено взаимно однозначное соответствие между объединением множеств A_n и бесконечным подмножеством натурального ряда. В силу первого утверждения это подмножество счётное. Теорема доказана. □

Пример.

∘ Декартово произведение двух счётных множеств счётное, так как

$$A \times B = \cup_{a \in A} \{a\} \times B.$$

∘ Декартово произведение $n > 0$ счётных множеств счётное.

∘ Множество A^* всех слов в счётном алфавите A счётное, так как является счётным объединением счётных множеств:

$$A^* = \cup_n A^n.$$

∘ Множество целых чисел счётное, так как $\mathbb{Z} = (-\mathbb{N}) \cup \mathbb{N}$.

∘ Множество рациональных чисел счётное.

∘ Алгебраическим числом называется комплексный корень многочлена с рациональными коэффициентами. Множество алгебраических чисел счётное.

Упражнения. Докажите следующие утверждения.

∘ Бесконечное множество равномощно некоторому собственному подмножеству.

∘ $|A \cup B| = |A|$, если A — бесконечное и B — конечное или счётное.

∘ $|A \setminus B| = |A|$, если A — несчётное бесконечное и B — конечное или счётное.

4. Несчётное множество

Имеет место

Теорема Кантора. *Для любого множества A верно*

$$|A| \neq |\mathcal{P}(A)|.$$

Доказательство. Никакая функция $\xi : A \to \mathcal{P}(A)$ не может быть сюръективной, так как множество

$$M = \{m | m \in A, m \notin \xi(m)\}$$

не является образом. (Проверьте.) □

Следствие. *Множество $\mathcal{P}(\mathbb{N})$ несчётное.* □

Упражнение. Докажите, что для любого натуральноого числа $k \geqslant 2$ функция $A \to [\mathbb{N}, k)^A$ не может быть сюръективной.

Множество, равномощное $\mathcal{P}(\mathbb{N})$, называется множеством *мощности континуума*. Например, прямая (множество действительных чисел) и любой отрезок на прямой имеют такую мощность.

5. Операции над мощностями

Пусть α, β — мощности непересекающихся множеств A, B. Корректными являются следующие определения:

$$\alpha + \beta = |A \sqcup B|, \alpha \cdot \beta = |A \times B|, \alpha^\beta = |A^B|.$$

Отметим следующие свойства операций над мощностями:

- $\alpha + \beta = \beta + \alpha$, $\alpha \cdot \beta = \beta \cdot \alpha$;
- $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$, $\alpha \cdot \beta\gamma = \alpha\beta \cdot \gamma$;
- $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$;
- $\alpha^{\beta+\gamma} = \alpha^\beta \alpha^\gamma$
- $\alpha^{\beta\gamma} = (\alpha^\beta)^\gamma$;
- $(\alpha\beta)^\gamma = \alpha^\gamma \beta^\gamma$;
- $\alpha + \beta \leqslant \alpha + \gamma$ *и* $\alpha \cdot \beta \leqslant \alpha \cdot \gamma$, *если* $\beta \leqslant \gamma$;
- $\alpha^\beta \leqslant \alpha^\gamma$ *и* $\beta^\alpha \leqslant \gamma^\alpha$, *если* $\beta \leqslant \gamma$.

Здесь α, β, γ — произвольные мощности.

Упражнение. Докажите корректность сделанных определений и записанных свойств.

С использованием записанных равенств можно получать новые соотношения для мощностей. Рассмотрим соответствующий

Пример. Имеют место соотношения для мощностей:

$$\mathfrak{c} \leqslant \mathfrak{c}^2 = 2^{2\aleph_0} = 2^{\aleph_0} = \mathfrak{c}, \text{ откуда } \mathfrak{c} = \mathfrak{c}^2;$$

$$2^{\mathfrak{c}} \leqslant \aleph_0^{\mathfrak{c}} \leqslant \mathfrak{c}^{\mathfrak{c}} = 2^{\aleph_0 \mathfrak{c}} \leqslant 2^{\mathfrak{c}^2} = 2^{\mathfrak{c}}, \text{ откуда } 2^{\mathfrak{c}} = \aleph_0^{\mathfrak{c}} = \mathfrak{c}^{\mathfrak{c}};$$

$$\mathfrak{c}^{\aleph_0} = 2^{\aleph_0^2} = 2^{\aleph_0} = \mathfrak{c}.$$

Здесь использовались обычные обозначения: $\aleph_0 = |\mathbb{N}|$ и $\mathfrak{c} = |\mathcal{P}(\mathbb{N})|$.

Упражнение. Объясните приведённые соотношения.

ГЛАВА 5

Вполне упорядоченное множество

В этой главе изучаются вполне упорядоченные множества.

1. Теорема Цермело и лемма Цорна

Аксиома выбора имеет ряд переформулировок. Вот некоторые из них.

Теорема. *Следующие четыре утверждения равносильны.*

(1. Аксиома выбора.) *Для любого непустого множества M существует «функция выбора»*

$$\varphi : \mathcal{P}(M) \setminus \{\emptyset\} \to M, \text{ такая, что } \varphi(A) \in A$$

для любого непустого подмножества A множества M.

(2. Теорема Цермело.) *Всякое непустое множество можно вполне упорядочить.*

(3. Теорема Хаусдорфа.) *Всякая цепь частично упорядоченного множества содержится в максимальной цепи.*

(Цепью называется подмножество частично упорядоченного множества, линейно упорядоченное индуцированным порядком.)

(4. Лемма Цорна.) *Частично упорядоченное множество содержит максимальный элемент, если в нём каждая цепь имеет верхнюю грань.*

Доказательство. Докажем последовательно ряд импликаций.

$(1 \to 2)$ Аксиома выбора влечёт теорему Цермело.

Пусть M — множество и в каждом его непустом подмножестве A выбран элемент $\phi(A)$. Подмножество A назовём *отмеченным*, если его можно полностью упорядочить некоторым отношением $\leqslant$, так, что

$$a = \phi(M \setminus [A, a))$$

для любого a из A. Например, отмеченным является множество $A = \{\phi(M)\}$, так как $[A, \phi(M)) = \emptyset$ и, следовательно, $\phi(M) = \phi(M \setminus [A, a))$.

Заметим, что элемент $\phi(M)$ является наименьшим в любом отмеченном множестве. В частности, любые два отмеченных множества имеют общее начало и тогда имеют наибольшее общее начало (равное объединению всех общих начал). Наибольшее общеее начало C произвольных двух отмеченных множеств A, B совпадает с одним из них, так как в противном

случае

$$C = [A, a) = [B, b) \text{ для некоторых } a \text{ и } b,$$

$$a = \phi(M \setminus C) = b$$

и тогда $C \cup \{\phi(M \setminus C)\}$ — большее общее начало. Таким образом, для любых двух отмеченных множеств одно является начальным отрезком другого. Далее следует проверить, что объединение отмеченных множеств является отмеченным множеством (проверьте это самостоятельно) и совпадает со всем множеством M (иначе его можно расширить элементом из дополнения). Требуемая импликация доказана.

$(2 \to 3)$ Теорема Цермело влечёт теорему Хаусдорфа.

Пусть теорема Цермело имеет место и A — цепь частично упорядоченного множества M, отличная от него самого. По теореме Цермело множество $B = M \setminus A$ можно вполне упорядочено некоторым отношением $\leqslant$. Выделим в нём подмножество B' следующим образом. Наименьший элемент множества B (относительно полного упорядочения $\leqslant$) отнесём к множеству B', если он сравним (по отношению порядка, заданному в M) со всеми элементами цепи A и далее, по индукции, произвольный элемент b из B отнесём к B', если он сравним по упорядочению в M со всеми элементами цепи A и всеми элементами отрезка $[B, b)$, ранее отнесёнными к B'. (Отрезок определён относительно полного упорядочения $\leqslant$, введённого в множестве B.) Тогда $A \cup B'$ является максимальной цепью в B и требуемая импликация доказана.

$(3 \to 4)$ Теорема Хаусдорфа влечёт лемму Цорна.

Предположим, теорема Хаусдорфа выполняется и для частично упорядоченного множества M выполняется условие леммы Цорна. В этом случае верхняя грань максимальной цепи является максимальным элементом частично упорядоченного множества M и требуемая импликация доказана.

$(4 \to 1)$ Лемма Цорна влечёт аксиому выбора.

Предположим, выполняется лемма Цорна и M — непустое множество. Будем рассматривать функции выбора, определённые на системах подмножеств множества M. Множество всех таких функций упорядочим, положив $\phi \leqslant \psi$ для функций ϕ и ψ, определённых на системах S и T, таких, что $S \subseteq T$, и совпадающих на системе S. По лемме Цорна существует максимальная функция выбора. Она определена на всех непустых подмножествах множества M. Тогда имеет место аксиома выбора. Теорема доказана.

Приведём пример использования леммы Цорна.

Пример. Любой частичный порядок можно продолжить до линейного.

Действительно. Пусть на множестве A задано отношение частичного порядка. Рассмотрим множество всех частичных порядков на A, включающих это отношение. Это множество, упорядоченное включением, удовлетворяет условиям леммы Цорна: в качестве верхней грани нужно взять объединение цепи. Максимальный по включению порядок здесь является искомым линейным порядком. □

2. Порядковый тип

Подмножество вполне упорядоченного множества называется *начальным отрезком*, если вместе с любым своим элементом оно содержит все меньшие элементы. Во вполне упорядоченном множестве A собственный (отличный от всего множества) начальный отрезок имеет вид $[A, a)$ для некоторого элемента a (почему?).

Будем говорить, что вполне упорядоченные множества A, B имеют один порядковый тип и писать

$$\mathrm{o}(A) = \mathrm{o}(B),$$

если между ними существует изоморфизм. Будем писать

$$\mathrm{o}(A) \leqslant \mathrm{o}(B)$$

и говорить, что порядковый тип множества A меньше или равен порядковому типу множества B, если существует изоморфизм упорядоченных множеств, отображающий множество A на начальный отрезок в B.

Можно пользоваться словами «порядковый тип» как фигурой речи, заменяющей более длинное объяснение. Но можно считать порядковые типы отдельными объектами, совпадающими с классами изоморфных вполне упорядоченных множеств или совпадающие с выбранными представителями этих классов. В этом смысле порядковые типы называются также порядковыми (или ординальными) числами. Имеет место

Теорема. *Порядковые типы вполне упорядочены отношением «меньше или равно».*

Доказательство. Рассмотрим отношение $\leqslant$ для порядковых типов. Очевидно, оно рефлексивно и транзитивно. Докажем последовательно, что оно антисимметрично и, следовательно, является порядком, что этот порядок линейный и полный.

∘ Отношение $\leqslant$ антисимметрично, является отношением порядка.

Пусть $\phi : A \to A$ строго монотонное отображение вполне упорядоченного множества A в себя. Свойство строгой монотонности означает,

что

$$\phi(x) < \phi(y), \text{ если } x < y$$

для любых элементов x, y из A. Тогда в A для любого элемента x выполняется неравенство

$$x \leqslant \phi(x),$$

так как в противном случае в A можно было бы найти наименьший элемент x со свойством $\phi(x) < x$; тогда $\phi^2(x) < \phi(x) < x$, что противоречит условию минимальности элемента x. Так как изоморфизм вполне упорядоченных множеств обладает свойством строгой монотонности, сказанное выше также означает, что не существует изоморфизма $\phi : A \to [A, a)$ (так как у a нет образа). Отсюда следует, что отношение $\leqslant$ антисимметрично для порядковых типов. Действительно, пусть A', B' — начальные отрезки вполне упорядоченных множеств A, B, таких, что

$$\mathrm{o}(B) \leqslant \mathrm{o}(A), \mathrm{o}(A) \leqslant \mathrm{o}(B).$$

Тогда произведение соответствующих изоморфизмов $A \to B'$, $B \to A'$ должно быть изоморфизмом, отображающим A на себя, начальные отрезки A', B' не могут быть собственными, верно равенство $\mathrm{o}(A) = \mathrm{o}(B)$.

∘ Отношение $\leqslant$ является отношением линейного порядка.

Требуется доказать, что для любых вполне упорядоченных множеств A, B одно изоморфно начальному отрезку другого. Пусть $*$ — элемент, не принадлежащий множеству B. Рассмотрим отображение

$$\phi : A \to B \cup \{*\},$$

такое, что для любого элемента a из A верно следующее:

$$\phi(a) = \begin{cases} \inf B \setminus \phi[A, a), & \text{если } B \setminus \phi[A, a) \neq \emptyset, \\ *, & \text{противном случае.} \end{cases}$$

Здесь

$$\phi[A, a) = \{\phi(a') | a' \in [A, a)\}.$$

Заметим, что множества

$$A' = \{a | \phi(a) \neq *\}, \phi A' = \{\phi(a) | a \in A'\}$$

являются начальными отрезками в множествах A, B и функция ϕ устанавливает между ними изоморфизм. Осталось проверить, что включения $A' \subseteq A, \phi A' \subseteq B$ не могут быть оба строгими.

∘ Отношение $\leqslant$ является отношением полного порядка.

Пусть имеется семейство вполне упорядоченных множеств. Нужно доказать, что в семействе найдётся множество, изоморфное начальному отрезку каждого из множеств. Пусть A — произвольное множество из

семейства. Если оно не обладает требуемым свойством, то в силу предыдущего свойства некоторый его собственный начальный отрезок $[A, a)$ изоморфен какому-то множеству B из семейства. Выберем такое наименьшее a. Тогда соответствующее ему множество B обладает требуемым свойством.

Все нужные свойства доказаны. □

Следствие. *Любое множество кардинальных чисел вполне упорядочено отношением* $\leqslant$. □

3. Свойства бесконечных мощностей

Имеет место

Теорема. *Пусть* α, β *— бесконечные мощности. Имеют место следующие утверждения.*

(I) $\alpha \cdot \aleph_0 = \alpha$.

(II) $\alpha + \beta = \max\{\alpha, \beta\}$, *в частности,* $\alpha + \alpha = \alpha$.

(III) $\alpha \cdot \beta = \max\{\alpha, \beta\}$, *в частности,* $\alpha \cdot \alpha = \alpha$.

Доказательство. Пусть A, B — множества мощностей α, β. Докажем первое утверждение. Полностью упорядочим множество A. Его элемент a назовём *предельным*, если в начальном отрезке $[A, a)$ нет наибольшего элемента. Пусть L — множество предельных элементов. Заметим, что в нём для любых соседних предельных элементов b, c (таких, что не существует предельного элемента d между ними, удовлетворяющего условию $b < d < c$) отрезок $[b, c) = \{a | a \in A, b \leqslant a < c\}$ изоморфен натуральному ряду, а для наибольшего предельного элемента b отрезок $[b, A] = \{a | a \in A, b \leqslant a\}$ изоморфен начальному отрезку натурального ряда. Отсюда следует, что

$$\alpha = |L| \cdot \aleph_0 = |L| \cdot \aleph_0 \cdot \aleph_0 = \alpha \cdot \aleph_0.$$

Первое утверждение доказано. Докажем второе. Пусть $\alpha \leqslant \beta$. Тогда

$$\beta \leqslant \alpha + \beta \leqslant \beta + \beta \leqslant \beta \cdot \aleph_0 = \beta \text{ и } \alpha + \beta = \beta = \max\{\alpha, \beta\}.$$

Второе утверждение доказано. Докажем третье. Пусть, по-прежнему, $\alpha \leqslant \beta$. Нужно доказать, что $\beta^2 = \beta$, так как тогда

$$\beta \leqslant \alpha \cdot \beta \leqslant \beta \cdot \beta = \beta \text{ и } \alpha \cdot \beta = \beta = \max\{\alpha, \beta\}.$$

Отметим, что в множестве B имеются подмножества, равномощные своим квадратам. (Например, счётные подмножества обладают этим свойством.) Систему всех таких подмножеств упорядочим, считая $C \leqslant D$, если $C \subseteq D$ и биекцию между множеством C и его квадратом можно продолжить до биекции между множеством D и его квадратом. Упорядоченная так

система подмножеств удовлетворяет условиям леммы Цорна и содержит максимальное подмножество C. Если $|C| = \beta$, то доказывать нечего. В противном случае, $|C| < \beta$ и

$$\beta = |B| = |C \sqcup (B \setminus C)| = |C| + |B \setminus C| = \max\{|C|, |B \setminus C|\} = |B \setminus C|.$$

Стало быть, существует равномощное C подмножество $C_0 \subseteq B \setminus C$. Заметим, что множество

$$(C \cup C_0)^2 \setminus C^2 = C_0^2 \cup (C \times C_0) \cup (C_0 \times C)$$

равномощно множествам C_0^2, C_0. В частности, существует биекция между множеством C_0 и записанным выше множеством. Её можно продолжить до биекции между множеством $C \cup C_0$ и его квадратом (посредством биекции между множествами C, C^2). Это противоречит максимальности множества C. Полученное противоречие доказывает третье утверждение. Теорема полностью доказана.

Следствие. *Имеют место следующие утверждения.*

(I) *Множество всех слов в бесконечном алфавите равномощно алфавиту.*

(II) *Бесконечное множество равномощно множеству всех его конечных подмножеств.*

Доказательство. Второе утверждение является следствием первого. Докажем первое. Пусть A — бесконечное множество. Тогда $|A^n| = |A|$ для любого натурального $n > 0$ в силу доказанной теоремы. Используя это, получаем:

$$|A^*| = 1+|A|+|A|^2+\ldots = 1+|A|+|A|+\ldots = 1+|A|\cdot\aleph_0 = 1+|A| = |A|. \square$$

ГЛАВА 6

Подстановки

В этой главе изучаются подстановки, заданные на конечном множестве.

1. Умножение подстановок

Подстановкой на множестве X называется биекция $\alpha : X \to X$. Будем рассматривать далее подстановки на конечном множестве X. Их множество обозначается S_X, а также S_n, если X состоит из чисел $1, \ldots, n$. Отметим основные свойства умножения подстановок.

◦ *Произведение подстановок является подстановкой.*

◦ *Умножение подстановок ассоциативно: для любых подстановок α, β, γ имеет место равенство*

$$\alpha \cdot \beta\gamma = \alpha\beta \cdot \gamma. \square$$

◦ *Тождественное отображение*

$$\mathrm{id}_X : X \to X, x \mapsto x,$$

является подстановкой. Для любой подстановки α верно:

$$\alpha\, \mathrm{id}_X = \mathrm{id}_X\, \alpha = \alpha. \square$$

◦ *Для любой подстановки α существует единственная обратная подстановка α^{-1}, такая, что*

$$\alpha\alpha^{-1} = \alpha^{-1}\alpha = \mathrm{id}_X\,. \square$$

◦ *Для любых подстановок α, β, γ выполняются законы сокращения:*

$$\alpha = \beta, \text{ если } \alpha\gamma = \beta\gamma \text{ или } \gamma\alpha = \gamma\beta. \square$$

Подстановку на конечном множестве X можно задать таблицей из двух строк, где в первой строке записаны элементы множества X, а во второй — их образы. Другой способ задания, связанный с разложением на циклы, рассматривается далее.

2. Разложение на циклы

Неподвижные и мобильные элементы. Пусть α — подстановка на множестве X. Элемент a из X, который отображается на себя подстановкой α, называется её неподвижным элементом. Элемент, который

отображается на отличный от него элемент, называется мобильным. Подстановки без общих мобильных элементов называются независимыми. Отметим следующее свойство.

∘ *Независимые подстановки перестановочны.* □

Теорема о разложении. Подстаноку β назовём *циклом* длины k, где k — целое положительное число, если она отображает циклически друг на друга какие-то k различных элементов множества X и оставляет неподвижными остальные элементы, иными словами

$$\beta : x_1 \mapsto x_2 \mapsto \ldots \mapsto x_k \mapsto x_1$$

для некоторых различных элементов $x_1, \ldots, x_k$ из X и

$$\beta : x \mapsto x$$

для любого элемента x из X, отличного от элементов $x_1, \ldots, x_k$. Подстановка β в этом случае обозначается следующим образом:

$$(x_1, x_2, \ldots, x_k).$$

Цикл единичной длины по определению — тождественная подстановка.

Теорема (о разложении). *Подстановку на конечном множестве можно представить в виде произведения независимых циклов.*

Подобное представление единственно с точностью по порядка сомножетелей и с точностью до циклов длины один.

Теорема будет доказана позднее.

Порядок подстановки. Положим $\alpha^0 = \mathrm{id}_X$ и по индукции $\alpha^{n+1} = \alpha\alpha^n$ для любого натурального n. Пусть также $\alpha^{-n} = (\alpha^n)^{-1}$. Отметим пару свойств.

∘ *Для подстановки α на конечном множестве X существует положительное число n, такое, что $\alpha^n = \mathrm{id}_X$.* (Наименьшее такое n называется *порядком* подстановки α.)

Доказательство. В последовательности

$$\alpha, \alpha^2, \alpha^3, \ldots$$

должны быть повторения, то есть существуют положительные $i < j$, такие, что $\alpha^i = \alpha^j$. Наименьшее такое i равно 1 в силу закона сокращения. Тогда число $n = j - i$ положительное и $\alpha^n = \alpha^j\alpha^{-i} = \mathrm{id}$. □

∘ *Для элементов a, b из X и подстановки α из S_X следующие условия равносильны:*

(1) *для некоторого целого числа n выполняется равенство $a\alpha^n = b$;*

(2) *для некоторого натурального n выполняется равенство $a\alpha^n = b$.*

Доказательство. Достаточно заметить, что степени α^k, α^m подстановки α совпадают, если показатели k, m отличаются слагаемым, кратным её порядку. □

Элементы a, b, удовлетворяющие условиям (1,2), назовём эквивалентными для подстановки α.

Орбиты. Введённое отношение действительно является эквивалентностью на множестве X. Классы этой эквивалентности называются *орбитами* подстановки α. Иными словами, орбита с элементом a состоит из элементов $a\alpha^n$, где n — произвольное натуральное число. Отметим ряд свойств.

∘ *Орбиты подстановки α разбивают множество X.* □

∘ *Подстановка индуцирует цикл длины k на k-элементной орбите.*

Доказательство почти полностью повторяет доказательство первого свойства в предыдущем разделе. В последовательности

$$x\alpha, x\alpha^2, x\alpha^3, \ldots$$

содержатся все элементы орбиты и должны быть повторения, то есть существуют положительные $i < j$, такие, что $x\alpha^i = x\alpha^j$. Наименьшее такое i равно 1 в силу инъективности α. При этом j совпадает с числом элементов в орбите элемента x. □

Цикл, о котором говорится в последнем свойстве, продолжим тождественно до цикла на всём множестве X, и назовём его тогда *циклом подстановки α* (связанным с соответствующей орбитой).

∘ *Подстановка на конечном множестве является произведением своих циклов.*

Доказательство. Непосредственно видно, что подстановка и произведение её циклов одинаково действуют на элементы из X. □

Доказательство теоремы о разложении. Возможность разложения установлена выше. С другой стороны, если подстановка каким-то образом разложена в произведение независимых циклов, то элементы каждого цикла составляют отдельную орбиту. Следовательно, данное разложение совпадает с разложением в произведение независимых циклов, связанных с орбитами. □

Упражнение. Докажите следующие утверждения.

∘ Число элементов орбиты делит порядок подстановки.

∘ Порядок подстановки равен наименьшему общему кратному мощностей орбит.

3. Транспозиции и декремент

Цикл длины два называется *транстпозицией*. Иными словами, это подстановка (i, j), которая элементы i, j отображает друг на друга, а остальные элементы оставляет на месте.

Пусть подстановка α на n-элементном множестве X имеет m независимых циклов, тогда её *декрементом* называется число

$$\operatorname{dec}(\alpha) = n - m.$$

Примеры.

∘ Тождественная подстановка имеет минимально возможный декремент, равный нулю.

∘ Цикл длины n имеет максимальный декремент, равный $n - 1$.

Теорема. *Подстановку на конечном множестве можно представить в виде произведения транспозиций с числом сомножителей, равным её декременту.*

(Считаем, что тождественная подстановка представляется произведением без сомножителей.)

Доказательство. Заметим, что цикл длины k можно представить в виде произведения $k - 1$ транспозиции:

$$(a_1, \ldots, a_k) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_k).$$

Пусть далее подстановка содержит l_k независимых циклов длины k (где $1 \leqslant k \leqslant n$). Запишем её в виде произведения независимых циклов, а затем независимые циклы представим в виде произведения транспозиций, как указано выше. Получим представление подстановки в виде произведения транспозиций с числом сомножителей

$$\sum_k (k-1) l_k = \sum_k k l_k - \sum_k l_k = n - m.$$

Теорема доказана. □

Замечание. Разложение подстановки в произведение транспозиций не однозначно; более того, число сомножителей в различных разложениях может не совпадать. Например,

$$(13)(12) = (132) = (123)(123) = (12)(13)(12)(13).$$

Следующая теорема говорит о возможном числе сомножителей.

Теорема. *Пусть подстановка α на конечном множестве разложена в произведение транспозиций. Тогда число сомножителей в этом разложении равно* $\operatorname{dec}(\alpha) + 2q$ *для некоторого натурального q.*

Доказательство. Ключевым является следующее наблюдение: при умножении подстановки на транспозицию слева её декремент изменяется на 1. Он уменьшается на 1, если элементы транспозиции попадают в один цикл подстановки, либо увеличивается на единицу, в противном случае. Это так в силу соотношений

$$(i_1, j_1)(i_1, i_2, \dots, i_m)(j_1, j_2, \dots, j_n) = (j_1, i_2, \dots, i_m, i_1, j_2, \dots, j_n),$$

$$(i_1, j_1)(j_1, i_2, \dots, i_m, i_1, j_2, \dots, j_n) = (i_1, i_2, \dots, i_m)(j_1, j_2, \dots, j_n).$$

Пусть теперь $\tau_1, \tau_2, \dots$ — произвольные транспозиции и

$$\alpha_N = \tau_N \dots \tau_1;$$

в том числе $\alpha_0 = \mathrm{id}_X$. Тогда, используя сформулированное свойство, можно записать последовательно

$$\begin{aligned} \mathrm{dec}(\alpha_N) &= \mathrm{dec}(\alpha_{N-1}) \pm 1 \\ &= \mathrm{dec}(\alpha_{N-2}) \pm 1 \pm 1 \\ &\dots \\ &= \mathrm{dec}(\alpha_0) \pm 1 \pm 1 \dots \pm 1 \\ &= \pm 1 \pm 1 \dots \pm 1, \end{aligned}$$

где количество членов в последнем выражении равно N и каждый входит с тем или иным знаком. Обозначив буквой q число положительных слагаемых здесь, получим

$$\mathrm{dec}(\alpha_N) = (N - q) - q, \text{ откуда } N = \mathrm{dec}(\alpha_N) + 2q.$$

Теорема доказана. □

4. Инверсии и транспозиции соседних элементов

Пусть конечное множество X линейно упорядочено отношением $\leqslant$. Можно считать для простоты, что оно состоит из чисел $1, \dots, n$, упорядоченных естественно. *Инверсией* подстановки α назовём пару $\{i, j\}$ элементов из X, где $i < j$ и $i\alpha > j\alpha$. Число инверсий обозначим через $\mathrm{inv}(\alpha)$.

Упражнение. Транспозицией соседних элементов будем называть транспозицию (i, j), где элемент j непосредственно следует за элементом i в частично упорядоченном множестве X. Убедитесь, что при умножении подстановки на транспозицию (i, j) соседних элементов число инверсий изменяется на 1. Оно уменьшается на 1, если пара $\{i, j\}$ является инверсией подстановки, либо увеличивается на 1 в противном случае.

Теорема. *Подстановку на конечном линейно упорядоченном множестве можно представить в виде произведения транспозиций соседних*

элементов с числом сомножителей, совпадающим с числом инверсий подстановки.

Если подстановка α разложена в произведение транспозиций соседних элементов, то число сомножителей в этом разложении равно $\mathrm{inv}(\alpha) + 2q$ для некоторого натурального числа q.

Доказательство теоремы опирается на последнее упражнение. Станем умножать подстановку α слева на транспозиции соседних элементов τ_1, τ_2, ..., выбирая очередную подстановку τ_k так, чтобы число инверсий в произведении

$$\tau_k \cdots \tau_1 \alpha$$

постоянно убывало, пока это возможно, то есть пока не получим не имеющую инверсий тождественную подстановку

$$\mathrm{id}_X = \tau_k \cdots \tau_1 \alpha$$

при $k = \mathrm{inv}(\alpha)$. Возможность такого постоянного уменьшения числа инверсий гарантируется последним упражнением. Тогда

$$\alpha = \tau_1 \cdots \tau_k$$

и первая часть теоремы доказана. Вторая часть доказывается аналогично предыдущей теореме. □

Упражнение. Проведите доказательство теоремы подробно. Сформулируйте способ разложения подстановки в произведение транспозиций соседних элементов с минимальным числом сомножителей.

5. Чётные подстановки

Имеет место

Теорема. *Если подстановка на конечном множестве разложена в произведение транспозиций, то чётность числа сомножителей не зависит от разложения. Она совпадает с чётностью декремента и с чётностью числа инверсий подстановки.*

Доказательство следует из ранее доказанных теорем.

Для подстановки $\alpha = \tau_1 \cdots \tau_N$, где $\tau_1, \ldots, \tau_N$ — произвольные транспозиции, число

$$\mathrm{sign}\,\alpha = (-1)^{\mathrm{dec}\,\alpha} = (-1)^{\mathrm{inv}\,\alpha} = (-1)^N,$$

называется её *знаком*. Подстановка называется *чётной*, если её знак равен единице. Это означает, что чётными являются её декремент, число инверсий, а также число сомножителей в любом разложении в произведение транспозиций. У нечётной подстановки эти величины нечётные. Отметим следующие свойства.

∘ *Для любых подстановок* α, β *верно*

$$\operatorname{sign}\alpha\beta = \operatorname{sign}\alpha \operatorname{sign}\beta. \quad \square$$

∘ *В частности, произведение чётных подстановок является чётной подстановкой. Обратная подстановка для чётной сама чётная.* □

∘ *При* $n \geqslant 2$ *число чётных подстановок на* n*-элементном множестве совпадает с числом нечётных и равно* $n!/2$.

Доказательство. Пусть β — произвольная нечётная подстановка (например транспозиция). Отображение

$$R_\beta : S_X \to S_X, \alpha \mapsto \alpha\beta,$$

биективно отображает чётные подстановки на нечётные и наоборот. Следовательно, тех и других — одинаковое количество. □

ГЛАВА 7

Комбинаторные числа

В этой главе изучаются элементы комбинаторики.

1. Основные комбинаторные принципы

Пусть A, B — конечные множества. Следующие три свойства называются основными комбинаторными принципами или правилами.

∘ Правило суммы. $|A \sqcup B| = |A| + |B|$.

∘ Правило произведения. $|A \times B| = |A| \cdot |B|$.

∘ Принцип Дирихле. *Имеет место неравенство* $|A| \leqslant |B|$, *если существует инъективная функция* $A \to B$.

∘ *В частности,* $|A| = |B|$, *если существует биекция между* A *и* B.

Упражнение. Проверьте следующие свойства.

∘ $|A_1 \times A_2 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.

∘ $|A^n| = |A|^n$.

∘ $|\mathcal{P}(A)| = |2^A| = 2^{|A|}$.

∘ Пусть n птиц расположились на m ветках. Тогда на какой-то ветке располагаются не менее $\lceil n/m \rceil$ птиц, а на некоторой — не более $\lfloor n/m \rfloor$.

Воспользуемся основными комбинаторными принципами для подсчёта размещений, сочетаний и некоторых других комбинаторных объектов.

2. Размещения и сочетания

Будем рассматривать наборы длины k, составленные из элементов конечного множества A, содержащего n элементов. Набор, в котором все компоненты различные, называется *размещением из* n *по* k.

Теорема. *Пусть* $0 \leqslant k \leqslant n$. *Число размещений из* n *по* k *равно*

$$\frac{n!}{(n-k)!}.$$

Доказательство. Докажем это для произвольного фиксированного n индукцией по k. Это так при $k = 1$. Предположим, $k > 1$ и утверждение теоремы верно, если взять $k - 1$ вместо k. Разобьём все размещения на n непересекающихся классов, где в каждом классе находятся размещения с

одинаковым значением последней компоненты. Заметим, что размещения в каждом классе находятся во взаимно однозначном соответствии с размещениями из $n-1$ по $k-1$; по предположению индукции их

$$\frac{(n-1)!}{(n-1-(k-1))!} = \frac{(n-1)!}{(n-k)!}.$$

По принципу суммы общее число размещений равно

$$n\frac{(n-1)!}{(n-k)!} = \frac{n!}{(n-k)!}. \quad \square$$

Подмножество из k элементов в n-элементном множестве также называется *сочетанием из n по k*, их число обозначается $\binom{n}{k}$.

Очевидно, $\binom{n}{0} = \binom{n}{n} = 1$.

Теорема. *Пусть $0 \leqslant k \leqslant n$. Имеет место формула*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Доказательство. Размещения из n по k разобьем на не пересекающиеся классы, где в одном классе находятся размещения с одним и тем же множеством элементов. Ясно, что число классов равно $\binom{n}{k}$. Размещения в одном классе отличаются перестановкой компонент и находятся во взаимно однозначном соответствии с подстановками на k-элементном множестве (номеров компонент); их, следовательно, $k!$. По принципу суммы

$$\frac{n!}{(n-k)!} = \binom{n}{k} \cdot k!,$$

откуда следует доказываемая формула. $\square$

Продолжим изучение чисел сочетаний.

Теорема. Пусть $0 < k < n$. Имеет место соотношение

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Доказательство. В n-элементном множестве A выберем произвольно элемент a и все k–элементные подмножества разобьём на два класса: к одному классу отнесём подмножества, содержащие этот элемент, к другому — не содержащие его. Элементы первого класса находятся во взаимно однозначном соответствии с подмножествами множества $A \setminus \{a\}$ мощности $k-1$, их число есть $\binom{n-1}{k-1}$. Элементы второго класса находятся во взаимно однозначном соответствии с подмножествами мощности k множества $A \setminus \{a\}$, их число совпадает с $\binom{n-1}{k}$. Осталось воспользоваться принципом суммы. $\square$

Упражнение. Выведите рекуррентную формулу для сочетаний из явной формулы, и наоборот.

При помощи рекуррентной формулы можно последовательно находить значения биномиальных коэффициентов, располагая их в виде следующей треугольной таблицы:

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
\dots & & \dots & & \dots & & \dots & & \dots & & \dots & & \dots
\end{array}
$$

Подобная таблица называется «треугольник Паскаля».

Упражнение. Рассмотрим треугольную таблицу

$$
\begin{array}{ccccccccccccc}
 & & & & & & (0,0) & & & & & & \\
 & & & & & (1,0) & & (1,1) & & & & & \\
 & & & & (2,0) & & (2,1) & & (2,2) & & & & \\
 & & & (3,0) & & (3,1) & & (3,2) & & (3,3) & & & \\
\dots & & & & \dots & & \dots & & \dots & & & \dots &
\end{array}
$$

Докажите, что биномиальный коэффициент $\binom{k}{s}$ равен числу нисходящих путей в этой таблице, начинающихся в клетке $(0,0)$ и заканчивающихся в клетке (k,s). (В каждой клетке путь может продолжиться в одну из двух ближайших клеток, расположенных уровнем ниже.)

3. Биномиальная формула и обращение

Верна следующая

Теорема (биномиальная формула). *Для любого натурального n имеет место формула:*

$$(x+y)^n = \sum_{k\geqslant 0} \binom{n}{k} x^k y^{n-k}.$$

Доказательство. Предположим, это верно для некоторого n. Тогда

$$
\begin{aligned}
(x+y)^{n+1} &= (x+y)\cdot(x+y)^n \\
&= (x+y)\cdot \sum_{k\geqslant 0} \tbinom{n}{k} x^k y^{n-k} \\
&= \sum_{k\geqslant 0} \tbinom{n}{k} x^{k+1} y^{n-k} + \sum_{k\geqslant 0} \tbinom{n}{k} x^k y^{n-k+1}
\end{aligned}
$$

$$= \tbinom{n}{0}x^0y^{n+1} + \sum_{k\geqslant 1}[\tbinom{n}{k-1} + \tbinom{n}{k}]x^ky^{n-k+1}$$
$$= \tbinom{n+1}{0}x^0y^{n+1} + \sum_{k\geqslant 1}\tbinom{n+1}{k}x^ky^{n-k+1}$$
$$= \sum_{k\geqslant 0}\tbinom{n+1}{k}x^ky^{n+1-k}. \square$$

Следствие. *Для любого натурального n выполняется соотношение*

$$\sum_{k\geqslant 0}(-1)^k\binom{n}{k} = [n=0].$$

Доказательство. Данное соотношение получается с использованием биномиальной формулы, где нужно положить $x=0$, $y=-1$. $\square$

Следствие (соотношение ортогональности). *Для любых натуральных s, n имеет место соотношение*

$$\sum_{k\geqslant 0}(-1)^{n+k}\binom{n}{k}\binom{k}{s} = [n=s].$$

Доказательство. Имеют место равенства

$$\sum_{k\geqslant 0}(-1)^{n+k}\binom{n}{k}\binom{k}{s} = \binom{n}{s}\sum_{k\geqslant 0}(-1)^{n+k}\binom{n}{k}\binom{k}{s}\binom{n}{s}^{-1}$$
$$= (-1)^{n+s}\sum_{k\geqslant s}(-1)^{k-s}\binom{n-s}{k-s}$$
$$= (-1)^{n+s}\sum_{k\geqslant 0}(-1)^{k}\binom{n-s}{k}$$
$$= (-1)^{n+s}[n-s=0]$$
$$= [n=s].$$

Здесь использовалось соотношение

$$\binom{n}{k}\binom{k}{s}\binom{n}{s}^{-1} = \binom{n-s}{k-s},$$

которое проверяется непосредственно. $\square$

Следствие (формулы обращения). *Для числовых последовательностей a_n и b_n, где $n\in\mathbb{N}$, следующие условия равносильны:*

(1) *для любого натурального n имеет место равенство*

$$a_n = \sum_{k\geqslant 0}(-1)^k\tbinom{n}{k}b_k;$$

(2) *для любого натурального n имеет место равенство*

$$b_n = \sum_{k\geqslant 0}(-1)^k\tbinom{n}{k}a_k.$$

Доказательство. Пусть выполняется второе условие. Тогда

$$\begin{aligned}\sum_{k\geqslant 0}(-1)^k\tbinom{n}{k}b_k &= \sum_{k\geqslant 0}(-1)^k\tbinom{n}{k}\sum_{s\geqslant 0}(-1)^s\tbinom{k}{s}a_s\\ &= \sum_{s\geqslant 0}a_s(-1)^{n+s}\sum_{k\geqslant 0}(-1)^{k+n}\tbinom{n}{k}\tbinom{k}{s}\\ &= \sum_{s\geqslant 0}a_s(-1)^{n+s}[n=s]\\ &= a_n.\end{aligned}$$

Этого достаточно для доказательства. □

Пример. Обозначим $\operatorname{sur}(m,n)$ число сюръективных функций, действующих из m-элементного множества в n-элементное. Ясно, что

$$n^m = \sum_{k\geqslant 0}\tbinom{n}{k}\operatorname{sur}(m,k).$$

Отсюда по формулам обращения получаем

$$\operatorname{sur}(m,n) = \sum_{k\geqslant 0}(-1)^{n-k}\tbinom{n}{k}k^m.$$

4. Мультимножества

Пусть задано конечное множество B, содержащее m элементов $b_1,\ldots,b_m$, а также функция

$$k : B\to\mathbb{N}, b_i\mapsto k_i;$$

пусть $n = k_1+\ldots+k_m$. Пару (B,k) назовём *n-мультимножеством*, определённым над множеством B, или *неупорядоченным набором* длины n, составленным из элементов множества B. Такое мультимножество обозначается обычно следующим образом

$$[b_1^{k_1},\ldots,b_m^{k_m}].$$

Его можно мыслить как «множество» или «набор», где элемент b_i присутствует k_i раз. При этом два таких «множества» или «набора» считаются равными, если все элементы в них встречаются одинаково часто.

Найдём число n-мультимножеств над m-элементным множеством.

Теорема. *Число n-мультимножеств над m-элементным множеством совпадает с числом двоичных наборов веса $m-1$ и длины $n+m-1$. Оно совпадает с биномиальным коэффициентом*

$$\binom{n+m-1}{m-1},\ \textit{а также}\ \binom{n+m-1}{n}.$$

(Весом двоичного набора называют число единиц в нём.)

Доказательство. Для доказательства нужно лишь заметить, что существует следующая биекция между мультимножествами и наборами

$$[b_1^{k_1}, \ldots, b_m^{k_m}] \mapsto 0^{k_1}10^{k_2}1 \ldots 10^{k_m}.$$

Здесь 0^k — набор из k нулей. □

Мультимножество, порождённое множеством B, называется *сюръективным*, если каждый элемент из B встречается в мультимножестве.

Следствие. *Число сюръективных n-мультимножест над m-элементным множеством равно*

$$\binom{n-1}{m-1}.$$

Доказательство. Станем рассматривать n-мультимножества над m-элементным множеством. Их число равно числу решений уравнения

$$n = x_1 + \ldots + x_m$$

в натуральных числах. Заметим, что число сюръективных мультимножеств совпадает с числом целых положительных решений записанного уравнения и тогда совпадает с числом натуральных решений уравнения

$$n - m = x_1 + \ldots + x_m.$$

Таким образом, число сюръективных n-мультимножеств совпадает с общим числом $(n-m)$-мультимножеств. □

5. Полиномиальная формула

Пусть A — n-элементное множество и m — целое положительное число. Рассмотрим следующий вопрос: сколько существует способов представить множество A в виде упорядоченного объединения попарно не пересекающихся подмножеств (такие объединения станем называть дизъюнктными) с заданными или произвольными мощностями.

Для произвольного набора натуральных чисел $k_1, \ldots, k_m$, где

$$k_1 + \ldots + k_m = n,$$

обозначим через

$$\binom{n}{k_1, \ldots, k_m}$$

количество упорядоченных наборов $(A_1, \ldots, A_m)$, где

$$A = A_1 \sqcup \ldots \sqcup A_m \text{ и } |A_1| = k_1, \ldots, |A_m| = k_m.$$

Введённые числа называются *полиномиальными коэффициентами*, так как верна

Теорема (полиномиальная формула).

$$(x_1 + \ldots + x_m)^n = \sum_{k_1+\ldots+k_m=n} \binom{n}{k_1, \ldots, k_m} x_1^{k_1} \cdots x_m^{k_m}.$$

Доказательство. Нужно раскрыть скобки в выражении слева. □

Следствие.

$$m^n = \sum_{k_1+\ldots+k_m=n} \binom{n}{k_1,\ldots,k_m}.$$

Доказательство получается в результате подстановки значения 1 вместо всех переменных в полиномиальную формулу. □

Это следствие даёт ответ на вопрос о количестве упорядоченных представлений множества в виде упорядоченного дизъюнктного объединения подмножеств с произвольными мощностями.

Теорема. *Число* $\binom{n}{k_1,\ldots,k_m}$ *равно количеству наборов длины* n *над* m*-элементным множеством, в которых* j*-й элемент множества встречается* k_j *раз. Имеет место формула:*

$$\binom{n}{k_1,\ldots,k_m} = \frac{n!}{k_1!\cdots k_m!}.$$

Доказательство Пусть множество B состоит из чисел $1, \ldots, m$. Тогда между наборами, о которых говорится в теореме, и дизъюнктными разложениями множества $A = \{a_1, \ldots, a_n\}$ на m частей имеется биекция

$$(b_1, \ldots, b_n) \mapsto A_1 \sqcup \ldots \sqcup A_m, \text{ где } A_j = \{a_i | b_i = j\}.$$

Первая часть теоремы доказана. Докажем вторую.

Пусть M есть множество всех наборов длины n, составленных из элементов $1, \ldots, m$, где элемент j встречается k_j раз. Заметим, что все такие наборы получаются из одного-единственного набора $\overline{a} = (1^{k_1}, \ldots, m^{k_m})$ перестановками компонент. В связи с этим обозначим через $\overline{a}^\alpha$ набор, полученный из $\overline{a}$ перестановкой компонент в соответствии с подстановкой α из S_n и рассмотрим отображение

$$S_n \to M, \alpha \mapsto \overline{a}^\alpha.$$

Это отображение сюръективно. Следовательно, $|M| = |S_n/\varepsilon|$, где ε — ядро этого отображения. Иными словами, множество S_n разбивается на классы подстановок, одинаково действующих на набор $\overline{a}$ и количество классов совпадает с числом наборов в множестве M. Осталось заметить, что каждый класс подстановок, одинаково действующих на $\overline{a}$, содержит ровно $k_1! \cdots k_m!$ подстановок (докажите это в качестве упражнения). Тогда $|M| = n!/(k_1! \cdots k_m!)$ и теорема доказана. □

Упражнения.

∘ Восполните детали доказательства теоремы.

∘ Сколько различных слов, не обязательно осмысленных, можно получить из слова «математика» перестановками букв?

6. Числа Стирлинга и числа Белла

В этом разделе изучаются ещё два вида комбинаторных чисел — числа Стирлинга первого и второго рода.

Числа Стирлинга первого рода. Количество подстановок на n-элементном множестве с k независимыми циклами обозначается $\left[{n \atop k}\right]$ и называется *числом Стирлинга первого рода*. По-определению считается, что $\left[{0 \atop 0}\right] = 1$ и тогда $\left[{n \atop 0}\right] = [n = 0]$ для любого n.

В соответствии с определением для любого целого положительного числа n выполняются равенства $\left[{n \atop n}\right] = 1$, $\left[{n \atop n-1}\right] = n \cdot (n-1)$, $\left[{n \atop 1}\right] = (n-1)!$.

Теорема. *Для любых натуральных чисел k, n, таких, что $0 < k < n$, имеет место следующая рекуррентная формула*

$$\left[{n \atop k}\right] = \left[{n-1 \atop k-1}\right] + (n-1) \cdot \left[{n-1 \atop k}\right].$$

Доказательство. В n-элементном множестве A выберем произвольно элемент a и подстановки с k циклами на этом множестве разобьём на два класса. В одном классе элемент a всегда попадает в отдельный одноэлементный цикл, во втором — содержатся в цикле с другими элементами. Подстановки первого класса находятся во взаимно однозначном соответствии с подстановками на множестве $A \setminus \{a\}$ с $k-1$ циклами; здесь $\left[{n-1 \atop k-1}\right]$ подстановок. Подстановки во втором классе можно получить так: выписать в циклической форме все $\left[{n-1 \atop k}\right]$ подстановок на множестве $A \setminus \{a\}$ с k циклами и добавить в каждую элемент a вслед за некоторым записанным элементом, в его цикл. Из каждой имеющейся подстановки получаем $n-1$ новых. Таким образом, число подстановок во втором классе равно $(n-1) \cdot \left[{n-1 \atop k}\right]$. Для завершения доказательства нужно применить принцип суммы. □

Треугольник Паскаля для чисел Стирлинга первого рода выглядит так:

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 2 & & 3 & & 1 & & & & \\
 & & & 6 & & 11 & & 6 & & 1 & & & \\
 & & 24 & & 50 & & 35 & & 10 & & 1 & & \\
 & 120 & & 274 & & 225 & & 85 & & 15 & & 1 & \\
\ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots
\end{array}$$

Многочлены

$$x^{\underline{n}} = x(x-1)\cdots(x-n+1),$$
$$x^{\overline{n}} = x(x+1)\cdots(x+n-1).$$

называются факториальными степенями, убывающей и возрастающей соответственно.

Следствие. *Для любого натурального n имеют место формулы:*

$$x^{\underline{n}} = \sum_{k\geqslant 0}(-1)^{n-k}\begin{bmatrix} n \\ k \end{bmatrix} x^k,$$
$$x^{\overline{n}} = \sum_{k\geqslant 0}\begin{bmatrix} n \\ k \end{bmatrix} x^k.$$

Доказательство. Докажем первую формулу. Она верна при $n = 1$. Пусть она верна для некоторого n. Тогда

$$\begin{aligned} x^{\underline{n+1}} &= (x-n)\cdot x^{\underline{n}} \\ &= (x-n)\cdot\sum_{k\geqslant 0}(-1)^{n-k}\begin{bmatrix} n \\ k \end{bmatrix} x^k \\ &= x\cdot\sum_{k\geqslant 0}(-1)^{n-k}\begin{bmatrix} n \\ k \end{bmatrix} x^k - n\cdot\sum_{k\geqslant 0}(-1)^{n-k}\begin{bmatrix} n \\ k \end{bmatrix} x^k \\ &= \sum_{k\geqslant 1}(-1)^{n+1-k}\left(\begin{bmatrix} n \\ k-1 \end{bmatrix} + n\cdot\begin{bmatrix} n \\ k \end{bmatrix}\right) x^k \\ &= \sum_{k\geqslant 1}^{n}(-1)^{n+1-k}\begin{bmatrix} n+1 \\ k \end{bmatrix} x^k \\ &= \sum_{k\geqslant 0}^{n}(-1)^{n+1-k}\begin{bmatrix} n+1 \\ k \end{bmatrix} x^k. \ \square \end{aligned}$$

Числа Стирлинга второго рода. Количество k-блочных разбиений n-элементного множества обозначается $\left\{ {n \atop k} \right\}$ и называется числом Стирлинга второго рода. По-определению считается, что $\left\{ {0 \atop 0} \right\} = 1$ и тогда $\left\{ {n \atop 0} \right\} = [n = 0]$ для любого натурального n.

В соответствии с определением для любого целого положительного числа n выполняются равенства $\left\{ {n \atop 1} \right\} = \left\{ {n \atop n} \right\} = 1, \left\{ {n \atop n-1} \right\} = \binom{n}{2}$.

Теорема. *Для любых натуральных чисел k, n, таких, что $0 < k < n$, имеет место следующая рекуррентная формула*

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k\left\{ {n-1 \atop k} \right\}.$$

Доказательство. В n-элементном множестве A выберем произвольно элемент a и разбиения этого множества с k блоками разделим на два

класса. В одном классе элемент a всегда попадает в отдельный одноэлементный блок, во втором — содержатся в блоке с другими элементами. Разбиения первого класса находятся во взаимно однозначном соответствии с разбиениями множества $A \setminus \{a\}$ на $k-1$ части; здесь $\left\{ {n-1 \atop k-1} \right\}$ разбиений. Разбиения второго класса получаются из k-блочных разбиений множества $A \setminus \{a\}$ добавлением элемента a в любой блок. Из каждого имеющегося разбиения получаем k новых. Таким образом, число разбиений во втором классе равно $k\left\{ {n-1 \atop k} \right\}$. Для завершения доказательства нужно применить принцип суммы. $\square$

Теперь треугольник Паскаля выглядит так:

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 1 & & & & \\
 & & & 1 & & 7 & & 6 & & 1 & & & \\
 & & 1 & & 15 & & 25 & & 10 & & 1 & & \\
 & 1 & & 31 & & 90 & & 65 & & 15 & & 1 & \\
\dots & & \dots & & \dots & & \dots & & \dots & & \dots & & \dots
\end{array}
$$

Следствие. *Для любого натурального n имеют место формулы:*

$$x^n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} x^{\underline{k}},$$

$$x^n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} (-1)^{n-k} x^{\overline{k}}. \ \square$$

Теорема (свойство ортогональности). *Пусть $0 \leqslant s \leqslant n$. Имеют место формулы*

$$\sum_{k \geqslant 0} (-1)^{s+k} \left\{ {n \atop k} \right\} \left[{k \atop s} \right] = [s = n],$$

$$\sum_{k \geqslant 0} (-1)^{s+k} \left[{n \atop k} \right] \left\{ {k \atop s} \right\} = [s = n].$$

Доказательство. Для доказательства первой формулы запишем:

$$\begin{aligned} x^n &= \sum_{k \geqslant 0} \left\{ {n \atop k} \right\} x^{\underline{k}} \\ &= \sum_{k \geqslant 0} \left\{ {n \atop k} \right\} \sum_{s \geqslant 0} (-1)^{s-k} \left[{k \atop s} \right] x^s \\ &= \sum_{s \geqslant 0} x^s \sum_{k \geqslant 0} (-1)^{s-k} \left\{ {n \atop k} \right\} \left[{k \atop s} \right]. \end{aligned}$$

Вторая формула доказывается аналогично. □

Следствие (формулы обращения). *Пусть имеются числовые последовательности a_k и b_k, где $k \in \mathbb{N}$. Тогда следующие условия равносильны:*

(1) $a_n = \sum_k (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix} b_k$ *для любого натурального n;*

(2) $b_n = \sum_k \left\{ {n \atop k} \right\} a_k$ *для любого натурального n.* □

Число Белла. Число Белла B_n даёт число разбиений n-элементного множества. Имеет место

Теорема.

$$\left\{ {n+1 \atop k+1} \right\} = \sum_s \binom{n}{s} \left\{ {s \atop k} \right\}. \square$$

Следствие.

$$B_{n+1} = \sum_s \binom{n}{s} B_s. \square$$

7. Формула включений и исключений

Формула включений и исключений выражает число элементов в объединении нескольких множеств через мощности пересечений. Легко записать эту формулу для двух множеств:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Не очень сложно сделать это и для трёх множеств:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

В общем случае ответ даёт

Теорема. *Для конечных множеств $A_1, \ldots, A_n$ верно равенство:*

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots.$$

Доказательство. Пусть U — множество, включающее все множества $A_1, \ldots, A_n$. Для произвольного подмножества $B \subseteq U$ определим функцию

$$\chi[B] : U \to \{0,1\}, x \mapsto [x \in B] = \begin{cases} 1, & \text{если } x \in B \\ 0, & \text{в противном случае.} \end{cases}$$

Отметим следующие свойства:

$$\chi[A \cup B](x) = \chi[A](x)\chi[B](x),\ \chi[A'](x) = 1 - \chi[A](x),\ |A| = \sum_x \chi[A](x).$$

Запишем

$$A_1 \cup A_2 \cup \ldots \cup A_n = (A_1 \cup A_2 \cup \ldots \cup A_n)'' = (A_1' \cap A_2' \cap \ldots \cap A_n')'.$$

Используя это, получаем

$$\chi[A_1 \cup A_2 \cup \ldots \cup A_n](x) = \chi[(A_1' \cap A_2' \cap \ldots \cap A_n')'](x) =$$
$$1 - (1 - \chi[A_1](x))(1 - \chi[A_2](x)) \cdots (1 - \chi[A_n](x)) =$$
$$\sum_i \chi[A_i](x) - \sum_{i<j} \chi[A_i \cap A_j](x) + \sum_{i<j<k} \chi[A_i \cap A_j \cap A_k](x) - \ldots.$$

Для завершения доказательства осталось просуммировать полученные значения по всем значениям x из множества A. $\square$

Упражнения.

$\circ$ Докажите формулу включений и исключений индукцией по n.

$\circ$ Докажите, что если поменять местами знаки объединения и пересечения, то формула останется верной.

$\circ$ Сколько чисел в последовательности $1, 2, \ldots, 1000$ не делится ни на одно из чисел $6, 10, 15$?

Число беспорядков. Подстановка без неподвижных точек называется *беспорядком*. Найдём число беспорядков на множестве из n элементов. С этой целью в множестве S_n всех подстановок на множестве чисел $1, \ldots, n$ выделим подмножества B_k (где $1 \leqslant k \leqslant n$), состоящие из подстановок с неподвижной точкой k. Тогда объединение $\cup_k B_k$ состоит из подстановок, имеющих хотя бы одну неподвижную точку. По формуле включений и исключений

$$|\cup_k B_k| = n(n-1)! - \tbinom{n}{2}(n-2)! + \tbinom{n}{3}(n-3)! - \ldots.$$

Тогда число беспорядков есть $n! - |\cup_k B_k|$ и равно

$$\sum_k (-1)^k \tbinom{n}{k}(n-k)!.$$

Доля беспорядков среди всех подстановок равна

$$1 - 1/2! + 1/3! - \ldots + (-1)^n/n! \to 1/e, n \to \infty.$$

Число наложений. Найдём ещё раз число $\mathrm{sur}(m, n)$ сюръективных отображений m-элементного множества на n-элементное. Для этого из всех функций между этими множествами выделим подмножества A_k (где $1 \leqslant k \leqslant n$), состоящие из функций, не принимающих значения k. Объединение $\cup_k A_k$ состоит из функций, не являющихся сюръективными. По формуле включений и исключений

$$|\cup_k A_k| = n(n-1)^m - \tbinom{n}{2}(n-2)^m + \tbinom{n}{3}(n-3)^m - \ldots$$

и

$$\mathrm{sur}(m, n) = \sum_k (-1)^k \tbinom{n}{k}(n-k)^m = \sum_k (-1)^{n-k} \tbinom{n}{k} k^m.$$

Функция Эйлера. Целые числа n и k называются взаимно простыми, если их наибольший общий делитель равен единице. Количество чисел, взаимно простых с n, в последовательности чисел от 1 до n обозначается $\varphi(n)$. При этом φ называется функцией Эйлера. Пусть

$$n = p_1^{k_1} \cdots p_m^{k_m},$$

где $p_1, \ldots, p_n$ — различные простые множители числа n. Найдём значение функции Эйлера для этого числа. Для этого из последовательности чисел от 1 до n выделим подмножества A_k (где $1 \leqslant k \leqslant m$), состоящие из чисел, делящихся на p_k. Тогда по формуле включений и исключений

$$|\cup_k A_k| = n(\sum_k 1/p_k - \sum_{k<l} 1/(p_k p_l) + \ldots).$$

и

$$\begin{aligned}\varphi(n) =& n(1 - \sum_k 1/p_k + \sum_{k<l} 1/(p_k p_l) - \ldots) = \\ =& n(1 - 1/p_1) \cdots (1 - 1/p_m).\end{aligned}$$

Часть II

Целые числа, матрицы и многочлены

ГЛАВА 8

Целые числа

В этой главе изучаются целые числа.

1. Построение целых чисел

Уравнение

$$a + x = b$$

(где a, b заданы, x — неизвестная величина) не всегда разрешимо в числовой системе натуральных чисел. Целые числа появляются в результате пополнения множества натуральных чисел решениями таких уравнений, причём пополнение удаётся выполнить с сохранением основных свойств сложения и умножения натуральных чисел (таких, как ассоциативность, коммутативность, дистрибутивность и некоторые другие). Опишем формальную конструкцию целых чисел.

Рассмотрим множество пар (a, b) натуральных чисел. Каждая такая пара в дальнейшем будет использоваться для представления разности $b-a$, являющейся решением записанного уравнения. Имеет смысл складывать пары покомпонентно:

$$(a, b) + (c, d) = (a + c, b + d);$$

тогда сложение будет согласовано со сложением натуральных чисел. Чтобы выполнялось свойство дистрибутивности

$$(b - a)(d - c) = (ac + bd) - (ad + bc),$$

умножение следует определить так

$$(a, b)(c, d) = (ad + bc, ac + bd).$$

Полученная система всё еще не устраивает нас, так как одно и то же натуральное число очень многими способами записывается в виде разности натуральных чисел и, следовательно, представляется многими парами. Некоторые пары нужно отождествить. В связи с этим поступим так.

На множестве пар рассмотрим отношение $\sim$, считая

$$(a, b) \sim (c, d) \Leftrightarrow b + c = a + d.$$

Это отношение является эквивалентностью, обозначим $(b - a)$ класс эквивалентности пары (a, b). Классы эквивалентности будем называть

целыми числами. Сложение и умножение пар индуцируют следующие операции для целых чисел:

$$(b-a)+(d-c)=(b+d)-(a+c),$$

$$(b-a)\cdot(d-c)=(bd+ac)-(ad+bc).$$

Осталось отождествить целое число $(a-0)$ с натуральным a. Это корректно, так как указанные целые и натуральные числа складываются и перемножаются одинаково. Класс $(0-a)$ обозначается $-a$ и называется противоположным для a. Он удовлетворяет соотношению

$$a+(-a)=0.$$

Числовая система целых чисел построена. Будем обозначать её $\mathbb{Z}$.

Упражнение. Проверьте следующие свойства.

∘ Сложение и умножение целых чисел определены корректно.

∘ Для операций сложения и умножения целых чисел сохраняются основные свойства сложения и умножения натуральных чисел, такие, как коммутативность, ассоциативность, дистрибутивность, свойства нуля и единицы, законы сокращения.

∘ Натуральные числа следующим образом вкладываются в построенную систему целых чисел:

$$\mathbb{N}\to\mathbb{Z}, c\mapsto(c-0).$$

∘ Для любого целого числа: или оно само или противоположное ему является натуральным.

∘ Отношение $\leqslant$ следующим образом продолжается для целых чисел:

$$a\leqslant b\Leftrightarrow b-a\in\mathbb{N}.$$

∘ Определим для целых чисел *отношение делимости* $|$, считая

$$a\mid b\Leftrightarrow a\cdot c=b \text{ для некоторого } c\ .$$

Отношение делимости рефлексивно и транзитивно, но не антисимметрично. (Отношение с таким набором свойств называются предпорядком.) Это отношение индуцирует отношение порядка, на множествах $\{0\},\{\pm1\},\{\pm2\},\ldots$.

2. Деление с остатком

Имеет место

Теорема. *Для любых целых чисел a,b, где $b\neq0$, существует единственная пара целых чисел q,r, таких, что*

$$a=b\cdot q+r,\ 0\leqslant r\leqslant|b|-1.\ \square$$

Числа q и r, о которых говорится в теореме, имеют свои обозначения и названия. Число q называется неполным частным, или целой частью, и r — остатком при делении a на b. Для них используются обозначения:

$$q = \lfloor a/b \rfloor,\ r = a \mod b.$$

Например,

$$12 \mod 5 = 12 \mod -5 = 2,\ -12 \mod 5 = -12 \mod -5 = 3.$$

Отметим

Следствие. *Пусть k — целое положительное число, такое, что $k \geqslant 2$. Для любого натурального a существует единственный набор чисел $a_0, a_1, \ldots$, таких, что*

$$a = a_0 \cdot k^0 + a_1 \cdot k^1 + a_2 \cdot k^2 + \ldots,$$

где $0 \leqslant a_n \leqslant k-1$ для любого n. $\square$

Упражнение. Докажите теорему о делении с остатком и её следствие.

3. Алгоритм Евклида

Станем рассматривать далее целые числа с отношением делимости, которое определяется следующим образом. Будем говорить, что число a является делителем числа b, или a делит b, или b кратно a, или b делится на a, если для некоторого c выполняется соотношение $ac = b$. Будем писать $a|b$ в этом случае.

Отношение делимости рефлексивно и транзитивно, но не антисимметрично на целых числах (числа, делящие друг друга не обязаны совпадать, но могут отличаться знаком).

Число d назовём *общим делителем* чисел $a, b, c, \ldots$, если d является делителем каждого из них, и назовём *наибольшим общим делителем* этих чисел, если дополнительно d кратно любому их общему делителю.

Наибольший общий делитель определён с точностью до знака. Будем обозначать его $\gcd(a, b, c, \ldots)$. Ясно, что наибольший общий делитель определяется множеством чисел $a, b, c, \ldots$: он не изменится, если эти числа записать в другом порядке, добавить или убрать повторения. Он не изменяется при добавлении нулей. Нахождение наибольшего общего делителя для произвольного набора чисел сводится к вычислению его для двух чисел (не равных нулю):

$$\gcd(a, b, c, \ldots) = \gcd(a, \gcd(b, \gcd(c, \ldots))).$$

(Равенство в подобных выражениях понимается с точностью до знака.) Для нахождения наибольшего общего делителя двух чисел имеется эффективный алгоритм, который называется алгоритмом Евклида. Он основывается на следующей теореме.

Теорема (алгоритм Евклида). *Пусть имеется набор целых чисел* $a_0, \ldots, a_n$, *отличных от нуля, где*

(1) $a_{i-1} \mod a_i = a_{i+1}$ *для* $1 \leqslant i \leqslant n-1$;

(2) $a_{n-1} \mod a_n = 0$.

Тогда $a_n = \gcd(a_0, a_1)$.

Доказательство опирается на следующие наблюдения

$$\gcd(a, 0) = a, \text{ и } \gcd(a, b) = \gcd(b, r), \text{ если верно равенство } a = b \cdot q + r.$$

С использованием этого получаем

$$\gcd(a_0, a_1) = \gcd(a_1, a_2) = \ldots = \gcd(a_{n-1}, a_n) = \gcd(a_n, 0) = a_n. \square$$

Таким образом, наибольший общий делитель не равных нулю чисел a_0, a_1 можно найти так. Вычислим последовательность остатков

$$a_0 \mod a_1 = a_2, \quad a_1 \mod a_2 = a_3, \ldots.$$

Данная последовательность заканчивается на некотором шаге нулевым остатком, так как остатки образуют строго убывающую последовательность натуральных чисел. Последний ненулевой остаток в этой последовательности является наибольшим общим делителем чисел a_0, a_1. Описанный алгоритм называется алгоритмом Евклида. Имеет место

Следствие (линейное выражение для НОД). *Пусть* d — *наибольший общий делитель чисел* a_0, a_1. *Тогда для некоторых чисел* s, t *верно равенство:*

$$d = s \cdot a_0 + t \cdot a_1.$$

Подобное выражение называется линейным выражением для наибольшего общего делителя чисел a_0, a_1, а числа s, t называются далее *коэффициентами Безу.*

Доказательство. В условиях предыдущей теоремы обозначим через q_i неполное частное при делении a_{i-1} на a_i, так что

$$a_{i-1} = a_i q_i + a_{i+1}$$

при $1 \leqslant i \leqslant n-1$. Докажем индукцией по i, где $0 \leqslant i \leqslant n$, что для некоторых чисел s_i, t_i выполняется равенство

$$a_i = s_i a_0 + t_i a_1.$$

Можно взять

$$s_0 = 1, t_0 = 0;$$

$$s_1 = 0, t_1 = 1;$$

и

$$s_{i+1} = s_{i-1} - s_i q_i,$$
$$t_{i+1} = t_{i-1} - t_i q_i$$

для $1 \leqslant i \leqslant n-1$. $\square$

Вычисление коэффициентов Безу по этим формулам называется *расширенным алгоритмом Евклида.*

Пример. Найдём наибольший общий делитель и коэффициенты Безу для чисел $a_0 = 54$ и $a_1 = 35$. Вычисления удобно записать в таблицу.

i	0	1	2	3	4	5
a_i	54	35	19	16	3	1
q_i		1	1	1	5	
s_i	1	0	1	-1	2	-11
t_i	0	1	-1	2	-3	17

Линейное выражение выглядит так:

$$1 = (-11) \cdot 54 + 17 \cdot 35.$$

4. Простые числа

Отметим ряд свойств.

$\circ$ *Для любого целого числа p, отличного от чисел $0, \pm 1$, равносильны следующие условия:*

(1) *для любых целых a и b:*

$$p \mid a \text{ или } p \mid b, \text{ если } p \mid ab.$$

(2) *число p не имеет делителей, кроме $\pm 1, \pm p$.*

Доказательство. Предположим, имеет место первое условие. Пусть $a|p$, то есть $ab = p$ для некоторого b. В силу первого условия $p|a$ или $p|b$. Тогда $a = \pm p$ или $a = \pm 1$ в силу закона сокращения и имеет место второе условие. Обратно, пусть выполняется второе условие и $p|ab$. Если p не является делителем a, то $\gcd(p, a) = 1$ и для некоторых s, t выполняются равенства:

$$1 = s \cdot p + t \cdot a \quad \text{и} \quad b = s \cdot p \cdot a + t \cdot a \cdot b,$$

Во втором равенстве p делит оба слагаемых справа, а значит делит и b. $\square$

Число p, отличное от $0, \pm 1$, называется *простым*, если удовлетворяет условиям (1–2); в противном случае оно называется *составным.*

$\circ$ *Всякое целое число, отличное от $0, \pm 1$, является произведением простых чисел.*

Доказательство. Это доказывается индукцией по абсолютной величине целого числа. □

∘ *Простых чисел бесконечно много.*

Доказательство. Предположим, это не так и $p_1, \ldots, p_n$ — все простые числа. Но простой делитель числа

$$1 + p_1 \cdots p_n,$$

существующий по предыдущему свойству, не может совпадать ни с одним из чисел $p_1, \ldots, p_n$. Противоречие. □

Имеет место

Теорема (Основная теорема Арифметики). *Всякое целое число, отличное от* $0, \pm 1$*, можно представить в виде произведения простых чисел, причём единственным образом с точностью до порядка и знака сомножителей.*

Доказательство. Докажем единственность разложения на простые множители. Предположим, имеет место равенство

$$p_1 \cdots p_n = \pm q_1 \cdots q_m,$$

где все числа p_i, q_j — простые. Нужно доказать, что $n = m$ и после надлежащей перенумерации сомножителей выполняются равенства

$$p_1 = \pm q_1, \ldots, p_n = \pm q_n.$$

В силу первого свойства число p_1 делит какой-то из множителей $q_1, \ldots, q_m$. Перенумеровав эти множители, будем считать, что $p_1 | q_1$. Тогда $p_1 = \pm q_1$ и записанное выше равенство можно сократить на p_1. В результате получается

$$p_2 \cdots p_n = \pm q_2 \cdots q_m.$$

Повторив это рассуждение нужное число раз, получим доказательство. □

5. Классы вычетов

Пусть m — целое число. Будем говорить, что числа a и b *сравнимы по модулю* m, и писать $a \equiv b \mod m$, если $m | (a - b)$. Это отношение не зависит от знака числа m и совпадает с равенством при $m = 0$. В связи с этим будем считать далее, что $m > 0$. Отметим следующие свойства.

∘ *Отношение сравнимости по модулю* m *является эквивалентностью на множестве целых чисел.*

Доказательство. Это проверяется непосредственно. □

Класс всех чисел, сравнимых с заданным числом a по модулю m, называется классом вычетов числа a по модулю m и обозначается далее

$$[a], [a]_m, \overline{a}, \text{ а также } m\mathbb{Z} + a.$$

Он состоит из чисел, которые отличаются от a слагаемым, кратным m.

∘ *Два числа попадают в один класс, если и только если имеют одинаковые остатки при делении на m. В частности, имеется ровно m различных классов*

$$[0], \ldots, [m-1]. \square$$

∘ *Операции сложения и умножения целых чисел индуцируют операции над классами вычетов. Именно, корректны следующие определения:*

$$[a] + [b] = [a+b], [a][b] = [ab].$$

Доказательство. Нужно проверить, что

$$m|(a+b) - (a'+b'), \text{ если } m|(a-a') \text{ и } m|(b-b'),$$

$$m|(a \cdot b) - (a' \cdot b'), \text{ если } m|(a-a') \text{ и } m|(b-b').$$

Это действительно так. $\square$

∘ *Для сложения и умножения классов вычетов выполняются основные свойства сложения и умножения целых чисел: коммутативность, ассоциативность, дистрибутивность, законы сокращения для сложения.*

Доказательство. Легко убедиться, что все алгебраические соотношения для целых чисел, записываемые с использованием сложения и умножения, остаются верными, если числа заменить их классами. $\square$

Числовая система классов вычетов целых чисел по модулю m, рассматриваемых с операциями сложения и умножения обозначается через $\mathbb{Z}/m\mathbb{Z}$ и называется *кольцом классов вычетов* целых чисел по модулю m.

Числа a и b, как и их классы $[a]$ и $[b]$, называются *взаимно обратными* по модулю m, если выполняются следующие равносильные условия

$$ab \equiv 1 \mod m, \ [a][b] = [1];$$

тогда каждое из этих чисел (каждый из классов) по отношению к другому называется *обратным по модулю m*. Число (класс), для которого существует обратное (обратный) по модулю m, называется *обратимым* по модулю m.

∘ *Произведение классов (чисел), обратимых по модулю m, обратимо по модулю m.*

Доказательство. Достаточно заметить, что если a, b и c, d — взаимно обратные пары чисел по модулю m, то и пары ac, bd — тоже. $\square$

Таким образом, мы можем рассматривать операцию умножения на множестве обратимых по модулю m чисел и на множестве обратимых классов. Множество обратимых классов вычетов по модулю m, рассматриваемое

с операцией умножения, обозначается $(\mathbb{Z}/m\mathbb{Z})^\times$ и называется *мультипликативной группой* классов вычетов.

Теорема. *Для целых чисел a и m следующие условия равносильны:*

(1) *a обратимо по модулю m;*

(2) $\gcd(a, m) = 1$.

Доказательство. Если число s обратное по модулю m для числа a, то для некоторого t выполняется соотношение

$$as + mt = 1.$$

Тогда a и m не имеют общих делителей, кроме ± 1. Обратно, если наибольший общий делитель чисел a и m равен единице, то их коэффициент Безу, стоящий рядом с a является обратным для a по модулю m. □

Следствие. $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$.

∘ *Обозначим классы $[0], \ldots, [m-1]$ через $0, \ldots, m-1$. Теперь*

$$\mathbb{Z}/m\mathbb{Z} = \{0, \ldots, m-1\}.$$

При таких обозначениях сумма и произведение классов a, b совпадают с классами

$$a + b \mod m, ab \mod m. \ \square$$

(В последнем выражении выполнено сложение и умножение целых чисел.)

6. Целые m-адические числа

Пусть задано целое число $m \geqslant 2$. Выражение

$$a = a_0 m^0 + a_1 m^1 + \ldots, \text{ где } 0 \leqslant a_k \leqslant m-1 \text{ для всех } k \text{ из } \mathbb{N},$$

назовём *(целым) m-адическим числом*. Отметим, что натуральные числа записываются m-адическими числами, у которых почти все (то есть все кроме конечного числа) коэффициенты равны нулю. Мы можем записать формулы для вычисления коэффициентов суммы и произведения натуральных чисел a и b. Эти формулы будут выглядеть примерно так:

$$(a+b)_n = f_n(a_0, \ldots, a_n; b_0, \ldots, b_n) \text{ и } (a \cdot b)_n = g_n(a_0, \ldots, a_n; b_0, \ldots, b_n),$$

где f_n, g_n — некоторые функции вида $(\mathbb{Z}/m\mathbb{Z})^{n+1} \to \mathbb{Z}/m\mathbb{Z}$. Важно, что в вычислении значения каждого разряда не участвуют значения более старших разрядов. Это позволяет использовать указанные формулы для определения сложения и умножения произвольных m-адических чисел. Множество всех целых m-адических чисел, рассматриваемое с операциями сложения и умножения, определёнными описанным способом, обозначается $\mathbb{Z}_m$ и называется *кольцом целых m-адических чисел*.

Упражнение. Проверьте следующие свойства.

∘ В числовой системе $\mathbb{Z}_m$ сохраняются основные свойства сложения и умножения натуральных чисел, такие, как коммутативность, ассоциативность, дистрибутивность, свойства нуля и единицы, а также закон сокращения для сложения. Закон сокращения для умножения сохранится при простом m.

∘ В числовой системе $\mathbb{Z}_m$ для любого числа a имеется противоположное число $-a$, такое, что $a + (-a) = 0$. В частности, здесь содержатся не только все натуральные числа, но и все целые числа.

∘ Назовём целое m-адическое число a обратимым, если для него существует обратное целое m-адическое число b, такое что $ab = 1$. Опишите обратимые элементы числовой системы $\mathbb{Z}_m$. Отметим, что в рассматриваемой числовой системе содержатся не только все целые числа (в соответствии с предыдущим свойством), но и обратные величины для значительной части целых чисел и тогда значительную часть рациональных чисел.

∘ Опишите явно функции для вычисления n-го разряда суммы и произведения двух целых m-адических чисел (функции f_n, g_n выше).

ГЛАВА 9

Алгебраические структуры

Логика изучения числовых систем приводит к необходимости рассмотрения алгебраических структур. В данной главе определяются основные алгебраические структуры — группы, кольца, поля.

1. Алгебраическая операция

Пусть A — непустое множество, n — натуральное число и для любого набора a из A^n в множестве A однозначно определён элемент $\alpha(a)$. В этой ситуации говорят, что на множестве A задана n-местная операция α. Иными словами, n-местная операция на множестве A — это отображение

$$\alpha : A^n \to A, a \mapsto \alpha(a).$$

При $n = 0$ говорят о нульместной операции, которую отождествляют с выделенным элементом множества A. При $n = 1$ операция называется *преобразованием* множества A. При $n = 2$ говорят о бинарной операции, которую называют также *законом композиции*.

Подмножество $B \subseteq A$ называется *замкнутым* операцией α, если оно содержит элемент $\alpha(b)$ для любого набора b из множества B^n. Можно рассматривать α как операцию на множестве B в этом случае.

Под алгебраической структурой понимают непустое множество, рассматриваемое вместе с некоторым набором операций на нём, при этом операции могут удовлетворять некоторым специальным тождествам. Алгебраические структуры обычно рассматриваются с точностью до изоморфизма, где под изоморфизмом понимается переобозначение элементов множества, то есть биекция между множествами, согласованная с операциями. Понятие изоморфизма в дальнейшем будет уточнено. Особое значение имеет ряд алгебраических структур с одной или двумя бинарными операциями, таких, как определяемые далее группы, кольца и поля.

2. Коммутативность и ассоциативность

Пусть на множестве A задана бинарная операция умножения:

$$(\cdot) : A^2 \to A, (x, y) \mapsto xy.$$

Она называется *коммутативной*, если $ab = ba$, и называется *ассоциативной*, если $a(bc) = (ab)c$ (для любых элементов a, b, c из множества A). Свойства коммутативности и ассоциативности независимы. Например, сложение целых чисел коммутативно и ассоциативно, умножение подстановок ассоциативно, но не коммутативно, операция

$$\mathbb{Z}^2 \to \mathbb{Z}, (x, y) \mapsto -x - y,$$

коммутативна, но не ассоциативна. Рассмотрим подробнее свойства коммутативности и ассоциативности.

Обобщённая ассоциативность. Ассоциативность позволяет не писать скобки в произведениях с тремя сомножителями. Для четырёх сомножителей выполняется аналогичное свойство, так как имеют место равенства

$$(a(bc))d = ((ab)c)d = (ab)(cd) = a(b(cd)) = a((bc)d),$$

где присутствуют все способы корректной расстановки скобок. Можно опускать скобки в любых произведениях, так как имеет место

Теорема (обобщённый закон ассоциативности). *Пусть умножение ассоциативно в множестве A. Тогда для любых элементов $a_1, \ldots, a_n$ из A все произведения, полученные корректной расстановок скобок в выражении*

$$a_1 \cdots a_n,$$

равны.

Доказательство. Назовём левонормированным произведение

$$a_1 * \ldots * a_n = (\ldots (a_1 a_2) a_3 \ldots) a_n.$$

Докажем, что любое произведение равно левонормированному. Это так при $n \leqslant 3$. Докажем это утверждение для заданного значения $n > 3$ в предположении, что для меньших значений n оно выполняется. Используя предположение индукции, отметим, что при любой корректной расстановке скобок произведение $a_1 \cdots a_n$ можно записать как

$$A = a_1 * \ldots * a_k \cdot a_{k+1} * \ldots * a_n,$$

где $k < n$. Если $k = n - 1$, то доказывать нечего. Пусть $k < n - 1$. Тогда с использованием предположения индукции и ассоциативности, получаем:

$$a_1 * \ldots * a_k \cdot a_{k+1} * \ldots * a_n = a_1 * \ldots * a_k \cdot (a_{k+1} * \ldots * a_{n-1} \cdot a_n) =$$

$$= (a_1 * \ldots * a_k \cdot a_{k+1} * \ldots * a_{n-1}) \cdot a_n = a_1 * \ldots * a_{n-1} \cdot a_n = a_1 * \ldots * a_n. \quad \square$$

Обобщённая коммутативность. Предположим теперь, что умножение коммутативно и ассоциативно. Тогда значение произведения ab с двумя сомножителями не зависит от их порядка. Для трёх сомножителей это тоже так:

$$abc = acb = cab = cba = bca = bac.$$

Аналогичное выполняется для любых произведений, так как верна

Теорема (обобщённый закон коммутативности). *Пусть умножение коммутативно и ассоциативно в множестве A. Тогда для любых элементов $a_1, \ldots, a_n$ из A все произведения, полученные перестановкой сомножителей в выражении*

$$a_1 \cdots a_n,$$

равны.

Доказательство. Для подстановки

$$\alpha : \{1, \ldots, n\} \to \{1, \ldots, n\}, k \mapsto k\alpha,$$

из S_n положим

$$\alpha a = a_{1\alpha} \cdots a_{n\alpha}.$$

Докажем, что значения всех произведений αa, где α из S_n, равны.

Обозначим $(a)_k$ k-ый множитель произведения a. Для любых подстановок α и β получаем

$$(\alpha\beta \cdot a)_k = a_{k\alpha\beta} = (\beta a)_{k\alpha} = (\alpha \cdot \beta a)_k \quad \text{и } \alpha\beta \cdot a = \alpha \cdot \beta a.$$

Разложим α в произведение транспозиций соседних элементов:

$$\alpha = \tau_1 \ldots \tau_N.$$

Используя индукцию по N и коммутативность, получаем:

$$\alpha a = \tau_1 \cdots \tau_N a = \tau_1 \cdots \tau_{N-1} \cdot \tau_N a = \tau_1 \cdots \tau_{N-1} a = a. \ \square$$

3. Полугруппа, моноид, группа

Пусть в множестве A задана ассоциативная операция умножения. Тогда множество A, рассматриваемое вместе с этой операцией, называется *полугруппой*. В ней элемент e называется *нейтральным* элементом или *единицей*, если для любого элемента a выполняется равенство

$$ae = ea = a.$$

Может существовать не более одной единицы, так как

$$e = ee' = e',$$

если e и e' — единицы. Полугруппа с единицей, называется *моноидом*. В моноиде элемент a называется обратимым, если для некоторого элемента b выполняется равенство

$$ab = ba = e.$$

В этом случае элемент b называется обратным для a. Может существовать не более одного обратного элемента, так как

$$b = bab' = b',$$

если элементы b и b' — обратные для a. Элемент, обратный для a, обозначается a^{-1}.

Моноид, в котором все элементы обратимы (обладают обратными), называется *группой*. Коммутативная группа называется также *абелевой*.

Замечание. Операция в моноиде (и в группе) не обязательно обозначается умножением. Часто для обозначения операции используется сложение. Тогда нейтральный элемент называется *нулём* и обозначается 0. В этом случае говорят не об обратных, а о противоположных элементах. Через $-a$ обозначается элемент, противоположный к a. Моноид со сложением называется аддитивным, с умножением — мультипликативным.

Примеры.

∘ В моноиде M произведение обратимых элементов a, b обратимо и

$$(ab)^{-1} = b^{-1}a^{-1};$$

(пусть моноид M мультипликативный). Отсюда следует, что множество обратимых элементов моноида замкнуто умножением и образует группу. Группа обратимых элементов моноида M обозначается $M^\times$.

∘ Целые числа со сложением образуют группу, с умножением — моноид. Группа обратимых элементов здесь

$$\mathbb{Z}^\times = \{\pm 1\}.$$

∘ Множество $\mathbb{Z}/m\mathbb{Z}$ классов вычетов целых чисел по модулю m образуют (аддитивную) группу с операцией сложения и (мультипликативный) моноид с операцией умножения. Группа обратимых элементов этого моноида

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{a + m\mathbb{Z} | a \in \mathbb{Z}, \gcd(a, m) = 1\}.$$

Группа $\mathbb{Z}/m\mathbb{Z}$ с операцией сложения и группа $(\mathbb{Z}/m\mathbb{Z})^\times$ с умножением называются соответственно *аддитивной* и *мультипликативной* группами классов вычетов по модулю m.

∘ Пусть X — непустое множество, содержащее n элементов. Преобразования этого множества с операцией умножения отображений образуют моноид, где единицей является тождественная подстановка id_X. Группа

обратимых элементов этого моноида состоит из подстановок. Она обозначается S_X или S_n и называется *симметрической группой подстановок* на множестве X.

∘ Чётные подстановки (разлагающиеся в произведение транспозиций с чётным числом сомножителей) также образуют группу. Она обозначается A_X или A_n и называется *знакопеременной группой подстановок*.

∘ Следующие четыре подстановки

$$(12)(34), (13)(24), (14)(23), \mathrm{id}$$

на множестве чисел $1, 2, 3, 4$ образует группу, которая называется *четверной группой Клейна* и обозначается V_4.

Отображение

$$f : G \to H, g \to g',$$

между группами называется *гомоморфизмом*, если оно перестановочно с групповыми операциями в группах G и H, то есть

$$f : gh \mapsto g'h'$$

(отображает произведение элементов на произведение их образов) в случае мультипликативных групп. Обратимый гомоморфизм называется *изоморфизмом*. Группы, между которыми имеется изоморфизм, называются *изоморфными*. Обычно группы рассматриваются с точностью до изоморфизма, изоморфные группы считаются копиями.

Примеры.

∘ Имеется гомоморфизм групп:

$$S_n \to \{\pm 1\}, \alpha \mapsto \operatorname{sign} \alpha.$$

∘ Имеется гомоморфизм аддитивных групп:

$$\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, a \mapsto a + m\mathbb{Z}.$$

∘ Пусть p — простое. Имеется гомоморфизм групп:

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}, a + p\mathbb{Z} \mapsto \left(\frac{a}{p}\right).$$

Здесь

$$\left(\frac{a}{p}\right) = 1 \;\Leftrightarrow\; a \equiv b^2 \mod p \text{ для некоторого целого числа } b.$$

Иными словами, равенство $\left(\frac{a}{p}\right) = 1$ означает, что класс $a + p\mathbb{Z}$ является квадратом в числовой системе $\mathbb{Z}/p\mathbb{Z}$.

Упражнение. Гомоморфизм групп единицу отображает на единицу и взаимно обратные элементы отображает на взаимно обратные.

4. Кольцо

Непустое множество R, в котором определены бинарные операции сложения и умножения, называется *ассоциативным кольцом*, если выполняются следующие условия.

1. Со сложением элементы из R образуют абелеву группу; эта группа называется *аддитивной группой кольца*.

2. С умножением элементы кольца составляют полугруппу; это *мультипликативная* полугруппа кольца.

3. Сложение и умножение связаны законами дистрибутивности:

$$a(b+c) = ab + ac, (a+b)c = ac + bc;$$

здесь a, b, c — произвольные элементы кольца.

Замечание. В дальнейшем вместо «ассоциативное кольцо» будем говорить просто «кольцо».

Упражнение. Определим вычитание в кольце, положив

$$a - b = a + (-b).$$

Проверьте, что в кольце выполняются тождества:

$$a(b-c) = ab - ac, (a-b)c = ac - bc, a0 = 0a = 0.$$

Если умножение в кольце коммутативно, то и кольцо называется коммутативным. Если в кольце есть единица, то говорят о кольце с единицей, которое называют также *унитальным* кольцом. Обратимые элементы в таком кольце образуют группу $R^\times$, которая называется *мультипликативной группой* кольца. Область математики, изучающая коммутативные кольца с единицей, называется *коммутативной алгеброй*.

Примеры.

∘ Имеется нулевое кольцо $\{0\}$. Единственный элемент этого кольца является нейтральным элементом по сложению и умножению одновременно. Это единственное кольцо, где $1 = 0$. (Действительно, если $1 = 0$, то для любого элемента a верно: $a = 1a = 0a = 0$.)

∘ Целые числа составляют коммутативное кольцо с единицей.

∘ Классы вычетов целых чисел по модулю m образуют коммутативное кольцо с единицей.

∘ Целые m-адические числа образуют коммутативное кольцо с единицей.

5. Гомоморфизмы колец

Пусть R и L — кольца. Отображение

$$f : R \to L, a \mapsto a',$$

называется *гомоморфизмом колец*, если оно согласовано со сложением и умножением в кольцах, так что

$$f : a + b \mapsto a' + b', a \cdot b \mapsto a' \cdot b'.$$

Оно называется *унитальным* гомоморфизмом между кольцами с единицей, если дополнительно выполняется условие

$$f : 1 \mapsto 1.$$

Подмножество кольца, которое само является кольцом с теми же операциями сложения и умножения, называется подкольцом. Оно называется *унитальным* подкольцом в кольце с единицей, если содержит единицу кольца. Отметим следующие свойства.

∘ Гомоморфный образ подкольца области определения является подкольцом области значений.

В силу этого свойства часто можно ограничиться рассмотрением только сюръективных гомоморфизмов.

∘ Полный прообраз подкольца области значений при гомоморфизме является подкольцом области определения.

∘ Произведение гомоморфизмов, если оно корректно определено, является гомоморфизмом.

∘ Если гомоморфизм обратим, то обратное отображение также является гомоморфизмом.

Обратимый гомоморфизм называется *изоморфизмом* и кольца, между которыми он существует, называются *изоморфными*. Обычно кольца изучаются с точностью до изоморфизма: изоморфные кольца особо не различаются, они считаются копиями одного и того же кольца.

Сюръективный гомоморфизм называется *эпиморфизмом*. Любой гомоморфизм является одновременно эпиморфизмом между областью определения и образом.

Инъективный гомоморфизм называется *мономорфизмом* или *изоморфным вложением*. Он устанавливает изоморфизм между областью определения и образом.

Примеры.

∘ Эпиморфизмом колец является отображение

$$\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, x \mapsto x + m\mathbb{Z},$$

∘ Эпиморфизмом колец является отображение

$$\mathbb{Z}_m \to \mathbb{Z}/m^k\mathbb{Z}, a_0 + a_1 m + \ldots \mapsto (a_0 + \ldots + a_{k-1}m^{k-1}) + m^k\mathbb{Z}.$$

∘ Гомоморфизмом колец является отображение

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, x + mn\mathbb{Z} \mapsto x + m\mathbb{Z}.$$

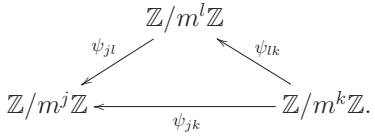
6. Кольцо целых m-адических чисел*

В этом разделе рассматривается кольцо целых m-адических чисел и формулируется его универсальное свойство. Тем самым, этому кольцу даётся ещё одно определение.

Заметим, что для любых целых положительных чисел l, k, таких, что $l \leqslant k$, существует эпиморфизм

$$\psi_{l,k} : \mathbb{Z}/m^k\mathbb{Z} \to \mathbb{Z}/m^l\mathbb{Z}, x + m^k\mathbb{Z} \mapsto x + m^l\mathbb{Z},$$

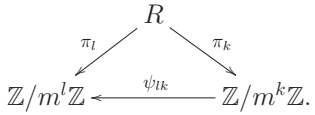
причём для чисел j, l, k, таких, что $j \leqslant l \leqslant k$, коммутативна диаграмма



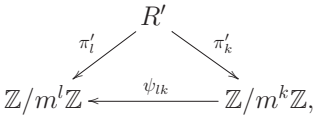
Имеет место

Теорема. *Существует единственное с точностью до изоморфизма кольцо R, удовлетворяющее указанным ниже условиям* (1,2). *Кольцо R изоморфно кольцу $\mathbb{Z}_m$.*

(1) *Для любого целого положительного числа l существует гомоморфизм $\pi_l : R \to \mathbb{Z}/m^l\mathbb{Z}$, причём для любого целого $k > l$ коммутативна диаграмма:*

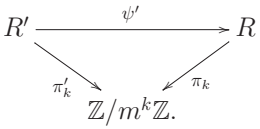


(2) *Пусть кольцо R' также удовлетворяет условию* (1), *то есть существуют гомоморфизмы $\pi'_l : R' \to \mathbb{Z}/m^l\mathbb{Z}$ и коммутативны диаграммы:*



где l, k — целые положительные числа, такие, что $l < k$.

Тогда существует единственный гомоморфизм $\psi' : R' \to R$, такой, что для любого целого положительного k коммутативна диаграмма



Замечание. Кольцо $R = \mathbb{Z}_m$ обладает свойством (1) и однозначно с точностью до изоморфизма определяется им. Имея ввиду это, кольцо $\mathbb{Z}_m$ называют *проективным пределом* набора колец $\mathbb{Z}/m^k\mathbb{Z}$.

Доказательство теоремы состоит из трёх частей.

1. *Кольцо R, удовлетворяющее условиям* (1,2)*, существует.*

Составим его из последовательностей

$$a = a(1)a(2)\ldots,$$

где $a(k)$ — элемент кольца $\mathbb{Z}/m^k\mathbb{Z}$ для любого k и

$$a(1) \xleftarrow{\psi_{12}} a(2) \xleftarrow{\psi_{23}} \ldots.$$

Последовательности складываются и перемножаются покомпонентно, каждая компонента в соответствующем кольце $\mathbb{Z}/m^k\mathbb{Z}$. Первое условие выполняется для гомоморфизмов

$$\pi_k : R \to \mathbb{Z}/m^k\mathbb{Z}, a \mapsto a(k).$$

Предположим, что кольцо R' также удовлетворяет первому условию. Тогда существует гомоморфизм

$$\psi' : R' \to R, \text{ такой, что } x \mapsto a, \text{ если } \pi'_k(x) = a(k) \text{ для всех } k.$$

Это единственный гомоморфизм, обеспечивающий выполнение второго условия.

2. *Кольцо R, удовлетворяющее условиям* (1,2)*, единственно с точностью до изоморфизма.*

Предположим, что кольца R и R' удовлетворяют этими условиям. Рассмотрим для них гомоморфизмы, о которых говорится во втором условии. Их произведения

$$R \to R' \to R, R' \to R \to R',$$

являются тождественными отображениями в силу единственности. Следовательно, они взаимно обратны и являются изоморфизмами.

3. *Имеет место очевидный изоморфизм:*

$$\mathbb{Z}_m \to R, a_0 + a_1m^1 + \ldots \mapsto [a_0]_m[a_0 + a_1m]_{m^2}\ldots. \quad \square$$

Упражнение. Докажите, что кольца $\mathbb{Z}_m$ и $\mathbb{Z}_n$ изоморфны, если и только если числа m и n имеют одинаковые наборы простых делителей.

7. Целостное кольцо и поле

Пусть R — кольцо с единицей. Если в нём для некоторых элементов a и b, таких, что $b \neq 0$, выполняется равенство $ab = 0$, то элемент a называется (левым) *делителем нуля*. Аналогично определяются правые делители нуля. Если единственным делителем нуля является 0, то говорят о кольце *без делителей нуля*. Коммутативное кольцо с единицей, отличной от нуля, и без делителей нуля называется *целостным*. Отметим следующий

Закон сокращения. *На элемент, не являющийся левым делителем нуля можно сокращать слева: в кольце для любых элементов a, b и c, где a не является левым делителем нуля, имеет место импликация*

$$(ab = ac) \to (b = c).$$

Доказательство. Равенство $ab = ac$ влечёт $ab - ac = 0$ и $a(b - c) = 0$, откуда получаем $b - c = 0$ и тогда $b = c$, так как a не является левым делителем нуля. □

В частности, в целостном кольце можно сокращать на любой отличный от нуля элемент. Такое кольцо называют также *кольцом с сокращением*.

Примеры. Следующие кольца целостные.

∘ Кольцо целых чисел.

∘ Кольцо классов вычетов целых чисел по простому модулю.

∘ Кольцо целых p-адических чисел при простом p.

Если в кольце с единицей для элементов a, b выполняется равенство

$$ab = ba = 1,$$

то такие элементы называются взаимно обратными и каждый из них по отношению к другому называется обратным. Элемент, для которого существует обратный, называется обратимым. Коммутативное кольцо с $1 \neq 0$, где все ненулевые элементы обратимы, называется *полем*. В поле мультипликативная группа состоит из всех ненулевых элементов.

Отметим пару свойств.

∘ *Делители нуля необратимы. В частности, поле является целостным кольцом.*

∘ Доказательство. Если равенство $ab = 0$ выполняется для обратимого элемента a, то левым умножением на элемент a^{-1} получаем $b = 0$. □

∘ *Конечное целостное кольцо является полем.*

Доказательство. Для ненулевого элемента a отображение

$$R \to R, x \mapsto ax$$

инъективно в силу закона сокращения, имеющего место в целостном кольце, и тогда также сюръективно, так как является отображением конечного множества в себя. Отсюда следует, что элемент a обратим. $\square$

Примеры.

$\circ$ Кольцо классов вычетов целых чисел по модулю m является полем при простых m.

$\circ$ В кольце целых m-адических чисел число $a = a_0 m^0 + \ldots$ обратимо тогда и только тогда, когда коэффициент a_0 обратим по модулю m (упражнение).

8. Поле частных целостного кольца

Рассмотрим условия, при которых целостное кольцо R можно расширить до поля (вложить изоморфно в поле).

Предположим сначала, что кольцо R содержится в некотором поле. Тогда поле содержит элемент ab^{-1} для любых a, b из R, где $b \neq 0$. Такой элемент обозначается также a/b и называется *дробью* с числителем a и знаменателем b, а также *отношением* или *частным* элементов a, b. Отметим следующие свойства дробей:

(1) $a/b = c/d \;\Leftrightarrow\; ad = bc$;

(2) $a/b + c/d = (ad + bc)/bd$;

(3)$(a/b)(c/d) = (ac)/(bd)$;

они выполняются для любых дробей a/b и c/d. Имеет место

Теорема. *Всякое целостное кольцо R обладает полем частных,* $\mathrm{Frac}(R)$*, состоящим из элементов a/b, где a, b из R и $b \neq 0$, для которых выполняются условия (1–3), записанные выше.*

Существует следующее изоморфное вложение колец:

$$R \to \mathrm{Frac}(R), a \mapsto a/1.$$

Доказательство. На множестве $R \times (R \setminus 0)$ рассмотрим отношение $\sim$, такое, что

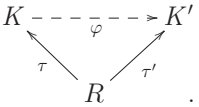
$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Не сложно проверить, что это эквивалентность. Обозначим через a/b класс эквивалентности пары (a, b) и определим операции сложения и умножения для классов в соответствии со свойствами (2) и (3). Не сложно проверить корректность этих определений. После этого следует проверить, что дроби, определённые таким образом, образуют поле и отождествить дробь вида $a/1$ с элементом a из R. $\square$

Теорема (универсальное свойство поля частных).

Пусть R — целостное кольцо и $K = \mathrm{Frac}(R)$ — его поле частных.

Существует изоморфное вложение $\tau : R \to K$, такое, что для любого поля K' и изоморфного вложения $\tau' : R \to K'$ имеется единственное вложение $\varphi : K \to K'$, делающее коммутативной диаграмму



Обратно, если для некоторого поля K выполняются записанные условия, то имеет место изоморфизм $K \simeq \mathrm{Frac}(R)$.

Доказательство. Вложение

$$\tau : R \to \mathrm{Frac}(R), a \mapsto a/1,$$

обладает нужным свойством. Действительно, для произвольного вложения τ', о котором говорится в теореме, отображение φ может быть только следующим

$$\varphi : K \to K', a/b \mapsto \tau'(a)/\tau'(b).$$

С другой стороны, непосредственно проверяется, что φ корректно определяется записанным условием и является изоморфным вложением. Тем самым, первая часть теоремы доказана. Докажем вторую.

Пусть некоторое поле K обладает указанным свойством. Тогда можно рассмотреть композиции

$$K \to \mathrm{Frac}(R) \to K, \mathrm{Frac}(R) \to K \to \mathrm{Frac}(R),$$

составленные из отображений φ, о которых говорится в первой части теоремы. Обе композиции также обладают свойством отображения φ, указанным в первой части, и являются тогда тождественными отображениями. Следовательно, оба отображения φ являются изоморфизмами. □

Примеры.

∘ Полем частных для кольца целых чисел является поле $\mathbb{Q}$ рациональных чисел.

∘ Пусть p — простое. В этом случае кольцо $\mathbb{Z}_p$ целостное и обладает полем частных, которое обозначается $\mathbb{Q}_p$ и называется *полем p-адических чисел*. Введём следующие обозначения. Для любого натурального n пусть $(p^n)^{-1} = p^{-n}$ и $a_0p^{-n} + a_1p^{1-n} + a_2p^{2-n} + \ldots = p^{-n}(a_0p^0 + a_1p^1 + a_2p^2 + \ldots)$. Элементы поля $\mathbb{Q}_p$, таким образом, записываются формальными суммами

$$a_0p^{-n} + a_1p^{1-n} + \ldots,$$

где n — произвольное натуральное и $0 \leqslant a_k \leqslant p-1$ для всех k.

9. Кольцо частных, локализация*

В данном разделе кольца предполагаются коммутативными и с единицей, отличной от нуля, а их гомоморфизмы унитальны.

Пусть S — непустое подмножество кольца R. Будем интересоваться следующим вопросом: как построить нетривиальный гомоморфизм из кольца R, делающий все элементы из множества S обратимыми.

Множество S назовём *мультипликативным*, если

$$1 \in S, 0 \notin S, S^2 \subseteq S.$$

Будем решать указанную задачу для мультипликативного множества.

Примеры.

∘ Элемент a кольца R называется *нильпотентным*, если $a^n = 0$ для некоторого целого положительного n. Если элемент a не является нильпотентным, то множество элементов $a^0, a^1, a^2, \ldots$ обладает свойством мультипликативности.

∘ Мультипликативным является множество всех элементов кольца, которые не являются делителями нуля.

Определим на множестве пар $R \times S$ отношение $\sim$, считая

$$(a, b) \sim (c, d), \text{ если } ads = bcs \text{ для некоторого } s \in S.$$

Отметим следующие свойства.

∘ *Отношение $\sim$ является эквивалентностью на множестве $R \times S$.*

Доказательство. Это проверяется непосредственно. □

Обозначим через a/b класс этой эквивалентности, содержащий (a, b).

∘ *Очевидно,*

$$a/b = c/d \Leftrightarrow ads = bcs \text{ для некоторого } s \in S.$$

∘ *На фактор-множестве $(R \times S)/\sim$ корректно определены операции сложения и умножения:*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Фактор-множество $(R \times S)/\sim$ является кольцом относительно данных операций.

Построенное кольцо обозначается RS^{-1} и называется *локализацией* или *кольцом частных* кольца R с множеством знаменателей S.

∘ *Отображение*

$$\tau_S : R \to RS^{-1}, a \mapsto a/1,$$

является гомоморфизмом колец.

Доказательство. Это проверяется непосредственно. □

Таким образом, имеет место

Теорема. *Для кольца R и его мультипликативного множества S, существует кольцо RS^{-1}, состоящее из элементов a/b, где $a \in R$ и $b \in S$, для которых выполняются соотношения, указанные выше.*

Отображение

$$\tau_S : R \to RS^{-1}, a \mapsto a/1,$$

является гомоморфизмом колец. □

Теорема (универсальное свойство кольца частных). *Пусть S — мультипликативное множество кольца R.*

Кольцо $K = RS^{-1}$ обладает следующими свойствами.

(1) *Существует гомоморфизм $\tau_S : R \to K$, переводящий элементы из S на обратимые элементы кольца K.*

(2) *Для любого кольца K' и гомоморфизма $\tau'_S : R \to K'$, переводящего элементы из S на обратимые элементы, существует единственный гомоморфизм $\varphi : K \to K'$, делающий коммутативной диаграмму*

$$\begin{array}{ccc} K & \overset{\varphi}{\dashrightarrow} & K' \\ & {\scriptstyle\tau_S}\nwarrow \quad \nearrow{\scriptstyle\tau'_S} & \\ & R & \end{array} .$$

Обратно, если для некоторого кольца K выполняются записанные условия, то имеет место изоморфизм $K \simeq RS^{-1}$.

Доказательство этой теоремы аналогично доказательству универсального свойства поля частных. □

10. Характеристика кольца

В данном разделе кольца и подкольца предполагаются унитальными.

В кольце R для произвольного элемента a положим

$$ma = \begin{cases} \underbrace{a + \ldots + a}_{m}, & \text{при } m > 0; \\ \underbrace{(-a) + \ldots + (-a)}_{-m}, & \text{при } m < 0; \\ 0, & \text{при } m = 0. \end{cases}$$

Если для некоторого положительного числа m выполняется равенство $m \cdot 1 = 0$, то наименьшее такое m назовём *характеристикой* кольца R; будем считать характеристику равной нулю, если такого m не существует. Обозначим $\mathrm{char}R$ характеристику кольца R. Отметим ряд свойств.

∘ *В любом кольце среди подколец имеется наименьшее по включению.* Оно совпадает с пересечением всех подколец и состоит из целочисленных кратных единицы.

∘ *В любом поле имеется наименьшее по включению подполе.* Оно совпадает с пересечением всех подполей, является полем частных наименьшего подкольца и называется *простым (под)полем.*

∘ *Наименьшее подкольцо нулевой характеристики изоморфно кольцу целых чисел. Простое подполе нулевой характеристики изоморфно полю рациональных чисел.*

∘ *В кольце положительной характеристики m наименьшее подкольцо изоморфно кольцу $\mathbb{Z}/m\mathbb{Z}$.*

∘ *Характеристика целостного кольца (в частности, поля) не может быть составным числом.*

∘ *В поле простой характеристики p наименьшее подкольцо совпадает с простым подполем и изоморфно кольцу $\mathbb{Z}/p\mathbb{Z}$.*

Упражнение. Пусть K — коммутативное кольцо с единицей простой характеристики p. Тогда выполняются следующие условия.

∘ В кольце K для любых элементов x, y и для любого натурального числа n выполняется соотношение

$$(x+y)^{p^n} = x^{p^n} + y^{p^n}.$$

∘ Отображение

$$K \to K, x \mapsto x^{p^n},$$

является эндоморфизмом колец.

ГЛАВА 10

Степенные ряды

В данной главе изучаются степенные ряды одной переменной с коэффициентами в коммутативном кольце с единицей.

1. Степенные ряды и ряды Лорана

Пусть R — коммутативное кольцо с единицей и x — элемент, не принадлежащий ему. Рассмотрим выражение

$$a_0x^0 + a_1x^1 + a_2x^2 + \dots,$$

где $a_0, a_1, \dots$ — произвольные элементы кольца R. Такое выражение называется (формальным) степенным рядом над кольцом R от переменной x и элементы $a_0, a_1, \dots$ называются его коэффициентами.

Пусть заданы степенные ряды

$$a(x) = \sum_k a_k x^k, b(x) = \sum_k b_k x^k.$$

Их суммой называется ряд

$$\sum_k c_k x^k, \text{ где } c_k = a_k + b_k \text{ для всех } k,$$

их произведением называется ряд

$$\sum_k d_k x^k, \text{ где } d_k = a_0b_k + \dots + a_kb_0 \text{ для всех } k.$$

Непосредственно проверяется, что степенные ряды над коммутативным кольцом с единицей R сами образуют коммутативное кольцо с единицей с операциями сложения и умножения, определёнными выше. Это кольцо называется кольцом степенных рядов над кольцом R от переменной x и обозначается $R[[x]]$. В нём нулём является нулевой ряд, у которого все коэффициенты равны нулю. Единицей является ряд $1x^0 + 0x^1 + 0x^2 + \dots$. Имеет место изоморфное вложение колец:

$$R \to R[[x]], a \mapsto a + 0x^0 + 0x^2 + \dots.$$

Для ненулевого ряда $a(x)$, записанного выше, наименьшее значение n, такое, что $a_n \neq 0$, назовём *индексом* и обозначим $\operatorname{ind} a$. Коэффициент a_n назовём *младшим коэффициентом* степенного ряда a. Удобно считать $\operatorname{ind} 0 = +\infty$. Отметим следующее свойство.

∘ *Для ненулевых рядов* $a(x), b(x)$ *имеют место соотношения*

$$\operatorname{ind}(a(x)+b(x)) \geqslant \max(\operatorname{ind} a(x), \operatorname{ind} b(x)),$$
$$\operatorname{ind}(a(x)b(x)) \geqslant \operatorname{ind} a(x) + \operatorname{ind} b(x).$$

∘ *Второе неравенство строгое в единственном случае — когда младшие коэффициенты рядов* a, b *в произведении дают ноль.*

∘ *Для целостного кольца* R *это невозможно.* □

Таким образом, верна

Теорема. *Кольцо формальных степенных рядов над целостным кольцом целостное.* □

Сделаем пару замечаний.

∘ Пусть K — поле. Тогда кольцо $K[[x]]$ целостное и обладает полем частных, которое обозначается $K((x))$. Введём следующие обозначения. Для произвольного натурального n положим

$$x^{-n} = (x^n)^{-1} \text{ и } a_0x^{-n} + a_1x^{1-n} + \ldots = x^{-n}(a_0x^0 + a_1x^1 + \ldots).$$

Тогда элементы поля частных записываются в виде рядов

$$a_0x^{-n} + a_1^{-n+1} + \ldots,$$

где n — натуральное и $a_0, a_1, \ldots$ — элементы из K. Такие ряды называются *рядами Лорана.*

∘ Последовательным добавлением переменных $x_1, \ldots, x_n$ получается кольцо

$$R[[x_1, \ldots, x_n]] = R[[x_1]] \ldots [[x_n]]$$

формальных степенных рядов с коэффициентами в кольце R от переменных $x_1, \ldots, x_n$, а также поле

$$K((x_1, \ldots, x_n)) = K((x_1)) \ldots ((x_n))$$

формальных степенных рядов Лорана с коэффициентами в поле K от переменных $x_1, \ldots, x_n$.

Упражнение. Свободным членом степенного ряда называется коэффициент, стоящий при нулевой степени переменной. Проверьте, что ряд тогда и только тогда обратим в кольце $R[[x]]$, когда его свободный член обратим в кольце R.

2. Дифференцирование рядов

По-прежнему пусть R — коммутативное кольцо с единицей и рассматриваются степенные ряды от одной переменной с коэффициентами в

кольце R. *Производной* ряда $a(x) = \sum_{k\geqslant 0} a_k x^k$ называется ряд

$$\sum_{k\geqslant 1} k a_k x^{k-1}.$$

Производная обозначается $a'(x)$ или $(d/dx)a(x)$.

Упражнение. Введём ещё одну переменную t и, действуя в кольце $R[[x,t]]$, раскроем скобки в выражении

$$a(x+t) = A_0(x) + A_1(x)t + A_2(x)t^2 \dots .$$

Проверьте, что

$$A_0(x) = a(x), A_1(x) = a'(x)$$

и тогда производную $a'(x)$ можно получить, подставив $t = 0$ в ряд

$$(a(x+t) - a(x))/t = A_1 + A_2 t + \dots .$$

Отметим следующие свойства производной.

∘ *Производная константы равна нулю.*

∘ *Над кольцом нулевой характеристики верно обратное: ряд с нулевой производной является константой.*

∘ $(a(x) + b(x))' = a'(x) + b'(x)$.

∘ $(\alpha a(x))' = \alpha a'(x)$ *для любой константы* α *из* R.

∘ $(a(x)b(x))' = a'(x)b(x) + a(x)b'(x)$.

∘ $(a(b(x))' = a'(b(x))b'(x)$ *для любого ряда* $b(x)$ *без свободного члена.*

Здесь $a(x), b(x)$ — ряды с коэффициентами в кольце R.

Упражнения.

∘ Докажите перечисленные свойства.

∘ Над полем положительной характеристики p ряд имеет нулевую производную тогда и только тогда, когда является p-й степенью. Указание: полезно, предварительно проверив, воспользоваться равенством

$$a(x)^p = a(x^p).$$

Далее рассматриваются ряды над полем K нулевой характеристики.

∘ Докажите, что для любого ряда $a(x)$ существует единственный ряд без свободного члена, чья производная равна $a(x)$. Такой ряд называется *первообразной* или *интегралом* ряда $a(x)$ и обозначается $\int a(x)dx$. Проверьте, что

$$\int a(x)dx = \sum_{k\geqslant 1} \frac{a_{k-1}}{k} x^k.$$

∘ Ряды

$$\exp(x) = \sum_{k\geqslant 0} \frac{x^k}{k!}, \ln(1+x) = \sum_{k\geqslant 1} (-1)^{k-1} \frac{x^k}{k}$$

называются соответственно *экспонентой* и *логарифмом*. Докажите, что

$$\exp(\ln(1+x)) = 1+x, \ln(\exp(x)) = x.$$

∘ Проверьте, что $\exp(x)$ — единственный ряд, совпадающий со своей производной.

∘ Проверьте, что

$$\ln(1+x) = \int \frac{dx}{1+x}.$$

3. Алгебраические операции над рядами

Пусть T — произвольное множество. Напомним, что через $R[[x]]^T$ обозначается множество наборов

$$\alpha = (\alpha_s(x) | \alpha_s(x) \in R[[x]], s \in T),$$

индексированных элементами из множества T.

Пусть A — некоторое множество наборов из $R[[x]]^T$. Функцию

$$A \to R[[x]], \alpha \mapsto \overline{\alpha}(x),$$

где

$$\overline{\alpha}(x) = \sum_{k\geqslant 0} \overline{\alpha}_k x^k,$$

будем называть алгебраической операцией над степенными рядами, если для любого набора α из множества A вычисление любого коэффициента $\overline{\alpha}_k$ ряда $\overline{\alpha}$ требует выполнения в кольце R конечного числа операций сложения и умножения над коэффициентами рядов $\alpha_s(x)$, где $s \in T$.

Примеры.

∘ Сложение и умножение являются алгебраическими операциями.

∘ Алгебраической является операция обращения

$$R[[x]]^\times \to R[[x]]^\times, a(x) \mapsto 1/a(x).$$

∘ Алгебраическими операциями является дифференцирование

$$(d/dx) : R[[x]] \to R[[x]], a(x) \mapsto a'(x)$$

и интегрирование

$$\int : R[[x]] \to xR[[x]], a(x) \mapsto \int a(x)dx.$$

(Композиция.) Обозначим через

$$xR[[x]]$$

множество рядов без свободного члена. Алгебраической является операция

$$R[[x]] \times xR[[x]] \to R[[x]], (a(x), b(x)) \mapsto a(b(x))$$

подстановки ряда без свободного члена вместо переменной в произвольный степенной ряд.

Множество $A \subseteq (R[[x]])^T$ назовём суммируемым, если в нём для любого набора α, для любого натурального k и почти всех индексов s из множества T k-й коэффициент α_{sk} ряда $\alpha_s(x) = \sum_k \alpha_{sk} x^k$ равен нулю.

Пусть далее множество A является суммируемым.

(Суммирование.) Алгебраической является операция

$$\Sigma : A \to R[[x]], \alpha \mapsto \overline{\alpha}(x),$$

где

$$\overline{\alpha}_k = \sum_{s \in T} \alpha_{sk}.$$

(Произведение.) Обозначим через

$$1 + xR[[x]]$$

множество рядов с единичным свободным членом.

Пусть $A \subseteq (1 + xR[[x]])^T$. Алгебраической является операция

$$\Pi : A \to R[[x]], \alpha \mapsto \overline{\alpha}(x),$$

где

$$\overline{\alpha}_k = \sum_r \sum_{s_1,\ldots,s_r} \sum_{k_1+\ldots+k_r=k} \alpha_{s_1 k_1} \cdots \alpha_{s_1 k_r}.$$

для любого натурального k. Здесь сумма вычисляется для всевозможных наборов элементов $s_1, \ldots, s_r$ из множества T и натуральных чисел $k_1, \ldots, k_r$, где $k_1 + \ldots + k_r = k$.

4. Экспоненцирование и логарифмирование

Далее рассматриваются степенные ряды от переменной x с коэффициентами в поле K нулевой характеристики. Для ряда $a(x)$ без свободного члена ряды

$$\exp(a(x)) = \sum_{k \geqslant 0} \frac{a(x)^k}{k!}, \ln(1 + a(x)) = \sum_{k \geqslant 1} \frac{(-1)^{k-1} a(x)^k}{k},$$

называются *экспонентой* ряда $a(x)$ и *логарифмом* ряда $1+a(x)$. Таким образом определены алгебраические операции

$$\exp : xK[[x]] \to 1+xK[[x]], a(x) \mapsto \exp(a(x)),$$

$$\ln : 1+xK[[x]] \to xK[[x]], 1+a(x) \mapsto \ln(1+a(x)),$$

которые называются *экспоненцированием* и *логарифмированием*.

Отметим, что множества $xK[[x]]$ и $1+xK[[x]]$ являются абелевыми группами, первая с операцией сложения, вторая — с умножением. Верна

Теорема. *Экспоненцирование и логарифмирование являются взаимно обратными изоморфизмами абелевых групп.*

Доказательство теоремы опирается на следующее

Упражнение. Ответьте на вопрос и докажите утверждения ниже.

∘ Чему равна логарифмическая производная $(\ln(a(x)))'$ ряда $a(x)$ с единичным свободным членом?

∘ Для рядов $a(x), b(x)$ с единичным свободным членом равносильны условия:

(1) $a'(x) = b'(x)$;

(2) $a(x) = b(x)$;

(3) $a'(x)/a(x) = b'(x)/b(x)$;

(4) $\ln(a(x)) = \ln(b(x))$.

∘ Для рядов без свободного члена равносильны условия (1,2).

Доказательство теоремы. С использованием упражнения для ряда $a(x)$ без свободного члена проверяются соотношения

$$\exp(\ln(1+a(x))) = 1+a(x), \ln(\exp(a(x))) = a(x);$$

то есть exp и ln — взаимно обратные отображения. Далее следует проверить, что логарифмирование является гомоморфизмом групп. □

Упражнение. Восполните пропущенные детали доказательства.

5. Биномиальная формула

По-прежнему рассматриваются степенные ряды над полем K нулевой характеристики. Для элемента α из K и ряда $a(x)$ без свободного члена положим

$$(1+a(x))^\alpha = \exp(\alpha \ln(1+a(x))).$$

Этот ряд называется степенью ряда $1+a(x)$ с показателем α. Тем самым определена (алгебраическая) операция

$$1+xK[[x]] \to 1+xK[[x]], 1+a(x) \mapsto (1+a(x))^\alpha,$$

которая называется операцией возведения в степень с показателем α. Заметим, что для натурального показателя эта операция совпадает с естественным её пониманием. Отметим ряд свойств этой операции.

- $(1+a(x))^{\alpha}(1+a(x))^{\beta} = (1+a(x))^{\alpha+\beta}$;
- $((1+a(x))^{\alpha})^{\beta} = (1+a(x))^{\alpha\beta}$;
- $((1+a(x)(1+b(x)))^{\alpha} = (1+a(x))^{\alpha}(1+b(x))^{\alpha}$;

Здесь α, β — произвольные элементы поля K и $a(x), b(x)$ — ряды без свободного члена с коэффициентами в K.

Обозначим через $\binom{\alpha}{k}$ коэффициенты ряда $(1+x)^{\alpha}$, так что

$$(1+x)^{\alpha} = \sum_{k \geqslant 0} \binom{\alpha}{k} x^k.$$

Теорема. *Имеет место равенство*

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{1\cdot 2\cdots k}.$$

Доказательство. Продифференцируем разложение бинома, записанное выше, и в полученном равенстве приравняем коэффициенты при степени k слева и справа. В результате получается равенство

$$\binom{\alpha-1}{k-1}\alpha = \binom{\alpha}{k}k.$$

Далее по индукции получаем

$$\begin{aligned}\binom{\alpha}{k} &= \frac{\alpha}{k}\binom{\alpha-1}{k-1}k \\ &= \frac{\alpha(\alpha-1)}{k(k-1)}\binom{\alpha-2}{k-2} \\ &\cdots \\ &= \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k\cdot(k-1)\cdots 1}. \ \square\end{aligned}$$

Упражнения. Проверьте следующие формулы.

- Для любого целого положительного n верно:

$$\binom{-n}{k} = (-1)^k\binom{n+k-1}{k-1} = (-1)^k\binom{n+k-1}{n-1}.$$

- Для любого целого положительного n верно:

$$\binom{1/n}{k} = \frac{(-1)^{k-1}}{n^k}\cdot\frac{(n-1)(2n-1)\cdots((k-1)n-1)}{k!}.$$

∘ В частности, при $n = 2$ получаем:

$$\binom{1/2}{k} = \frac{1}{4^k} \cdot \frac{(-1)^{k-1}}{(2k-1)} \binom{2k}{k}.$$

В завершение раздела рассмотрим

Пример (числа Каталана). Положим $c_0 = 1$ и для любого целого положительного числа k через c_k обозначим количество способов корректно расставить скобки в произведении, содержащем $k+1$ сомножителей. Получаемые так числа

$$c_0 = 1, c_1 = 1, c_2 = 2, c_3 = 5, \ldots,$$

называются *числами Каталана*. Можно заметить, что $c_1 = c_0 c_0$ и для любого $k \geqslant 2$ выполняется равенство

$$c_k = c_1 c_{k-2} + c_2 c_{k-3} + \ldots c_{k-2} c_1.$$

Отсюда следует, что *ряд Каталана* $c(x) = \sum_k c_k x^k$ удовлетворяет соотношению

$$xc(x)^2 = c(x) - 1$$

и является корнем уравнения

$$xt^2 - t - 1 = 0.$$

Корнями этого уравнения в поле $\mathbb{Q}((x))$ являются ряды

$$(1 \pm \sqrt{1-4x})/(2x),$$

но лишь с положительным знаком здесь получается ряд из $\mathbb{Z}[[x]]$.

Следовательно,

$$c(x) = (1 + \sqrt{1+4x})/(2x) \text{ и } c_k = \frac{1}{k+1}\binom{2k}{k} \text{ для любого } k.$$

Упражнение. В примере выше проведите все вычисления подробно.

ГЛАВА 11

Многочлены

Степенной ряд, у которого почти все коэффициенты равны нулю, называется многочленом. Многочлены от переменной x с коэффициентами в коммутативном кольце R, содержащем единицу, сами образуют коммутативное кольцо с единицей, которое является подкольцом в кольце степенных рядов $R[[x]]$. Кольцо многочленов обозначается $R[x]$.

Последовательным присоединением переменных $x_1, \ldots, x_n$ получается кольцо

$$R[x_1, \ldots, x_n] = R[x_1] \ldots R[x_n]$$

многочленов с коэффициентами в кольце R от переменных $x_1, \ldots, x_n$.

В этой главе изучаются многочлены от одной переменной.

1. Многочлены и рациональные выражения

Пусть R — коммутативное кольцо с единицей. Будем рассматривать многочлены от пременной x с коэффициентами в R. Имеет место

Теорема. *Кольцо многочленов над целостным кольцом целостное.*

Доказательство. Это так, поскольку кольцо многочленов содержится в кольце степенных рядов, для которого аналогичная теорема верна. □

Для ненулевого многочлена $a(x) = \sum_k a_k x^k$ наибольшее значение n, для которого $a_n \neq 0$, называется его *степенью* и обозначим $\deg a$. Коэффициент a_n называется *старшим коэффициентом* многочлена $a(x)$. Удобно считать $\deg 0 = -\infty$. Отметим следующие свойства.

∘ Для ненулевых многочленов $a(x), b(x)$ имеют место соотношения

$$\deg(a(x) + b(x)) \leqslant \max(\deg a(x), \deg b(x)),$$
$$\deg(a(x)b(x)) \leqslant \deg a(x) + \deg b(x).$$

∘ Второе неравенство строгое, когда старшие коэффициенты многочленов a, b в произведении дают ноль (что невозможно в целостном кольце).

∘ Существует изоморфное вложение

$$R \to R[x], a \mapsto ax^0 + 0x^1 + 0x^2 + \ldots.$$

Элементы кольца R отождествляются с многочленами в соответствии с этим вложением. Кольцо R, таким образом, содержится в кольце $R[x]$.

Поле частных целостного кольца $R[x]$ обозначается $R(x)$ и называется также полем рациональных выражений над R от переменной x.

2. Деление с остатком

Имеет место

Теорема (о делении с остатком). *Пусть R — коммутативное кольцо с единицей. Тогда в кольце $R[x]$ для любых многочленов f, g, где g — ненулевой многочлен с обратимым старшим коэффициентом, существуют и определены однозначно многочлены q, r, такие, что*

$$f = gq + r, r = 0 \text{ или } \deg r < \deg g. \ \square$$

В условиях теоремы многочлены q, r называют *неполным частным* и *остатком* при делении многочлена f на многочлен g; для остатка используют обозначение $f \mod g$.

Следствие (разложение по степеням). *Пусть R — коммутативное кольцо с единицей. Тогда в кольце $R[x]$ для любого многочлена f и любого многочлена g положительной степени с обратимым старшим коэффициентом существует и определена однозначно последовательность многочленов $f_0, f_1, \ldots$, таких, что*

$$f = f_0 + f_1 g + f_2 g^2 + \ldots, \deg f_k < \deg g \text{ для всех } k. \ \square$$

(Очевидно, почти все многочлены последовательности нулевые.)

3. Алгоритм Евклида

Пусть K — поле. Будем рассматривать многочлены от переменной x с коэффициентами в поле K. Говорят, что многочлен f делит многочлен g, или многочлен f является *делителем* многочлена g, и пишут $f|g$, если для некоторого многочлена h выполняется равенство $fh = g$. Многочлены f, g называются *ассоциированными*, если каждый из них является делителем другого. Это означает, что многочлены отличаются множителем, равным ненулевой константе из K. Будем писать $f \sim g$ в этой ситуации. Многочлен f называют *наибольшим общим делителем* набора многочленов $f_0, f_1, \ldots$, если он является общим делителем этих многочленов и сам делится на любой их общий делитель.

Наибольший общий делитель определён с точностью до ассоциированности. Несмотря на это будем писать $f = \gcd(f_0, f_1, \ldots)$, если f — наибольший общий делитель многочленов $f_0, f_1, \ldots$; равенство здесь означает ассоциированность.

Отметим, что наибольший общий делитель не изменяется при перестановке многочлено f_k, при добавлении к ним нулевого или повторяющегося

многочлена. Вычисление наибольшего общего делителя для набора многочленов $f_0, \ldots, f_n$ сводится в вычислению наибольшего общего делителя двух многочленов, так как выполняется соотношение

$$\gcd(f_0, \ldots, f_n) = \gcd(f_0, \gcd(f_1, \ldots, f_n));$$

(для доказательства этого соотношения следует проверить, что общие делители у набора многочленов $f_0, \ldots, f_n$ и у пары многочленов f_0, $\gcd(f_1, \ldots, f_n)$ одни и те же). Для вычисления наибольшего общего делителя пары многочленов существует эффективный алгоритм, который называется алгоритмом Евклида. Он основывается на следующей теореме.

Теорема (алгоритм Евклида). *Пусть в кольце $K[x]$ для ненулевых многочленов $f_0, \ldots, f_n$ выполняются условия*

(1) $f_{i-1} \mod f_i = f_{i+1}$ *для* $1 \leqslant i \leqslant n-1$;

(2) $f_{n-1} \mod f_n = 0$;

Тогда $f_n = \gcd(f_0, f_1)$. $\square$

Следствие (линейное выражение для НОД). *Пусть f — наибольший общий делитель многочленов f_0, f_1 в кольце $K[x]$. Тогда для некоторых многочленов s, t из $K[x]$ верно равенство:*

$$f = s \cdot f_0 + t \cdot f_1. \ \square$$

Записанная теорема и её следствие доказываются также как для чисел.

4. Разложение на неприводимые множители

Будем рассматривать многочлены с коэффициентами в поле K. Отметим следующие свойства.

∘ *Для многочлена f положительной степени следующие условия равносильны:*

(1) *для любых многочленов g, h верна импликация:*

$$f|g \text{ или } f|h, \text{ если } f|gh;$$

(2) *для любых многочленов g, h верна импликация:*

$$g \in K^\times \text{ или } h \in K^\times, \text{ если } f = gh.$$

Многочлен положительной степени, для которого выполняются условия (1–2), называется *tнеприводимым* над полем K. Отметим ряд свойств.

∘ *Многочлен положительной степени имеет неприводимый делитель.*

∘ *Существует бесконечно много попарно неассоциированных неприводимых многочленов.*

Теорема (об однозначном разложении). *В кольце $K[x]$ любой многочлен положительной степени можно представить в виде произведения неприводимых многочленов. Подобное представление единственно с точностью до порядка сомножителей и их ассоциированности.*

Доказательства записанных свойств и теоремы такие же как для чисел.

5. Классы вычетов многочленов

По-прежнему рассматриваются многочлены с коэффициентами в поле K, от переменной x. Пусть $f(x)$ — некоторый такой многочлен. Многочлены g, h назовём *сравнимыми по модулю* многочлена f, если $f|(g-h)$, иными словами, это означает, что многочлены g, h отличаются слагаемым, кратным f. Будем писать $g \equiv h \mod f$ в этом случае.

Будем считать, что многочлен f имеет положительную степень, равную n (отношение сравнимости имеет тривиальный смысл в остальных случаях). Отметим ряд свойств.

∘ *Отношение сравнимости по модулю многочлена f является эквивалентностью на кольце $K[x]$.* □

Классы этой эквивалентности называются *классами вычетов по модулю* f. Класс вычетов многочлена g обозначается

$$[g], [g]_f \text{ или } g(x) + f(x)K[x].$$

Он состоит из многочленов, которые отличаются от многочлена g слагаемым, кратным f.

∘ *Два многочлена тогда и только тогда принадлежат одному и тому же классу вычетов по модулю многочлена f, когда имеют одинаковые остатки при делении на f.*

Это означает, что в каждом классе вычетов имеется единственный многочлен степени, меньшей n. Он совпадает с остатком, который дают при делении на f многочлены этого класса.

∘ *Сложение и умножение многочленов индуцирует следующие операции сложения и умножения классов вычетов:*

$$[f] + [g] = [f + g], [f][g] = [fg].$$ □

∘ *Классы вычетов по модулю f образует коммутативное кольцо с единицей с операциями сложения и умножения, определёнными выше.*

Это кольцо называется *кольцом классов вычетов* кольца $K[x]$ по модулю многочлена f и обозначается $K[x]/f(x)K[x]$ или $K[x]/f(x)$.

∘ *Для многочленов g, h равносильны условия:*

(1) $gh \equiv 1 \mod f$;

(2) $[g][h] = [1]$. $\square$

Классы (многочлены), для которых эти условия выполняются, называются взаимно обратными и каждый из них по отношению к другому называется обратным (по модулю многочлена f). Класс (многочлен), для которого существует обратный, называется *обратимым* по модулю f.

$\circ$ *Произведение классов (многочленов), обратимых по модулю многочлена $f(x)$, обратимо по модулю многочлена $f(x)$.*

Обратимые классы вычетов образуют группу $(K[x]/f(x)K[x])^{\times}$. Это — мультипликативна группа классов вычетов по модулю многочлена $f(x)$. Имеет место

Теорема. *В кольце $K[x]$ следующие условия равносильны:*

(1) *многочлен $g(x)$ обратим по модулю многочлена $f(x)$;*

(2) $\gcd(f(x), g(x)) = 1$. $\square$

Следствие. *Кольцо $K[x]/f(x)$ тогда и только тогда является полем, когда многочлен $f(x)$ неприводим над полем K.*

Доказательство. Если кольцо $K[x]/f(x)$ является полем, то многочлен $f(x)$ неприводим, так как иначе для некоторых многочленов $g(x)$ и $h(x)$ положительной степени выполняется равенство $f(x) = g(x)h(x)$. Тогда в кольце $K[x]/f(x)$ для ненулевых классов $[g(x)]$ и $[h(x)]$ выполняется равенство

$$[g(x)][h(x)] = [0],$$

что противоречит отсутствию делителей нуля в поле. Обратно, если многочлен $f(x)$ неприводим, то любой ненулевой многочлен степени, меньшей n, взаимно прост с многочленом $f(x)$ и тогда обратим по его модулю. Тогда любой ненулевой класс вычетов обратим в кольце $K[x]/f(x)$ и это кольцо является полем. $\square$

6. Присоединение корня

Пусть многочлен $f(x)$ неприводимый над полем K, степени n. Кольцо $K[x]/f(x)$ является полем в этом случае. Продолжим изучение свойств этого поля.

$\circ$ *Имеет место изоморфное вложение:*

$$K \to K[x]/f(x), a \mapsto [a].$$

Отождествим элементы поля K с их образами при этом вложении (можно говорить тогда, что поле K содержится в поле $K[x]/f(x)$), а класс $[x]$ станем обозначать буквой γ.

Поле $K[x]/f(x)$ обозначается теперь $K[\gamma]$ или $K(\gamma)$ и называется *полем, полученным присоединением к полю K корня γ многочлена $f(x)$.*

В соответствии со сказанным имеется изоморфизм полей

$$K[x]/f(x) \to K(\gamma), [g(x)] \mapsto g(\gamma).$$

Замечание. Отметим, что алгебраические структуры $K[x]$ и $K[\gamma]$ не изоморфны, как и $K(x)$ и $K(\gamma)$, несмотря на однотипные обозначения. В общем случает обозначения типа $K[\cdot]$ и $K(\cdot)$ используются соответственно для наименьшего кольца и поля, включающего поле K и элементы, указанные в скобках. Отметим также, что

$$K[\gamma] = K(\gamma), K[x] \neq K(x).$$

$\circ$ *Каждый элемент поля $K(\gamma)$ единственным образом записывается как*

$$a_0 + a_1\gamma + \ldots + a_{n-1}\gamma^{n-1},$$

где $a_0, a_1, \ldots, a_{n-1}$ — элементы поля K.

В частности, $|K(\gamma)| = q^n$, если $|K| = q$.

Записанные так элементы складываются и перемножаются как многочлены от переменной γ (как если бы γ являлось переменной) с последующей заменой результата остатком по модулю многочлена $f(\gamma)$ (для сложения вычисление остатка не изменяет результата). В частности, для элемента γ в поле $K(\gamma)$ выполняется равенство $f(\gamma) = 0$ (элемент γ является корнем многочлена f).

Поле E называется *расширением* поля K и K называется *подполем* поля E, если имеет место включение $K \subseteq E$ и операции над общими элементами в обоих полях выполняются одинаково. Иными словами, тождественное отображение

$$\mathrm{id}_K : K \to E, a \mapsto a,$$

является изоморфным вложением. Имеет место

Теорема. *Многочлен положительной степени с коэффициентами в поле K имеет корень в некотором расширении поля K.*

Присоединение корня неприводимого многочлена к полю используется для построения конечных полей. Рассмотрим соответствующие примеры.

$\circ$ Пусть p — простое число. Поле $\mathbb{F}_{p^n}$ порядка p^n можно построить как расширение $\mathbb{F}_p(\gamma)$, присоединив к простому полю $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ корень γ неприводимого многочлена $f(x)$ степени n. Элементы этого расширения записываются многочленами от γ, имеющими коэффициенты из поля $\mathbb{F}_p$ и степень, меньшую n, над которыми операции сложения и умножения выполняются с учётом равенства $f(\gamma) = 0$ (иначе говоря — по модулю многочлена $f(\gamma)$).

Известно, что порядок конечного поля является степенью простого числа, существует единственное с точностью до изоморфизма конечное поле порядка p^n и его можно построить указанным способом. Это будет установлено позднее, при изучении конечных полей. В частности, всегда найдётся неприводимый многочлен f степени n, необходимый для построения. Единственное с точностью до изоморфизма поле порядка p^n получается описанным способом при выборе любого многочлена f степени n, неприводимого над полем $\mathbb{F}_p$.

∘ Поле $\mathbb{F}_4$ порядка 4 получается как расширение $\mathbb{F}_2(\gamma)$, где γ — корень многочлена $f(x) = x^2 + x + 1$. Оно состоит из многочленов

$$0, 1, \gamma, \gamma + 1,$$

над которыми операции выполняются по модулю многочлена $\gamma^2 + \gamma + 1$. В том числе выполняется соотношение $\gamma^2 + \gamma + 1 = 0$.

Можно записать явные формулы

$$(a\gamma + b) + (c\gamma + d) = (a + c)\gamma + (b + d),$$

$$(a\gamma + b) \cdot (c\gamma + d) = (ac + ad + bc)\gamma + (ac + bd),$$

где операции над коэффициентами a, b, c, d выполняются в поле $\mathbb{F}_2$. Формула для умножения получена в результате раскрытия скобок

$$(a\gamma + b) \cdot (c\gamma + d) = (ac)\gamma^2 + (ad + bc)\gamma + (bd)$$

с использование соотношения $\gamma^2 = \gamma + 1$

Такой же вид будут иметь формулы для сложения и умножения в любом расширении $K(\gamma)$, где многочлен $x^2 - x - 1$ неприводим над полем K и γ — его корень. В этом случае поле состоит из элементов $a\gamma + b$, где a, b из K, и коэффициенты a, b, c, d в записанных формулах — призвольные элементы из K.

∘ Поле $\mathbb{F}_8$ порядка 8 получается присоединием к простому полю $\mathbb{F}_2 = \{0, 1\}$ корня γ неприводимого многочлена $f(x) = x^3 + x + 1$. Оно состоит из многочленов

$$0, 1, \gamma, \gamma + 1, \gamma^2, \gamma^2 + 1, \gamma^2 + \gamma, \gamma^2 + \gamma + 1,$$

над которыми операции выполняются по модулю многочлена $\gamma^3 + \gamma + 1$. В том числе здесь $\gamma^3 + \gamma + 1 = 0$.

∘ Поле $\mathbb{F}_9$ порядка 9 получается, присоединием к простому полю $\mathbb{F}_3 = \{0, 1, 2\}$ корня γ неприводимого многочлена $f(x) = x^2 + 1$. Оно состоит из многочленов

$$0, 1, 2, \gamma, \gamma + 1, \gamma + 2, 2\gamma, 2\gamma + 1, 2\gamma + 2,$$

над которыми операции выполняются по модулю многочлена $\gamma^2 + 1$.

Явные формулы выглядят так:

$$(a\gamma + b) + (c\gamma + d) = (a + c)\gamma + (b + d),$$
$$(a\gamma + b) \cdot (c\gamma + d) = (ad + bc)\gamma + (bd - ac),$$

где операции над коэффициентами a, b, c, d выполняются в поле $\mathbb{F}_3$.

Такой же вид имеют формулы для сложения и умножения в любом расширении $K(\gamma)$, где многочлен $x^2 + 1$ неприводим над полем K (то есть -1 не является квадратом) и γ — его корень.

Заметим, что многочлен $x^2 - x - 1$ неприводим над $\mathbb{F}_3$ и его можно использовать для построения поля из 9 элементов. Формулы для сложения и умножения в этом случае будут выглядеть как в одном из примеров выше (каком именно?).

7. Разложение на простейшие дроби

Станем рассматривать рациональные выражения (дроби) из поля $K(x)$. Дробь с взаимно простыми числителем и знаменателем называется *несократимой*. Дробь, в которой знаменатель является степенью неприводимого многочлена, называется *простейшей*.

Теорема. *Пусть в кольце $K[x]$ имеет место разложение:*

$$g(x) = g_1(x)^{m_1} \cdots g_l(x)^{m_l},$$

где многочлены $g_1(x), \ldots, g_l(x)$ — попарно неассоциированные и неприводимые над K, $m_1, \ldots, m_l$ — целые положительные числа. Тогда в кольце $K[x]$ для любого многочлена $f(x)$, взаимно простого с $g(x)$, имеется единственное представление

$$\frac{f(x)}{g(x)} = q(x) + \sum_{i=1}^{l} \sum_{j=1}^{m_i} \frac{f_{ij}(x)}{g_i(x)^j},$$

где для многочленов $q(x), f_{ij}(x)$ выполняются соотношения

$$\deg q(x) = \deg f(x) - \deg g(x), \text{ если } \deg f(x) > \deg g(x), \text{ иначе } q(x) = 0;$$
$$\deg f_{ij}(x) < \deg g_i(x), \text{ где } 1 \leqslant i \leqslant l, 1 \leqslant j \leqslant m_i.$$

Доказательство теоремы следует из свойств, устанавливаемых ниже. □

∘ *В условиях теоремы имеется единственное представление*

$$\frac{f(x)}{g(x)} = q(x) + \sum_{i=1}^{r} \frac{f_i(x)}{g_i(x)},$$

где

$$\deg q(x) = \deg f(x) - \deg g(x), \text{ если } \deg f(x) > \deg g(x), \text{ иначе } q(x) = 0;$$
$$\deg f_i(x) < \deg g_i(x), \text{ где } 1 \leqslant i \leqslant l.$$

Доказательство. Достаточно доказать это для $l = 2$. Для этого разделим f на g с остатком, то есть представим в виде

$$f = gq + r, \text{ где } \deg g < \deg f \text{ или } g = 0;$$

и запишем линейное выражение для $\gcd(g_1, g_2)$, то есть запишем

$$1 = sg_1 + tg_2$$

для подходящих многочленов s, t. Тогда для многочленов

$$f_1 = rt \mod g_1 \text{ и } f_2 = rs \mod g_2$$

выполняются соотношения

$$r = f_2 g_1 + f_1 g_2, \deg f_1 < \deg g_1, \deg f_2 < \deg g_2.$$

Отсюда

$$\frac{f}{g} = q + \frac{f_1}{g_1} + \frac{f_2}{g_2}.$$

Обратно, если записанное соотношение имеет место, то многочлен q определён однозначно, так как является неполным частным при делении f на g. В этой ситуации многочлен $f_1 g_2 + f_2 g_1$ совпадает с остатком r. Многочлены f_1, f_2 определы однозначно, так как являются представителями наименьшей степени в соответствующих классах

$$[r][g_2]^{-1} \text{ кольца } K[x]/g_1(x), \text{ и } [r][g_1]^{-1} \text{ кольца } K[x]/g_2(x). \square$$

∘ *Пусть l — целое положительное число. В кольце $K[x]$ для любых многочленов $h(x), g(x)$, таких, таких, что $\deg h < \deg g^l$ имеется единственное представление*

$$\frac{h}{g^l} = \sum_{i=1}^{l} \frac{h_i}{g^i},$$

где h_i — многочлены из $K[x]$, такие что выполняются соотношения

$$\deg h_i < \deg g, \text{ где } 1 \leqslant i \leqslant l.$$

Доказательство следует из существования и единственности для многочлена h разложения по степеням многочлена g. $\square$

Замечание. Выражение, записанное в теореме, называется разложением дроби f/g на простейшие. Наиболее просто оно выглядит в случае, когда многочлен g разлагается над полем K на линейные множители (первой степени). Тогда многочлены f_{ij} — константные. Они легко находятся из соотношений, которые получаются подстановкой значений из поля K вместо переменной в записанное разложение (которое удобно предварительно умножить на многочлен g). Если к тому же все показатели m_i единичные, то простые соотношения для нахождения коэффициентов получаются при подстановке корней.

Упражнение. Выпишите в явном виде выражения для нахождения коэффициентов в последнем случае.

Замечание. Поле $K(x)$ изоморфно вкладывается в поле $K((x))$. Это позволяет рациональное выражение над полем K представить в виде ряда Лорана, и даже в виде степенного ряда — если свободный член знаменателя не нулевой. В силу доказанной теоремы достаточно уметь это делать для рационального выражения, являющегося простейшей дробью.

Наиболее легко это получается, когда знаменатель дроби разлагается на линейные множители над полем K (причём всегда можно добиться этого, расширив поле K). В этом случае задача сводится к обращению дробей вида

$$\frac{1}{(1-\alpha x)^m},$$

где α — значение, обратное ненулевому корню знаменателя. Степенной ряд для такой дроби был вычислен ранее:

$$\frac{1}{(1-\alpha x)^m} = \sum_{k\geqslant 0} \alpha^k \binom{m+k-1}{m-1} x^k.$$

8. Линейные рекуррентные последовательности

Пусть K — поле нулевой характеристики и

$$c_0, c_1, \ldots,$$

— последовательность его элементов, такая, что для некоторых n элементов $a_1, \ldots, a_n$ и любого натурального $k \geqslant n$ выполняется соотношение

$$c_k + a_1 c_{k-1} + \ldots + a_n c_{k-n} = 0.$$

Иными словами, k-й элемент последовательности, начиная с $k = n$, выражается линейно через n предшествующих элементов следующим образом:

$$c_k = -(a_1 c_{k-1} + \ldots + a_n c_{k-n}).$$

Вся последовательность, таким образом, однозначно определяется своими первыми n членами. В этом случае рассматриваемая последовательность называется рекуррентной над полем K и многочлен

$$a(x) = 1 + a_1 x + \ldots + a_n x^n$$

называется её характеристическим многочленом.

Опишем, как можно получить явную формулу для k-го члена линейной рекуррентной последовательности. Рассмотрим степенной ряд

$$b(x) = a(x)c(x), \text{ где } c(x) = \sum_{k \geqslant 0} c_k x^k.$$

Он является в действительности многочленом степени, меньшей n, с коэффициентами

$$b_0 = c_0, b_1 = c_1 + a_1 c_0, \ldots, b_{n-1} = c_{n-1} + a_1 c_{n-2} + \ldots + a_{n-1} c_0.$$

и мы можем найти формулу для k-го члена, представив дробь

$$c(x) = \frac{b(x)}{a(x)}$$

в виде степенного ряда способом, описанным ранее.

Пример (числа Фибоначчи). Рассмотрим линейную рекуррентную последовательность чисел Фибоначчи

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots,$$

определяемую условиями

$$c_0 = 0, c_1 = 1, \text{ и } c_k = c_{k-1} + c_{k-2} \text{ для всех } k \geqslant 2.$$

Её характеристический многочлен равен

$$a(x) = 1 - x - x^2.$$

Тогда $b(x) = x$ и

$$c(x) = \frac{b(x)}{a(x)} = \frac{x}{1 - x - x^2}$$

Найдём явное выражение для чисел Фибоначчи. Для этого запишем характеристический многочлен в виде

$$a(x) = (1 - a_+ x)(1 - a_- x),$$

где $a_\pm$ — величины, обратные корням многочлена $a(x)$, то есть корни многочлена $x^2 - x - 1$, равные

$$a_\pm = \frac{1 \pm \sqrt{5}}{2}.$$

Тогда

$$\begin{aligned} c(x) &= \frac{b(x)}{a(x)} \\ &= \frac{x}{(1-a_+x)(1-a_-x)} \\ &= \frac{x}{a_+-a_-}\Big(\frac{a_+}{1-a_+x} - \frac{a_-}{1-a_-x}\Big) \\ &= \frac{1}{a_+-a_-}\sum_{k\geqslant 1}(a_+^k - a_-^k)x^k \\ &= \frac{1}{a_+-a_-}\sum_{k\geqslant 0}(a_+^k - a_-^k)x^k. \end{aligned}$$

Отсюда получается явная формула для k-го члена:

$$\begin{aligned} c_k &= \frac{1}{a_+-a_-}(a_+^k - a_-^k) \\ &= \frac{1}{\sqrt{5}}\Big(\Big(\frac{1+\sqrt{5}}{2}\Big)^k - \Big(\frac{1-\sqrt{5}}{2}\Big)^k\Big) \\ &= \frac{(1+\sqrt{5})^k - (1-\sqrt{5})^k}{2^k\sqrt{5}}. \end{aligned}$$

Получили формулу Бине для чисел Фибоначчи:

$$c_k = \frac{(1+\sqrt{5})^k - (1-\sqrt{5})^k}{2^k\sqrt{5}} \text{ при } k \geqslant 0.$$

ГЛАВА 12

Корни многочленов

Продолжим изучение многочленов от одной переменной и с коэффициентами в поле.

1. Теорема Безу и схема Горнера

Пусть K — коммутативное кольцо с единицей. Будем рассматривать многочлены от одной переменной с коэффициентами в кольце K. Подставим в многочлен $f(x)$ вместо переменной элемент c из кольца и выполним вычисления. Элемент $f(c)$, который получается в результате, называется *значением* многочлена $f(x)$ в точке c. Элемент c, такой, что $f(c) = 0$, называется *корнем* многочлена $f(x)$.

Теорема Безу. *Пусть $f(x)$ — многочлен с коэффициентами в коммутативном кольце с единицей K и c — элемент этого кольца. В кольце $K[x]$ для некоторого многочлена $q(x)$ выполняется соотношение*

$$f(x) = (x - c)q(x) + f(c).$$

Иными словами,

$$f(x) \equiv f(c) \mod (x - c).$$

В частности, элемент c является корнем многочлена $f(x)$ тогда и только тогда, когда многочлен $f(x)$ делится на двучлен $(x - c)$. □

Доказательство. При делении многочлена $f(x)$ на двучлен $(x - c)$ в остатке получается константа. Эта константа совпадает со значением $f(c)$, в чём можно убедиться, подставив c вместо x. □

В условиях теоремы Безу коэффициенты многочлена

$$q(x) = b_0x^{n-1} + \ldots + b_{n-1} \text{ и значение } b_n = f(c)$$

можно вычислить рекурсивно следующим образом:

$$b_0 = a_0, b_1 = a_1 + b_0c, \ldots, b_n = a_n + b_{n-1}c.$$

Такое вычисление называется *схемой Горнера*. Многократное применение схемы Горнера позволяет найти разложение многочлена $f(x)$ по степеням двучлена $(x - c)$.

2. Кратные корни

Пусть $f(x)$ — многочлен с коэффициентами в целостном кольце K и c — его корень, принадлежащий кольцу. Целое положительное число k называется *кратностью корня* c, если

$$(x-c)^k | f(x) \text{ и } (x-c)^{k+1} \nmid f(x).$$

Это равносильно тому, что в кольце $K[x]$ для некоторого многочлена $g(x)$ выполняются условия

$$f(x) = (x-c)^k g(x) \text{ и } g(c) \neq 0.$$

Корень называется *простым* при $k = 1$, или *кратным*, если $k > 1$.

Упражнение. Проверьте равносильность указанных условий.

Имеет место

Теорема (о кратных корнях). *Пусть K — целостное кольцо, $f(x)$ — многочлен с коэффициентами в кольце K и $c_1 \dots c_m$ — различные корни многочлена $f(x)$, принадлежащие кольцу K и имеющие кратности $k_1, \dots, k_m$ соответственно. Тогда в кольце $K[x]$ для некоторого многочлена $g(x)$, такого, что элементы $c_1, \dots, c_m$ не являются его корнями, выполняется равенство*

$$f(x) = (x-c_1)^{k_1} \cdots (x-c_m)^{k_m} g(x).$$

В частности, количество корней многочлена с учётом их кратностей (так что корень кратности k учитывается k раз) не превосходит степени многочлена:

$$\deg f(x) \geqslant k_1 + \ldots + k_m.$$

Доказательство. Теорема доказывается индукцией по числу m различных корней. Предположим по-индукции, что выполняется равенство

$$f(x) = (x-c_1)^{k_1} \cdots (x-c_{m-1})^{k_{m-1}} g(x),$$

где элементы $c_1, \dots, c_{m-1}$ не являются корнями многочлена $g(x)$. Элемент c_m является корнем многочлена $f(x)$ и является корнем многочлена $g(x)$, поскольку кольцо K целостное. Обозначим через l его кратность для многочлена $g(x)$. Тогда двучлен $(x-c_m)^l$ является делителем многочленов $f(x), g(x)$. Заметим, что элемент c_m не является корнем многочленов $f(x)/(x-c_m)^l$, $g(x)/(x-c_m)^l$. Это означает, что $l = k_m$. Теорема доказана. □

Следствие. *Многочлен степени n с коэффициентами в целостном кольце однозначно определяется своими значениями в любых $n+1$ различных точках.*

Доказательство. Предположим, два многочлена степени n принимают одинаковые значения в $n+1$ точках. Все эти точки являются корнями разности данных многочленов, которая является нулевым многочленом по теореме о числе корней. Таким образом, многочлены совпадают.

3. Интерполяция

Имеет место

Теорема. *Пусть n — целое неотрицательное число, $a_0, \ldots, a_n$ — различные и $b_0, \ldots, b_n$ — произвольные элементы из поля K. Тогда в кольце $K[x]$ существует единственный многочлен $f(x)$ степени, не превосходящей n, такой, что $f(a_k) = b_k$ для всех $k, 0 \leqslant k \leqslant n$.*

Доказательство. Задача определения многочлена $f(x)$ в условиях теоремы называется *задачей интерполяции*. Далее будут рассмотрены три классических метода решения этой задачи. Тем самым, будет доказано существание многочлена $f(x)$. Его единственность устанавливается предыдущим следствием. □

Метод Лагранжа. Многочлен $f(x)$ находится следующим образом:

$$f(x) = \sum_k b_k L_k(x)/L_k(a_k), \text{ где } L_k(x) = (x-a_1)\cdots(x-a_n)/(x-a_k).$$

Метод Ньютона. Многочлен $f(x)$ записывается как

$$f(x) = u_0 + u_1(x-a_0) + \ldots + u_n(x-a_0)\cdots(x-a_{n-1}),$$

где коэффициенты $u_0, \ldots, u_{n-1}$ находятся из соотношений

$$b_0 = u_0,$$

$$b_1 = u_0 + u_1(a_1 - a_0),$$

$$\ldots$$

$$b_n = u_0 + u_1(a_n - a_0) + \ldots + u_n(a_n - a_0)\cdots(a_n - a_{n-1}),$$

которые получаются подстановкой значений $a_0, \ldots, a_n$ вместо переменной x и значений $b_0, \ldots, b_n$ вместо $f(x)$ в записанное выше равенство.

Метод линейных уравнений. Коэффициенты многочлена $f(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_0$ можно найти, решив систему уравнений

$$\begin{array}{ccccccccc} c_0 & + & a_0 c_1 & + & \ldots & + & a_0^n c_n & = & b_0, \\ c_0 & + & a_1 c_1 & + & \ldots & + & a_1^n c_n & = & b_1, \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ c_0 & + & a_n c_1 & + & \ldots & + & a_n^n c_n & = & b_n. \end{array}$$

Это система из $n+1$ уравнений с таким же числом неизвестных $c_0, \ldots, c_n$, имеющая единственное решение.

4. Производная и формула Тейлора

Пусть

$$f(x) = \sum_k a_k x^k$$

— многочлен с коэффициентами в коммутативном кольце K. Его производной называется многочлен

$$f'(x) = \sum_k k a_k x^{k-1}.$$

Пусть g — ещё один многочлен с коэффициентами в K. Отметим следующие свойства.

- Производная константы равна нулю: $f' = 0$, если $f \in K$.
- $(f+g)' = f' + g'$.
- $(fg)' = f'g + fg'$.
- $\deg f' \leqslant \deg f - 1$.
- $\deg f' = \deg f - 1$, если $\deg f > 0$ и $\mathrm{char} K = 0$.

Имеет место

Теорема (формула Тейлора). *Пусть K — поле нулевой характеристики, c — его элемент и $f(x)$ — многочлен с коэффициентами в K. Тогда верно равенство*

$$f(x) = f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \frac{f'''(c)}{3!}(x-c)^3 + \dots.$$

Доказательство. Пусть

$$f(x) = a_0 + a_1(x-c) + a_2(x-c)^2 + \dots.$$

Тогда

$$\begin{aligned}
&f'(x) = 1 \cdot a_1 + 2 \cdot a_2(x-c) + 3 \cdot a_3(x-c)^2 + \dots,\\
&f''(x) = 1 \cdot 2 \cdot a_2 + 2 \cdot 3 \cdot a_3(x-c) + 3 \cdot 4 \cdot a_4(x-c)^2 + \dots,\\
&f'''(x) = 1 \cdot 2 \cdot 3 \cdot a_3 + 2 \cdot 3 \cdot 4 \cdot a_4(x-c) + 3 \cdot 4 \cdot 5(x-c)^2 + \dots,\\
&\dots
\end{aligned}$$

и имеют место соотношения:

$$f(c) = a_0, f'(c) = 1 \cdot a_1, f''(c) = 1 \cdot 2 \cdot a_2, f'''(c) = 1 \cdot 2 \cdot 3 \cdot a_3, \dots,$$

Отсюда

$$a_0 = f(c), a_1 = f'(c)/1!, a_2 = f''(c)/2!, a_3 = f'''(c)/3!, \dots. \square$$

5. Производная и кратные корни

Пусть $f(x)$ — многочлен с коэффициентами в целостном кольце K и c — его корень кратности k. Тогда для некоторого многочлена $g(x)$ выполняется равенство $f(x) = (x-c)^k g(x)$, откуда

$$\begin{aligned} f'(x) &= k(x-c)^{k-1}g(x) + (x-c)^k g'(x) \\ &= (x-c)^{k-1}(kg(x) + (x-c)g'(x)). \end{aligned}$$

Отметим следующие свойства.

∘ Простой корень многочлена не является корнем его производной.

∘ Корень многочлена кратности $k > 1$ является корнем его производной кратности не менее $k-1$.

∘ Над целостным кольцом нулевой характеристики корень многочлена кратности $k > 1$ является корнем его производной кратности $k-1$.

Имеет место

Теорема (о кратном корне). *Пусть K — поле нулевой характеристики и $f(x)$ — многочлен с коэффициентами в K. Элемент из K тогда и только тогда является k-кратным корнем многочлена $f(x)$, когда он является корнем многочленов $f(x), f'(x), \ldots, f^{(k-1)}$ и не является корнем многочлена $f^{(k)}(x)$.* □

Пусть $f(x)$ — многочлен в коэффициентами в поле K. Будем говорить, что он имеет кратный корень, если он имеет кратный корень в некотором расширении поля K. В соответствии с этим, многочлен не имеет кратных корней, если не существует расширения поля K, содержащего кратный корень многочлена. Имеет место

Теорема (критерий существования кратного корня). *Многочлен с коэффициентами в поле не имеет кратных корней тогда и только тогда, когда он взаимно прост со своей производной.* □

Доказательство. Если многочлен имеет кратный корень c, то двучлен $(x-c)$ является общим делителем этого многочлена и его производной. Обратно. Пусть многочлен имеет общий делитель $g(x)$ положительной степени со своей производной. Вспомним, что существует расширение поля K, содержащее корень многочлена $g(x)$.(Это расширение можно получить, присоединив корень символически.) Заметим, что корень многочлена $g(x)$ является кратным корнем многочлена $f(x)$. □

Следствие. *Над полем нулевой характеристики неприводимый многочлен не имеет кратных корней.*

Доказательство. Над полем нулевой характеристики производная неприводимого многочлена не равна нулю и тогда взаимно проста с ним. □

Замечание. Утверждение, аналогичное последнему следствию, выполняется для конечного поля, но в бесконечном поле положительной характеристики данное свойство может нарушаться.

6. Производная и кратные множители

Будем рассматривать многочлены от переменной x и с коэффициентами в поле K. Пусть $q(x)$ — неприводимый делитель многочлена $f(x)$. В этой ситуации для некоторого целого положительного числа k выполняются условия

$$q(x)^k | f(x) \text{ и } q(x)^{k+1} \nmid f(x);$$

и тогда для некоторого многочлена $g(x)$ выполняются соотношения:

$$f(x) = q(x)^k g(x), q(x) \nmid g(x).$$

Такое число k назовём *кратностью* неприводимого делителя $q(x)$.

В этом случае имеют место равенства

$$\begin{aligned} f'(x) &= kq(x)^k q'(x)g(x) + q(x)^k g'(x) \\ &= q(x)^{k-1}(kq'(x)g(x) + q(x)g'(x)). \end{aligned}$$

Отметим следующие свойства.

∘ Неприводимый делитель кратности один не является делителем производной.

∘ Неприводимый делитель кратности $k > 1$ является делителем производной кратности не менее $k - 1$.

∘ Над полем нулевой характеристики неприводимый делитель кратности $k > 1$ является делителем производной кратности $k - 1$.

Имеет место

Теорема (о кратном множителе). *Пусть K — поле нулевой характеристики, $f(x)$ — многочлен с коэффициентами в K и $q(x)$ — неприводимый многочлен с коэффициентами в K. Многочлен $q(x)$ тогда и только тогда является k-кратным делителем многочлена $f(x)$, когда он является делителем многочленов $f(x), f'(x), \ldots, f^{(k-1)}$ и не является делителем многочлена $f^{(k)}(x)$.* □

Многочлен без кратных корней назовём *свободным от квадратов* и многочлен $g(x)$ назовём *свободной от квадратов частью* многочлена $f(x)$, если $g(x)$ является свободным от квадратов делителем многочлена $f(x)$ и эти многочлены имеют одни и те же корни. Неприводимые многочлены над

полем нулевой характеристики и над конечным полем не имеют кратных корней (см. следствие и замечание выше), поэтому над этими полями свободная от квадратов часть многочлена совпадает с произведением его неприводимых делителей, выбранных из разных классов ассоциированности. Заметим, что в этих случаях коэффициенты многочлена и его свободной от квадрата части принадлежат одному и тому же полю.

Теорема (о свободной от квадратов части). *Свободная от квадратов часть многочлена $f(x)$ над полем нулевой характеристики равна* $f(x)/\gcd(f(x), f'(x))$.

Доказательство. Пусть над полем K имеет место разложение на неприводимые множители:

$$f(x) = q_1(x)^{k_1} \cdots q_m(x)^{k_m},$$

где $q_j(x)$ — неассоциированные неприводимые делители многочлена $f(x)$. Тогда в силу сформулированных выше свойств для некоторого многочлена $g(x)$, взаимно простого с $f(x)$, верно:

$$f'(x) = q_1(x)^{k_1-1} \cdots q_m(x)^{k_m-1} g(x).$$

Отсюда следует утверждение теоремы. □

Упражнение. Как найти свободную от квадратов часть многочлена над полем положительной характеристики?

7. Полиномиальные функции над целостным кольцом

Пусть K — целостное кольцо. В этом разделе рассматриваются многочлены от n переменных $x_1, \ldots, x_n$ и с коэффициентами в K. Всякий такой многочлен f определяет (индуцирует) функцию

$$\overline{f} : K^n \to K, \overline{f} : a \mapsto f(a).$$

Такие функции называются *полиномиальными*.

Обозначим через $\mathrm{Fun}(K^n, K)$ множество всех функций, отображающих K^n в K. Заметим, что это множество является кольцом с поточечными операциями сложения и умножения функций, такими, что

$$(fg)(a) = f(a)f(a), (f+g)(a) = f(a) + g(a)$$

для любых функций f, g и любого набора a из K^n. Отображение

$$K[x_1, \ldots, x_n] \to \mathrm{Fun}(K^n, K), f \mapsto \overline{f},$$

является, как легко понять, гомоморфизмом колец.

Будем интересоваться следующими вопросами:

∘ является ли это отображение инъективным; иными словами, определяют ли различные многочлены различные функции;

∘ является ли это отображение сюръективным; иными словами, всякая ли функция в множестве $\mathrm{Fun}(K^n, K)$ полиномиальна.

Первый вопрос имеет содержание для бесконечного кольца K, второй — для конечного.

∘ Упражнение. Докажите, что записанное отображение не является инъективным для конечного кольца и сюръективным для бесконечного.

Функции над бесконечным кольцом. Рассмотрим сначала случай, когда K — бесконечное целостное кольцо. Имеет место

Теорема. *Над бесконечным целостным кольцом различные многочлены определяют различные функции.*

Доказательство. Поскольку разность полиномиальных функций является полиномиальной функцией, достаточно доказать, что ненулевой многочлен не может определять нулевую функцию. Будем доказывать это утверждение индукцией по n. Это так при $n = 1$ в силу теоремы о числе корней многочлена над целостным кольцом. Докажем это утверждение для произвольного значения $n > 1$ в предположении, что при меньших значениях оно выполняется. Рассмотрим многочлен f от n переменных. Запишем его в виде разложения по степеням переменной x_n:

$$f(x_1, \ldots, x_n) = \sum_j f_j(x_1, \ldots, x_{n-1}) x_n^j.$$

Пусть $a_1, \ldots, a_{n-1}$ — произвольные элементы кольца K. Предположим, что многочлен f определяет нулевую функцию. Тогда многочлен

$$f(a_1, \ldots, a_{n-1}, x_n) = \sum_j f_j(a_1, \ldots, a_{n-1}) x_n^j$$

от переменной x_n также определяет нулевую функцию и тогда является нулевым многочленом; его коэффициенты

$$f_j(a_1, \ldots, a_{n-1})$$

равны нулю. В силу произвольности выбора элементов $a_1, \ldots, a_{n-1}$, функции $\overline{f_j}$ также нулевые. По предположению индукции многочлены f_j нулевые. Тогда и многочлен f — нулевой. Теорема доказана. □

Функции над конечным кольцом. Пусть теперь K — конечное целостное кольцо, содержащее q элементов. (В действительности, оно является полем, это доказывалось раньше.)

Многочлен с коэффициентами в кольце K, имеющей по каждой переменной степень, строго меньшую q, назовём редуцированным. Имеет место

Теорема. *Различные редуцированные многочлены над конечным целостным кольцом определяют различные функции.*

Доказательство. Доказательство этой теоремы почти полностью совпадает с доказательством предыдущей теоремы. □

Следствие. *Пусть K — конечное целостное кольцо. Тогда всякая функция в множестве* $\mathrm{Fun}(K^n, K)$ *полиномиальна.*

Доказательство. Это так, поскольку число функций совпадает с числом редуцированных многочленов. □

Упражнения. Докажите утверждения ниже.

∘ Теорема Ферма. В конечном поле, содержащем q элементов, каждый элемент является корнем многочлена $x^q - x$. Таким образом, многочлены x^q, x определяют одну функцию (тождественную) и ненулевой многочлен $x^q - x$ определяет нулевую функцию.

∘ Теорема Вильсона. В конечном поле произведение всех ненулевых элементов равно -1.

∘ Над конечным полем, содержащем q элементов, многочлен от переменных $x_1, \ldots, x_n$ тогда и только тогда определяет нулевую функцию, когда его можно представить в виде

$$\sum_j f_j(x_1, \ldots, x_n)(x_j^q - x_j),$$

где f_j — произвольные многочлены с коэффициентами в поле K.

Упражнение. Как для многочлена с коэффициентами в конечном поле найти редуцированный многочлен, определяющий ту же функцию?

ГЛАВА 13

Матрицы

Пусть K — кольцо с единицей. *Матрицей* размера $m \times n$, или $(m \times n)$-матрицей, над кольцом K называется прямоугольная таблица

$$a = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

составленная из его элементов. Множество всех таких матриц обозначается $K^{m,n}$. Матрица называется квадратной, если у неё число строк совпадает с числом столбцов, то есть $m = n$. Матрица с одним столбцом называется столбцом. Матрица с одной строкой называется строкой.

Матрица a записывается по столбцам или по строкам следующим образом:

$$a = (a_1\!\downarrow, \dots, a_n\!\downarrow) = \begin{pmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_m} \end{pmatrix},$$

где $a_j\!\downarrow$ — j-й столбец и $\overrightarrow{a_i}$ — i-я строка матрицы a.

1. Операции над матрицами

Рассмотрим далее основные операции над матрицами.

Сложение. Суммой $(m \times n)$-матриц a, b называется матрица c того же размера, такая, что

$$c_{ij} = a_{ij} + b_{ij},\ 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n.$$

С операцией сложения матрицы образуют абелеву группу, где нулём является *нулевая матрица*, у которой все значения нулевые. Для произвольной матрицы противоположная получается заменой всех её элементов противоположными.

Умножение на элемент кольца. Для любого элемента λ из кольца и любой $(m \times n)$-матрицы a определены матрицы $\lambda \cdot a$ и $a \cdot \lambda$. Они получаются соответственно правым и левым умножением всех элементов матрицы a

на элемент λ:

$$(\lambda \cdot a)_{ij} = \lambda \cdot a_{ij},$$
$$(a \cdot \lambda)_{ij} = a_{ij} \cdot \lambda.$$

Введённые операции наделяют множество $m \times n$-матриц алгебраической структурой правого и левого модуля над кольцом K.

Для любых матриц a_k одного размера и произвольных элементов λ_k из кольца K, где $1 \leqslant k \leqslant N$, матрицы

$$\lambda_1 a_1 + \ldots + \lambda_N a_N,$$
$$a_1 \lambda_1 + \ldots + a_N \lambda_N$$

называются *линейными комбинациями*, соответственно левой и правой, матриц a_k; элементы λ_k называются *коэффициентами* этих линейных комбинаций.

Матричные единицы. Матрица с одним ненулевым элементом, равным единице, называется матричной единицей. Договоримся обозначать e_{ij} матричную единицу с ненулевым элементом в i-й строке и j-м столбце. Любую $(m \times n)$-матрицу a можно теперь записать в виде линейной комбинации матричных единиц:

$$a = \sum_{ij} a_{ij} \mathrm{e}_{ij} = \sum_{ij} \mathrm{e}_{ij} a_{ij}.$$

Умножение. Произведением матрицы a размера $m \times n$ на матрицу b размера $n \times s$ называется матрица ab размера $m \times s$, где

$$(ab)_{ij} = \sum_k a_{ik} b_{kj}.$$

Отметим, что произведение определено только в том случае, если число столбцов матрицы a равно числу строк матрицы b.

∘ *Умножение матриц ассоциативно, когда определено.* Для любых матриц a, b, c верно равенство

$$(ab)c = a(bc), \text{ если все произведения определены.}$$

∘ *Сложение и умножение матриц связаны законами дистрибутивности*, имеют место равенства

$$(a + b)c = ac + bc,$$
$$c(a + b) = ca + cb,$$

где a, b — матрицы размера $m \times n$ и c — матрица размера $n \times s$ в первом случае и размера $s \times m$ во втором (m, n, s — произвольные целые положительные числа).

В частности, с операциями сложения и умножения квадратные матрицы фиксированного размера образуют кольцо с единицей. Здесь единицей является *единичная матрица*

$$\mathrm{e} = \sum_k \mathrm{e}_{kk}.$$

Если кольцо K коммутативно, то с операциями сложения, умножения и умножения на элементы кольца квадратные матрицы фиксированного размера образуют алгебраическую структуру, которая называется алгеброй над кольцом K.

Упражнение. Проверьте ассоциативность матричного умножения, а также свойство дистрибутивности для сложения и умножения матриц.

Транспонирование. Пусть K — коммутативное кольцо. *Транспонированием* называется отображение

$$K^{m,n} \to K^{n,m}, a \mapsto a^{\mathrm{T}}, \text{ где } (a^{\mathrm{T}})_{ji} = a_{ij}, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n.$$

При этом матрица a^{T} называется *транспонированной* матрицей a. Транспонирование является изоморфизмом модулей, то есть является биекцией, перестановочной со сложением и умножением на элементы кольца. Транспонирование следующим образом связано с умножением:

$$(ab)^{\mathrm{T}} = b^{\mathrm{T}}a^{\mathrm{T}}, \text{ если произведения определены.}$$

Действительно,

$$(ab)_{ij} = \sum_k a_{ik}b_{kj}, \ (b^{\mathrm{T}}a^{\mathrm{T}})_{ji} = \sum_k (b^{\mathrm{T}})_{jk}(a^{\mathrm{T}})_{ki} = \sum_k b_{kj}a_{ik} = \sum_k a_{ik}b_{kj}.$$

Упражнения.

∘ Пусть K — кольцо. Противоположным ему называется кольцо K^0, где сложение совпадает со сложением в K и умножение $\circ$ определено так:

$$a \circ b = ba.$$

Ясно, что коммутативное кольцо совпадает со своим противоположным.

Проверьте, что кольца $M(n, K)^0$ и $M(n, K^0)$ изоморфны.

∘ Проверьте следующее правило умножения матриц, разбитых на блоки:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}.$$

Предполагается, матрицы разбиты на четыре блока горизонтальной и вертикальной линиями так, что произведения справа корректны.

2. Элементарные матрицы

Пусть λ — ненулевой элемент кольца K. Следующая квадратная матрица (размера n для определённости)

$$t_{ij}(\lambda) = \mathrm{e} + \lambda \cdot \mathrm{e}_{ij}, \text{ где } i \neq j,$$

называется *элементарной трансвекцией*. Иными словами, эта матрица кроме единиц на диагонали содержит единственный ненулевой элемент, который находится в позиции ij и равен λ.

Пусть ξ — обратимый элемент кольца K. Квадратная матрица (пусть того же размера n)

$$d_i(\xi) = \mathrm{e} + (\xi - 1)\mathrm{e}_{ii}$$

называется *псевдоотражением*. Это матрица, которая получается из единичной, если в ней i-й элемент на диагонали заменить на ξ.

Трансвекции и псевдоотражения называются также элементарными матрицами. Посмотрим, что происходит с произвольной матрицей при умножении на элементарную матрицу. Отметим ряд свойств.

∘ *Для матрицы a размера $n \times m$ и матрицы b размера $m \times n$ имеют место равенства:*

$$t_{ij}(\lambda) \cdot a = a + \lambda \mathrm{e}_{ij} \cdot a,$$
$$b \cdot t_{ij}(\lambda) = b + b \cdot \lambda \mathrm{e}_{ij}.$$

Отсюда можно увидеть, что левое умножение на матрицу t_{ij} приводит к тому, что в матрице a к i-й строке прибавляется j-ая, умноженная на λ:

$$t_{ij}(\lambda) \cdot \begin{pmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_n} \end{pmatrix} = \begin{pmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i} + \lambda \overrightarrow{a_j} \\ \vdots \\ \overrightarrow{a_n} \end{pmatrix}.$$

При умножении на матрицу t_{ij} справа в матрице b к j-му столбцу прибавляется i-й, умноженный на λ:

$$(b_1\!\downarrow, \ldots, b_j\!\downarrow, \ldots, b_n\!\downarrow) \cdot t_{ij}(\lambda) = (b_1\!\downarrow, \ldots, b_j\!\downarrow + b_i\!\downarrow \lambda, \ldots, b_n\!\downarrow)$$

∘ *Элементарная трансвекция обратима, выполняется равенство:*

$$t_{ij}(\lambda)t_{ji}(-\lambda) = t_{ji}(\lambda)t_{ij}(-\lambda) = \mathrm{e}.$$

∘ *Для матрицы a размера $n \times m$ и матрицы b размера $m \times n$ имеют место равенства:*

$$d_i(\xi) \cdot a = a + (\xi - 1)\mathrm{e}_{ii} \cdot a,$$
$$b \cdot d_i(\xi) = b + b \cdot \mathrm{e}_{ii} \cdot (\xi - 1).$$

Иными словами, при левом умножении на матрицу $d_i(\xi)$ в матрице a i-я строка умножается на ξ:

$$d_i(\xi)\cdot\begin{pmatrix}\overrightarrow{a_1}\\ \vdots\\ \overrightarrow{a_i}\\ \vdots\\ \overrightarrow{a_n}\end{pmatrix}=\begin{pmatrix}\overrightarrow{a_1}\\ \vdots\\ \xi\overrightarrow{a_i}\\ \vdots\\ \overrightarrow{a_n}\end{pmatrix}.$$

При умножении на матрицу $d_i(\xi)$ справа в матрице b i-й столбец умножается на ξ:

$$(b_1\downarrow,\dots,b_i\downarrow,\dots,b_n\downarrow)\cdot d_i(\xi)=(b_1\downarrow,\dots,b_i\downarrow\xi,\dots,b_n\downarrow).$$

- *Псевдоотражение обратимо, имеет место равенство:*

$$d_i(\xi^{-1})d_i(\xi)=d_i(\xi)d_i(\xi^{-1})=\mathrm{e}.$$

Описанные выше действия, состоящие в левом (правом) умножении матрицы на элементарную трансвекцию либо псевдоотражение, называются *элементарными преобразованиями* строк (столбцов) матрицы.

Упражнение. Как посредством элементарных преобразований строк (столбцов) поменять местами две строки (два столбца)?

3. Ступенчатая матрица

Будем рассматривать матрицы над полем. Первый ненулевой элемент строки назовём главным. Матрицу назовём *ступенчатой*, если главный элемент каждой ненулевой её строки находится правее главного элемента предыдущей строки и нулевые строки находятся внизу матрицы. Матрицу назовём *специальной ступенчатой*, если она ступенчатая, главные элементы её строк равны единице и являются единственными ненулевыми элементами своих столбцов.

Упражнение. Обратимая квадратная матрица в специальной ступенчатой форме является единичной матрицей.

Теорема (метод Гаусса). *Матрицу над полем последовательностью элементарных преобразований строк можно привести к виду специальной ступенчатой матрицы.*

Доказательство. Найдём строку, в которой главный элемент находится в наиболее левом положении; пусть i — номер столбца с этим элементом. Поставим эту строку на первое место. Это можно сделать при помощи элементарных преобразований строк. Умножим первую строку на элемент, обратный её главному элементу. Теперь главный элемент первой строки равен единице. Далее, последовательно вычитая из каждой

строки первую, умноженную на элемент очередной строки, стоящий в i-й позиции, добьёмся того, чтобы главный элемент первой строки был единственным ненулевым элементом в i-м столбце. Далее, в подматрице, образованной строками, лежащими ниже первой, найдём строку с максимально левым главным элементом, поставим её на первое место, обозначим через i номер столбца с этим элементом и т. д. В результате получается специальная ступенчатая матрица. □

Следствие. *Обратимая квадратная матрица над полем является произведением элементарных матриц.*

Доказательство. Элементарными преобразованиями строк приведём обратимую матрицу a к виду специальной ступенчатой матрицы. Полученная в результате специальная ступенчатая матрица является единичной матрицей, а элементарные преобразования строк реализуются умножением слева на элементарные матрицы $\tau_1, \ldots, \tau_n$. Таким образом, получаются равенства

$$\tau_n \cdots \tau_1 \cdot a = \mathrm{e} \text{ и } \tau_1^{-1} \cdots \tau_n^{-1} = a.$$

Поскольку обратные матрицы для элементарных также являются элементарными, следствие доказано. □

Следствие. *Квадратная матрица над полем тогда и только тогда обратима, когда она является произведением элементарных матриц.*

Доказательство. Необходимость этого утверждения доказана в предыдущем следствии. Достаточность имеет место в силу того, что элементарные матрицы обратимы. □

Упражнение. Докажите, что для квадратной матрицы a над полем следующие условия равносильны.

(1) Матрица a обратима.

(2) Матрица a является произведением элементарных матриц.

(3) Из матрицы a элементарными преобразованиями строк можно получить единичную матрицу.

(4) Из матрицы a элементарными преобразованиями столбцов можно получить единичную матрицу.

(5) Из матрицы a элементарными преобразованиями строк и столбцов можно получить единичную матрицу.

4. Система линейных уравнений

Системой линейных алгебраических уравнений над кольцом K называется система уравнений

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n & = & b_m. \end{array}$$

Здесь a_{ij} и b_k — заданные элементы кольца K, x_j — неизвестные элементы кольца K, которые нужно найти. Данную систему уравнений можно записать в матричной форме

$$ax = b,$$

где a — матрица размера $m \times n$, составленная из коэффициентов a_{ij}, x — столбец высоты n, составленный из неизвестных x_j, и b — столбец высоты m, составленный из элементов b_i. Матрица a называется *матрицей системы уравнений* и матрица $(a \mid b)$, размера $m \times (n+1)$, полученная из a добавлением ещё одного столбца, равного b, называется *расширенной матрицей* системы уравнений.

Решением системы называется набор значений переменных x_j из кольца K, при которых система уравнений превращается в систему равенств. Это означает также, что столбец b выражается в виде линейной комбинации столбцов матрицы a:

$$\sum_j a_{j\downarrow} \cdot x_j = b,$$

где $a_{j\downarrow}$ — j-й столбец матрицы a.

Отметим ряд свойств. Две системы с одними и теми же переменными называются *эквивалентными*, если они имеют одни и те же решения.

∘ *Система линейных уравнений над полем эквивалентна системе со специальной ступенчатой матрицей.* □

Именно, система $ax = b$ эквивалентна системе $cax = cb$ для любой обратимой квадратной матрицы c размера m. Матрицу c всегда можно выбрать так, чтобы матрица $(ca|cb)$ стала специальной ступенчатой; более того, матрица c находится эффективно методом Гаусса. (На практике c явно не ищется, просто матрица $(a \mid b)$ приводится к ступенчатому виду.)

∘ *Пусть матрица a специальная ступенчатая. Система $ax = b$ тогда и только тогда имеет решение, когда матрицы a и $(a \mid b)$ содержат одинаковое число ненулевых строк.* □

Переменные, соответствующие главным элементам строк матрицы a (находящейся в специальной ступенчатой форме), назовём *главными* переменными рассматриваемой системы уравнений. Остальные переменные будем называть *свободными*.

∘ *Пусть матрица a специальная ступенчатая и система $ax = b$ имеет решение. Тогда любой набор значений свободных переменных однозначно продолжается до решения системы.* □

Упражнение. Когда система уравнений со ступенчатой матрицей имеет единственное решение?

5. Линейная зависимость*

Ряд свойств, связанных с алгебраической структурой множества решений системы линейных алгебраических уравнений над полем, а также с отношением линейной зависимости между векторами, будет сформулирован ниже в виде упражнений. Окончательный смысл этих свойств раскрывается при изучении векторных пространств.

Упражнение (неоднородная система). Докажите утверждения.

∘ Пусть x_0 — решение системы $ax = 0$ (такая система называется однородной). Тогда для любого решения x_b системы $ax = b$ столбец $x_0 + x_b$ также является её решением.

∘ Обратно, пусть x_b — решение системы $ax = b$. Тогда любое решение этой системы можно единственным способом записать в виде суммы $x_0 + x_b$, где x_0 — некоторое решение однородной системы.

∘ Линейная комбинация решений однородной системы линейных уравнений также является её решением.

Замечание. В соответствии с первыми двумя свойствами описание множества всех решений неоднородной системы уравнений сводится к нахождению некоторого одного её решения и всех решений соответствующей однородной системы. Последнее свойство означает, что множество решений однородной системы линейных уравнений над полем образует алгебраическую структуру векторного пространства и, как будет указано в следующем упражнении, определяется полностью набором линейно независимых базисных решений.

Упражнение (однородная система). Набор матриц (в частности, строк или столбцов) одинакового размера над полем называется линейно независимым, если никакая из матриц не является линейной комбинацией остальных (с коэффициентами в данном поле). Докажите следующие утверждения.

∘ Однородная система со специальной ступенчатой матрицей, имеющая n' свободных переменных, имеет n' линейно независимых решений. Назовём любой набор таких решений базисным.

∘ Множество всех решений однородной системы совпадает с множеством линейных комбинаций базисных решений.

∘ Каждое решение однородной системы линейных уравнений над полем единственным образом записывается в виде линейной комбинации набора базисных решений.

Следующее упражнение направлено на изучение отношения линейной зависимости.

Упражнение (ранг матрицы). Максимальное число линейно независимых строк (столбцов) матрицы над полем называется её строчным (столбцовым) рангом. Докажите следующие утверждения.

∘ Элементарные преобразования строк не изменяют соотношений линейной зависимости между столбцами матрицы. Двойственное утверждение выполняется для строк матрицы.

∘ Столбцовый ранг не меняется при элементарных преобразованиях строк. Двойственное свойство выполняется для строчного ранга.

∘ Строчный ранг не увеличивается при элементарных преобразованиях строк. Двойственное свойство выполняется для столбцового ранга.

∘ Если в матрице столбцы линейно независимы, то элементарными преобразованиями строк её можно привести к такому виду

$$\begin{pmatrix} \mathrm{e} \\ 0 \end{pmatrix},$$

где e — единичная и 0 — нулевая матрицы. В частности, число столбцов не превосходит числа строк в этом случае. Двойственное свойство выполняется для матрицы с линейно независимыми строками.

∘ Если в матрице столбцы линейно независимы и их число равно n, то какие-то n её строк также линейно независимы. Двойственное утверждение выполняется для строк.

∘ Строчный и столбцовый ранги матрицы над полем совпадают.

∘ Максимальное по включению линейно независимое множество столбцов матрицы назовём базисным. Докажите, что все базисные множества содержат одинаковое число столбцов. Двойственное свойство выполняется для строк.

6. Определитель

Будем рассматривать квадратные матрицы размера n над коммутативным кольцом K. *Определителем* матрицы a называется элемент

$$\det a = \sum_{\alpha} \operatorname{sign}(\alpha) a_{1,1\alpha} \cdots a_{n,n\alpha},$$

где сумма вычисляется в кольце K по всем подстановкам

$$\alpha : \{1, \ldots, n\} \to \{1, \ldots, n\}, k \mapsto k\alpha$$

из множества S_n.

Например, при $n = 2$:

$$\begin{aligned} \det a &= \operatorname{sign} \begin{pmatrix} 1,2 \\ 1,2 \end{pmatrix} a_{11}a_{22} + \operatorname{sign} \begin{pmatrix} 1,2 \\ 2,1 \end{pmatrix} a_{12}a_{21} \\ &= a_{11}a_{22} - a_{12}a_{21}. \end{aligned}$$

При $n = 3$:

$$\begin{aligned} \det a = \\ = \quad & \operatorname{sign} \begin{pmatrix} 1,2,3 \\ 1,2,3 \end{pmatrix} a_{11}a_{22}a_{33} + \operatorname{sign} \begin{pmatrix} 1,2,3 \\ 2,3,1 \end{pmatrix} a_{12}a_{23}a_{31} \\ & + \operatorname{sign} \begin{pmatrix} 1,2,3 \\ 3,1,2 \end{pmatrix} a_{13}a_{21}a_{32} + \operatorname{sign} \begin{pmatrix} 1,2,3 \\ 1,3,2 \end{pmatrix} a_{11}a_{23}a_{32} \\ & + \operatorname{sign} \begin{pmatrix} 1,2,3 \\ 3,2,1 \end{pmatrix} a_{13}a_{22}a_{31} + \operatorname{sign} \begin{pmatrix} 1,2,3 \\ 2,1,3 \end{pmatrix} a_{12}a_{21}a_{33} \end{aligned}$$

и тогда $\det a =$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33}.$$

Упражнение. Для диагональной матрицы

$$\det a = a_{11} \cdots a_{nn}.$$

То же самое верно для верхнетреугольной матрицы, где

$$a_{ij} = 0 \text{ при } i > j,$$

а также для нижнетреугольной матрицы, такой, что

$$a_{ij} = 0 \text{ при } i < j.$$

Отметим ряд свойств определителя.

- $\det a = \det a^{\mathrm{T}}$.

  Доказательство. Достаточно заметить, что

  $$a_{1,1\alpha} \cdots a_{n,n\alpha} = a_{1\alpha^{-1},1} \cdots a_{n\alpha^{-1},n} \text{ и } \operatorname{sign} \alpha = \operatorname{sign} \alpha^{-1}. \square$$

- $\det a = 0$, *если в матрице a есть совпадающие строки.*

Доказательство. Пусть строки с номерами i и j совпадают и $\beta = (i, j)$. Тогда

$$a_{1,1\alpha} \cdots a_{n,n\alpha} = a_{1,1\beta\alpha} \cdots a_{n,n\beta\alpha} \text{ и } \operatorname{sign}\alpha = -\operatorname{sign}\beta\alpha$$

для любой подстановки α из S_n. Отсюда, поскольку отображение

$$S_n \to S_n, \alpha \mapsto \beta\alpha,$$

является биекцией, следует, что $\det a = -\det a$. Если характеристика кольца K не равна 2, то это сразу означает, что $\det a = 0$. В действительности, записанное равенство для определителей выполняется не только в кольце K, но и в кольце целочисленных многочленов от переменных a_{ij}, то есть в кольце характеристики 0. □

∘ *Если какая-то строка матрицы a является суммой двух строк, то определитель матрицы a равен сумме определителей двух матриц a' и a'', получаемых из a оставлением в этой строке одного из слагаемых:*

$$\det \begin{pmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i'} + \overrightarrow{a_i''} \\ \vdots \\ \overrightarrow{a_n} \end{pmatrix} = \det \begin{pmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i'} \\ \vdots \\ \overrightarrow{a_n} \end{pmatrix} + \det \begin{pmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i''} \\ \vdots \\ \overrightarrow{a_n} \end{pmatrix}.$$

Доказательство. Действительно, тогда

$$\begin{aligned} \det a = & \sum_\alpha \operatorname{sign}(\alpha) a_{1,1\alpha} \cdots (a'_{i,i\alpha} + a''_{i,i\alpha}) \cdots a_{n,\alpha n} \\ = & \sum_\alpha \operatorname{sign}(\alpha) a_{1,1\alpha} \cdots (a'_{i,i\alpha}) \cdots a_{n,\alpha n} \\ & + \sum_\alpha \operatorname{sign}(\alpha) a_{1,1\alpha} \cdots (a''_{i,i\alpha}) \cdots a_{n,\alpha n} \\ = & \det a' + \det a''. \ \square \end{aligned}$$

∘ *Множитель, принадлежащий кольцу K, можно выносить из любой строки за знак определителя:*

$$\det \begin{pmatrix} \overrightarrow{a_1} \\ \vdots \\ \lambda \cdot \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_n} \end{pmatrix} = \lambda \cdot \det \begin{pmatrix} \overrightarrow{a_1} \\ \vdots \\ \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_n} \end{pmatrix}. \ \square$$

∘ *Пусть матрица a_β получена из матрицы a перестановкой строк в соответствии с подстановкой β из S_n (вместо i-й строки записана*

строка с номером $i\beta$). Тогда определители матриц a и a_β отличаются множителем $\operatorname{sign}\beta$*:*

$$\det\begin{pmatrix}\overrightarrow{a_{1\beta}}\\ \vdots\\ \overrightarrow{a_{n\beta}}\end{pmatrix}=\operatorname{sign}\beta\cdot\det\begin{pmatrix}\overrightarrow{a_1}\\ \vdots\\ \overrightarrow{a_n}\end{pmatrix}$$

Доказательство.

$$\det a_\beta=\sum_\alpha\operatorname{sign}(\alpha)a_{1\beta,1\alpha}\cdots a_{n\beta,n\alpha}=\sum_\alpha\operatorname{sign}(\alpha)a_{1,1\beta^{-1}\alpha}\cdots a_{n,n\beta^{-1}\alpha}$$

$$=\operatorname{sign}\beta\sum_{\beta^{-1}\alpha}\operatorname{sign}(\beta^{-1}\alpha)a_{1,1\beta^{-1}\alpha}\cdots a_{n,n\beta^{-1}\alpha}=\operatorname{sign}\beta\det a.\square$$

∘ *Определитель произведения двух матриц равен произведению их определителей:*

$$\det ab=\det a\cdot\det b.$$

Доказательство. Имеют место равенства:

$$\det ab=\det\begin{pmatrix}\overrightarrow{a_1}\\ \vdots\\ \overrightarrow{a_n}\end{pmatrix}b=\det\begin{pmatrix}\overrightarrow{a_1}b\\ \vdots\\ \overrightarrow{a_n}b\end{pmatrix}=\det\begin{pmatrix}\sum_j a_{1j}\overrightarrow{b_j}\\ \vdots\\ \sum_j a_{nj}\overrightarrow{b_j}\end{pmatrix}=$$

$$=\sum_\beta\det\begin{pmatrix}a_{1,1\beta}\overrightarrow{b_{1\beta}}\\ \vdots\\ a_{n,n\beta}\overrightarrow{b_{n\beta}}\end{pmatrix}=\sum_\beta a_{1,1\beta}\cdots a_{n,n\beta}\cdot\det\begin{pmatrix}\overrightarrow{b_{1\beta}}\\ \vdots\\ \overrightarrow{b_{n\beta}}\end{pmatrix}=$$

$$=\sum_\beta a_{1,1\beta}\cdots a_{n,n\beta}\cdot\operatorname{sign}\beta\cdot\det\begin{pmatrix}\overrightarrow{b_1}\\ \vdots\\ \overrightarrow{b_n}\end{pmatrix}=\det a\cdot\det b,$$

где сумма сначала вычисляется сначала по всем преобразованиям β на множестве чисел $1,\dots,n$, а затем — по всем подстановкам. $\square$

∘ *Взаимно обратные матрицы имеют взаимно обратные определители:*

$$\det(a^{-1})=(\det a)^{-1}.\ \square$$

Упражнение. Докажите, что

$$\det\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}=\det a\cdot\det b$$

для любых матриц $a\in K^{n,n}$, $b\in K^{n,m}$ и $d\in K^{m,m}$.

7. Разложение определителя по строке

Пусть a — квадратная матрица размера n над коммутативным кольцом K. Обозначим через $m_{ij}(a)$ её подматрицу, образованную вычёркиванием i-й строки и j-го столбца. Её определитель, называется *минором* элемента a_{ij}; значение

$$\widehat{a}_{ij} = (-1)^{i+j} \det m_{ij}(a)$$

называется *алгебраическим дополнением* элемента a_{ij}. Пусть также матрица $M_{ij}(a)$ получена из a заменой элемента a_{ij} единицей и заменой всех остальных элементов i-й строки и j-го столбца нулями. Отметим следующие свойства.

∘ *Имеет место равенство*

$$\det M_{ij}(a) = (-1)^{i+j} \det m_{ij}(a) = \widehat{a}_{ij}.$$

Доказательство. Достаточно заметить, что

$$\det M_{ij}(a) = (-1)^{i+j} \det \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & m_{ij}(a) & \\ 0 & & & \end{pmatrix}. \square$$

∘ *Определитель равен сумме произведений миноров элементов любой строки (любого столбца) матрицы на их алгебраические дополнения:*

$$\det a = \sum_k a_{ik}\widehat{a}_{ik} = \sum_k a_{kj}\widehat{a}_{kj}.$$

Доказательство. Обозначим через e_k строку, у которой в k-й позиции единица, а в остальных — нули. Представим i-ю строку матрицы a как

$$\overrightarrow{a}_i = \sum_k a_{ik}\mathrm{e}_k.$$

Сделаем следующее наблюдение: если заменить в матрице i-ю строку на e_k, то определитель полученной матрицы (обозначим её a'_k) совпадёт с определителем матрицы $M_{ik}(a)$; для доказательства нужно представить k-й столбец матрицы a'_k в виде линейной комбинации столбцов $\mathrm{e}_i^{\mathrm{T}}$ и воспользоваться свойствами определителя. Используя это, получаем

$$\det a = \sum_k a_{ik} \det a'_k = \sum_k a_{ik} \det M_{ik}(a) = \sum_k a_{ik}\widehat{a}_{ik}. \square$$

∘ *Имеет место равенство*

$$\sum_k a_{ik}\widehat{a}_{jk} = \sum_k a_{kj}\widehat{a}_{ki} = \delta_{ij} \det a,$$

где

$$\delta_{ij} = \begin{cases} 1, & \text{если } i = j \\ 0, & \text{в противном случае.} \end{cases}$$

Доказательство. В первом случае записан определитель матрицы, полученный из a заменой j-й строки на i-ю. Он равен нулю, если $i \neq j$. $\square$
Составим из алгебраических дополнений новую матрицу

$$\widehat{a} = \begin{pmatrix} \widehat{a}_{11} & \widehat{a}_{12} & \dots & \widehat{a}_{1n} \\ \widehat{a}_{21} & \widehat{a}_{22} & \dots & \widehat{a}_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \widehat{a}_{n1} & \widehat{a}_{n2} & \dots & \widehat{a}_{nn} \end{pmatrix}.$$

Транспонированная для неё матрица $\operatorname{adj} a = \widehat{a}^{\mathrm{T}}$ называется *союзной* к a.

∘ *Имеют место матричные равенства*

$$(\operatorname{adj} a)a = a(\operatorname{adj} a) = \det a.$$

Доказательство. Непосредственно вычисляем:

$$(a\widehat{a}^{\mathrm{T}})_{ij} = \sum_k a_{ik}\widehat{a}_{jk} = \delta_{ij} \det a. \ \square$$

Объединяя это свойство с последним свойством из предыдущего раздела, получаем следующую теорему.

Теорема. *Квадратная матрица тогда и только тогда обратима над коммутативным кольцом с единицей, когда её определитель обратим в этом кольце. Для обратимой матрицы a верно*

$$a^{-1} = (\det a)^{-1} \operatorname{adj} a.$$

Упражнение. Докажите, что

$$\det \begin{pmatrix} a_1^0 & a_1^1 & \dots & a_1^{n-1} \\ a_2^0 & a_2^1 & \dots & a_2^{n-1} \\ \vdots & \vdots & & \vdots \\ a_n^0 & a_n^1 & \dots & a_n^{n-1} \end{pmatrix} = \prod_j \prod_{i,i<j} (a_j - a_i).$$

Определитель в этой формуле называется определителем Вандермонда.

8. Формулы Крамера

Рассмотрим систему линейных алгебраических уравнений

$$ax = b$$

с квадратной матрицей a размера n над коммутативным кольцом K. Положим

$$d = \det a \text{ и } d_k = \det(a_1\downarrow, \dots, a_{k-1}\downarrow, b, a_{k+1}\downarrow, \dots, a_n\downarrow).$$

Имеет место

Теорема Крамера. *Пусть* $ax = b$, *тогда*

$$d \cdot x_k = d_k$$

для любого k, такого, что $1 \leqslant k \leqslant n$.

Доказательство. Для любого i, такого что $1 \leqslant i \leqslant n$, выполняется равенство

$$\sum_j a_{ij} x_j = b_i.$$

Умножим это равенство на $\widehat{a}_{ik}$ и просуммируем по k. Получим

$$\sum_k \widehat{a}_{ik} \sum_j a_{ij} x_j = \sum_k b_i \widehat{a}_{ik}.$$

В правой части записан определитель матрицы, полученной из a заменой k-го столбца на b, он равен d_k. Рассмотрим подробнее левую часть:

$$\sum_k \widehat{a}_{ik} \sum_j a_{ij} x_j = \sum_j x_j \sum_k a_{ij} \widehat{a}_{ik} = \sum_j x_j \cdot \delta_{jk} d = x_k \cdot d. \ \square$$

9. Характеристический многочлен*

Будем рассматривать матрицы, составленные из элементов коммутативного кольца с единицей. Сделаем следующие определения.

∘ *Следом* матрицы называется сумма её диагональных элементов:

$$\operatorname{tr} a = \sum_k a_{kk}.$$

∘ Квадратные матрицы a, b называются *подобными*, если существует обратимая матрица c, такая, что $a = c^{-1}bc$.

∘ Многочлен $\det(xe - a)$ называется *характеристическим* многочленом квадратной матрицы a.

Упражнение. Докажите следующие факты.

∘ $\operatorname{tr}(ab) = \operatorname{tr}(ba)$ для любых матриц $a \in K^{n,m}, b \in K^{m,n}$.

∘ $\operatorname{tr}(a + b) = \operatorname{tr} a + \operatorname{tr} b$.

∘ Подобные матрицы имеют равные определители.

∘ Подобные матрицы имеют равные следы.

∘ У подобных матриц характеристические многочлены совпадают.

∘ Пусть $x^n + a_{n-1}x^{n-1} + \ldots + a_0$ — характеристический многочлен матрицы a. Тогда $\det a = (-1)^n a_0$ и $\operatorname{tr} a = -a_{n-1}$.

ГЛАВА 14

Свободные модули и векторные пространства

В этой главе вводится в рассмотрение алгебраическая структура модуля над кольцом. Изучаются основные свойства свободных модулей и векторных пространств.

1. Модуль и алгебра

Пусть R — ассоциативное кольцо с единицей и M — абелева группа, записанная аддитивно. Она называется *правым модулем* над кольцом R, или правым R-модулем, если определено умножение

$$M \times R \to M,\ (u, \lambda) \mapsto u \cdot \lambda,$$

удовлетворяющее условиям:

(1) $(u + v)\lambda = u\lambda + v\lambda$;

(2) $u(\lambda + \mu) = u\lambda + u\mu$;

(3) $u \cdot \lambda\mu = u\lambda \cdot \mu$;

(4) $u \cdot 1 = u$.

для любых λ, μ из R, u, v из M. Элементы кольца называют *скалярами*; элементы модуля часто называют *векторами*. Заметим, что наряду с записанными выше условиями в модуле выполняются следующие:

(5) $u(\lambda - \mu) = u\lambda - u\mu$;

(6) $(u - v)\lambda = u\lambda - v\lambda$;

а также

(7) $u0 = 0$;

(8) $0\lambda = 0$;

(9) $-u\lambda = (-u)\lambda = u(-\lambda)$.

Упражнение. Докажите свойства (5–9).

Двойственным образом определяется *левый модуль* над кольцом R, а если выполняются оба определения, то говорят о *бимодуле*. В случае коммутативного кольца разница между правым и левым модулем над ним в значительной степени формальная, тем не менее полезно придерживаться определённых правил. В дальнейшем, в зависимости от контекста под модулем будем понимать левый или правый модуль, обычно правый.

Модуль над коммутативным кольцом называется *алгеброй*, если в нём определена ещё одна операция умножения и выполняются условия

(10) $u\lambda \cdot v = u \cdot v\lambda = (u \cdot v)\lambda$;

(11) $(u + v)w = uw + vw$ и $u(v + w) = uv + uw$;

для любых элементов λ из R и u, v, w из M. Таким образом, алгебра над коммутативным кольцом R — это кольцо, возможно неассоциативное, где дополнительно определено умножение на элементы кольца R, обладающее перечисленными выше свойствами. Если в алгебре имеется нейтральный элемент относительно операции умножения, то он называется *единицей*; в этом случае говорят об алгебре с единицей. Если умножение в алгебре ассоциативно, то алгебра называется ассоциативной. Далее рассматриваются только ассоциативные алгебры.

Замечание. Над некоммутативным кольцом алгебра не определяется, так как не ясно как выносить множители в произведении $u\alpha \cdot v\beta$.

Примеры.

∘ Всякий модуль над коммутативным кольцом можно рассматривать как *алгебру с нулевым умножением*, где произведение любых двух элементов равно нулю.

∘ Пусть A — кольцо с единицей. В нём элементы, перестановочные со всеми элементами, образует подкольцо, коммутативное и содержащее единицу. Его называют *центром* кольца A и обозначают $\mathrm{Z}(A)$. Кольцо можно рассматривать как алгебру над любым его подкольцом, содержащим единицу и лежащим в центре. На этом пути получаются все алгебры с единицей, поскольку имеет место

Ещё одно замечание.

∘ Пусть A — алгебра над (коммутативным) кольцом R. Отображение

$$\xi : R \to \mathrm{Z}(A), \lambda \mapsto \lambda' = 1 \cdot \lambda,$$

является гомоморфизмом колец; этот гомоморфизм инъективный, если кольцо R является полем. Заметим, что выполняется соотношение

$$a\lambda' = a \cdot 1\lambda = a1 \cdot \lambda = a\lambda,$$

где a — произвольный элемент алгебры и λ — произвольный скаляр. Таким образом, умножение элементов алгебры на скаляр λ производит такое же действие как умножение на элемент λ' внутри алгебры. Сделанное наблюдение позволяет элементы кольца отождествить с элементами из центра по отображению ξ и рассматривать алгебру далее уже над кольцом $\mathrm{im}\,\xi$, содержащимся в её центре.

Упражнение. Докажите, что любая алгебра вкладывается изоморфно в алгебру с единицей. Именно, пусть A — алгебра над коммутативным кольцом R. Определим на множестве $R \times A$ операции умножение на скаляры из R и сложения покомпонентно, следующим образом

$$\lambda(\mu, v) = (\lambda\mu, \lambda v);$$
$$(\lambda, u) + (\mu, v) = (\lambda + \mu, u + v).$$

Определим умножение, положив

$$(\lambda, u)(\mu, v) = (\lambda\mu, \lambda v + \mu u + uv).$$

Здесь λ, μ — произвольные скаляры из кольца R и u, v — произвольные элементы алгебры A. Проверьте, что множество $R \times A$ является алгеброй над кольцом R, в которую алгебра A и кольцо R вкладываются изоморфно следующим образом

$$A \to R \times A, u \mapsto (0, u), \quad u \in A,$$
$$R \to R \times A, \lambda \mapsto (\lambda, 0), \quad \lambda \in R.$$

Примеры. Пусть R — коммутативное кольцо с единицей. Алгебрами над кольцом R являются следующие кольца:

∘ кольцо $R[x]$ многочленов;

∘ кольцо $R[[x]]$ степенных рядов;

∘ кольцо $R^{n,n}$ матриц.

∘ Множество R^n столбцов высоты n является модулем над кольцом R и (левым) модулем над матричным кольцом $R^{n,n}$.

∘ Абелева группа является $\mathbb{Z}$-модулем.

Упражнение. Докажите, что центром алгебры квадратных матриц размера n над полем является множество скалярных матриц $\lambda \mathrm{e}_n$, где λ — произвольный элемент поля, e_n — единичная матрица.

2. Линейные отображения

Пусть M, N — модули над кольцом R. Отображение

$$g : M \to N, u \mapsto g(u)$$

называется *гомоморфизмом* модулей, или *линейным* отображенем, если оно перестановочно с операциями сложения и умножения на скаляры, то есть выполняются условия:

(1) $g(u + v) = g(u) + g(v)$;

(2) $g(u\lambda) = g(u)\lambda$;

для любых u, v из M, λ из R. Линейные отображения $\mathbb{Z}$-модулей называются также гомоморфизмами абелевых групп. Множество всех гомоморфизмов между R-модулями M и N обозначается

$$\mathrm{Hom}_R(M, N).$$

Линейное отображение модуля в себя называется его *линейным преобразованием* или *эндоморфизмом*. Множество всех эндоморфизмов модуля M обозначается

$$\mathrm{End}_R(M).$$

Отображение между алгебрами M, N называется *гомоморфизмом алгебр*, если в дополнение к условиям (1,2) оно перестановочно с умножением, то есть выполняется условие

(3) $g(u \cdot v) = g(u) \cdot g(v)$

для любых u из M и λ из R.

Биективный гомоморфизм называется *изоморфизмом*. Обычно модули и алгебры (как и другие алгебраические структуры) рассматриваются с точностью до изоморфизма, так что изоморфные алгебраические структуры (между которыми имеется изоморфизм) особо не различаются и считаются копиями друг друга. Рассмотрим следующие

Примеры.

∘ Пусть a — матрица размера $n \times m$ над коммутативным кольцом R. Отображение

$$R^m \to R^n,\ x \mapsto ax$$

является гомоморфизмом модулей. Здесь предполагается, что наборы в множествах R^m, R^n записываются в виде столбцов.

∘ Если кольцо R — коммутативное, то для любого его элемента λ следующее отображение R-модуля U в себя является эндоморфизмом:

$$M \to M, u \mapsto u \cdot \lambda.$$

∘ Множество $\mathrm{Hom}_R(M, N)$ является абелевой группой со сложением, определённым поточечно — следующим образом:

$$(g + h)(u) = g(u) + h(u)$$

для любых гомоморфизмов g, h и любого элемента u из M. Нулём этой группы является гомоморфизм, тождественно равный нулю. Для любого гомоморфизма противоположным является гомоморфизм, принимающий противоположные значения при любых значениях аргумента.

∘ Если кольцо R коммутативно, то произведение гомоморфизма на скаляр также является гомоморфизмом. В этом случае множество

$\mathrm{Hom}_R(M,N)$ является модулем со сложением, определённым выше, и с умножением на скаляры, определённым поточечно следующим образом:

$$(g\lambda)(u) = g(u)\lambda$$

для любого гомоморфизма g и скаляра λ из R.

∘ Композиция гомоморфизмов модулей (если она корректна) является гомоморфизмом, причём выполняются законы дистрибутивности:

$f\circ(g+h) = f\circ g + f\circ h, (f+g)\circ h = f\circ h + g\circ h$ (если композиции корректны).

В частности, множество $\mathrm{End}_R(M)$ является кольцом со сложением, определённым выше, где умножение совпадает с композицией. Это множество является алгеброй с поточечным умножением на скаляры из кольца R, если это кольцо коммутативно.

Алгебры линейных преобразований (эндоморфизмов) модулей играют особую роль в силу следующей теоремы.

Теорема. *Алгебра над коммутативным кольцом изоморфна некоторой алгебре линейных преобразований.*

Доказательство. Достаточно доказать теорему для алгебры с единицей. Пусть A — алгебра с единицей над полем K. Обозначим через $\widehat{A}$, модуль, пролученный из алгебры A «забыванием» умножения. Отметим пару свойств.

(1) *Для любого элемента a из алгебры A отображение*

$$\widehat{A} \to \widehat{A}, \mu_a : x \mapsto ax,$$

является эндоморфизмом модуля $\widehat{A}$.

(2) *Отображение*

$$A \to \mathrm{End}_K(\widehat{A}), a \mapsto \mu_a,$$

является изоморфным вложением алгебр.

Записанные свойства проверяются непосредственно, их достаточно для доказательства теоремы. □

Упражнение. Проверьте записанные свойства.

3. Свободный модуль и векторное пространство

В этом разделе опредляются алгебраические структуры свободного модуля и векторного пространства.

Свободный модуль. Пусть M — модуль над кольцом R и T — некоторое множество, где для каждого его элемента s задан вектор u_s, принадлежащий модулю M. Иными словами, задан набор векторов

$$(u_s|s \in T).$$

Если все вектора различные, то будем говорить также о множестве векторов

$$\{u_s|s \in T\}.$$

Линейной комбинацией этих векторов называется выражение

$$\sum_s u_s\lambda_s,$$

где почти все коэффициенты λ_s равны нулю. Линейная комбинация называется тривиальной, если все её коэффициенты нулевые.

Набор векторов u_s, где $s \in T$, называется *линейно независимым*, если только тривиальная линейная комбинация этих векторов равна нулю. В противном случае набор называется *линейно зависимым*. Заметим, что все вектора линейно независимого набора различные, так что можно говорить о линейно независимом множестве векторов.

Набор векторов u_s, где $s \in T$, называется *порождающим* (модуль M), если любой вектор из модуля выражается линейной комбинацией этих векторов. Линейно независимый порождающий набор (также множество) векторов u_s, где $s \in T$, называется *базисом* модуля. Равносильным образом, каждый вектор v, принадлежащий модулю, единственным образом выражается в виде линейной комбинации

$$v = \sum_s u_s\lambda_s.$$

В этом случае коэффициенты λ_s однозначно определяются вектором v и называются его *координатами* относительно данного базиса. Модуль, в котором есть базис, называется *свободным*.

Примеры.

$\circ$ Пусть T — множество индексов. Напомним, что через R^T обозначается множество всех наборов

$$u = (u_s|u_s \in R, s \in T),$$

составленных из элементов кольца R и индексированных элементами из множества T. Такие наборы составляют модуль над кольцом R с покомпонентным сложением и с умножением на скаляры, выполняемыми следующим образом:

$$(u + v)_s = u_s + v_s, (u\lambda)_s = u_s\lambda \text{ для всех } s \text{ из } T,$$

где u, v — произвольные наборы и λ — произвольный скаляр. Над коммутативным кольцом R рассматриваемые наборы составляют алгебру с покомпонентным умножением, таким, что

$$(uv)_s = u_s v_s \text{ для всех } s \text{ из } T.$$

Наборы, у которых почти все компоненты нулевые, образуют свободный модуль (а также и алгебру), который обозначается $\oplus_T R$. Здесь имеется базис, состоящий из наборов δ_s, где $s \in T$, и

$$\delta_{st} = \begin{cases} 1, & \text{если } s = t; \\ 0, & \text{в противном случае;} \end{cases}$$

для любых $s, t \in T$.

∘ Пусть R — коммутативное кольцо с единицей. Заметим, что алгебра $R[[x]]$ формальных степенных рядов является также R-модулем, а содержащаяся в ней алгебра многочленов, $R[x]$, является свободным модулем с базисом

$$x^0, x^1, x^2, \ldots.$$

Имеется изоморфизм R-модулей (но не алгебр)

$$R^{\mathbb{N}} \to R[[x]], u \mapsto \sum_s u_s x^s,$$

отображающий $\oplus_{\mathbb{N}} R$ на $R[x]$.

Имеет место

Теорема. *Свободные модули (над одним кольцом) с равномощными базисами изоморфны.*

Доказательство. Если наборы векторов u_s и v_s (где $s \in T$) составляют базисы модулей M и N, то имеется изоморфизм:

$$M \to N, \sum_s u_s \lambda_s \mapsto \sum_s v_s \lambda_s. \; \square$$

Отметим далее пару свойств базисов свободного модуля.

Модуль, содержащий конечное порождающее множество, называется *конечно порождённым.*

∘ *В конечно порождённом свободном модуле все базисы конечные.*

Доказательство. Рассмотрим в свободном модуле порождающее множество S и базис B. Заметим, что элементы порождающего множества выражаются в виде линейных комбинаций через элементы базиса. Обозначим через B_α (конечное) множество векторов из базиса, через которые выражается вектор α. Тогда

$$B = \cup_\alpha B_\alpha,$$

здесь объединение вычисляется по всем векторам α из множества S. Отсюда, базис B конечный, если множество S конечное. $\square$

$\circ$ *B модуле с бесконечным базисом все базисы равномощны.*

Доказательство. Продолжим рассуждение. Предположим дополнительно, что модуль содержит бесконечный базис. Тогда все базисы бесконечные в силу свойства, установленного выше. Пусть теперь S, B — бесконечные базисы, для которых выполняется неравенство $|S| \leqslant |B|$. В этом случае также должны выполняться неравенства

$$|S| \leqslant |B| = |\cup_\alpha B_\alpha| \leqslant \aleph_0 |S| = |S|,$$

откуда $|S| = |B|$. $\square$

Важным примером свободного модуля является

Векторное пространство. Модуль над полем называется *векторным пространством*. Имеет место

Теорема. *Векторное пространство содержит базис.*

Доказательство. Рассмотрим упорядоченное включением множество всех линейно независимых подмножеств векторного пространства. Это частично упорядоченное множество удовлетворяет условиям леммы Цорна, а значит, содержит максимальное множество; оно и является базисом. $\square$

Теорема о размерности векторного пространства. *B векторном пространстве все базисы равномощны.*

Доказательство этой теоремы опирается на установленные выше свойства базисов свободного модуля, а также на лемму Штейница, которая будет доказана ниже.

В векторном пространстве два набора векторов назовём *эквивалентными*, если они порождают один и тот же подмодуль.

Лемма Штейница о замене. Пусть в векторном пространстве линейно независимые вектора $v_1, \ldots, v_s$ выражаются линейно через вектора $u_1, \ldots, u_r$. Тогда $s \leqslant r$ и после надлежащей перенумерации векторов $u_1, \ldots, u_r$ их набор эквивалентен набору векторов $v_1, \ldots, v_s$, $u_{s+1}, \ldots, u_r$.

Доказательство. При $s = 0$ доказывать нечего. Пусть $s > 0$. Предположим по-индукции, что $s - 1 \leqslant r$ и набор векторов $u_1, \ldots, u_r$ эквивалентен набору векторов $v_1, \ldots, v_{s-1}$, $u_s, \ldots, u_r$. Тогда вектор v_s линейно выражается через вектора каждого из этих наборов. А так как вектора v_k линейно независимые, то минимальное множество векторов из второго набора, через которые выражается вектор v_s, должно содержать вектор u_s после надлежащей перенумерации векторов $u_s, \ldots, u_r$. Не сложно понять

далее, что набор векторов $v_1, \ldots, v_s,\ u_{s+1}, \ldots, u_r$ эквивалентен набору $v_1, \ldots, v_{s-1},\ u_s, \ldots, u_r$ и тогда набору $u_1, \ldots, u_r$. $\square$

Следствие. *В конечно порождённом векторном пространстве любые два базиса равномощны.* $\square$

Доказательство теоремы о размерности. В силу свойств базисов свободного модуля, достаточно доказать теорему для конечно порождённого векторного пространства, а в этом случае теорема является следствием леммы Штейница. $\square$

Упражнение. В векторном пространстве любое линейно независимое множество векторов можно расширить до базиса.

В завершение раздела перечислим ряд примеров алгебр над полем.

$\circ$ Кольцо многочленов $K[x]$ с коэффициентами в поле K является алгеброй с единицей над этим полем. Здесь базис составляют многочлены

$$1, x, x^2, x^3, \ldots.$$

$\circ$ Кольцо многочленов $K[x_1, \ldots, x_n]$ от переменных $x_1, \ldots, x_n$ с коэффицентами в поле K является алгеброй с единицей. Естественным базисом здесь является множество мономов

$x_1^{k_1} \cdots x_n^{k_n}$, где $k_1, \ldots, k_n$ — произвольные натуральные числа.

$\circ$ Квадратные матрицы размера n, составленные из элементов поля, образуют алгебру размерности n^2 над ним.

$\circ$ Над произвольным полем верхнетреугольные матрицы (у которых нули ниже главной диагонали) и нижнетреугольные матрицы (с нулями выше диагонали) образуют изоморфные алгебры.

Упражнение. Докажите, что алгебры в последнем примере действительно изоморфны. Какова их размерность?

4. Координаты вектора

В этом разделе продолжается изучение свободных модулей.

Пусть $e = (e_1, \ldots, e_m)$ — набор векторов R-модуля M и a —матрица размера $m \times n$ из $R^{m,n}$. Определим произведение

$$ea = (\sum_k e_k a_{k1}, \sum_k e_k a_{k2}, \ldots, \sum_k e_k a_{kn}).$$

Отметим далее ряд свойств.

$\circ$ Для любых матриц a, b размера $m \times n, n \times s$, составленных из элементов кольца R, имеет место равенство

$$e \cdot ab = ea \cdot b. \ \square$$

Пусть далее e — базис свободного модуля M.

∘ Для любого вектора u из модуля M существует столбец $u\downarrow$, принадлежащий модулю $R^m = R^{m,1}$, такой, что выполняется равенство

$$u = e \cdot u\downarrow, \text{ где } u\downarrow = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix}. \square$$

Компоненты столбца $u\downarrow$ однозначно определены и называются *координатами* вектора u в базисе e.

∘ Отображение

$$c_e : M \to R^m, u \mapsto u\downarrow,$$

является изоморфизмом модулей. $\square$

Пусть теперь $e' = (e'_1, \ldots, e'_{m'})$ — ещё один базис. (Вопрос о том, выполняется ли равенство $m = m'$, рассмотрим позднее.)

∘ Существует матрица $c_{ee'}$ размера $m \times m'$, составленная из элементов кольца R, для которой выполняется равенство

$$e' = ec_{ee'}.$$

Матрица $c_{ee'}$ определена однозначно, так как её столбцы являются наборами координат базисных векторов базиса e' в базисе e. Она называется *матрицей перехода* от базиса e к базису e'. $\square$

∘ Пусть e'' — ещё один базис. Тогда имеет место равенство:

$$c_{ee''} = c_{ee'}c_{e'e''}.$$

В частности, имеют место равенства:

$$c_{ee'}c_{e'e} = \mathrm{e}_m,\ c_{e'e}c_{ee'} = \mathrm{e}_{m'},$$

где e_m — еденичная матрица размера m. $\square$

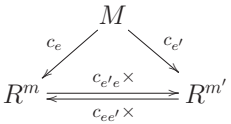
∘ Обозначим через $u'\downarrow$ набор координат вектора u в базисе e', тогда

$$e'u'\downarrow = ec_{ee'}u'\downarrow,$$

откуда

$$u\downarrow = c_{ee'}u'\downarrow . \square$$

Получили закон изменения координат при смене базиса: при смене базиса набор координат в старом базисе получаются из набора координат в новом умножением на матрицу перехода. Сказанное можно проиллюстрировать следующей диаграммой.



Упражнение. Докажите сформулированные свойства.

5. Матрица линейного отображения

Пусть M, N — свободные R-модули с конечными базисами

$$e = (e_1, \dots, e_m), g = (g_1, \dots, g_n).$$

Пусть также

$$h : M \to N, u \mapsto h(u)$$

— линейное отображение (гомоморфизм) R-модулей. Распространим его действие на наборы, считая

$$h : M^k \to N^k, (u_1 \dots, u_k) \mapsto (h(u_1), \dots, h(u_k))$$

для любого целого положительного k. Отметим ряд свойств.

∘ Для некоторой матрицы $\overline{h}_{ge}$ размера $n \times m$ (составленной из элементов кольца R) выполняется условие

$$h : e \mapsto g\overline{h}_{ge}.$$

Эта матрица определена однозначно, так как её столбцы — наборы координат в базисе g для образов при отображении h векторов из базиса e. Она называется *матрицей линейного отображения* h.

∘ Коммутативна следующая диаграмма:

$$\begin{array}{ccc} M & \xrightarrow{h} & N \\ {\scriptstyle c_e}\downarrow & & \downarrow{\scriptstyle c_g} \\ R^m & \xrightarrow{\overline{h}_{ge}\times} & R^n. \end{array}$$

∘ Отображение

$$\mathrm{Hom}_R(M, N) \to R^{n,m}, h \mapsto \overline{h}_{ge}$$

является изоморфизмом R-модулей в случае коммутативного кольца R. Если $M = N$, то данное отображение является изоморфизмом колец, и является изоморфизмом алгебр в случае коммутативного кольца R. Таким образом, в этом последнем случае имеет место изоморфизм алгебр

$$\mathrm{End}_R(M) \to R^{m,m}, h \mapsto \overline{h}_{ge}.$$

(В алгебре эндоморфизмов в роли умножения выступает операция композиции отображений.)

Посмотрим, что происходит с матрицей отображения при смене базиса.

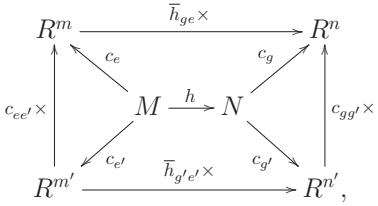
∘ Пусть $e' = (e'_1, \dots, e'_{m'})$ и $g = (g'_1, \dots, g'_{n'})$ — ещё одна пара базисов модулей M и N, $\overline{h}_{g'e'}$ — матрица линейного отображения h для неё. Тогда

$$h : e' = ec_{ee'} \mapsto g\overline{h}_{ge}c_{ee'} = g'c_{g'g}\overline{h}_{ge}c_{ee'}.$$

Получаем следующий закон изменения матрицы линейного отображения при смене базисов:

$\overline{h}_{g'e'} = c_{g'g}\overline{h}_{ge}c_{ee'}$, в частности, $\overline{h}_{e'e'} = c_{e'e}\overline{h}_{ee}c_{ee'}$ при $M = N, e = g, e' = g'$.

Ситуацию можно проиллюстрировать коммутативной диаграммой



где все негоризонтальные стрелки обратимы.

Отметим ещё одно следствие полученных результатов. Пусть R — коммутативное кольцо с единицей. Будем рассматривать квадратные матрицы размера n, составленные из элементов этого кольца. Матрицы a и b называются *подобными*, если для некоторой обратимой матрицы c выполняется равенство

$$a = c^{-1}bc.$$

Это равенство означает, что матрицы a, b являются матрицами одного и того же линейного преобразования свободного модуля R^n в некоторых базисах, переход между которыми определяется посредством матрицы c. Таким образом, имеет место

Теорема. *Две матрицы тогда и только тогда подобны над коммутативным кольцом с единицей, когда являются матрицами одного и того же линейного преобразования над ним.* □

6. Инвариантность размерности

Отметим следующее свойство.

∘ *Для кольца R следующие условия равносильны.*

(1) *В любом свободном модуле над кольцом R все базисы равномощны.*

(2) *В любом конечно-порождённом свободном модуле над кольцом R все базисы равномощны.*

(3) *Для различных натуральных чисел m, n R-модули R^m, R^n не изоморфны.*

Доказательство. Равносильность первых двух условий следует из установленных ранее свойств базисов в свободном модуле. Равносильность последних двух условий следует из того, что свободный R-модуль с базисом мощности m изоморфен модулю R^m. □

Кольцо, удовлетворяющее условиям (1–3), называется *кольцом с инвариантной размерностью*. Мощность базиса в свободном модуле M над кольцом с инвариантной размерностью называется его *размерностью* или *рангом* и обозначается

$$\dim M, \operatorname{rank} M.$$

Примеры.

∘ Конечное кольцо является кольцом с инвариантной размерностью.

∘ Поле является кольцом с инвариантной размерностью.

Имеет место

Теорема. *Коммутативное кольцо является кольцом с инвариантной размерностью.*

Доказательство. Пусть кольцо R коммутативно. Доказательство разобьём на три части.

(1) *Сюръективный гомоморфизм $h : R^n \to R^n$ инъективен.*

Пусть $e = (e_1, \ldots, e_n)$ базис в R^n. Так как h сюръективен, в R^n для некоторого набора $v = (v_1, \ldots, v_n)$ векторов выполняется

$$h : v \mapsto e.$$

Рассмотрим линейное преобразование

$$g : R^n \mapsto R^n, \text{ где } g : e \mapsto v.$$

Заметим, что композиция $h \circ g$ является тождественным преобразованием. Следовательно, для матриц $\overline{h}, \overline{g}$ линейных преобразований g, h в произвольном базисе выполняется равенство

$$\overline{h} \cdot \overline{g} = \mathrm{e}_n, \ \det \overline{h} \cdot \det \overline{g} = 1.$$

Отсюда, матрица $\overline{h}$ обратима, как и преобразование h.

(2) *Для сюръективного гомоморфизма $h : R^n \to R^m$ выполняется неравенство $m \leqslant n$.*

Пусть $m \geqslant n$ и тогда $m = n + k$ для некоторого натурального k. В этом случае гомоморфизм

$$g : R^{n+k} \to R^m, g(u, v) \mapsto h(u)$$

сюръективен и по предыдущему свойству инъективен. Тогда $k = 0$.

(3) *Для изоморфизма $h : R^n \to R^m$ выполняется равенство $m = n$.*

Это следует из предыдущих двух свойств. Теорема доказана. □

7. Теорема Гамильтона-Кэли

В этом разделе рассматривается векторное пространство V размерности m над полем K и линейное преобразование h этого пространства.

Собственные вектора и значения. Естественным является вопрос: как следует выбирать базис в пространстве V, чтобы матрица линейного преобразования h в этом базисе имела по-возможности простой вид (скажем, была бы диагональной, или содержала диагональный блок). Имея в виду данный вопрос, выделим в пространстве V вектора, которые преобразуются наиболее простым способом, именно — умножаются на некоторый скаляр при действии h. Такие вектора и скаляры называются собственными. Выясним, как можно находить собственные вектора и соответствующие собственные значения; можно ли из собственных векторов составить базис, или хотя бы часть базиса.

Пусть u — ненулевой вектор из пространства V и λ — произвольный скаляр из поля K. Будем называть вектор u собственным вектором преобразования h, относящимся к собственному значению λ, если выполняется равенство

$$h(u) = u\lambda.$$

Зафиксируем в пространстве V базис e. Пусть $\overline{h}$ — матрица линейного преобразования h в этом базисе, то есть выполняется соотношение

$$h : e \mapsto e\overline{h}.$$

Отметим ряд свойств собственных векторов и значений линейного преобразования h.

∘ *Собственные вектора, относящиеся к собственному значению λ, суть всевозможные такие ненулевые вектора и пространства V, для которых выполняется равенство*

$$(\mathrm{e}_m\lambda - \overline{h})u{\downarrow} = 0{\downarrow},$$

где $u{\downarrow}$ — набор координат вектора u в базисе e, то есть набор, принадлежащий векторному пространству $K^{n,1}$ и удовлетворяющий условию

$$u = eu{\downarrow}\,.$$

Доказательство. В силу изморфизма

$$M \to K^{n,1}, u \mapsto u{\downarrow},$$

при котором

$$h(u) \mapsto \overline{h}u{\downarrow},$$

соотношение

$$u\lambda - h(u) = 0,$$

выполняющееся в пространстве V для собственного вектора u, отвечающего собственному значению λ, равносильно соотношению

$$(\mathrm{e}_m\lambda - \overline{h})u\downarrow = 0\downarrow,$$

выполняющему в пространстве $K^{n,1}$. □

Матрица $(\mathrm{e}_m x - \overline{h})$ называется *характеристической матрицей* матрицы $\overline{h}$, а также *характеристической матрицей* преобразования h в базисе e. Она составлена из многочленов кольца $K[x]$ и принадлежит кольцу $K[x]^{m,m}$. Многочлен с коэффициентами в поле K, равный определителю этой матрицы, называется *характеристическим* многочленом матрицы $\overline{h}$ и преобразования h.

∘ *Собственные значения линейного преобразования h суть всевозможные корни его характеристического многочлена $\chi_h(x)$, где*

$$\chi_h(x) = \det(\mathrm{e}_m x - \overline{h}).$$

Доказательство. В соответствии с предыдущим свойством собственные значения суть всевозможные значения λ, при которых система линейных однородных уравнений с матрицей $\mathrm{e}_m\lambda - \overline{h}$ имеет ненулевое решение. Это происходит в том и только том случае, когда эта матрица необратима, то есть когда её определитель равен нулю. □

∘ *Характристический многочлен не изменяется при смене базиса.*

Доказательство. Это следует из предыдущего свойства, но можно и непосредственно проверить, что подобные матрицы имеют совпадающие характеристические многочлены. □

∘ *Множество собственных векторов, относящихся к одному собственному значению, пополненное нулевым вектором, образует векторное пространство.*

Доказательство. Это следует из первого свойства.

∘ *Набор собственных векторов линейно независим, если в нём собственные вектора, относящиеся к любому одному собственному, значению линейно независимы.*

Доказательство. Пусть $\lambda_1, \ldots, \lambda_n$ — различные собственные значения преобразования h и для каждого значения λ_i (где $1 \leqslant i \leqslant n$) задан линейно незавимый набор относящихся к нему собственных векторов

$$u_{i1}, \ldots, u_{ik(i)}.$$

Докажем, что набор из всех векторов

$$u_{11}, \ldots, u_{1k(1)}, \ldots, u_{n1}, \ldots, u_{nk(n)}.$$

линейно независим. Это так при $n = 1$ по условию. Предположим, по индукции, что $n > 1$ и свойство выполняется для первых $n-1$ собственных значений. Заметим, что соотношение линейной зависимости

$$\sum_{ij} a_{ij}u_{ij} = 0 \text{ (где } 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant k(i))$$

между собственными векторами u_{ij} приводит к следующему соотношению линейной зависимости

$$\sum_{ij} \lambda_i a_{ij}u_{ij} = 0$$

между их гомоморфными образами $h(u_{ij}) = \lambda_i u_{ij}$. Отсюда

$$\sum_{ij}(\lambda_i - \lambda_n)a_{ij}u_{ij} = \sum_{ij} \lambda_{ij}a_{ij}u_{ij} - \lambda_n \sum_{ij} a_{ij}u_{ij} = 0.$$

Получили соотношение линейной зависимости между собственными векторами, относящимися к собственным значениям $\lambda_1, \ldots, \lambda_{n-1}$. По предположению индукции все коэффициенты в этом соотношении — нулевые. Тогда равны нулю и пропорциональные им коэффициенты a_{ij}, относящиеся к первым $n-1$ собственным значениям λ_i (где $1 \leqslant i \leqslant n-1$). Но тогда в силу условия остальные коэффициенты a_{nj}, относящиеся к значению λ_n, также нулевые. □

Теорема Кэли-Гамильтона. Пусть A — алгебра над полем K и d — её элемент. Заметим, что имеется гомоморфизм алгебр

$$\xi : K[x] \to A, \sum_i a_i x^i \mapsto \sum_i a_i d^i.$$

Образ многочлена $f(x)$ при этом гомоморфизме обозначается через $f(d)$. Говорят, что элемент d является корнем многочлена $f(x)$, если в алгебре A выполняется соотношение $f(d) = 0$.

Образ $\operatorname{im}\xi$ самого гомоморфизма ξ обозначается через $K[d]$. Он совпадает с наименьшей по включению алгеброй, содержащейся в A и содержащей единицу и элемент d. В частности, можно говорить об алгебрах $K[h], K[\overline{h}]$. Заметим, что между ними имеется следующий изоморфизм

$$K[h] \to K[\overline{h}], f(h) \mapsto f(\overline{h}).$$

Имеет место

Теорема Гамильтона-Кэли. *Линейное преобразование над полем является корнем своего характеристического многочлена.*

Замечание. В силу записанного выше изоморфизма в теореме слова «линейное преобразование» можно заменить на «квадратная матрица».

Доказательство теоремы. Докажем, что матрица $\overline{h}$ является корнем её характеристического многочлена

$$\chi_h(x) = a_0 x^m + \ldots + a_m.$$

Положим $X = \mathrm{e}_m x$ и рассмотрим следующее соотношение

$$\mathrm{adj}(X - \overline{h})(X - \overline{h}) = \chi_h(X).$$

имеющее место в матричном кольце $K[x]^{m,m}$. Заметим, что в этом кольце всякую матрицу можно однозначно записать в виде «многочлена» от переменной X, где коэффициентами являются матрицы из $K^{m,m}$. В том числе, можно записать

$$\mathrm{adj}(X - \overline{h}) = \overline{b}_0 X^{m-1} + \ldots + \overline{b}_{m-1}.$$

В этом выражении $\overline{b}_i$ — некоторые однозначно определённые матрицы из кольца $K^{m,m}$. Коэффициенты многочленов $\mathrm{adj}(X - \overline{h})$ и $\chi_h(X)$ связаны следующими соотношениями:

$$\begin{aligned} a_0 &= \overline{b}_0, \\ a_1 &= \overline{b}_1 - \overline{b}_0\overline{h}, \\ &\ldots \\ a_{m-1} &= \overline{b}_{m-1} - \overline{b}_{m-2}\overline{h} \\ a_m &= -\overline{b}_{m-1}\overline{h}. \end{aligned}$$

Отсюда видно, что коэффициенты $\overline{b}_0, \ldots, \overline{b}_{m-1}$ многочлена $\mathrm{adj}(X - \overline{h})$ принадлежат коммутативному кольцу $K[\overline{h}]$, вслед за коэффициентами $a_0, \ldots, a_m$ многочлена χ_h. Таким образом, записанное выше разложение многочлена $\chi_h(X)$ в действительности имеет место в кольце $K[\overline{h}][X]$. Рассматривая образ этого соотношения по гомоморфизму

$$K[\overline{h}][X] \to K[\overline{h}], \sum_i c_i X^i \mapsto \sum_i c_i \overline{h}^i,$$

приходим к равенству $\chi_h(\overline{h}) = 0$. $\square$

Упражнение. Проверьте следующие факты.

$\circ$ У подобных матриц характеристические многочлены совпадают.

$\circ$ Для квадратной матрицы над полем равносильны условия:

(1) она обратима;

(2) нуль не является её собственным значением;

(3) характеристический многочлен имеет ненулевой свободный член.

$\circ$ Для квадратной матрицы $\overline{h}$ размера m над полем K тогда и только тогда существует обратная матрица $\overline{h}^{-1}$, когда в кольце $K[x]$ существует

многочлен $s(x)$, обратный для многочлена x по модулю многочлена $\chi_h(x)$, так, что

$$xs(x) \equiv 1 \mod \chi_h(x).$$

в этом случае $\overline{h}^{-1} = s(\overline{h})$.

∘ Для обратимой квадратной матрицы $\overline{h}$ размера m над полем K обратную матрицу можно записать как

$$\overline{h}^{-1} = -a_m^{-1}\overline{b}_{m-1},$$

где a_m — свободный член многочлена $\chi_h(x)$ и $\overline{b}_{m-1}$ — свободный член многочлена $\mathrm{adj}(X - \overline{h})$. Матрица $\overline{b}_{m-1}$ принадлежит кольцу $K[\overline{h}]$ и записывается в виде многочлена от $\overline{h}$ степени, меньшей m, с коэффициентами в поле K. Этот многочлен можно найти посредством схемы Горнера. (Указание: смотрите доказательство теоремы Кэли-Гамильтона.)

Норма и след элемента алгебры. Пусть A — алгебра ранга n с единицей над полем K, a — её элемент. Ниже определяются норма и след элемента a, формулируются некоторые свойства этих функций.

Упражнение. Проверьте следующее свойство.

∘ Отображение

$$\mu_a : A \to A, x \mapsto ax.$$

является линейным преобразованием алгебры A.

Определитель и след этого линейного преобразования (то есть его матрицы в произвольном базисе) называются соответственно *нормой* и *следом* элемента a. Для нормы и следа используются обозначения $\mathrm{nr}(a), \mathrm{tr}(a)$. Характеристический многочлен преобразования μ_a называется *характеристическим многочленом* элемента a и обозначается $\chi_a(x)$.

∘ Проверьте следующие свойства характеристического многочлена.

(∘) $\chi_a(x) = x^n - \mathrm{tr}(a)x^{n-1} + \ldots + (-1)^n \mathrm{nr}(a)$ для любого a из A.

(∘) Элемент алгебры является корнем своего характеристического многочлена.

(∘) Элемент алгебры тогда и только тогда обратим, когда его норма отлична от нуля.

∘ Проверьте следующие свойства нормы.

(∘) $\mathrm{nr}(a) \in K$ для любого a из A.

(∘) $\mathrm{nr}(a) = a^n$ для любого a из K.

(∘) $\mathrm{nr}(1) = 1$.

(∘) $\mathrm{nr}(ab) = \mathrm{nr}(a)\,\mathrm{nr}(b)$ для любых a, b из A.

∘ Проверьте следующие свойства следа.

(∘) $\mathrm{tr}(a) \in K$ для любого a из A.

(∘) $\mathrm{tr}(a) = na$ для любого a из K.

(∘) $\mathrm{tr}(0) = 0$.

(∘) $\mathrm{tr}(a + b) = \mathrm{tr}(a) + \mathrm{tr}(b)$ для любых a, b из A.

(∘) $\mathrm{tr}(ab) = \mathrm{tr}(ba)$ для любых a, b из A.

ГЛАВА 15

Симметрические многочлены и результант

В главе изучаются симметрические многочлены от нескольких переменных, с коэффициентами в поле. Они рассматриваются как функции, определяющие преобразования корней и коэффициентов многочленов от одной переменной.

1. Многочлены нескольких переменных

Пусть K — коммутативное кольцо с единицей. Будем рассматривать многочлены от переменных $x_1, \dots, x_n$ с коэффициентами в кольце K. Сделаем некоторые определения.

Основные определения. Положим $x = (x_1, \dots, x_n)$. Пусть также $i = (i_1, \dots, i_n)$ — некоторый набор натуральных чисел. Многочлен

$$x^i = x_1^{i_1} \cdots x_n^{i_n}$$

называется *мономом* и многочлен

$$ax^i = a \cdot x_1^{i_1} \cdots x_n^{i_n},$$

где a — ненулевой элемент из K, называется *термом* с коэффициентом a. Многочленом называется (конечная) линейная комбинация мономов, то есть выражение

$$\sum_i a_i x^i,$$

где почти все коэффициенты a_i равны нулю и суммирование ведётся по наборам i из множества $\mathbb{N}^n$. Сложение и умножение многочленов осуществляется в соответствии с правилами

$$\sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i + b_i) x^i;$$

$$\Big(\sum_i a_i x^i\Big)\Big(\sum_j b_j x^j\Big) = \sum_k \Big(\sum_{i+j=k} a_i b_j\Big) x^k,$$

где сложение наборов показателей выполняется покомпонентно, так что

$$(i_1, \dots, i_n) + (j_1, \dots, j_n) = (i_1 + j_1, \dots, i_n + j_n).$$

Многочлены образуют коммутативное кольцо с единицей, обозначаемое $K[x_1, \dots, x_n]$, куда кольцо K изоморфно вкладывается отображением

$K \to K[x_1, \dots, x_n], a \mapsto ax^0,$ где 0 — нулевой набор показателей.

Степень многочлена. *Степенью* монома x^i называется число

$$\deg x^i = i_1 + \ldots + i_n,$$

равное сумме его показателей. *Степенью* ненулевого многочлена $f(x) = \sum_i a_i x^i$ называется величина

$$\deg f = \max\{\deg x^i : i \in \mathbb{N}^n, a_i \neq 0\},$$

равная наибольшей из степеней мономов, входящих в многочлен f. Многочлен называется *однородным* или *формой* степени n, если все его мономы имеют одну и ту же степень, равную n. Нулевой многочлен считается формой произвольной заданной степени. Заметим, что любой многочлен f можно представить в виде суммы однородных многочленов

$$f = f_0 + f_1 + \ldots,$$

где $f_0, f_1, \ldots$ — формы степени $0, 1, \ldots$, которые называются *однородными компонентами* многочлена f. Однородную компоненту, степень которой совпадает со степенью многочлена, назовём *старшей*. Отметим следующее

Соотношение для степеней. *Для ненулевых многочленов f, g выполняются соотношения:*

$$\deg(f + g) \leqslant \max\{\deg f, \deg g\},$$

$$\deg(f \cdot g) \leqslant \deg f + \deg g.$$

Второе неравенство строгое, если и только если старшие однородные компоненты многочленов в произведении дают нуль.

Доказательство. Для доказательства нужно записать многочлены в виде суммы однородных компонент и заметить, что сумма форм одной степени является формой той же степени и произведение форм степеней i, j является формой степени $i + j$.

Упражнение. Многочен f из кольца $K[x_1, \ldots, x_n]$ является формой степени m тогда и только тогда, когда в кольце $K[x_0, x_1, \ldots, x_n]$ выполняется соотношение

$$f(x_0 x_1, \ldots, x_0 x_n) = x_0^m f(x_1, \ldots, x_n).$$

Упорядочения мономов. Пусть далее кольцо K целостное. Будем рассматривать многочлены от переменных $x_1, \ldots, x_n$ с коэффициентами в кольце K. Пусть множество мономов упорядочено отношением $\leqslant$. Станем называть это упорядочение *правильным*, если выполняются следующие условия.

(1) Отношение $\leqslant$ является полным порядком на множестве мономов. Иными словами, это отношение является линейным порядком, относительно которого не существует бесконечных строго убывающих цепей.

(2) Для любых мономов x^i, x^j, x^k выполняется импликация:

$$(x^i < x^j) \to (x^i x^k < x^j x^k).$$

Примеры.

∘ Лексикографическое упорядочение. Будем считать $x^i < x^j$, если $i \neq j$ и первая компонента, по которой наборы i и j различаются, меньше в наборе i. Такое упорядочение является правильным. Оно называется лексикографическим.

∘ Градуированное лексикографическое упорядочение. Будем считать $x^i < x^j$, если $\deg x^i < \deg x^j$, а также, если $\deg x^i = \deg x^j$ и моном x^i меньше монома x^j по лексикографическому упорядочению. Такое упорядочение является правильным. Оно называется градуированным лексикографическим.

Будем считать далее, что на множестве мономов задано некоторое правильное упорядочение $\leqslant$. Будем обозначать

$$\mathrm{LM}(f), \mathrm{LT}(f)$$

старший (наибольший) моном и соответствующий терм ненулевого многочлена f (входящие в него с ненулевым коэффициентом). Коэффициент, с которым входит старший моном, называется *старшим коэффициентом*. Старший коэффициент многочлена f обозначается

$$\mathrm{LC}(f).$$

Отметим следующее

Свойство старших термов. *Пусть f, g — ненулевые многочлены над целостным кольцом K. Тогда*

$$\mathrm{LT}(fg) = \mathrm{LT}(f)\,\mathrm{LT}(g).$$

Доказательство. Свойство выполняется в силу определения правильного упорядочения.

2. Теорема Гаусса о симметрических многочленах

По-прежнему рассматриваются многочлены от переменных $x_1, \ldots, x_n$ с коэффициентами в целостном кольце K. Многочлен f называется *симметрическим*, если он не меняется при любой перестановке переменных. Иными словами, для любой подстановки α из множества S_n имеет место равенство

$$f(x_1, \ldots, x_n) = f(x_{1\alpha}, \ldots, x_{n\alpha}).$$

Симметрический многочлен называется *моногенным*, если все его термы получаются из одного перестановками переменных. Будем обозначать

$$M + \ldots$$

моногенный симметрический многочлен с термом M.

Примеры.

∘ Элементарными называются симметрические многочлены

$$\begin{aligned}\sigma_1 &= x_1 + \dots,\\ \sigma_2 &= x_1x_2 + \dots,\\ \sigma_2 &= x_1x_2x_3 + \dots,\\ &\dots\\ \sigma_n &= x_1 \cdots x_n.\end{aligned}$$

∘ Многочленами Ньютона называются симметрические многочлены

$$\begin{aligned}s_1 &= x_1 + \dots,\\ s_2 &= x_1^2 + \dots,\\ s_3 &= x_1^3 + \dots,\\ &\dots\\ s_n &= x_1^n + \dots.\end{aligned}$$

Теорема (Гаусса о симметрических многочленах). *Пусть K — область целостности. Тогда в кольце $K[x_1, \dots, x_n]$ для любого симметрического многочлена f существует единственный многочлен g, такой, что*

$$f(x) = g(\sigma).$$

Коэффициенты многочлена g являются целочисленными линейными комбинациями коэффициентов многочлена f.

Здесь используются обозначения $x = (x_1, \dots, x_n)$ и $\sigma = (\sigma_1, \dots, \sigma_n)$.

Доказательство. Будем рассматривать лексикографическое упорядочение на множестве мономов. Пусть

$$f(x) = ax^{\overline{k}} + \dots$$

— симметрический многочлен со старшим термом $ax^{\overline{k}}$ и для симметрических многочленов с меньшим старшим мономом всё доказано. Заметим, что компоненты набора $\overline{k} = (\overline{k}_1, \dots, \overline{k}_n)$ упорядочены по убыванию:

$$\overline{k}_1 \geqslant \overline{k}_2 \geqslant \dots \geqslant \overline{k}_n.$$

Рассмотрим многочлен

$$\sigma^k = \sigma_1^{k_1} \cdots \sigma_n^{k_n}, \text{ где } k_1 = \overline{k}_1 - \overline{k}_2, k_2 = \overline{k}_2 - \overline{k}_1, \dots, k_n = \overline{k}_n.$$

Вычислим его старший моном:

$$\begin{aligned}\mathrm{LM}(\sigma^k) &= \mathrm{LM}(\sigma_1)^{k_1}\cdots\mathrm{LM}(\sigma_n)^{k_n} = \\ &= x_1^{k_1}(x_1x_2)^{k_2}\cdots(x_1\cdots x_n)^{k_n} = \\ &= x_1^{k_1+\ldots+k_n}x_2^{k_2+\ldots+k_n}\cdots x_n^{k_n} = \\ &= x^{\overline{k}}.\end{aligned}$$

Он такой же, как у многочлена f. Следовательно,

$$\mathrm{LM}(f(x)-a\sigma^k) < \mathrm{LM}(f),\ \text{и}\ f(x)-a\sigma^k = h(\sigma)$$

для некоторого многочлена $h(x)$ по предположению индукции. Тогда

$$f(x) = g(\sigma),\ \text{где}\ g(x) = ax^k + h(x).$$

Существование многочлена g доказано. Докажем его единственность.

Поскольку разность симметрических многочленов является симметрическим многочленом, достаточно доказать, что для ненулевого многочлена $g(x)$ многочлен $g(\sigma)$ также не нулевой. Итак, пусть $g(x)$ — ненулевой многочлен. Каждому его мономy x^k теперь сопоставим моном $x^{\overline{k}}$, где

$$\overline{k}_1 = k_1+\ldots+k_n, \overline{k}_2 = k_2+\ldots+k_n, \ldots, \overline{k}_n = k_n.$$

Пусть $x^{\overline{k}_*}$ — наибольший из мономов $x^{\overline{k}}$. Заметим, что

$$\mathrm{LM}(\sigma^k) = x^{\overline{k}},\ \text{откуда}\ \mathrm{LM}(g(\sigma)) = x^{\overline{k}_*}.$$

Многочлен $g(\sigma)$ не нулевой. Теорема доказана. □

Замечание. Симметрические многочлены образует кольцо, обозначим его $K[x_1,\ldots,x_n]^{S_n}$. В силу теоремы имеется изоморфизм колец:

$$K[x_1,\ldots,x_n] \to K[x_1,\ldots,x_n]^{S_n}, g(x)\mapsto g(\sigma).$$

Ещё замечание. В доказательстве теоремы для симметрического многочлена $f(x)$ многочлен $g(x)$, такой, что $f(x)=g(\sigma)$ находится в виде

$$g(x) = a(1)x^{k(1)} + a(2)x^{k(2)} + \ldots,$$

где

$$\begin{aligned}&a(1) = \mathrm{LC}(f),\\ &x^{\overline{k}(1)} = \mathrm{LM}(f(x))\ \text{и}\\ &x^{\overline{k}(1)} > x^{\overline{k}(2)} > \ldots.\end{aligned}$$

Это наблюдение можно использовать для практического отыскания многочлена $g(x)$ методом неопределённых коэффициентов. В связи с этим отметим также, что мономы $x^{\overline{k}(1)}, x^{\overline{k}(2)}, \ldots$, для которых соответствующие коэффициенты $a(1), a(2), \ldots$ не нулевые, имеют степень n, если многочлен $f(x)$ является формой степени n. Рассмотрим ряд примеров.

∘ Пусть $n = 2$; непосредственно находим разложение

$$(x_1 - x_2)^2 = \sigma_1^2 - 4\sigma_2.$$

∘ Для произвольного $n \geqslant 2$ непосредственно находится разложение

$$s_2 = \sigma_1^2 - 2\sigma_2.$$

∘ Для произвольного $n \geqslant 2$ выразим многочлен s_3 через элементарные симметрические. В соответствии с замечанием выше получаем следующие значения:

$$\begin{aligned}
&\overline{k}(1) = (3, 0, 0, 0, \ldots), && k(1) = (3, 0, 0, 0, \ldots),\\
&\overline{k}(2) = (2, 1, 0, 0, \ldots), && k(2) = (1, 1, 0, 0, \ldots),\\
&\overline{k}(3) = (1, 1, 1, 0, \ldots), && k(3) = (0, 0, 1, 0, \ldots).
\end{aligned}$$

Тогда

$$s_3 = \sigma_1^3 + a(2)\sigma_1\sigma_2 + a(3)\sigma_3.$$

Подставляя $x = (1, 1, 0, 0, \ldots), (1, 1, 1, 0, \ldots)$ вместо переменных, получаем

$$\begin{aligned}
2 =& 8 + 2a(2),\\
3 =& 27 + 3a(2) + a(3);
\end{aligned}$$

откуда находим $a(2) = -3, a(3) = 1$. Окончательно имеем

$$s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + \sigma_3.$$

∘ Пусть $n = 3$. Выразим симметрический многочлен

$$\Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

через элементарные. В соответствии с замечанием получаем следующие значения:

$$\begin{aligned}
&\overline{k}(1) = (4, 2, 0), && k(1) = (2, 2, 0),\\
&\overline{k}(2) = (4, 1, 1), && k(2) = (3, 0, 1),\\
&\overline{k}(3) = (3, 3, 0), && k(3) = (0, 3, 0),\\
&\overline{k}(4) = (3, 2, 1), && k(4) = (1, 1, 1),\\
&\overline{k}(5) = (2, 2, 2), && k(5) = (0, 0, 2).
\end{aligned}$$

Отсюда

$$\Delta = \sigma_1^2\sigma_2^2 + a(2)\sigma_1^3\sigma_3 + a(3)\sigma_2^3 + a(4)\sigma_1\sigma_2\sigma_3 + a(5)\sigma_3^2.$$

Упражнение. Найдите коэффициенты в предыдущем примере.

3. Симметрические функции корней

Пусть K — поле. Рассмотрим многочлен

$$f(z) = a_0 z^n + a_1 z^{n-1} \ldots + a_n.$$

от переменной z, степени n, с коэффициентами в поле K. Предположим он разлагается на линейные множители над полем K, то есть имеет место равенство

$$f(z) = a_0(z - x_1) \cdots (z - x_n),$$

где $x_1, \ldots, x_n$ — корни многочлена. Заметим, что верны соотношения:

$$\frac{a_1}{a_0} = -\sigma_1, \frac{a_2}{a_0} = \sigma_2, \ldots, \frac{a_n}{a_0} = (-1)^n \sigma_n,$$

где $\sigma_1, \sigma_2, \ldots, \sigma_n$ — значения элементарных симметрических многочленов от корней. Записанные соотношения называются *формулами Виета.*

Теорема. *Пусть F — симметрический многочлен от n переменных с коэффициентами в поле K, имеющий степень m по переменной. Тогда существует форма G степени m от $n+1$ переменной с коэффициентами в поле K, такая, что*

$$a_0^m F(x_1, \ldots, x_n) = G(a_0, \ldots, a_n).$$

Коэффициенты многочлена G являются целочисленными линейными комбинациями коэффициентов многочлена F.

Доказательство. Следует повторить доказательство теоремы Гаусса о симметрических многочленах, где взять вместо многочленов f, g многочлены $a_0^m F, G$ и воспользоваться формулами Виета. □

Пример (дискриминант). Пусть

$$\Delta(x_1, \ldots, x_n) = \prod_{i<j} (x_i - x_j)^2.$$

Этот многочлен симметрический с целыми коэффициентами степени $2n-2$ по переменной. В соответствии с теоремой существует целочисленная форма $\mathrm{disc}(f)$ степени $2n-2$ от коэффициентов многочлена f, такая, что

$$\mathrm{disc}(f) = a_0^{2n-2} \Delta(x_1, \ldots, x_n).$$

Эта форма называется дискриминантом многочлена f.

Примеры.

∘ Пусть $n = 2$. Найдём дискриминант многочлена

$$f(x) = a_0 x^2 + a_1 x + a_2.$$

Воспользуемся примером из предыдущего раздела.

$$\operatorname{disc}(f) = a_0^2\Delta(x_1, x_2) = a_0^2(x_1 - x_2)^2 = a_0^2(\sigma_1^2 - 4\sigma_2) =$$
$$= a_0^2\Big(\Big(-\frac{a_1}{a_0}\Big)^2 - 4\frac{a_2}{a_0}\Big) = a_1^2 - 4a_0a_2.$$

∘ Пусть $n = 3$. Рассмотрим многочлен

$$f(x) = a_0x^3 + a_1x^2 + a_2x + a_3.$$

Найдём его дискриминант. Воспользуемся примером и упражнением из предыдущего раздела:

$$\operatorname{disc}(f) = a_0^4\Delta(x_1, x_2, x_2) = a_0^4(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 =$$
$$= a_0^4(\sigma_1^2\sigma_2^2 + a(2)\sigma_1^3\sigma_3 + a(3)\sigma_2^3 + a(4)\sigma_1\sigma_2\sigma_3 + a(5)\sigma_3^2) =$$
$$= a_1^2a_2^2 + a(2)a_1^3a_3 + a(3)a_0a_2^3 + a(4)a_0a_1a_2a_3 + a(5)a_0^2a_3^2.$$

Известны коэффициенты: $a(2) = a(3) = -4$, $a(4) = 18$, $a(5) = -27$.

4. Результант двух многочленов

Пусть K — поле. Рассмотрим пару многочленов

$$f(z) = a_0z^n + a_1z^{n-1} + \ldots + a_n,$$
$$g(z) = b_0z^m + b_1z^{m-1} + \ldots + b_m$$

от переменной z, с коэффициентами в поле K. Не будем предполагать, что коэффициенты a_0, b_0 отличены от нуля. В связи с этим будем называть их формальными старшими коэффициентами и числа n, m будем называть формальными степенями многочленов f, g. Будем интересоваться вопросом: при каких условиях многочлены имеют общий делитель положительной степени или, что равносильно, имеют общий корень в некотором расширении поля. Имеет место

Теорема. *Пусть хотя бы один из коэффициентов a_0, b_0 отличен от нуля. Многочлены $f(z), g(z)$ тогда и только тогда имеют общий делитель положительной степени, когда найдутся многочлены $C(z), D(z)$ с коэффициентами в поле K, для которых выполняются следующие условия.*

(1) *Имеет место равенство $f(z)C(z) + g(z)D(z) = 0$.*

(2) *Хотя бы один из многочленов $C(z), D(z)$ не нулевой.*

(3) $\deg C(z) < m, \deg D(z) < n$.

Доказательство. Если многочлены f, g имеют общий делитель h положительной степени, то их можно представить в виде

$$f(z) = h(z)D(z),$$
$$g(z) = -h(z)C(z)$$

где для многочленов C, D выполняются записанные условия (проверьте). Обратно, пусть выполнены записанные условия для многочленов C, D. В частности, имеет место равенство

$$f(z)C(z) = -g(z)D(z).$$

Если многочлен C не нулевой, то все неприводимые делители многочлена g не могут входить в многочлен C с теми же кратностями в силу третьего условия. Некоторый делитель будет общим для f, g. Теорема доказана. □

Следствие (основное свойство результанта). *Пусть хотя бы один из коэффициентов a_0, b_0 отличен от нуля. Многочлены $f(z), g(z)$ тогда и только тогда имеют общий делитель положительной степени, когда равен нулю следующий определитель*

$$\det \begin{pmatrix} a_0 & a_1 & \dots & a_n & & & & \\ & \ddots & & & \ddots & & & \\ & & \ddots & & & \ddots & & \\ & & & \ddots & & & \ddots & \\ & & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & \dots & & b_m & & \\ & \ddots & & & & & \ddots & \\ & & b_0 & b_1 & \dots & \dots & & b_m \end{pmatrix}.$$

Здесь на местах, где не находятся коэффициенты многочленов, стоят нули. Записанный определитель называется результантом многочленов f, g и обозначается $\mathrm{res}(f, n, g, m)$. Матрица, находящаяся под знаком определителя, называется *матрицей Сильвестра*.

Доказательство. Наряду с многочленами f, g рассмотрим пару многочленов

$$C(z) = c_0 z^{m-1} + c_1 z^{m-2} + \ldots + c_{m-1},$$
$$D(z) = d_0 z^{n-1} + d_1 z^{n-2} + \ldots + d_{n-1}.$$

Заметим, что равенство $f(z)C(z)+g(z)D(z)=0$ равносильно набору из $n+m$ сотношений:

$$\begin{array}{lllllll}
a_0c_o & & & +b_0d_0 & & & =0;\\
a_1c_o & +a_0c_1 & & +b_1d_0 & +b_0d_1 & & =0;\\
\dots & \dots & \dots & \dots & \dots & & \\
 & \dots & \dots & & \dots & \dots & \\
 & & a_nc_{m-1} & & & +b_md_{n-1} & =0.
\end{array}$$

Записанные соотношения получены приравниванием нулю коэффициентов многочлена $f(z)C(z)+g(z)D(z)$ при убывающих степенях

$$z^{n+m-1}, z^{n+m-2}, \dots, z^0$$

переменной z. Станем рассматривать эти соотношения как систему линейных алгебраических уравнений относительно неизвестных коэффициентов многочленов $C(z), D(z)$. В соответствии с теоремой наличие общего делителя положительной степени у многочленов $f(z), g(z)$ равносильно существованию ненулевого решения этой системы и равносильно тогда равенству нулю определителя этой системы. Осталось заметить, что матрица этой системы в транспонированном виде совпадает с матрицей Сильвестра. □

Отметим пару свойств результанта.

∘ *Результант* $\operatorname{res}(f,n,g,m)$ *является целочисленным многочленом от переменных* $a_0,\dots,a_n,b_0,\dots,b_m$, *однородным степени* m *по переменным* $a_0,\dots,a_n$ *и однородным степени* n *по переменным* $b_0,\dots,b_m$.

Доказательство. Это следует из соотношений

$$\operatorname{res}(x_0f,n,g,m)=x_0^m\operatorname{res}(f,n,g,m),$$
$$\operatorname{res}(f,n,x_0g,m)=x_0^n\operatorname{res}(f,n,g,m).\ \square$$

∘ *Существуют многочлены* $A(z), B(z)$ *с коэффициентами в поле* K, *такие, что*

$$f(z)A(z)+g(z)B(z)=\operatorname{res}(f,n,g,m).$$

Доказательство. Над полем $K(z)$ рассмотрим систему линейных алгебраических уравнений

$$sx\downarrow = b\downarrow,$$

где $x\downarrow$ — столбец из $n+m$ неизвестных, $s = (s_0\downarrow, \ldots, s_{n+m-1}\downarrow)$ — матрица Сильвестра многочленов f, g и

$$b\downarrow = \begin{pmatrix} z^{m-1}f(z) \\ \vdots \\ z^0 f(z) \\ z^{n-1}g(z) \\ \vdots \\ z^0 g(z) \end{pmatrix}.$$

Эта система имеет решение

$$x\downarrow = \begin{pmatrix} z^{n+m-1} \\ \vdots \\ z^0 \end{pmatrix}.$$

Применим формулу Крамера для последней компоненты решения. Получаем соотношение

$$\det s = z^0 \det(s_0\downarrow, \ldots, s_{n+m-2}\downarrow, b\downarrow).$$

В левой части равенства находится $\mathrm{res}(f, n, g, m)$. Для завершения доказательства определитель в правой части нужно разложить по последнему столбцу и в полученной сумме из слагаемых вынести общие множители, равные многочленам $f(z), g(z)$. $\square$

Замечание (исключение неизвестной). Последнее свойство позволяет использовать результант для исключения неизвестной из системы алгебраических уравнений с несколькими неизвестными. Рассмотрим систему из двух алгебраических уравнений

$$\begin{aligned} F(y, z) &= 0, \\ G(y, z) &= 0; \end{aligned}$$

где F, G — многочлены от двух переменных с коэффициентами в поле K. Станем рассматривать эти многочлены как многочлены от переменной z, где коэффициенты являются многочленами от переменной y. Рассматривая многочлены в таком духе, будем использовать для них обозначения $F_y(z), G_y(z)$. Пусть

$$R(y) = \mathrm{res}(F_y(z), n, G_y(z), m),$$

где n, m — степени многочленов по переменной z. Отметим, что результант не зависит от переменной z. Из доказанного свойства следует, что уравнение

$$R(y) = 0$$

является следствием исходной системы, то есть для любого решения (y_0, z_0) системы компонента y_0 является решением этого уравнения. Мы можем найти значение y_0, решив это уравнение, а затем найти z_0, решив исходную систему, предварительно подставив в неё y_0 вместо y. Тем самым, решение системы сводится к решению уравнений с одной неизвестной.

Упражнение. В каких случаях частичное решение z_0 дополняется до полного решения (y_0, z_0)?

5. Результант как симметрическая функция корней

Пусть теперь многочлены f, g следующим образом разлагаются на линейные множители над полем K:

$$f(z) = a_0(z - x_1)\cdots(z - x_n),$$
$$g(z) = b_0(z - y_1)\cdots(z - y_m).$$

Здесь z — переменная, $x_1, \ldots, x_n$ — корни многочлена $f(z)$ и $y_1, \ldots, y_m$ — корни многочлена $g(z)$. В этих условиях имеет место

Теорема. *Имеют место равенства:*

$$\begin{aligned}\operatorname{res}(f, n, g, m) &= (-1)^{nm} b_0^n \prod_{j=1}^{m} f(y_j) \\ &= a_0^m \prod_{i=1}^{n} g(x_i) \\ &= a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(x_i - y_j).\end{aligned}$$

Доказательство. Заметим, что первые два выражения, стоящие в правой части, равны третьему и, таким образом, все три выражения справа равны. Рассматривая результант как целочисленный многочлен от корней и от старших коэффициентов, можно заметить, что он обращается в ноль при подстановке x_i вместо y_j. Отсюда следует, что он делится на многочлены $(x_i - y_j)$ и тогда на их произведение, так как эти многочлены взаимно просты. Поскольку результант однороден по коэффициентам многочленов f, g, он должен делиться на многочлен

$$a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(x_i - y_j).$$

Результант совпадает с этим многочленом с точностью до целочисленного множителя, так как рассматривая их как многочлены от коэффициентов (второй многочлен потребуется преобразовать для этого), замечаем, что оба они обладают одинаковыми степенями и однородны по обоим наборам

коэффициентов. Этот множитель равен единице, так как оба многочлена содержат моном $a_0^m b_m^n$. $\square$

Следствие. Имеет место следующее равенство:

$$\operatorname{res}(f, n, f', n-1) = (-1)^{\binom{n}{2}} a_0 \operatorname{disc}(f).$$

Доказательство. Вычислим производную:

$$\begin{aligned} f'(z) &= (a_0(z-x_1)\cdots(z-x_n))' = \\ &= a_0 \sum_{i=1}^{n} (z-x_1)\cdots\widehat{(z-x_i)}\cdots(z-x_n), \end{aligned}$$

где сверху помечена отсутствующая скобка. Отсюда

$$\begin{aligned} \operatorname{res}(f, n, f', n-1) &= a_0^{n-1} \prod_{i=1}^{n} f'(x_i) = (a_0(z-x_1)\cdots(z-x_n))' = \\ &= a_0^{2n-1} \prod_{i=1}^{n} (x_i-x_1)\cdots\widehat{(x_i-x_i)}\cdots(x_i-x_n) = \\ &= (-1)^{\binom{n}{2}} a_0^{2n-1} \prod_{i<j} (x_i-x_j)^2. \end{aligned}$$

Сравнивая полученное выражение с соотношением

$$\operatorname{disc}(f) = a_0^{2n-2} \prod_{i<j} (x_i-x_j)^2,$$

получаем требуемое равенство. $\square$

Упражнения. Проверьте следующие свойства.

- $\operatorname{res}(f, n, g, m) = \pm \operatorname{res}(g, m, f, n)$.
- $\operatorname{res}(f, n, gh, m+k) = \operatorname{res}(f, n, g, m) \operatorname{res}(f, n, h, k)$.
- $\operatorname{res}(f, n, g, m) = a_0^{n-k} \operatorname{res}(h, k, g, m)$, если $g(z) = f(z)q(z) + h(z)$.

Здесь $n = \deg f$, $m = \deg g$, $k = \deg h$ и a_0 — старший коэффициент многочлена f.

Часть III

Действительные и комплексные числа

ГЛАВА 16

Действительные числа

В главе изучается числовая система действительных чисел. Прежде всего, формулируются свойства, которые согласуются с интуитивным пониманием действительных чисел и однозначно определяют их числовую систему.

1. Упорядоченное кольцо

Пусть K — коммутативное кольцо с единицей. Назовём его *упорядоченным*, если в нём выделены подмножества K_+ *положительных* и K_- *отрицательных элементов*, и выполняются следующие условия.

(1) Положительные элементы противоположны отрицательным:

$$K_- = -K_+.$$

(2) Положительные, отрицательные элементы и ноль разбивают кольцо:

$$K = K_- \sqcup \{0\} \sqcup K_+.$$

(3) Множество K_+ замкнуто сложением:

$$K_+ + K_+ \subseteq K_+.$$

(4) Множество K_+ замкнуто умножением:

$$K_+ \cdot K_+ \subseteq K_+.$$

В этом случае на K определяется линейное упорядочение $\leqslant$, такое, что

$$a < b \Leftrightarrow b - a \in K_+;$$

и тогда выполняется следующее условие.

(5) Множество K_+ есть множество элементов кольца K, больших нуля.

Упражнение. Для заданного подмножества $K_+ \subseteq K$ существует не более одного упорядочения на K, удовлетворяющего условиям (1–5).

Отметим пару свойств.

∘ *Упорядоченное кольцо имеет нулевую характеристику.*

Это так потому, что элементы

$$1, 1+1, 1+1+1, \dots$$

все положительны. □

∘ *Упорядочение целостного кольца однозначно продолжается до упорядочения поля частных.*

Доказательство. Если поле частных $\mathrm{Frac}(K)$ упорядочено, то

$$a/b \in \mathrm{Frac}(K)_+ \Leftrightarrow ab \in K_+.$$

Это следует из того, что элемент b^2 положительный и умножение на положительный элемент не меняет знак (проверьте). Таким образом, упорядочение поля частных определено однозначно.

С другой стороны, записанное выражение корректно определяет упорядочение поля частных по упорядочению на кольце. Действительно, если $a/b = a'/b'$, то $ab' = a'b$. Тогда $abb'^2 = a'b'b^2$ и

$$\begin{aligned} ab \in K_+ &\Leftrightarrow abb'^2 \in K_+ \\ &\Leftrightarrow a'b'b^2 \in K_+ \\ &\Leftrightarrow a'b' \in K_+. \end{aligned}$$

Отсюда видно, что записанное выражение корректно определяет множество $\mathrm{Frac}(K)_+$.

Далее, предположим, дроби $a/b, c/d$ положительные. Тогда произведения ab, cd также положительны и дробь

$$a/b + c/d = (ad + bc)/bd$$

положительна вслед за произведением

$$(ad + bc)bd = abd^2 + b^2cd.$$

Таким образом множество $\mathrm{Frac}(K)_+$ замкнуто сложением. Замкнутость умножением проверяется не сложнее. □

Модулем или *абсолютным значением* называется следующая функция, определённая на упорядоченном кольце:

$$K \to K_+ \sqcup \{0\}, x \mapsto |x|,$$

где

$$|x| = \begin{cases} x, & \text{если } x \in K_+ \sqcup \{0\}; \\ -x, & \text{если } x \in K_-. \end{cases}$$

Упражнение. Докажите следующие утверждения.

∘ В упорядоченном поле $1 > 0$.

∘ В упорядоченном поле квадрат любого элемента положительный.

∘ В упорядоченном поле $a + b \leqslant c + d$, если $a \leqslant c$ и $b \leqslant d$.

∘ Существует единственное упорядочение кольца целых чисел.

∘ Существует единственное упорядочение поля рациональных чисел.

∘ (Неединственность порядка.) Поле

$$\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}b | a, b \in \mathbb{Q}\}$$

наряду с обычным упорядочением допускает ещё одно, при котором

$$\mathbb{Q}(\sqrt{2})_+ = \{a + \sqrt{2}b | a, b \in \mathbb{Q}, a > \sqrt{2}b\}.$$

∘ Придумайте другие примеры такого рода.

2. Аксиома Архимеда и систематические дроби

Поле действительных чисел не должно содержать бесконечно больших и бесконечно малых величин. Формальным выражением этого является аксиома Архимеда, которую мы здесь и рассмотрим. Заодно с этим возникает ещё одно важное понятие — систематической дроби.

Пусть $m \geqslant 2$ — целое число; зафиксируем его до конца главы. *Систематической дробью* с основанием m назовём выражение

$$a_0 + a_1/m + a_2/m^2 + \ldots,$$

где $a_0, a_1, a_2, \ldots$ — целые числа и $0 \leqslant a_k \leqslant m - 1$ для всех $k > 0$. Записанную систематическую дробь будем обозначать буквой a.

Условимся говорить, что дробь a *представляет* элемент α в упорядоченном поле K, если для любого натурального k выполняются неравенства

$$a(k) \leqslant \alpha < a(k) + 1/m^k,$$

где $a(k) = a_0 + a_1/m + \ldots + a_k/m^k$.

Замечание. Обратим внимание, что a_0 — целое число и его знак относится только к нему и не действует на остальные разряды дроби.

Теорема. *Для упорядоченного поля K равносильны условия:*

(1) *в K для любых положительных элементов a и b существует натуральное n, такое, что $a \cdot n > b$;*

(2) *в K для любых положительных элементов a и b существует натуральное n, такое, что $a > b/n$;*

(3) *каждый элемент поля представим систематической дробью.*

Каждое из условий, записанных в этой теореме, называются *аксиомой Архимеда*. Поле, в котором она выполняется, называется *архимедовым*.

Доказательство. Первые два условия очевидно равносильны. Докажем, что и третье условие им равносильно. Заметим, что возможность представить систематической дробью a элемент α означает, что её знаки

удовлетворяют неравенствам

$$a_0 \leqslant \alpha < a_0 + 1,$$
$$a_{k+1} \leqslant (m^{k+1}(\alpha - a(k)) < a_{k+1} + 1 \text{ для любого } k \geqslant 0$$

и тогда вычисляются следующим образом:

$$a_0 = \lfloor \alpha \rfloor, a_{k+1} = \lfloor m^{k+1}(\alpha - a(k)) \rfloor, \text{ где } k \geqslant 0.$$

Вместе с тем, при выполнении условий (1,2) целая часть

$$\lfloor \beta \rfloor = \max\{b | b \in \mathbb{Z}, b \leqslant \beta\}$$

существует для любого элемента β из K, тогда и систематическая дробь существует для представления любого элемента. Таким образом, третье условие является следствием первых двух. С другой стороны, пусть выполняется третье условие, α, β — положительные элементы, представленные систематическими дробями a, b. Тогда для некоторого значения k рациональные числа $a(k), b(k)$ положительны. Поскольку в поле рациональных чисел условия (1,2) выполняются, для некоторого значения n имеет место неравенство $b(k) + 1/m^k < a(k)n$. Отсюда $\beta < \alpha n$ и теорема доказана. □

3. Систематические и обыкновенные дроби

Отметим ещё несколько свойств систематических дробей. В том числе установим, что рациональные числа (обыкновенные дроби) в любом упорядоченном поле представляются периодическими с некоторого места систематическими дробями.

∘ *Различные систематические дроби не могут представлять один элемент.*

Доказательство. Элементы, представимые дробями a, b, лежат в интервалах

$$[a(k), a(k) + 1/m^k) \text{ и } [b(k), b(k) + 1/m^k),$$

которые не пересекаются, если $a_k \neq b_k$. □

Систематическую дробь a назовём *стандартной*, если существует бесконечно много натуральных значений k, для которых выполняется неравенство $a_k \neq m - 1$. Иными словами, систематическая дробь a не является стандартной, если для всех достаточно больших номеров k выполняется равенство $a_k = m - 1$.

∘ *Систематическая дробь, представляющая элемент архимедова поля, — стандартная.*

Доказательство. Предпололожим, нестандартная систематическая дробь a представляет элемент α архимедова поля. Тогда для некоторого натурального числа k и для любого натурального r выполняются условия:

$$a_{k+r} = m - 1,$$

$$a(k+r) \leqslant \alpha < a(k+r) + 1/m^{k+r},$$

$$0 < a(k+r) + 1/m^{k+r} - \alpha \leqslant 1/m^{k+r}.$$

Но

$$\begin{aligned} a(k+r)+\frac{1}{m^{k+r}} = \\ &= a(k) + (m-1)\Big(\frac{1}{m^{k+1}} + \frac{1}{m^{k+2}} + \ldots + \frac{1}{m^{k+r}}\Big) + \frac{1}{m^{k+r}} \\ &= a(k) + \frac{m-1}{m^{k+r}}\Big(m^{r-1} + m^{r-2} + \ldots + m^0\Big) + \frac{1}{m^{k+r}} \\ &= a(k) + \frac{(m-1)}{m^{k+r}}\frac{(m^r-1)}{(m-1)} + \frac{1}{m^{k+r}} \\ &= a(k) + \frac{1}{m^k}. \end{aligned}$$

Это значение не зависит от r. Следовательно,

$$a(k) + 1/m^k - \alpha = a(k+r) + 1/m^{k+r} - \alpha \leqslant 1/m^{k+r}.$$

Записанное условие выполняется при любом r. Это противоречит аксиоме Архимеда. □

Теорема. *В любом упорядоченном поле рациональные числа и только они представимы периодическими с некоторого места систематическими дробями.*

(Периодической с некоторого места называется систематическая дробь

$$a_0 + a_1/m + a_2/m^2 + \ldots,$$

где выполняются равенства $a_n = a_{n+T}$, для некоторого положительного T и всех достаточно больших n; значение T называют периодом дроби.)

Доказательство. Рассмотрим рациональное число q/r, где $r > 0$. Разделим q на r с остатком, получаем

$$q = a_0 r + q_1,$$
$$q/r = a_0 + q_1/r,$$

где $0 \leqslant q_1 < r$.

Далее разделим $m \cdot q_1$ на r с остатком. Получаем

$$mq_1 = a_1 r + q_2,$$
$$q_1/r = a_1/m + q_2/(mr),$$
$$q/r = a_0 + a_1/m + q_2/(mr),$$

где $0 \leqslant a_1 = \lfloor mq_1/r \rfloor < m$, $0 \leqslant q_2 < r$. И т. д. На k-м шаге получаем

$$q/r = a_0 + a_1/m + \ldots + a_k/m^k + q_{k+1}/(m^k r),$$

где $0 \leqslant a_k = \lfloor mq_k/r \rfloor < m$, $0 \leqslant q_{k+1} < r$; заметим здесь

$$a_0 + a_1/m + \ldots + a_k/m^k \leqslant q/r < a_0 + a_1/m + \ldots + a_k/m^k + 1/m^k.$$

Таким образом возникает следующее представление обыкновенной дроби q/r в виде систематической:

$$q/r = a_0 + a_1/m + a_2/m^2 + a_3/m^3 + \ldots.$$

При делении чисел $m \cdot q_k$ на r остатки в какой-то момент повторятся. Так что дробь оказывается периодической с некоторого места. Необходимость доказана. Доказательство достаточности опустим. □

Упражнение. Докажите, что периодическая с некоторого места стандартная дробь естественно представляет рациональное число. Указание: сначала докажите это для дроби $1 + 1/m^T + 1/m^{2T} + \ldots$, затем — для произвольной дроби с периодом T.

4. Аксиома Кантора

Представление о действительных числах тесно связано с непрерывностью. Их отождествляют с точками прямой линии, расположенными непрерывно. Если удалить хоть одну точку, это свойство исчезнет. Дальнейший ряд аксиом, равносильных между собой, выражает формально это свойство.

В упорядоченном множестве отрезком или интервалом называется множество

$$[a, b] = \{x | a \leqslant x \leqslant b\},$$

где $a < b$. Система отрезков $[a_k, b_k]$, где $k \in \mathbb{N}$, называется *системой вложенных отрезков*, если выполняются включения

$$[a_0, b_0] \supseteq [a_1, b_1] \supseteq [a_2, b_2] \supseteq \ldots.$$

В упорядоченном поле система вложенных отрезков, длины которых становятся сколь угодно малыми, так что для любого натурального $n > 0$ имеется номер k со свойством

$$b_k - a_k < 1/n,$$

называется *системой стягивающихся отрезков*.

Теорема. *В упорядоченном поле следующие условия равносильны.*

(1) *Выполняется аксиома Архимеда и следующая аксиома Кантора: всякая система вложенных отрезков содержит общую точку.*

(2) *Выполняется следующая усиленная аксиома Кантора: всякая система стягивающихся отрезков содержит единственную общую точку.*

Доказательство. Установим нужные импликации.

$(1 \to 2)$. Аксиомы Архимеда и Кантора совместно влекут усиленную аксиому Кантора.

Если бы система стягивающихся отрезков содержала элементы a, b, такие, что $a < b$, то разность $b - a$ являлась бы бесконечно малой величиной, меньшей $1/n$ для любого натурального $n \neq 0$; в архимедовом поле это невозможно.

$(2 \to 1)$. Усиленная аксиома Кантора влечёт аксиомы Архимеда и Кантора.

Предположим, что выполняется усиленная аксиома Кантора. Пусть a, b — положительные элементы. Заметим, что 0 является общей точкой системы стягивающихся отрезков $[0, b/k]$ и является их единственной общей точкой в силу усиленной аксиомы Кантора. Следовательно, некоторый отрезок $[0, b/n]$ не содержит a; тогда $a > b/n$ и выполняется аксиома Архимеда.

Далее, пусть задана система вложенных отрезков $[a_k, b_k]$. Построим систему стягивающихся отрезков $[a'_k, b'_k] \subseteq [a_k, b_k]$ следующим образом. Сначала отрезок $[a_0, b_0]$ разделим на 2 части посредстом элемента $x = (b_0 - a_0)/2$ и выберем в качестве $[a'_0, b'_0]$ любой один из отрезков $[a_0, x]$ или $[x, b_0]$, который имеет непустое пересечение с бесконечным числом отрезков $[a_k, b_k]$ и тогда со всеми этими отрезками, в силу их вложенности. Такой выбор возможен. Далее, предположим, отрезок $[a'_n, b'_n] \subseteq [a_n, b_n]$ уже построен. Пересечём его с отрезком $[a_{n+1}, b_{n+1}]$ и полученный в результате пересечения отрезок разделим на две части; теперь в качестве $[a'_{n+1}, b'_{n+1}]$ следует снова взять ту из частей, которая пересекается со всеми отрезками $[a_k, b_k]$. В результате получается система стягивающихся отрезков $[a'_k, b'_k]$ с общей точкой, принадлежащей всем отрезкам $[a_k, b_k]$. Таким образом, выполняется аксиома Кантора. □

Упражнение. Докажите, что получатся условия, равносильные условиям (1,2), если вместо «отрезков» говорить об «отрезках с рациональными концами».

5. Аксиома Дедекинда

Напомним, в упорядоченном множестве элемент c называется верхней гранью (под)множества A, если неравенство

$$a \leqslant c$$

выполняется для любого элемента a из A. Множество, имеющее верхнюю грань, называется ограниченным сверху. Наименьная из верхних граней, если существует, называется *точной верхней гранью* и обозначается $\sup A$. Двойственным образом определяется нижняя грань, точная нижняя грань и ограниченное снизу множество.

Сечением упорядоченного поля K назовём разбиение $K = A \sqcup B$, где элементы множества A меньше элементов из B. Элемент c называется *граничной точкой* сечения, если он является верхней гранью множества A и, одновременно, нижней гранью множества B. В этом случае он является точной верхней гранью множества A и точной нижней гранью для B.

Теорема. *В упорядоченном поле следующие условия равносильны.*

(1) *Выполняется аксиома Дедекинда: всякое сечение имеет граничную точку.*

(2) *Выполняется следующая аксиома о верхней грани: всякое непустое ограниченное сверху множество элементов имеет точную верхнюю грань.*

Доказательство. Установим необходимые импликации.

$(1 \to 2)$. Аксиома Дедекинда влечёт аксиому о верхней грани.

Пусть выполнено первое условие и множество X ограничено сверху. Образуем сечение

$$K = A \sqcup B, \text{ где } A = \{a | a \in K, a \leqslant x \text{ для некоторого } x \in X\}.$$

Не сложно понять, что граничная точка этого сечения является точной верхней гранью множества X; из первого условия следует второе.

$(2 \to 1)$. Аксиома Дедекинда следует из аксиомы о верхней грани.

Предположим, выполнено второе условие. Тогда для любого сечения $A \sqcup B$ точная верхняя грань множества A является и точной нижней гранью множества B и является тогда граничной точкой сечения. Таким образом из второго условия следует первое. □

Упражнение. Проверьте следующие факты.

∘ В теореме выше получатся равносильные условия, если вместо «множества элементов» говорить «множество рациональных чисел».

∘ Аксиома Архимеда следует из аксиомы Дедекинда и аксимы о верхней грани.

6. Фундаментальные последовательности

В архимедовом поле K рассмотрим последовательность элементов

$$a = a_0 a_1 \dots .$$

Элемент a_* назовём *пределом* этой последовательности (а также пределом последовательности элементов a_k при $k \to \infty$), если для любого положительного ε найдётся натуральное число $n(\varepsilon)$, такое что для всех $k > n(\varepsilon)$ выполняется неравенство

$$|a_* - a_k| < \varepsilon.$$

Иными словами, члены последовательности сколь угодно близко подходят к a_*: какое бы малое расстояние ε мы ни взяли, почти все элементы последовательности находятся от элемента a_* на расстоянии, меньшем ε.

Последовательность, имеющая предел, называется *сходящейся* (к нему). Предел сходящейся последовательности элементов a_k в архимедовом поле определён однозначно (проверьте это) и обозначается

$$\lim_{k\to\infty} a_k,$$

Пример. Предел последовательности $1/k$ при $k \to \infty$ равен нулю.

Последовательность a называется фундаментальной, если для любого положительного ε существует натуральное число $N(\varepsilon)$, такое, что для любых $k, l > N(\varepsilon)$ выполняется неравенство

$$|a_k - a_l| < \varepsilon.$$

Иначе говоря, элементы последовательности сближаются друг с другом: какое бы мы ни взяли расстояние, для почти всех членов последовательности расстояние между любыми двумя из них меньше этого расстояния.

Имеет место

Теорема. *В упорядоченном поле следующие условия равносильны.*

(1) *Выполняется аксиома Дедекинда.*

(2) *Выполняется усиленная аксиома Кантора.*

(3) *Выполняется аксиома Архимеда и следующая аксиома о фундаментальной последовательности: всякая фундаментальная последовательность имеет предел.*

Доказательство. Докажем необходимый ряд импликаций.

(1 → 2). Аксиома Дедекинда влечёт усиленную аксиому Кантора.

Предположим, первое условие имеет место и задана система вложенных отрезков $[a_k, b_k]$, где $k \in \mathbb{N}$. Определим сечение

$$K = A \sqcup B, \text{ где } A = \{a | a \in K, a < b_k \text{ для любого } k \in \mathbb{N}\}.$$

Заметим, что левые концы отрезков попадают в множество A, правые — в B и граничная точка сечения принадлежит всем отрезкам. Таким образом, имеет место аксиома Кантора. Следствием аксиомы Дедекинда является также аксиома Архимеда (см. упражнения выше) и тогда усиленная аксиома Кантора (см.теоремы выше).

$(2 \to 3)$. Аксиома Архимеда и аксиома о фундаментальной последовательности следуют из усиленной аксиомы Кантора.

Предположим, в упорядоченном поле выполняется второе условие, то есть верна усиленная аксиома Кантора. Из неё можно вывести аксиому Архимеда. Это было сделано при доказательстве одной из предыдущих теорем. Выведим аксиому о фундаментальной последовательности.

Пусть a_k — фундаментальная последовательность элементов поля. Построим систему стягивающихся отрезков, где в каждом отрезке содержатся почти все элементы последовательности. Сделаем это следующим образом. Так как фундаментальная последовательность ограничена (см. упражнения), все её элементы помещаются в некотором отрезке $[b_0, c_0]$. Далее, если отрезок $[b_k, c_k]$ содержит почти все элементы последовательности, то в соответствии с определением фундаментальной последовательности почти все её элементы должны попасть во вложенный отрезок

$$[b_k, c_k] \cap [a_{N(\varepsilon)+1} - \varepsilon, a_{N(\varepsilon)+1} + \varepsilon]$$

для любого $\varepsilon > 0$. Возьмём этот интервал в качестве $[b_{k+1}, c_{k+1}]$ при

$$\varepsilon = (c_k - b_k)/4.$$

Таким образом получается система стягивающихся отрезков, общая точка которой является пределом последовательности. Таким образом, имеет место аксиома о фундаментальной последовательности.

$(3 \to 1)$. Аксиома Архимеда и аксиома о фундаментальной последовательности совместно влекут аксиому Дедекинда.

Предположим, имеет место третье условие и задано сечение $A \sqcup B$. Определим последовательность элементов

$$a_0 a_1 \ldots,$$

выбрав элементы a_0, a_1 произвольно из разных множеств сечения и положив

$$a_{k+1} = (a_k + b_k)/2, \text{ где } k \geqslant 2 \text{ и}$$

b_k — последний из элементов, выбранных ранее элемента a_k, и принадлежащих другому множеству сечения, нежели он. Построенная последовательность фундаментальная в соответствии с упражнением ниже, так как для любого $k \geqslant 1$ почти все её элементы лежат в отрезке с концами a_k, b_k

длины, не превосходящей величины $(a_0 - a_1)/2^{k-1}$. В силу аксиомы о фундаментальной последовательности, построенная последовательность имеет предел a_*. Он определён однозначно в силу аксиомы Архимеда (см. упражнение). Заметим, что предел последовательности принадлежит отрезкам с концами a_k, b_k, находящимися в разных множествах сечения. Отсюда легко следует, что предел последовательности является граничной точкой сечения. □

Упражнение. Докажите следующие факты.

∘ В последней теореме получится ещё одно равносильное условие, если вместо «последовательностей» говорить о «последовательностях рациональных чисел».

∘ В архимедовом поле фундаментальная последовательность имеет не более одного предела.

∘ Последовательность фундаментальная, если имеется система стягивающихся отрезков, где каждый отрезок содержит почти все её элементы.

∘ Сходящаяся последовательность является фундаментальной.

∘ Фундаментальная последовательность ограничена сверху и снизу.

∘ Подпоследовательность

$$a_{k_0} a_{k_1} \ldots, \text{ где } 0 \leqslant k_0 < k_1 < \ldots,$$

фундаментальной последовательности

$$a_0 a_1 \ldots,$$

также фундаментальная.

∘ Подпоследовательность сходящейся последовательности сходится к тому же пределу

∘ Докажите, что

$$a_* + b_* = \lim_{k\to\infty} (a_k + b_k),$$
$$a_* \cdot b_* = \lim_{k\to\infty} (a_k \cdot b_k),$$

если

$$a_* = \lim_{k\to\infty} a_k,$$
$$b_* = \lim_{k\to\infty} b_k;$$

а также

$$1/b_* = \lim_{k\to\infty} (1/b_k), \text{ если } b_* = \lim_{k\to\infty} b_k \text{ и}$$

элементы b_* и b_k при всех k отличны от нуля.

7. Поле действительных чисел

Условия, выделенные в предыдущих трёх теоремах, равносильны между собой. Каждое из них назовём *аксиомой непрерывности*. Упорядоченное поле, в котором выполняется аксиома непрерывности, называется полем *действительных* или полем *вещественных* чисел.

Изоморфизмом упорядоченных полей или порядковым изоморфизмом полей называют биекцию между упорядоченными полями, которая является одновременно изоморфизмом полей и частично упорядоченных множеств. Имеет место

Теорема. *Поле действительных чисел существует. Оно единственно с точностью до изоморфизма упорядоченных полей.*

Доказательство. Разобьём доказательство на пять частей. В первых четырёх частях доказывается существование. Здесь приводится конструкция Вейерштрасса поля действительных чисел. Его элементы определяются как стандартные систематические дроби, для которых определяются упорядочение и операции сложения и умножения, проверяются необходимые условия. В пятой части доказывается, что любое поле действительных чисел отображается на построенное поле порядковым изоморфизмом, тождественным на рациональных числах.

(1) Существование. Элементы поля и упорядочение.

В качестве элементов поля будут выступать стандартные систематические дроби. Упорядочим их лексикографически, считая

$$a_0 + a_1/m + a_2/m^2 + \ldots < b_0 + b_1/m + b_2/m^2 + \ldots,$$
$$\text{если } a_0 = b_0, \ldots, a_{i-1} = b_{i-1}, a_i < b_i \text{ для некоторого } i.$$

Отождествим рациональные числа с представляющими их стандартными систематическими дробями. Такое отождествление согласуется с упорядочением рациональных чисел.

(2) Существование. Аксиома Кантора.

Убедимся, что всякая система вложенных отрезков в таком упорядоченном множестве имеет общую точку. Действительно, пусть $[a_i, b_i]$ — система вложенных отрезков нашего упорядоченного множества, где

$$a_i = a_{i,0} + a_{i,1}/m + a_{i,2}/m^2 + \ldots,$$
$$b_i = b_{i,0} + b_{i,1}/m + b_{i,2}/m^2 + \ldots$$

для любого натурального номера i. Для натурального k рассмотрим убывающую последовательность

$$b_0(k) \geqslant b_1(k) \geqslant b_2(k) \geqslant \ldots.$$

Эта последовательность стабилизируется, что можно проверить индукцией по k; то есть для некоторого натурального значения n_k выполняются равенства

$$b_{n_k}(k) = b_{n_k+1}(k) = b_{n_k+2}(k) = \dots.$$

В частности, для некоторого значения c_k выполняются равенства

$$c_k = b_{n_k,k} = b_{n_k+1,k} = b_{n_k+2,k} = \dots.$$

Заметим, что для любых натуральных i, k выполняются неравенства

$$a_i \leqslant a_i(k) \leqslant a_n(k) \leqslant b_n(k) = c(k) \leqslant b_i(k) \leqslant b_i,$$

где $n = \max(n_k, i)$. Отсюда можно увидеть, что дробь

$$c = c_0 + c_1/m + c_2/m^2 + \dots$$

стандартная и принадлежит всем отрезкам $[a_k, b_k]$.

(3) Существование. Усиление аксиомы Кантора.

Заметим, что общий элемент системы стягивающихся отрезков с рациональными концами определён однозначно. Это следует из того, что для любых стандартных систематических дробей c', c, где $c' < c$, в отрезке $[c', c]$ найдутся два различных рациональных числа, проверьте это в качестве упражнения. (Достаточно проверить наличие одного числа.) Действительно, если бы система отрезков содержала два общих элемента, то она содержала бы два рациональных числа, разность которых была бы бесконечно малой величиной. Данное рассуждение доказывает единственность общего элемента для любой системы стягивающихся отрезков (не только с рациональными концам), при условии, что определено сложение.

(4) Существование. Сложение и умножение.

Определим сложение и умножение. Сумму и произведение дробей a и b определим в каждом случае как единственную общую точку соответствующей системы стягивающихся отрезков с рациональными концами:

$$[a(k) + b(k) - 2/m^k, a(k) + b(k) + 2/m^k], \text{ и}$$

$$[a(k) \cdot b(k) - \varepsilon_k, a(k) \cdot b(k) + \varepsilon_k],$$

где $\varepsilon_k = (|a_0| + |b_0| + 3)/m^k$. Сделанное определение согласуется со сложением и умножением рациональных чисел. Заметим, что суммы $a + b, b + a$ содержатся во всех отрезках первой системы. Следовательно, эти элементы совпадают и сложение коммутативно. Аналогично, произведения ab, ba принадлежат всем отрезкам второй системы и умножение коммутативно. Остальные аксиомы упорядоченного поля проверяются не намного сложнее.

(5) Единственность поля действительных чисел.

Обозначим через $\mathbb{R}$ построенное выше поле действительных чисел. Пусть P — произвольное архимедово поле. Каждый его элемент a можно представить единственной стандартной систематической дробью, обозначим её a^*. Таким образом возникает инъективное отображение

$$P \to \mathbb{R}, a \mapsto a^*,$$

действующее тождественно на рациональных числах. Это отображение устаналивает изоморфизм между упорядоченным полем P и упорядоченным полем, являющимся образом данного отображения. Это так, поскольку в обоих полях операции определяются одним и тем же способом через операции и упорядочение для рациональных чисел. Если же архимедово поле P является полем действительных чисел, то записанное отображение также сюръективно и является, следовательно, изоморфизмом: на стандартную систематическую дробь

$$a_0 + a_1/m + a_2/m^2 + \dots$$

из поля $\mathbb{R}$ отображается элемент поля P, являющийся пределом фундаментальной последовательности

$$\begin{aligned} &a_0, \\ &a_0 + a_1/m, \\ &a_0 + a_1/m + a_2/m^2, \\ &\dots . \end{aligned}$$ □

Поле действительных чисел принято обозначать буквой $\mathbb{R}$.

Упражнение. Восполните детали доказательства последней теоремы и докажите следующие факты.

∘ Для стандартных систематических дробей c', c, где $c' < c$, в отрезке $[c', c]$ содержится рациональное число (то есть периодическая с некоторого места стандартная систематическая дробь).

∘ Любое архимедово поле порядково изоморфно подполю поля действительных чисел.

∘ В поле действительных чисел каждый элемент является пределом некоторой фундаментальной последовательности рациональных чисел.

∘ В поле действительных чисел каждый элемент является точной верхей гранью некоторого множества рациональных чисел.

∘ Конструкция Кантора. Будем рассматривать фундаментальные последовательности рациональных чисел. Определим покомпонентно сумму, разность и произведение последовательностей. Две последовательности назовём эквивалентными, если их разность сходится к нулю. Введённые

операции согласованы с этим отношением эквивалентности, поэтому можно говорить о сумме, разности и произведении классов эквивалентних последовательностей. Множество классов с этими операциями является полем действительных чисел. Проверьте данное рассуждение. Ответьте на следующие вопросы. Как в построенное поле вкладывается поле рациональных чисел? Как определено отношение меньше для классов? Что получится, если в описанной выше конструкции вместо $\mathbb{Q}$ взять произвольное архимедово поле?

$\circ$ Конструкция Дедекинда. Сечение $\mathbb{Q} = A \sqcup B$ назовём замкнутым, если

$$A = \{x | x \in \mathbb{Q}, x \leqslant a\}$$

для некоторого $a \in \mathbb{Q}$: назовём его открытым, если такого a не существует. Произвольной фундаментальной последовательности a, составленной из рациональных чисел, сопоставим сечение

$$A \sqcup B, \text{ где } A = \{x | x \in \mathbb{Q}, x < a_k \text{ для почти всех } k\}.$$

Данное сопоставление индуцирует взаимно однозначное соответствие между классами фундаментальных последовательностей и сечениями. Тогда операции поля действительных чисел можно определить на множестве сечений. Проделайте это.

ГЛАВА 17

Корни вещественных многочленов

В главе изучаются многочлены с вещественными коэффициентами.

1. Непрерывность и теорема Вейерштрасса

Для любых действительных чисел a, b, таких, что $a < b$, множество

$$(a, b) = \{c | c \in \mathbb{R}, a < c < b\}$$

называется открытым интервалом.

Пусть множество A является объединением открытых интервалов. Иными словами, оно состоит из действительных чисел и вместе с любым своим числом включает целиком некоторый содержащий его интервал.

Пусть также задана функция

$$f : A \to \mathbb{R},$$

для которой множество A является областью определения. Имеет место следующее свойство.

∘ *Для любого элемента a_* из множества A следующие условия равносильны.*

(1) *Для любого положительного ε существует положительное $\delta(\varepsilon)$, такое что для любого элемента a из множества A верно:*

$$|f(a) - f(a_*)| < \varepsilon, \text{ если } |a - a_*| < \delta(\varepsilon).$$

(2) *Для любой последовательности $a_0, a_1, \ldots$ чисел из множества A верно:*

$$f(a_k) \to f(a_*), \text{ если } a_k \to a_* \text{ при } k \to \infty.$$

Доказательство. Докажем необходимые импликации.

(1 → 2) Из первого условия следует второе.

Пусть выполняется первое условие и последовательность a_k сходится к значению a_*. Для любого положительного числа ε почти все члены этой последовательности лежат в интервале $(a_* - \delta(\varepsilon), a_* + \delta(\varepsilon))$; тогда в силу первого условия почти все члены последовательности $f(a_k)$ принадлежат интервалу $(f(a_*) - \varepsilon, f(a_*) + \varepsilon)$; следовательно, последовательность $f(a_k)$ сходится к элементу $f(a_*)$ и выполняется второе условие.

(2 → 1) Из второго условия следует первое.

Предположим, что первое условие не выполняется. Тогда для некоторого ε и любого δ_k найдётся значение a_k, такое, что

$$|f(a_k) - f(a_*)| \geqslant \varepsilon, \text{ и } |a_k - a_*| < \delta_k.$$

Возьмём последовательность δ_k, сходящуюся к нулю при $k \to \infty$. Тогда последовательность a_k сходится к a_*, но последовательность $f(a_k)$ не сходится к $f(a_*)$. Таким образом, второе условие также не выполняется. □

Функция, удовлетворяющая условиям (1,2), называется *непрерывной* в точке a_*. Она называется *непрерывной* (на множестве A), если эти условия выполняются для любого действительного числа a_* из множества A.

Упражнение. Докажите, что сумма и произведение непрерывных функций — непрерывны; композиция непрерывных функций непрерывна на области, где она корректно определена; полиномиальная функция непрерывна.

Имеет место

Теорема Вейерштрасса. *Пусть функция f непрерывна на отрезке $[a_0, a_1]$ и принимает значения разного знака в точках a_0, a_1. Тогда она принимает значение 0 в некоторой точке отрезка.*

Доказательство. Для доказательства достаточно построить фундаментальную последовательность a_k элементов из отрезка $[a_0, a_1]$, где любые два значения $f(a_k), f(a_{k+1})$ разного знака. Тогда для значения $a = \lim_{k\to\infty} a_k$ в силу непрерывности f выполняется равенство $f(a) = 0$. □

2. Корни и степени

Выведем из теоремы Вейерштрасса пару следствий о корнях вещественных многочленов.

Следствие. *Пусть n — целое положительное число. В поле действительных чисел для любого положительного числа a существует единственное положительное число b, такое, что*

$$b^n = a.$$

Число b обычно обозначается как $\sqrt[n]{a}$ и называется (арифметическим) корнем степени n из числа a.

Доказательство. При достаточно большом M многочлен $x^n - a$ принимает значения разного знака на концах интервала $[0, M]$ и тогда имеет корень внутри этого интервала. Двух положительных корней быть не может, так как значения записанного многочлена строго возрастают при положительных значениях аргумента. □

Положим

$$a^{m/n} = (\sqrt[n]{a})^m$$

для произвольного рационального числа m/n, такого, что $n > 0$, а также

$$a^r = \lim_{k\to\infty} a^{r_k}$$

для действительного числа r, являющегося пределом последовательности рациональных чисел r_k.

Упражнение. Проверьте корректность сделанного определения. Проверьте, что для любого вещественного значения a функции

$$\mathbb{R} \to \mathbb{R}, x \mapsto a^x,$$
$$\mathbb{R} \to \mathbb{R}, x \mapsto x^a,$$

непрерывны.

Следствие. *Вещественный многочлен нечётной степени имеет вещественный корень.*

Доказательство. Достаточно доказать следствие для многочлена

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$$

со старшим коэффициентом, равным единице. Пусть

$$M = \max\{1, |a_1| + \ldots + |a_n|\}.$$

Убедимся сначала, что

$$f(s) > 0 \text{ при } s > M,$$
$$(-1)^n f(s) > 0 \text{ при } s < -M.$$

Действительно, при $s > M$:

$$\begin{aligned} f(s) =& s^n + a_1 s^{n-1} + \ldots + a_n s^0 \geqslant s^n - (|a_1 s^{n-1}| + \ldots + |a_n s^0|) \geqslant \\ & s^n - s^{n-1}(|a_1| + \ldots + |a_n|) \geqslant s^n - s^{n-1} M \geqslant s^{n-1}(s - M) > 0. \end{aligned}$$

При $s < -M$:

$$\begin{aligned} (-1)^n f(s) = & \\ & (-1)^n(s^n + a_1 s^{n-1} + \ldots + a_n) \geqslant |s|^n - (|a_1 s^{n-1}| + \ldots + |a_n|) \geqslant \\ & |s|^n - |s|^{n-1}(|a_1| + \ldots + |a_n|) \geqslant |s|^n - |s|^{n-1} M = \\ & |s|^{n-1}(|s| - M) > 0. \end{aligned}$$

Осталось заметить, что при нечётной степени n для любого $s > M$ многочлен $f(x)$ принимает значения противоположных знаков на концах интервала $[-s, s]$. Следовательно, он имеет корень внутри интервала.

3. Локализация корней и последовательность Штурма

Задача локализации корней вещественного многочлена состоит в определении числа его корней, принадлежащих заданному интервалу, а также в выделении интервалов, содержащих единственный корень. Эта задача решается теоремой Штурма.

Набор

$$S = (f_0(x), \ldots, f_s(x))$$

вещественных многочленов называется *последовательностью Штурма* многочлена $f_0(x)$ на интервале $[a, b]$, если выполнены условия.

(1) Многочлен f_s не имеет корней, принадлежащих интервалу $[a, b]$.

(2) Значения $f_0(a), f_0(b)$ отличны от нуля.

(3) Значения $f_{k-1}(c), f_{k+1}(c)$ разного знака, если c — корень многочлена f_k, принадлежащий интервалу $[a, b]$, и $1 \leqslant k \leqslant s-1$. В частности, соседние многочлены последовательности не имеют общих корней в интервале.

(4) Произведение $f_0(x)f_1(x)$ меняет знак с минуса на плюс при возрастании x в интервале $(c-\delta, c+\delta)$ для некоторого положительного δ, если c — корень многочлена $f_0(x)$, принадлежащий интервалу $[a, b]$.

Для произвольного действительного числа c обозначим через $W_S(c)$ число перемен знака после удаления нулевых значений в последовательности

$$f_0(c), \ldots, f_s(c).$$

Имеет место

Теорема Штурма. *Пусть S — последовательность Штурма многочлена $f_0(x)$ на интервале $[a, b]$. Тогда число корней данного многочлена на этом интервале совпадает со значением $W_S(a) - W_S(b)$.*

Доказательство. Пусть корни многочленов последовательности S, упорядоченные по возрастанию, содержатся среди значений $a_1, \ldots, a_n$, где

$$a_1 < \ldots < a_n.$$

Заметим, что значение $W_S(c)$ не изменяется внутри интервалов

$$(-\infty, a_1), (a_1, a_2), \ldots, (a_{n-1}, a_n), (a_n, +\infty),$$

поэтому достаточно доказать теорему в случае, когда интервал $[a, b]$ содержит единственный корень, пусть a_i, некоторого из многочленов

$$f_0(x), \ldots, f_{s-1}(x).$$

Многочлен f_s не участвует в этом перечислении в силу первого условия в определении последовательности Штурма. Пусть $0 \leqslant k \leqslant s-1$. Сделаем последовательно ряд наблюдений.

∘ Если значение a_i не является корнем многочлена $f_k(x)$, то для всех значений c из интервала $[a, b]$ знак величины $f_k(c)$ не меняется.

(Напомним, в интервале содержится единственный корень многочленов последовательности.)

∘ Если значение a_i является корнем многочлена $f_k(x)$ и $k > 0$, то для всех значений c из интервала $[a, b]$ в последовательности

$$f_{k-1}(c), f_k(c), f_{k+1}(c)$$

знаки крайних значений не меняются и противоположные в силу третьего условия в определении. Число перемен знака в этой последовательности не изменяется при различных значениях c.

∘ Тогда оно не изменяется и в последовательности $f_1(c), \ldots, f_s(c)$.

∘ Оно не изменяется также в последовательности $f_0(c), \ldots, f_s(c)$, если значение a_i не является корнем многочлена $f_0(x)$.

∘ Наконец, значения $f_0(a), f_0(b)$ разного знака, если значение a_i является корнем многочлена $f_0(x)$. Это следует из четвёртого условия с учётом третьего условия, гарантирующего, что a_i не является корнем многочлена $f_1(x)$.

Сделанных наблюдений достаточно для доказательства. □

4. Стандартная последовательность Штурма

Имеет место

Теорема. *Набор ненулевых вещественных многочленов*

$$f_0(x), \ldots, f_s(x)$$

является последовательностью Штурма многочлена $f_0(x)$ *на интервале* $[a, b]$, *если выполняются следующие условия*:

(1) *многочлен* $f_0(x)$ *свободен от квадратов;*

(2) $f_0(a)f_0(b) \neq 0$;

(3) $f_1(x) = f_0'(x)$;

(4) $f_{i+1}(x) = -f_i(x) \mod f_{i-1}(x)$ *при* $1 \leqslant i \leqslant s-1$;

(5) $f_s(x) \mod f_{s-1}(x) = 0$.

Доказательство. Многочлен $f_s(x)$ является наибольшим общим делителем многочленов $f_0(x), f_0'(x)$ и является ненулевой константой, так как многочлен $f_0(x)$ свободен от квадратов. Следовательно, для рассматриваемой последовательности многочленов первое условие в определении последовательности Штурма выполняется. Второе условие определения выполняется в силу второго условия теоремы. Далее, если c — корень

многочлена $f_k(x)$ и $k > 0$, то значения $f_{k-1}(c), f_{k+1}(c)$ взаимно противоположные. Они не могут равняться нулю, иначе c является корнем всех многочленов $f_{k-1}(x), \ldots, f_s(x)$, откуда $f_s(c) = 0$ и тогда $f_s(x) = 0$ — противоречие. Таким образом, третье условие определения выполняется. Наконец, пусть c — корень многочлена $f_0(x)$. Тогда

$$\begin{aligned} f_0(x) &= (x-c)q(x), \\ f_1(x) &= f_0'(x) \\ &= q(x) + (x-c)q'(x), \\ f_0(x)f_1(x) &= (x-c)(q(x)^2 + (x-c)q(x)q'(x)) \end{aligned}$$

для некоторого многочлена $q(x)$. Заметим, что значение $x = c$ не является корнем этого многочлена, так как многочлен $f_0(x)$ не имеет кратных корней. Следовательно, при $x = c$ значение многочлена

$$q(x)^2 + (x-c)q(x)q'(x)$$

положительное и это значение остаётся положительным в достаточно малом открытом интервале, содержащем точку $x = c$. В этом интервале при возрастании аргумента значение произведения $f_0(x)f_1(x)$ изменяется с отрицательного на положительное в силу записанного выше равенства. Таким образом, выполняется четвёртое условие определения последовательности Штурма. Теорема доказана. □

ГЛАВА 18

Комплексные числа и кватернионы

В главе изучаются алгебры комплексных чисел и кватернионов.

1. Комплексные числа

Начнём с поля комплексных чисел.

Алгебраическая форма. Поле $\mathbb{C}$ комплексных чисел есть расширение $\mathbb{R}(\mathrm{i})$ поля действительных чисел, полученное присоединением корня i многочлена x^2+1. Этим поле $\mathbb{C}$ определяется однозначно с точностью до изоморфизма, оставляющего на месте действительные числа и переставляющего корни $\pm\mathrm{i}$ многочлена x^2+1. Проведём построение поля $\mathbb{C}$, независимое от описанной ранее конструкции присоединения корня.

Итак, мы хотим расширить поле $\mathbb{R}$, причём в расширении должен присутствовать корень многочленая x^2+1, то есть элемент i, такой, что $\mathrm{i}^2=-1$. Очевидно, расширению должны принадлежать элементы

$$a+\mathrm{i}b,$$

где a,b — произвольные действительные числа. Всякий такой элемент называется *комплексным числом*, а элементы a,b называются его *действительной* и *мнимой* частью. Различным парам a,b соответствуют различные комплексные числа, иначе число i было бы корнем линейного многочлена с действительными коэффициентами. С учётом свойств сложения и умножения в поле, выполняются равенства:

$$(a+\mathrm{i}b)+(c+\mathrm{i}d)=(a+c)+\mathrm{i}(b+d),\,(a+\mathrm{i}d)(c+\mathrm{i}d)=(ac-bd)+\mathrm{i}(ad+bc).$$

С другой стороны, эти равенства можно рассматривать как определения для операций сложения и умножения комплексных чисел; последние тогда образуют коммутативное кольцо с единицей, включающее поле действительных чисел (все необходимые свойства легко проверяются). Осталось проверить обратимость отличных от нуля элементов этого кольца и тогда комплексные числа образуют поле.

Комплексные числа $\alpha=a+\mathrm{i}b$ и $\alpha^*=a-\mathrm{i}b$, отличающиеся знаком мнимой части, называются по отношению друг к другу *сопряжёнными*. Операция сопряжения

$$(\cdot)^*:\mathbb{C}\to\mathbb{C},\alpha\mapsto\alpha^*,$$

является автоморфизмом (изоморфизмом на себя) кольца (в действительности — поля) $\mathbb{C}$, то есть она биективна и обладает свойствами:

$$(\cdot)^* : \alpha + \beta \mapsto \alpha^* + \beta^*, \alpha\beta \mapsto \alpha^*\beta^*.$$

Отображение

$$\mathrm{nr} : \mathbb{C} \to \mathbb{R}_+ \sqcup \{0\}, \alpha \mapsto \alpha\alpha^*,$$

называется (комплексной) *нормой* и обладает свойствами

- $\mathrm{nr}(\alpha) \geqslant 0$;
- $\mathrm{nr}(\alpha) = 0 \Leftrightarrow \alpha = 0$;
- $\mathrm{nr}(\alpha\beta) = \mathrm{nr}(\alpha)\,\mathrm{nr}(\beta)$.

(Здесь α, β — произвольные комплексные числа.)

Из перечисленных свойств видно, что в числовой системе комплексных чисел для любого числа α, отличного от нуля, существует обратное число

$$\alpha^{-1} = \frac{\alpha^*}{\mathrm{nr}(\alpha)}.$$

Упражнение.

- Проверьте свойства сопряжения и нормы.

- Докажите, что комплексное число может быть корнем вещественного многочлена только одновременно с сопряжённым.

- Два действительных числа записаны в виде суммы двух квадратов. Запишите аналогичным образом произведение этих чисел.

Геометрический смысл. Комплексные числа отождествляются с точками плоскости следующим естественным образом:

$$\mathbb{C} \to \mathbb{R}^2, a + \mathrm{i}b \mapsto (a, b).$$

Комплексные числа можно мыслить также как вектора, исходящие из начала координат комплексной плоскости и направленные в соответствующие точки плоскости. Такие вектора складываются по правилу треугольника. Обычно вектора на плоскости рассматривают с точностью до параллельного переноса так, что два вектора считаются равными, если, соединяя отрезками их начала и концы, получаем параллелограмм. При таком рассмотрении, комплексные вектора могут быть приложены к любой точке плоскости, тогда для сложения можно также пользоваться правилом параллелограмма.

Для комплексного числа $\alpha = a + \mathrm{i}b$ длина соответствующего вектора, равная $\sqrt{\mathrm{nr}(\alpha)}$, называется *модулем* и обозначается $|\alpha|$. Комплексное число $\alpha \neq 0$ можно представить тогда в тригонометрической форме как

$$\alpha = |\alpha|(\cos\phi_\alpha + \mathrm{i}\sin\phi_\alpha),$$

где ϕ_α — угол, определённый с точностью до слагаемого, кратного 2π. Этот угол называется *аргументом* комплексного числа α.

Геометрический смысл умножения комплексных чисел проясняет

Теорема. *При умножении отличных от нуля комплексных чисел их модули перемножаются, а аргументы складываются. Иными словами, для комплексных чисел α, β из множества $\mathbb{C} \setminus 0$ положительное действительное число $|\alpha| \cdot |\beta|$ является модулем и действительное число $\phi_\alpha + \phi_\beta$ является аргументом комплексного числа $\alpha\beta$.*

Доказательство. Утверждение о модулях очевидно, а утверждение об аргументах достаточно доказать для чисел с модулем единица.

Обозначим через $S(\alpha, \beta)$ площадь параллелограмма, построенного на векторах α, β, приложенных к одной точке. Условимся, что площадь берётся со знаком «плюс», если параллелограмм находится в секторе, полученном вращением вектора α против часовой стрелки в направлении вектора β на угол, не превосходящий π. В противном случае площадь берётся со знаком «минус». В соответствии с этим площадь равна нулю, если угол между векторами кратен π. Доказательство опирается на

Упражнение. Проверьте последовательно следующие свойства:

- $S(\alpha, \beta) = -S(\beta, \alpha)$;
- $S(c\alpha, \beta) = S(\alpha, c\beta) = cS(\alpha, \beta)$;
- $S(\alpha, \beta + \gamma) = S(\alpha, \beta) + S(\alpha, \gamma)$, $S(\alpha + \beta, \gamma) = S(\alpha, \gamma) + S(\beta, \gamma)$;
- $S(\alpha, \beta) = ad - bc$;
- $S(1\gamma, \mathrm{i}\gamma) = |\gamma|$;
- $S(\alpha\gamma, \beta\gamma) = S(\alpha, \beta)|\gamma|$.

Здесь c — произвольное действительное число, α, β, γ — произвольные комплексные числа, причём $\alpha = a + \mathrm{i}b$, $\beta = c + \mathrm{i}d$.

Далее, для комплексного числа γ с единичной нормой рассмотрим операцию

$$\mu_\gamma : \mathbb{C} \to \mathbb{C}, z \mapsto z\gamma.$$

Это операция сохраняет расстояние между точками комплексной плоскости (проверьте). Она сохраняет площати параллелограммов, как видно из упражнения, и тогда сохраняет углы между векторами. Это означает, что к аргументу каждого комплексного числа z прибавляется некоторая величина, зависящая от γ. Эта величина равна аргументу числа γ, что легко проверить, взяв $z = 1$. □

Замечание. Геометрические понятия площади и угла между векторами не были изначально точно определены в доказательстве. Вместе

с тем, проанализировав приведённое рассуждение, эти понятия можно уточнить и придать им абсолютно строгий вид.

Упражнение. Для комплексных чисел α, β и целого положительного числа n докажите следующие формулы.

- $\alpha\beta = |\alpha||\beta|(\cos(\phi_\alpha + \phi_\beta) + \mathrm{i}\sin(\phi_\alpha + \phi_\beta))$.
- (Формула Муавра) $\alpha^n = |\alpha|^n(\cos(n\phi_\alpha) + \mathrm{i}\sin(n\phi_\alpha))$.

Упражнение. Докажите следующие тригонометрические формулы.

- Формулы косинуса и синуса суммы двух углов:

$$\begin{aligned}\cos(\alpha+\beta) &= \cos(\alpha)\cos(\alpha) - \sin(\alpha)\sin(\alpha);\\ \sin(\alpha+\beta) &= \cos(\alpha)\sin(\alpha) + \sin(\alpha)\cos(\alpha)\end{aligned}$$

- Формулы косинуса и синуса кратного угла:

$$\begin{aligned}\cos(n\phi) &= \sum_{k=0}^{k=\lfloor n/2\rfloor} (-1)^k \binom{n}{2k} (\cos\phi)^{n-2k}(\sin\phi)^{2k},\\ \sin(n\phi) &= \sum_{k=0}^{k=\lfloor n/2\rfloor} (-1)^k \binom{n}{2k+1} (\cos\phi)^{n-2k-1}(\sin\phi)^{2k+1}.\end{aligned}$$

Извлечение корней. Отметим ряд свойств, связанных с извлечением корней и решением алгебраических уравнений в поле комплексных чисел. Комплексное число β называется корнем степени n из комплексного числа α, если имеет место равенство

$$\alpha = \beta^n.$$

- *Для любого целого положительного числа n из любого отличного от нуля комплексного числа извлекается n различных комплексных корней степени n.*

Доказательство. Действительно, различными корнями степени n из комплексного числа α являются значения

$$\sqrt[n]{|\alpha|}\Big(\cos\Big(\frac{\phi_\alpha + 2\pi k}{n}\Big) + \mathrm{i}\sin\Big(\frac{\phi_\alpha + 2\pi k}{n}\Big)\Big),\ \text{где } 0 \leqslant k \leqslant n-1.\ \square$$

Обратим внимание, что эти значения получаются из любого одного корня умножением на различные корни степени n из единицы, равные

$$\cos\Big(\frac{2\pi k}{n}\Big) + \mathrm{i}\sin\Big(\frac{2\pi k}{n}\Big),\ \text{где } 0 \leqslant k \leqslant n-1.$$

- *Формулы для квадратных корней.*

Получим выражения для квадратных корней в алгебраической форме.

Пусть $\alpha = a + \mathrm{i}b$, $\beta = c + \mathrm{i}d$, $\alpha = \beta^2$. Тогда последовательно получаем

$$c^2 - d^2 = a, b = 2cd;$$
$$(c^2 + d^2)^2 = a^2 + b^2;$$
$$c^2 + d^2 = \sqrt{a^2 + b^2}.$$

Отсюда, используя первое и последнее равенства, можно записать

$$c = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}, d = \pm\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}.$$

Эти формулы можно использовать для нахождения корней. Действительно, выражения под корнем неотрицательное в обоих случаях, так что записанные арифметические значения корней существуют. Знаки следует выбрать так, чтобы выполнялось равенство $b = 2cd$. □

Упражнение. Убедитесь, что знаки здесь всегда удаётся подобрать.

∘ *В поле комплексных чисел многочлен второй степени имеет корень.*

Доказательство. Это достаточно проверить для многочлена z^2+pz+q со старшим коэффициентом, равным единице. Для этого запишем его следующим образом:

$$z^2 + pz + q = \left(z + \frac{p}{2}\right)^2 - \left(\frac{p^2}{4} - q\right).$$

Видно, что корнями многочлена являются комплексные числа

$$\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}. \ \square$$

В действтительности, имеет место

Теорема. *В поле комплексных чисел многочлен положительной степени имеет корень.* □

По историческим причинам записанную теорему принято называть «основный теоремой Алгебры». Она будет доказано позднее.

Корни из единицы. Пусть n — целое положительное число. Элемент a коммутативного кольца с единицей называется *корнем степени n из единицы*, если он удовлетворяет соотношению $a^n = 1$. Такие элементы образуют относительно операции умножения группу, обозначим её через $\mathrm{T}_n(K)$. В поле комплексных чисел имеется ровно n различных корней из единицы степени n, именно $\varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{n-1}$, где

$$\varepsilon_n = \cos\left(\frac{2\pi}{n}\right) + \mathrm{i}\sin\left(\frac{2\pi}{n}\right) \text{ и}$$
$$\varepsilon_n^k = \cos\left(\frac{2\pi k}{n}\right) + \mathrm{i}\sin\left(\frac{2\pi k}{n}\right), \text{ для любого } k \in \mathbb{Z}.$$

Их умножение подчиняется следующим закону:

$$\varepsilon_n^k \varepsilon_n^l = \varepsilon_n^{(k+l) \bmod n},$$

таким образом, имеется изоморфизм групп

$$\mathrm{T}_n(\mathbb{C}) \to \mathbb{Z}/n\mathbb{Z}, \varepsilon_n^k \mapsto k + n\mathbb{Z}.$$

Отметим, что корни из единицы являются степенями одного из них; например, ε_n обладает таким свойством. Корень с таким свойством называется *первообразным*.

Упражнение. Проверьте, что корень ε_n^k тогда и только тогда первообразный, когда числа k, n — взаимно простые. В частности, в поле комплексных чисел имеется ровно $\varphi(n)$ первообразных корней степени n из единицы.

2. Основная теорема Алгебры

Поле называется *алгебраически замкнутым*, если всякий многочлен положительной степени с коэффициентами в этом поле имеет в нём корень, и тогда многочлены положительной степени разлагаются над этим полем на линейные множители. Имеет место

Основная теорема Алгебры. *Поле* $\mathbb{C}$ *алгебраически замкнуто.*

Доказательство теоремы разбито на части с номерами 1, 2, 3, 3.1, 3.2, 4. Проверим сначала выполнение следующего условия.

(1) *В любом расширении поля комплексных чисел всякий корень* γ *комплексного многочлена* $f(x)$ *является одновременно корнем некоторого вещественного многочлена.*

Это достаточно доказать для многочлена $f(x)$, неприводимого над полем $\mathbb{C}$. Пусть n — его степень. В этом случае расширение $\mathbb{C}(\gamma)$ является векторным пространством разметрности n над полем $\mathbb{C}$ с базисом

$$\gamma^0, \gamma^1, \ldots, \gamma^{n-1}$$

и векторным пространством над полем $\mathbb{R}$ размерности $2n$ с базисом

$$\gamma^0, \gamma^1, \ldots, \gamma^{n-1}, \mathrm{i}\gamma^0, \mathrm{i}\gamma^1, \ldots, \mathrm{i}\gamma^{n-1}.$$

В силу сказанного, набор элементов

$$\gamma^0, \gamma^1, \ldots, \gamma^{2n}$$

линейно зависим над полем $\mathbb{R}$. Отсюда следует, что элемент γ является корнем вещественного многочлена степени, не превосходящей $2n$.

Далее проверим выполнение следующего условия.

(2) *Предположим, каждый вещественный многочлен положительной степени имеет комплексный корень. Тогда каждый такой многочлен разлагается над полем комплексных чисел на линейные множители.*

Действительно, пусть γ — комплексный корень вещественного многочлена $f(x)$. Тогда в кольце $\mathbb{R}[x]$ выполняется альтернатива

$$(x-\gamma)|f(x) \text{ либо } (x-\gamma)(x-\gamma^*)|f(x).$$

Далее нужно воспользоваться индукцией по степени многочлена.

Теперь для доказательства теоремы достаточно проверить следующее.

(3) *Вещественный многочлен положительной степени имеет комплексный корень.*

Поскольку неприводимые многочлены над полем нулевой характеристики не имеют кратных корней, достаточно доказать это для вещественного многочлена $f(x)$ без кратных корней. Пусть $n = 2^q m$ — степень этого многочлена, где $2 \nmid m$. Сформулированное утверждение будем доказывать индукцией по q. Степень нечётная при $q = 0$, в этом случае утверждение доказано ранее. Предположим, $q > 0$ и утверждение верно для меньших значений q. Присоединим к полю $\mathbb{C}$ корни $\alpha_1, \ldots, \alpha_n$ многочлена $f(x)$. Выберем действительное число c так, чтобы значения

$$\alpha_i\alpha_j + c(\alpha_k + \alpha_l), 1 \leqslant i < j \leqslant n, 1 \leqslant k < l \leqslant n,$$

отвечающие различным значениям $\alpha_k + \alpha_l$, были различными. Это возможно, так как поле $\mathbb{C}(\alpha_1, \ldots, \alpha_n)$ бесконечное.

В продолжение доказательства убедимся в следующем.

(3.1.) *Полю комплексных чисел принадлежит некоторая комбинация*

$$\beta_{ij} = \alpha_i\alpha_j + c(\alpha_i + \alpha_j), \text{ где } \leqslant i < j \leqslant n.$$

Рассмотрим многочлен

$$g(x) = \prod_{\{i,j\}} (x - \beta_{ij}), \text{ где } 1 \leqslant i < j \leqslant n.$$

Он имеет степень, равную

$$\binom{n}{2} = 2^{q-1}m(2^q m - 1),$$

а также действительные коэффициенты. В самом деле, коэффициенты многочлена $g(x)$ выражаются посредством вещественных симметрических многочленов через корни многочлена $f(x)$ и тогда выражаются посредством вещественных многочленов через коэффициенты многочлена $f(x)$; таким образом, коэффициенты многочлена $g(x)$ действительные вслед за коэффициентами многочлена $f(x)$.

Учитывая значение степени многочлена $g(x)$, по предположению индукции заключаем, что некоторый его корень, пусть β_{12}, — комплексный и тогда $\mathbb{R}(\beta_{12}) \subseteq \mathbb{C}$.

Далее проверим следующее.

(3.2) *Значения $\alpha_1\alpha_2, \alpha_1 + \alpha_2$ принадлежат полю $\mathbb{R}(\beta_{12})$.*

Этого будет достаточно для завершения доказательства условия (3), так как тогда многочлен

$$(x - \alpha_1)(x - \alpha_2).$$

имеет комплексные коэффициенты. В этом случае его корни α_1, α_2 также комплексные. (Ранее доказано, что корни комплексного многочлена второй степени — комплексные.) Заметим в связи с этим, что многочлен

$$\prod_{\{i,j\}} (x - (\alpha_i + \alpha_j)), \text{ где } 1 \leqslant i < j \leqslant n.$$

имеет вещественные коэффициенты (почему это так?). Следовательно, некоторый его неприводимый над $\mathbb{R}$ делитель $s(x)$ имеет корень, равный $\alpha_1 + \alpha_2$ и остальные корни вида $\alpha_i + \alpha_j$. Аналогично, существует неприводимый над $\mathbb{R}$ многочлен $p(x)$ с корнями вида $\alpha_i\alpha_j$ и корнем $\alpha_1\alpha_2$. Значение $\alpha_1 + \alpha_2$ является общим корнем многочленов $s(x)$ и $p(\beta_{12} - cx)$, причём единственным общим корнем в силу выбора c. Тогда

$$\gcd(s(x), p(\beta_{12} - cx)) = x - (\alpha_1 + \alpha_2).$$

Отсюда видно, что значение $\alpha_1 + \alpha_2$ содержится в поле $\mathbb{R}(\beta_{12})$. Но тогда величина $\alpha_1\alpha_2 = \beta_{12} - c(\alpha_1 + \alpha_2)$ также принадлежит этому полю.

Теперь можно завершить доказательство.

(4) *Поле комплексных чисел алгебраически замкнуто.*

В соответствии с третьим условием вещественный многочлен положительной степени имеют комплексный корень, откуда в силу второго условия он разлагается на линейные множители и тогда с учётом первого условия комплексный многочлен имеет комплексный корень. Теорема доказана. □

Упражнение. Докажите, следующие утверждения.

∘ Неприводимый вещественный многочлен имеет первую или вторую степень.

∘ Поле комплексных чисел получается присоединением к полю действительных чисел корня любого неприводимого многочлена второй степени.

3. Кватернионы

Естественным, но не очевидным, обобщением комплексных чисел являются кватернионы, рассматриваемые далее.

Алгебра кватернионов. Алгеброй кватернионов называется четырёхмерная алгебра с единицей над полем действительных чисел с базисом

$$1, \mathrm{i}, \mathrm{j}, \mathrm{k},$$

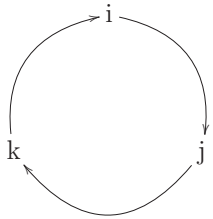
где выполняются соотношения

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1,$$

а также соотношения

$$\begin{aligned} \mathrm{ij} &= \mathrm{k}, \;\; \mathrm{ji} = -\mathrm{k}, \\ \mathrm{jk} &= \mathrm{i}, \;\; \mathrm{kj} = -\mathrm{i}, \\ \mathrm{ki} &= \mathrm{j}, \;\; \mathrm{ik} = -\mathrm{j}, \end{aligned}$$

которые можно проиллюстрировать диаграммой



Алгебра кватернионов обозначается буквой $\mathbb{H}$, её элементы называются *кватернионами*. Из определения следует, что умножение кватернионов ассоциативно и некоммутативно. Кватернионы $\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}$ с операцией умножения образуют восьмиэлементную группу, которая называется *группой кватернионов*.

Для кватерниона $\alpha = 1\alpha_1 + \mathrm{i}\alpha_\mathrm{i} + \mathrm{j}\alpha_\mathrm{j} + \mathrm{k}\alpha_\mathrm{k}$ действительное число α_1 называется *действительной* или *скалярной* частью, а кватернион

$$\overrightarrow{\alpha} = \mathrm{i}\alpha_\mathrm{i} + \mathrm{j}\alpha_\mathrm{j} + \mathrm{k}\alpha_\mathrm{k}$$

без скалярной части называется его *мнимой* или *векторной* частью.

Кватернионы α, α^*, которые отличаются знаком мнимой части, называются *сопряжёнными*. Отображение

$$(\cdot)^* : \mathbb{H} \to \mathbb{H}, \alpha \mapsto \alpha^*,$$

называется *сопряжением*. Оно обладает свойствами:

$$\alpha + \beta \mapsto \alpha^* + \beta^*, \alpha\beta \mapsto \beta^*\alpha^*.$$

Отображение

$$\mathrm{nr} : \mathbb{H} \to \mathbb{R}_+ \sqcup \{0\}, \alpha \mapsto \alpha\alpha^*,$$

называется *нормой* и обладает следующими свойствами, аналогичными свойствам комплексной нормы:

- $\mathrm{nr}(\alpha) \geqslant 0$;
- $\mathrm{nr}(\alpha) = 0 \Leftrightarrow \alpha = 0$;
- $\mathrm{nr}(\alpha\beta) = \mathrm{nr}(\alpha)\,\mathrm{nr}(\beta)$.

(Здесь q, r — произвольные кватернионы.) Отображение

$$|\cdot| : \mathbb{H} \to \mathbb{R}_+ \sqcup \{0\}, \alpha \mapsto |\alpha|, \text{ где } |\alpha| = \sqrt{\mathrm{nr}(\alpha)},$$

называется *модулем*.

Из перечисленных свойств видно, что для любого кватерниона α, отличного от нуля, существует обратный кватернион

$$\alpha^{-1} = \frac{\alpha^*}{\mathrm{nr}(\alpha)}.$$

Упражнение.

- Проверьте свойства сопряжения и нормы для кватернионов.
- Два действительных числа записаны в виде суммы четырёх квадратов. Запишите аналогичным образом произведение этих чисел. Тождество, которое здесь получается, называется *тождеством Эйлера* для четырёх квадратов.

Теорема Фробениуса. Алгебра с единицей, отличной от нуля, где каждый ненулевой элемент обратим, называется *алгеброй с делением*. Имеет место

Теорема (Фробениус). *Конечномерная ассоциативная алгебра с делением над полем действительных чисел изоморфна одной из следующих:*

$$\mathbb{R}, \mathbb{C}, \mathbb{H}.$$

Доказательство. Пусть A — конечномерная алгебра с делением над полем действительных чисел. Поскольку она содержит единицу, будем считать далее, что поле $\mathbb{R}$ содержится в её центре.

Заметим также, что для любых элементов $\alpha, \beta, \ldots$ среди алгебр, содержащихся в A (такие алгебры называются подалгебрами алгебры A) и содержащих указанные элементы, имеется наименьшая по включению. Она совпадает с пересечение всех таких алгебр, обозначается $\langle \alpha, \beta, \ldots \rangle$ и называется (под)алгеброй, *порождённой* элементами $\alpha, \beta, \ldots$.

Дальнейшие рассуждения разобьём на три части.

(1) *Пусть $\alpha \in A \backslash \mathbb{R}$. Тогда имеет место изоморфизм алгебр $\langle \alpha \rangle \simeq \mathbb{C}$.*

Пусть n — размерность алгебры $\langle\alpha\rangle$. Элементы $1, \alpha, \ldots, \alpha^n$ линейно зависимы над полем $\mathbb{R}$, так что существует ненулевой вещественный многочлен с корнем α. Нормированный такой многочлен минимальной возможной степени называется минимальным многочленом элемента α. Минимальный многочлен имеет степень, равную n. Он неприводим над полем $\mathbb{R}$ и, тогда, $n = 2$. Не сложно увидить далее, что алгебра $\langle\alpha\rangle$ совпадает с алгеброй $\mathbb{R}[\alpha]$, состоящей из значений вещественных многочленов, вычисленных в точке α. (Проверьте перечисленные свойства.) Обозначим через α' комплексный корень минимального многочлена. Для завершения доказательства первой части осталось заметить, что имеет место следующий изоморфизм алгебр:

$$\langle\alpha\rangle \to \mathbb{C}, a + b\alpha \mapsto a + b\alpha',$$

(где a, b — произвольные действительные числа). Записанное отображение определено корректно и является изоморфизмом, так как в алгебрах $\langle\alpha\rangle$ и $\mathbb{C}$ базисные элементы $1, \alpha$ и $1, \alpha'$, соответствующие друг другу при этом отображении, перемножаются сходным образом (как именно?).

(2) *Пусть* $\alpha \in A \setminus \mathbb{R}$ *и* $\beta \in A \setminus \langle\alpha\rangle$. *Тогда* $\langle\alpha, \beta\rangle \simeq \mathbb{H}$.

Пусть $1, i$ и $1, i'$ — базисы алгебр $\langle\alpha\rangle$ и $\langle\beta\rangle$, такие, что $i^2 = i'^2 = -1$. Проверим последовательно, что значения

$$\mu = \frac{ii' + i'i}{2}, \nu = \frac{1}{\sqrt{1 - \mu^2}}$$

действительные и для элементов

$$j = \mu\nu i + \nu i', k = ij,$$

отображение

$$\mathbb{H} \to \langle\alpha, \beta\rangle, a + \mathrm{i}b + \mathrm{j}c + \mathrm{k}d \mapsto a + ib + jc + kd$$

является изоморфизмом алгебр. Пусть

$$m_+(x) = x^2 - b_+x - a_+, m_-(x) = x^2 - b_-x - a_-,$$

— минимальные многочлены элементов $i \pm i'$ над полем действительных чисел. Тогда верны соотношения

$$\begin{aligned}(i \pm i')^2 &= -2 \pm (ii' + i'i) \\ &= b_\pm(i \pm i') - a_\pm,\end{aligned}$$

откуда сложением получаем

$$-4 = (b_+ + b_-)i + (b_+ - b_-)i' + (a_+ + a_-).$$

Поскольку элементы $1, i, i'$ линейно независимы над $\mathbb{R}$, верны равенства

$$b_+ \pm b_- = 0, b_+ = b_- = 0.$$

Следовательно, величина μ действительная. Так как многочлены $m_{\pm}(x) = x^2 - a_{\pm}$ неприводимы над полем действительных чисел, величины $a_{\pm}$ отрицательные и из записанных соотношений получаем неравенства

$$-2 < -(2 + a_-) = ii' + i'i = 2 + a_+ < 2.$$

Отсюда $|\mu| < 1$ и величина ν является действительным числом.

Далее, элементы $1, i, j$ линейно независимы, так как $\nu \neq 0$. Элементы $1, i, j, k$ также линейно независимы. Иначе выполняется соотношение

$$k = a + ib + jc$$

для некоторых действительных значений a, b, c, тогда

$$\begin{aligned} j &= ki \\ &= ia - b - kc \\ &= ia - b - (a + ib + cj)c \\ &= -(b + ca) + (a - cb)i - c^2 j, \end{aligned}$$

откуда $1 = -c^2$, получили противоречие. Таким образом, записанное отображение является изоморфизмом векторных пространств. Для завершения второй части доказательства достаточно проверить следующее:

$$\begin{aligned} j^2 = -1, ij + ji = 0, \\ k^2 = -1, ik + jk = 0. \end{aligned}$$

Пропустим эту часть доказательства.

(3) *Пусть* $\alpha \in A \setminus \mathbb{R}$ *и* $\beta \in A \setminus \langle \alpha \rangle$. *Тогда* $\langle \alpha, \beta \rangle = A$.

В силу установленного изоморфизма будем считать, что $\langle \alpha, \beta \rangle = \mathbb{H}$ и будем использовать для элементов этой алгебры стандартные обозначения, установленные ранее. Предположим, равенство $\langle \alpha, \beta \rangle = A$ не выполняется. Для элемента γ из множества $A \setminus \langle \alpha, \beta \rangle$ в алгебре $\langle \gamma \rangle$ выберем базис $1, i'$, где $i'^2 = -1$. Рассуждая как в доказательстве предыдущей части, убеждаемся, что значения

$$\rho_{\mathrm{i}} = \mathrm{i}i' + i'\mathrm{i}, \rho_{\mathrm{j}} = \mathrm{j}i' + i'\mathrm{j}, \rho_{\mathrm{k}} = \mathrm{k}i' + i'\mathrm{k}$$

действительные. Тогда

$$\begin{aligned} i'\mathrm{k} = i'(\mathrm{ij}) &= (i'\mathrm{i})\mathrm{j} = (\rho_{\mathrm{i}} - \mathrm{i}i')\mathrm{j} \\ &= \rho_{\mathrm{i}}\mathrm{j} - (\mathrm{i}i')\mathrm{j} = \rho_{\mathrm{i}}\mathrm{j} - \mathrm{i}(i'\mathrm{j}) \\ &= \rho_{\mathrm{i}}\mathrm{j} - \mathrm{i}(\rho_{\mathrm{j}} - \mathrm{j}i') = \rho_{\mathrm{i}}\mathrm{j} - \rho_{\mathrm{j}}\mathrm{i} + \mathrm{k}i' \\ &= \rho_{\mathrm{i}}\mathrm{j} - \rho_{\mathrm{j}}\mathrm{i} + \rho_{\mathrm{k}} - i'\mathrm{k}, \text{ и} \\ 2i'\mathrm{k} &= \rho_{\mathrm{i}}\mathrm{j} - \rho_{\mathrm{j}}\mathrm{i} + \rho_{\mathrm{k}}, \text{ откуда правым умножением на k получаем} \\ -2i' &= \rho_{\mathrm{i}}\mathrm{i} + \rho_{\mathrm{j}}\mathrm{j} + \rho_{\mathrm{k}}\mathrm{k}. \end{aligned}$$

Следовательно, элементы i', γ принадлежат подалгебре $\langle \alpha, \beta \rangle$. Полученное противоречие завершает доказательство третьей части.

Теорема полностью доказана. $\square$

Геометрическая интерпретация. Кватернионы находят применение для описания вращений пространства. Рассмотрим, как это делается. Отождествим кватернионы без скалярной части с точками пространства $\mathbb{R}^3$ посредством следующего отображения

$$\mathbb{R}^3 \to \mathbb{H}, (\alpha_\mathrm{i}, \alpha_\mathrm{j}, \alpha_\mathrm{k}) \mapsto \mathrm{i}\alpha_\mathrm{i} + \mathrm{j}\alpha_\mathrm{j} + \mathrm{k}\alpha_\mathrm{k},$$

являющегося изоморфным вложением векторных пространств над полем $\mathbb{R}$. В свою очередь точки пространства (и тогда соответствующие им кватернионы) отождествим с направленными в них векторами, исходящими из начала координат.

Пусть γ — кватернион с единичной нормой, такой, что $\mathrm{nr}(\gamma) = 1$. Отметим следующие свойства.

$\circ$ *Существует действительное число θ и вектор (кватернион без скалярной части) γ', удовлетворяющие равенству*

$$\gamma = \cos\left(\frac{\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right)\gamma'.$$

Доказательство. По условию

$$1 = \mathrm{nr}(\gamma) = \gamma_1^2 + |\overrightarrow{\gamma}|^2.$$

Следовательно, существует действительное число θ, такое, что

$$\cos\left(\frac{\theta}{2}\right) = \gamma_1, \sin\left(\frac{\theta}{2}\right) = |\overrightarrow{\gamma}|.$$

Следует взять $\gamma' = 0$, если $|\overrightarrow{\gamma}| = 0$; в противном случае положим

$$\gamma' = \overrightarrow{\gamma}/|\overrightarrow{\gamma}|. \square$$

Замечание. Существует две возможности выбрать ненулевой вектор γ' так, чтобы выполнялось записанное равенство, именно $\gamma' = \pm\overrightarrow{\gamma}/|\overrightarrow{\gamma}|$. Отметим, что тогда выполняются равенства

$$\cos\left(\frac{\theta}{2}\right) = \gamma_1, \sin\left(\frac{\theta}{2}\right) = \pm|\overrightarrow{\gamma}|.$$

$\circ$ *Пусть для числа θ и вектора γ' верно равенство*

$$\gamma = \cos\left(\frac{\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right)\gamma'.$$

Тогда отображение

$$\mathrm{I}_\gamma : \mathbb{R}^3 \to \mathbb{R}^3, \alpha \mapsto \gamma\alpha\gamma^{-1}$$

осуществляет поворот простанства $\mathbb{R}^3$ на угол θ вокруг вектора γ'.

Схема доказательства. Тройке векторов α, β, δ сопоставим действительное значение, равное объему параллелепипеда, образованного этими векторами. Объём договоримся учитывать со знаком «плюс», если внутри параллелепипеда вращение от вектора α к вектору β осуществляется против часовой стрелки. В противном случае будем учитывать его со знаком «минус». Далее следует убедиться, что записанное отображение сохраняет расстояния между точками пространства и объёмы параллелепипедов, учитываемые со знаком. Это означает, что рассматриваемое отображение является вращением пространства. Далее проверяется, что вектор γ' отображается на кратный вектор и, следовательно, лежит на оси вращения. Остаётся проверить, что угол вращения равен θ. Для этого следует подействовать рассматриваемым отображением на какой-нибудь вектор, ортогональный γ'. Детали этого рассуждения можно уточнить на основе упражнений, приведённых ниже. □

∘ *Кватернионы γ, δ с единичной нормой тогда и только тогда осуществляют один и тот же поворот пространства описанным выше способом, когда они совпадают с точностью до знака. Иными словами, верна равносильность*

$$\mathrm{I}_\gamma = \mathrm{I}_\delta \Leftrightarrow \gamma = \pm\delta.$$

Доказательство. Запишем кватернионы γ, δ следующим образом:

$$\gamma = \cos\left(\frac{\theta_\gamma}{2}\right) + \sin\left(\frac{\theta_\gamma}{2}\right)\gamma',$$
$$\delta = \cos\left(\frac{\theta_\delta}{2}\right) + \sin\left(\frac{\theta_\delta}{2}\right)\delta',$$

где

$$\gamma' = \overrightarrow{\gamma}/|\overrightarrow{\gamma}|, \sin\left(\frac{\theta_\gamma}{2}\right) = \overrightarrow{\gamma},$$
$$\delta' = \overrightarrow{\delta}/|\overrightarrow{\delta}|, \sin\left(\frac{\theta_\delta}{2}\right) = \overrightarrow{\delta}.$$

Если кватернионы γ, δ противоположные, то и вектора $\overrightarrow{\gamma}, \overrightarrow{\delta}$ тоже противоположные, как и значения $\cos(\theta_\gamma/2), \cos(\theta_\delta/2)$, а значения $\sin(\theta_\gamma/2), \sin(\theta_\delta/2)$ совпадают. Тогда углы $\theta_\gamma, \theta_\delta$ (измеряемые с точностью до слагаемого, кратного 2π) также противоположные. Таким образом, кватернионы γ, δ осуществляют вращения на противоположные углы относительно противположных векторов. Такие вращения совпадают. Достаточность доказана. Обратно, предположим, что вращения $\mathrm{I}_\gamma, \mathrm{I}_\delta$ совпадают. Так как вектора γ', δ' лежат на оси вращения и имеют единичную норму, они совпадают с точностью до знака. Если эти вектора

совпадают, то и углы $\theta_\gamma, \theta_\delta$ совпадают. В противном случае, эти углы противоположные. В обоих случаях кватернионы γ, δ совпадают. $\square$

Точный смысл геометрических понятий, встречающихся в формулировках и доказательствах записанных свойств, проясняют упражнения ниже.

Упражнение (скалярное произведение). Отображение

$$\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}_+ \sqcup \{0\}, (\alpha, \beta) \mapsto \alpha \cdot \beta,$$

где

$$\alpha \cdot \beta = \alpha_{\mathrm{i}}\beta_{\mathrm{i}} + \alpha_{\mathrm{j}}\beta_{\mathrm{j}} + \alpha_{\mathrm{k}}\beta_{\mathrm{k}},$$

называется скалярным произведением. (Чтобы не возникало путаницы, договоримся всегда писать точку для скалярного произведения, а обычное произведение кватернионов записывать без точки.) Проверьте следующие свойства.

∘ Скалярное произведение не изменяется при перестановке аргументов.

∘ Скалярное произведение линейно над $\mathbb{R}$ по каждому аргументу.

∘ Для любых векторов α, β найдётся единственное значение $\varphi(\alpha, \beta)$, принадлежащее отрезку $[0, \pi]$, такое, что

$$\alpha \cdot \beta = |\alpha||\beta| \cos \varphi(\alpha, \beta).$$

Это значение называется *углом* между векторами α, β.

∘ Убедитесь, что сделанное определение согласуется с обычным пониманием угла между векторами.

Упражнение (векторное произведение). Отображение

$$\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3, (\alpha, \beta) \mapsto \alpha \times \beta,$$

где

$$\begin{aligned}\alpha \times \beta &= \det \begin{pmatrix} \mathrm{i} & \mathrm{j} & \mathrm{k} \\ \alpha_{\mathrm{i}} & \alpha_{\mathrm{j}} & \alpha_{\mathrm{k}} \\ \beta_{\mathrm{i}} & \beta_{\mathrm{j}} & \beta_{\mathrm{k}} \end{pmatrix} \\ &= \mathrm{i} \det \begin{pmatrix} \alpha_{\mathrm{j}} & \alpha_{\mathrm{k}} \\ \beta_{\mathrm{j}} & \beta_{\mathrm{k}} \end{pmatrix} - \mathrm{j} \det \begin{pmatrix} \alpha_{\mathrm{i}} & \alpha_{\mathrm{k}} \\ \beta_{\mathrm{i}} & \beta_{\mathrm{k}} \end{pmatrix} + \mathrm{k} \det \begin{pmatrix} \alpha_{\mathrm{i}} & \alpha_{\mathrm{j}} \\ \beta_{\mathrm{i}} & \beta_{\mathrm{j}} \end{pmatrix}.\end{aligned}$$

называется векторным произведением. Проверьте следующие свойства.

∘ Векторное произведение меняет знак при перестановке аргументов.

∘ Векторное произведение линейно над $\mathbb{R}$ по каждому аргументу.

∘ Для любых векторов α, β верно равенство

$$|\alpha \times \beta| = |\alpha||\beta| \sin \varphi(\alpha, \beta),$$

где $\varphi(\alpha, \beta)$ — угол между векторами α, β.

∘ Эта величина совпадает с площадью параллелограмма, построенного на векторах α, β.

∘ Выясните, чем определяется знак векторного произведения.

∘ Для любых векторов α, β выполняются *тождества*:

$$\alpha\beta = \alpha \times \beta - \alpha \cdot \beta,$$
$$\alpha \cdot \beta = -\frac{1}{2}(\alpha\beta + \beta\alpha),$$
$$\alpha \times \beta = \frac{1}{2}(\alpha\beta - \beta\alpha).$$

∘ Для любых векторов α, β, γ выполняется *тождество Якоби*:

$$(\alpha \times \beta) \times \gamma + (\beta \times \gamma) \times \alpha + (\gamma \times \alpha) \times \beta = 0.$$

Упражнение (Смешанное произведение). Отображение

$$\mathbb{R}^3 \times \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}_+ \sqcup \{0\}, (\alpha, \beta, \gamma) \mapsto \alpha \cdot (\beta \times \gamma),$$

называется *смешанным произведением*. Проверьте, что

$$\begin{aligned}\alpha \cdot (\beta \times \gamma) &= \det \begin{pmatrix} \alpha_{\mathrm{i}} & \alpha_{\mathrm{j}} & \alpha_{\mathrm{k}} \\ \beta_{\mathrm{i}} & \beta_{\mathrm{j}} & \beta_{\mathrm{k}} \\ \gamma_{\mathrm{i}} & \gamma_{\mathrm{j}} & \gamma_{\mathrm{k}} \end{pmatrix} \\ &= \alpha_{\mathrm{i}} \det \begin{pmatrix} \beta_{\mathrm{j}} & \beta_{\mathrm{k}} \\ \gamma_{\mathrm{j}} & \gamma_{\mathrm{k}} \end{pmatrix} - \alpha_{\mathrm{j}} \det \begin{pmatrix} \beta_{\mathrm{i}} & \beta_{\mathrm{k}} \\ \gamma_{\mathrm{i}} & \gamma_{\mathrm{k}} \end{pmatrix} + \alpha_{\mathrm{k}} \det \begin{pmatrix} \beta_{\mathrm{i}} & \beta_{\mathrm{j}} \\ \gamma_{\mathrm{i}} & \gamma_{\mathrm{j}} \end{pmatrix}.\end{aligned}$$

ГЛАВА 19

Метрические и нормированные пространства

В этой главе изучаются метрические пространства, нормированные кольца и векторные пространства.

1. Метрические пространства

Введём в рассмотрение основные конструкции, связанные с метрическими и нормированными пространствами.

Метрика. Пусть X — множество. Функция

$$d : X^2 \to \mathbb{R}_+ \sqcup \{0\}$$

называется *метрикой* или *расстоянием*, а множество X, рассматриваемое вместе с этой функцией, называется *метрическим пространством*, если для любых его элементов x, y, z выполняются следующие условия:

(1) $d(x, y) = 0 \Leftrightarrow x = y$;

(2) $d(x, y) = d(y, x)$;

(3) $d(x, z) \leqslant d(x, y) + d(y, z)$.

Замечание. Из определения сразу следует ещё одно свойство

(4) $d(x, z) \geqslant d(x, y) - d(y, z)$.

Метрика называется *неархимедовой*, если вместо третьего условия выполняется более сильное условие

(3') $d(x, z) \leqslant \max\{d(x, y), d(y, z)\}$.

Метрическое пространство на множестве X с метрикой d обозначается (X, d). *Изометрией* между метрическими пространствами (X, d), (X^*, d^*) называется биекция

$$X \to X^*, x \mapsto x^*,$$

сохраняющая расстояния между точками, то есть обладающая свойством

$$d(x, y) = d^*(x^*, y^*) \text{ для любых } x, y \text{ из } X.$$

Естественно рассматривать метрические пространства с точностью до изометрии.

Примеры.

∘ Для действительных чисел определена метрика

$$\mathrm{r} : \mathbb{R} \to \mathbb{R}_+ \sqcup \{0\}, (x, y) \mapsto |x - y|.$$

∘ Подпространство. Метрика, определённая в множестве X, индуцирует метрику с теми же значениями на любом подмножестве $Y \subseteq X$. Подмножество, рассматриваемое с индуцированной метрикой, называется *подпространством* метрического пространства.

∘ Произведения. Пусть $(X_1, d), \ldots, (X_n, d)$ — метрические пространства (где в каждом пространстве метрика обозначена буквой d). Пусть функция

$$\rho : (\mathbb{R}_+ \sqcup \{0\})^n \to \mathbb{R}_+ \sqcup \{0\},$$

обладает свойствами

(невырожденность) $\rho(a) = 0 \Leftrightarrow a = 0$;

(субаддитивность) $\rho(a + b) \leqslant \rho(a) + \rho(b)$;

(монотонность) $\rho(a) \leqslant \rho(b)$, если $a \leqslant b$;

где a, b — произвольные наборы из $(\mathbb{R}_+ \sqcup \{0\})^n$, операции и отношения действуют на наборах покоординатно. В этом случае отображение

$$d^* : (X_1 \times \ldots \times X_n)^2 \to \mathbb{R}_+ \sqcup \{0\}, (x, y) \mapsto \rho(d(x_1, y_1), \ldots, d(x_n, y_n)),$$

является метрикой на произведении метрических пространств (проверьте). В частности, таким образом определяется p-метрика

$$d_p : (X_1 \times \ldots \times X_n)^2 \to \mathbb{R}_+ \sqcup \{0\}, (x, y) \mapsto \Big(\sum_k d(x_k, y_k)^p \Big)^{1/p},$$

для любого действительного $p \geqslant 1$, а также метрика

$$d_\infty : (X_1 \times \ldots \times X_n)^2 \to \mathbb{R}_+ \sqcup \{0\}, (x, y) \mapsto \max_k d(x_k, y_k).$$

Свойство субаддитивности для соответствующей функции

$$\rho_p : (\mathbb{R}_+ \sqcup \{0\})^n \to \mathbb{R}_+ \sqcup \{0\}, a \mapsto \Big(\sum_k a_k^p \Big)^{1/p}$$

при $p \neq \infty$ называется неравенством Минковского, а также неравенством Коши-Буняковского при $p = 2$.

Метрика, определённая подобным образом на n-й декартовой степени пространства $(\mathbb{R}, \mathrm{r})$, обозначается далее r_p (где $p \in [1, \infty)$ или $p = \infty$).

∘ На множестве A^* всех слов в алфавите A определяется метрика:

$d : (A^*)^2 \to \mathbb{R}_+ \sqcup \{0\}, (x, y) = \alpha^k,$ где k — длина общего начала слов x, y;

здесь α — фиксированное действительное число, такое, что $0 < \alpha < 1$.

∘ Ряд метрик, связанных с нормированиями алгебраических структур, рассматриваются далее.

Нормированное кольцо. Пусть K — кольцо с единицей. Функция

$$K \to \mathbb{R}_+ \sqcup \{0\}, x \mapsto ||x||$$

называется *нормой* и кольцо K, рассматриваемое вместе с этой функцией, называется *нормированным*, если для любых его элементов x, y выполнены условия:

(1) $||x|| = 0 \Leftrightarrow x = 0$;

(2) $||x \cdot y|| = ||x|| \cdot ||y||$;

(3) $||x + y|| \leqslant ||x|| + ||y||$.

Замечание. Из определения следуют дополнительно свойства

(4) $||x - y|| \geqslant ||x|| - ||y||$.

(5) $||y|| = || - y||$ (так как $||y||^2 = || - y||^2$);

(6) $||1|| = 1$ (так как $||y|| = ||1|| \cdot ||y||$).

Норма на кольце называется *неархимедовой*, если вместо третьего условия выполняется более сильное условие

(3') $||x + y|| \leqslant \max\{||x||, ||y||\}$.

Нормированное кольцо $(K, || \cdot ||)$ является одновременно метрическим пространством (K, d), где

$$d(x, y) = ||x - y|| \text{ для любых } x, y \text{ из } K.$$

Упражнение. Если нормирование на кольце неархимедово, то и метрика получается тоже неархимедовой. Проверьте это.

Примеры.

∘ Абсолютное значение. Функция «абсолютное значение» является нормой на архимедовом поле. В частности, в поле действительных чисел определена естественная норма $|\cdot|$, совпадающая с абсолютным значением, а также связанная с ней естественная метрика r.

∘ p-Адическая норма на $\mathbb{Q}$. Всякое рациональное число a можно записать единственным образом в виде

$$a = \pm \prod_{p \text{ — простое}} p^{\upsilon_p(a)},$$

где функция $\upsilon_p : \mathbb{Q} \to \mathbb{Z}$ указывает на сколько чаще простое число p входит в числитель дроби, представляющей число a, чем в знаменатель; мы считаем $\upsilon_p(0) = 0$. Тогда p-адическое нормирование $|\cdot|_p$ определяется следующим образом:

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+ \sqcup \{0\}, x \mapsto \alpha^{\upsilon_p(x)},$$

где α — произвольное фиксированное число из $(0,1)$. Далее всегда будем брать $\alpha = 1/p$ (конкретное значение не существенно, как будет понятно в дальнейшем); тогда

$$|x|_p = p^{-v_p(x)}.$$

Например,

$$|100/33|_5 = 1/25,\ |100/33|_3 = 3.$$

$\circ$ p-Адическая норма на $\mathbb{Q}_p$. Для p-адического ряда

$$a = a_l p^l + a_{l+1} p^{l+1} + \dots,$$

где $l \in \mathbb{Z}$, его p-адическая норма определяется как и раньше для рационального числа:

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+ \sqcup \{0\}, x \mapsto \alpha^{v_p(x)},$$

но теперь

$$v_p(a) = k,\ \text{где — наименьшее целое, такое, что } a_k \neq 0.$$

Упражнение. Проверьте, что в обоих случаях получается неархимедова норма и обе они совпадают на рациональных числах.

Нормированное пространство. Пусть V — векторное пространство над нормированным полем K. Функция

$$V \to \mathbb{R}_+ \sqcup \{0\}, x \mapsto ||x||$$

называется *нормой* и пространство V, рассматриваемое вместе с этой функцией, называется *нормированным*, если для любых элементов x, y из V, λ из K выполненяются условия:

(1) $||x|| = 0 \Leftrightarrow x = 0$;

(2) $||\lambda \cdot y|| = |\lambda| \cdot ||y||$, где $|\cdot|$ — нормирование поля K;

(3) $||x + y|| \leqslant ||x|| + ||y||$.

Замечание. Как и раньше из определения следуют свойства

(4) $||x - y|| \leqslant ||x|| - ||y||$.

(5) $||y|| = ||-y||$ (так как $||-y|| = |-1| \cdot ||y|| = ||y||$).

Норма называется неархимедовой, если вместо третьего свойства выполняется более сильное условие

(3') $||x + y|| \leqslant \max\{||x||, ||y||\}$.

Нормированние алгебры A определяется дополнительным условием

(2') $||x \cdot y|| \leqslant ||x|| \cdot ||y||$.

Как и ранее нормированние порождает метрику; причём неархимедово нормирование порождает неархимедову метрику.

Примеры.

∘ Произведения. Пусть заданы нормированные пространства

$$(V_1, ||\cdot||_1), \ldots, (V_n, ||\cdot||_n)$$

над полем K и функция

$$\rho : (\mathbb{R}_+ \sqcup \{0\})^n \to \mathbb{R}_+ \sqcup \{0\},$$

обладающая свойствами невырожденности, субаддитивности и монотонности, определёнными в предыдущем разделе, и ещё одним свойством

(∘) $\rho(\lambda x) = \lambda\rho(x)$ для любых элементов λ из $\mathbb{R}_+$, x из $(\mathbb{R}_+ \sqcup \{0\})^n$.

Тогда отображение

$$||\cdot|| : V_1 \times \ldots \times V_n \to \mathbb{R}_+ \sqcup \{0\}, x \mapsto \rho(||x_1||_1, \ldots, ||x_n||_n),$$

является нормированием прямого произведения пространств. В том числе, таким образом для любого p из множества $[1, \infty)$ определяется p-норма:

$$||\cdot||_p : \mathbb{R}^n \to \mathbb{R}_+ \sqcup \{0\}, x \mapsto \Big(\sum_k |x_k|^p\Big)^{1/p},$$

а также определяется норма

$$||\cdot||_\infty : \mathbb{R}^n \to \mathbb{R}_+ \sqcup \{0\}, x \mapsto \max_k |x_k|.$$

∘ В конечно мерном векторном пространстве над полем комплексных чисел можно определить следующую норму:

$$|x| = \Big(\sum_k x_k x_k^*\Big)^{1/2}.$$

2. Топология метрического пространства

В этом разделе вводится ряд понятий, связанных с топологией метрического пространства.

Шары и окрестности. Пусть X — метрическое пространство с метрикой d. Для любого его элемента s и любого положительного действительного числа ε множество

$$B_\varepsilon(s) = \{x | x \in X, d(x, s) < \varepsilon\}$$

называется *открытым шаром* радиуса ε с центром в точке s. Всякое множество, включающее открытый шар с центром в точке s, называется её *окрестностью*.

Подмножество метрического пространства называется *открытым*, если оно является объединением открытых шаров и называется *замкнутым*, если оно является дополнением некоторого открытого множества.

Примеры.

∘ На действительной прямой открытый шар — это отрезок без концевых точек.

∘ В нормированном поле $\mathbb{Q}_p$ p-адических чисел открытый шар радиуса $1/p^k$ с центром в точке s, где

$$s = s_l p^l + s_{l+1} p^{l+1} + \dots \text{ и } l \leqslant k,$$

совпадает с множеством

$$s + p^{k+1}\mathbb{Z}_p$$

и состоит из p-адических чисел

$$s_l p^l + \dots + s_k p^k + s'_{k+1} p^{k+1} + s'_{k+2} p^{k+2} + \dots,$$

где коэффициенты $s_l, \dots, s_k$ фиксированы и остальные коэффициенты $s'_{k+1}, s'_{k+2}, \dots$ произвольные. Любой элемент шара является его центром.

Упражнение. Как выглядит открытый шар в каждом из пространств $(\mathbb{R}^2, \mathrm{r}_2), (\mathbb{R}^2, \mathrm{r}_1), (\mathbb{R}^2, \mathrm{r}_\infty)$?

Открытые множества и внутренность. Отметим ряд свойств открытых множеств.

∘ Система открытых множеств обладает свойствами:

(1) множества $\emptyset$ и X открыты;

(2) объединение любого набора открытых множеств открыто;

(3) пересечение конечного набора открытых множеств открыто. □

Система открытых множеств называется *топологией* метрического пространства.

Рассмотрим далее в метрическом пространстве (X, d) произвольное подмножество S и отметим ряд свойств.

∘ Среди открытых множеств, содержащихся в заданном множестве S, есть наибольшее по включению. □

Оно совпадает с объединением этих открытых множеств, называется *внутренностью* S и обозначается $\operatorname{Int} S$.

∘ Внутренность множества состоит из элементов, которые содержатся в нём вместе с некоторой окрестностью. □

В связи с этим выполняется следующее свойство.

∘ Имеет место равенство

$$\operatorname{Int} S = \{x | x \in X, d(x, S') > 0\}, \text{ где } S' = X \setminus S, d(x, S') = \inf_{s \in S'} d(x, s).$$

Число $d(x, S')$ называется *расстоянием от точки x до множества S'*.

Замкнутые множества и замыкание. Обратимся к свойствам замкнутых множеств.

∘ Система замкнутых множеств обладает свойствами:

(1) множества $\emptyset$ и X замкнуты;

(2) пересечение любого набора замкнутых множеств замкнуто;

(3) объединение конечного набора замкнутых множеств замкнуто. □

∘ Среди замкнутых множеств, содержащих заданное множество S, есть наименьшее по включению. □

Оно совпадает с пересечением всех этих замкнутых множеств, называется *замыканием* S и обозначается через $\operatorname{Clo} S$.

∘ Замыкание множества состоит из элементов, у которых любая окрестность пересекается с этим множеством. □

В связи с этим выполняется следующее свойство.

∘ Имеет место равенство

$$\operatorname{Clo} S = \{x | x \in X, d(x, S) = 0\}. \square$$

Граница. *Границей* множества S называется множество

$$\partial S = \operatorname{Clo} S \setminus \operatorname{Int} S.$$

∘ Имеет место равенство

$$\partial S = \{x | x \in X, d(x, S') = d(x, S) = 0\}. \square$$

Рассмотрим

Пример. Канторово множество — это множество $\mathcal{K}$ действительных чисел, которое определяется следующим образом:

$$\begin{aligned} \mathcal{K} = \cap_n I_n, \text{ где } & I_0 = [0, 1], \\ & I_1 = [0, 1/3] \sqcup [2/3, 1], \\ & I_2 = [0, 1/9] \sqcup [2/9, 1/3] \sqcup [2/3, 7/9] \sqcup [8/9, 1] \\ & \dots . \end{aligned}$$

Здесь каждое следующее множество получается из предыдущего удалением в каждом его интервале средней трети без концевых точек. Канторово множество совпадает со своей границей:

$$\mathcal{K} = \partial\mathcal{K}.$$

Действительно, $d(x, I'_n) < 1/3^n$ для любого x из $\mathcal{K}$. Тогда $d(x, \mathcal{K}') < 1/3^n$, так как $I'_n \subseteq \mathcal{K}'$. Это верно для любого n. Следовательно, $d(x, \mathcal{K}') = 0$ и $\mathcal{K} \subseteq \partial\mathcal{K}$. Обратно, для любого x из $\mathcal{K}'$ найдется такое n, что $x \notin I_n$. Тогда $0 < d(x, I_n) \leqslant d(x, \mathcal{K})$, x не принадлежит границе $\partial\mathcal{K}$ и выполняется равенство $\mathcal{K} = \partial\mathcal{K}$. □

Упражнение. Докажите, что в метрическом пространстве для любого подмножества S выполняются равенства

$$\operatorname{Clo}\operatorname{Clo} S = \operatorname{Clo} S, \operatorname{Int}\operatorname{Int} S = \operatorname{Int} S, \partial\partial S = \partial S, (\operatorname{Clo} S)' = \operatorname{Int}(S').$$

Замечание. Топология метрического пространства не определяет метрику однозначно. Различные метрические пространства могут обладать одной топологией.

Упражнение. Метрики на одном множестве называются *топологически эквивалентными*, если их топологии совпадают. Убедитесь, что все p-метрики на множестве $\mathbb{R}^n$ топологически эквивалентны.

3. Последовательности и полнота

В этом разделе рассматривается ряд свойств метрических пространств, связанных со сходимостью последовательностей.

Полнота. Последовательность a элементов $a_0a_1\ldots$ метрического пространства (X, d) называется *фундаментальной*, если для любого положительного ε почти все её члены лежат в некотором шаре радиуса ε.

Последовательность называется *сходящейся к* элементу a_* и он называется *пределом* последовательности, если для любого положительного ε почти все члены последовательности лежат в шаре радиуса ε с центром в точке a_*. В этом случае пишут

$$a_k \to a_*, k \to \infty, \text{ а также } a_* = \lim_{k\to\infty} a_k.$$

Иными словами, последовательность a_k сходится к элементу a_* в метрическом пространстве (X, d), если в пространстве $(\mathbb{R}, \mathrm{r})$ имеет место следующее соотношение сходимости:

$$d(a_k, a_*) \to 0, k \to \infty.$$

Ясно, что сходящаяся последовательность фундаментальна. Если верно обратное, то есть всякая фундаментальная последовательность сходится, то пространство называется *полным*. Отметим далее ряд свойств.

∘ Подмножество метрического пространства тогда и только тогда замкнуто, когда оно содержит предел любой сходящейся последовательности своих элементов.

Доказательство. Данное свойство является частным случаем следующего.

∘ В метрическом пространстве замыкание подмножества S состоит из всевозможных элементов, являющихся пределами сходящихся последовательностей, составленных из элементов множества S. □

Доказательство. Достаточно заметить, что пределы сходящихся последовательностей, составленных из элементов множества S — это в точности те элементы пространства, которые не обладают окрестностью, целиком лежащей в S'. □

Плотность. В метрическом пространстве подмножество S называется *плотным*, если его замыкание совпадает со всем пространством. Это равносильно тому, что всякий элемент пространства является пределом некоторой последовательности, составленной из элементов множества S; а также тому, что в любой окрестности содержится элемент множества.

∘ Пусть S — плотное подмножество метрического пространства (X, d). Тогда равносильны следующие условия.

(1) В пространстве (X, d) сходится любая фундаментальная последовательность, то есть пространство полное.

(2) В пространстве (X, d) сходится любая фундаментальная последовательность, составленная из элементов множества S.

Доказательство. Это свойство является следствием предыдущих. □

Примеры.

∘ В метрическом пространстве $(\mathbb{R}, \mathrm{r})$ выполянются соотношения:

$$1/k \to 0,$$
$$(k-1)/k \to 1, \text{ при } k \to \infty.$$

∘ В нормированном кольце $(\mathbb{Z}_p, |\cdot|_p)$ выполняется соотношение:

$$k! \to 0 \text{ при } k \to \infty.$$

∘ Пусть $a_1, a_2 \ldots$ — последовательность, составленная из чисел

$$0, 1, \ldots, 9.$$

В метрическом пространстве $([0, 1], \mathrm{r})$ пределом последовательности рациональных чисел

$$a_1 10^{-1},$$
$$a_1 10^{-1} + a_2 10^{-2},$$
$$a_1 10^{-1} + a_2 10^{-2} + a_3 10^{-3},$$
$$\ldots$$

является элемент, который записывается десятичной дробью

$$0, a_1 a_2 \ldots.$$

∘ Пусть $a_0, a_1, \ldots$ — последовательность, составленная из чисел

$$0, 1, \ldots, p-1,$$

где p — простое число. Последовательность рациональных чисел

$$a_l p^l,$$
$$a_l p^l + a_{l+1} p^{l+1},$$
$$a_l p^l + a_{l+1} p^{l+1} + a_{l+2} p^{l+2},$$
$$\dots,$$

где l — целое, сходится в метрическом пространстве $(\mathbb{Q}_p, |\cdot|_p)$ и её пределом является p-адическое число

$$a = a_l p^l + a_{l+1} a^{l+1} + \dots.$$

∘ Пространства $(\mathbb{R}, \mathrm{r})$, $(\mathbb{Z}_p, |\cdot|_p)$, $(\mathbb{Q}_p, |\cdot|_p)$ — полные.

∘ Пространства $(\mathbb{Q}, \mathrm{r})$, $(\mathbb{Q}, |\cdot|_p)$ — не полные.

∘ Подмножество $\mathbb{Q}$ плотное в $(\mathbb{R}, \mathrm{r})$, $(\mathbb{Q}_p, |\cdot|_p)$.

∘ Подмножество $\mathbb{N}$ плотное в $(\mathbb{Z}_p, |\cdot|_p)$.

Упражнение. Рассмотрим в метрическом пространстве (X, d) пару последовательностей

$$a = a_0 a_1 \dots, b = b_0 b_1 \dots$$

и в метрическом пространстве (X^2, d_1) последовательность пар

$$a \times b = (a_0 b_0)(a_1 b_1) \dots.$$

Проверьте следующие свойства.

∘ Последовательности a, b фундаментальные тогда и только тогда, когда последовательность $a \times b$ фундаментальная.

∘ Последовательности a, b сходятся тогда и только тогда, когда последовательность $a \times b$ сходится.

∘ Если все последовательности сходятся (в своих пространствах), то выполняется соотношение

$$\lim_{k\to\infty} (a_k, b_k) = (\lim_{k\to\infty} a_k, \lim_{k\to\infty} b_k).$$

4. Непрерывность

В этом разделе определяются непрерывные и равномерно непрерывные отображения между метрическими пространствами.

Непрерывность. Имеет место

Теорема (непрерывность в точке). *Пусть $f : X \to Y$ — отображение между метрическими пространствами $(X, d), (Y, d')$. Тогда для любого элемента a_* из X следующие условия равносильны.*

(1) *В множестве* $\mathbb{R}_+$ *для любого* ε *существует* δ*, такое, что*

$$f(B_\delta(a_*)) \subseteq B_\varepsilon(f(a_*)), \text{ то есть}$$
$$f(x) \in B_\varepsilon(f(a_*)), \text{ если } x \in B_\delta(a_*).$$

(2) *Для любой последовательности элементов* a_k *из* X *верно*

$$\lim_{k\to\infty} f(a_k) = f(a_*), \text{ если } \lim_{k\to\infty} a_k = a_*.$$

Доказательство. Пусть выполняется первое условие и последовательность элементов a_k сходится к a_*. Тогда для любого ε и соответствующего δ почти все элементы последовательности a_k попадают в шар радиуса δ с центром в a_* и тогда в силу сделанного предположения почти все элементы последовательности $f(a_k)$ попадают в шар радиуса ε с центром $f(a_*)$. Таким образом выполняется второе условие.

Предположим теперь, что первое условие не выполняется. Тогда имеется некоторое такое значение ε, что для любого δ существует элемент $a = a(\delta)$, обладающий свойством:

$$a \in B_\delta(a_*), \text{ но } f(a) \notin B_\varepsilon(f(a_*)).$$

Теперь пусть $\delta_k \to 0$ при $k \to \infty$. Тогда последовательность элементов $a_k = a(\delta_k)$ сходится к a_*. Вместе с тем, последовательность $f(a_k)$ к $f(a_*)$ не сходится. □

В условиях доказанной теоремы функция f, для которой выполняются условия (1,2), называется *непрерывной в точке* a. Функция, непрерывная в любой точке пространства X, называется *непрерывной* на X.

Следствие (непрерывность). *В условиях теоремы равносильны следующие условия.*

(1) *Функция* f *непрерывна.*

(2) *Полный прообраз открытого подмножества в* Y *является открытым в* X*.*

(3) *Полный прообраз замкнутого подмножества в* Y *является замкнутым в* X*.*

Доказательство. Докажем равносильность первых двух условий. Пусть функция f непрерывна. Выберем произвольно: в множестве Y открытое подмножество Z и в полном прообразе множества Z точку x. Так как множество Z открытое, оно содержит некоторый открытый шар $B_\varepsilon(f(x))$. По определению непрерывности имеется открытый шар $B_\delta(x)$, такой, что

$$f(B_\delta(x)) \subseteq B_\varepsilon(f(x)).$$

Полный прообраз множества Z является объединением таких открытых шаров $B_\delta(x)$ и является открытым множеством. Таким образом выполняется второе условие. Предположим теперь, что выполнено второе условие. Возьмём в множестве Y открытый шар $B_\varepsilon(f(x))$ произвольного радиуса ε для произвольного элемента x из множества X. Его полный прообраз является открытым множеством и тогда включает некоторый открытый шар $B_\delta(x)$ с центром x. Отсюда, функция f непрерывная. Первые два условия равносильны. □

Упражнение. Докажите, равносильность условий (2,3).

Следствие. *Непрерывное отображение между метрическими пространствами однозначно определяется его значениями на плотном подмножестве области определения.* □

Равномерная непрерывность. Пусть по-прежнему функция $f : X \to Y$ осуществляет отображение между метрическими пространствами. Она называется *равномерно непрерывной* на пространстве X, если в множестве $\mathbb{R}_+$ для любого ε найдётся δ такое, что для любых x, y из X выполняется условие

$$d'(f(x), f(y)) < \varepsilon, \text{ если } d(x, y) < \delta.$$

Часто говорят о равномерной непрерывности функции на том или ином подпространстве, имея ввиду её ограничение на это подпространство.

Упражнение. Докажите, что *образом фундаментальной последовательности при равномерно непрерывном отображении является фундаментальная последовательность.* Для непрерывной функции это не всегда так. □

Примеры.

∘ Для любого элемента a метрического пространства (X, d) отображение

$$(X, d) \to (\mathbb{R}, \mathrm{r}), x \mapsto d(a, x),$$

непрерывно. Действительно, если $a_k \to a_*$ при $k \to \infty$, то

$$\mathrm{r}(d(a, a_*), d(a, a_k)) = |d(a, a_*) - d(a, a_k)| \leqslant d(a_*, a_k) \to 0, k \to \infty.$$

Более того, оно равномерно непрерывно, так как

$$\mathrm{r}(d(a, x), d(a, y)) = |d(a, x) - d(a, y)| \leqslant d(x, y)$$

∘ Говорят, что отображение $f : X \to Y$ между метрическими пространствами $(X, d), (Y, d')$ удовлетворяет *условию Липшица* с коэффициентом $k \in \mathbb{R}_+$, если

$$d'(f(x), f(y)) \leqslant k \cdot d(x, y)$$

для всех x, y из X. Такое отображение равномерно непрерывно. Например, в предыдущем примере отображение $d(a, \cdot)$ удовлетворяет условию Липшица с коэффициентом 1.

∘ Метрика

$$d : X^2 \to \mathbb{R}_+ \sqcup \{0\}$$

пространства (X, d) равномерно непрерывна как отображение между метрическими пространствами (X^2, d_1), $(\mathbb{R}, \mathrm{r})$. Она удовлетворяет условию Липшица с коэффициентом 1. Действительно, в множестве X^2 для любых элементов $x = (x_1, x_2), y = (y_1, y_2)$, таких, что $d(x) \geqslant d(y)$, верно:

$$\begin{aligned} \mathrm{r}(d(x), d(y)) &= d(x) - d(y) = d(x_1, x_2) - d(y_1, y_2) \\ &\leqslant d(x_1, y_1) + d(y_1, x_2) - (d(y_1, x_2) - d(x_2, y_2)) \\ &= d(x_1, y_1) + d(x_2, y_2) \\ &= d_1(x, y). \end{aligned}$$

∘ Пусть K — нормированное кольцо с нормой $|\cdot|$. Будем рассматривать его как метрическое пространство с метрикой d, где $d(x, y) = |x - y|$. Норма равномерно непрерывна как отображение между метрическими пространствами (K, d), $(\mathbb{R}, \mathrm{r})$, так как удовлетворяет условию Липшица с коэффициентом 1:

$$\mathrm{r}(|x|, |y|) = |x| - |y| \leqslant |x - y| = d(x, y) \text{ при } \ |x| \geqslant |y|.$$

∘ В тех же условиях сложение в нормированном кольце K равномерно непрерывно как отображение между метрическими пространствами (K^2, d_1), (K, d), так как для наборов $x = (x_1, x_2), y = (y_1, y_2)$ из K^2 выполняются неравенства:

$$\begin{aligned} d(x_1 + x_2, y_1 + y_2) &= |x_1 + x_2| - |y_1 + y_2| \leqslant |x_1 + x_2 - y_1 - y_2| \\ &\leqslant |x_1 - y_1| + |x_2 - y_2| = d(x_1, y_1) + d(x_2, y_2) \\ &= d_1(x, y) \text{ при } \ |x_1 + x_2| \geqslant |y_1 + y_2|. \end{aligned}$$

Упражнение. В тех же условиях умножение в кольце K непрерывно.

5. Пополнения

В этом разделе рассматривается возможность расширения метрического пространства либо нормированного кольца до полного.

Пополнение метрического пространства. Метрическое пространство $\widehat{X}$ называется *пополнением* пространства X, если выполнены условия:

(1) Пространство X является подпространством пространства $\widehat{X}$.

(2) Подмножество X плотное в $\widehat{X}$;

(3) Пространство $\widehat{X}$ полное.

Примеры.

∘ Пространство $(\mathbb{R}, \mathrm{r})$ является пополнением пространства $(\mathbb{Q}, \mathrm{r})$.

∘ Пространство $(\mathbb{Q}_p, |\cdot|_p)$ является пополнением $(\mathbb{Q}, |\cdot|_p)$.

∘ Пространство $(\mathbb{Z}_p, |\cdot|_p)$ является пополнением $(\mathbb{Z}, |\cdot|_p)$.

Теорема. *Всякое метрическое пространство обладает пополнением. Пополнение определено однозначно с точностью до изометрии, оставляющей на месте элементы пространства.*

Доказательство. Доказательство разобьём на две части.

(1) Существование.

Рассмотрим метрическое пространство (X, d). Обозначим через $F(X)$ множество всех фундаментальных последовательностей, составленных из его элементов. Постараемся превратить $F(X)$ в метрическое пространство. С этой целью определим метрическое отображение

$$d_F : (F(X))^2 \to \mathbb{R}_+ \sqcup \{0\}, (x, y) \mapsto \lim_{k\to\infty} d(x_k, y_k).$$

(Здесь x, y — произвольные фундаментальные последовательности пространства X, составленные из его элементов x_k, y_k.) Такое определение полностью корректно: последовательность пар (x_k, y_k) является фундаментальной в метрическом пространстве (X^2, d_1), тогда последовательность расстояний $d(x_k, y_k)$ является фундаментальной в пространстве $(\mathbb{R}, \mathrm{r})$, поскольку метрика d равномерно непрерывна между этими пространствами; наконец, предел существует, так как пространство $(\mathbb{R}, \mathrm{r})$ полное.

Отметим, что имеется вложение

$$X \to F(X), x \mapsto \overline{x}, \text{ где } \overline{x} = xxx \ldots,$$

сохраняющее метрические значения, так что

$$d(x, y) = d_F(\overline{x}, \overline{y}) \text{ для любых } x, y \text{ из } X.$$

Функция d_F не является метрикой, поскольку в определении метрики нарушается первое условие, причём другие два условия выполняются (проверьте). В связи с этим рассмотрим на $F(X)$ отношение $\sim$, где

$$x \sim y \Leftrightarrow d(x, y) = 0.$$

Заметим, что это отношение является эквивалентностью и отображение d_F индуцирует на фактор-множестве $\widehat{X} = F(X)/\sim$ метрику

$$\widehat{d} : \widehat{X}^2 \to \mathbb{R} \sqcup \{0\}, ([x], [y]) \mapsto d_F(x, y).$$

Пространство (X, d) изометрически вкладывается в $(\widehat{X}, \widehat{d})$ отображением

$$X \to \widehat{X}, x \mapsto [\overline{x}].$$

Обозначим через $\overline{X}$ множество, на которое отображается X. Отметим, что для последовательности

$$x = x_0 x_1 \ldots,$$

фундаментальной в пространстве (X, d), в пространстве $(\widehat{X}, d)$ выполняется соотношение

$$[x] = \lim_{k\to\infty} [\overline{x_k}],$$

поскольку

$$d_F(x, \overline{x_k}) = \lim_{l\to\infty} d(x_l, x_k) \to 0, k \to \infty.$$

Из этих соотношений следует, что пространство $\widehat{X}$ полное и в нём подмножество $\overline{X}$ плотное. Осталось отождествоить элементы пространств X и $\widehat{X}$ в соответствии с отображением, записанным выше. Существование пополнения доказано.

(2) Единственность.

Ранее установлено, что метрика $\widehat{d}$ является непрерывным отображением между метрическими пространствами $(\widehat{X}^2, \widehat{d}_1)$ и $(\mathbb{R}, d)$. Единственность пополнения является следствием этого факта. Действительно, пусть метрическое пространство $(\widehat{X}, \widehat{d})$ является пополнением пространства (X, d). Тогда для любых фундаментальных последовательностей

$$a = a_0 a_1 \ldots, b = b_0 b_1 \ldots$$

пространства (X, d) выполняются соотношения

$$\begin{aligned}\widehat{d}(\lim_{k\to\infty} a_k, \lim_{k\to\infty} b_k) = \\ &= \widehat{d}(\lim_{k\to\infty} (a_k, b_k)) \\ &= \lim_{k\to\infty} \widehat{d}(a_k, b_k) \\ &= \lim_{k\to\infty} d(a_k, b_k),\end{aligned}$$

где во второй строчке предел последовательности пар (a_k, b_k) вычисляется в метрическом пространстве $(\widehat{X}^2, \widehat{d}_1)$. В силу этих соотношений метрика $\widehat{d}$ определяется метрикой d однозначно. Тогда для любого пополнения (X', d') пространства (X, d) имеет место изометрия:

$$X' \to \widehat{X}, \lim_{k\to\infty} a_k \mapsto \lim_{k\to\infty} a_k,$$

где a_k — элементы произвольной фундаментальной последовательности пространства (X, d). Теорема доказана. □

Пополнение нормированного кольца. Пополнением нормированного кольца K называется нормированное кольцо $\widehat{K}$, для которого выполняются условия:

(1) Кольцо K является подкольцом и подпространством в $\widehat{K}$.

(2) Подмножество K плотное в пространстве $\widehat{K}$.

(3) Пространство $\widehat{K}$ полное.

Здесь нормированное кольцо одновременно рассматривается как метрическое пространство с индуцированной метрикой.

Теорема. *Всякое нормированное кольцо обладает пополнением. Пополнение определено однозначно с точностью до изоморфизма нормированных колец. Пополнение нормированного поля является полем.*

Доказательство. Принцип пополнения такой же как для метрических пространств. Пусть $F(K)$ — множество всех фундаментальных последовательностей, составленных из элементов нормированного кольца K. Это множество является кольцом с покомпонентным сложением и умножением последовательностей. Попробуем перенести норму на это кольцо следующим образом:

$$||x|| = \lim_{k\to\infty} ||x_k||.$$

При таком определении нарушается первое требование для нормы и выполняются оставшиеся. Пусть $O(K)$ — множество последовательностей, сходящихся к нулю. Для любых двух фундаментальных последовательностей x, y положим

$$x \sim y, \text{ если } x - y \in O(K).$$

Это эквивалентность и на фактор-множестве $F(X)/O(X)$ индуцируется структура нормированного кольца. Этого достаточно для доказательства. Недостающие детали можно почерпнуть из доказательства предыдущей теоремы. □

Упражнение. Сформулируйте и докажите теорему о существовании и единственности пополнения для нормированных пространств.

6. Теорема Островского

Нормирвания, определённые на одном множестве, назовём *эквивалентными*, если они определяют одну топологию. *Тривиальным* называется нормирование, при котором норма любого отличного от нуля элемента равна 1.

Теорема (Островский). *Нетривиальное нормирование поля рациональных чисел эквивалентно $|\cdot|$ или $|\cdot|_p$ для некоторого простого числа p.*

Доказательство. Рассмотрим на рациональных числах нетривиальное нормирование $||\cdot||$. Пусть p, q — простые числа из $\mathbb{Z}_+$ и

$$p^n = \sum_{k=1}^{m} a_k q^k, \text{ где } a_m \neq 0, \text{ то есть } m \leqslant n \log_q p < m+1.$$

Тогда

$$||p||^n = ||p^n|| = ||\sum_k a_k q^k|| \leqslant (q-1)(m+1)\max(||q||, ||q||^m).$$

Рассмотрим далее два случая.

(1) *Предположим, что* $||p|| > 1$.

Тогда $||q|| > 1$ для любого простого q (и даже для любого целого), так как выполняется неравенство

$$||p||^n/(m+1) \leqslant (q-1)\max(||q||, ||q||^m),$$

где значение справа ограничено при $||q|| \leqslant 1$ и $n \to \infty$, в отличие от значения слева. Тогда

$$||p|| \leqslant \sqrt[n]{(q-1)(m+1)} \cdot ||q||^{\log_q p + 1/n} \to ||q||^{\log_q p}, n \to \infty.$$

Следовательно,

$$||p|| \leqslant ||q||^{\log_q p} \text{ и } p^{\log_p ||p||} \leqslant q^{\log_q p \log_q ||q||} = p^{\log_q ||q||},$$

$$\text{откуда } \log_p ||p|| \leqslant \log_q ||q||.$$

Здесь должно быть равенство, так как p и q — произвольные простые. Тогда

$$||p|| = p^\alpha, \text{ где } \alpha = \log_p ||p|| = \log_q ||q||.$$

Для произвольного рационального числа x должно выполняться

$$||x|| = |x|^\alpha.$$

Такая норма эквивалентна норме «абсолютное значение».

(2) *Пусть теперь* $||p|| \leqslant 1$.

Тогда $||q|| \leqslant 1$ для любого простого q и $||p|| < 1$ для некоторого простого p, так как нормирование нетривиальное. Заметим, что $||q|| = 1$ любого простого $q \neq p$, так как иначе

$$||p||^n, ||q||^n < 1/2, sp^n + tq^n = 1$$

для некоторого натурального числа n и целых s, t. Тогда

$$1 = ||1|| \leqslant ||s||||p||^n + ||t||||q||^n \leqslant ||p||^n + ||q||^n < 1/2 + 1/2 = 1$$

— противоречие. В рассматриваемом случае

$$||x|| = ||p||^{v_p(x)} = |x|_p^\alpha \text{ для } \alpha = \log_p ||p||.$$

Нормирование эквивалентно p-адическому. $\square$

ГЛАВА 20

Евклидовы и эрмитовы пространства

В главе изучаются евклидовы и эрмитовы пространства.

1. Евклидово пространство

Начнём с евклидова пространства.

Определение. Пусть V — векторное пространство над полем действительных чисел. Функция

$$V \times V \to \mathbb{R}_+ \sqcup \{0\}, (u, v) \mapsto \langle u, v \rangle$$

называется (евклидовым) *скалярным произведением* и пространтство V, рассматриваемое вместе с ней, называется *евклидовым*, если для любых элементов u, v, w из V и λ из $\mathbb{R}$ выполнены следующие условия.

(1. Билинейность.)

$$\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle,$$
$$\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle,$$
$$\langle \lambda u, v \rangle = \langle u, \lambda v \rangle = \lambda \langle u, v \rangle.$$

(2. Симметричность.)

$$\langle u, v \rangle = \langle v, u \rangle.$$

(3. Положительность.)

$$\langle u, u \rangle > 0 \text{ при } u \neq 0.$$

Замечание. Из определения следует, что

$$\langle u, u \rangle = 0 \Leftrightarrow u = 0.$$

Скалярное произведение в евклидовом пространстве может обозначаться иначе. Часто используются круглые скобки, часто оно обозначается точкой между векторами.

Изоморфизмом между евклидовыми пространствами V, W называется изоморфизм векторных пространств

$$V \to W, u \mapsto u',$$

сохраняющий скалярное произведение, такой, что

$$\langle u, v \rangle = \langle u', v' \rangle$$

для всех u, v из V.

Примеры.

∘ Стандартное пространство. *Стандартным* евклидовым пространством называется векторное пространство $\mathbb{R}^n$, где скалярное произведение определено следующим образом:

$$\langle u, v\rangle = \sum_k u_k v_k.$$

Здесь u, v — произвольные наборы из $\mathbb{R}^n$.

∘ Стандартное произведение. Пусть V — конечно-мерное векторное пространство над полем действительных чисел. При произвольном выборе базиса *стандартное скалярное произведение* определяется в нём следующим образом

$$\langle u, v\rangle = \sum_k u_k v_k.$$

Здесь u, v — произвольные вектора из V и u_k, v_k — их координаты в выбранном базисе.

∘ Непрерывные функции $f : [a, b] \to \mathbb{R}$ образуют векторное пространство с поточечными операциями умножения на скаляры и сложения. Скалярное произведение здесь можно ввести следующим образом:

$$\langle f, g\rangle = \int_a^b f(x)g(x)dx.$$

Неравенство Шварца. Отметим далее ряд свойств.

∘ Неравенство Шварца. *В евклидовом пространстве V для любых векторов u, v выполняется неравенство Шварца:*

$$\langle u, v\rangle \leqslant \sqrt{\langle u, u\rangle}\sqrt{\langle v, v\rangle}.$$

Доказательство. Для линейно зависимых векторов неравенство выполняется (проверьте). Для линейно независимых векторов u, v и любой константы λ выполняется строгое неравенство

$$\langle u + \lambda v, u + \lambda v\rangle > 0.$$

В силу этого квадратное уравнение (относительно λ)

$$\lambda^2\langle v, v\rangle - 2\lambda\langle u, v\rangle + \langle u, u\rangle = 0$$

имеет отрицательный дискриминант:

$$4\langle u, v\rangle^2 - 4\langle u, u\rangle\langle v, v\rangle < 0.$$

Отсюда следует неравенство Шварца. □

∘ *Отображение*

$$|\cdot| : V \to \mathbb{R}_+ \sqcup \{0\},\ u \mapsto |u|,\ \textit{где}\ |u| = \sqrt{\langle u, u\rangle}$$

является нормированием векторного пространства V.

Доказательство. Неравенство треугольника выглядит так

$$\sqrt{\langle u+v, u+v\rangle} \leqslant \sqrt{\langle u,u\rangle} + \sqrt{\langle v,v\rangle},$$

откуда после возведения в квадрат и приведения получается

$$\langle u,v\rangle \leqslant \sqrt{\langle u,u\rangle\langle v,v\rangle}$$

— неравенство Шварца. Таким образом, оба неравенства равносильны. □

Упражнение. Когда в неравенстве Шварца выполняется равенство?

В силу последнего свойства евклидово пространство является одновременно и нормированным пространством, причём всякий изоморфизм между евклидовыми пространствами (сохраняющий скалярное произведение) является и изоморфизмом нормированных пространств (то есть сохраняет норму). В действительности, верно и обратное: изоморфизм векторных пространств, сохраняющий евклидову норму, сохраняет и скалярное произведение, так как имеет место следующее свойство.

∘ *В евклидовом пространстве скалярное произведение следующим образом выражается через норму:*

$$2\langle u,v\rangle = |u+v|^2 - |u|^2 - |v|^2.$$

Доказательство. Это проверяется непосредственно. □

∘ Угол между векторами. *Для ненулевых векторов u, v имеется единственное значение φ, принадлежащее интервалу $[0,\pi]$, такое, что*

$$\cos\varphi = \frac{\langle u,v\rangle}{|u||v|}.$$

Доказательство. Это следует из неравенства Шварца. □

Величина φ называется *углом между векторами* u, v. Это действительно угол между ними в содержащем их двумерном пространстве, если это двумерное пространство определённым образом отождествить с плоскостью. В стандартном евклидовом пространстве это так в силу теоремы косинусов. Действительно, следствием этой теоремы является равенство

$$|u-v|^2 = |u|^2 + |v|^2 - 2|u||v|\cos\varphi,$$

где φ — угол между векторами u, v; из которого в результате сокращений получается соотношение

$$\sum_k u_k v_k = |u||v|\cos\varphi.$$

Далее будет доказано, что конечно мерные евклидовы пространства одной размерности изоморфны, так что рассмотренного здесь стандартного пространства вполне достаточно.

Теорема Грама-Шмидта. Набор векторов $\alpha_1, \ldots, \alpha_n$ евклидова пространства назовём *ортогональным*, если выполнено условие

$$\langle \alpha_i, \alpha_j \rangle = 0$$

для всех i, j, таких, что $1 \leqslant i < j \leqslant n$, и назовём *ортонормированным*, если дополнительно

$$\langle \alpha_i, \alpha_i \rangle = 1,$$

для всех i, таких, что $1 \leqslant i \leqslant n$.

Как видно, ортонормированным является базис, в котором скалярное произведение принимает стандартный вид. Имеет место

Теорема Грама-Шмидта. *Конечно-мерное евклидово пространство содержит ортонормированный базис.*

Доказательство. Пусть в пространстве V размерности n имеется ортонормированный набор векторов $u_1, \ldots, u_m$, где $m < n$. Выберем произвольно вектор v в множестве

$$V \setminus (\mathbb{R}u_1 + \ldots + \mathbb{R}u_m).$$

Пусть

$$p(v) = \langle v, u_1 \rangle u_1 + \ldots + \langle v, u_m \rangle u_m.$$

Тогда вектор $v - p(v)$ ортогонален всем векторам набора и не принадлежит пространству, порождаемому ими. Следовательно, имеющийся ортонормированный набор можно расширить ещё одним вектором

$$u_{m+1} = (v - p(v))/|v - p(v)|. \; \square$$

Следствие. *Существует единственное с точностью до изоморфизма конечно-мерное евклидово пространство заданной размерности.*

Доказательство. Между евклидовым пространством V размерности n и стандартным евклидовым пространством имеется изоморфизм:

$$V \to \mathbb{R}^n, u \mapsto (u_1, \ldots, u_n)^{\mathrm{T}},$$

где u_k — координаты вектора u в ортонормированном базисе. $\square$

Отметим, что в доказательстве теоремы Грама-Шмидта использовалось следующее свойство.

$\circ$ *В евклидовом пространстве V для любого вектора v и любого подпространства U существует единственная пара векторов $p_U(v)$ и $q_U(v)$, таких, что*

$$v = p_U(v) + q_U(v), \;\; p_U(v) \in U, \;\; \langle q_U(v), u \rangle = 0 \text{ для любого } \; u \in U.$$

(Вектор $p_U(v)$ с описанными свойствами называется *проекцией* вектора v на подпространство U.)

Доказательство. В доказательстве теоремы Грама-Шмидта в роли вектора $p_U(v)$ выступал вектор $p(v)$, а в роли подпространства U — подпространство, порождённое векторами $u_1, \ldots, u_m$. $\square$

Сделаем следующее определение. В векторном пространстве V *суммой* подпространств U_1, U_2 называется подпространство

$$U_1 + U_2 = \{u_1 + u_2 | u_1 \in U_1, u_2 \in U_2\};$$

сумма называется прямой и для неё используется обозначение $U_1 \oplus U_2$, если $U_1 \cap U_2 = 0$. Иными словами, сумма подпространств состоит из векторов пространства, которые можно представить в виде суммы со слагаемыми из подпространств; а в прямой сумме подобное представление для любого вектора единственно. Ещё одним следствием последнего свойства является

Теорема. *В евклидовом пространстве V для любого подпространства U множество*

$$U^\perp = \{v | v \in V, \langle u, v\rangle = 0 \text{ для всех } u \in U\}$$

является подпространством и имеет место разложение

$$V = U \oplus U^\perp.$$

В частности, $\dim V = \dim U + \dim U^\perp$.

Доказательство. Условие $U \cap U^\perp = 0$ является следствием положительности скалярного произведения. Условие $U + U^\perp = V$ следует из последнего свойства. $\square$

Подпространство $U^\perp$ называется *ортогональным дополнением* U в V.

Упражнение. Проверьте, что в евклидовом пространстве выполняются следующие свойства.

$\circ$ Ортогональный набор векторов линейно независим.

$\circ$ Для ортогонального набора векторов $e_1, \ldots, e_n$ и произвольного вектора $u = \sum_i u_i e_i$ имеют место равенства

$$u_i = \frac{\langle u, e_i\rangle}{\langle e_i, e_i\rangle}, 1 \leqslant i \leqslant n.$$

$\circ$ Равенство Парсеваля. Ортонормированная система векторов $e_1, \ldots, e_n$ тогда и только тогда является базисом, когда для любого вектора u выполняется равенство

$$\langle u, u\rangle = \sum_i \langle u, e_i\rangle^2.$$

2. Матрица Грама и объём параллелепипеда

В данном разделе вводится в рассмотрение матрица Грама и даётся геометрическая интерпретация определителю.

Матрица Грама. Рассмотрим следующую ситуацию. Предположим, что в евклидовом пространстве каждый из векторов u, v является линейной комбинацией набора векторов $\alpha = (\alpha_1, \ldots, \alpha_n)$, так, что выполняются равенства:

$$u = \sum_k u_k \alpha_k, \;\; v = \sum_k v_k \alpha_k.$$

Заметим, что значение скалярного произведения $\langle u, v\rangle$ однозначно определяется координатами векторов u, v и произведениями $\langle \alpha_i, \alpha_j\rangle$. Составим из этих произведений матрицу

$$G(\alpha) = \begin{pmatrix} \langle \alpha_1, \alpha_1\rangle & \ldots & \langle \alpha_1, \alpha_n\rangle \\ \vdots & & \vdots \\ \langle \alpha_n, \alpha_1\rangle & \ldots & \langle \alpha_n, \alpha_n\rangle \end{pmatrix}.$$

Такая матрица называется *матрицей Грама* системы векторов α относительно заданного скалярного умножения. Отметим, что выполняется следующее условие.

∘ Имеет место равенство:

$$\langle u, v\rangle = (u_1, \ldots, u_n) G(\alpha) (v_1, \ldots, v_n)^T;$$

это верно для любых векторов u, v из пространства, порождённого набором векторов α. □

Отметим также следующее.

∘ Матрица $G(\alpha)$ однозначно определяется предыдущим условием, если набор α линейно независимый. □

Запишем, каким образом матрица Грама изменяется при линейном преобразовании векторов.

∘ Имеет место равенство

$$G(\beta) = C_{\alpha\beta}^T \cdot G(\alpha) \cdot C_{\alpha\beta},$$

если наборы векторов α, β и квадратная матрица $C_{\alpha\beta}$ связаны соотношением

$$\beta = \alpha C_{\alpha\beta}. \; \square$$

(Чтобы убедиться в этом, нужно подставить новые координаты векторов u, v в предыдущую формулу.) Имеет место

Теорема. *Пусть $G(\alpha)$ — матрица Грама относительно евклидова скалярного произведения. Её определитель положителен, если набор векторов α линейно независимый; и равен нулю в противном случае.*

Доказательство. В силу линейности скалярного произведения по первому аргументу линейная зависимость между векторами приводит к

зависимости между строками матрицы Грама с теми же коэффициентами. Следовательно, определитель матрицы равен нулю в случае линейной зависимости. Предположим, вектора линейно независимы и составляют тогда базис пространства. Пусть $\beta = \alpha C_{\alpha\beta}$ — ортонормированный базис. Тогда

$$\mathrm{e} = G(\beta) = C_{\alpha\beta}^{\mathrm{T}} \cdot G(\alpha) \cdot C_{\alpha\beta} = G(\alpha).$$

Отсюда, определитель матрицы $G(\alpha)$ положительный. $\square$

Упражнение. Докажите записанные выше свойства, получите неравенство Шварца как следствие последней теоремы при $n = 2$.

Неориентированный объём параллелепипеда. Далее установим связь матрицы Грама с определителем и выясним их геометрический смысл. *Параллелепипедом*, натянутым на систему векторов $\alpha = (\alpha_1, \ldots, \alpha_n)$, называется множество

$$\Pi(\alpha_1, \ldots, \alpha_n) = \{\sum_k \lambda_k a_k | 0 \leqslant \lambda_k \leqslant 1 \text{ для всех } k\}.$$

При этом $\Pi(\alpha_1, \ldots, \alpha_{n-1})$ называется *основанием* параллелепипеда и вектор $q_U(\alpha_n)$, где $U = \mathbb{R}\alpha_1 + \ldots + \mathbb{R}\alpha_{n-1}$, называется его *высотой*. Напомним, что вектор $q_U(\alpha_n)$ опредляется из условия

$$\alpha_n = p_U(\alpha_n) + q_U(\alpha_n), p_U(\alpha_n) \in U, q_U(\alpha_n) \in U^{\perp};$$

вектора $p_U(\alpha_n), q_U(\alpha_n)$ называются проекциями вектора α_n на пространства $U, U^{\perp}$. (Здесь $U^{\perp}$ — дополнительное для U подпространство пространства $V = \langle \alpha_1, \ldots, \alpha_n \rangle$.)

Неориентированный объём параллелепипеда определяется по-индукции условиями:

$$V(\alpha_1, \ldots, \alpha_n) = V(\alpha_1, \ldots, \alpha_{n-1}) \cdot |q_U(\alpha_n)| \text{ и } V(\alpha_1) = |\alpha_1|.$$

Теорема. $(V(\alpha))^2 = \det G(\alpha)$.

Доказательство проводится индукцией по n. Теорема верна для $n = 1$. При $n > 1$ запишем

$$p_U(\alpha_n) = \sum_{k<n} \lambda_k \alpha_k \text{ и } \alpha_n = p_U(\alpha_n) + q_U(\alpha_n) = \sum_{k<n} \lambda_k \alpha_k + q_U(\alpha_n)$$

и подставим α_n в матрицу Грама. После сокращений получаем

$$\det G(\alpha_1, \ldots, \alpha_n) = \det \begin{pmatrix} \langle \alpha_1, \alpha_1 \rangle & \ldots & \langle \alpha_1, \alpha_{n-1} \rangle & 0 \\ \vdots & & \vdots & \\ \langle \alpha_{n-1}, \alpha_1 \rangle & \ldots & \langle \alpha_{n-1}, \alpha_{n-1} \rangle & 0 \\ \langle \alpha_n, \alpha_1 \rangle & \ldots & \langle \alpha_n, \alpha_{n-1} \rangle & \langle \alpha_n, q_U(\alpha_n) \rangle \end{pmatrix},$$

откуда

$$\begin{aligned}\det G(\alpha_1,\dots,\alpha_n) = \\ &= \det G(\alpha_1,\dots,\alpha_{n-1})\langle \alpha_n, q_U(\alpha_n)\rangle \\ &= \det G(\alpha_1,\dots,\alpha_{n-1})|q_U(\alpha_n)|^2,\end{aligned}$$

так как

$$\begin{aligned}\langle \alpha_n, q_U(\alpha_n)\rangle &= \langle p_U(\alpha_n) + q_U(\alpha_n), q_U(\alpha_n)\rangle \\ &= \langle p_U(\alpha_n), q_U(\alpha_n)\rangle + \langle q_U(\alpha_n), q_U(\alpha_n)\rangle \\ &= \langle q_U(\alpha_n), q_U(\alpha_n)\rangle \\ &= |q_U(\alpha_n)|^2.\end{aligned}$$

Теперь доказательство следует по предположению индукции. □

Ориентированный объём параллелепипеда. Имеет место

Теорема. *Пусть $\alpha = (\alpha_1,\dots,\alpha_n)$ — набор векторов в евклидовом пространстве размерности n и каждый столбец матрицы A является набором координат соответствующего вектора в некотором фиксированном ортонормированном базисе $e = (e_1,\dots,e_n)$, иными словами*

$$\alpha = eA.$$

Тогда имеет место равенство

$$A^{\mathrm{T}}A = G(\alpha).$$

В частности, $\det A = \pm V(\alpha)$.

Доказательство. Непосредственная проверка. □

Определим теперь *ориентированный объём* параллелепипеда, натянутого на набор векторов α, как величину

$$v_e(\alpha_1,\dots,\alpha_n) = \det A,$$

где матрица A указана в теореме. Геометричекский смысл определителя проясняет следующая

Теорема. *Пусть $h : V \to V$ — линейное преобразование евклидова пространства V. Тогда имеет место соотношение*

$$v_e(h(\alpha_1),\dots,h(\alpha_n)) = \det \overline{h}\cdot v_e(\alpha_1,\dots,\alpha_n),$$

где $\overline{h}$ — матрица преобразования h в базисе e.

Доказательство. Если столбцы матрицы A являются наборами координат векторов α_k, то столбцы матрица $\overline{h}A$ суть наборы координат векторов $h(\alpha_1),\dots,h(\alpha_n)$ в том же базисе. Следовательно,

$$v_e(h(\alpha_1),\dots,h(\alpha_n)) = \det(\overline{h}A) = \det\overline{h}\cdot\det A = \det\overline{h}\cdot v_e(\alpha_1,\dots,\alpha_n).\ \square$$

3. Изометрии евклидова пространства

Пусть V — евклидово пространство размерности n с базисом e, G — матрица Грама, записанная для набора векторов e и скалярного произведения в V. Имеет место

Теорема. *Для преобразования $h : V \to V$ равносильны условия:*

(1) *h является изометрией пространства V, фиксирующей 0;*

(2) *преобразование h сохраняет скалярное произведение в V;*

(3) *отображение h является линейным преобразованием, его матрица $\overline{h}$ в базисе e удовлетворяет соотношению*

$$G = \overline{h}^T G \overline{h}.$$

Доказательство. Докажем необходимые имликации.

$(1 \to 2)$.

Пусть h является изометрией, фиксирующей 0. Тогда для любых векторов u, v выполняются равенства

$$\langle u - v, u - v\rangle = |u - v|^2 = |h(u) - h(v)|^2 = \langle h(u) - h(v), h(u) - h(v)\rangle.$$

Последовательно положив $v = 0, u = 0$, убеждаемся, что

$$\langle u, u\rangle = \langle h(u), h(u)\rangle, \langle v, v\rangle = \langle h(v), h(v)\rangle,$$

затем, раскрыв скобки и выполнив сокращения в том же равенстве, получаем $\langle u, v\rangle = \langle h(u), h(v)\rangle$; из первого условия следует второе.

$(2 \to 3)$.

Пусть выполняется второе условие, $e'_1, \ldots, e'_n$ — ортонормированный базис пространства V и ξ — линейное преобразование, совпадающее с h на этих векторах. Такое преобразование существует. Композиция $h\xi^{-1}$ сохраняет скалярное произведение вслед за h и ξ. Она действует тождественно на базисных векторах. Следовательно, для любого вектора u и любого базисного вектора e'_i выполняется равенство

$$\langle h\xi^{-1}(u), e'_i\rangle = \langle h\xi^{-1}(u), h\xi^{-1}(e'_i)\rangle = \langle u, e'_i\rangle,$$

откуда для вектора $u = \sum_j u_j e'_j$ получаем

$$\langle h\xi^{-1}(u), e'_i\rangle = \langle h\xi^{-1}(\sum_j u_j e'_j), e'_i\rangle = \langle \sum_j u_j e'_j, e'_i\rangle = u_i \text{ и } h\xi^{-1}(u) = u.$$

Таким образом, произведение $h\xi^{-1}$ является тождественным отображением. Тогда $h = \xi$. Соотношение для матриц G и $\overline{h}$ получается из соотношения для матрицы Грама при смене базиса. Доказано, что из второго условия следует третье.

$(3 \to 1)$.

Пусть выполняется третье условие. Из соотношения для матрицы Грама при смене базиса следует, что функция h сохраняет скалярное произведение. Тогда она сохраняет норму и метрику; из третьего условия следует первое.

Теорема доказана. □

Линейный оператор, обладающий свойствами (1–3), называется *ортогональным*. Если базис e выбрать ортонормированным, то соотношение, записанное в третьем пункте будет выглядеть так

$$\mathrm{e} = \overline{h}^T \overline{h}.$$

Это означает, что для матрицы $\overline{h}$ обратная совпадает с транспонированной. Матрицы с таким свойством называются *ортогональными*.

Следствие. *Для квадратной действительной матрицы $\overline{h}$ размера n следующие условия равносильны.*

(1) *Матрица $\overline{h}$ ортогональная.*

(2) *В стандартном евклидовом пространстве $\mathbb{R}^n$ для любых векторов u, v выполняется равенство*

$$\langle u, v\rangle = \langle \overline{h}u, \overline{h}v\rangle.$$

(3) *Столбцы матрицы $\overline{h}$ образуют ортонормированную систему относительно стандартного скалярного произведения в $\mathbb{R}^n$.*

Доказательство. Первое и второе условия следствия являются переформулировками соответственно третьего и второго условия в предыдущей теореме, а первое и третье условия следствия являются переформулировками друг друга. □

4. Эрмитово пространство

Пусть V — векторное пространство над полем $\mathbb{C}$ комплексных чисел. Функция

$$V \times V \to \mathbb{R}_+ \cup \{0\}, (u, v) \mapsto \langle u, v\rangle$$

называется (эрмитовым) *скалярным произведением* и векторное пространство V, рассматриваемое вместе с ней, называется *эрмитовым*, если для любых элементов u, v, w из V, λ из $\mathbb{C}$ выполнены условия.

(1. Полуторалинейность.)

$$\langle u + v, w\rangle = \langle u, w\rangle + \langle v, w\rangle,$$
$$\langle u, v + w\rangle = \langle u, v\rangle + \langle u, w\rangle,$$
$$\lambda\langle u, v\rangle = \langle \lambda^* u, v\rangle = \langle u, \lambda v\rangle.$$

(2. Эрмитова симметричность.)

$$\langle u, v\rangle = \langle v, u\rangle^*.$$

(3. Положительность.)

$$\langle u, u\rangle > 0 \text{ при } u \neq 0.$$

Замечание. Из определения следует, что

$$\langle u, u\rangle \Leftrightarrow u = 0.$$

Изоморфизмом между эрмитовыми пространствами V, W называется изоморфизм векторных пространств

$$V \to W, u \mapsto u',$$

сохраняющий скалярное произведение, то есть такой, что

$$\langle u, v\rangle \mapsto \langle u', v'\rangle$$

для всех u, v из V.

Примеры.

∘ В конечно-мерном векторном пространстве V над полем комплексных чисел выберем базис. При заданном выборе базиса *стандартное скалярное произведение* определяется следующим образом

$$\langle u, v\rangle = \sum_k u_k v_k^*,$$

где u_k, v_k — координаты векторов u, v в выбранном базисе.

В том числе в пространстве $\mathbb{C}^n$ столбцов высоты n, составленных из комплексных чисел, можно выбрать базис из единичных векторов и определить стандартное скалярное произведение для этого базиса. Полученное так эрмитово пространство называется *стандартным*.

∘ На множестве непрерывных функций $f : D \to \mathbb{C}$ евклидово скалярное произведение можно определить так:

$$\langle f, g\rangle = \int_D f(z)g(z)^* dz.$$

Здесь D — область на комплексной плоскости, по которой можно интегрировать.

Отметим далее без доказательства ряд свойств.

∘ Неравенство Шварца. В эрмитовом пространстве V для любых векторов u, v выполняется неравенство Шварца:

$$\langle u, v\rangle \leqslant \sqrt{\langle u, u\rangle}\sqrt{\langle v, v\rangle}. \square$$

∘ Пусть задано эрмитово пространство V. Тогда отображение

$$V \to \mathbb{R}_+ \sqcup \{0\},\ u \mapsto |u|,\ \text{где } |u| = \sqrt{\langle u, u\rangle},$$

является нормированием векторного пространства V. □

∘ В эрмитовом пространстве скалярное произведение следующим образом выражается через норму:

$$2\langle u, v\rangle = |u+v|^2 - |u+iy|^2. \square$$

∘ Угол между векторами. В эрмитовом пространстве для ненулевых векторов u, v существует единственный угол $\varphi \in [0, \pi/2]$, такой что

$$\cos\varphi = \frac{|\langle u, v\rangle|}{|u||v|}. \square$$

Теорема Грама-Шмидта. Конечно-мерное эрмитово пространство содержит ортонормированный базис. □

Следствие. Конечно-мерное эрмитово пространство заданной размерности единственно с точностью до изоморфизма. □

Теорема. В эрмитовом пространстве V для любого подпространства U множество

$$U^\perp = \{v | \langle u, v\rangle = 0 \text{ для всех } u \in U\}$$

также является подпространством и имеет место равенство

$$V = U \oplus U^\perp. \square$$

Теорема. Пусть $G(\alpha)$ — матрица Грама для набора α векторов эрмитова пространства (относительно определённого в нём эрмитова скалярного произведения). Её определитель положителен, если набор α линейно независим; и равен нулю в противном случае. □

Теорема. Пусть V — эрмитово пространство размерности n с базисом e и G — матрица Грама базисного набора векторов относительно скалярного произведения в V. Тогда для преобразования $h : V \to V$ следующие условия равносильны:

(1) h является изометрией пространства V, фиксирующей 0;

(2) преобразование h сохраняет скалярное произведение в V;

(3) преобразование h линейное, его матрица $\overline{h}$ в базисе e удовлетворяет соотношению

$$G = \overline{h}^{*\mathrm{T}} G \overline{h}. \square$$

Следствие. Для квадратной комплексной матрицы $\overline{h}$ следующие условия равносильны.

(1) Выполняется равенство

$$\mathrm{e} = \overline{h}^{*\mathrm{T}} \overline{h}.$$

(2) В стандартном эрмитовом пространстве $\mathbb{C}^n$ для любых векторов u, v (записываемых столбцами) выполняется равенство

$$\langle u, v\rangle = \langle \overline{h}u, \overline{h}v\rangle.$$

(3) Столбцы матрицы $\overline{h}$ образуют ортонормированную систему относительно стандартного эрмитова скалярного произведения в $\mathbb{C}^n$. $\square$

Линейный оператор, удовлетворящий условиям (1–3) записанной выше теоремы, называется *унитарным*, как и его матрица $\overline{h}$ в ортонормированном базисе, удовлетворяющая условиям (1–3) записанного выше следствия.

Часть IV

Кольца и модули

ГЛАВА 21

Кольцо

В этой главе продолжается изучение ассоциативных колец, начатое ранее. Напомним, что ассоциативное кольцо (далее — кольцо) суть непустое множество, рассматриваемое вместе с определёнными в нём операциями сложения и умножения, такими, что

(1) со сложением элементы кольца образуют абелеву группу;

(2) с умножением элементы кольца образуют полугруппу;

(3) сложение и умножение связаны законами дистрибутивности.

В этой главе под кольцом понимается ассоциативное кольцо.

1. Идеал кольца

Пусть R — произвольное кольцо. Непустое подмножество J в нём называется *левым идеалом*, если выполнены условия:

∘ Выполняется включение $J - J \subseteq J$. Иными словами, множество J замкнуто вычитанием, является группой относительно сложения.

∘ Выполняется включение $RJ \subseteq J$. Иными словами, множество J замкнуто левым умножением на элементы кольца.

Аналогично определяются правые идеалы, нужно только заменить RJ на JR во втором условии. Подмножество, которое является одновременно левым и правым идеалом, называется *двусторонним идеалом*.

Примеры.

∘ Всякое кольцо содержит тривиальные двусторонние идеалы $0, R$. Первый состоит из одного нуля и называется нулевым идеалом. Второй содержит все элементы кольца и называется единичным идеалом.

∘ Для любого элемента a подмножество

$$Ra = \{ra | r \in R\}$$

является левым идеалом кольца R. Элемент a принадлежит этому идеалу, если в кольце есть единица.

Отметим ряд свойств.

∘ *Для любого подмножества $A \subseteq R$ среди левых идеалов кольца R, включающих A, имеется наименьший по включению.*

Доказательство. Действительно, этот идеал совпадает с пересечением всех левых идеалов, включающих множество A. □

∘ *Этот идеал совпадает с пересечением всех левых идеалов, включающих множество A, он состоит из элементов, которые записываются конечными суммами*

$$\sum_a r_a a + \sum_a n_a a, \text{ где } r_a \in R, n_a \in \mathbb{Z}, a \in A.$$

(Конечность записанной суммы означает, что почти все коэффициенты r_a, n_a равны нулю.)

Доказательство. Это так, поскольку указанные суммы принадлежат рассматриваемому идеалу и сами образуют идеал; и то и другое проверяется непосредственно. □

∘ *В кольце с единицей рассматриваемый идеал состоит из конечных сумм*

$$\sum_a r_a a, \text{ где } r_a \in R.$$

Доказательство. В кольце для любого элемента a и любого целого числа n выполняется равенство $na = (n \cdot 1)a$, откуда видно, что целочисленные кратные являются одновременно обычными кратными. □

Идеал, о котором идёт речь, называется *левым идеалом, порождённым множеством A*. Аналогично, можно говорить о правом и о двусторонним идеале, порождённом множеством A. Последний обозначается

$$(A), \text{ или } (a_1, \ldots, a_n) \text{ при } A = \{a_1, \ldots, a_n\}.$$

Идеал, порождаемый одним элементом, называется *главным*.

Пусть далее I, J — левые идеалы кольца R.

∘ *Левым идеалом кольца R является множество*

$$I + J = \{a + b | a \in I, b \in J\}.$$

Это наименьший по включению левый идеал среди левых идеалов кольца R, включающих идеалы I, J. □

∘ *Левым идеалом кольца R является множество $I \cap J$. Этот идеал является наибольшим по включению среди левых идеалов кольца R, содержащихся в идеалах I, J.* □

∘ *Множество*

$$I \cdot J = \{a_1 b_1 + \ldots a_n b_n | a_1, \ldots, a_n \in I, b_1, \ldots, b_n \in J, n \in \mathbb{N}\}$$

является левым идеалом в R. Он порождается произведениями ab, где $a \in I$ и $b \in J$. □

Свойства, аналогичные перечисленным выше, выполняются для правых и двусторонних идеалов.

Далее рассматриваются идеалы в коммутативном кольце с единицей.

Примеры.

∘ В кольце целых чисел все идеалы главные. Действительно, пусть J — ненулевой идеал в $\mathbb{Z}$ и b — отличный от нуля элемент из J с минимально возможным абсолютным значением. Достаточно показать, что $J \subseteq b\mathbb{Z}$. Для этого произвольное число a из J разделим на b с остатком: $a = bq + r$. Остаток $r = a - bq$ принадлежит идеалу J и тогда равен нулю. Следовательно, элемент $a = bq$ принадлежит идеалу $b\mathbb{Z}$. □

∘ Аналогично в кольце многочленов от одной переменной над полем все идеалы главные. □

∘ В кольце целых p-адических чисел (p — простое) каждый идеал главный. Ненулевой идеал порождается элементом вида p^r с наименьшим возможным показателем. □

∘ В кольце формальных степенных рядов над полем от переменной x каждый идеал главный. Ненулевой идеал порождается элементом вида x^r с наименьшим возможным показателем. □

Имеет место

Теорема. *Коммутативное кольцо R с $1 \neq 0$ тогда и только тогда является полем, когда не содержит идеалов, кроме $0, R$.*

Доказательство. В поле единица кратна любому ненулевому элементу и тогда содержится в любом ненулевом идеале. Ненулевой идеал, следовательно, содержит все элементы поля. Обратно, если в кольце нет нетривиальных идеалов, то любой ненулевой элемент порождает идеал, совпадающий со всем полем, и тогда является делителем единицы, то есть обратимым элементом. □

2. Фактор-кольцо

Пусть J — двусторонний идеал кольца R. Для любого элемента a из кольца множество

$$a + J = \{a + b | b \in J\}$$

называется *смежным классом* элемента a по идеалу J. Иными словами, это множество состоит из элементов, отличающихся от элемента a слагаемым, принадлежащим идеалу. Отметим ряд свойств смежных классов кольца R по идеалу J.

∘ *Для любых элементов a, b из кольца равносильны условия:*

$$a \in b + J, b \in a + J, a - b \in J, a + J = b + J.$$

Доказательство. Легко понять, что для любого элемента j из кольца равносильны условия

$$a = b + j, b = a + (-j), a - b = j.$$

Отсюда следует равносильность первых трёх условий. Не сложно убедиться, что и четвёртое условие им равносильно. □

∘ *Смежные классы разбивают кольцо.* □

Доказательство. Достаточно проверить, что различные смежные классы не пересекаются. Предположим, смежные классы элементов a, b содержат общий элемент c. Тогда в силу предыдущего свойства

$$a + J = c + J = b + J. \square$$

∘ *Пара элементов принадлежит одному смежному классу тогда и только тогда, когда их разность принадлежит идеалу.* □

∘ *Отношение «лежать в одном смежном классе» является эквивалентностью на кольце.* □

Это отношение называется *отношением сравнимости* по идеалу J.

∘ *Операции кольца индуцируют следующие операции сложения и умножения над смежными классами:*

$$(a + J) + (b + J) = (a + b) + J, (a + J) \cdot (b + J) = (ab) + J.$$

Доказательство. Необходимо проверить корректность сделанного определения. Иными словами, нужно проверить, что

$$(a + b) - (a' + b') \in J \text{ и } (ab) - (a'b') \in J, \text{ если } (a - a') \in J, (b - b') \in J.$$

Это действительно так. □

∘ *С операциями сложения и умножения, определёнными выше, смежные классы образуют кольцо.*

Это кольцо обозначается R/J и называется фактор-кольцом кольца R по идеалу J.

Доказательство. В силу определения операций над смежными классами все алгебраические соотношения, выполняющиеся между элементами кольца, продолжают выполняться, если элементы кольца, входящие в них, заменить смежными классами этих элементов. В том числе все тождества, определяющие кольцо, продолжают выполняться. □

Пример. Кольцо $\mathbb{Z}/m\mathbb{Z}$ классов вычетов целых чисел есть фактор-кольцо кольца целых чисел по идеалу $m\mathbb{Z}$, порождённому числом m.

Подкольцом кольца R называется подмножество кольца, которое само является кольцом с индуцированными на нём операциями. Иными словами, это непустое подмножество, замкнутое вычитанием и умножением.

В частности, идеал является подкольцом. Обозначим через $\mathrm{Sub}(L, R)$ множество всех подколец кольца R, включающих подкольцо L.

Теорема (о подкольцах фактор-кольца). *Для любого двустороннего идеала J кольца R существует биекция*

$$\mathrm{Sub}(J, R) \to \mathrm{Sub}(0, R/J), L \mapsto L/J.$$

Эта биекция отображает взаимно-однозначно левые (соответственно правые и двусторонние) идеалы кольца R, включающие идеал J, на левые (соответственно правые и двусторонние) идеалы фактор-кольца R/J.

Доказательство. Отображение определено корректно, так как J является двусторонним идеалом в любом подкольце L из $\mathrm{Sub}(J, L)$ и фактор-кольцо L/J является покольцом кольца R/J. Данное отображение является биекцией, так как для него существует обратное отображение

$$\mathrm{Sub}(0, R/J) \to \mathrm{Sub}(J, R), H \mapsto \cup H,$$

где $\cup H$ — объединение смежных классов, принадлежащих подкольцу $H \leqslant R/J$. Остальные условия также проверяются непосредственно. □

3. Теоремы об изоморфизмах

В этом разделе изучаются гомоморфизмы колец, устанавливается ряд канонических изоморфизмов.

Гомоморфизмы. Рассмотрим гомоморфизм колец

$$f : R \to L, a \to f(a).$$

Иными словами, отображение f согласовано со сложением и умножением:

$$f : a + b \mapsto f(a) + f(b), ab \mapsto f(a)f(b).$$

Отметим следующие свойства.

∘ Гомоморфизм нуль отображает на нуль, взаимно противоположные элементы на взаимно противоположные. Эпиморфизм единицу кольца (если она есть) отображает на единицу и (тогда) взаимно обратные элементы на взаимно обратные.

∘ Гомоморфизм подкольцо области определения отображает на подкольцо области значений. При этом левый идеал области определения отображается на левый идеал образа.

∘ Полный прообраз подкольца области значений является подкольцом области определения. Полный прообраз левого идеала является левым идеалом.

Первая теорема об изоморфизме. Полный прообраз нуля при гомоморфизме f называется его *ядром* и обозначается $\ker f$. Отметим некоторые свойства гомоморфизма.

∘ Ядро является двусторонним идеалом области определения.

Это так, поскольку оно является полным прообразом нулевого идеала.

∘ Всякий двусторонний идеал кольца является ядром некоторого гомоморфизма, действующего из этого кольца.

Действительно, для двустороннего идеала J кольца R отображение

$$\mu_J : R \to R/J, a \mapsto a + J,$$

является эпиморфизмом колец с ядром $\ker \mu_J = J$. Это отображение называется *каноническим эпиморфизмом*.

∘ Два элемента области определения тогда и только тогда имеют одинаковые образы при гомомофизме, когда они сравнимы по ядру.

Это проверяется непосредственно: пусть $f : R \to \operatorname{im} f$ — гомоморфизм колец; тогда для любых элементов a, b из области определения верно:

$$\begin{aligned} f(a) = f(b) &\Leftrightarrow f(a) - f(b) = 0 \\ &\Leftrightarrow f(a - b) = 0 \\ &\Leftrightarrow a - b \in \ker f \\ &\Leftrightarrow a + \ker f = b + \ker f. \ \square \end{aligned}$$

∘ В частности, существует биекция

$$R/\ker f \to \operatorname{im} f, a + \ker f \mapsto f(a). \ \square$$

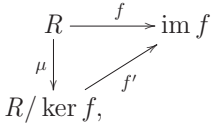
∘ Эта биекция является изоморфизмом колец.

Проверим:

$$(a + \ker f) + (b + \ker f) = (a + b) + \ker f \mapsto f(a + b) = f(a) + f(b).$$

Аналогично для умножения. Тем самым доказана

Теорема (первая об изоморфизме). *Для любого эпиморфизма* $f : R \to \operatorname{im} f$ *существует изоморфизм* $f' : R/\ker f \to \operatorname{im} f$*, такой, что коммутативна диаграмма*



где $\mu : R \to R/\ker f, a \mapsto a + \ker f$, *— кононический эпиморфизм.* $\square$

Следствие. *Гомоморфный образ кольца изоморфен фактор-кольцу по ядру гомоморфизма.* $\square$

Вторая теорема об изоморфизме. Имеет место

Теорема (вторая об изоморфизме). *Пусть H — подкольцо и K — двусторонний идеал кольца R. Тогда имеют место утверждения.*

(1) $H \cap K$ — *двусторонний идеал кольца* R.

(2) $H + K = \{a + b | a \in H, b \in K\}$ — *подкольцо кольца* R.

(3) K — *двусторонний идеал кольца* $H + K$.

(4) *Существует изоморфизм*

$$H/(H \cap K) \to (H + K)/K, h + (H \cap K) \mapsto h + K.$$

Доказательство. Рассмотрим гомоморфизм колец

$$f : R \to \operatorname{im} f, a \mapsto f(a)$$

с ядром K. Его ограничение

$$f_H : H \to \operatorname{im} f, h \mapsto f(h)$$

является гомоморфизмом с ядром $H \cap K$. Имеет место изоморфизм

$$f'_H : H/(H \cap K) \to \operatorname{im} f_H, h + (H \cap K) \mapsto f(h).$$

Полный прообраз кольца $\operatorname{im} f_H$ в кольце R при гомоморфизме f совпадает с множеством $H + K$ и можно рассмотреть ограничение f_{H+K}. Его ядро совпадает с идеалом K и имеет место изоморфизм

$$f'_{H+K} : (H + K)/K \to \operatorname{im} f_H, h + K \mapsto f(h).$$

Тогда композиция $f'_H (f'_{H+K})^{-1}$ является изоморфизмом, о существовании которого говорится в теореме. □

Третья теорема об изоморфизме. Имеет место

Теорема (об эпиморфизме). *Пусть $f : R \to L$ — эпиморфизм колец с ядром K и J — двусторонний идеал кольца R, такой, что $J \leqslant K$. Тогда существует единственное отображение $f' : R/J \to L$, такое, что коммутативна диагарамма*

$$\begin{array}{ccc} R & \xrightarrow{f} & \operatorname{im} f \\ {\scriptstyle \mu_J}\downarrow & \nearrow_{f'} & \\ R/J & & \end{array}$$

Отображение f' является эпиморфизмом колец с ядром K/J.

Доказательство. Если отображение f' существует, то оно определено однозначно, как

$$f' : R \to R/J, a \mapsto a + J.$$

С другой строны, записанное выражение можно использовать как определение. Это определение корректно, так как J содержится в ядре гомоморфизма f. Оставшиеся свойства проверяются непосредственно. $\square$

Первая теорема об изоморфизме является следствием данной теоремы. Ещё одним следствием является

Теорема (третья об изоморфизме). *Пусть J и K — двусторонние идеалы кольца R, такие, что $J \leqslant K$. Тогда существует изоморфизм*

$$(R/J)/(K/J) \cong R/K.$$

Доказательство. Нужно в условиях предыдущей теоремы применить первую теорему об изоморфизме к гомоморфным образам $\operatorname{im} f = \operatorname{im} f'$. $\square$

4. Прямые суммы

В этом разделе изучается конструкция прямой суммы колец.

Внешняя прямая сумма. Пусть заданы кольца $R_1, \ldots, R_n$. Их декартово произведение является кольцом с покомпонентным сложением и умножением наборов. Это кольцо называется (внешней) *прямой суммой* колец R_k и обозначается

$$R_1 \oplus \ldots \oplus R_n.$$

Для любого k, такого, что $1 \leqslant k \leqslant n$, положим

$$\overline{R}_k = \{(0, 0, \ldots, 0, a, 0, \ldots, 0) | a \text{ находится в } k\text{-ой позиции и } a \in R_k\}.$$

Пусть $R = R_1 \oplus \ldots \oplus R_n$. Отметим, что для множеств $\overline{R}_1, \ldots, \overline{R}_n$ выполняются следующие условия.

(1) Множества $\overline{R}_1, \ldots, \overline{R}_n$ являются двусторонними идеалами в R.

(2) Имеет место равенство

$$R = \overline{R}_1 + \ldots + \overline{R}_n.$$

Иными словами, каждый элемент кольца R является суммой элементов, выбранных из подколец $\overline{R}_1, \ldots, \overline{R}_n$.

(3) Каждый элемент кольца R можно представить единственным образом в виде суммы элементов, выбранных последовательно из подколец $\overline{R}_1, \ldots, \overline{R}_n$.

(4) Имеют место равенства

$$\overline{R}_k \cap \sum_{j \neq k} \overline{R}_j = 0, 1 \leqslant k \leqslant n.$$

(5) Произведение элементов, выбранных последовательно из различных подколец $\overline{R}_1, \ldots, \overline{R}_n$, равно нулю.

Внутренняя прямая сумма. Пусть теперь R — произвольное кольцо. Оно называется *внутренней прямой суммой* подколец $R_1, \ldots, R_n$, если имеется изоморфизм

$$R_1 \oplus \ldots \oplus R_n \to R, (a_1, \ldots, a_n) \mapsto a_1 + \ldots + a_n.$$

Подкольца $R_1, \ldots, R_n$ являются изоморфными образами подколец $\overline{R}_1, \ldots, \overline{R}_n$ при этом изоморфизме. Для них выполняются записанные выше условия (1–5). (Следует заменить $\overline{R}_1, \ldots, \overline{R}_n$ на $R_1, \ldots, R_n$ в формулировках условий.) Данные условия являются необходимыми для того, чтобы кольцо R было прямой суммой подколец R_i. Они являются также и достаточными, так как имеют место следующие теоремы.

Теорема. *Кольцо R является прямой суммой подколец $R_1, \ldots, R_n$, если выполняются условия (3,5), где $\overline{R}_1, \ldots, \overline{R}_n$ следует заменить на $R_1, \ldots, R_n$.*

Доказательство. Отображение

$$R_1 \oplus \ldots \oplus R_n \to R, (a_1, \ldots, a_n) \mapsto a_1 + \ldots + a_n,$$

является биекцией в силу третьего условия и изоморфизмом в силу пятого. □

Теорема. *Кольцо R является прямой суммой подколец $R_1, \ldots, R_n$, если выполняются условия (1,2,4), где $\overline{R}_1, \ldots, \overline{R}_n$ следует заменить на $R_1, \ldots, R_n$.*

Доказательство. Предположим, что в условиях теоремы выполняется равенство $\sum_k a_k = \sum_k b_k$. Тогда $a_n - b_n = \sum_{k<n}(b_k - a_k)$. Этот элемент принадлежит множеству $\overline{R}_n \cap \sum_{k<n} \overline{R}_k = 0$. Следовательно, $a_n = b_n$. Аналогично, $a_k = b_k$ для любого k. Таким образом, выполняется третье условие. Так как пятое условие следует из первого с третьим, теорема доказана. □

Упражнение. Условие (4) в этой теореме можно заменить на

(4') Для любого $k, 2 \leqslant k \leqslant n$, имеет место равенство

$$\overline{R}_k \cap \sum_{j<k} \overline{R}_j = 0.$$

Теорема. *Кольцо R является прямой суммой подколец $R_1, \ldots, R_n$, если выполняются условия (1,3), где $\overline{R}_1, \ldots, \overline{R}_n$ следует заменить на $R_1, \ldots, R_n$.*

Доказательство. Достаточно проверить, что выполняется пятое условие. Это действительно так (убедитесь). □

Пример. Пусть a, b — взаимно простые целые числа. Тогда:

$$\mathbb{Z}/ab\mathbb{Z} = b\mathbb{Z}/ab\mathbb{Z} \oplus a\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}.$$

Отсюда следует, что имеет место разложение

$$\mathbb{Z}/p_1^{l_1}\cdots p_n^{l_n}\mathbb{Z} \simeq \mathbb{Z}/p_1^{l_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_n^{l_n}\mathbb{Z},$$

если p_k — различные простые и l_k — целые положительные числа.

Упражнение. Кольцо назовём неразложимым, если его невозможно представить в виде прямой суммы нетривиальных подколец. Проверьте, что кольцо $\mathbb{Z}/p^l\mathbb{Z}$, где p — простое, является неразложиммым.

Разложение кольца с единицей. Пусть R — кольцо с единицей, разлагающееся в прямую сумму подколец $R_1, \ldots, R_n$. Тогда единицу можно представить единственным образом в виде суммы

$$1 = e_1 + \ldots + e_n,$$

где слагаемые принадлежат соответствующим подкольцам. Легко проверяются следующие условия:

- элементы e_k перестановочны со всеми элементами кольца R;

(элементы кольца с этим свойством будем называть *центральными*;)

- $e_k e_k = e_k$;

(такие элементы называются *идемпотентами*; в том числе, элементы $0, 1$ называются *тривиальными* идемпотентами;)

- $e_k e_l = 0$, если $k \neq l$.

(такие элементы называются *ортогональными*;)

- $R_k = e_k R$;
- $R_k \in \{0, R\}$, если $e_k \in \{0, 1\}$.

Здесь l, k — произвольные целые числа, такие, что $1 \leqslant k, l \leqslant n$.

Теорема. *Кольцо с единицей тогда и только тогда разлагается в прямую сумму из n нетривиальных подколец, когда в нём единица разлагается в сумму из n центральных, попарно ортогональных нетривиальных идемпотентов.*

Доказательство. Нужно доказать достаточность. Пусть R — кольцо с единицей, содержащее n центральных, попарно ортогональных идемпотентов $e_1, \ldots, e_n$, дающих в сумме единицу. Так как элементы e_k центральные, множества $e_k R$ являются идеалами. Поскольку 1 разлагается в сумму этих элементов, произвольный элемент a из кольца R можно представить в виде

$$a = e_1 a + \ldots + e_n a.$$

Далее, если элемент a принадлежит пересечению $e_nR \cap \sum_{k<n} e_kR$, то имеет место равенство

$$a = e_n a_n = \sum_{k<n} e_k a_k$$

для некоторых элементов $a_1, \ldots, a_n$, откуда умножением на e_n получаем $a_n e_n = 0$ и $a = 0$. Таким образом, равенство

$$e_k R \cap \sum_{j \neq k} e_j R = 0$$

выполняется при $k = n$. Аналогично проверяется, что это равенство имеет место при любом k. Таким образом, кольцо R является прямой суммой идеалов e_kR. Эти идеалы нетривиальны. Действительно, очевидно, они ненулевые. Если же $R = e_kR$, то $1 = e_k a$ для некоторого a. Тогда $e_l = 0$ для $l \neq k$. Следовательно, $n = 1$ и $e_k = 1$ — противоречие. □

Следствие. *Кольцо с единицей тогда и только тогда разлагается в прямую сумму двух нетривиальных подколец, когда оно содержит нетривиальный центральный идемпотент.*

Доказательство. Пусть e — нетривиальный центральный идемпотент. Тогда элемент $1 - e$ также является нетривиальным центральным идемпотентом. По теореме кольцо разлагается в прямую сумму двух нетривиальных подколец. □

Пример. Пусть a, b — взаимно простые целые числа, s, t — коэффициенты Безу, такие, что

$$as + bt = 1.$$

Тогда

$$(as)^2 = as(1 - bt) \equiv as \mod ab$$

и имеет место разложение

$$\mathbb{Z}/ab\mathbb{Z} = (as)(\mathbb{Z}/ab\mathbb{Z}) \oplus (bt)(\mathbb{Z}/ab\mathbb{Z}).$$

Упражнение. Проверьте, что тогда также имеют место изоморфизмы

$$\mathbb{Z}/b\mathbb{Z} \cong (as)(\mathbb{Z}/ab\mathbb{Z}),$$
$$\mathbb{Z}/a\mathbb{Z} \cong (bt)(\mathbb{Z}/ab\mathbb{Z}).$$

Китайская теорема об остатках. Имеет место

Теорема (китайская об остатках). *Пусть R — коммутативное кольцо с единицей и $R_1, \ldots, R_n$ — идеалы в нём, такие, что $R_k + R_l = R$ при $1 \leqslant k < l \leqslant n$. Тогда в кольце R для любых элементов $a_1, \ldots, a_n$ найдётся элемент a, такой, что*

$$a \equiv a_1 \mod R_1, \ldots, a \equiv a_n \mod R_n.$$

Идеалы R_k в условиях теоремы называются (попарно) *взаимно простыми.*

Доказательство. При $n = 2$ имеем $1 = u_1 + u_2$ для некоторых элементов u_1, u_2 из соответствующих идеалов R_1, R_2. Тогда для элемента $a = a_2u_1 + a_1u_2$ верно:

$$\begin{aligned} a &= a_2u_1 + a_1(1 - u_1) \equiv a_1 \mod R_1, \\ &= a_2(1 - u_2) + a_1u_2 \equiv a_2 \mod R_2. \end{aligned}$$

Таким образом, теорема верна при $n = 2$. Предположим, что $n > 2$. Для каждого $k, 1 < k \leqslant n$, выберем элементы u_k, v_k в соответствующих идеалах R_1, R_k, такие, что $1 = u_k + v_k$. Тогда

$$1 = \prod_k (u_k + v_k) = u_2 \cdots u_n + \ldots + v_2 \cdots v_n \in R_1 + R_2 \cap \cdots \cap R_n.$$

Таким образом, идеалы R_1 и $R_2 \cap \cdots \cap R_n$ — взаимно простые. Следовательно, при $k = 1$ существует элемент b_k, такой, что

$$b_k \equiv 1 \mod R_k, \text{ и } b_k \equiv 0 \mod R_l \text{ для } l \neq k.$$

Очевидно, элементы с этим свойством должны существовать при любом k. Тогда для завершения доказательства нужно взять

$$a = a_1b_1 + \ldots a_nb_n. \quad \square$$

Следствие. *В условиях теоремы отображение*

$$R \to R/R_1 \oplus \ldots \oplus R/R_n, a \to ([a], \ldots [a])$$

является эпиморфизмом и имеет место изоморфизм колец

$$R/R_1 \cap \ldots \cap R_n \to R/R_1 \oplus \ldots \oplus R/R_n, [a] \to ([a], \ldots [a]). \quad \square$$

Пример. Пусть a, b — взаимно простые целые числа. Тогда идеалы $a\mathbb{Z}$ и $b\mathbb{Z}$ также взаимно простые и имеет место равенство $ab\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. Снова получаем разложение:

$$\mathbb{Z}/ab = \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/a\mathbb{Z}.$$

ГЛАВА 22

Теория делимости

В этой главе изучается теория делимости в целостном кольце.

1. Простые и неприводимые элементы

Введём основные понятия теории делимости.

Максимальные и простые идеалы. Пусть J — идеал целостного кольца R, причём $J \neq R$. Отметим ряд свойств.

∘ *Следующие условия равносильны.*

(1) *Для любых элементов a и b из R верна импликация:*

$$a \in J \text{ или } b \in J, \text{ если } ab \in J.$$

(2) *Фактор-кольцо R/J — целостное.*

Доказательство. Это так в силу определения целостного кольца. □

∘ *Следующие условия равносильны.*

(1) *Идеал J максимальный по включению среди собственных идеалов.*

(2) *Фактор-кольцо R/J является полем.*

Доказательство. Это так в силу теоремы об идеалах фактор-кольца. □

∘ *Максимальный идеал является простым.*

Доказательство. Это так, поскольку поле является целостным кольцом. □

Примеры. В кольце целых чисел идеал, порождённый простым числом, максимальный. В кольце многочленов над полем идеал, порождённый неприводимым многочленом, максимальный. В этих кольцах простыми являются максимальные идеалы и нулевой идеал.

Делимость и ассоциированность. Будем говорить, что элемент a является *делителем* элемента b, или a *делит* b, если в кольце R для некоторого элемента c выполняется равенство $ac = b$. Это равносильно тому, что для главных идеалов выполняется включение $bR \subseteq aR$. В этой ситуации пишем $a|b$. Отношение делимости рефлексивно и транзитивно.

Элементы a, b называются *ассоциированными*, если каждый из них является делителем другого; это равносильно тому, что элементы отличаются обратимым множителем и равносильно равенству $aR = bR$.

Отношение ассоциированности является эквивалентностью и отношение делимости индуцирует порядок на классах этой эквивалентности.

Элемент a называется *наибольшим общим делителем* набора элементов $a_0, a_1, \ldots$, если выполнены условия:

(1) a является общим делителем этих элементов, то есть соотношение $a|a_k$ выполняется для всех k;

(2) всякий общий делитель этих элементов является делителем элемента a, то есть $b|a$, если для всех k выполняется соотношение $b|a_k$.

Наибольший общий делитель, если существует, отпределён с точностью до ассоциированности, тем не менее будем писать $a = \gcd(a_0, a_1, \ldots)$ в этом случае; равенство в подобных ситуациях следует понимать как ассоциированность.

Простота и неприводимость. В кольце R отличный от нуля и необратимый элемент p называется *простым*, если в R для любых элементов a, b выполняется импликация:

$$p|a \text{ или } p|b, \text{ если } p|ab.$$

Это равносильно тому, что идеал pR — простой в R. Элемент p называют *неприводимым*, если любой его делитель обратим или ассоциирован с ним, то есть для любых элементов a, b выполняется импликация:

$$p \in R^\times \text{ или } p \in R^\times, \text{ если } p = ab.$$

Это равносильно тому, что идеал pR максимальный по включению среди главных идеалов, отличных от всего кольца R. Отметим следующее свойство простых элементов.

∘ *Простые элементы неприводимы.*

Доказательство. Пусть $p = ab$ — простой элемент. Тогда $p|a$ или $p|b$. В первом случае, $p \sim a$ и тогда b обратим. Во втором случае обратим a. □

Разложение на множители. Соотношение

$$a = p_1 \cdots p_n,$$

имеющее место в кольце R, называется *разложением* элемента a *на простые* (соответственно *неприводимые*) *множители*, если все элементы p_k — простые (соответственно неприводимые).

Теорема о разложении на простые множители. *В целостном кольце для любого элемента разложение на простые множители, если существует, единственно с точностью до порядка сомножителей и их ассоциированности.*

Доказательство. Предположим, что

$$p_1 \cdots p_n \sim q_1 \cdots q_s$$

— два разложения на простые множители. Тогда p_1 делит некоторый из элементов q_k и тогда ассоциирован с ним. Будем считать, что $k = 1$ (этого можно добиться, поменяв порядок сомножителей при необходимости). В результате сокращения получаем

$$p_2 \cdots p_n \sim q_2 \cdots q_s.$$

Продолжая в том же духе для $p_2, p_3 \ldots$, получаем, что $n = s$ и $p_k \sim q_k$ для всех k. □

2. Область с однозначным разложением

Целостное кольцо R называется *областью с разложением*, или ОР, если в нём все необратимые элементы кроме нуля имеют разложение на неприводимые множители. Оно называется *областью с однозначным разложением*, или ООР, если дополнительно в нём любое разложение на неприводимые множители единственно с точностью до порядка сомножителей и их ассоциированности.

Теорема о разложении на неприводимые множители. *Пусть R — область с разложением. Следующие условия равносильны.*

(1) *R является областью с однозначным разложением.*

(2) *В R неприводимые элементы просты.*

Доказательство. Пусть в области с однозначным разложением для неприводимого элемента p выполняется соотношение $p|ab$. Иными словами, для некоторого элемента c выполняется равенство $pc = ab$. В этом равенстве запишем элементы a, b, c в виде произведения неприводимых множителей. В силу единственности разложения на неприводимые множители элемент p ассоциирован с некоторым неприводимым множителем справа и тогда $p|a$ или $p|b$. Тогда элемент p — простой и из первого условия следует второе. Из второго условия следует первое, так как разложение на простые множители единственно. □

Область главных идеалов. Целостное кольцо R называется *областью главных идеалов*, или ОГИ, если в нём каждый идеал — главный, то есть имеет вид aR для некоторого элемента a.

Примеры. Кольцо целых чисел, кольцо многочленов над полем, кольцо целых p-адических чисел (где p — простое) и кольцо степенных рядов над полем являются областями главных идеалов.

Имеет место

Теорема (о разложении в ОГИ). *Область главных идеалов является областью с однозначным разложением на неприводимые множители.*

Доказательство теоремы разобьём на три части.

1. *Пусть p — отличный от нуля необратимый элемент области главных идеалов R. Тогда следующие условия равносильны.*

(I) *Элемент p неприводимый.*

(II) *Идеал pR максимальный.*

(III) *Идеал pR простой.*

Из первого условия второе следует по определению неприводимого элемента. Из второго третье следует, так как поле является целостным кольцом. Из третьего следует первое в силу доказанного ранее свойства простых элементов.

2. *В области с однозначным разложением не существует бесконечной строго возрастающей цепи идеалов.*

Объединение возрастающей цепи идеалов является идеалом. Этот идеал главный и порождается некоторым элементом. Этот элемент содержится в некотором идеале цепи. Этот идеал совпадает с объединением всей цепи. Таким образом цепь стабилизируется.

3. *Область главных идеалов является областью с разложением.*

Пусть a — ненулевой необратимый элемент области главных идеалов R. Докажем, что он обладает разложением на неприводимые множители. Если он неприводим, то доказывать нечего, в противном случае существует разложение $a = a_1 a_2$, где $aR \subset a_1 R$ и $aR \subset a_2 R$. Если какой-то из элементов a_k не является неприводимым, то разложим его как $a_k = a_{k1} a_{k2}$ и т. д. Данный процесс заканчивается после некоторого количества шагов разложением на неприводимые множители для элемента a, так как иначе существует бесконечная последовательность элементов $a_k, a_{kl}, a_{klr}, \ldots$, не имеющих разложения, и тогда существует бесконечная строго возрастающая цепь идеалов $a_k R \subset a_{kl} R \subset a_{klr} R \subset \ldots$, что противоречит доказанному во второй части.

Доказательство теоремы получается теперь по теореме об однозначном разложении в силу доказанного в первой и третьей частях. $\square$

Теорема (о нод в ОГИ). *В области главный идеалов для любых элементов $a_1, \ldots, a_n$ существуют элементы $d, s_1, \ldots, s_n$, такие, что*

$$\begin{aligned} d &= \gcd(a_1, \ldots, a_n) \\ &= a_1 s_1 + \ldots + a_n s_n. \end{aligned}$$

Доказательство. Легко проверяется, что элемент d, такой, что

$$dR = a_1R + \ldots + a_nR$$

является наибольшим общим делителем элементов a_k. Тогда и элементы s_k с нужным свойством тоже существуют.

Элементы s_k, о которых говорится в теореме, называются *коэффициентами Безу* для набора элементов a_k.

Следствие. *Пусть a — ненулевой и необратимый элемент области главных идеалов R. Класс $b+aR$ обратим в кольце R/aR, если и только если* $\gcd(a,b) = 1$. □

Евклидова область. Целостное кольцо R называется *евклидовой областью*, или ЕО, если существует функция $\lambda : R \setminus 0 \to \mathbb{N}$ и в R для любых элементов a, b, таких, что $b \neq 0$, существует пара элементов q, r, таких, что

$$a = bq + r, r = 0 \text{ или } \lambda(r) < \lambda(b).$$

Функция λ называется *евклидовой нормой*.

Примеры. Кольцо целых чисел и кольцо многочленов над полем от одной переменной являются евклидовыми областями.

Упражнение. Проверьте, что кольцо

$$\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$$

целых гауссовых чисел евклидово с евклидовой нормой

$$\mathrm{nr} : a + ib \mapsto a^2 + b^2.$$

Проверьте также, что евклидовыми являются кольца

$$\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b | a, b \in \mathbb{Z}\},$$
$$\mathbb{Z}[\sqrt{-2}] = \{a + \sqrt{-2}b | a, b \in \mathbb{Z}\}.$$

Теорема. *Евклидова область является областью главных идеалов.*

Доказательство. Пусть J — ненулевой идеал евклидовой области R и b — его ненулевой элемент с минимально возможным значением $\lambda(b)$. Достаточно показать, что $J \subseteq bR$, так как обратное включение очевидно выполняется. С этой целью произвольный элемент a из J запишем в виде $a = qb + r$, где $r = 0$ или $\lambda(r) < \lambda(q)$. Заметим, что элемент $r = a - bq$ принадлежит идеалу J вслед за элементами a, b. Тогда в силу выбора элемента b выполняется равенство $r = 0$. Теорема доказана. □

В частности, из доказанной теоремы следует, что евклидова область является областью с однозначным разложением, в ней существуют наибольшие общие делители и коэффициенты Безу.

Для вычисления наибольшего общего делителя и коэффициентов Безу в евклидовой области существует эффективный алгоритм, который называется (расширенным) алгоритмом Евклида. Он основывается на следующей теореме и её следствии.

Теорема (алгоритм Евклида). *Пусть в евклидовой области R элементы $a_0, \ldots, a_{n+1}$ и $q_1, \ldots, q_n$ обладают свойствами:*

(1) $a_{k-1} = a_k q_k + a_{k+1}$ *для всех k, таких, что $1 \leqslant k \leqslant n$;*

(2) $\lambda(a_{k+1}) < \lambda(a_k)$ *для $1 \leqslant k \leqslant n$;*

(3) $a_{n+1} = 0$;

Тогда $a_{n-1} = \gcd(a_0, a_1)$.

Доказательство. Легко проверяются равенства

$$\gcd(a_0, a_1) = \gcd(a_1, a_2) = \ldots = \gcd(a_n, a_{n+1}) = \gcd(a_n, 0) = a_n. \square$$

Следствие (расширенный алгоритм Евклида). *Пусть в условиях теоремы имеют место равенства*

$$s_0 = 1, t_0 = 0,$$

$$s_1 = 0, t_1 = 1,$$

а также

$$s_{k+1} = s_{k-1} - s_k q_k,$$

$$t_{k+1} = t_{k-1} - t_k q_k,$$

для всех k, таких, что $1 \leqslant k \leqslant n$. Тогда для тех же значений k верны равенства $a_k = a_0 s_k + a_1 t_k$.

Доказательство. Индукция по k. $\square$

3. Нётерово кольцо

Пусть R — коммутативное кольцо. В нём идеал J называется конечно порождённым, если для некоторого конечного множества A его элементов $a_1, \ldots, a_n$ выполняется равенство

$$J = (a_1, \ldots, a_n).$$

Множество A называется *базисом* идеала J. Имеет место

Теорема. *Пусть R — коммутативное кольцо. Следующие условия равносильны.*

(1) *Всякий идеал кольца R конечно порождён.*

(2) *Не существует бесконечной строго возрастающей последовательности идеалов кольца R.*

(3) *В любом непустом множестве идеалов кольца R имеется максимальный по включению идеал.*

Доказательство. Пусть выполнено первое условие и имеется возрастающая последовательность идеалов

$$J_0 \subseteq J_1 \subseteq \dots.$$

Заметим, что объединение этой последовательности также является идеалом. В силу первого условия этот идеал конечно порождён, то есть для некоторых элементов $a_1, \dots, a_n$ кольца выполняется равенство

$$\cup_k J_k = (a_1, \dots, a_n).$$

Элементы $a_1, \dots, a_n$ содержатся в некотором идеале J_k и тогда последовательность идеалов стабилизируется

$$J_k = J_{k+1} = \dots = \cup_k J_k.$$

Тем самым, выполняется второе условие.

Предположим, что выполянется второе условие и X — непустое множество идеалов. В множестве X выберем произвольно иделал J_0. Если он не максимальный, то выберем идеал J_1, такой, что $J_0 \subset J_1$ и т. д. Так как бесконечной строго возрастающей цепи идеалов не существует, на каком-то шаге будет найден максимальный идеал. Таким образом, верно третье условие.

Предположим, что выполнено третье условие и J — произвольный идеал кольца R. Заметим, что максимальный идеал в множестве всех конечно порождённых идеалов, включённых в идеал J, совпадает с ним. Таким образом, идеал J конечно порождён. Теорема доказана. □

Кольцо, для которого выполняются условия (1–3) из теоремы, называется *нётеровым.*

Теорема (Гильберта о базисе). *Кольцо многочленов над нётеровым кольцом нётерово.*

Доказательство. Пусть кольцо R нётерово и J — идеал в кольце многочленов $R[x]$. Заметим, что старшие коэффициенты многочленов из J, степень, которых не превосходит натурального числа n, при добавлении нуля образуют идеал в кольце R; обозначим его A_n. Пусть элементы $a_{n,1}, \dots, a_{n,m_n}$ образуют базис данного идеала и являются страшими коэффициентами многочленов $f_{n,1}, \dots, f_{n,m_n}$ степени n из J.

Идеалы A_n образуют возрастающую последовательность, которая стабилизируется, пусть A_r — наибольший идеал этой последовательности. Обозначим через J' идеал кольца многочленов, порождённый многочленами $f_{n,l}$, где $1 \leqslant n \leqslant r$ и $1 \leqslant l \leqslant m_n$. Покажем, что $J = J'$. Достаточно доказать включение $J \subseteq J'$, так как обратное влючение очевидно выполняется. С этой целью в идеале J выберем многочлен f степени n,

предположив, по-индукции, что многочлены меньшей степени принадлежат J'. Пусть $n < r$ и старший коэффициент многочлена f выражается комбинацией

$$\sum_l a_{n,l} b_l$$

для некоторых элементов b_l из R (здесь $1 \leqslant l \leqslant m_n$). Тогда многочлен

$$g = f - \sum_l f_{n,l} b_k$$

принадлежит J' по предположению индукции (так как имеет степень, меньшую n и принадлежит идеалу J). Но тогда и многочлен f должен принадлежать J'. Если $n \geqslant r$ и старший коэффициент равен $\sum_l a_{r,l} b_l$, то надо рассмотреть многочлен $g = f - x^{n-r} \sum_l f_{r,l} b_l$. Теорема доказана. □

4. Разложение в кольце многочленов

В этом разделе изучаются вопросы, связанные с разложением на неприводимые множители в кольце многочленов над областью с однозначным разложением.

Теорема Гаусса о факториальности. Имеет место

Теорема (Гаусса о факториальности). *Кольцо многочленов над областью с однозначным разложением является областью с однозначным разложением.*

Докажем ряд вспомогательных утверждений.

Содержанием многочлена f с коэффициентами в области с однозначным разложением назовём наибольший общий делитель его коэффициентов. Обозначим содержание через $\operatorname{cont} f$. Как и наибольший общий делитель содержание определено с точностью до ассоциативности; оно совпадает (с точностью до ассоциативности) с константой c, такой, что для некоторого многочлена f_1 с содержанием единица выполняется равенство $f = cf_1$. Имеет место

Лемма (Гаусса о содержании). *Произведение многочленов с содержанием единица над областью с однозначным разложением является многочленом с содержанием единица.*

Доказательство. Пусть $f = \sum_k a_k x^k$ и $g = \sum_k b_k x^k$ — многочлены с содержанием 1, p — простой (неприводимый) элемент области R и m, l — наименьшие натуральные числа, такие, что коэффициенты a_m и b_l не делятся на p. Коэффициент многочлена fg, стоящий при x^{m+l}, равен

$$a_m b_l + a_{m-1} b_{l+1} + a_{m-2} b_{l+2} + \ldots + a_{m+1} b_{l-1} + a_{m+2} b_{l-2} + \ldots.$$

Как видно, он не делится на p. Таким образом, не все коэффициенты многочлена fg делятся на p. Так как p — произвольный неприводимый элемент области R, содержание многочлена fg равно единице. $\square$

Следствие 1. *Содержание произведения двух многочленов над областью с однозначным разложением равно произведению их содержаний.*

Доказательство. Запишем многочлены f и g в виде

$$f = \operatorname{cont}(f) f_1, g = \operatorname{cont}(g) g_1,$$

где f_1 и g_1 — многочлены с содержанием 1. Тогда

$$fg = \operatorname{cont}(f) \operatorname{cont}(g) f_1 g_1 \text{ и } \operatorname{cont}(fg) = \operatorname{cont}(f) \operatorname{cont}(g),$$

поскольку $\operatorname{cont}(f_1 g_1) = 1$. $\square$

Следствие 2. *Пусть f — многочлен с коэффициентами в области с однозначным разложением R. Тогда, если он разлагается над полем частных кольца R в произведение многочленов положительной степени, то он разлагается подобным образом уже над R.*

Доказательство. Пусть многочлен f с коэффициентами в области R с однозначным разложением разлагается над полем частных как $f = gh$. Тогда над R имеет место разложение

$$abf = (ag)(bh),$$

где a, b — некоторые элементы из R, ag, bh — многочлены с коэффициентами в R. Заметим, что всякий неприводимый делитель произведения ab является делителем содержания какого-то из многочленов ag или bh в силу предыдущего следствия и можно произвести сокращение в записанном соотношении на такой неприводимый элемент. С учётом этого можно считать, что $a = b = 1$. $\square$

Следствие 3. *Пусть R — область с однозначным разложением. Тогда неприводимыми элементами кольца $R[x]$ являются в точности неприводимые элементы из R (рассматриваемые как многочлены нулевой степени) и многочлены с содержанием единица, не разлагающиеся в произведение многочленов положительной степени (то есть неприводимые над полем частных кольца R).* $\square$

Доказательство теоремы Гаусса. Кольцо $R[x]$ является областью с разложением: чтобы разложить многочлен f на неприводимые множители, следует содержание $\operatorname{cont}(f)$ разложить в кольце R, многочлен $f / \operatorname{cont}(f)$ разложить в кольце $R[x]$. Покажем, что разложение на неприводимые множители единственно. Пусть имеется два разложения:

$$a_1 \cdots a_n \cdot f_1 \cdots f_m = b_1 \cdots b_{n'} \cdot g_1 \cdots g_{m'},$$

где $a_l, b_{l'}$ — неприводимые константы из R и $f_k, g_{k'}$ — многочлены с коэффициентами в кольце R, неприводимые над его полем частных. В силу леммы Гаусса имеет место разложение для содержания:

$$a_1 \cdots a_n = b_1 \cdots b_{n'}.$$

Это равенство выполняется с точностью до ассоциированности, но можно считать его точным. В силу единственности разложения в кольце R, имеем $n = n'$ и $a_k \sim b_k$ при надлежащей перенумерации элементов. Далее, в результате сокращения получаем

$$f_1 \cdots f_m = g_1 \cdots g_{m'}.$$

Это разложение имеет место над кольцом R, но также является разложением на неприводимые множители над его полем частных. В силу единственности разложения в кольце многочленов над полем имеем $m = m'$ и $f_k \sim g_k$ при некоторой перенумерации многочленов. Данное соотношение ассоциированности, выполняющееся над полем частных кольца R, имеет место и над кольцом R, в чём легко убедиться. □

Разложение в конечное число шагов. Пусть $f(x)$ — многочлен положительной степени с коэффициентами в области с однозначным разложением R. Требуется разложить его над кольцом R в произведение многочленов положительной степени либо установить, что такого разложения не существует (когда f неприводим над полем частных $Q = \operatorname{Frac} R$ кольца R). Оказывается, сформулированная задача может быть решена за конечное число шагов. Опишем *метод Кронекера* решения этой задачи. Он опирается на следующие очевидные замечания.

∘ Если многочлен $f(x)$ разлагается, то степень какого-то из сомножителей не более k, где $k = \lfloor n/2 \rfloor$. □

Итак, будем искать в кольце $R[x]$ делитель $g(x)$ многочлена $f(x)$ степени k или менее.

∘ Пусть $a_0, \ldots, a_k$ различные элементы кольца R. Многочлен $g(x)$ степени, не превосходящей k, однозначно определяется по значениям $b_0 = g(a_0), \ldots, b_k = g(a_k)$. □

∘ Пусть $c_0 = f(a_0), \ldots, c_k = f(a_k)$. Если в кольце $R[x]$ выполняется соотношение $g(x)|f(x)$, то в кольце R выполняется ряд соотношений $b_0|c_0 \ldots, b_k|c_k$. □

В связи со сделанными наблюдениями корректным является следующий

Метод Кронекера разложения в конечное число шагов.

1. Выберем в R различные элементы $a_0, \ldots, a_k$.
2. Вычислим значения $c_0 = f(a_0), \ldots, c_k = f(a_k)$.

3. Выберем в R очередной набор $b_0, \ldots, b_k$, где $b_0 | c_0, \ldots, b_k | c_k$.

4. В кольце $Q[x]$, где $Q = \mathrm{Frac}(R)$, найдём многочлен $g(x)$ степенеи, не превосходящей k, такой, что $b_0 = g(a_0), \ldots, b_k = g(a_k)$.

5. В кольце $Q[x]$ разделим многочлен $f(x)$ на многочлен $g(x)$ с остатком, то если найдём разложение

$$f(x) = g(x)h(x) + r(x), \text{ где } r(x) = 0 \text{ или } \deg r(x) < \deg g(x).$$

6. Задача решена, если остаток $r(x)$ нулевой и многочлены $g(x), h(x)$ принадлежат кольцу $R[x]$.

7. Возвращаемся к шагу 3, если это не так.

8. Разложения не существует, если оно не было найдено, но все наборы делителей на шаге 3 исчерпаны.

Признаки неприводимости. Пусть R — область с однозначным разложением и $Q = \mathrm{Frac}(R)$ — её поле частных. Зададимся вопросом: как убедиться, что многочлен $f(x)$ положительной степени с коэффициентами в кольце R не разлагается над ним в произведение многочленов положительной степени, то есть является неприводимым над полем Q? (Такой многочлен является неприводимым и над кольцом R, если имеет содержание 1). Имеет место

Критерий Эйзенштейна. *Пусть p — простой элемент области с однозначным разложением R. Многочлен*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

не разлагается над кольцом R в произведение многочленов положительной степени, если выполнены условия:

(1) $a_n \not\equiv 0 \mod p$;

(2) $a_i \equiv 0 \mod p$ *для всех* i, *таких, что* $0 \leqslant i \leqslant n-1$;

(3) $a_0 \not\equiv 0 \mod p^2$.

Доказательство. Предположим, что многочлен $f(x)$ обладает записанными свойствами и является произведением многночленов

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots + b_0,$$
$$h(x) = c_k x^k + c_{k-1} x^{k-1} + \ldots + c_0.$$

положительных степеней m, k. Заметим, что $a_0 = b_0 c_0$. В силу второго и третьего условий для многочлена $f(x)$ элемент p делит один и только один из коэффициентов b_0, c_0. Пусть этим коэффициентом является b_0.

Поскольку p делит элементы $a_1, \ldots, a_m$, из соотношений

$$a_1 = b_0c_1 + b_1c_0,$$
$$a_2 = b_0c_2 + b_1c_1 + b_2c_0,$$
$$\ldots$$
$$a_m = b_0c_m + \ldots + b_mc_0,$$

получаем последовательно, что p делит элементы $b_1, \ldots, b_m$ и тогда делит все коэффициенты многочлена $g(x)$. Это противоречит первому условию для многочлена $f(x)$. $\square$

Примеры.

$\circ$ Многочлен $x^2 - 2$ неприводим над полем рациональных чисел. Число $\sqrt{2}$, следовательно, иррациональное.

$\circ$ Пусть p — простое число. Покажем, что многочлен

$$f(x) = x^{p-1} + \ldots + x^0$$

неприводим над полем рациональных чисел. Критерий Эйзенштейна не применим к этому многочлену. Но он применим к многочлену $f(x+1)$. Действительно, заметим, что

$$f(x) = (x^p - 1)/(x - 1).$$

Тогда

$$f(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}.$$

Этот многочлен неприводим над полем рациональных чисел по критерию Эйзенштейна, так как биномиальные коэффициенты

$$\binom{p}{k}, 0 < k < p,$$

делятся на p. Тогда и многочлен $f(x)$ неприводим.

Сформулируем ещё один признак непрводимости. Имеет место

Редукционный критерий. *Пусть*

$$\upsilon : R \to L, a \mapsto a^{\upsilon},$$

— *гомоморфизм коммутативных колец и*

$$\upsilon : R[x] \to L[x], f(x) \mapsto f^{\upsilon}(x),$$

— *его естественное продолжение, где*

$$f^{\upsilon}(x) = \sum_j a_j^{\upsilon} x^j \text{ для } f(x) = \sum_j a_j x^j.$$

Пусть для некоторого многочлена $f(x)$ с коэффициентами в кольце R выполняется условие

$$\deg(f(x)) = \deg(f^v(x)).$$

Тогда многочлен $f(x)$ не разлагается над кольцом R в произведение многочленов положительной степени, если многочлен $f^v(x)$ не разлагается подобным образом над кольцом L.

Доказательство. В условиях теоремы разложение

$$f(x) = g(x)h(x)$$

над R приводит к разложению

$$f^v(x) = g^v(x)h^v(x)$$

над кольцом L, при этом степени сомножителей сохраняются при гомоморфизме. $\square$

Для простого числа p рассмотрим гомоморфизм

$$(\cdot) \mod p : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, a \mapsto a + p\mathbb{Z}.$$

и его естественное продолжение на полиномиальные кольца.

Следствие. *Пусть p — простое число. Целочисленный многочлен $f(x)$ с единичным старшим коэффициентом неприводим над полем рациональных чисел, если многочлен $f(x) \mod p$ неприводим над полем $\mathbb{Z}/p\mathbb{Z}$.*

Пример. Многочлен $x^2 + x + 1$ неприводим над полем рациональных чисел, так как он неприводим над полем $\mathbb{Z}/2\mathbb{Z}$.

ГЛАВА 23

Поля

В главе изучаются поля.

1. Определение и основные конструкции

Напомним, полем называется коммутативное кольцо с единицей, отличной от нуля, где все ненулевые элементы обратимы. Иными словами, полем является непустое множество K с заданными на нём операциями сложения и умножения, обладающими следующими свойствами.

(1) С операцией сложения элементы из K образуют абелеву группу. Она называется аддитивной группой поля.

(2) С операцией умножения ненулевые элементы из K образуют абелеву группу. Она называется мультипликативной группой поля.

(3) Операции сложения и умножения связаны законом дистрибутивности, то есть для любых элементов a, b, c из K выполняется равенство

$$a(b + c) = ab + ac.$$

Рассмотрим далее основные

Примеры и конструкции.

∘ Кольцо целых чисел не является полем.

∘ Каждая из числовых систем: рациональных, действительных и комплексных чисел является полем.

∘ Числовая система $\mathbb{Q}_p$ является полем, если p — простое число.

∘ Кольцо классов вычетов $\mathbb{Z}/p\mathbb{Z}$ является полем тогда и только тогда, когда число p простое.

∘ Пусть K — поле. Кольцо классов вычетов $K[x]/f(x)K[x]$ является полем тогда и только тогда, когда многочлен $f(x)$ неприводим над полем K.

∘ Более общая ситуация. Пусть R — область главных идеалов. Кольцо классов вычетов R/aR является полем тогда и только тогда, когда элемент a неприводим в кольце R.

∘ Ещё более общий случай. Пусть I — ненулевой и неединичный идеал унитарного коммутативного кольца R. Кольцо классов вычетов R/I является полем тогда и только тогда, когда идеал I максимальный.

∘ Целостное кольцо R обладает полем частных $\mathrm{Frac}(R)$. Это наименьшее поле, включающее кольцо R. Оно состоит из дробей a/b, где a, b из R и $b \neq 0$.

∘ Напомним, через $K[x_1, \ldots, x_n]$ обозначается кольцо многочленов от переменных $x_1, \ldots, x_n$ с коэффициентами из K. Поле частных этого кольца обозначается через $K(x_1, \ldots, x_n)$ и называется полем рациональных выражений от переменных $x_1, \ldots, x_n$ с коэффициентами из K.

Расширения колец. Пусть K, E — коммутативные кольца. Кольцо K называется подкольцом кольца E и кольцо E называется расширением кольца K, если K включено в E и операции над общими элементами в этих кольцах выполняются одинаково. Пишут $K \leqslant E$ в этом случае.

Говорят, что расширение E порождается элементами $a_1, \ldots, a_n$ над кольцом K или получается присоединением элементов $a_1, \ldots, a_n$ к кольцу K, если оно является наименьшим по включению расширением кольца K, содержащим эти элементы. В этом случае для E используется обозначение $K[a_1, \ldots, a_n]$.

Расширения полей. Пусть K, E — поля. Поле K называется подполем поля E и поле E называется расширением поля K, если K включено в E и операции над общими элементами в этих полях выполняются одинаково.

Говорят, что расширение E порождается элементами $a_1, \ldots, a_n$ над полем K, или получается присоединением этих элементов к полю K, если оно является наименьшим по включению расширением поля K, содержащим эти элементы. В этом случае для E используется обозначение $K(a_1, \ldots, a_n)$.

Алгебраическая зависимость. Пусть, как и выше, $a_1, \ldots, a_n$ — элементы из расширения поля K и $x_1, \ldots, x_n$ — переменные. Тогда корректно определён эпиморфизм колец:

$$K[x_1, \ldots, x_n] \to K[a_1, \ldots, a_n], f(x_1, \ldots, x_n) \mapsto f(a_1, \ldots, a_n).$$

Если это отображение является изоморфизмом, то элементы $a_1, \ldots, a_n$ называются *алгебраически независимыми* над полем K, а при $n = 1$ говорят об элементе a_1, *трансцендентном* над полем K. Если это не так, то элементы $a_1, \ldots, a_n$ называются *алгебраически зависимыми* над полем K, а при $n = 1$ говорят об *алгебраическом* над полем K элементе a_1.

2. Степень расширения

Пусть E — расширение поля K. Будем рассматривать его как векторное пространство над полем K. Размерность этого пространства называется *степенью* расширения и обозначается $[E : K]$. Имеет место

Теорема (о степенях). *Пусть* $K \leqslant E \leqslant F$. *Тогда*

$$[F : K] = [F : E][E : K].$$

Доказательство. Пусть I, J — множества, наборы элементов e_i, где $i \in I$, и f_j, где $j \in J$, являются базисами расширений E над K и F над E. Для доказательства теоремы нужно проверить, что набор элементов $g_{ij} = e_i f_j$, где $(i, j) \in I \times J$, является базисом F над K. □

Упражнение. Восполните пробел в доказательстве теоремы.

3. Алгебраические и конечные расширения

Пусть E — расширение поля K. Элемент расширения называется *алгебраическим* над полем K, если он является корнем ненулевого многочлена с коэффициентами из K; в противном случае элемент называется *трансцендентным* над K. Расширение называется *алгебраическим*, если всякий его элемент алгебраичен над полем K.

Расширение называется *конечным*, если его степень конечна.

Примеры.

∘ Пусть x — переменная. Рассмотрим поле $K(x)$ как расширение поля K. Это расширение не является конечным и не является алгебраическим.

∘ Рассмотрим расширение $K(\gamma)$ поля K, где γ — корень неприводимого над K многочлена степени n. Это расширение конечное степени n с базисом

$$\gamma^0, \gamma^1, \ldots, \gamma^{n-1}.$$

Теорема. *Конечное расширение алгебраично. Оно получается присоединением конечного числа алгебраических элементов.*

Доказательство. Пусть E — конечное расширение поля K степени n. Для любого элемента γ из E набор элементов

$$\gamma^0, \gamma^1, \ldots, \gamma^n$$

линейно зависим над K. Элемент γ является, следовательно, корнем ненулевого многочлена с коэффициентами в K степени, не превосходящей n. Тем самым, первое утверждение теоремы доказано. Пусть теперь

$$e_1, \ldots, e_n$$

— базис расширения E. Тогда $E = K(e_1, \ldots, e_n)$. Теорема доказана. □

Замечание. Для первого утверждения теоремы обратное не имеет места, так как поле алгебраических чисел является бесконечным алгебраическим расширением поля рациональных чисел. Вместе с тем, для второго утверждения верно и обратное; это будет установлено позднее.

4. Простое расширение

Простым называется расширение, получаемое присоединением одного элемента. В этом разделе изучаются простые расширения.

Рассмотрим простое расширение

$$E = K(\gamma),$$

полученное присоединением к полю K элемента γ. Пусть x — переменная. Отметим, что имеется следующий эпиморфизм колец:

$$\upsilon_\gamma : K[x] \to K[\gamma], f(x) \mapsto f(\gamma).$$

Простое трансцендентное расширение. Предположим, элемент γ трансцендентен над K. Тогда отображение υ_γ является изоморфизмом целостных колец, который продолжается до изоморфизма между полями частных

$$K(x) \to K(\gamma), f(x)/g(x) \mapsto f(\gamma)/g(\gamma).$$

Таким образом, *простое расширение поля K, полученное присоединением трансцендентного элемента, изоморфно полю $K(x)$ рациональных выражений над K*. Подобное расширение единственно с точностью до изоморфизма, оставляющего неподвижными элементы основного поля и отображающего друг на друга присоединяемые элементы.

Простое алгебраическое расширение. Пусть теперь элемент γ алгебраический над полем K, то есть является корнем ненулевого многочлена с коэффициентами в поле K.

∘ *Среди ненулевых многочленов с коэффициентами в поле K, корнем которых является элемент γ, имеется единственный нормированный многочлен минимальной степени.*

Доказательство. Всегда существует нормированный многочлен минимальной степени, его можно получить, умножив произвольный многочлен минимальной степени на значение, обратное старшему коэффициенту. Нормированный многочлен минимальной степени единствен, иначе разность двух таких многочленов имеет меньшую степень. □

Многочлен, о котором говорится в последнем свойстве, называется *минимальным* многочленом элемента γ над полем K, а также *минимальным* многочленом расширения K. Обозначим через $m(x)$ этот многочлен и через n его степень. Отметим следующие свойства.

∘ *Имеет место изоморфизм*

$$K[\gamma] \to K[x]/m(x)K[x], f(\gamma) \mapsto f(x) + m(x)K[x].$$

Доказательство. Это так в силу первой теоремы об изоморфизмах колец, поскольку $\ker \upsilon_\gamma = m(x)K[x]$. □

∘ *Многочлен $m(x)$ неприводим над полем K.*

Доказательство. Это следует из определения многочлена $m(x)$. □

∘ *Имеет место равенство $K(\gamma) = K[\gamma]$.*

Доказательство. Равенство имеет место в силу того, что $K(\gamma)$ — поле частных кольца $K[\gamma]$ и это кольцо само уже является полем. □

∘ *Имеет место изоморфизм полей*

$$K[x]/m(x)K[x] \to K(\gamma), f(x) + m(x)K[x] \mapsto f(\gamma).$$

Доказательство. Это следует из предыдущих свойств. □

∘ *Имеет место равенство $[K(\gamma) : K] = n$.*

Доказательство. Элементы $\gamma^0, \gamma^1, \ldots, \gamma^{n-1}$ образуют базис расширения $K(\gamma)$ над полем K. □

Таким образом, имеет место

Теорема. *Расширение, полученное присоединением алгебраического элемента, конечное. Его степень совпадает со степенью минимального многочлена.* □

Замечание. Расширение $K(\gamma)$ состоит из элементов, однозначно представимых в виде многочленов

$$a_0\gamma^0 + a_1\gamma^1 + \ldots + a_{n-1}\gamma^{n-1}$$

от γ степени, меньшей n, с коэффициентами $a_0, a_1, \ldots, a_{n-1}$, принадлежащими полю K. Операции сложения и умножения над такими элементами выполняются с учётом равенства $m(\gamma) = 0$.

Некоторые следствия. Отметим ряд следствий этой теоремы.

Следствие 1. *Расширение, полученное присоединением конечного числа алгебраических элементов, конечное.*

Доказательство. Предположим, элементы $\gamma_1, \ldots, \gamma_n$ алгебраические над полем K. Рассмотрим последовательность расширений

$$K \leqslant K(\gamma_1) \leqslant K(\gamma_1, \gamma_2) \leqslant \ldots \leqslant K(\gamma_1, \gamma_2, \ldots, \gamma_n).$$

Каждое расширение в этой последовательности — простое алгебраическое и конечное в силу доказанной теоремы. Тогда и расширение $K(\gamma_1, \gamma_2, \ldots, \gamma_n)$ конечное над полем K по теореме о степенях. □

Следствие 2. Расширение тогда и только тогда конечное, когда оно конечно порождённое и алгебраическое.

Доказательство. Это так в силу следствия выше и теоремы, доказанной в предыдущем разделе. □

Следствие 3. *Суммы, разности, произведения и частные (отличных от нуля) элементов, алгебраических над полем K, алгебраичны над полем K.*

Доказательство. Пусть γ_1, γ_2 — алгебраические над полем K элементы, отличные от нуля. Тогда элементы

$$\gamma_1 + \gamma_2, \gamma_1 - \gamma_2, \gamma_1 \cdot \gamma_2, \gamma_1/\gamma_2$$

принадлежат расширению $K(\gamma_1, \gamma_2)$. Это расширение алгебраическое над полем K по предыдущему следствию. Значит и перечисленные элементы алгебраические над K. □

Следствие 4. *В любом расширении поля K множество элементов, алгебраических над полем K, образует поле.*

Доказательство. Данное утверждение является непосредственным следствием предыдущего. □

Пример. Алгебраические числа (то есть комплексные числа, алгебраические над полем рациональных чисел) образуют поле.

Символическое присоединение корней. Естественно поставить вопрос о существовании простого алгебраического расширения с заданным минимальным многочленом. Ответ на этот вопрос даёт следующая

Теорема. *Для любого нормированного неприводимого над полем K многочлена $m(x)$ существует простое алгебраическое расширение поля K с минимальным многочленом $m(x)$.*

Доказательство. Существует изоморфное вложение полей:

$$K \to K[x]/m(x)K[x], a \mapsto a + m(x)K[x].$$

Отождествим элементы в соответствии с этим вложением. Обозначим буквой γ смежный класс $x + m(x)K[x]$. В результате получаем простое алгебраическое расширение

$$K(\gamma) = K[x]/m(x)K[x]$$

поля K с минимальным многочленом $m(x)$. □

Построение простого алгебраического расширения методом, описанным в доказательстве теоремы, называется символическим присоединением корня многочлена $m(x)$ к полю K.

Единственность простого расширения. Естественно также поставить вопрос об единственности простого алгебраического расширения. Ответ на этот вопрос содержит следующая

Теорема. *Пусть γ_1, γ_2 — алгебраические над полем K элементы (принадлежащие некоторым расширениям этого поля). Тогда следующие условия равносильны.*

(1) *Между полями $K(\gamma_1), K(\gamma_2)$ имеется изоморфизм, оставляющий на месте элементы поля K и отображающий друг на друга элементы γ_1, γ_2.*

(2) *Элементы γ_1, γ_2 имеют над полем K совпадающие минимальные многочлены.*

Доказательство. Предположим, выполняется первое условие и m_1, m_2 — минимальные многочлены элементов γ_1, γ_2. Тогда $m_1(\gamma_2) = m_1(\gamma_1) = 0$ в силу изоморфизма. Элемент γ_2 является общим корнем многочленов $m_1(x), m_2(x)$. Отсюда, многочлены имеют общий делитель положительной степени и тогда ассоциированы над полем K в силу неприводимости. Они совпадают, так как нормированные. Таким образом, из первого условия следует второе.

Пусть выполняется второе условие. Тогда имеются изоморфизмы

$$\upsilon_i : K(\gamma_i) \to K[x]/m(x)K[x], f(\gamma_i) \mapsto f(x) + m(x)K[x],$$

где $i = 1, 2$, а изоморфизмом, удовлетворяющим требованиям первого условия, является произведение отображений

$$\upsilon_1 \upsilon_2^{-1} : K(\gamma_1) \to K(\gamma_2). \square$$

Если в условиях теоремы элементы γ_1, γ_2 содержатся в общем расширении поля K, то они называются *сопряжёнными* над полем K, а изоморфизм, о котором говорится в первом условии, называется *сопряжением* над полем K.

5. Поле разложения

Пусть E — расширение поля K и $f(x)$ — многочлен положительной степени n с коэффициентами в поле K. Поле E называется *полем разложения* многочлена f над полем K, если поле E содержит все корни многочлена $f(x)$ и является минимальным расширением поля K с этим свойством; иными словами, выполняются следующие условия.

(1) Многочлен f разлагается на линейные множители над полем E, то есть для некоторых элементов $\gamma_1, \ldots, \gamma_n$ из E выполняется равенство

$$f(x) = (x - \gamma_1) \cdots (x - \gamma_n).$$

(2) Поле E порождается корнями многочлена $f(x)$ над полем K, то есть выполняется равенство

$$E = K(\gamma_1, \ldots, \gamma_n).$$

Примеры.

∘ Полем разложения многочлена x^2+1 над полем действительных чисел является поле комплексных чисел.

∘ Полем разложения многочлена x^2-2 над $\mathbb{Q}$ является поле $\mathbb{Q}(\sqrt{2})$.

Существование поля разложения. Имеет место

Теорема. *Пусть $f(x)$ — многочлен положительной степени с коэффициентами в поле K. Существует поле разложения многочлена $f(x)$ над полем K. Оно является конечным расширением поля K, степени, не превосходящей $n!$.*

Доказательство. Разложим многочлен f на неприводимые множители над полем K. Если все множители линейные, то доказывать нечего. В противном случае присоединим к полю K символически корень γ_1 любого нелинейного неприводимого делителя и многочлен f разложим на неприводимые множители над полученным расширением $K(\gamma_1)$ ... и т. д. Будем повторять подобные действия до тех пор, пока не получим расширение $K(\gamma_1,\dots,\gamma_i)$, над которым многочлен f полностью разлагается. Это расширение является полем разложения. Заметим, что степень расширения, возникающего на каждом шаге совпадает со степенью соответствующего неприводимого делителя и не превосходит величины $n-j$, где j — количество расширений, выполненных ранее. По теореме о степенях степень поля разложения тогда не превосходит произведения $n\cdot(n-1)\cdots 2\cdot 1$. Теорема доказана. □

Единственность поля разложения. Имеет место

Теорема. *Пусть $f(x)$ — многочлен положительной степени с коэффициентами в поле K. Поле разложения многочлена f над полем K единственно с точностью до изоморфизма, оставляющего на месте элементы поля K.*

Докажем сначала вспомогательную лемму.

Лемма. Пусть имеется изоморфизм полей

$$\upsilon : K \to K^*, a \mapsto a^*.$$

Пусть также E, E^* — поля разложения многочленов

$$f(x)=\sum a_i x^i, f^*(x)=\sum a_i^* x^i$$

положительной степени над соответствующими полями K, K^*. Тогда изоморфизм υ можно продолжить до изоморфизма полей E, E^*.

Доказательство. Пусть имеются вложения полей

$$K \leqslant F \leqslant E, K^* \leqslant F^* \leqslant E^*,$$

и изоморфизм υ продолжен уже до изоморфизма

$$\upsilon : F \to F^*, a \mapsto a^*.$$

В этой ситуации имеется также изоморфизм колец многочленов

$$\Upsilon : F[x] \to F^*[x], g(x) \mapsto g^*(x), \text{ где } (\sum b_i x^i)^* = b_i^* x^i.$$

Разложим многочлены f, f^* над соответствующими полями F, F^* на неприводимые множители:

$$f = f_1 \cdots f_m, f^* = f_1^* \cdots f_m^*.$$

Отметим, что соответствующие множители f_i, f_i^* в этих разложениях — одной степени. Пусть k множителей в каждом разложении имеют первую степень, а остальные имеют большую степень. Каждое из полей F, F^*, таким образом, содержит ровно k корней соответствующих многочленов f, f^*, где корни посчитаны с учётом их кратностей. Предположим, что число k максимально возможное при данном выборе подполей F, F^*. Докажем, что $k = n$ и тогда поля F, F^* совпадают с полями разложений E, E^*. Предположим, это не так и γ, γ^* — какие-то корни многочленов f_{k+1}, f_{k+1}^* в соответствующих полях E, E^*. Тогда имеется цепочка изоморфизмов

$$F(\gamma) \to F[x]/f_{k+1}(x)F[x] \to F^*[x]/f_{k+1}^*(x)F^*[x] \to F^*(\gamma^*),$$
$$g(\gamma) \mapsto [g(x)] \mapsto [g^*(x)] \mapsto g^*(\gamma^*)$$

и изоморфизм υ между полями F, F^* продолжается далее до изоморфизма

$$\upsilon : F(\gamma) \to F^*(\gamma^*), g(\gamma) \mapsto g^*(\gamma^*).$$

Многочлены f, f разлагаются над полями $F(\gamma), F^*(\gamma^*)$ с числом линейных сомножителей, превосходящим k. Получили противоречие. Лемма доказана. □

Доказательство теоремы. Нужно взять в условиях леммы совпадающие поля K, K^* и тождественное отображение υ. □

6. Теорема о примитивном элементе

Присоединение нескольких алгебраических величин к полю нулевой характеристики можно заменить присоединением одной величины. Об этом говорит следующая теорема.

Теорема о примитивном элементе. *Пусть K — поле нулевой характеристики и его расширение $E = K(\gamma_1, \ldots, \gamma_n)$ получено присоединением элементов $\gamma_1, \ldots, \gamma_n$, алгебраических над полем K. Тогда найдётся элемент γ_0 в E, такой, что*

$$K(\gamma_0) = K(\gamma_1, \ldots, \gamma_n).$$

Доказательство. Достаточно доказать эту теорему для двух алгебраических элементов. Пусть α, β — алгебраические элементы над полем K, содержащиеся в общем расширении. Пусть $m_\alpha(x), m_\beta(x)$ — их минимальные многочлены над этим полем. Эти многочлены не имеют кратных корней, так как взаимно просты со своими производными. (Напомним, что характеристика полей нулевая.) Пусть $\alpha_1 \ldots, \alpha_n$ и $\beta_1 \ldots, \beta_m$ — корни этих многочленов в некотором расширении поля K, причём $\alpha_1 = \alpha, \beta_1 = \beta$. Выберем в поле K элемент c таким образом, чтобы равенство

$$\alpha_1 + c\beta_1 = \alpha_i + c\beta_j$$

могло выполняться только при $j = 1$ (тогда и $i = 1$). Такой выбор возможен, так как поле K бесконечное и только для конечного множества элементов c это условие не выполняется. Покажем, что для элемента $\gamma = \alpha + c\beta$ имеет место равенство

$$K(\gamma) = K(\alpha, \beta).$$

Для этого заметим, что в силу выбора элемента c верно

$$\gcd(m_\alpha(\gamma - cx), m_\beta(x)) = x - \beta.$$

Коэффициенты этого многочлена должны принадлежать полю $K(\gamma)$. Тогда элемент β лежит в этом поле. Элемент $\alpha = \gamma - c\beta$ принадлежит этому полю вслед за элементами β, γ. Теорема доказана. □

7. Задача Чирнгауза

Пусть $K(\gamma)$ — простое алгебраическое расширение поля K с минимальным многочленом $m(x)$ степени n. Пусть в этом расширении выбран элемент

$$\alpha = a_0\gamma^0 + \ldots a_{n-1}\gamma^{n-1}.$$

Задача Чирнгауза состоит в нахождении многочлена $g(x)$ с коэффициентами в поле K, корнем которого является элемент γ. Такой многочлен существует, так как расширение $K(\gamma)$ алгебраическое над K. Более того, существует единственный нормированный неприводимый многочлен с таким свойством (именно — минимальный многочлен элемента α над полем K). Неприводимый такой многочлен имеет степень, не превосходящую n, так как имеют место включения

$$K \leqslant K(\alpha) \leqslant K(\gamma).$$

Будем рассматривать эту задачу в предположении, что многочлен $m(x)$ не имеет кратных корней. Это условие обязательно выполняется, если поле K имеет нулевую характеристику или конечное. Итак, положим

$$f(x) = a_0x^0 + \ldots a_{n-1}x^{n-1}.$$

Опишем далее два способа, позволяющих решить задачу Чиргаузена.

Первый способ. Пусть $\gamma_1, \dots, \gamma_n$ — корни многочлена $m(x)$ в некотором расширении поля $K(\gamma)$. Тогда коэффициенты многочлена

$$g(x) = (x - f(\gamma_1)) \cdots (x - f(\gamma_n))$$

принадлежат полю K и элемент α является корнем этого многочлена.

Доказательство. Коэффициенты многочлена $g(x)$ выражаются посредством симметрических многочленов с коэффициентами в K от величин $\gamma_1, \dots, \gamma_n$ и тогда выражаются посредством многочленов с коэффициентами в поле K через коэффициенты многочлена $m(x)$. □

Второй способ. Пусть выполняются равенства

$$\begin{array}{lcccccccc}
\alpha\gamma^0 & = & a_{0,0}\gamma^0 & + & a_{0,1}\gamma^1 & + & \dots & + & a_{0,n-1}\gamma^{n-1}, \\
\alpha\gamma^1 & = & a_{1,0}\gamma^0 & + & a_{1,1}\gamma^1 & + & \dots & + & a_{1,n-1}\gamma^{n-1}, \\
 & & & & & & \dots & & \\
\alpha\gamma^{n-1} & = & a_{n-1,0}\gamma^0 & + & a_{n-1,1}\gamma^1 & + & \dots & + & a_{n-1,n-1}\gamma^{n-1},
\end{array}$$

где коэффициенты $a_{i,j}$ принадлежат полю K. Тогда коэффициенты многочлена

$$g(x) = \det \begin{pmatrix}
a_{0,0} - x & a_{0,1} & \dots & a_{0,n-1} \\
a_{1,0} & a_{1,1} - x & \dots & a_{1,n-1} \\
\vdots & \vdots & & \vdots \\
a_{n-1,0} & a_{n-1,1} & \dots & a_{n-1,n-1} - x
\end{pmatrix}.$$

принадлежат полю K и элемент α является корнем этого многочлена.

Доказательство. Набор элементов $\gamma^0, \dots, \gamma^{n-1}$ является ненулевым решением системы линейных алгебраических уравнений с матрицей

$$\begin{pmatrix}
a_{0,0} - \alpha & a_{0,1} & \dots & a_{0,n-1} \\
a_{1,0} & a_{1,1} - \alpha & \dots & a_{1,n-1} \\
\vdots & \vdots & & \vdots \\
a_{n-1,0} & a_{n-1,1} & \dots & a_{n-1,n-1} - \alpha
\end{pmatrix},$$

её определитель равен нулю; тогда α — корень многочлена $g(x)$. □

8. Конечные поля

В этом разделе доказываются основные теоремы о конечных полях.

Предварительные замечания. Нам понадобится следующая

Теорема (Ферма). *В конечном поле порядка q каждый элемент является корнем двучлена*

$$x^q - x.$$

Доказательство. Пусть F — поле порядка q с ненулевыми элементами $a_1, \dots a_{q-1}$ и a — произвольный ненулевой элемент. Отображение

$$F \setminus \{0\} \to F \setminus \{0\}, x \mapsto ax,$$

является подстановкой на множестве ненулевых элементов поля. Следовательно, имеют место равенства

$$a_1 \cdots a_{q-1} = aa_1 \cdots aa_{q-1} = a^{q-1} \cdot a_1 \cdots a_{q-1}.$$

Отсюда $a^{q-1} = 1$ и $a^q = a$. $\square$

Полезным для дальнейшего является

Упражнение. Докажите следующие утверждения, где k, m, p — целые положительные числа, p — простое.

$\circ$ Следующие условия равносильны:

($\circ$) $(x^k - 1)|(x^m - 1)$;

($\circ$) $(p^k - 1)|(p^m - 1)$;

($\circ$) $(x^{p^k} - x)|(x^{p^m} - x)$;

($\circ$) $k|m$.

(Первое и третье соотношения верны в кольце $\mathbb{Z}[x]$, остальные — в $\mathbb{Z}$.)

$\circ$ В поле характеристики p корни многочлена $x^{p^m} - x$ образуют подполе.

Основные теоремы. Докажем основные теоремы о конечных полях.

Теорема (о порядке конечного поля). *Характеристика конечного поля — простое число. Конечное поле характеристики p содержит p^n элементов, где n — некоторое целое положительное число.*

Доказательство. Характеристика положительна, так как поле конечное. Составное число не является характеристикой конечного поля, так как в поле нет делителей нуля. Если простое число p является характеристикой конечного поля, то поле содержит простое подполе, изоморфное полю $\mathbb{Z}/p\mathbb{Z}$ и является векторным пространством размерности n над ним. В этом случае число элементов в поле равно p^n. $\square$

Теорема (о существовании конечного поля). *Пусть p, n — целые положительные числа, p — простое. Существует конечное поле порядка p^n.*

Доказательство. Поле разложения многочлена $x^{p^n} - x$ над простым полем состоит из корней этого многочлена. Это следует из соотношений:

$$(a - b)^{p^n} = a^{p^n} + (-1)^{p^n} b^{p^n} = a^{p^n} - b^{p^n} = a - b;$$
$$(a/b)^{p^n} = a^{p^n}/b^{p^n} = a/b;$$

выполняющихся для любых корней a, b этого многочлена. Вместе с тем, число различных корней многочлена совпадает с его степенью, поскольку он взаимно прост со своей производной

$$(x^{p^n} - x)' = -1.$$

Существование поля доказано. □

Теорема (о единственности конечного поля). *Пусть p, n — целые положительные числа, p — простое. Поле порядка p^n является полем разложения двучлена $x^{p^n} - x$ над своим простым подполем. В частности, оно единственно с точностью до изоморфизма.*

Доказательство. Достаточно отметить, что в поле порядка p^n каждый элемент является корнем двучлена $x^{p^n} - x$. (Теорема Ферма.) □

Подполя конечного поля. Имеет место

Теорема (о подполях конечного поля). *Пусть K — подполе конечного поля E, содержащее q элементов. Тогда верны утверждения.*

(1) *Поле E содержит q^n элементов для некоторого целого положительного числа n.*

(2) *Всякое поле H, такое, что $K \leqslant H \leqslant E$, содержит q^k элементов для некоторого целого положительного числа k, такого, что $k|n$;*

(3) *Для любого целого положительного числа k, такого, что $k|n$, существует единственное поле H, содержащее q^k элементов, такое, что $K \leqslant H \leqslant E$.*

Доказательство. Поле E является конечным расширением поля K. Для степени n этого расширения должно выполняться первое утверждение. Второе утверждение доказывается аналогичными аргументами. Докажем третье. Пусть $n = km$. Тогда выполняются равенства

$$p^n - 1 = (p^k - 1)M,$$
$$x^{p^n-1} - 1 = (x^{p^k-1} - 1)(1 + x^{p^k-1} + \ldots + x^{(p^k-1)(M-1)}),$$

где $M = 1 + p^k + \ldots + p^{k(m-1)}$. В частности,

$$(x^{p^k} - x)|(x^{p^n} - x).$$

Далее заметим, что поле E состоит из корней многочлена $x^{p^n} - x$ и корни многочлена $x^{p^k} - x$ образуют в нём подполе порядка p^k. □

Упражнение. Докажите утверждения.

∘ Пусть K — поле порядка q и E — его расширение степени n. Тогда поле E является полем разложения двучлена $x^{q^n} - x$ над полем K.

∘ Пусть K — поле порядка q и E — его расширение. Отображение

$$E \to E, x \mapsto x^q,$$

есть автоморфизм поля E, оставляющий неподвижными элементы из K.

Корни неприводимых многочленов. Верна

Теорема (о корнях неприводимого многочлена). *Пусть K — конечное поле порядка q, $f(x)$ — неприводимый многочлен над полем K степени n. Пусть α — корень многочлена $f(x)$ в некотором расширении E поля K. Тогда имеют место следующие утверждения.*

(1) *Элементы $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ различные.*

(2) *Над полем E имеет место разложение:*

$$f(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}}).$$

В частности, простое расширение $K(\alpha)$ совпадает с полем разложения многочлена $f(x)$ над полем K.

Доказательство. Рассмотрим последовательность элементов

$$\alpha, \alpha^q, \alpha^{q^2}, \ldots.$$

Все они являются корнями многочлена $f(x)$ вслед за элементом α, так как в поле E для любого элемента β выполняется равенство

$$f(\beta)^q = f(\beta^q)$$

(см. последнее упражнение). Поле $K(\alpha)$ содержит q^n элементов. В силу теоремы Ферма имеет место равенство $\alpha = \alpha^{q^n}$ и рассматриваемая последовательность периодическая с периодом $m|n$. Элементы последовательности являются корнями многочлена $x^{q^m} - x$ и тогда принадлежат расширению поля K, состоящему из корней этого многочлена и содержащему q^m элементов. Отсюда $m \geqslant n$ и теорема доказана. □

Число неприводимых многочленов.

Теорема (о числе неприводимых многочленов). *Пусть q — степень простого числа и $\theta_q(n)$ — число неприводимых нормированных многочленов степени n над полем из q элементов. Тогда для любого целого положительного числа n имеют место равенства:*

$$q^n = \sum_{d|n} \theta_q(d)d,$$

$$\theta_q(n) = \frac{1}{n}\sum_{d|n} q^d \mu(\frac{n}{d}),$$

где

$$\mu(n) = \begin{cases} (-1)^k, & \text{если } n \text{ есть произведение } k \text{ различных простых;} \\ 0, & \text{если } n \text{ не свободно от квадратов.} \end{cases}$$

Функция μ называется *функцией Мёбиуса*.

Сформулированная теорема является следствием следующей леммы.

Лемма. Пусть K — поле порядка q. Тогда для любого целого положительного числа n над полем K имеет место разложение

$$x^{q^n} - x = \prod_{d|n} M_{q,d}(x),$$

где $M_{q,d}(x)$ — произведение всех нормированных неприводимых над полем K многочленов степени d.

Доказательство. Пусть E — поле разложения двучлена $x^{q^n} - x$ над полем K. Оно состоит из корней этого двучлена и имеет порядок q^n. Любой неприводимого делитель этого двучлена, имеющий степень d и корень γ, определяет простое расширение $K(\gamma)$ порядка q^d содержащееся между K и E; отсюда $d|n$.

С другой стороны, произвольный неприводимый над K многочлен $f(x)$ степени $d|n$ является минимальным многочленом простого расширения, которое совпадает с полем разложения этого многочлена, содержит q^d элементов и его можно расширить далее до поля порядка q^n (так как $d|n$), которое оказывается полем разложения двучлена $x^{q^n} - x$ и состоит из его корней. Отсюда, многочлен $f(x)$ является делителем этого двучлена.

Итак, из проведённых рассуждений видно, что неприводимые делители двучлена $(x^{q^n} - x)$ — это в точности неприводимые нормированные многочлены спененей, делящих n. Поскольку двучлен не имеет кратных корней, теорема доказана. □

Доказательство теоремы. Первое соотношение является непосредственным следствием леммы. Второе получается из первого по принципу обращения Мёбиуса, который устанавливается в упражнении ниже. □

Упражнение. Докажите утверждения и ответьте на вопросы.

∘ Пусть R — коммутативное кольцо с единицей. Множество функций

$$f : \mathbb{Z}_+ \to R$$

является коммутативным моноидом с операцией $*$, определённой так:

$$f * g(n) = \sum_{d|n} f(d)g(n/d) \text{ для любого } n \in \mathbb{Z}_+.$$

Обозначим $\mathrm{Fun}(\mathbb{Z}_+, R)$ этот моноид. Операция $*$ называется *свёрткой*.

∘ Что является единицей этого моноида?

∘ Какие функции обратимы в этом моноиде?

∘ Функция Мёбиуса является обратной для функции

$$1 : \mathbb{Z}_+ \to R, n \mapsto 1.$$

∘ (Принцип обращения Мёбиуса.) В моноиде $\mathrm{Fun}(\mathbb{Z}_+, R)$ для любых функций f, g следующие условия равносильны:

(∘) имеет место равенство $f * 1 = g$;

(∘) имеет место равенство $g * \mu = f$.

ГЛАВА 24

Модуль над кольцом

В этой главе продолжается изучение алгебраической структуры модуля над кольцом R. В понимании модуля и алгебры будем придерживаться определений и пояснений, данных ранее.

Если иное не оговорено, то под словами «модуль», «алгебра», «гомоморфизм» и т. д. будем понимать далее R-модуль, R-алгебру, R-гомоморфизм и т. д. Приведём ряд примеров модулей и алгебр.

∘ Многочлены и степенные ряды образуют алгебры $R[x], R[[x]]$.

∘ Всякое поле является алгеброй над любым своим подполем.

∘ Кольцо является алгеброй над любым подкольцом, лежащим в центре и содержащим единицу.

∘ Матрицы образуют модуль $R^{m,n}$.

∘ Квадратные матрицы, составленные из элементов коммутативного кольца R, образуют алгебру $R^{m,m}$.

∘ Гомоморфизмы, действующие между модулями M, N над коммутативным кольцом R, образуют модуль $\mathrm{Hom}_R(M, N)$.

∘ Эндоморфизмы модуля M над коммутативным кольцом R, образуют алгебру $\mathrm{End}_R(M)$. Она изоморфна матричной алгебре $R^{m,m}$, если модуль M — свободный ранга m.

1. Подмодуль

Непустое подмножество модуля, замкнутое умножением на элементы из кольца и сложением, можно рассматривать как модуль над тем же кольцом (с индуцированными операциями). Такое подмножество называется *подмодулем*. Аналогично определяется *подалгебра* алгебры (в дополнение к сказанному надо потребовать замкнутость умножением).

Примеры.

∘ Рассмотрим кольцо R как левый модуль над собой. Тогда подмодули в нём — непустые подмножества, замкнутые сложением и левым умножением на элементы кольца. Напомним, такие подмножества называются левыми идеалами кольца.

∘ Понятия правого, левого и двустороннего идеалов распространяются и на алгебры. Так, левыми идеалами называются подмножества алгебры,

замкнутые сложением, умножением на элементы кольца и левым умножением на элементы самой алгебры. Например, в алгебре квадратных матриц левый идеал образуют матрицы, у которых столбцы с определёнными номерами нулевые.

∘ В произвольной алгебре A элементы, перестановочные со всеми её элементами, образуют коммутативную подалгебру $\mathrm{Z}(A)$. Эта подалгебра называется *центром* алгебры, а её элементы называются центральными. Напомним, что алгебру с единицей можно рассматривать как алгебру над некоторым подкольцом, лежащим в её центре.

Отметим ряд свойств.

∘ Пересечение любой совокупности подмодулей является подмодулем.

∘ Объединение любой совокупности подмодулей, линейно упорядоченной по отношению включения, является подмодулем.

∘ Для произвольной совокупности подмодулей M_s модуля M, где $s \in T$, определим их сумму $\sum_s M_s$ как множество элементов, представимых конечными суммами

$$\sum_s u_s$$

(где элементы $u_s \in M_s$ почти все равны нулю). Заметим, что данный подмодуль — наименьший по включению среди подмодулей, включающих все M_s.

∘ Среди подмодулей модуля M, включающих заданное подмножество X, есть наименьший по включению. Он совпадает с пересечением всех этих подмодулей и состоит из всевозможных конечных линейных комбинаций

$$\sum_u u\lambda_u,$$

где суммирование выполняется по всем элементам u из X и почти все коэффициенты λ_s нулевые. Этот подмодуль обозначается $\langle X \rangle$ и называется подмодулем, порождённым множеством X. Заметим, что данный подмодуль совпадает с суммой подмодулей

$$uR = \{u\lambda | \lambda \in R\},$$

порождаемых одиночными элементами u из X.

Упражнение. Проверьте выполнение всех перечисленных свойств. Сформулируйте аналогичные свойства для подалгебр и идеалов алгебры.

2. Фактор-модуль

Пусть N — подмодуль модуля M, принято писать

$$N \leqslant M$$

в этой ситуации. Пусть v — произвольный элемент из M. Множество

$$v + N = \{v + u | u \in N\}$$

называется *смежным классом* модуля M по подмодулю N. Иными словами, это множество состоит из элементов модуля M, которые отличаются от элемента v слагаемым из N. Отметим ряд свойств.

∘ Для любых элементов v, w из M имеет место ряд равносильностей:

$$v \in w + N \Leftrightarrow v - w \in N \Leftrightarrow w - v \in N \Leftrightarrow w \in v + N. \ \square$$

∘ Смежные классы разбивают модуль. □

∘ Операции модуля M индуцируют следующие операции над смежными классами:

$$(v + N) + (w + N) = (v + w) + N, \ (v + N)\lambda = v\lambda + N,$$

где v, w из M и λ из R.

Доказательство. Непосредственно проверяется корректность таких определений. Для сложения нужно проверить, что

$$v + w - (v' + w') \in N, \text{ если } v - v' \in N, w - w' \in N;$$

для умножения на скаляры — нужно проверить, что

$$v\lambda - v'\lambda \in N, \text{ если } v - v' \in N.$$

И то и другое верно. □

∘ С записанными операциями смежные классы образуют модуль. □

Этот модуль обозначается

$$M/N$$

и называется *фактор-модулем* модуля M по подмодулю N.

Примеры.

∘ Рассмотрим векторное пространство $\mathbb{R}^3$ над полем $\mathbb{R}$, где сложение векторов и умножение на скаляры выполняются покомпонентно. Здесь плоскость, образованная осями OX и OY, является подмодулем и все параллельные ей плоскости являются смежными классами.

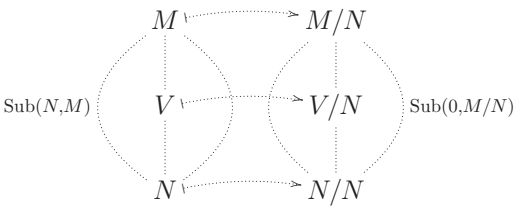
∘ Пусть R — коммутативное кольцо с единицей. Рассмотрим модуль R^n столбцов высоты n. В нём множество решений линейной системы $ax = b$ либо пусто, либо является смежным классом по подмодулю, состоящему из решений однородной системы $ax = 0$. Здесь a — матрица размера $m \times n$ и b — столбец высоты m, составленные из элементов кольца, x — столбец неизвестных высоты n.

В завершение раздела сформулируем теорему о подмодулях фактор-модуля. Обозначим через $\mathrm{Sub}(N, M)$ множество всех подмодулей модуля M, включающих заданный подмодуль N.

Теорема о подмодулях фактор-модуля. Пусть N — подмодуль модуля M. Тогда существует биекция

$$\mathrm{Sub}(N, M) \to \mathrm{Sub}(0, M/N), V \mapsto V/N. \square$$

Проиллюстрируем теорему следующей диаграммой.



Упражнение. Докажите теорему о подмодулях фактор-модуля.

3. Теоремы об изоморфизмах

Пусть M, N — модули над кольцом R. Напомним, отображение

$$g : M \to N, u \mapsto g(u)$$

называется *гомоморфизмом* или *линейным* отображенем модулей над кольцом R, если оно перестановочно со сложением и с операциями умножения на элементы кольца, то есть обладает свойствами:

(1) $g(u + v) = g(u) + g(v)$;

(2) $g(u\lambda) = g(\lambda)$;

для любых u, v из M, λ из R. Полный прообраз нуля при гомоморфизме называется его *ядром*. Отметим, что ядро гомоморфизма является подмодулем области определения и всякий подмодуль модуля является ядром некоторого гомоморфизма. Имеют место следующие теоремы.

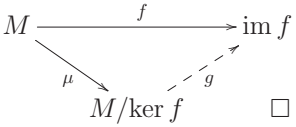
Теорема (первая об изоморфизме). Пусть

$$f : M \to \mathrm{im}\, f$$

— эпиморфизм модулей. Отображение

$$\mu : M \to M/\ker f, u \mapsto u + \ker f,$$

является эпиморфизмом модулей и существует единственный изоморфизм g, такой, что коммутативна диаграмма



$\square$

Теорема (вторая об изоморфизме). Пусть N, K — подмодули модуля M. Тогда существует изоморфизм модулей

$$N/(N \cap K) \to (N+K)/K, u + (N \cap K) \mapsto u + K. \square$$

Теорема (третья об изоморфизме). Пусть N, K — подмодули модуля M, такие, что $K \leqslant N \leqslant M$. Тогда существует изоморфизм модулей

$$M/N \cong (M/K)/(N/K). \square$$

Последняя теорема дополняет теорему о подмодулях фактор-модуля.

Упражнение. Докажите теоремы об изоморфизмах.

4. Прямые произведения и суммы

В этом разделе определяются прямые произведения и прямые суммы модулей, рассматривается свободный модуль.

Прямые произведения. Пусть имеется множество T, элементы которого называются *индексами*, и для каждого индекса s задан модуль V_s над кольцом R. Будем говорить в этой ситуации, что задан набор модулей

$$(V_s | s \in T).$$

Станем рассматривать функции

$$f : T \to \cup_s V_s, f \mapsto f_s, \text{ где } f_s \in V_s \text{ для всех } s.$$

Такие функции станем называть наборами или последовательностями. Они составляют модуль над кольцом R, где операции определены так:

$$(f+g)_s = f_s + g_s, \ (f\lambda)_s = f_s\lambda;$$

здесь s — индекс, f, g — наборы, λ из R. Данный модуль обозначается

$$\prod_s V_s,$$

называется *прямым произведением* модулей V_s.

Теорема (универсальное свойство прямого произведения).

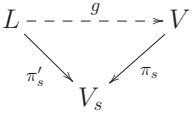
Модуль $V = \prod_s V_s$ обладает следующим свойством. Существует такой набор гомоморфизмов

$$(\pi_s | \pi_s \in \mathrm{Hom}_R(V, V_s), s \in T),$$

что для любого модуля L и любого набора гомоморфизмов

$$(\pi'_s | \pi'_s \in \mathrm{Hom}_R(L, V_s), s \in T),$$

найдётся единственный гомоморфизм $g : L \to V$, делающий коммутативными диаграммы



для всех s из T. (Иными словами, выполняются равенства $\pi_s \circ g = \pi'_s$.)

Обратно, всякий модуль V с этим свойством изоморфен $\prod_s V_s$.

Доказательство. Гомоморфизмы π_s — это естественные проекции

$$\pi_s : \prod_t V_t \to V_s, f \mapsto f_s,$$

указывающие значения функции (компоненты набора) f. Гомоморфизм g определён однозначно в описанной ситуации, так как для произвольного элемента u из L набор $g(u)$ удовлетворяет соотношениям

$$g(u)_s = \pi_s(g(u)) = \pi'_s(u).$$

Данные соотношения определяют все значения $g(u)_s$, для любого s, и тогда полностью и однозначно определяют значение $g(u)$. С другой стороны, такое определение корректно и g является гомоморфизмом.

Обратно. Если некоторый модуль V обладает описанным свойством, то можно рассмотреть последовательности гомоморфизмов

$$V \to \prod_s V_s \to V, \prod_s V_s \to V \to \prod_s V_s,$$

где в каждом случае действует гомоморфизм g, о котором говорится в теореме. Записанные композиции совпадают с тождественными отображениями в силу свойства единственности для гомоморфизма g. Следовательно, гомоморфизмы, действующие между модулями $V, \prod_s V_s$ являются взамно обратными изоморфизмами. □

Упражнение. Докажите следующие утверждения.

∘ Обозначим через $\mathrm{Fun}(A, B)$ множество всех функций из A в B. Пусть B — модуль над кольцом R. Множество таких функций является модулем над кольцом R, где операции умножения на скаляры и сложения определены поточечно — следующим образом

$$(f + g)(a) = f(a) + g(a), (f\lambda)(a) = f(a)\lambda;$$

здесь a из A, λ из R.

∘ Для модуля V и набора модулей $(V_s | s \in T)$ над кольцом R имеется изоморфизм модулей

$$\mathrm{Fun}(V, \prod_s V_s) \to \prod_s \mathrm{Fun}(V, V_s), h \mapsto \overline{h},$$

где

$$\overline{h}_s : V \to V_s, v \mapsto h(v)_s \text{ для любого индекса } s.$$

∘ Если кольцо R коммутативно, то меет место изоморфизм модулей

$$\mathrm{Hom}_R(V, \prod_s V_s) \simeq \prod_s \mathrm{Hom}_R(V, V_s).$$

Прямая сумма. В произведении $\prod_s M_s$ наборы, у которых почти все значения нулевые, образуют подмодуль. Он обозначается

$$\oplus_s M_s$$

и называется *прямой суммой* модулей V_s; для конечного множества T прямые суммы и произведения совпадают. Для множества T, состоящего из чисел $1, \ldots, n$, прямая сумма обычно обозначается

$$V_1 \oplus V_2 \oplus \ldots \oplus V_n,$$

а её функции (наборы) записываются векторами

$$(f_1, f_2, \ldots, f_n).$$

Прямые суммы характеризует следующая

Теорема (универсальное свойство прямой суммы).

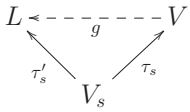
Модуль $V = \oplus_s V_s$ обладает следующим свойством. Существует такой набор гомоморфизмов

$$(\tau_s | \tau_s \in \mathrm{Hom}_R(V_s, V), s \in T),$$

что для любого модуля L и любого набора гомоморфизмов

$$(\tau'_s | \tau'_s \in \mathrm{Hom}_R(V_s, L), s \in T),$$

найдётся единственный гомоморфизм $g : V \to L$, делающий коммутативными диаграммы



для всех s из T. (Иными словами, выполняются равенства $g \circ \tau_s = \tau'_s$.)

Обратно, всякий модуль V с этим свойством изоморфен $\oplus_s V_s$.

Доказательство. Речь идёт о естественных вложениях

$$\tau_s : V_s \to \oplus_t V_t, v \mapsto \tau_s(v),$$

$$\text{где } \tau_s(v)_t = \begin{cases} v, & \text{если } s = t; \\ 0, & \text{в противном случае.} \end{cases}$$

Здесь v — произвольный элемент модуля V_s. Если гомоморфизм g существует, то он определён однозначно, так как модуль $\oplus_s V_s$ порождается

элементами $\tau_s(v)$, где $v \in V_s$, $s \in T$. Единственный такой гомоморфизм определяется условием

$$g(v) = \sum_s \tau'_s(v_s) \text{ для любого } v \in V.$$

Такое определение корректно и обладает нужным свойством.

Обратно. Если некоторый модуль V обладает описанным свойством, то можно рассмотреть последовательности гомоморфизмов

$$\oplus_s V_s \to V \to \oplus_s V_s, V \to \oplus_s V_s \to V,$$

где в каждом случае действует гомоморфизм g, о котором говорится в теореме. Записанные композиции совпадают с тождественными изоморфизматими в силу свойства единственности для гомоморфизма g. Тогда гомоморфизмы между модулями $V, \oplus_s V_s$ являются взаимно обратными изоморфизмами. □

Замечание. Диаграммы для произведения и суммы отличаются направлением стрелок.

Упражнение. Докажите, что для любого модуля V и набора модулей $(V_s | s \in T)$ над коммутативным кольцом R имеется изоморфизм модулей

$$\mathrm{Hom}_R(\oplus_s V_s, V) \to \prod_s \mathrm{Hom}_R(V_s, V), h \mapsto \overline{h},$$

где

$$\overline{h}_s = \tau_s h \text{ для любого } s.$$

Внутренняя прямая сумма. Пусть задан модуль V над кольцом R и набор его подмодулей

$$(V_s | s \in T).$$

Модуль V называется *внутренней* прямой суммой этих подмодулей, если имеется изоморфизм

$$\oplus_s V_s \to V, v \mapsto \sum_s v_s.$$

Здесь слева записана «обычная», «внешняя», прямая сумма, но в дальнейшем внутренние и внешние прямые суммы будем обозначать одинаково. Отметим следующие свойства:

(1) имеет место равенство $\sum_s V_s = V$;

(2) каждый элемент модуля V можно представить в виде конечной суммы элементов из различных подмодулей V_s;

(3) каждый элемент модуля V единственным образом представим в виде конечной суммы элементов из различных подмодулей V_s;

(4) если конечная сумма элементов, выбранных из различных подмодулей V_s, равна нулю, то в ней все слагаемые равны нулю;

(5) для любого индекса s выполняется равенство $V_s \cap \sum_{t\neq s} V_t = 0$.

Имеет место

Теорема. *Если выполнены условия (1–5), то модуль V является внутренней прямой суммой набора подмодулей $(V_s|s \in T)$.*

Пример. $R[x] = \oplus_{s\in\mathbb{N}} Rx^s$.

Упражнение. Докажите теорему и выделите различные достаточные множества условий.

Свободный модуль. Пусть V — модуль над кольцом R. Он называется *свободным*, если содержит набор векторов

$$(v_s|s \in T), \text{ где } T \text{ некоторое множество,}$$

такой, что в модуле V всякий вектор u единственным образом записывается в виде конечной линейной комбинации

$$u = \sum_{s\in T} v_s\lambda_s$$

векторов v_s с коэффициентами λ_s из R (которые почти все равны нулю). Набор векторов v_s в этом случае называется *базисом* свободного модуля V. Все базисные вектора обязаны быть различными, поэтому можно говорить о множестве, а не о наборе базисных векторов.

Иными словами, свободный модуль — это модуль, который можно представить в виде прямой суммы

$$V = \oplus_s v_s R,$$

где для каждого прямого слагаемого имеется изоморфизм модулей

$$R \to v_s R, \lambda \mapsto v_s\lambda.$$

В частности, свободные модули с равномощными базисами изоморфны.

Слово «свободный» означает, что в модуле есть базис — порождающее множество, в котором вектора не связаны нетривиальными линейными соотношениями, свободны от них.

Примеры.

∘ Модуль $R[x]$ свободный с базисом $1, x, x^2, \ldots$.

∘ Свободный модуль с n-элементным базисом изоморфен R^n.

Теорема (универсальное свойство свободного модуля).

Для свободного R-модуля V с базисом B выполняются условия:

(1) *множество B порождает R-модуль V;*

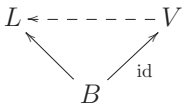
(2) *для любого R-модуля L всякое отображение $g : B \to L$ (однозначно) продолжается до гомоморфизма модулей $g : V \to L$.*

Обратно, всякий R-модуль V, для которого выполняются записанные условия, является свободным с базисом B.

Доказательство. Свободный модуль, очевидно, обладает перечисленными свойствами. Обратно, если модуль V обладает отмеченными свойствами, то B — базис. Действительно, всякий элемент представим линейной комбинацией базисных элементов, в силу первого условия. Такое представление однозначно в силу второго условия. □

Следствие. *Всякий R-модуль является гомомрфным образом свободного модуля.* □

Проиллюстрируем содержание теоремы коммутативной диаграммой.



Упражнение. Докажите, что базис является максимальным независимым и минимальным порождающим подмножеством свободного модуля.

5. Двойственный модуль*

Пусть R — коммутативное кольцо с единицей. Будем рассматривать модули над кольцом R и гомоморфизмы между ними. Пусть W — некоторый такой модуль.

Контравариантный функтор. Для модуля M положим

$$M^* = \mathrm{Hom}(M, W)$$

и для гомоморфизма

$$h : M \to N,$$

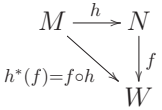
определим функцию

$$h^* : N^* \to M^*, f \mapsto h^*(f), \text{ где } h^*(f) = f \circ h.$$

Иными словами, для любого элемента u из M выполняется равенство

$$h^*(f)(u) = f(h(u)).$$

Ситуацию можно проиллюстрировать следующими диаграммами.



Отметим ряд свойств.

- Отображение h^* является гомоморфизмом R-модулей.
- Гомоморфизм h^* инъективный, если h сюръективный.

∘ Гомоморфизм h^* сюръективный, если h инъективный и модуль $\operatorname{im} h$ выделяется прямым слагаемым в N.

∘ Пусть R — поле. Отображение h^* тогда и только тогда инъективно (сюръективно), когда h сюръективно (соответственно инъективно).

∘ Отображение h^* является изоморфизмом, если h — изоморфизм; в этом случае имеет место равенство:

$$(h^*)^{-1} = (h^{-1})^*.$$

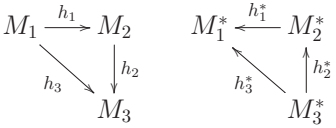
∘ Для любых гомоморфизмов

$$h_1 : M_1 \to M_2,$$
$$h_2 : M_2 \to M_3$$

и модулей M_1, M_2, M_3 над кольцом R имеет место равенство

$$(h_2 \circ h_1)^* = h_1^* \circ h_2^*$$

Проиллюстрируем последнее свойство парой диаграмм.



Замечание. Обозначим Module_R класс всех модулей над кольцом R и гомоморфизмов между ними. Выше было определено «отображение»

$$\mathrm{Module}_R \to \mathrm{Module}_R, M \mapsto M^*, h \mapsto h^*,$$

где M — произвольный модуль и h — произвольный гомоморфизм. При данном отображении «стрелки» (гомоморфизмы) между модулями меняют направление. На языке теории категорий подобное отображение называется контравариантным функтором, отображающим категорию модулей над кольцом R в себя.

Двойственность. Пусть модуль W совпадает с кольцом R. Теперь

$$M^* = \mathrm{Hom}(M, R)$$

для произвольного модуля M. Модуль M^* называется *двойственным* по отношению к M, а его элементы называются *ковекторами* или *линейными функционалами* над кольцом R. Отметим ряд свойств.

Теорема. *Пусть M — свободный модуль ранга m над кольцом R с базисом*

$$e = (e_1, \ldots, e_m).$$

Тогда модуль M^* также свободный ранга m, с базисом

$$e^* = (e_1^*, \ldots, e_m^*),$$

где

$$e_k^* : M \to R, \sum_j e_j \lambda_j \mapsto \lambda_k, (1 \leqslant k \leqslant m).$$

Базис e^* называется *двойственным* к базису e.

Доказательство. Станем рассматривать кольцо R как свободный модуль единичной размерности с базисом $\{1\}$. Имеется изоморфизм

$$M^* \to R^{1,m}, h \mapsto \overline{h},$$

где $\overline{h}$ — матрица из $R^{1,m}$ являющаяся матрицей линейного отображения h относительно заданных базисов в M и R. Иными словами, матрица h определяется условием

$$h : e \mapsto \overline{h}.$$

Заметим, что функции из набора e^* линейные и отображаются записанным изоморфизмом на единичные вектора — имеющие единственную ненулевую компоненту, причём равную 1. Поскольку единичные вектора образуют базис модуля строк, вектора из набора e^* образуют базис модуля M. □

Замечание. Базис e^*, двойственный к e, определяется условием

$$u = \sum_k e_k e_k^*(u)$$

для любого u из M.

Теорема. *Пусть M, N — конечно порождённые свободные модули над кольцом R с базисами e, g и $h : M \to N$ — линейное отображение с матрицей $\overline{h}$ относительно выбранных базисов. Тогда для матрицы $\overline{h^*}$ линейного отображения $h^* : M^* \to N^*$ относительно базисов g^*, e^* выполняется равенство*

$$\overline{h^*} = \overline{h}^T$$

Доказательство. Напомним, что матрицы $\overline{h}, \overline{h^*}$ принадлежат модулям $R^{n,m}, R^{m,n}$ и определяются условиями

$$h : e \mapsto g\overline{h}, h^* : g^* \mapsto e^*\overline{h^*}.$$

В соответствии с этим, для элементов этих матриц выполняются равенсва:

$$\overline{h^*}_{ij} = h^*(g_j^*)(e_i) = g_j^*(h(e_i)) = g_j^*(g\overline{h} \downarrow_i) = \overline{h}_{ji}. \square$$

Примеры.

∘ Пусть R — поле нулевой характеристики и V — векторное пространство над ним, состоящее из многочленов с коэффициентами в поле R,

зависящих от одной переменной и имеющих степень, строго меньшую n. Для любого элемента a из поля R многочлены

$$e_k = \frac{(x-a)^k}{k!}, 0 \leqslant k \leqslant n-1,$$

составляют базис этого пространства. Двойственный базис составляют линейные функционалы

$$e_k^* : V \to R, f(x) \mapsto \frac{d^k f}{dx^k}(a) \text{ где } , 0 \leqslant k \leqslant n-1.$$

В результате разложения $f = \sum_k e_k e_k^*(f)$ получается формула Тейлора.

∘ Пусть R — поле и V — векторное пространство над ним, состоящее из многочленов с коэффициентами в поле R, зависящих от одной переменной и имеющих степень, строго меньшую n. Для любых различных элементов $a_1, \ldots, a_n$ из поля R (пусть $|R| \geqslant n$) многочлены

$$e_k = \frac{(x-a_1)\ldots\widehat{(x-a_k)}\ldots(x-a_n)}{(a_k-a_1)\ldots\widehat{(a_k-a_k)}\ldots(a_k-a_n)}, \text{ где } 0 \leqslant k \leqslant n-1,$$

составляют базис этого пространства (сверху отмечена отсутствующая скобка). Двойственный базис составляют линейные функционалы

$$e_k^* : V \to R, f(x) \mapsto f(a_k).$$

На этом пути получается интерполяционная формула Лагранжа.

Упражнение. Восполните детали в приведённых примерах.

Билинейная форма. Для модуля M над кольцом R определим отображение

$$F_M : M^* \times M \to R, (f, v) \mapsto f(v).$$

Отметим ряд свойств.

∘ Отображение F_M линейно над кольцом R по каждому аргументу. Иными словами, верны равенства

$$F_M(f_1\lambda_1 + f_2\lambda_2, v) = F_M(f_1, v)\lambda_1 + F_M(f_2, v)\lambda_2,$$
$$F_M(f, v_1\lambda_1 + v_2\lambda_2) = F_M(f, v_1)\lambda_1 + F_M(f, v_2)\lambda_2;$$

для любых $\lambda, \lambda_1, \lambda_2$ из R, v, v_1, v_2 из M и f, f_1, f_2 из M^*.

∘ Пусть $h : M \to N$ — линейное отображение модулей над кольцом R. Тогда выполняется равенство

$$F_N(f, h(v)) = F_M(h^*(f), v)$$

для любых элементов v из M и f из N^*.

Пусть теперь модуль M свободный ранга m над кольцом R с базисом e. Модуль M^* также свободный ранга m. Он содержит двойственный базис e^*. Отождествим элементы в модулях M, M^* с наборами координат из $R^{m,1}$ в выбранных базисах e, e^*.

∘ Имеет место равенство

$$F_M(f, v) = f^{\mathrm{T}} v.$$

Здесь f, v — произвольные вектора из модулей $R^{m,1}$

Пусть задан ещё один свободный над кольцом R модуль N ранга n. Выберем в модулях N, N^* двойственные базисы g, g^* и отождествим элементы этих модулей с координатными наборами из $R^{n,1}$.

∘ Имеют место равенства

$$F_N(f, \overline{h}v) = F_M(\overline{h}^{\mathrm{T}} f, v) = f^{\mathrm{T}} \overline{h} v.$$

Здесь f, v — произвольные вектора из модулей $R^{n,1}, R^{m,1}$ и $\overline{h}$ — произвольная матрица из $R^{n,m}$.

Ковариантный функтор. Для модуля M над кольцом R определим отображение

$$\psi_M : M \to M^{**}, v \mapsto \psi_M(v),$$

где

$$\psi_M(v) : M^* \to R, f \mapsto f(v),$$

Имеет место

Теорема. *Пусть M, N — модули над кольцом R. Для линейного над R отображения $h : M \to N$ коммутативна диаграмма*

$$\begin{array}{ccc} M & \xrightarrow{\psi_M} & M^{**} \\ \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h^{**}} \\ N & \xrightarrow{\psi_N} & N^{**}. \end{array}$$

Если M — конечно порождённый свободный модуль над кольцом R, то отображение ψ_M является изоморфизмом.

Доказательство. Пусть α — линейный функционал из модуля N^* и выполняется равенство $h(u) = v$ для пары элементов u, v из модулей M, N. Тогда

$$\begin{aligned} h^{**}(\varphi_M(u))(\alpha) &= \varphi_M(u)(h^*(\alpha)) = \varphi_M(u)(\alpha \circ h) \\ &= \alpha \circ h(u) = \alpha(h(u)) = \alpha(v) \\ &= \varphi_N(v)(\alpha), \text{ откуда} \\ h^{**}(\varphi_M(u)) &= \varphi_N(v) \end{aligned}$$

и диаграмма коммутативна. Далее, выполняются равенства

$$\varphi_M(e_i)(e_j^*) = e_j^*(e_i) = [i = j], \text{ то есть}$$
$$\varphi_M(e_i) = e_i^{**}.$$

Таким образом, отображение φ_M линейно и базис e модуля M отображает на базис e^{**} модуля M^{**}. Это отображение является изоморфизмом. □

Замечание. Рассмотрим отображение

$$\mathrm{Module}_R \to \mathrm{Module}_R, M \mapsto M^{**}, h \mapsto h^{**},$$

определённое для произвольных модуля M и гомоморфизма h модулей над кольцом R. Данное отображение осуществляет преобразование модулей с сохранением стрелок (гомоморфизмов) между ними. На языке теории категорий подобное отображение называется ковариантным функтором, отображающим категорию модулей над кольцом R в себя.

6. Билинейные формы

Пусть R — коммутативное кольцо с единицей и M, N — модули над ним. Отображение

$$F : M \times N \to R, (u, v) \mapsto \langle u, v\rangle_F,$$

называется *билинейной формой* над кольцом R, если отображения

$$M \to R, x \mapsto \langle x, v\rangle_F,$$
$$N \to R, y \mapsto \langle u, y\rangle_F,$$

линейны над R для любых $u \in M$ и $v \in N$. Иными словами, равенства

$$\langle u_1\lambda_1 + u_2\lambda_2, v\rangle_F = \langle u_1, v\rangle_F\lambda_1 + \langle u_2, v\rangle_F\lambda_2,$$
$$\langle u, v_1\lambda_1 + v_2\lambda_2\rangle_F = \langle u, v_1\rangle_F\lambda_1 + \langle u, v_2\rangle_F\lambda_2$$

верны для любых значений $\lambda, \lambda_1, \lambda_2$ из R, u, u_1, u_2 из M и v, v_1, v_2 из N.

Модуль билинейных форм. Обозначим через $\mathrm{L}^2(M, N, R)$ множество всех таких билинейных форм и отметим следующие свойства.

∘ Множество $\mathrm{L}^2(M, N, R)$ является R-модулем, где

$$\langle x, y\rangle_{F+G} = \langle x, y\rangle_F + \langle x, y\rangle_G,$$
$$\langle x, y\rangle_{F\lambda} = \langle x, y\rangle_F\lambda$$

для любых билинейных форм F, G и скаляра λ из кольца R.

∘ Для билинейной формы F отображение

$$\varphi_F : M \to N^*, u \mapsto \varphi_F(u),$$
$$\text{где } \varphi_F(u) : N \to R, v \mapsto \langle u, v\rangle_F,$$

является гомоморфизмом R-модулей.

∘ Аналогично, гомоморфизмом R-модулей является отображение

$$\psi_F : N \to M^*, v \mapsto \psi_F(v),$$
$$\text{где } \psi_F(v) : M \to R, u \mapsto \langle u, v\rangle_F.$$

∘ Изоморфизмами R-модулей является следующие отображения

$$\mathrm{L}^2(M, N, R) \to \mathrm{Hom}(M, N^*), F \mapsto \varphi_F$$
$$\mathrm{L}^2(M, N, R) \to \mathrm{Hom}(N, M^*), F \mapsto \psi_F.$$

Задание билинейной формы F равносильно заданию любого из линейных отображений φ_F, ψ_F. Эти линейные отображения называются её *корреляциями*, левой и правой. Форма F называется *неособой слева* или *неособой справа*, если соответствующая корреляция является изоморфизмом. Форма называется *неособой*, если оба эти отображения — изоморфизмы. В случае неособой формы модули M, N, на которых она определена, могут отождествляться, посредством корреляций, с соответствующими двойственными модулями N^*, M^*.

Формы и эндоморфизмы. Продолжим изучение билинейных форм над кольцом R, определённых на паре модулей M, N. Все такие формы можно получить из единственной неособой формы в соответствии со следующим свойством.

∘ Пусть форма F неособая. Тогда отображения

$$\mathrm{End}(M) \to \mathrm{L}^2(M, N, R), h \mapsto ((x, y) \mapsto \langle h(x), y\rangle_F,$$
$$\mathrm{End}(N) \to \mathrm{L}^2(M, N, R), h' \mapsto ((x, y) \mapsto \langle x, h'(y)\rangle_F,$$

являются изоморфизмами R-модулей.

∘ Пусть форма F неособая. Для любого эндоморфизма $h \in \mathrm{End}(M)$ найдётся единственный эндоморфизм $h' \in \mathrm{End}(N)$, такой, что выполняется равенство

$$\langle h(x), y\rangle_F = \langle x, h'(y)\rangle_F,$$

для любой пары элементов x, y из модулей M, N. Отображение

$$\mathrm{End}(M) \to \mathrm{End}(N), h \mapsto h',$$

является изморфизмом R-модулей.

Эндоморфизмы h, h' называются сопряжёнными относительно формы F.

Пример. Пусть M — конечно порождённый свободный модуль. Тогда отображения h, h^* из модулей $\mathrm{End}(M), \mathrm{End}(M^*)$ сопряжены относительно формы

$$F_M : M^* \times M \to R, (f, u) \mapsto f(u).$$

Симметрические и антисимметрические формы. Пусть модули M, N совпадают. Рассмотрим билинейную форму $F : M^2 \to R$. Она называется *симметрической*, если выполняется равенство

$$\langle x, y\rangle_F = \langle y, x\rangle_F$$

для всех x, y из M. Она называется *альтернированной* или *антисимметрической*, если

$$\langle x, x\rangle_F = 0$$

для любого x из M. В этом случае

$$\langle x, y\rangle_F = -\langle y, x\rangle_F.$$

для всех x, y из M.

Симметрические билинейные формы, также как антисимметрические, образуют модуль. Эти модули обозначим

$$\mathrm{L}^2_s(M, R), \mathrm{L}^2_a(M, R).$$

Пусть теперь форма F неособая симметрическая. Эндоморфизм h из множества $\mathrm{End}(M)$ назовём *симметрическим* относительно формы F, если он совпадает с сопряжённым, $h = h'$. Назовём его *антисимметрическим*, если он противоположен сопряжённому, $h = -h'$, а также выполняется равенство

$$\langle h(x), x\rangle_F = 0$$

для всех x из M.

∘ Пусть форма F неособая симметрическая и h — эндоморфизм из модуля $\mathrm{End}(M)$. Форма

$$M^2 \to R, (x, y) \mapsto \langle h(x), y\rangle_F$$

тогда и только тогда симметрична (антисимметрична), когда эндоморфизм h симметричен (антисимметричен) относительно формы F.

Доказательство. Пусть записанная форма симметрична или антисимметрична. В силу симметричности формы F для любых элементов x, y из модуля M выполняются равенства

$$\langle h(x), y\rangle_F = \pm\langle h(y), x\rangle_F = \pm\langle y, h'(x)\rangle_F = \langle h'(x), y\rangle_F.$$

Отсюда видно, что эндоморфизм h симметричен для симметрической формы и антисимметричен для антисимметрической.

Теперь предположим, что эндоморфизм симметричен или антисимметричен. Тогда выполняются равенства

$$\langle h(x), y\rangle_F = \pm\langle x, h(y)\rangle_F = \pm\langle h(y), x\rangle_F = \langle y, h(x)\rangle_F.$$

Отсюда, форма симметричена для симметрического гомоморфизма и антисимметрична для антисимметрического. □

С учётом ранее доказанного свойства, можно заметить, что эндоморфизм, симметричный или антисимметричный относительно некоторой неособой симметрической формы, сохраняет своё свойство относительно любой такой формы. В связи с этим такие эндоморфизмы будем называть просто симметрическими или антисимметрическими. Симметрические эндоморфизмы, как и антисимметрические, образуют модуль. Обозначим эти модули

$$\mathrm{Sym}(M), \mathrm{Alt}(M).$$

Свойства, записанные выше, можно уточнить следующим образом.

∘ Пусть форма F неособая симметрическая. Тогда имеются следующие изоморфизмы R-модулей:

$$\mathrm{Sym}(M) \to \mathrm{L}^2_s(M,R), h \mapsto ((x,y) \mapsto \langle h(x), y\rangle_F),$$
$$\mathrm{Alt}(N) \to \mathrm{L}^2_a(M,R), h \mapsto ((x,y) \mapsto \langle h(x), y\rangle_F). \square$$

Примеры.

∘ Определитель матрицы размера 2 над коммутативным кольцом является антисимметрической билинейной формой от столбцов матрицы.

∘ Пусть A — алгебра конечного ранга над полем R. Функция

$$A^2 \to R, (x,y) \mapsto \mathrm{tr}(xy)$$

является билинейной формой над полем R. Эта форма симметрическая, если алгебра коммутативна.

7. Матрицы и билинейные формы

Пусть R — коммутативное кольцо с единицей и M, N — свободные модули рангов m, n над кольцом R с базисами e, g. Пусть также

$$F : M \times N \to R, (x,y) \mapsto \langle x, y\rangle,$$

— билинейная форма над кольцом R.

Матрица билинейной формы. Матрицу

$$\begin{pmatrix} \langle e_1, g_1\rangle & \dots & \langle e_1, g_n\rangle \\ \vdots & \vdots & \vdots \\ \langle e_m, g_1\rangle & \dots & \langle e_m, g_n\rangle \end{pmatrix}$$

называют *матрицей Грама* формы F или просто *матрицей* формы F относительно выбранных базисов. Будем обозначать её

$$G(F)_{e,g}, G_{e,g}, G.$$

Отметим ряд свойств этой матрицы.

∘ Пусть $x\downarrow, y\downarrow$ — вектор-столбцы из $R^{m,1}, R^{n,1}$ координат элементов x, y из модулей M, N в соответствующих базисах e, g. Иными словами, имеют место равенства

$$x = ex\downarrow, y = gy\downarrow .$$

Тогда

$$\langle x, y\rangle = \overrightarrow{x} G y\downarrow,$$

где $\overrightarrow{x} = (x\downarrow)^{\mathrm{T}}$.

Доказательство. В силу линейности достаточно проверить это равенство для базисных элементов $x = e_i, y = g_j$. □

∘ Имеет место изоморфизм R-модулей:

$$\mathrm{L}^2(M, N, R) \to R^{m,n}, F \mapsto G(F)_{e,g}.$$

Доказательство. Все свойства изоморфизма выполнены. □

∘ Пусть e', g' — ещё одна пара базисов модулей M, N и $c_{ee'}, c_{gg'}$ — матрицы перехода между базисами, такие, что

$$e' = ec_{ee'}, g' = gc_{gg'}.$$

Тогда

$$G_{e'g'} = c_{ee'}^{\mathrm{T}} G_{e,g} c_{gg'}.$$

Доказательство. Для доказательства нужно подставить $c_{ee'}x\downarrow, c_{gg'}y\downarrow$ вместо $x\downarrow, y\downarrow$ в выражение из первого свойства выше. Действительно, на этом пути получаем соотношения

$$\langle e'x\downarrow, e'y\downarrow\rangle = \langle ec_{ee'}x\downarrow, ec_{gg'}y\downarrow\rangle = \overrightarrow{x} c_{ee'}^{\mathrm{T}} G_{eg} c_{gg'} y\downarrow,$$

откуда следует требуемое равенство. □

Теорема. *Следующие условия равносильны.*

(1) *Форма F неособая слева.*

(2) *Форма F неособая справа.*

(3) *Форма F неособая.*

(4) *Матрица G квадратная и обратимая над кольцом R.*

Доказательство. Первое условие равносильно тому, что отображение

$$R^{n,1} \to R^{n,1}, x \mapsto x^{\mathrm{T}} G,$$

биективно и тогда равносильно четвёртому условию. Остальные случаи рассматриваются аналогично. □

Матрицы эндоморфизмов. Рассмотрим вопрос: как связаны между собой матрицы эндоморфизмов модулей M, N, сопряженных относительно неособой формы F. Отметим следующее свойство.

∘ Пусть форма F неособая, h, h' — эндоморфизмы из модулей $\mathrm{End}(M)$, $\mathrm{End}(N)$, сопряжённые относительно формы F, такие, что равенство

$$\langle h(x), y\rangle = \langle x, h'(y)\rangle$$

выполняется для всех пар x, y из модулей M, N. Пусть также $\overline{h}, \overline{h'}$ — матрицы этих эндоморфизмов в соответствующих базисах e, g, выбранных в модулях M, N, то есть выполняются соотношения

$$h : e \mapsto e\overline{h},$$
$$h' : g \mapsto g\overline{h'}.$$

Тогда верно равенство

$$\overline{h'} = G^{-1}\overline{h}^{\mathrm{T}}G.$$

В частности, $\overline{h'} = \overline{h}^{\mathrm{T}}$, если матрица G единичная.

Симметричные и антисимметричные матрицы. Станем рассматривать квадратные матрицы размера m, составленные из элементов кольца R. Матрица a называется симметричной, если она совпадает с транспонированной, $a = a^{\mathrm{T}}$. Она называется антисимметричной, если она противоположна транспонированной, $a = -a^{\mathrm{T}}$, и содержит нули на диагонали. Симмметричные матрицы, как и антисимметричные, образуют модуль над кольцом R. Обозначим эти модули следующим образом:

$$\mathrm{Sym}(m, R), \mathrm{Alt}(m, R).$$

∘ Пусть M — свободный модуль ранга n над коммутативным кольцом R. Имеют место следующие изоморфизмы R-модулей:

$$\mathrm{L}^2_s(M, R) \to \mathrm{Sym}(m, R), F \mapsto G(F)_{ee},$$
$$\mathrm{L}^2_s(M, R) \to \mathrm{Alt}(m, R), F \mapsto G(F)_{ee}. \square$$

Матрицы автоморфизмов. Пусть по-прежнему R — коммутативное кольцо с единицей, рассматриваются модули над кольцом R. Обратимый эндоморфизм модуля M называется его *автоморфизмом*. Автоморфизмы образуют группу относительно операции композиции. Эта группа обозначается

$$\mathrm{Aut}(M).$$

Автоморфизм h модуля M называется автоморфизмом формы

$$F : M^2 \to R, (x, y) \mapsto \langle x, y\rangle,$$

если равенство

$$\langle x, y\rangle = \langle h(x), h(y)\rangle$$

имеет место для всех x, y из M. Легко понять, что автоморфизмы формы с операцией композиции образуют группу (которая содержится в группе всех автоморфизмов модуля M). Эта группа обозначается

$$\mathrm{Aut}(F).$$

Отметим следующее свойство.

∘ Пусть форма F неособая, h — автоморфизм модуля M и h' — сопряжённый к нему относительно формы F эндоморфизм модуля M. Тогда равносильны условия.

(1) Отображение h является автоморфизмом формы F.

(2) Выполняется равенство

$$h \circ h' = \mathrm{id}_M\,.$$

Иными словами, h' является обратным для h автоморфизмом.

Доказательство. Пусть h — автоморфизм формы F. Тогда для любых x, y из M верно

$$\langle h(x), y\rangle = \langle x, h'(y)\rangle = \langle h(x), h(h'(y))\rangle,$$

откуда $h \circ h' = \mathrm{id}_M$. Таким образом, из первого условия следует второе. Обратно, если h', h^{-1} совпадают, то

$$\langle h(x), h(y)\rangle = \langle x, h^{-1}(h((y))\rangle = \langle x, y\rangle.$$

Таким образом из второго условия следует первое. □

Теорема. *Пусть модуль M свободный ранга m с базисом e, F — неособая билинейная форма на M и $\overline{h}$ — матрица из $R^{m,m}$. Тогда следующие условия равносильны.*

(1) *$\overline{h}$ является матрицей автоморфизма формы F в базисе e.*

(2) *Выполняется равенство*

$$\overline{h}^{\mathrm{T}} G_{ee} \overline{h} = G_{ee}.$$

Доказательство. Можно считать $\overline{h}$ матрицей эндоморфизма h модуля M, записанной в базисе e, так что выполняется соотношение

$$h : e \mapsto e\overline{h}.$$

Тогда для матрицы сопряжённого эндоморфизма в том же базисе выполняется равенство

$$\overline{h'} = G_{ee}^{-1} \overline{h}^{\mathrm{T}} G_{ee}.$$

Пусть выполняется первое условие и h является автоморфизмом формы F. Тогда h' является обратным автоморфизмом и матрицы $\overline{h}, \overline{h'}$ взаимно обратные. Второе условие получается из записанного соотношения умножением на $\overline{h}$ справа и G_{ee} слева. Если же выполняется второе условие, то из записанного соотношения в результате правого умножения на матрицу $\overline{h}$ получается равенство $\overline{h'h} = \mathrm{e}$, откуда видно, что h' — обратное для h отображение и тогда h является автоморфизмом формы F. $\square$

8. Точные последовательности*

Пусть задана последовательность гомоморфизмов между R-модулями:

$$\ldots \xrightarrow{f_{i-1}} V_i \xrightarrow{f_i} V_{i+1} \xrightarrow{f_{i+1}} \ldots .$$

Она называется *точной в i-м члене*, если $\operatorname{im} f_i = \ker f_{i+1}$, и называется *точной*, если она точна в каждом члене. Точная последовательность

$$0 \longrightarrow A \xrightarrow{f} V \xrightarrow{g} B \longrightarrow 0.$$

называется *короткой точной последовательностью*. Для неё точность в A значает, что гомоморфизм f инъективен, точность в B означает, что гомоморфизм g сюръективен и, тогда, точность в V означает, что $B \simeq V/A$.

Будем говорить, что записанная выше короткая точная последовательность *расщепляется справа*, если для гомоморфизма g имеется правый обратный гомомофизм $h : B \to V$, такой, что $g \circ h = \mathrm{id}_B$. Последовательность *расщепляется слева*, если для гомоморфизма f есть левый обратный гомоморфизм $e : V \to A$, такой, что $e \circ f = \mathrm{id}_A$. Проиллюстрируем ситуацию диаграммой

$$0 \longrightarrow A \underset{f}{\overset{e}{\rightleftarrows}} V \underset{g}{\overset{h}{\rightleftarrows}} B \longrightarrow 0.$$

Имеет место

Теорема (о короткой точной последовательности).

Для точной последовательности

$$0 \longrightarrow A \xrightarrow{f} V \xrightarrow{g} B \longrightarrow 0$$

следующие условия равносильны.

(1) *Последовательность расщепляется слева.*

(2) *Последовательность расщепляется справа.*

(3) *Для некоторого изоморфизма* $u : V \to A \oplus B$ *коммутативна диаграмма:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & V & \xrightarrow{g} & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}_A} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle \mathrm{id}_B} & & \\ 0 & \longrightarrow & A & \xrightarrow[\tau_A]{} & A \oplus B & \xrightarrow[\pi_B]{} & B & \longrightarrow & 0, \end{array}$$

где

$$\tau_A : A \to A \oplus B, a \mapsto (a, 0), \ \textit{(стандартное вложение)}$$
$$\pi_B : A \oplus B \to B, (a, b) \mapsto b, \ \textit{(стандартная проекция).}$$

Третье условие означает, что V разлагается в прямую сумму модулей A и B, причём отображения f и g вполне аналогичны соответствующим стандартному вложению и стандартной проекции. Последовательность, для которой выполняются условия (1–3), называется *расщепляемой.*

Докажем сначала вспомогательную лемму.

Лемма. *Пусть имеются гомоморфизмы* R*-модулей*

$$g : V \to B, h : B \to V,$$

такие, что $g \circ h = \mathrm{id}_B$*. Тогда отображение*

$$\overline{g} : \mathrm{im}\, h \to B, v \mapsto g(v),$$

является изоморфизмом R*-модулей и выполняются соотношения*

$$\overline{g} \circ h = \mathrm{id}_B, h \circ \overline{g} = \mathrm{id}_C, \ \textit{где } C = \mathrm{im}\, g.$$

Имеет место разложение в прямую сумму подмодулей:

$$V = \ker g \oplus \mathrm{im}\, h.$$

Иными словами, отображение $\overline{g}$ является ограничением гомоморфизма g и обратным отображением для изоморфизма $h : B \to \mathrm{im}\, h$.

Доказательство леммы. Элементы одного смежного класса фактор-модуля $V/\ker g$ одинаково отображаются гомоморфизмом g. Отсюда следует, что подмодуль $\mathrm{im}\, h \leqslant V$ пересекается по единственному элементу с каждым смежным классом и функция $\overline{g}$ действительно обладает указанными в формулировке свойствами. Отсюда следует также, что имеют место равенства

$$\ker g + \mathrm{im}\, h = V, \ker g \cap \mathrm{im}\, h = 0.$$

Лемма доказана. □

Доказательство теоремы. Докажем необходимые имликации.

$(3 \to 1, 2)$ *Третье условие влечёт первые два.*

Предположим существует изоморфизм u. Тогда имеет место разложение во внутреннюю прямую сумму $V = A' \oplus B'$, где

$$u : V = A' \oplus B' \to A \oplus B, a' + b' \mapsto (a, b),$$

для любых $a' \in A', b' \in B'$. Последовательность расщепляется слева и справа с помощью функций

$$e : V \to A, a' + b' \mapsto a;$$
$$h : B \to V, b \mapsto b'.$$

$(1 \to 3)$ *Первое условие влечёт третье.*

Предположим, выполняется первое условие и последовательность расщепляется слева посредством функции e. В силу леммы имеет место разложение

$$V = \operatorname{im} f \oplus \ker e$$

и изоморфизм

$$\overline{e} : \operatorname{im} f \to A, v \mapsto e(v).$$

Отметим, что ограничение

$$\overline{g} : \ker e \to B, v \mapsto g(v),$$

также является изоморфизмом, так как подмодуль $\ker e$ пересекается с каждым смежным классом фактор-модуля $V/\operatorname{im} f = V/\ker g$ по единственному элементу. Таким образом, имеется изоморфизм

$$u : V \to A \oplus B, a' + b' \mapsto (\overline{e}(a'), \overline{g}(b')),$$

для любых $a' \in \operatorname{im} f, b' \in \ker e$. Он обладает нужным свойством.

$(2 \to 3)$ *Второе условие влечёт третье.*

Предположим, выполняется второе условие и последовательность расщепляется справа посредством функции h. В силу леммы имеет место разложение

$$V = \operatorname{im} h \oplus \ker g$$

и изоморфизм

$$\overline{g} : \operatorname{im} h \to B, v \mapsto g(v).$$

Ограничение

$$\overline{f} : A \to \operatorname{im} f = \ker g, v \mapsto f(v),$$

является изоморфизмом, так как функция f инъективна. Таким образом, имеется изоморфизм

$$u : V \to A \oplus B, a' + b' \mapsto (\overline{f}^{-1}(a'), \overline{g}(b')),$$

где $a' \in \ker g, b' \in \operatorname{im} h$, обладающий нужным свойством.

Теорема доказана. $\square$

Доказанную теорему можно вывести также из следующей леммы.

Лемма (о пяти гомоморфизмах). Пусть коммутативна диаграмма

$$\begin{array}{ccccccccc} D & \xrightarrow{e} & A & \xrightarrow{f} & M & \xrightarrow{g} & B & \xrightarrow{h} & C \\ \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle t} & & \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle w} \\ D' & \xrightarrow[e']{} & A' & \xrightarrow[f']{} & M' & \xrightarrow[g']{} & B' & \xrightarrow[h']{} & C \end{array}$$

и последовательности в её строках точные. Тогда выполняются условия.

(1) Гомоморфизм u сюръективен, если гомоморфизмы t, v сюръективны и w инъективен.

(2) Гомоморфизм u инъективен, если гомоморфизмы t, v инъективны и s сюръективен.

(3) Гомоморфизм u является изоморфизмом, если s, t, v, w — изоморфизмы.

Доказательство. Докажем первое свойство. Для этого выберем произвольно элемент $m' \in M'$ и рассмотрим диаграмму

$$\begin{array}{ccccc} m & \xmapsto{g} & b & \xmapsto{h} & 0 \\ & & \downarrow{\scriptstyle v(sur)} & & \downarrow{\scriptstyle w(inj)} \\ m' & \xmapsto[g']{} & g'(m') & \xmapsto[h']{} & 0. \end{array}$$

Элемент b со свойством, указанным в диаграмме, существует, поскольку v сюръективен. Нижний элемент справа равен нулю, так как элемент $g'(m')$ принадлежит множеству $\operatorname{im} g' = \ker h$. Верхний элемент справа равен нулю, так как w инъективен. Наконец, элемент m существует, поскольку $b \in \ker h = \operatorname{im} g$. Теперь рассмотрим диаграмму

$$\begin{array}{ccc} a & \xmapsto{f} & f(a) \\ \downarrow{\scriptstyle t(sur)} & & \downarrow{\scriptstyle u(sur?)} \\ a' & \xmapsto[f']{} & m' - u(m). \end{array}$$

Элемент a' существует, так как элемент $m' - u(m)$ принадлежит множеству $\ker g' = \operatorname{im} f'$; существование элемента a следует из сюръективности t. Тогда

$$m' = u(m) + u(f(a)) = u(m + f(a))$$

и $m' \in \operatorname{im} u$. Поскольку элемент m' был выбран произвольно в M', гомоморфизм u сюръективен. Первое свойство доказано. Второе свойство доказывать не станем. Третье свойство следует из первых двух. $\square$

ГЛАВА 25

Модуль над областью главных идеалов

В главе изучаются модули над областью главных идеалов (ОГИ), в частности, над евклидовой областью (ЕО). Устанавливается кононическая форма Смита матрицы над ОГИ. На основе этого даётся описание конечно порождённнх модулей над ОГИ. Устанавливаются нормальные формы матриц над полем.

1. Векторное пространство и ранг матрицы

Поскольку поле является областью главных идеалов с наиболее простой (точнее — тривиальной) теорией делимости, имеет смысл начать изучение с рассмотрения векторного пространства (модуля над полем). Напомним, в связи с этим, некоторые свойства векторного пространства.

Векторное пространство. Имеет место

Теорема. *Пусть V — векторное пространство над полем K, B — множество векторов из V. Тогда следующие условия равносильны.*

(1) *Подмножество B линейно независимое и порождает векоторное пространство V, то есть является базисом в нём.*

(2) *Подмножество B линейно независимое и максимальное по включению с этим свойством.*

(3) *Подмножество B порождает векторное пространство V и является минимальным по включению с этим свойством.* □

Следствие. *В векторооном пространстве любое независимое подмножество можно расширить до базиса.*

Доказательство. Независимое подмножество можно расширить до максимального по включению независимого множества в силу леммы Цорна, так как объединение цепи линейно независимых подмножеств линейно независимо. □

Следствие. *В векторооном пространстве существует базис.*

Доказательство. Пустое множество можно расширить до базиса. □

Следствие. *В векторооном пространстве любое подпространство является прямым слагаемым: для любого подпространства $U \leqslant V$ существует такое подпространство $W \leqslant V$, что имеет место разложение $V = U \oplus W$.*

Доказательство. Базис подпространства U можно расширить до базиса всего пространства. Тогда добавленные базисные вектора порождают некоторое подпространство W, для которого выполняется условие, указанное в формулировке. □

Следствие. *Пусть $f : V \to U$ — линейное отображение векторных пространств. Тогда*

$$\dim V = \dim \operatorname{im}(f) + \dim \ker(f).$$

Доказательство. Запишем $V = \ker(f) \oplus W$ на основании предыдущего следствия и заметим, что ограничение f на W является изоморфизмом, то есть $\operatorname{im}(f) \simeq W$. □

Упражнение. Докажите сформулированную выше теорему и следующие утверждения.

∘ В векторном пространстве для любых подпространств U, V имеет место соотношение

$$\dim(U + V) = \dim U + \dim V - \dim(U \cap V).$$

∘ Каноническая матрица над полем. Докажите, что матрицу над полем элементарными преобразованиями строк и столбцов можно привести к диагональному виду, где на диагонали могут быть только единичные и нулевые значения, причём нулевые строки находятся внизу матрицы. Диагональная форма матрицы определена однозначно.

Ранг матрицы над полем. Пусть b — матрица размера $m \times n$, составленная из элементов поля K. Размерность пространства её строк (это подпространство в K^n, порождённое строками) называется *строчным рангом* матрицы b. Аналогично, *столбцовый ранг* — это размерность пространства столбцов. Верна следующая

Теорема. *Строчный и столбцовый ранги матрицы над полем совпадают.*

Доказательство опирается на следующую лемму.

Лемма. *Для обратимых матриц a, c размеров m, n и матрицы b размера $m \times n$, составленных из элементов поля K, строчные ранги матриц b и abc совпадают. Аналогичное верно для столбцовых рангов.*

Доказательство леммы. Пространства столбцов матриц b, abc — это образы линейных отображений $b^*, a^* \circ b^* \circ c^*$, где

$$b^* : K^n \to K^m, x \mapsto bx,$$

и линейные преобразования a^*, c^* определены аналогично. Эти образы изоморфны и имеют одинаковую размерность, так как a^*, b^* — изоморфизмы. Для строк можно воспользоваться транспонированием. □

Доказательство теоремы. Приведём матрицу b элементарными преобразованиями строк и столбцов к диагональному виду и увидим, что получится матрица с равными строчным и столбцовым рангами. Но элементарные преобразования не меняют рангов. Теорема доказана. □

Так как строчный ранг квадратной матрицы над полем совпадает со столбцовым, и тот и другой называется просто *рангом*. Для ранга матрицы b используется обозначение

$$\operatorname{rank} b.$$

2. Каноническая форма Смита

В это разделе вводится каноническая форма матрицы над ОГИ.

Инвариантные множители. Пусть K — коммутативное кольцо с единицей. Будем рассматривать матрицы, составленные из элементов этого кольца. Матрицы b, d одинаковых размеров $m \times n$ называются *эквивалентными* (над кольцом K), если существуют обратимые квадратные матрицы a, c размеров m, n, такие, что выполняется равенство

$$abc = d.$$

Имеет место

Теорема. *Над областью главных идеалов K всякая матрица b эквивалентна диагональной матрице вида*

$$d = \begin{pmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_s & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix},$$

где элементы $d_1, \ldots, d_s$ ненулевые и в кольце K выполняются условия

$$d_1 | d_2, \ldots, d_{s-1} | d_s.$$

Матрицу над евклидовой областью можно привести к указанному виду элементарными преобразованиями строк и столбцов.

В условиях теоремы матрица d называется *канонической формой Смита* матрицы b или просто канонической формой матрицы b, а элементы $d_1, \ldots, d_s$ называются её *инвариантными множителями.*

Доказательство. Разобьём доказательство на четыре части. Обозначим через $J(b)$ идеал кольца K, порождённый всеми элементами матрицы b, и через b' элемент, порождающий этот идеал, такой, что $J(b) = Kb'$.

(1) *Для любых матриц a, c подходящего размера верны включения*

$$J(ab) \subseteq J(b),\ J(bc) \subseteq J(b)\ \textit{и}\ J(abc) \subseteq J(b).$$

Здесь выполняются равенства, если матрицы a, b обратимы.

Первое включение выполняется, так как элементы матрицы ab записываются линейными комбинациями элементов матрицы b, где коэффициентами служат элементы матрицы a. Если матрица a обратима, то $J(b) = J(a^{-1}ab) \subseteq J(ab)$ и в первом включении — равенство. Второе включение рассматривается аналогично.

(2) *Среди матриц, эквивалентных ненулевой матрице b, имеется матрица с элементом b', находящимся в первой позиции (в первой строке и первом столбце) и являющимся единственным ненулевым элементом первой строки и первого столбца.*

Действительно, так как в области главных идеалов наибольший общий делитель любых элементов является их линейной комбинацией, можно (см. упражнение ниже) обратимым преобразованием столбцов (правым умножением на обратимую матрицу) в первую позицию поставить наибольший общий делитель элементов первой строки. Аналогичное действие возможно для первого столбца. Так как в области главных идеалов не существует бесконечной строго возрастающей цепочки идеалов, то, чередуя подобные действия, можно добиться того, чтобы в первой позиции находился наибольший общий делитель элементов первой строки и первого столбца. После этого посредством элементарных преобразований строк и столбцов следует сделать этот элемент единственным ненулевым элементом первой строки и первого столбца. В результате получается матрица вида

$$d = \begin{pmatrix} d_{11} & 0 & \dots & 0 \\ 0 & d_{22} & \dots & d_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & d_{m2} & \dots & d_{mn} \end{pmatrix}.$$

Рассуждая по-индукции, можно считать, что элемент d_{22} является наибольшим общим делителем всех элементов матрицы, кроме d_{11}. Остаётся прибавить вторую строку к первой и снова выполнить выделение наибольшего общего делителя в первой строке.

(3) *Матрицу с указанным свойством можно получить элементарными преобразованиями строк и столбцов матрицы b, если кольцо K является евклидовой областью.*

Действительно, в этом случае наибольший общий делитель находится алгоритмом Евклида. Это позволяет выделение наибольшего общего делителя выполнить посредством элементарных преобразований (см. упражнения ниже).

(4) *Теперь теорема доказывается индукцией по длине диагонали.*

Сначала матрица приводится к записанному выше виду обратимыми (для евклидовой области — элементарными) преобразованиями, где d_{11} — наибольший общий делитель всех элементов матрицы. Затем аналогичные преобразования производятся для остальных строк и столбцов. Это можно сделать, не затрагивая первую строку и первый столбец. И так далее. □

Следствие. *Обратимая квадратная матрица над евклидовой областью является произведением элементарных матриц.*

Упражнение. Пусть

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

— матрица, составленная из элементов кольца K, обратимая над ним. Преобразование

$$M(m,n,K) \to M(m,n,K),$$
$$\begin{pmatrix} \vdots \\ \overrightarrow{a_i} \\ \vdots \\ \overrightarrow{a_j} \\ \vdots \end{pmatrix} \mapsto \begin{pmatrix} \vdots \\ \alpha\overrightarrow{a_i} + \beta\overrightarrow{a_j} \\ \vdots \\ \gamma\overrightarrow{a_j} + \delta\overrightarrow{a_j} \\ \vdots \end{pmatrix},$$

где $1 \leqslant i < j \leqslant m$, называется *обобщённым элементарным преобразованием строк*. Иными словами, в результате такого преобразования строки матрицы с номерами i, j заменяются линейными комбинациями, как указано выше, а другие строки не меняются. Аналогично, преобразование

$$M(m,n,K) \to M(m,n,K),$$
$$(\ldots, a_i\downarrow, \ldots, a_j\downarrow, \ldots) \mapsto (\ldots, \alpha a_i\downarrow + \beta a_j\downarrow, \ldots, \gamma a_i\downarrow + \delta a_j\downarrow, \ldots),$$

где $1 \leqslant i < j \leqslant n$, называется *обобщённым элементарным преобразованием столбцов*. Заметим, что введённые ранее элементарные преобразования строк и столбцов являются обобщёнными элементарными. Докажите следующее свойство.

∘ В матрице над областью главных идеалов при помощи обобщённого элементарного преобразования строк или столбцов пару элементов (x, y), стоящих в одном столбце или в одной строке, можно заменить парой

элементов $(\gcd(x,y),0)$, а в матрице над евклидовой областью такую замену можно осуществить, выполнив ряд элементарных преобразований.

Указание. Можно воспользоваться следующими свойствами

$$(x,y)\begin{pmatrix}\alpha & y/\delta\\ \beta & -x/\delta\end{pmatrix}=(\delta,0),\ \text{если } \delta=\alpha x+\beta y;$$

$$(x,y)\begin{pmatrix}1 & 0\\ -\gamma & 1\end{pmatrix}=(\delta,y),\ \text{если } x=y\gamma+\delta.$$

Инвариантные делители. Продолжим изучать матрицы над областью главных идеалов. Напомним, что минор порядка k — это опредлитель, составленный из элементов, находящихся в каких-то k строках и k столбцах матрицы. Обозначим $\delta_k(b)$ наибольший общий делитель миноров k-го порядка матрицы b. Эти элементы называются *инвариантными делителями* матрицы a. Отметим ряд свойств.

∘ *У эквивалентных матриц инвариантные делители одного порядка совпадают (с точночность до ассоциированности).*

Доказательство. Строки матрицы ab являются линейными комбинациями строк матрицы b. Это же можно сказать и о минорах указанных матриц любого порядка. Отсюда $\delta_k(b)|\delta_k(ab)$. Если матрица a обратима, то $\delta_k(ab)|\delta_k(b)$, так как $b=a^{-1}(ab)$. Значения $\delta_k(b),\delta_k(ab)$ ассоциированы. □

∘ *Инвариантные множители $d_1,\dots,d_s$ матрицы b следующим образом связаны с инвариантными делителями:*

$$\delta_1(b)=d_1,\delta_2(b)=d_1d_2,\dots,\delta_s(b)=d_1\cdots d_s,\delta_{s+1}(b)=\ldots=\delta_n(b)=0.$$

Доказательство. Это следует из предыдущего. □

∘ *У эквивалентных матриц наборы инвариантных множителей совпадают (с точночность до ассоциированности).*

Доказательство. Это следует из предыдущих свойств. □

Таким образом, имеет место

Теорема. *Каноническая форма Смита для матрицы над областью главных идеалов определена однозначно с точностью до ассоциированности её элементов.*

3. Свободный модуль над областью главных идеалов

В данном разделе каноническая форма матрицы используется для изучения подмодулей свободного модуля над областью главных идеалов. Это будет использоваться в дальнейшем для описания конечно порождённых модулей.

Подмодуль свободного модуль над ОГИ. Имеет место

Теорема (о подмодуле свободного модуля). *Подмодуль свободного модуля ранга n над областью главных идеалов свободен; его ранг не превосходит n.*

Доказательство. Пусть U — подмодуль свободного модуля K^n над областью главных идеалов K. Теорема верна при $n = 1$, так как подмодули в K имеют вид dK. При $n > 1$ применим индукцию. Для прямой суммы $K^n = K^{n-1} \oplus K$ запишем естественное вложение и естественную проекцию:

$$\tau : K^{n-1} \to K^n, (a_1, \dots a_{n-1}) \mapsto (a_1, \dots a_{n-1}, 0),$$
$$\pi : K^n \to K, (a_1, \dots a_n) \mapsto a_n.$$

Имеется короткая точная последовательность

$$0 \longrightarrow U \cap \tau(K^{n-1}) \xrightarrow{\text{id}} U \xrightarrow{\pi} \pi(U) \longrightarrow 0.$$

Она расщепляется (справа) и имеет место изоморфизм

$$U \simeq (U \cap \tau(K^{n-1})) \oplus \pi(U).$$

По предположению индукции U является свободным модулем и его ранг не превосходит значения n. □

Ранг матрицы над областью главных идеалов. Рассмотрим матрицу размера $m \times n$, составленную из элементов области главных идеалов K. Строки этой матрицы порождают подмодуль в K^n, причём свободный в силу доказанной теоремы. Его ранг назовём строчным рангом матрицы. Аналогично, столбцы порождают подмодуль в K^m, ранг которого станем называть столбцовым рангом матрицы. Имеет место

Теорема (о ранге матрицы). *Строчный и столбцовый ранги матрицы над областью главных идеалов совпадают.*

Доказательство. Строчный и столбцовый ранги совпадают с числом ненулевых инвариантных множителей матрицы.

Так как строчный и столбцовый ранги совпадают, етественно называть и тот и другой просто рангом матрицы.

Теорема о базисах. Имеет место

Теорема. *Пусть V — конечно порождённый свободный модуль ранга n над областью главных идеалов K, U — его подмодуль ранга s. Тогда существуют базис $v_1 \dots, v_n$ в V и базис $u_1, \dots, u_s$ в U, а также ненулевые элементы $d_1, \dots, d_s$ в K, такие, что*

$$u_k = v_k \cdot d_k \text{ при } 1 \leqslant k \leqslant s \text{ и } \ d_k | d_{k+1} \text{ при } 1 \leqslant k \leqslant s-1.$$

Доказательство. Пусть в модулях U, V каким-то образом выбраны базисы e, g. Рассмотрим диаграмму

$$\begin{array}{ccccc} V & \xrightarrow{c_e} & K^n & \xleftarrow{a\times} & K^n \\ {\scriptstyle \mathrm{id}}\uparrow & & {\scriptstyle b\times}\uparrow & & {\scriptstyle d\times}\uparrow \\ U & \xrightarrow{c_g} & K^s & \xrightarrow{c\times} & K^s, \end{array}$$

где c_e, c_g — координатные изоморфизмы, id — тождественное вложение, остальные отображения состоят в умножении столбца на матрицу, указанную рядом со стрелкой. В том числе, b оказывается матрицей линейного отображения id относительно выбранных базисов. Пусть d — каноническая форма Смита матрицы b и a, c — некоторые обратимые матрицы, существующие в силу теоремы о канонической матрице. В записанной диаграмме горизонтальные стрелки обратимы. Отсюда видно, что в модулях U, V можно выбрать новые базисы u, v так, чтобы они отобразились по срелкам (или против стрелок, где необходимо) на канонические базисы (состоящие из единичных векторов) в модулях K^n, K^s, стоящих в диаграмме справа. Иными словами, матрица d является матрицей линейного отображения id в новых базисах. Новые базисы удовлетворяют требованиям теоремы. □

4. Конечно-порождённый модуль над ОГИ

В этом разделе доказывается следующая теорема, характеризующая конечно порождённые модули над областью главных идеалов.

Теорема (о конечно порождённых модулях над ОГИ).

Пусть V — конечно порождённый модуль над областью главных идеалов K. Имеет место разложение

$$V \simeq K/Kd_1 \oplus \ldots \oplus K/Kd_s \oplus K^t$$

для некоторых натуральных s, t и ненулевых необратимых элементов $d_1, \ldots, d_s$ из K, таких, что в кольце K выполняются соотношения:

$$d_1 | d_2, \ldots, d_{s-1} | d_s.$$

Числа s, t определены однозначно, набор элементов $d_1, \ldots, d_s$ определён однозначно с точностью до ассоциированности в кольце K.

Элементы $d_1, \ldots, d_s$ в условиях теоремы называются *инвариантными множителями* модуля V.

Доказательство существования. Существование разложения следует из теоремы о базисах учётом упражнения ниже, так как модуль V с n образующими является гомоморфным образом свободного модуля ранга n. Единственность будет доказана позднее, в конце раздела. □

Упражнение. Пусть имеют место включения

$$A' \leqslant A, B' \leqslant B$$

модулей (над кольцом K). Тогда существует изоморфизм

$$(A \oplus B)/(A' \oplus B') \simeq (A/A') \oplus (B/B').$$

Элементарные делители. Пусть p — простой элемент кольца K и k — целое положительное число. Фактор-модуль K/Kp^k называется *примарным* и модуль Kp^k называется его *аннулятором*. Переформулировкой теоремы о конечно-порождённом модуле является следующая

Теорема. *Конечно-порождённый модуль над областью главных идеалов разлагается в прямую сумму свободного и ряда примарных подмодулей. В таком разложении ранг свободного подмодуля и набор аннуляторов примарных подмодулей определены однозначно.*

Равносильность теорем. С учётом упражнения ниже сформулированная теорема равносильна предыдущей, так как по китайской теореме об остатках имеет место разложение

$$K/Kd \simeq K/Kp_1^{k_1} \oplus \ldots \oplus K/Kp_m^{k_m},$$

где $d = p_1^{k_1} \cdots p_m^{k_m}$ и $p_1, \ldots, p_m$ — попарно неассоциированные простые элементы. $\square$

Примарные подмодули, являющиеся слагаемыми при разложении модуля в прямую сумму, будем называть его *примарными компонентами*, а соответствующие элементы p^k называются его *элементарными делителями*. Сформулированная теорема утверждает, что набор элементарных делителей модуля над областью главных идеалов определён однозначно с точностью до ассоциированности. Это утверждение равносильно утверждению о единственности набора инвариантных множителей, содержащемуся в предыдущей теореме.

Упражнение. Как связаны элементарные делители и элементарные множители? Как по набору одних найти набор других?

Подмодуль кручения. Пусть V — конечно порождённый модуль над областью главных идеалов K. Элемент v из V называется *элементом кручения*, если

$$v\lambda = 0 \text{ для некоторого отличного от нуля элемента } \lambda \in K.$$

Элементы кручения составляют подмодуль, который обозначается

$$\mathrm{Tors}(V)$$

и называется *подмодулем кручения*. Модуль V называется *модулем кручения*, если $\mathrm{Tors}(V) = V$ и *модулем без кручения*, если $\mathrm{Tors}(V) = 0$. Отметим ряд свойств.

∘ *Свободный модуль над ОГИ не имеет кручения.* □

∘ *Пусть модуль V разлагается как указано в теореме о конечно-порождённом модуле, тогда*

$$\mathrm{Tors}(V) \simeq K/Kd_1 \oplus \ldots \oplus K/Kd_s;$$
$$V/\mathrm{Tors}(V) \simeq K^t;$$

и имеет место разложение

$$V \simeq \mathrm{Tors}(V) \oplus V/\mathrm{Tors}(V). \square$$

∘ *Над ОГИ конечно порождённый модуль без кручения свободен.* □

∘ *Фактор-модуль $V/\mathrm{Tors}(V)$ не имеет кручения и свободен.* □

p-кручение. Пусть, как и раньше, V — конечно-порождённый модуль над областью главных идеалов K. Пусть также p — простой элемент кольца K. Элемент v из V называется *элементом p-кручения*, если

$$vp^k = 0 \text{ для некоторого целого положительного числа } k.$$

Элементы p-кручения составляют подмодуль, который обозначается

$$\mathrm{Tors}_p(V)$$

и называется *подмодулем p-кручения*. Имеет место следующее свойство.

∘ *Пусть V — конечно-порождённый модуль над ОГИ K. Подмодуль кручения в V разлагается в прямую сумму подмодулей p-кручения:*

$$\mathrm{Tors}(V) \simeq \oplus_p \mathrm{Tors}_p(V),$$

где сумма берётся по набору простых элементов p кольца K, выбранных из различных классов ассоциированности и таких, что $\mathrm{Tors}_p(V) \neq 0$.

Доказательство. Записанное разложение получается из разложения на примарные компоненты, которые для каждого простого элемента p, рассматриваемого с точностью до ассоциированности, следует объеденить в одну прямую сумму. С учётом упражнения ниже для любого p такое объединение совпадает с подмодулем $\mathrm{Tors}_p(V)$. □

Упражнение. Для неассоциированных простых элементов p, q кольца K и целого положительного числа k отображение

$$K/Kp^k \to K/Kp^k, v \mapsto vq,$$

является автоморфизмом модулей.

Доказательство теоремы о конечно-порождённом модуле. Рассмотрим конечно-порождённый модуль V над областью главных идеалов K. В силу доказанного, он разлагается в прямую сумму свободного и ряда примарных подмодулей. Свободный модуль в этом разложении изоморфен $V/\operatorname{Tors}(V)$ и его ранг определён однозначно. Требуется доказать, что набор аннуляторов примарных компонент в этом разложении определён однозначно. В силу свойств, сформулированных выше, достаточно сделать это для модуля $V = \operatorname{Tors}_p(V)$, где p — простой элемент кольца K. Иными словами, нужно доказать, что для модуля

$$V = K/Kp^{k_1} \oplus \ldots \oplus K/Kp^{k_m}$$

набор показателей $k_1, \ldots, k_m$, таких, что $k_1 \geqslant \ldots \geqslant k_m \geqslant 1$ определён однозначно, то есть не существует другого такого убывающего набора показателей. Это так, если $k_1 = k_2 = \ldots = k_m = 1$, поскольку в этом случае V является векторным пространством над полем K/Kp размерности m. Будем доказывать теорему с учётом этого замечания индукцией по величине $k_1 + \ldots + k_m$. В общем случае рассмотрим линейное преобразование

$$V \to V, v \mapsto vp.$$

Его ядро разлагается в прямую сумму из m примарных модулей, изоморфных K/Kp. Образом этого линейного преобразования является модуль

$$Vp = Kp/Kp^{k_1} \oplus \ldots \oplus Kp/Kp^{k_m}.$$

В силу упражнения ниже имеет место изоморфизм

$$Vp \simeq K/Kp^{k_1-1} \oplus \ldots \oplus K/Kp^{k_m-1}.$$

Применяя индукцию и сделанное ранее замечание, заключаем, что наборы аннуляторов для ядра и образа определены однозначно. Но они однозначно определяют аннуляторы примарных компонент разложения модуля V. Теорема доказана. □

Упражнение. Пусть p — простой элемент области главных идеалов K, k — целое положительное число. Имеются следующие эпиморфизм и изоморфизм:

$$K/Kp^k \to Kp/Kp^k, v \mapsto vp,$$
$$K/Kp^{k-1} \to Kp/Kp^k, v + Kp^{k-1} \mapsto vp + Kp^k.$$

5. Нормальные формы матриц

Пусть V — векторное пространство размерности n над полем K,

$$h : V \to V, h : v \mapsto hv$$

— линейный оператор и $\overline{h}_e$ — его матрица в базисе $e = (e_1, \ldots, e_n)$.

Рассмотрим вопрос: как выбрать базис, чтобы матрица линейного преобразования приняла по-возможности простой вид.

Модуль с оператором. Начнём с предварительных замечаний.

∘ Векторное пространство V (над полем K) является одновременно левым модулем над кольцом $\operatorname{End} V$. □

∘ Сказанное остаётся в силе, если вместо кольца $\operatorname{End} V$ рассматривать его коммутативное подкольцо $K[h]$, порождённое эндоморфизмом h. □

∘ Имеется гомоморфизм колец

$$K[x] \to K[h], f(x) \mapsto f(h). \square$$

∘ Ядро данного гомоморфизма ненулевое. □

Доказательство. Действительно, над полем K векторное пространство $\operatorname{End} V$ имеет размерность n^2 и, следовательно, оператор h является корнем ненулевого многочлена степени, не превосходящей n^2. (На самом деле, существует многочлен степени n с этим свойством, именно — характеристический многочлен.) □

∘ Ядро этого гомоморфизма порождается (как идеал) нормированным многочленом минимальной степени, который определён однозначно и называется *минимальным многочленом* линейного оператора h. □

∘ Векторное пространство V (над полем K) является также левым модулем над областью главных идеалов $K[x]$, где умножение на скаляры определено следующим образом:

$$f(x)v = f(h)v. \square$$

Обозначим этот модуль (V, h). Можно применить к нему теорему о конечно порождённом модуле над областью главных идеалов; сделаем это далее. Отметим пока следующее.

∘ Модуль (V, h) является модулем кручения.

Доказательство. Здесь говорится о том, что всякий элемент модуля аннулируется некоторым ненулевым многочленом из кольца $K[x]$ (так, что получается ноль при умножении многочлена на элемент). Действительно, любой многочлен, кратный минимальному, аннулирует все элементы модуля. □

∘ При выборе базиса $e = (e_1, \ldots, e_n)$ в векторном пространстве V возникает изоморфное векторное пространство K^n с изоморфизмом

$$c_e : V \to K^n, v \mapsto v{\downarrow},$$

где $v{\downarrow}$ — столбец координат вектора v в базисе e, такой, что $v = ev{\downarrow}$. Одновременно для модуля с оператором (V, h) возникает изоморфный

модуль (K^n, h_e^*) над кольцом $K[x]$ с тем же изоморфизмом, где

$$h_e^* : K^n \to K^n, v\downarrow \mapsto \overline{h}_e v\downarrow,$$
$$f(x)v\downarrow = f(h_e^*)v\downarrow = f(\overline{h}_e)v\downarrow .\square$$

∘ Итак, *имеется изоморфизм $K[x]$-модулей*

$$(V,h) \to (K^n, h_e^*), v \mapsto v\downarrow . \square$$

Разложение модуля с оператором. Итак, линейному оператору h на векторном пространстве V сопоставлен «модуль с оператором» (V,h) над кольцом $K[x]$. Зафиксируем некоторые его свойства.

В векторном пространстве V над полем K подпространство U называется *инвариантным* (относительно оператора h), если выполняется включение $h(U) \subseteq U$.

∘ *Инвариантные подпространства векторного пространства V совпадают с подмодулями модуля (V,h).*

Доказательство. Это видно непосредственно. □

Предположим, что модуль (V,h) разлагается в прямую сумму:

$$(V,h) = V_1 \oplus \ldots \oplus V_s.$$

Выберем в каждом подпространстве V_l базис $e(l)$, а базис e всего пространства V пусть будет их объединением.

∘ *Матрица преобразования h имеет в базисе e блочно-диагональный вид*

$$\overline{h}_e = \begin{pmatrix} \overline{h}_{e(1)} & & & \\ & \overline{h}_{e(2)} & & \\ & & \ddots & \\ & & & \overline{h}_{e(s)} \end{pmatrix}.$$

∘ Учитывая, что модуль (V,h) является модулем кручения, на основании теоремы о конечно порождённых модулях над ОГИ *запишем разложение с инвариантными множителями*

$$(V,h) \simeq K[x]/d_1(x) \oplus \ldots \oplus K[x]/d_s(x),$$

где для нормированных многочленов $d_1(x), \ldots, d_s(x)$ положительной степени в кольце $K[x]$ выполняются соотношения:

$$d_1(x) | d_2(x), \ldots, d_{s-1}(x) | d_s(x).$$

Отметим, что старший инвариантный множитель $d_s(x)$ является минимальным многочленом.

∘ *Запишем примарное разложение*

$$(V,h) \simeq K[x]/p_1(x)^{k_1} \oplus \ldots \oplus K[x]/p_r(x)^{k_r},$$

где неприводимые над K нормированные многочлены $p_1(x), \ldots, p_r(x)$ не предполагаются различными.

Жордановы клетки. Проясним вид матрицы $\overline{h}_e$ в разных случаях.

∘ Рассмотрим случай $(V, h) \simeq K[x]/d(x)$, где

$$d(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0.$$

Отождествим элементы модуля со смежными классами по изоморфизму, а смежные классы с многочленами минимальной степени в них. Модуль V состоит тогда из многочленов степени меньшей n (которые при умножении на элементы кольца $K[x]$ приводятся по модулю многочлена $d(x)$) и в нём многочлены $1, x, \ldots, x^{n-1}$ составляют базис. Линейный оператор на базисные многочлены действует следующим образом:

$$\begin{aligned}
&h : 1 \mapsto x;\\
&h : x \mapsto x^2;\\
&\quad \ldots\\
&h : x^{n-2} \mapsto x^{n-1};\\
&h : x^{n-1} \mapsto -a_{n-1}x^{n-1} - \ldots - a_0.
\end{aligned}$$

В этом базисе матрица линейного оператора, обозначим её $C(d)$, выглядит так

$$C(d) = \begin{pmatrix} & & -a_0 \\ 1 & & -a_1 \\ & \ddots & \vdots \\ & 1 & -a_{n-1} \end{pmatrix}.$$

Она называется *сопровождающей матрицей* многочлена $d(x)$.

∘ Рассмотрим случай $(V, h) \simeq K[x]/d(x)$, где

$$d(x) = (x - \lambda)^n.$$

Выберем базис $(x-\lambda)^{n-1}, (x-\lambda)^{n-2}, \ldots, (x-\lambda), 1$. Тогда

$$\begin{aligned}
&h :1 \mapsto (x - \lambda) + \lambda,\\
&h :(x - \lambda) \mapsto (x - \lambda)^2 + \lambda(x - \lambda),\\
&\quad \ldots\\
&h :(x - \lambda)^{n-2} \mapsto (x - \lambda)^{n-2} + \lambda(x - \lambda)^{n-1},\\
&h :(x - \lambda)^{n-1} \mapsto \lambda(x - \lambda)^{n-1}.
\end{aligned}$$

Матрица линейного оператора выглядит теперь так

$$J(d) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \lambda & 1 \\ & & & \lambda \end{pmatrix}.$$

Такая матрица называется *жордановой клеткой*. Возвращаясь к разложению с инвариантными множителями, получаем следующее свойство.

∘ Матрицей оператора h в некотором базисе является матрица

$$\begin{pmatrix} C(d_1) & & & \\ & C(d_2) & & \\ & & \ddots & \\ & & & C(d_s) \end{pmatrix},$$

где d_i — нормированные многочлены и $d_1|d_2, \ldots, d_{s-1}|d_s$. Здесь набор матриц $C(d_i)$, где $1 \leqslant i \leqslant s$, определён однозначно с точностью до порядка. Записанная матрица называется *первой нормальной формой* матрицы линейного оператора h. Возвращаясь к примарному разложению, получаем следующее свойство.

∘ Матрицей оператора h в некотором базисе является матрица

$$\begin{pmatrix} C(p_1^{k_1}) & & & \\ & C(p_2^{k_2}) & & \\ & & \ddots & \\ & & & C(p_r^{k_r}) \end{pmatrix},$$

где $p_i(x)$ — нормированные неприводимые многочлены над K, k_i — целые положительные числа. Здесь набор матриц $C(p_i^{k_i})$, где $1 \leqslant i \leqslant r$, определён однозначно с точностью до порядка. Записанная матрица называется *второй нормальной формой*, а также *рациональной формой*, матрицы линейного оператора. Имеет место

Теорема. *Для любой матрицы, составленной из элементов поля, найдётся подобная матрица над этим полем, находящаяся в рациональной форме. Рациональная форма определена однозначно с точностью до перестановки диагональных блоков.* □

∘ Предположим, что инвариантные множители $d_1(x), d_2(x), \ldots, d_s(x)$ линейного оператора h разлагаются на линейные множители. Элементарные делители $p_i^{k_i}(x)$ являются тогда степенями нормированных линейных многочленов и матрицей линейного оператора h является следующая

матрица

$$\begin{pmatrix} J(p_1^{k_1}) & & & \\ & J(p_2^{k_2}) & & \\ & & \ddots & \\ & & & J(p_r^{k_r}) \end{pmatrix},$$

где $p_i(x)$ — нормированные линейные многочлены над полем K, k_i — целые положительные числа. Здесь матрицы $J(p_i^{k_i})$, где $1 \leqslant i \leqslant r$, определены однозначно с точностью до порядка. Записанная матрица называется *третьей нормальной формой*, а также *жордановой матрицей*, линейного оператора. Имеет место

Теорема. *Для любой матрицы, составленной из элементов алгебраически замкнутого поля, найдётся подобная матрица над этим полем, находящаяся в жордановой форме. Жорданова форма определена однозначно с точностью до перестановки диагональных блоков.* □

Характеристический многочлен. Напомним, матрица $(\mathrm{e}_n x - \overline{h})$ называется *характеристической* матрицей оператора h, её определитель называется *характеристическим* многочленом оператора h. Имеет место

Теорема. *Пусть $\overline{h}$ — матрица линейного оператора h над полем K. Тогда каноническая форма Смита матрицы $(\mathrm{e}_n x - \overline{h})$ над кольцом $K[x]$ имеет вид*

$$\begin{pmatrix} \mathrm{e}_{n-s} & & & \\ & d_1(x) & & \\ & & \ddots & \\ & & & d_s(x) \end{pmatrix},$$

где $d_1(x), \ldots, d_s(x)$ — инвариантные множители оператора h.

Иными словами, инвариантные множители линейного оператора совпадают с необратимыми инвариантными множителями его характеристической матрицы.

Доказательство. Матрицу $(\mathrm{e}_n x - \overline{h})$ можно привести к диагональному виду левым и правым умножением на матрицы, обратимые над кольцом $K[x]$, следующим образом. Можно считать, что матрица $\overline{h}$ находится в рациональной форме. Тогда матрица $(\mathrm{e}_n x - \overline{h})$ состоит из диагональных блоков вида

$$\mathrm{e}_m x - C(d) = \begin{pmatrix} x & & & a_0 \\ -1 & x & & a_1 \\ & \ddots & \ddots & \vdots \\ & & -1 & x + a_{m-1} \end{pmatrix},$$

где $d(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ — произвольный инвариантный множитель оператора h. Каждая такая диагональная клетка приводится далее к диагональному виду элементарными преобразованиями строк и столбцов. Для этого сначала к первой строке прибавляются остальные, умноженные на степени $x, x^2, \ldots, x^{m-1}$. В результате получается матрица

$$\begin{pmatrix} 0 & 0 & & d(x) \\ -1 & x & & a_1 \\ & \ddots & \ddots & \vdots \\ & & -1 & x + a_{m-1} \end{pmatrix}.$$

Далее строки этой матрицы циклически сдвигаются вверх, в результате получается верхнетреугольная матрица

$$\begin{pmatrix} -1 & x & & a_1 \\ & \ddots & \ddots & \vdots \\ & & -1 & x + a_{m-1} \\ 0 & \ldots & 0 & d(x) \end{pmatrix}.$$

Прибавляя к столбцам столбцы, кратные предшествующим, приводим матрицу к диагональной форме

$$\begin{pmatrix} -1 & & & \\ & \ddots & & \\ & & -1 & \\ & & & d(x) \end{pmatrix}.$$

После того, как каждая диагональная клетка характеристической матрицы приведена к такой диагональной форме, остаётся поменять знаки у части диагональных элементов и переставить их нужным образом. □

Следствием теоремы является

Теорема Гамильтона-Кэли. *Линейное преобразование h и его матрица $\overline{h}$ в произвольном базисе являются корнями многочлена*

$$\chi_h(x) = \det(\mathrm{e}_n x - \overline{h}).$$

Доказательство. По предыдущей теореме

$$\det(\mathrm{e}_n x - \overline{h}) = \prod_k d_k(x).$$

Это произведение аннулирует h, так как старший инвариантный множитель $g_s(x)$ совпадает с минимальным многочленом. □

ГЛАВА 26

Алгебраические числа

Алгебраическим называется комплексное число, алгебраическое над полем рациональных чисел, то есть являющееся корнем ненулевого многочлена с рациональными коэффициентами. Алгебраические числа составляют алгебраически замкнутое поле, которое является бесконечным алгебраическим расширением поля рациональных чисел.

Всякое конечное расширение поля рациональных чисел называется также *числовым полем*. Оно алгебраично, то есть состоит из алгебраических чисел, и получается присоединением к полю рациональных чисел конечного множества величин и даже некоторой одной величины, в силу теоремы о примитивном элементе.

Алгебраические числа, которые являются корнями целочисленных нормированных многочленов, называются *целыми алгебраическими*. Они образуют кольцо. Целые алгебраические числа, лежащие в числовом поле, также образуют кольцо, которое называется далее *числовым кольцом*.

К традиционным вопросам теории алгебраических чисел относятся следующие: в каких случаях в числовом кольце выполняется основная теорема арифметики, как разлагаются целые рациональные числа в числовых кольцах, как устроена мультипликативная группа числового кольца. Некоторые из этих вопросов будут рассмотрены в данной главе.

Далее, когда не оговаривается иное, кольца предполагаются целостными нулевой характеристики, последнее относится и к полям.

1. Целые элементы расширения колец

В этом разделе определяются целые алгебраические числа.

Целые алгебраические числа. Имеет место

Теорема. *Для алгебраического числа α равносильны условия:*

(1) *минимальный многочлен $p_\alpha(x)$ числа α (над полем рациональных чисел) имеет целые коэффициенты;*

(2) *число α является корнем нормированного целочисленного многочлена;*

(3) *кольцо $\mathbb{Z}[\alpha]$ является конечно-порождённым $\mathbb{Z}$-модулем;*

(4) *существует ненулевой конечно-порождённый $\mathbb{Z}$-модуль $M \leqslant \mathbb{C}$, для которого выполняется включение: $\alpha M \leqslant M$.*

Доказательство. Докажем необходимые имликации.

$(1 \to 2)$ Эта импликация очевидна.

$(2 \to 3)$ Пусть число α является корнем нормированного многочлена с целыми коэффициентами, то есть для некоторых целых чисел $a_1, \dots a_n$ выполняется равенство

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_n\alpha^0 = 0.$$

Тогда n-я степень α следующим образом выражается через предыдущие:

$$\alpha^n = (-a_1)\alpha^{n-1} + \ldots + (-a_n)\alpha^0.$$

Отсюда видно, что набор элементов

$$\alpha^0, \dots, \alpha^{n-1}$$

является образующим в $\mathbb{Z}$-модуле $\mathbb{Z}[\alpha]$, так, что

$$\begin{aligned}\mathbb{Z}[\alpha] =& \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \ldots \\ =& \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \ldots \mathbb{Z}\alpha^{n-1}.\end{aligned}$$

Таким образом, имеет место третье условие.

$(3 \to 4)$ Эта импликация очевидна, поскольку можно взять $M = \mathbb{Z}[\alpha]$.

$(4 \to 2)$ Рассмотрим $\mathbb{Z}$-модуль

$$M = \mathbb{Z}\beta_1 + \ldots + \mathbb{Z}\beta_n,$$

порождённый элементами $\beta_1, \dots, \beta_n$. Пусть выполняется включение $\alpha M \subseteq M$. Тогда для некоторой целочисленной матрицы $\overline{\mu}_\alpha$ размера n выполняются равенства:

$$\begin{aligned}&(\beta_1, \dots, \beta_n)\alpha = (\beta_1, \dots, \beta_n)\overline{\mu}_\alpha, \\ &(\beta_1, \dots, \beta_n)(\mathrm{e}\alpha - \overline{\mu}_\alpha) = 0, \\ &(\beta_1, \dots, \beta_n)(\mathrm{e}\alpha - \overline{\mu}_\alpha)\operatorname{adj}(\mathrm{e}\alpha - \overline{\mu}_\alpha) = 0.\end{aligned}$$

Вместе с тем,

$$(\mathrm{e}\alpha - \overline{\mu}_\alpha)\operatorname{adj}(\mathrm{e}\alpha - \overline{\mu}_\alpha) = \mathrm{e}\det(\mathrm{e}\alpha - \overline{\mu}_\alpha).$$

Отсюда видно, что число α является корнем целочисленного нормированного многочлена

$$\det(\mathrm{e}x - \overline{\mu}_\alpha).$$

$(2 \to 1)$ Предположим, что число α является корнем целочисленного нормированного многочлена, тогда оно является корнем некоторого такого многочлена, неприводимого над кольцом целых чисел. Он остаётся неприводимым и над полем рациональных чисел в силу леммы Гаусса о

содержании и совпадает тогда с минимальным многочленом элемента α. Таким образом, выполняется первое условие. Теорема доказана. $\square$

Комплексное число α, для которого выполняются условия этой теоремы, называется *целым алгебраическим*. Множество целых алгебраических чисел числового поля K обозначают через $\mathcal{O}_K$. Имеет место

Следствие. *Множество $\mathcal{O}_K$ является кольцом.*

Доказательство. Пусть целые алгебраические числа β, γ содержатся в конечно порождённых $\mathbb{Z}$-модулях

$$\mathbb{Z}[\beta] = \mathbb{Z}\beta^0 + \ldots + \mathbb{Z}\beta^n, \mathbb{Z}[\gamma] = \mathbb{Z}\gamma^0 + \ldots + \mathbb{Z}\gamma^m.$$

Из разность и произведение также являются целыми алгебраическими числами, так как принадлежат конечно порождённому $\mathbb{Z}$-модулю

$$\mathbb{Z}[\beta, \gamma] = \mathbb{Z}\beta^0\gamma^0 + \ldots + \mathbb{Z}\beta^n\gamma^m. \square$$

Кольцо $\mathcal{O}_K$ называется *числовым* кольцом (числового поля K).

Следствие. *Для любого элемента α из числового поля K найдётся целое число m, такое, что $m\alpha \in \mathcal{O}_K$. В частности, $K = \mathrm{Frac}(\mathcal{O}_K)$.*

Доказательство. Достаточно доказать первое утверждение. Пусть α — алгебраическое число. Оно является корнем многочлена с рациональными коэффициентами и тогда является корнем некоторого целочисленного многочлена. Таким образом, для некоторых целых чисел $a_0, \ldots, a_n$ выполняюся равенства

$$a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_n\alpha^0 = 0,$$
$$(a_0\alpha)^n + a_1(a_0\alpha)^{n-1} + \ldots + a_n a_0^{n-1}(a_0\alpha)^0 = 0,$$

где второе равенство получается из первого умножением на элемент a_0^{n-1}. Для завершения доказательства нужно взять $m = a_0$. $\square$

Целое замыкание. Пусть A, B — целостные кольца, причём A является подкольцом кольца B; в этом случае кольцо B называют также расширением кольца A и обозначается B/A. Доказанная в предыдущем разделе теорема имеет следующее естественное обобщение.

Теорема. *Пусть кольцо B является расширением кольца A. Тогда для любого элемента α из B следующие условия равносильны.*

(2) *Элемент α является корнем нормированного многочлена с коэффициентами в кольце A.*

(3) *Кольцо $A[\alpha]$ является конечно-порождённым A-модулем.*

(4) *Существует ненулевой конечно-порождённый A-модуль $M \leqslant B$, для которого выполняется включение: $\alpha M \leqslant M$.*

Доказательство этой теоремы принципиально не отличается от доказательства предыдущей. □

Элемент α, для которого выполняются условия (2–4) этой теоремы, называется *целым* над кольцом A, а также *целым элементом расширения* B/A. Множество всех таких элементов называется *целым замыканием* кольца A в кольце B.

Следствие. *Пусть кольцо A является подкольцом кольца B. Тогда множество элементов из B, целых над A, образует подкольцо в B.* □

Пусть кольцо C является целым замыканием кольца A в расширении B. В частности, имеют место включения

$$A \leqslant C \leqslant B.$$

В этой ситуации кольцо B называют *целым* над кольцом A, если $B = C$. Кольцо A называют *целозамкнутым* в B, если выполняется равенство $A = C$. Кольцо, целозамкнутое в своём поле частных, называют *целозамкнутым*. Имеет место

Замечание. Пусть кольцо A целозамкнуто. Тогда условиям (2–3) доказанной выше теоремы равносильно ещё одно, следующее, условие.

(1) *Коэффициенты минимального многочлена элемента α над полем $K = \mathrm{Frac}(A)$ содержатся в кольце A.*

Доказательство. Достаточно проверить, что из второго условия теоремы следует записанное выше первое условие. Пусть элемент α из кольца B является корнем некоторого многочлена $f(x)$ с коэффициентами в кольце A. Этот многочлен делится над полем K на минимальный для элемента α многочлен. В силу этого, все корни минимального многочлена (лежащие в некотором поле, включающем кольцо B) являются также корнями многочлена $f(x)$ и являются тогда целыми над кольцом A. Но тогда и коэффициенты минимального многочлена являются целыми над кольцом A. Они принадлежат этому кольцу в силу его целозамкнутости, а также в силу соотношений Виета. □

Теорема. *Область с однозначным разложением целозамкнута.*

Доказательство. Пусть a/b — дробь из поля частных области с однозначным разложением R. Предположим, она является корнем нормированного многочлена с коэффициентами в R, то есть для некоторых значений $a_1, \ldots, a_n$ из кольца R выполняется равенство:

$$(a/b)^n + a_1(a/b)^{n-1} + \ldots + a_n(a/b)^0 = 0.$$

Тогда

$$a^n + a_1 a^{n-1} b + \ldots + a_n a^0 b^n = 0.$$

Отсюда видно, что все простые делители знаменателя дроби являются делителями её числителя; знаменатель делит числитель; дробь принадлежит кольцу R; оно целозамкнуто. □

Конечные расширения колец. Расширение B кольца A называют *целым*, если все его элементы целые над A. Расширение B называют *конечным*, если оно является конечно-порождённым A-модулем; иными словами, для некоторых элементов $\beta_1, \ldots, \beta_m$ выполняется равенство:

$$B = A\beta_1 + \ldots + A\beta_m.$$

Оно называется *конечно-порождённым*, если получается в результате присоединения конечного числа элементов, так, что для некоторых элементов $\beta_1, \ldots, \beta_m$ выполняется равенство:

$$B = A[\beta_1, \ldots, \beta_m].$$

Имеет место

Теорема. *Расширение колец тогда и только тогда конечное, когда оно целое и конечно-порождённое.*

Доказательство. Пусть B — конечное расширение кольца A. Очевидно, оно является конечно-порождённым. Оно является целым, так как для любого его элемента α выполняется включение $\alpha B \subseteq B$. Необходимость доказана. Обратно, пусть кольцо B целое и конечно-порождённое. Предположим, оно получается присоединением к кольцу A целых над ним элементов $\beta_1, \ldots, \beta_m$, являющихся корнями нормированных многочленов с коэффициентами в кольце A степеней $n_1, \ldots, n_m$. В этом случае

$$B = \sum_{k_1,\ldots,k_m} A\beta_1^{k_1} \cdots \beta_m^{k_m},$$

где $k_1 < n_1, \ldots, k_m < n_m$. Таким образом, расширение B конечное. □

Следствие. *Кольцо целых элементов расширения колец целозамкнуто в нём.* □

Следствие. *Числовое кольцо целозамкнуто.* □

2. Норма и след

В этом разделе вводятся в рассмотрение две важные характеристики конечного расширения полей — функции нормы и следа.

Вложения полей. Пусть поле L является конечным расширением поля K степени n, Ω — алгебраически замкнутое поле и имеется изоморфное вложение полей

$$\tau : K \to \Omega, a \mapsto a^\tau;$$

которое далее вполне можно считать тождественным; оно продолжается до изоморфного вложения

$$\tau : K[x] \to \Omega[x], f(x) \mapsto f^\tau(x),$$

полиномиальных колец, где

$$\big(\sum a_i x^i\big)^\tau = \sum a_i^\tau x^i.$$

По теореме о примитивном элементе расширение L/K является простым и получается присоединением некоторого одного элемента α:

$$L = K(\alpha).$$

Обозначим через $p_\alpha(x)$ минимальный многочлен элемента α над полем K. Напомним, что это нормированный неприводимый над полем K многочлен с корнем α. Многочлен $p_\alpha^\tau(x)$ неприводим над полем

$$K^\tau = \{a^\tau | a \in K\}$$

и имеет в поле Ω ровно n различных корней, обозначим их

$$\alpha_1, \ldots, \alpha_n;$$

таким образом, над полем Ω имеется разложение

$$p_\alpha^\tau(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

Будем интересоваться вложениями

$$\sigma : L \to \Omega, \text{ где } \sigma|_K = \tau,$$

поля L в поле Ω, совпадающими с τ на K. Отметим ряд свойств.

∘ Имеются изоморфные вложения полей

$$\begin{array}{ccccc} K & \xrightarrow{\text{id}} & K(\alpha) & \xrightarrow{\cong} & K[x]/(p_\alpha(x)) \\ & & & & \downarrow \cong \\ \Omega & \xleftarrow{\text{id}} & K^\tau(\alpha_i) & \xleftarrow{\cong} & K^\tau[x]/(p_\alpha^\tau(x)), \end{array}$$

$$\begin{array}{cccc} \text{где} & f(\alpha) & \longmapsto & f(x) + (p_\alpha(x)) \\ & & & \downarrow \\ & f^\tau(\alpha) & \longmapsto & f^\tau(x) + (p_\alpha^\tau(x)). \end{array}$$

Здесь $f(x)$ — произвольный многочлен с коэффициентами в K. □

∘ Отсюда, имеется ровно n различных изоморфных вложений

$$\sigma_1, \ldots, \sigma_n : K(\alpha) \to \Omega, \text{ где } \sigma_1|_K = \ldots = \sigma_n|_K = \tau,$$

поля $K(\alpha)$ в поле Ω, совпадающих с τ на L. Эти вложения такие:

$$\sigma_i : K(\alpha) \to \Omega,$$
$$f(\alpha) \mapsto f^\tau(\alpha_i),$$

где $1 \leqslant i \leqslant n$. $\square$

Отметим ещё одно свойство.

$\circ$ Вложеия $\sigma_1, \ldots, \sigma_n$ линейно независимы над полем Ω. $\square$

Таким образом, имеет место

Теорема. *Существует ровно n различных изоморфных вложений конечного расширения L/K степени n в алгебраически замкнутое расширение Ω/K. Эти вложения линейно независимы над полем Ω.* $\square$

Здесь под изоморфным вложением расширения L/K в расширение Ω/K понимается изоморфное вложение поля L в поле Ω, тождественное на поле K.

Норма и след. Пусть задано конечное расширение полей L/K степени $n = [L : K]$ и некоторый его элемент α степени $s = [K(\alpha) : K]$. Рассмотрим отображение

$$\mu_\alpha : L \to L, x \mapsto \alpha x.$$

Это отображение является линейным преобразованием поля L, рассматриваемого как векторное пространство над полем K. Зафиксируем в этом векторном пространстве произвольный базис и обозначим $\overline{\mu}_\alpha$ матрицу рассматриваемого линейного преобразования в этом базисе. Характеристический многочлен

$$\chi_\alpha(x) = \det(\mathrm{e}_n x - \overline{\mu}_\alpha)$$

этого линейного преобразования называется характеристическим многочленом элемента α над полем K. Отметим следующее свойство.

$\circ$ *Пусть $s = [K(\alpha) : K]$ — степень элемента α и $p_\alpha(x)$ — его минимальный многочлен над полем K. Тогда имеет место равенство:*

$$\chi_\alpha(x) = p_\alpha(x)^{n/s}.$$

Доказательство. Пусть

$$\beta = (\beta_1, \ldots, \beta_s), \gamma = (\gamma_1, \ldots, \gamma_{n/s}),$$

— базисы расширений $K(\alpha)/K$ и $L/K(\alpha)$. Тогда базис расширения L/K составляют произведения

$$\beta_1\gamma_1, \ldots, \beta_s\gamma_1, \ldots, \beta_1\gamma_n, \ldots, \beta_s\gamma_n.$$

В этом базисе матрица преобразования μ_α блочно диагональная, где на диагонали находятся n/s блоков размера s, совпадающих с матрицей преобразования μ_α, ограниченного на подполе $K(\alpha)$. Тогда

$$\chi_\alpha(x) = \det(\mathrm{e}_n x - \overline{\mu}_\alpha) = \det(\mathrm{e}_s x - \overline{\mu})^{n/s},$$

где $\overline{\mu}_\alpha$ — матрица преобразования μ_α в записанном базисе и $\overline{\mu}$ — матрица ограниченного преобразования в базисе β. Осталось заметить, что

$$\det(\mathrm{e}_s x - \overline{\mu}) = p_\alpha(x). \ \square$$

Сделаем следующее

Определение. *Следом* и *нормой* в расширении L/K называются соответствующие функции

$$\mathrm{tr} : L \mapsto K, \alpha \mapsto \mathrm{tr}(\overline{\mu}_\alpha);$$
$$\mathrm{nr} : L \mapsto K, \alpha \mapsto \det(\overline{\mu}_\alpha).$$

Далее приведём ряд свойств, каждое из которых можно использовать в качестве альтернативного определения нормы и следа элемента α.

$\circ$ Имеет место равенство

$$\chi_\alpha(x) = x^n - \mathrm{tr}(\alpha)x^{n-1} + \ldots + (-1)^n \mathrm{nr}(\alpha)x^0.$$

$\circ$ Имеет место равенство

$$p_\alpha(x)^{n/s} = x^n - \mathrm{tr}(\alpha)x^{n-1} + \ldots + (-1)^n \mathrm{nr}(\alpha)x^0.$$

$\circ$ Пусть $\sigma_1, \ldots, \sigma_n$ — различные тождественные на поле K вложения поля L в алгебраически замкнутое поле, включающее K. Тогда

$$\mathrm{tr}(\alpha) = \sum_k \sigma_k(\alpha); \mathrm{nr}(\alpha) = \prod_k \sigma_k(\alpha).$$

$\circ$ Пусть $\sigma_1, \ldots, \sigma_s$ — различные тождественные на поле K вложения поля $K(\alpha)$ в алгебраически замкнутое поле, включающее K. Тогда

$$\mathrm{tr}(\alpha) = (n/s)\sum_k \sigma_k(\alpha); \mathrm{nr}(\alpha) = \prod_k \sigma_k(\alpha)^{n/s}.$$

$\circ$ Пусть $\alpha_1, \ldots, \alpha_s$ — различные корни многочлена $p_\alpha(x)$ в некотором расширении поля K, где многочлен $p_\alpha(x)$ разлагается на линейные множители следующим образом:

$$p_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_s).$$

Тогда

$$\mathrm{tr}(\alpha) = (n/s)\sum_k \alpha_k; \mathrm{nr}(\alpha) = \prod_k \alpha_k^{n/s}.$$

∘ Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена $\chi_\alpha(x)$ в некотором расширении поля K, где многочлен $p_\alpha(x)$ разлагается на линейные множители следующим образом:

$$\chi_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

Тогда

$$\mathrm{tr}(\alpha) = \sum_k \alpha_k; \mathrm{nr}(\alpha) = \prod_k \alpha_k.$$

Упражнение. Докажите записанные выше свойства.

Замечание. Норма и след зависят от расширения. Если понадобится расширение указать явно, запишем его в качестве нижнего индекса, так:

$$\mathrm{tr}_{L/K}, \mathrm{nr}_{L/K}\,.$$

Свойства нормы и следа. Пусть имеется конечное расширение полей L/K степени n. Пусть также α, β, γ — произвольные элементы этого расширения и c — элемент поля K. Отметим следующие свойства.

∘ *Значения функций* nr, tr *лежат в поле* K*:*

$$\mathrm{nr}(\alpha), \mathrm{tr}(\alpha) \in K.$$

Доказательство. Это видно из определения. □

∘ *Более того,*

$$\mathrm{nr}(\alpha), \mathrm{tr}(\alpha) \in R,$$

если элемент α *целый над кольцом* $R \leqslant K$*, целозамкнутым в* K*.*

Доказательство. Для любого тождественного на K вложения σ поля L в поле $\mathbb{C}$ комплексных чисел образ $\sigma(\alpha)$ элемента α является целым над кольцом R вслед за элементом α и тогда принадлежит этому кольцу в силу его целозамкнутости. Вместе с тем, норма $\mathrm{nr}(\alpha)$ и след $\mathrm{tr}(\alpha)$ могут быть определены как сумма и произведение таких образов $\sigma(\alpha)$. Следовательно, и они принадлежат кольцу R. □

∘ *В частности, эти значения рациональные:*

$$\mathrm{nr}(\alpha), \mathrm{tr}(\alpha) \in \mathbb{Q},$$

если α *— алгебраическое число. Они целые:*

$$\mathrm{nr}(\alpha), \mathrm{tr}(\alpha) \in \mathbb{Z},$$

если α *— целое алгебраическое.*

Доказательство. Это следует из предыдущих свойств. □

∘ *Для элемента* α *из* K *имеют место равенства*

$$\mathrm{nr}(\alpha) = \alpha^n, \mathrm{tr}(\alpha) = n\alpha$$

Доказательство. Для доказательства можно рассмотреть норму и след как произведение и сумму вложений. □

∘ *Норма мультипликативна:*

$$\mathrm{nr}(\alpha\beta) = \mathrm{nr}(\alpha)\,\mathrm{nr}(\beta); \mathrm{nr}(c\alpha) = c^n\,\mathrm{nr}(\alpha).$$

Доказательство. Для доказательства можно рассмотреть норму как произведение вложений. □

∘ В частности, $\mathrm{nr}(1) = 1$ и $\mathrm{nr}(1/\alpha) = 1/\,\mathrm{nr}(\alpha)$ для $\alpha \neq 0$.

Доказательство. Это следует из определения и предыдущих свойств. □

∘ *След аддитивен:*

$$\mathrm{tr}(\alpha + \beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta); \mathrm{tr}(c\alpha) = c\,\mathrm{tr}(\alpha).$$

Доказательство. Можно рассмотреть след как сумму вложений. □

∘ *Пусть имеется цепочка расширений полей $K \leqslant L \leqslant M$. Тогда имеют место следующие свойства транзитивности:*

$$\mathrm{nr}_{M/K} = \mathrm{nr}_{L/K} \circ \mathrm{nr}_{M/L}; \mathrm{tr}_{M/K} = \mathrm{tr}_{L/K} \circ \mathrm{tr}_{M/L}\,.$$

Доказательство. Это видно из определения нормы и следа как произведения и суммы вложений, так как вложениями расширения M/K в алгебраически замкнутое расширение Ω/K являются произведения

$$\sigma = \sigma'' \circ \sigma',$$

где σ', σ'' — вложения расширений M/L и L/K в расширения Ω/L и Ω/K. □

∘ *Пусть имеется цепочка расширений полей $K \leqslant L \leqslant M$. Тогда имеют место равенства*

$$\mathrm{nr}_{M/K}(\alpha) = \mathrm{nr}_{L/K}(\alpha)^{[M:L]}, \mathrm{tr}_{M/K}(\alpha) = [M : L]\,\mathrm{tr}_{L/K}(\alpha).$$

(Напомним, что $\alpha \in L$.)

Доказательство. Записанные равенства являются следствием предыдущего свойства. □

Упражнение. Докажите следующие факты:

∘ $\alpha \in \mathcal{O}_L^\times \Leftrightarrow \mathrm{nr}(\alpha) = 1$;

∘ элементы с простой нормой неприводимы в кольце $\mathcal{O}_L$.

Замечание. Пусть L/K — расширение колец, где кольцо L является конечно порождённым свободным модулем над кольцом K. Как в случае полей, для любого элемента α из кольца L можно рассмотреть отображение μ_α и с его помощью определить след и норму элемента α в расширении L/K.

Упражнение. Какие свойства нормы и следа сохранят силу при таком определении?

3. Дискриминант числового поля

В этом разделе определяется дискриминант числового поля.

Дискриминант расширения. Пусть, по-прежнему, L/K — конечное расширение полей степени n. Его *дискриминант* — это отображение

$$L^2 \to K, (x, y) \mapsto \mathrm{tr}(xy).$$

Отметим следующие свойства.

∘ Отображение tr симметрично, имеет место равенство:

$$\mathrm{tr}(\alpha\beta) = \mathrm{tr}(\beta\alpha).$$

для всех α, β из L.

∘ Отображение tr билинейно, верны равенства:

$$\begin{aligned}
&\mathrm{tr}((\alpha+\beta)\gamma) = \mathrm{tr}(\alpha\gamma) + \mathrm{tr}(\beta\gamma),\\
&\mathrm{tr}(\alpha(\beta+\gamma)) = \mathrm{tr}(\alpha\beta) + \mathrm{tr}(\alpha\gamma),\\
&\mathrm{tr}(c\alpha\beta) = \mathrm{tr}(\alpha c\beta) = c\,\mathrm{tr}(\alpha\beta)
\end{aligned}$$

для всех α, β из L, c из K.

∘ Билинейная форма tr невырождена: если равенство

$$\mathrm{tr}(\alpha\beta) = 0$$

выполняется при некотором α и всех β из L, то $\alpha = 0$.

Доказательство. Пусть $\sigma_1, \ldots, \sigma_n$ — различные вложения расширения L/K в алгебраически замкнутое расширение Ω/K. Заметим, что для любых значений α, β из поля L верно

$$\mathrm{tr}(\alpha\beta) = \sum_i \sigma_i(\alpha\beta) = \sum_i \sigma_i(\alpha)\sigma_i(\beta).$$

Тогда, если выполняется указанное условие, то имеет место следующее соотношение линейной зависимости между вложениями:

$$\sum_i \sigma_i(\alpha)\sigma_i = 0.$$

В силу линейной независимости вложений получаем набор равенств

$$\sigma_1(\alpha) = 0, \ldots, \sigma_n(\alpha) = 0,$$

любое из которых влечёт $\alpha = 0$. □

Матрица Грама. Пусть, по-прежнему, L/K — конечное расширение полей степени n. Для набора элементов

$$\overline{\alpha} = (\alpha_1, \ldots, \alpha_n),$$

принадлежащих полю L, рассмотрим матрицу

$$\mathrm{Tr}(\overline{\alpha}) = \begin{pmatrix} \mathrm{tr}(\alpha_1\alpha_1) & \mathrm{tr}(\alpha_1\alpha_2) & \ldots & \mathrm{tr}(\alpha_1\alpha_n) \\ \mathrm{tr}(\alpha_2\alpha_1) & \mathrm{tr}(\alpha_2\alpha_2) & \ldots & \mathrm{tr}(\alpha_2\alpha_n) \\ \vdots & \vdots & & \vdots \\ \mathrm{tr}(\alpha_n\alpha_1) & \mathrm{tr}(\alpha_n\alpha_2) & \ldots & \mathrm{tr}(\alpha_n\alpha_n) \end{pmatrix}.$$

Она называется *матрицей Грама* этого набора элементов относительно расширения L/K. Отметим ряд её свойств.

$\circ$ Для любых элементов x, y из поля L и элементов x_i, y_i из поля K, где $1 \leqslant i \leqslant n$, таких, что

$$x = \sum_i x_i\alpha_i, y = \sum_i y_i\alpha_i,$$

имеет место равенство

$$\mathrm{tr}(xy) = (x_1, \ldots, x_n)\,\mathrm{Tr}(\overline{\alpha})(y_1, \ldots, y_n)^{\mathrm{T}}.$$

$\circ$ Пусть наборы $\overline{\alpha}, \overline{\beta}$ элементов поля L связаны соотношением

$$\overline{\beta} = \overline{\alpha}c_{\alpha,\beta},$$

где $c_{\alpha,\beta}$ — некоторая квадратная матрица размера n, составленная из элементов поля K. Тогда верно равенство

$$\mathrm{Tr}(\overline{\beta}) = c_{\alpha,\beta}^{\mathrm{T}}\,\mathrm{Tr}(\overline{\alpha})c_{\alpha,\beta}. \square$$

Матрица вложений. По-прежнему, L/K — конечное расширение полей степени n, $\overline{\alpha}$ — набор из n элементов поля L. Рассмотрим матрицу

$$\Sigma(\overline{\alpha}) = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \ldots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \ldots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \ldots & \sigma_n(\alpha_n). \end{pmatrix},$$

где $\sigma_1, \ldots, \sigma_n$ — различные вложения расширения L/K в алгебраически замкнутое расширение Ω/K. Отметим ряд свойств этой матрицы.

$\circ$ Имеет место равенство.

$$\mathrm{Tr}(\overline{\alpha}) = \Sigma(\overline{\alpha})^{\mathrm{T}}\Sigma(\overline{\alpha}).$$

$\circ$ Следующие условия равносильны.

(1) Матрица $\mathrm{Tr}(\overline{\alpha})$ обратима.

(2) Матрица $\Sigma(\overline{\alpha})$ обратима.

(3) Элементы набора $\overline{\alpha}$ линейно независимы над полем K.

Замечание. Матрицы

$$\mathrm{Tr}(\overline{\alpha}), \Sigma(\overline{\alpha})$$

зависят от расширения. При необходимости эту зависимость можно указать нижним индексом:

$$\mathrm{Tr}_{L/K}(\overline{\alpha}), \Sigma_{L/K}(\overline{\alpha}).$$

Дуальный базис. Пусть L/K — расширение полей степени n с базисом $\overline{\alpha}$. Его матрица Грама обратима, набор векторов

$$\overline{\alpha}^* = (\alpha_1^*, \ldots, \alpha_n^*), \text{ где } \overline{\alpha}^* = \overline{\alpha}\,\mathrm{Tr}(\overline{\alpha})^{-1}$$

также является базисом. Такой базис называется *двойственным* для $\overline{\alpha}$. Отметим пару свойств двойственного базиса.

∘ *Имеет место равенство*

$$\mathrm{tr}(\alpha_i\alpha_j^*) = [i = j]$$

для любых номеров i, j*, таких, что* $1 \leqslant i, j \leqslant n$.

Доказательство.

$$\mathrm{tr}(\alpha_i\alpha_j^*) = \mathrm{tr}(\alpha_i \cdot \overline{\alpha}\,\mathrm{Tr}(\overline{\alpha})^{-1}{\downarrow_j}) = \overrightarrow{\mathrm{Tr}(\overline{\alpha})}_i\,\mathrm{Tr}(\overline{\alpha})^{-1}{\downarrow_j} = [i = j].\ \square$$

∘ *Для любых элементов* $x_1, \ldots, x_n$ *из поля* K *верна импликация*

$$x_i = \mathrm{tr}(x\alpha_i^*), \text{ если } x = \sum_i x_i\alpha_i.$$

Доказательство.

$$\mathrm{tr}(x\alpha_i^*) = \mathrm{tr}(\sum_i x_i\alpha_i\alpha_i^*) = \sum_i x_i\,\mathrm{tr}(\alpha_i\alpha_i^*) = x_i.\ \square$$

Дискриминант. Пусть по-прежнему задано расширение полей L/K и набор $\overline{\alpha}$, составленный из n элементов поля L. Элемент

$$\begin{aligned}\mathrm{disc}(\overline{\alpha}) &= \det \mathrm{Tr}(\overline{\alpha}) \\ &= \det \Sigma(\overline{\alpha})^2\end{aligned}$$

называется *дискриминантом* набора $\overline{\alpha}$ относительно расширения L/K. (Записанные значения равны в силу доказанного ранее.)

Замечание. При необходимости для дискриминанта можно использовать более точное обозначение

$$\mathrm{disc}_{L/K}(\overline{\alpha}).$$

∘ Набор $\overline{\alpha}$ тогда и только тогда линейно зависим над полем K, когда его дискриминант обращается в нуль. $\square$

∘ Пусть наборы $\overline{\alpha}, \overline{\beta}$ элементов поля L связаны соотношением

$$\overline{\beta} = \overline{\alpha} c_{\alpha,\beta},$$

где $c_{\alpha,\beta}$ — некоторая квадратная матрица размера n, составленная из элементов поля K. Тогда верно равенство

$$\operatorname{disc}(\overline{\beta}) = \operatorname{disc}(\overline{\alpha})(\det c_{\alpha,\beta})^2. \ \square$$

Дискриминант многочлена. Пусть $L = K(\alpha)$ — простое алгебраическое расширение степени n и $p_\alpha(x)$ — минимальный многочлен элемента α над полем K. Имеются взаимосвязи между дискриминантом степенного базиса

$$\overline{\alpha} = (1, \alpha, \ldots, \alpha^{n-1}),$$

дискриминантом многочлена $p_\alpha(x)$ и нормой значения его производной в точке α. Сформулируем соответствующее свойство.

∘ Имеют место равенства

$$\begin{aligned} \operatorname{disc}(\overline{\alpha}) &= \operatorname{disc}(p_\alpha(x)), \\ &= (-1)^{\binom{n}{2}} \operatorname{nr}(p'_\alpha(\alpha)). \end{aligned}$$

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена $p_\alpha(x)$ в алгебраически замкнутом расширении Ω и $\sigma_1, \ldots, \sigma_n$ — вложения расширения L/K в Ω/K, такие, что

$$\sigma_i : \alpha \mapsto \alpha_i$$

для любого $i, 1 \leqslant i \leqslant n$. Непосредственные вычисления дают

$$\det \Sigma(\overline{\alpha}) = \det \begin{pmatrix} 1 & \alpha_1 & \ldots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \ldots & \alpha_n^{n-1} \end{pmatrix} = \prod_{i<j} (\alpha_i - \alpha_j),$$

$$\operatorname{nr}(p'_\alpha(\alpha)) = \prod_i \sigma_i(p'_\alpha(\alpha)) = \prod_{i \neq j} (\alpha_i - \alpha_j) = (-1)^{\binom{n}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Следовательно,

$$\begin{aligned} \operatorname{disc}(\overline{\alpha}) = \det \Sigma(\overline{\alpha})^2 &= \prod_{i<j} (\alpha_i - \alpha_j)^2 \\ &= \operatorname{disc}(p_\alpha(x)) \\ &= (-1)^{\binom{n}{2}} \operatorname{nr}(p'_\alpha(\alpha)). \ \square \end{aligned}$$

Замечание. Пусть L/K — расширение колец, причём кольцо L является конечно порождённым свободным модулем над кольцом K. В

этом случае вслед за нормой и следом можно и дискриминант набора элементов определить относительно расширения L/K.

Упражнение. Какие свойства дискриминанта сохранятся в этом случае?

Целочисленная решётка. Пусть L — числовое поле степени n и Λ — конечно порождённая подгруппа его аддитивной группы. Иными словами, Λ является конечно порождённым $\mathbb{Z}$-модулем, причём свободным, так как не содержит элементов кручения. Будем называть его (целочисленной) решёткой. Отметим ряд свойств.

∘ *Базис решётки Λ является базисом порождаемого ей векторного пространства над полем $\mathbb{Q}$.*

Доказательство. Это так, поскольку линейная независимость над кольцом целых чисел набора элементов поля L влечёт их линейную независимость над полем рациональных чисел. □

Решётка Λ является, таким образом, свободным модулем ранга $r \leqslant n$. Будем называть её решёткой *полного ранга* при $r = n$.

∘ *В решётке полного ранга дискриминанты любых двух базисов совпадают.*

Доказательство. Любые два базиса $\overline{\alpha}, \overline{\beta}$ решётки связаны соотношением $\overline{\beta} = \overline{\alpha} c_{\alpha,\beta}$, где матрица $c_{\alpha,\beta}$ обратима над кольцом целых чисел. Их дискриминанты, следовательно, совпадают с точностью до множителя $\det(c_{\alpha,\beta})^2$, равного 1. Таким образом, они полностью совпадают. □

В связи с последним свойством будем говорить о дискриминанте $\operatorname{disc}(\Lambda/\mathbb{Z})$ полной решётки Λ, имея в виду дискриминант любого её базиса. Последнее свойство можно следующим образом усилить.

∘ *Пусть Λ, Λ' — решётки полного ранга, такие, что $\Lambda \subseteq \Lambda'$. Тогда фактор-модуль Λ'/Λ конечен и имеет место равенство:*

$$\operatorname{disc}(\Lambda/\mathbb{Z}) = \operatorname{disc}(\Lambda'/\mathbb{Z})|\Lambda'/\Lambda|^2.$$

Доказательство. Пусть β, β' — базисы в решётках Λ, Λ' и $c_{\beta',\beta}$ — матрица перехода между ними, такая, что $\beta = \beta' c_{\beta',\beta}$. Тогда для инвариантных множителей $d_1, \ldots, d_n$ этой матрицы выполняются соотношения:

$$\begin{aligned} |\det(c_{\beta',\beta})| &= |d_1| \cdots |d_n| \\ &= |\mathbb{Z}/\mathbb{Z}d_1 \oplus \ldots \oplus \mathbb{Z}/\mathbb{Z}d_n| \\ &= |\mathbb{Z}^n/(\mathbb{Z}d_1 \oplus \ldots \oplus \mathbb{Z}d_n)| \\ &= |\Lambda'/\Lambda|. \end{aligned}$$

Для завершения доказательства осталось воспользоваться соотношением

$$\operatorname{disc}(\Lambda/\mathbb{Z}) = \operatorname{disc}(\Lambda'/\mathbb{Z}) \det(c_{\beta',\beta})^2. \square$$

Заметим, что можно говорить о дискриминанте $\operatorname{disc}(\mathcal{O}_L/\mathbb{Z})$ числового кольца $\mathcal{O}_L$, поскольку верно следующее.

∘ *Числовое кольцо $\mathcal{O}_L$ является решёткой полного ранга.*

Доказательство. Выберем в поле L набор из n элементов, линейно независимых над полем $\mathbb{Q}$. Умножением на подходящее целое число из них получается n целых алгебраических чисел, по-прежнему линейно независимых. Порождённый ими $\mathbb{Z}$-модуль содержится в числовом кольце $\mathcal{O}_L$ и имеет ранг n. Значит, числовое кольцо также имеет ранг n. $\square$

Базис числового кольца $\mathcal{O}_L$, рассматриваемого как решётка, называется целочисленным базисом поля L.

Последнее свойство можно значительно усилить следующим образом.

∘ *Ненулевой идеал числового кольца $\mathcal{O}_L$ является решёткой полного ранга.*

Доказательство. Пусть A — ненулевой идеал числового кольца $\mathcal{O}_L$. Возьмём в поле L целочисленный базис. Заметим, что умножением на произвольный ненулевой элемент, принадлежащий идеалу A, из базисных элементов получается n элементов идеала, которые по-прежнему линейно независимы. $\mathbb{Z}$-модуль, порождённый этими элементами, содержится в идеале A и имеет ранг n. Значит, и идеал имеет ранг n. $\square$

Следствием доказанных свойств является

Теорема. *Числовое кольцо $\mathcal{O}_L$ нётерово.* $\square$

Замечание. Пусть кольцо L является конечно порождённым свободным модулем ранга n над кольцом K. Для любого содержащегося в L свободного K-модуля Λ ранга n можно определить его дискриминант $\operatorname{disc}(\Lambda/K)$, имея в виду дискриминант любого его базиса относительно расширения колец L/K или расширения полей $\operatorname{Frac}(L)/\operatorname{Frac}(K)$; в обоих случаях дискриминант опеределён в кольце K с точностью до обратимого множителя, являющегося квадратом.

Упражнение. Пусть L — числовое поле степени n. Набор из n элементов числового кольца $\mathcal{O}_L$ является целочисленным базисом в L, если его дискриминант свободен от квадратов. Докажите это утверждение. Верно ли обратное утверждение?

4. Дедекиндово кольцо

В этом разделе рассматриваются дедекиндовы кольца, к числу которых относятся числовые кольца; доказывается теорема об однозначном разложении идеала в дедекиндовом кольце.

Дедекиндово кольцо. Сделаем следующее

Определение. Кольцо называется *дедекиндовым*, если оно

(1) целостное,

(2) целозамкнутое,

(3) нётерово,

(4) любой его ненулевой простой идеал — максимальный.

Теорема. *Числовое кольцо дедекиндово.*

Доказательство. Числовое кольцо целостное, так как содержится в поле комплексных чисел. Ранее доказано, что оно целозамкнутое и нётерово. Осталось проверить четвёртое условие. Пусть P — ненулевой простой идеал числового кольца $\mathcal{O}_L$. Фактор-кольцо $\mathcal{O}_L/P$ является конечным целостным кольцом и тогда является полем. Следовательно, идеал P — максимальный. □

Упражнение. Натуральное число n назовём *размерностью Крулля* кольца, если это максимальное число, для которого существует цепочка

$$P_0 \subset P_1 \subset \ldots \subset P_n,$$

содержащая $n+1$ простых идеалов. Докажите следующие свойства.

∘ Размерность Крулля равна нулю в том и только том случае, если кольцо является полем.

∘ Она равна единице в том и только том случае, если кольцо дедекиндово и не является полем.

Теорема о разложении. Напомним, произведением идеалов A, B кольца R называется идеал AB, порождённый произведениями ab элементов a, b, принадлежащих соответствующим идеалам A, B.

Теорема. *В дедекиндовом кольце любой ненулевой идеал можно представить в виде произведения максимальных идеалов, причём единственным образом с точностью до порядка сомножителей.*

Доказательство теоремы будет приведено позже. Пока же установим

Следствие. *Дедекиндово кольцо тогда и только тогда является областью с однозначным разложением, когда оно является областью главных идеалов.*

Доказательство. Область главных идеалов является кольцом с однозначным разложением на неприводимые множители; это доказано ранее. Докажем обратное утверждение для дедекиндова кольца. Пусть в дедекиндовом кольце ненулевые элементы однозначно разлагаются на неприводимые множители. В частности, неприводимые и простые элементы в таком кольце совпадают. Нужно доказать, что идеалы такого кольца — главные. В силу теоремы достаточно это сделать лишь для максимальных идеалов. Но максимальный идеал содержит простой элемент (таким элементом является всякий неприводимый делитель любого ненулевого элемента) и тогда совпадает с идеалом, порождённым этим элементом. □

Умножение и обращение идеалов. Пусть R — целостное кольцо. Будем рассматривать R-модули (в том числе идеалы кольца R), содержащиеся в поле $K = \mathrm{Frac}(R)$. *Произведением* R-модулей A, B называется R-модуль

$$AB = \{\alpha_1\beta_1 + \ldots + \alpha_n\beta_n | \alpha_1, \ldots, \alpha_n \in A, \beta_1, \ldots, \beta_n \in B, n \in \mathbb{N}\}.$$

Отметим следующие свойства.

∘ Пусть R-модуль A порождается элементами α_i и R-модуль B порождается элементами β_j. Тогда R-модуль AB порождается элементами $\alpha_i\beta_j$. (Здесь $i \in I, j \in J$ и I, J — некоторые множества.)

Для идеала A кольца R *обратным идеалом* назовём R-модуль

$$A^{-1} = \{\beta | \beta \in K, \beta A \subseteq R\}.$$

∘ Для идеала A кольца R имеют место включения

$$R \subseteq A^{-1}, A^{-1}A \subseteq R,$$

∘ Для любого элемента α из R имеет место равенство $(R\alpha)^{-1} = R\alpha^{-1}$.

Вспомогательные свойства. Установим далее пять свойств, которые понадобятся при доказательстве теоремы о разложении.

(1) *Пусть в целостном кольце для идеалов $A_1, \ldots, A_n$ и простого идеала P выполняется включение $A_1 \cdots A_n \subseteq P$. Тогда для некоторого номера j, где $1 \leqslant j \leqslant n$, выполняется включение $A_j \subseteq P$.*

Доказательство. Если включение $A_j \subseteq P$ не выполняется, то можно выбрать элемент a_j в множестве $A_j \setminus P$. Если оно не выполняется для всех j, то произведение $a_1 \cdots a_n$ принадлежит множеству $A_1 \cdots A_n \setminus P$, противоречие. □

(2) *В нётеровом кольце любой ненулевой идеал включает произведение ненулевых простых идеалов.*

Доказательство. Пусть Ω — множество ненулевых идеалов нётерова кольца R, которые не включают произведения ненулевых простых идеалов. Предположим, оно не пустое. Тогда в нём найдётся максимальный по включению идеал A. Поскольку этот идеал не является простым, найдутся элементы a, b, такие, что эти элементы не принадлежат идеалу A, а их произведение — принадлежит. Идеалы

$$A + Ra, A + Rb$$

строго включают A и, следовательно, включают некоторые произведения

$$P_1 \cdots P_n, Q_1 \cdots Q_m$$

простых идеалов. Заметим, что имеют место включения

$$P_1 \cdots P_n Q_1 \cdots Q_m \subseteq (A + Ra)(A + Rb) \subseteq A^2 + Aa + Ab + Rab \subseteq A.$$

Получили противоречие. Следовательно, множество Ω пустое. $\square$

(3) *В дедекиндовом кольце R для ненулевого простого идеала P выполняется строгое включение $R \subset P^{-1}$.*

Доказательство. В силу определений идеала и обратного идеала выполняется включение $R \subseteq P^{-1}$. Поэтому достаточно найти элемент x, принадлежащий множеству $P^{-1} \setminus R$. Будем искать такой элемент в виде $a^{-1}b$, где элементы a, b принадлежат множествам P, R. Возьмём в качестве a произвольный ненулевой элемент из P. В соответствии с доказанным ранее свойством найдётся набор простых идеалов $P_1, \dots P_r$, для которых выполняется включение

$$P_1 \cdots P_r \subseteq aR;$$

пусть число r наименьшее возможное. Заметим, что $aR \subseteq P$ и, в соответствии с установленым ранее, для некоторого номера i выполняется включение $P_i \subseteq P$ и тогда здесь выполняется равенства, так как оба идеала P_i, P максимальные. Считая $i = 1$, рассмотрим два возможных случая.

Предположим $r = 1$.

Тогда идеалы P_1, P, aR совпадают и $P^{-1} = a^{-1}R$. Элемент a^{-1} принадлежит идеалу P^{-1} и не принадлежит кольцу R, так как элемент a необратим в R. (Иными словами, следует взять $b = 1$ в этом случае.)

Пусть теперь $r > 1$.

В силу выбора числа r найдётся элемент b, принадлежащий множеству

$$P_2 \cdots P_r \setminus aR.$$

Элемент $a^{-1}b$ принадлежит идеалу P^{-1}, так как

$$a^{-1}bP = a^{-1}P_1 \dots P_n \subseteq a^{-1}aR = R.$$

Он не принадлежит кольцу R, поскольку в противном случае

$$b = aa^{-1}b \in aR \subseteq R$$

— противоречие. Таким образом, свойство доказано. □

(4) *В дедекиндовом кольце для ненулевого идеала A и ненулевого простого идеала P выполняется неравенство $P^{-1}A \neq A$.*

Доказательство. Пусть ненулевой идеал A порождается как R-модуль набором элементов $\alpha = (\alpha_1, \ldots, \alpha_n)$. Выберем произвольно ненулевой элемент x в P^{-1}. Предположим, что $P^{-1}A = A$. В этом случае для некоторой матрицы M из кольца $R^{n,n}$ выполняются равенства

$$\alpha x = \alpha M, \alpha(\mathrm{e}_n x - M) = 0, \det(\mathrm{e}_n x - M) = 0.$$

Отсюда, элемент x целый над R. Поскольку кольцо R целозамкнуто, имеет место включение $P^{-1} \subseteq R$. Это противоречит предыдущему свойству. □

(5) *В дедекиндовом кольце для ненулевого простого идеала P выполняется равенство $P^{-1}P = R$.*

Доказательство. Имеют место включения

$$P \subseteq P^{-1}P \subseteq R.$$

Здесь первое включение получается как следствие включения $P \subseteq P^{-1}$, а второе — по определению обратного идеала. Поскольку идеал P максимальный и первое включение строгое в силу четвёртого свойства, во втором включении выполняется равенство. □

Существование разложения. Перейдём к доказательству теоремы о разложении. Докажем существование разложения. Рассмотрим множество собственных идеалов, которые невозможно записать в виде произведения простых. Докажем, что это множество пустое. Предположим, это не так, A — максимальный идеал в этом множестве и P — максимальный идеал кольца, включающий A. Имеют место включения

$$A \subseteq AP^{-1} \subseteq PP^{-1} = R.$$

Первое включение здесь строгое в силу четвёртого свойства. Следовательно, существует разложение

$$AP^{-1} = P_1 \cdots P_n$$

в произведение простых идеалов. С использованием пятого свойства получаем

$$A = AP^{-1}P = P_1 \cdots P_n P.$$

Получили противоречие. Существование разложения доказано.

Единственность разложения. Докажем теперь единственность разложения. Предположим, существуют два разложения для некоторого идеала и тогда выполняется равенство

$$P_1 \cdots P_n = Q_1 \cdots Q_m$$

для некоторых простых идеалов P_i, Q_j. В силу первого свойства для некоторого номера j выполняется включение $P_1 \subseteq Q_j$ и тогда выполняется равенство, так как оба идеала здесь максимальные. Считая $j = 1$, умножением записанного равенства на P^{-1} с использованием пятого свойства, получаем

$$P_2 \cdots P_n = Q_2 \cdots Q_m.$$

Рассуждая по-индукции, убеждаемся, что $n = m$ и после надлежащей перенумерации идеалы P_i, Q_i с одинаковыми номерами совпадают.

Теорема о разложении полностью доказана. ■

Отношение делимости для идеалов. Установим в этом разделе некоторые полезные свойства идеалов дедекиндова кольца R. Пусть A, B — идеалы дедекиндова кольца R. Отметим ряд свойств.

∘ Следующие условия равносильны:

(1) $A + B = R$;

(2) $a + b = 1$ для некоторой пары элементов a, b из A, B.

Доказательство. Это очевидно. □

Напомним, что идеалы A, B для которых выполняются указанные условия называются *взаимно простыми*.

Пример. Различные максимальные идеалы (очевидно) взаимно просты, как и их степени (см. дальше).

∘ Для взаимно простых идеалов A, B верно равенство $AB = A \cap B$.

Доказательство. Ясно, что выполняется включение $AB \subseteq A \cap B$, докажем обратное. Выберем в идеалах A, B пару элементов a, b, таких, что $1 = a+b$. Произвольный элемент x из пересечения $A \cap B$ записывается тогда в виде $x = xa + xb$ и принадлежит произведению AB вслед за слагаемыми xa, xb. □

∘ Для любых целых положительных чисел s, t идеалы A^s, B^t взаимно простые, если идеалы A, B взаимно простые.

Доказательство. Выберем в идеалах A, B пару элементов a, b, таких, что $1 = a + b$. Не сложно понять, что элемент

$$(a + b)^{s+t} = 1$$

принадлежит идеалу $A^s + B^t$ и тогда $A^s + B^t = R$. □

Обозначим $\mathrm{ord}_P(C)$ максимальный показатель степени максимального идеала P в разложении идеала C, иными словами имеет место разложение

$$C = \Pi_P P^{\mathrm{ord}_P(C)},$$

где произведение вычисляется по всем максимальным идеалам P, показатели $\mathrm{ord}_P(C)$ неотрицательны и почти все равны нулю.

$\circ$ Для любого максимального идеала P показатель $\mathrm{ord}_P(C)$ совпадает с максимальным натуральным числом $k(P)$, таким, что $C \subseteq P^{k(P)}$.

Доказательство. Идеалы $P^{\mathrm{ord}_P(C)}$ взаимно простые, поэтому их произведение совпадает с пересечением. Отсюда $\mathrm{ord}_P(C) \leqslant k(P)$ для любого максимального идеала P. Тогда выполняются включения

$$C \subseteq \Pi_P P^{k(P)} \subseteq \Pi_P P^{\mathrm{o}(P)} = \cap_P P^{\mathrm{o}(P)} = C,$$

где произведение вычисляется по всем максимальным идеалам P. Очевидно, здесь везде выполняются равенства и тогда в силу однозначности разложения для любого макимального идеала верно $\mathrm{ord}_P(C) = k(P)$. $\square$

$\circ$ Следующие условия равносильны:

(1) $A \subseteq B$;

(2) $\mathrm{ord}_P(B) \leqslant \mathrm{ord}_P(A)$ для любого максимального идеала P;

(3) $A = BC$ для некоторого идеала C.

Идеал B называют делителем идеала A и пишут $B \mid A$, если выполняются эти условия.

Доказательство. Импликация $(1 \to 2)$ выполняется, так как произведение идеалов $P^{\mathrm{ord}_P(A)}$ совпадает с пересечением. Импликация $(2 \to 3)$ столь же очевидна: нужно взять

$$C = \Pi_P P^{\mathrm{ord}_P(B) - \mathrm{ord}_P(A)}.$$

Наконец, импликация $(3 \to 1)$ верна в силу определения произведения идеалов. $\square$

$\circ$ Пусть идеал A ненулевой в кольце R. Тогда равносильны условия:

(1) $A \subseteq B$;

(2) $B = A + bR$ для некоторого элемента b.

Доказательство. Нужно доказать, что из первого условия следует второе. Для любого простого идеала P в множестве $P^{\mathrm{ord}_P(B)} \setminus P^{\mathrm{ord}_P(B)+1}$ выберем элемент b_P. По китайской теореме об остатках существует элемент b, такой, что

$$b \equiv b_P \mod P^{\mathrm{ord}_P(A)}$$

для любого простого идеала P. Остается проверить, что $B = A + bR$. $\square$

Теорема. *Пусть a — ненулевой элемент идеала B в дедекиндовом кольце R. Тогда для некоторого элемента b выполняется равенство $B = aR + bR$. В частности, в дедекиндовом кольце ненулевой идеал порождается двумя элементами.*

Доказательство. Применим последнее свойство для идеала $A = aR$. □

5. Группа классов идеалов

В этом разделе определяется группа классов идеалов дедекиндова кольца. Некоторым образом эта группа показывает в какой степени разложение на неприводимые множители в кольце не является однозначным. Доказывается теорема о конечности группы классов числового кольца.

Дробные идеалы. Пусть, по-прежнему, R — целостное кольцо с полем частных $K = \mathrm{Frac}(R)$. Будем рассматривать R-модули, содержащиеся в поле K.

∘ *Пусть R — нётерово кольцо с полем частных $K = \mathrm{Frac}(R)$. Тогда для подмножества $A \subseteq K$ следующие условия равносильны.*

(1) *Множество A является R-модулем и для некоторого элемента b из R выполняется включение $bA \subseteq R$.*

(2) *Множество A является $\mathbb{Z}$-модулем и для некоторого элемента b из R множество bA является идеалом кольца R.*

(3) *Множество A является конечно-порождённым R-модулем.*

Доказательство. Первые два условия равносильны, так как R-модуль, содержащийся в кольце R, является идеалом. Импликация $(1 \to 3)$ выполняется, так как идеал в дедекиндовом кольце порождается парой элементов и является конечно порождённым. Импликация $(3 \to 1)$ также верна: следует взять элемент b, кратный знаменателям элементов, порождающих модуль A. □

Модуль A, удовлетворяющий записанным условиям, называется *дробным идеалом* кольца R. «Обычные» идеалы кольца R называются также *целыми идеалами*. Отметим следующие свойства.

∘ Сумма, произведение и пересечение дробных идеалов являются дробными идеалами. □

∘ Для идеала дедекиндова кольца обратный идеал — дробный. □

∘ Ненулевые дробные идеалы дедекиндова кольца R относительно операции умножения идеалов образует абелеву группу, где единицей является идеал R. □

Группу дробных идеалов дедекиндова кольца R обозначим $\mathrm{Id}^{\times}(R)$.

Теорему об однозначном разложении идеалов в дедекиндовом кольце можно уточнить следующим образом.

Теорема. *В дедекиндовом кольце ненулевой дробный идеал A единственным образом записывается в виде произведения*

$$A = \Pi_P P^{\mathrm{ord}_P(A)},$$

где произведение вычисляется по множеству всех максимальных идеалов кольца R, показатели $\mathrm{ord}_P(A)$ целые, почти все равные нулю. Иными словами, группа $\mathrm{Id}^{\times}(R)$ свободная абелева, порождаемая максимальными идеалами. □

Отметим следующее свойство.

∘ Для любого элемента a из поля K множество

$$aR = \{ar | r \in R\}$$

является дробным идеалом. Такие дробные идеалы называются *главными*. Они образуют подгруппу $\mathrm{Pr}(R)$ в группе $\mathrm{Id}^{\times}(R)$. □

Группа классов. Фактор-группа

$$\mathrm{Cl}(R) = \mathrm{Id}^{\times}(R)/\mathrm{Pr}(R)$$

называется *группой классов идеалов* дедекиндова кольца R. Эту группу можно определить также следующим образом. Введём на множестве ненулевых дробных идеалов следующее отношение сравнимости по модулю подгруппы $\mathrm{Pr}(R)$. Будем считать, что идеалы A, B находятся в этом отношении и будем писать

$$A \equiv B \mod \mathrm{Pr}(R),$$

если их частное AB^{-1} является главным дробным идеалом. Это означает, что для некоторой дроби a/b выполняются равносильные равенства

$$AB^{-1} = R(a/b), Ab = Ba.$$

Введённое отношение является эквивалентностью. Обозначим через $[A]$ класс идеалов, сравнимых с идеалом A по модулю $\mathrm{Pr}(R)$. Группа $\mathrm{Cl}(R)$ состоит из таких классов, для которых умножение определяется так:

$$[A][B] = [AB].$$

∘ *Любой класс идеалов из группы $\mathrm{Cl}(R)$ содержит целый идеал.*

Доказательство. Пусть A — дробный идеал. Тогда для некоторого элемента b из кольца R идеал Ab целый, лежащий в одном классе с A. □

Теорема. *Для дедекиндова кольца R следующие условия равносильны.*

(1) *Кольцо R является областью с однозначным разложением.*

(2) *Кольцо R является областью главных идеалов.*

(3) *Группа* $\mathrm{Cl}(R)$ *тривиальная.*

Доказательство. Равносильность первых двух условий доказана ранее. Равносильность последних двух условий следует из свойства выше. □

Норма идеала. Пусть L — числовое поле и A — ненулевой идеал в числовом кольце $\mathcal{O}_L$. *Нормой идеала* A в числовом кольце $\mathcal{O}_L$ называется целое положительное число, определяемое как

$$\mathrm{nr}(A) = |\mathcal{O}_L/A|.$$

(Норма записывается относительно расширения $L/\mathbb{Q}$.)

Отметим ряд свойств.

∘ Пусть α, β — базисы $\mathbb{Z}$-модулей $\mathcal{O}_L, A$ и $c_{\alpha,\beta}$ — «матрица перехода» между ними из кольца $\mathbb{Z}^{n,n}$, такая, что $\beta = \alpha c_{\alpha,\beta}$. Тогда

$$\mathrm{nr}(A) = \pm \det(c_{\alpha,\beta}).$$

Доказательство. Это проверяется с использованием канонической формы Смита. Аналогичное рассуждение применялось ранее при изучении решёток в числовом поле. □

∘ В расширении $L/\mathbb{Q}$ норма целого алгебраического числа a, отличного от нуля, с точностью до знака совпадает с нормой идеала, порождённого этим числом в числовом поле $\mathcal{O}_L$:

$$\mathrm{nr}(a\mathcal{O}_L) = |\,\mathrm{nr}(a)|.\square$$

Доказательство. Заметим, что для целочисленного базиса

$$\alpha = (\alpha_1, \ldots, \alpha_n)$$

в поле L набор элементов

$$\beta = (a\alpha_1, \ldots, a\alpha_n)$$

является $\mathbb{Z}$-базисом идеала $a\mathcal{O}_L$. Матрица $c_{\alpha,\beta}$ совпадает в этом случае с матрицей $\overline{\mu}_a$ (записанной относительно базисов α, β). Отсюда в силу предыдущего свойства имеем

$$\mathrm{nr}(a\mathcal{O}_L) = \pm \det(c_{\alpha,\beta}) = \pm \det(\overline{\mu}_a) = \pm\,\mathrm{nr}(a).\ \square$$

Имеет место

Теорема. *Для любых идеалов A, B числового кольца $\mathcal{O}_L$ выполняется равенство:*

$$\mathrm{nr}(AB) = \mathrm{nr}(A)\,\mathrm{nr}(B).$$

Доказательство. Теорема верна для взаимно простых идеалов A, B. В этом случае по китайской теореме об остатках имеем разложение

$$\mathcal{O}_L/AB = \mathcal{O}_L/A \oplus \mathcal{O}_L/B,$$

откуда

$$\operatorname{nr}(AB) = |\mathcal{O}_L/AB| = |\mathcal{O}_L/A| \cdot |\mathcal{O}_L/B| = \operatorname{nr}(A)\operatorname{nr}(B).$$

В силу теоремы об однозначном разложении идеалов остаётся проверить равенство

$$\operatorname{nr}(P^m) = \operatorname{nr}(P)^m$$

для максимального идеала P. Это равенство следует из свойства, устанавливаемого ниже. □

∘ *Пусть m — целое положительное число. В числовом кольце $\mathcal{O}_L$ для максимального идеала P и произвольного элемента a из множества $P^m \setminus P^{m+1}$ отображение*

$$\mathcal{O}_L/P \to P^m/P^{m+1}, x + P \mapsto ax + P^{m+1},$$

определено корректно и является изоморфизмом $\mathbb{Z}$-модулей.

Доказательство. Достаточно доказать, что гомоморфизм

$$\mathcal{O}_L \to P^m/P^{m+1}, x \mapsto ax + P^{m+1},$$

— сюръективный с ядром P. Заметим, что образ этого гомоморфизма совпадает с фактор-модулем

$$(a\mathcal{O}_L + P^{m+1})/P^{m+1}.$$

Вместе с тем, имеют место следующие соотношения делимости:

$$P^m \mid (a\mathcal{O}_L + P^{m+1})|P^{m+1}.$$

Отсюда, в силу однозначности разложения идеал $a\mathcal{O}_L + P^{m+1}$ совпадает с одноим из идеалов P^m, P^{m+1}, причём второй вариант невозможен в силу выбора элемента a. Таким образом, рассматриваемый гомоморфизм сюръективен. Его ядро, очевидно, включает идеал P. Обратно, для любого элемента x из ядра должны выполняться соотношения

$$P^{m+1}|ax\mathcal{O}_L = a\mathcal{O}_L \cdot x\mathcal{O}_L \text{ и } P^{m+1} \not| a\mathcal{O}_L,$$

откуда $P \mid x\mathcal{O}_L$. Таким образом, ядро совпадает с идеалом P. □

Далее, для идеалов A, B числового кольца $\mathcal{O}_L$ норма дробного идеала AB^{-1} определяется следующим образом:

$$\operatorname{nr}(AB^{-1}) = \operatorname{nr}(A)/\operatorname{nr}(B).$$

Это определние корректно в силу установленных свойств. Отображение

$$\mathrm{Id}^\times(\mathcal{O}_L) \to \mathbb{Q}_+^\times, A \mapsto \operatorname{nr}(A),$$

(где $\mathbb{Q}_+^\times$ — мультипликативная группа положительных рациональных чисел) является гомоморфизмом абелевых групп ($\mathbb{Z}$-модулей).

Конечность группы классов. Пусть, как и раньше, L — числовое поле степени n. Имеет место

Теорема. *Группа классов идеалов числового поля конечная.*

Для доказательства этой теоремы установим ряд свойств.

∘ *Для любого положительного действительного числа M имеется лишь конечное число идеалов в кольце $\mathcal{O}_L$ с нормой, не превосходящей M.*

Доказательство. Достаточно доказать конечность числа идеалов с нормой m. Для любого такого идеала A в фактор-кольце R/A выполняется соотношение $mx = 0$ (см. упражнение ниже), следовательно, идеал A включает идеал $m\mathcal{O}_L$. Поскольку идеал $m\mathcal{O}_L$ имеет конечный индекс, существует лишь конечно число идеалов, включающих его. В частности, множество идеалов с нормой m конечно. □

∘ *Следующие условия равносильны.*

(1) *Группа* $\mathrm{Cl}(\mathcal{O}_L)$ *конечная.*

(2) *Для некоторого положительного действительного числа M каждый класс идеалов из группы* $\mathrm{Cl}(\mathcal{O}_L)$ *содержит целый идеал с нормой, не превосходящей M.*

Доказательство. Это легко проверяется. □

∘ *Для некоторого действительного положительного числа M любой ненулевой идеал A кольца $\mathcal{O}_L$ содержит элемент a, такой, что*

$$|\operatorname{nr}(a)| \leqslant M \operatorname{nr}(A).$$

Доказательство. Пусть A — ненулевой идеал числового кольца $\mathcal{O}_L$ с целочисленным базисом α. Найдём целое положительное число m , для которого выполняется неравенство

$$m^n \leqslant \operatorname{nr}(A) < (m+1)^n.$$

и рассмотрим в числовом кольце подмножество

$$\Sigma = \{\sum_i m_i\alpha_i | m_i \in \mathbb{Z}, 0 \leqslant m_i \leqslant m, 1 \leqslant i \leqslant n\}.$$

Поскольку мощность множества Σ, равная $(m+1)^n$, строго больше нормы $\operatorname{nr}(A)$ идеала A, в этом множестве найдётся пара различных элементов x, y, сравнимых по модулю A. Запишем разложение разности $a = x - y$

этих элементов в базисе α:

$$a = \sum_i m_i \alpha_i.$$

Для коэффициентов этого разложения выполняются неравенства

$$|m_i| \leqslant m, 1 \leqslant i \leqslant n.$$

С учётом этого получаем

$$|\operatorname{nr}(a)| = \prod_i |\sigma_i(z)| = \prod_i \sum_j |m_j||\sigma_i(\alpha_j)| \leqslant m^n M \leqslant \operatorname{nr}(A)M,$$

где

$$M = \prod_i \sum_j |\sigma_i(\alpha_j)|.$$

Здесь σ_i — различные вложения расширения L/K в алгебраически замкнутое расширение и $1 \leqslant i, j \leqslant n$. $\square$

$\circ$ *Существует действительное положительное число M, такое, что каждый класс идеалов из группы $\operatorname{Cl}(\mathcal{O}_L)$ содержит целый идеал с нормой, не превосходящей M.*

Доказательство. Пусть C — класс идеалов из группы $\operatorname{Cl}(\mathcal{O}_L)$, A — целочисленный идеал из класса C^{-1}, его элемент a и значение M определены как в предыдущем свойстве. Тогда

$$\operatorname{nr}(aA^{-1}) = |\operatorname{nr}(a)|/\operatorname{nr}(A) \leqslant M.$$

Осталось заметить, что идеал aA^{-1} принадлежит классу C. $\square$

Доказательство теоремы следует теперь из установленных свойств. $\square$

Упражнение. Докажите следующие утверждения.

$\circ$ В конечном кольце, содержащем m элементов, для любого элемента x выполняется равенство $mx = 0$.

$\circ$ Пусть M такое же, как в последнем свойстве. Следующие условия равносильны.

(1) Кольцо $\mathcal{O}_L$ является областью с однозначным разложением.

(2) В любом классе идеалов найдётся главный идеал с нормой, не превосходящей M.

6. Простые числа в расширении

Пусть, по-прежнему, L — числовое поле степени n. В этом разделе для простого целого рационального числа p изучается разложения идеала $p\mathcal{O}_L$ в числовом кольце $\mathcal{O}_L$.

Степень инерции. В числовом кольце $\mathcal{O}_L$ рассмотрим ненулевой простой идеал P. Отметим следующие свойства.

- *Для некоторого простого целого рационального числа p верно:*

$$P \cap \mathbb{Z} = p\mathbb{Z}.$$

Доказательство. Непосредственно проверяется, что пересечение $P \cap \mathbb{Z}$ является простым идеалом в кольце целых чисел. Этот идеал ненулевой, так как содержит норму любого элемента из P. $\square$

- *Идеал P содержит только одно простое целое рациональное число.*

Доказательство. Идеал $p\mathbb{Z}$ содержит единственное простое число, именно, p. $\square$

Идеал P называют в этом случае делителем числа p (имея в виду $P \mid p\mathcal{O}_L$).

- *Число p совпадает с характеристикой поля $\mathcal{O}_L/P$.*

Доказательство. Достаточно заметить, что ядро гомоморфизма

$$\mathbb{Z} \to \mathcal{O}_L/P, x \mapsto x + P,$$

совпадает с идеалом $p\mathbb{Z}$. В силу первой теоремы об изоморфизмах колец образ этого гомоморфизма изоморфен полю $\mathbb{Z}/p\mathbb{Z}$ и тогда содержится в качестве простого подполя в поле $\mathcal{O}_L/P$. $\square$

- *Для некоторого целого положительного числа $f(P)$ верно*

$$|\mathcal{O}_L/P| = p^{f(P)}$$

Доказательство. Число n совпадает со степенью, которую конечное поле $\mathcal{O}_L/P$ имеет над своим простым подполем. $\square$

Число $f(P)$ называется *степенью инерции* идеала P.

Индекс ветвления. Пусть p — простое целое рациональное число и в числовом кольце $\mathcal{O}_L$ имеет место следующее разложение идеалов:

$$p\mathcal{O}_L = P_1^{e(P_1)} \cdots P_m^{e(P_m)},$$

где P_i — различные простые идеалы кольца $\mathcal{O}_L$, делящие p, и $e(P_i)$ — целые положительные числа. Число $e(P)$ называется *индексом инерции* идеала P. Говорят, что простое число p *не разветвляется* в числовом кольце $\mathcal{O}_L$ (а также в числовом поле L), если в этом кольце индекс инерции любого простого идеала, делящего p, равен единице, то есть

$$e(P_1) = \ldots = e(P_m) = 1.$$

В противном случае, говорят, что p *разветвляется*. Имеет место

Теорема. *Для простого целого рационального числа p верна формула:*

$$\sum_P e(P)f(P) = n,$$

где суммирование выполняется по всем простым ненулевым идеалам числового кольца $\mathcal{O}_L$, делящим p.

Доказательство. Достаточно рассмотреть равенства

$$\begin{aligned}\mathrm{nr}(p) &= p^n \\ &= \mathrm{nr}(p\mathcal{O}_L) \\ &= \mathrm{nr}(P_1^{e(P_1)} \cdots P_m^{e(P_m)}) \\ &= \mathrm{nr}(P_1)^{e(P_1)} \cdots \mathrm{nr}(P_m)^{e(P_m)} \\ &= p^{f(P_1)e(P_1)} \cdots p^{f(P_m)e(P_m)}. \ \square\end{aligned}$$

Факторизационная лемма Куммера. Имеет место

Теорема (факторизационная лемма Куммера).

Пусть для некоторого целого алгебраического числа α верно равенство $\mathcal{O}_L = \mathbb{Z}[\alpha]$. Пусть $f(x)$ — минимальный многочлен элемента α и p — простое целое рациональное число. Предположим, в кольце $\mathbb{Z}/p\mathbb{Z}[x]$ имеет место следующее разложение на неприводимые множители:

$$\overline{f}(x) = \overline{f}_1^{e_1}(x) \cdots \overline{f}_m^{e_m}(x),$$

где $\overline{f}_i(x)$ — различные нормированные многочлены, неприводимые над полем $\mathbb{Z}/p\mathbb{Z}$, e_i — целые положительные числа для любого $i, 1 \leqslant i \leqslant m$. Тогда в кольце $\mathcal{O}_L$ имеет место разложение

$$p\mathcal{O}_L = P_1^{e_1} \cdots P_m^{e_m}.$$

Здесь P_i — различные простые идеалы, причём выполняются равенства

$$P_i = p\mathcal{O}_L + f_i(\alpha)\mathcal{O}_L, \mathrm{nr}(P_i) = p^{n_i}, \ \text{где } n_i = \deg(\overline{f}_i(x)),$$

для любого $i, 1 \leqslant i \leqslant m$.

(Обозначение типа $\overline{h}(x)$ используется здесь для многочлена, принадлежащего кольцу $\mathbb{Z}/p\mathbb{Z}[x]$, который получается из целочисленного многочлена $h(x)$ редукцией коэффициентов по модулю простого числа p.)

Доказательство. Обозначим через $\mathrm{Id}(A, R)$ решётку идеалов кольца R, включающих идеал A. Для доказательства достаточно заметить, что имеются решёточные изоморфизмы:

$$\begin{aligned}\mathrm{Id}((\overline{f}(x)), \mathbb{Z}/(p)[x]) \to \mathrm{Id}((p, f(x)), &\mathbb{Z}[x]/(p)) \to \mathrm{Id}((f(\alpha)), \mathbb{Z}[\alpha]), \\ (\overline{g}(x)) \mapsto (p, &g(x)) \mapsto (p, g(\alpha)),\end{aligned}$$

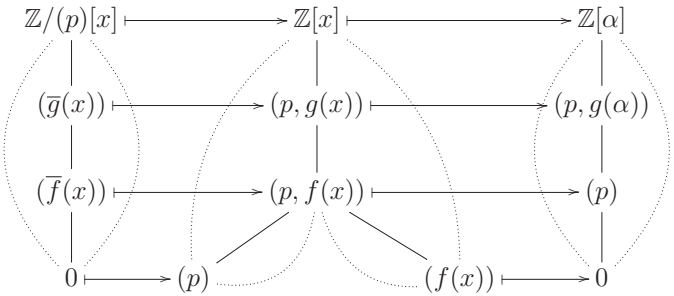
где $g(x)$ — произвольный целочисленный многочлен, такой, что $\overline{f}(x) | \overline{g}(x)$. Эти изоморфизмы индуцированы следующими изоморфизмами колец:

$$\begin{aligned}&\mathbb{Z}/(p)[x] \to \mathbb{Z}[x]/(p), \overline{g}(x) \mapsto g(x) + (p), \\ &\mathbb{Z}[x]/(f(x)) \to \mathbb{Z}[\alpha], g(x) + (f(x)) \mapsto g(\alpha).\end{aligned}$$

В том числе имеется решёточный изоморфизм

$$\mathrm{Id}((\overline{f}(x)), \mathbb{Z}/(p)[x]) \to \mathrm{Id}((p), \mathbb{Z}[\alpha]),$$
$$(\overline{g}(x)) \mapsto (p, g(\alpha)).$$

Ситуацию можно проиллюстрировать следующей диаграммой



□

Рекомендуемая литература

1. Ван дер Варден Б. Л. Алгебра. М.: Наука, 1976. 648 с.

2. Ленг С. Алгебра. М.: Мир, 1968. 564 с.

3. Кострикин А. И. Введение в алгебру.Часть I. Основы алгебры. Учебник для вузов. М.: Физико-математическая литература, 2000. 272 с.

4. Калужнин Л. А. Введение в общую алгебру. М.: Наука. 1973. 448 с.

5. Курош А. Г. Лекции по общей алгебре. Учебник. СПб.: Издательство «Лань», 2005. 560 с.

6. Фаддеев Д. К. Лекции по алгебре. Учебное пособие для вузов. М.: Наука, 1984. 416 с.

7. Вавилов Н. А. Конкретная теория колец.Учебное пособие по курсу алгебры СПбГУ. СПб.: СПбГУ, 2006. 129 с.

8. Городенцев А. Л. Алгебра. Учебник для студентов-математиков. Часть I. «МЦ НМО». 2013. 526 с.

9. Connell E. H. Elements of abstract and linear algebra. `http://www.math.miami.edu/~ec/book/`

10. Верещагин Н. К., Шень А. Лекции по математической логике и теории алгоритмов. Часть I. Начала теории множеств. М.: МЦНМО, 1999. 128 с.

11. Коэн П. Дж. Теория множеств и континуум-гипотеза. М.: Книжный дом «Либроком». 2010. 344 с.

12. Ларин С. В. Числовые системы.М.: Академия, 2001. 160с.

13. Прасолов В. В. Многочлены. М.: МЦНМО, 2001. 336 с.

14. Арнольд В. И. Геометрия комплексных чисел, кватернионов и спинов. М.: МЦНМО, 2014. 40 с.

15. Колосов В. А. Теоремы и задачи алгебры, теории чисел и комбинаторики. М.: Гелиос АРВ, 2001. 256 с.

16. Колмогоров А. Н., Фомин С. В. Элементы теории функций и функционального анализа. М.: Глав. ред. физико-математической литературы изд-ва «Наука», 1976. 543 с.

Учебное издание

Парватов Николай Георгиевич

ВВЕДЕНИЕ В МАТЕМАТИКУ

Учебное пособие

Издание подготовлено в авторской редакции.

Подписано в печать 07.08.2019 г. Формат $60\times84^{1}/_{16}$.
Бумага для офисной техники. Печ. л. 21,8. Усл. печ. л. 20,3.
Заказ 3876. Тираж 36 экз.

Отпечатано на оборудовании Издательского Дома Томского государственного университета,
634050, г. Томск, пр. Ленина, 36, тел. (3822) 529-849. E-mail: rio.tsu@mail.ru

ISBN 978-5-94621-833-7