Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

Н. И. ДУБРОВИН

ФУНДАМЕНТАЛЬНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

Учебное пособие

Владимир 2014

УДК 512(076)
ББК 22.14я73
Д56

Рецензенты:

Начальник отдела организации продаж и работы с партнерами
операционного офиса «Владимирский»
Ярославского филиала Акционерного коммерческого банка «Росбанк»
О. О. Бабин

Доктор физико-математических наук, профессор
зав. кафедрой физики и прикладной математики
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
С. М. Аракелян

Печатается по решению редакционно-издательского совета ВлГУ

Дубровин, Н. И.

Д56 Фундаментальная и компьютерная алгебра : учеб. пособие / Н. И. Дубровин ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2014. – 87 с. – ISBN 978-5-9984-0478-8.

Основная цель пособия – знакомство с классическими объектами алгебры: полями, кольцами вычетов, конечно-порожденными абелевыми группами, группой подстановок, алгеброй матриц, алгеброй многочленов, булевой алгеброй высказываний.

Предназначено для студентов-бакалавров, направление подготовки которых предполагает большое содержание математики. Для освоения курса необходимо знакомство с линейной алгеброй и математическим анализом в объеме первого семестра, а также нужна начальная компьютерная грамотность.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС 3-го поколения.

Ил. 3. Табл. 3. Библиогр.: 9 назв.

УДК 512(076)
ББК 22.14я73

ISBN 978-5-9984-0478-8

Оглавление

Введение

Курс «Фундаментальная и компьютерная алгебра» предназначен для студентов направлений «Математика», «Прикладная математика», «Математика и компьютерные науки», «Защита информации», «Математическое обеспечение и администрирование информационных сетей» и др. Он рассчитан на 36 лекционных часов и на 36 часов практики. Курс предполагает знания по линейной алгебре и началам анализа. Он также предполагает элементарную компьютерную грамотность и, в частности, знакомство с редакторами WinWord и Excel. Компьютерная часть курса базируется на среде Visual basic for applications (далее VBA), подсоединенной к упомянутым редакторам. Параллельно с развиваемой в курсе теорией развивается и компьютерная составляющая этой теории. Иными словами, каждый теоретический фрагмент доводится до состояния программного воплощения. В этой компьютерной составляющей дисциплины алгоритмически решаются задачи фундаментальной алгебры на основе VBA.

Основная цель данного пособия – знакомство как с классическими алгебраическими объектами, так и с их конструкциями. Перечислим их.

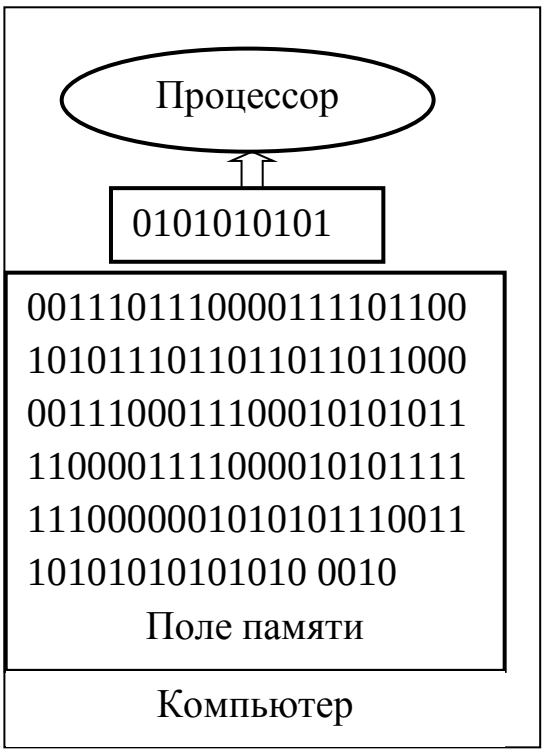
- Множество натуральных чисел $\mathbb{N}$ с операциями сложения и умножения, деления с остатком.
- Кольцо целых чисел $\mathbb{Z}$ с аналогичными операциями.
- Поле рациональных чисел $\mathbb{Q}$.
- Поле комплексных чисел $\mathbb{C}$ с операциями сложения, умножения, обращения, сопряжения, записью в показательной форме.
- Алгебра матриц $\mathrm{Mat}(K)$ над полем K.
- Булеан $\mathrm{Boolean} = \{0,1\}$ с операциями дизъюнкции $\vee$, конъюнкции $\wedge$, сложения, отрицания, импликации, тождества
- Алгебра Жегалкина $\mathbb{L}_n$ как кольцо многочленов от n переменных над булеаном, и в которой выполняется тождество $x^2 = x$. Операции на алгебре $\mathbb{L}_n$ те же, что и на булеане.
- Конечно-порожденные (и, в частности, циклические) абелевы группы $\mathbb{Z}^n/H$. Здесь H – подгруппа в свободной группе $\mathbb{Z}^n$.
- Группа подстановок S_n.
- Алгебра многочленов над полем, в частности, над полями действительных и комплексных чисел.
- Тело кватернионов.

1. НЕМНОГО О БЕЙСИКЕ

В математике имеют дело с такими объектами, как числа разной природы (натуральные, целые, рациональные, действительные, комплексные), многочлены одной и нескольких переменных, матрицы, рациональные функции, геометрические линии, фигуры и тела и т.д. К ним применяются различные операции и отображения; это правила «переработки» объектов одного типа в объекты другого (или того же самого) типа. Между алгебраическими объектами устанавливаются различного рода отношения (равно, больше, принадлежит, лежит, делит, перпендикулярно, параллельно и т.п.). В памяти компьютера, как объекты, так и операции и отношения записываются в виде бинарной строки вида

$$(\boldsymbol{\varepsilon}_1, \dots, \boldsymbol{\varepsilon}_n), \text{где все } \boldsymbol{\varepsilon}_j \in \{0,1\}.$$

На физическом уровне 0 и 1 соответствуют двум состояниям элементарной ячейки памяти – биту. В отвлеченном виде компьютер можно представлять как процессор, который перерабатывает поле памяти в соответствии с инструкцией, которая записана в виде битовой строки в том же самом поле памяти (см. рисунок). Переработка происходит через определенный интервал времени, обратная величина которого называется тактовой частотой процессора. В современных ПК тактовая частота 2.7 Ггц (= 2700000 тактов в секунду), а память 1 – 2 Тбт (1Тб =2^{10} Гбт = 2^{20}Мгб = 2^{30}кбт = 2^{40} бит). Количество бит, которые за один такт может обработать процессор, называется разрядностью процессора; сейчас это 32 бита. Процессор может находиться в одном из строго определенных состояний; число их невелико по сравнению с памятью компьютера. Результат «обработки» полностью определяется состоя-



нием памяти (т.е. распределением нулей и единиц) и состоянием процессора.

Основной наш инструмент решения задач на «компьютерном уровне» – язык программирования Бейсик, а точнее, Visual Basic for Application (кратко: VBA). В качестве “Application” почти всегда будем использовать электронные таблицы Excel. Автор рассчитывает на то, что вы знакомы с Excel на уровне пользователя, умеете открывать программу, записывать в ячейки числовые и строковые данные, копировать и перемещать различные области листов Excel и все это сохранять. Сохранять файлы Exel нам придется, выбрав опции

Сохранить как / Книга Excel с поддержкой макросов

для того, чтобы VBA был подключен к соответствующему файлу. Запустить VBA можно щелкнув на «Разработчик/Visual Basic». Нам нужны будут два окна VBA:

1. Окно “Module”, где пишутся коды программ (если оно отсутствует, то в VBA надо использовать опции Insert/Module).

2. Окно Immediate. В нем можно проводить простые и непосредственные вычисления. Например, набрав в этом окне

? sqr(9)*2^(-1)*exp(0)

и нажав “Enter”, мы получим строкой ниже результат 1,5. Окно Immediate нам понадобится и для распечатки результатов работы программы. Если в программе записать код

Debug.Print “значение=”;5 , (1)

то при запуске программы в окне Immediate появится

значение = 5. (2)

Если же в (1) знак “;” заменить на запятую, то в (2) после равенства появится большой пробел – (строковое выражение “значение=” и число 5), – они будут отпечатаны в режиме табуляции. Следует отметить одну полезную опцию

Debug.Print Newline,

означающую переход на новую строку при распечатке результатов. Однако чаще всего мы будем пользоваться ячейками Excel для записи результатов работы программы, а также для присвоения конкретных значений переменным. Разберем пример программы

```
Sub Деление_с_остатком()
Const n As Byte = 5
Dim m As Integer
Cells(2, 1) = "Делитель равен ": Cells(2, 3) = n
m = Cells (3, 3)
Cells (5, 1) = "Неполное частное от деления m на " & n & "="
Cells (5, 5) = m\n
Cells (6, 1) = "Остаток от деления m на " & n & " равен"
Cells (6, 5) = m Mod n
End Sub
```

Первая строка открывает программу с названием «Деление _ с _ остатком». В скобках пишутся входные данные программы; у нас сейчас их нет. Вторая строка объявляет константу n типа Byte, под которую в памяти компьютера отводится 8 бит (= 1 байт) и в эти восемь бит будет записано число 5 в двоичной системе: 00000101. Итак, тип Byte предназначен для записи и обработки целых чисел от 0 до 255 включительно. Заметим, что в теле программы константе запрещено присваивать какие-либо значения, т.е. она может встречаться только по правую сторону знака равенства. В третьей строке объявляется переменная m типа Integer. В общем, оператор вида

Dim идентификатор as тип переменной

выделяет область памяти с заранее оговоренными для данного типа объемом и структурой, а идентификатор есть ссылка и имя этого кусочка памяти.

Типу Integer отводится два байта для записи целого числа в пределах от -2^{15} до $2^{15}-1$. Один бит отводится под запись знака числа: если этот бит равен 0, то число неотрицательно, а если равен 1, то оно отрицательно. Запишем выделенные два байта в виде

$$(\mathrm{sgn}, \boldsymbol{\varepsilon}_0, \dots, \boldsymbol{\varepsilon}_{14}). \qquad (3)$$

Здесь первый бит указывает на знак числа. Если sgn = 0, то (3) кодирует число $\boldsymbol{\varepsilon_0} + \boldsymbol{\varepsilon}_1 \cdot 2 + \cdots + \boldsymbol{\varepsilon}_{14} \cdot 2^{14}$, пределы изменения которого от 0 до $2^{15}-1$. Если же sgn = 1, то (3) кодирует отрицательное число

$$-(1 + \overline{\boldsymbol{\varepsilon}_0} + \overline{\boldsymbol{\varepsilon}_1} \cdot 2 + \cdots + \overline{\boldsymbol{\varepsilon}_{14}} \cdot 2^{14}).$$

Чертой сверху обозначена унарная операция отрицания, в VBA она имеет имя not:

$$\mathrm{not}(\boldsymbol{\varepsilon}) \coloneqq \begin{cases} 1, \text{если } \boldsymbol{\varepsilon} = 0, \\ 0, \text{если } \boldsymbol{\varepsilon} = 1. \end{cases}$$

Итак, строка из шестнадцати единиц кодирует число -1, а (1, 0, 0, …, 0) кодирует -2^{15}. Следовательно, $-2^{15} \leq m \leq 2^{15} - 1$. Для работы с целыми числами имеется также тип Long, переменным которого выделяются четыре байта с тем же самым принципом кодирования чисел, что и для типа Integer. Следовательно, пределы изменения переменной типа Long – от -2^{31} до $2^{31} - 1$.

В четвертой строке программы мы записываем в активный лист Excel значение делителя. Еще раз подчеркнем, если активным листом был «Лист 2», то данные запишутся именно во второй лист. Двоеточие между операторами – удобный способ записи нескольких операторов в одной строке. В пятой строке переменной m присваивается значение, содержащееся в ячейке (3,3) (третья строка и третий столбец C). Если в этой ячейке ничего нет, то присваивается 0, если стоит вещественное число типа $6{,}27$ или $-0{,}5$, то присваивается ближайшее целое, т.е. 6 или 0 в данном случае (этому соответствует функция round(x) в VBA). Если же в ячейке C3 записать целое число за рамками отрезка $-2^{15} \leq m \leq 2^{15} - 1$, то возникла бы ситуация ошибки № 6 Overflow, о которой вас немедленно во время работы программы известит компилятор VBA. Кстати, перед запуском программы полезно запустить опцию Debug / Compile Project. Произойдет проверка на правильность записи программы. Однако ошибку времени исполнения программы по типу той, что отмечена выше, никакая компиляторная проверка вначале отследить не может.

В остальных строках происходит запись результатов деления с остатком.

Немного теории: любое натуральное число m можно поделить на натуральное число n с остатком так, что

$$m = n \cdot q + r; \quad 0 \leq r < n. \tag{4}$$

Целые числа q (неполное частное) и r (остаток) определяются в (4) однозначно и им в VBA соответствуют функции

$$q = m \backslash n; \quad r = m \bmod n. \tag{5}$$

Воспользовавшись окном «Immediate» в VBA, проверим работу этих функций:

?5\3 → 1, ? 5\(-3) → -1, ?(-5)\(-3) → 1, ?(-5)\3 → -1
?5 mod 3 → 2; ? 5 mod -3 → 2; ? -5 mod 3 → -2; ? -5 mod -3 → -2

Мы видим, что операция $m\backslash n$ нечетна по обоим аргументам, в то время как $m \bmod n$ нечетна по первому аргументу и четна по второму. Кроме того, подстановка нуля вместо делителя выдаст ожидаемую ошибку № 11 “Division by zero”.

Следует отметить также операцию соединения строк

“по”&”бе”&”да”→ “победа”

Вместо знака & можно пользоваться обычным знаком плюс (« +»).

2. НАИВНАЯ ТЕОРИЯ МНОЖЕСТВ

Математический текст состоит из определений и утверждений. Некоторые утверждения в зависимости от важности и отношения к другим утверждениям называются одним из следующих терминов: «Аксиома», «Теорема», «Предложение», «Свойство», «Следствие», «Лемма». В определении объясняется, что означает какой-либо математический объект или что означает отношение между объектами посредством сведения к ранее определенным понятиям. Эти понятия, в свою очередь, вводятся в математический текст на основе ранее сформулированных определений и т.д. Ввиду конечности любого самого полного и подробного математического текста, мы очень быстро приходим к базовым, неопределяемым понятиям и отношениям, которые не определяются, а лишь иллюстрируются на примерах, взятых "из жизни". Таким базовым понятием в математике является понятие множества M, N, A, … , а неопределяемым отношением – отношение принадлежности между множествами: a∈ A (считается, что "элемент a принадлежит множеству A"). Множество можно мыслить как некую совокупность объектов, взятую как единое целое: множество людей на Земле, множество рыб в океане, множество птиц в стае и пр. В математике, конечно, имеют дело с математическими, а значит, строго определенными множествами чисел, функций, геометрических фигур и т.д. Самый простой способ определить множество – перечислить все его элементы. Например, A: = {5, 1, 2, 0} – множество, элемента-

ми которого являются числа 0, 1, 2 и 5. Здесь использован также знак ":=", который заменяет слова "равно по определению".

Два множества M и N равны (записываем $M = N$), если они состоят из одних и тех же элементов, т.е. для всякого x принадлежность $x \in M$ равносильна принадлежности $x \in N$. Например, А совпадает с множеством {1, 1, 0, 5, 2}. Выше сформулирована одна из аксиом теории множеств. Аксиомы наряду с теоремами и предложениями также относятся к утверждениям, но в отличие от последних не доказываются, а принимаются на веру. На аксиомы в математической теории падает самая большая нагрузка и ответственность. Во-первых, их выбирают исходя из самых существенных и принципиальных характеристик описываемых явлений жизни, других нематематических наук и других математических теорий. Во-вторых, их следует выбрать так, чтобы теория не была противоречивой, т.е. в рамках этой теории не могло бы быть выведено какое-либо утверждение и в то же время отрицание этого утверждения (например, "а∈А и а∉ А"). Далее следует позаботиться о том, чтобы развиваемая теория адекватно и полно описывала те явления, ради которых она создавалась.

Заметим, что термин «элемент» с математической точки зрения эквивалентен термину «множество». Если мы хотим сказать, что элемент x не принадлежит множеству M, то пишем $x \notin M$. Другие аксиомы теории множеств являются фактически правилами построения новых множеств из уже имеющихся. В частности, постулируется существование пустого множества $\emptyset$. Это множество не содержит ни одного элемента, т. е. для любого элемента x верно $x \notin \emptyset$.

Для множества М постулируется существование множества $\mathcal{P}(M)$ всех его подмножеств. При этом множество N называется подмножеством множества M (записываем $N \subseteq M$ или $M \supseteq N$), если всякий элемент из N является также и элементом множества M. Пустое множество, а также все множества заведомо будут подмножествами множества M.

Перечислим все элементы множества $\mathcal{P}(\{a, b, c\})$:

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

Как мы видим, $\mathcal{P}(\{a, b, c\})$ содержит восемь элементов. Обозначим через $|M|$ количество элементов в множестве M. Тогда

$$|\mathcal{P}(M)| = 2^{|M|}. \qquad (1)$$

Действительно, обозначим $n = |M|$ и перенумеруем элементы множества M=$\{m_1, \dots, m_n\}$. Сопоставим подмножеству $N \subseteq M$ бинарную строку $(\boldsymbol{\varepsilon}_j)$ длины n так, что $\boldsymbol{\varepsilon}_j = 1$ в случае $m_j \in N$ и $\boldsymbol{\varepsilon}_j = 0$ в противном случае. Получаем биекцию между множеством $\mathcal{P}(M)$ и множеством E^n бинарных строк длины n. Так как $|E^n| = 2^n$, то и $|\mathcal{P}(M)| = 2^n$. Заодно мы получили способ нумерации элементов множества всех подмножеств.

Пример 1. M:={2,{0,3,1},0} – множество из трех элементов, один из которых есть множество {0,3,1}, и это множество не является подмножеством первого. С другой стороны, множество {{0,3,1}} состоит из одного элемента, принадлежащего также и множеству M, поэтому {{0,3,1}}$\subset M$. Здесь знак включения "$\subset$ " строгий. Это значит, что множество в левой части содержится в множестве M, но не совпадает с ним.

С множествами можно осуществлять операции объединения, пересечения, разности и декартова произведения:

- Объединением множеств M и N называется множество $M \cup N$, состоящее из всех элементов, принадлежащих либо M, либо N (не исключающее "либо").
- Пересечением множеств M и N называется множество $M \cap N$, состоящее из всех элементов, принадлежащих M и N одновременно.
- Разностью множеств M и N, или дополнением множества N до множества M, называется множество $M \setminus N$, состоящее из всех элементов, принадлежащих M, но не N.

Имеют место следующие числовые соотношения конечных множеств:

$$|M \cup N| = |M| + |N| - |M \cap N|;\ |M \setminus N| = |M| - |M \cap N| \quad (2)$$

2.1. Декартовы произведения

Упорядоченная пара, или просто пара элементов (m, n), – это одна из фундаментальных конструкций в математике. Представлять её можно как полочку с двумя местами – первым и вторым. Очень часто в математике неважно, как на самом деле устроен тот или иной объект, а важны правила обращения с ним. Подобно этому при игре в шахматы совершенно неважно, из чего сделаны фигуры и какой они в

точности формы, важны лишь правила игры. Правило обращения с парой одно:

$$(m,n) = (m',n') \overset{\text{аксиома}}{\Longleftrightarrow} m = m' \text{и } n = n'.$$

($\Leftrightarrow$ – логический знак, заменяющий слова "тогда и только тогда, когда", "если и только если" и т.п.) Далее индуктивно можно строить упорядоченные тройки элементов, четверки элементов и т. д.:

$$(m,n,k) = \big((m,n),k\big);\ (m,n,k,q) = \big((m,n,k),q\big), \ldots$$

Декартовым произведением $M \times N$ двух множеств M и N называется множество всех пар (m, n), где m пробегает M, а элемент n пробегает N. Существование пары элементов и декартова произведения – очередные аксиомы теории множеств.

Пример 2. Если $M = \{a,b,c\}$ и $N = \{1,2\}$, то

$$M \times N = \{a1, a2, b1, b2, c1, c2\} \neq N \times M \text{ и } |M \times N| = 6.$$

Общее правило подсчета элементов в декартовом произведении (правило умножения) таково:

$$|M \times\ N| = |M| \cdot |N|. \qquad (3)$$

3. НАТУРАЛЬНЫЕ ЧИСЛА

Числа {1,2,3,… }, которые можно получить из единицы операцией сложения, называют натуральными и обозначают $\mathbb{N}$. Аксиоматическое описание натуральных чисел может быть таким: это множество $\mathbb{N}$, на котором имеется выделенный элемент $1 \in \mathbb{N}$ (0-арная операция) и имеется унарная операция прибавления единицы, сопоставляющая всякому натуральному числу n натуральное число n + 1, причем выполняются следующие аксиомы:

– (N1) для любого натурального числа n результат n + 1 не равен единице;

– (N2) для любых двух натуральных чисел из равенства $n + 1 = m + 1$ вытекает равенство $n = m$;

– (N3) (**метод математической индукции**). Пусть $\mathcal{A}\langle n\rangle$ – какая-либо высказывательная форма с переменной $n \in \mathbb{N}$. Если высказывание $\mathcal{A}\langle 1\rangle$ верно и для любого натурального n из $\mathcal{A}\langle n\rangle$ вытекает $\mathcal{A}\langle n{+}1\rangle$, то утверждение $\mathcal{A}\langle n\rangle$ верно для всех натуральных n.

Теоретико-множественная интерпретация, а точнее, рекуррентное построение системы натуральных чисел вместе с нулем заключается в том, что мы полагаем $0 = \emptyset$ и для каждого следующего натурального $n + 1$ полагаем $n + 1 = n \cup \{n\}$. Тогда

$$1 = \{\emptyset\}; 2 = \{\emptyset, \{\emptyset\}\}; 3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\};$$
$$4 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$$

и т. д.

3.1. Рекурсия

От аксиом N1-N3 до знакомых всем операций сложения и умножения натуральных чисел, сравнения натуральных чисел между собой и свойств вида "от перемены мест слагаемых сумма не изменится" большая дистанция. Зачастую доказательство таких утверждений есть формальные проверки с многократным использованием метода математической индукции. Принципиальный момент – рекурсивные определения сложения и затем умножения натуральных чисел. В общем виде рекурсия – это метод построения или вычисления, когда каждый следующий объект строится (вычисляется) на основе предыдущих. Абстрактно рекурсия в простейшем виде описывается отображением $F{:}M \to M$ и начальным значением $x_1 \in M$. Далее объект x_{n+1} вычисляется как $x_{n+1} = F(x_n)$ в предположении, что x_n уже известен.

Метод математической индукции показывает, что тогда мы получаем отображение $n \to x_n$ или последовательность объектов из множества *M*. Сама формула $x_{n+1} = F(x_n)$ называется рекуррентной, и ее использование возможно лишь, если явно задан начальный объект x_1.

Определим сложение посредством рекуррентной формулы $m + +(n + 1) := (m + n) + 1$. Например, докажем, что $2 + 2 = 4$. По определению $2 := 1 + 1,\ 3 := 2 + 1,\ 4 := 3 + 1, \ldots, 9 := 8 + 1$ суть множество цифр в десятичной системе счисления. Тогда

$$2 + 2 = 2 + (1 + 1) = (2 + 1) + 1 = 3 + 1 = 4.$$

Умножение определяется явным заданием формулы умножения на единицу: $m \cdot 1 := m$, а также рекуррентной формулой $m\ (n+1) := m \cdot n + m$. В частности, единица есть нейтральный элемент операции умножения. Далее доказываются фундаментальные свойства операций сложения и умножения:

- (ассоциативность) для любых чисел m, n, k выполняются равенства $m + (n + k) = (m + n) + k; m(nk) = (mn)k$;
- (коммутативность) $m + n = n + m;\ mn = nm$;
- (дистрибутивность) $m(n + k) = mn + mk$.

Здесь специально вместо выражения "для любых натуральных чисел" употребляется выражение "для любых чисел"; эти фундаментальные свойства верны для всех чисел.

Докажем, например, ассоциативность сложения индукцией по k. Для $k = 1$ получаем формулу $(m + n) + 1 = m + (n + 1)$. Это равенство справедливо для всех натуральных чисел m и n по определению сложения. Допустим теперь, что равенство $(m + n) + k = m + (n + k)$ для некоторого k и при любых m и n установлено, и теперь нам надо проверить аналогично равенство для $k + 1$:

$$(m + n) + (k + 1) = \big((m + n) + k\big) + 1 = \big(m + (n + k)\big) + 1 = \\ = m + ((n + k) + 1) = m + (n + (k + 1)).$$

Здесь во втором равенстве использовано предположение индукции, а в остальных – определение сложения. Ассоциативность сложения доказана в силу принципа математической индукции (см. аксиому N3). Аналогично проверяются остальные свойства сложения и умножения.

Присоединим к множеству натуральных чисел элемент ноль, обладающий свойством нейтральности для сложения и свойством поглощения для умножения:

$$0 + n = n + 0 = n;\ \ 0 + 0 = 0;\ \ n \cdot 0 = 0 \cdot n = 0 \cdot 0 = 0.$$

(для любого $n \in \mathbb{N}$). Получаем множество $\mathbb{N}_0$ всех целых неотрицательных чисел, для которых перечисленные выше свойства ассоциативности, коммутативности и дистрибутивности сохраняются.

3.2. Порядок на множестве натуральных чисел

На множестве $\mathbb{N}_0$ имеется отношение линейного порядка. Скажем, что $n < m$, если найдется натуральное число k такое, что $n + k = m$. Отношение $n \leq m$ тогда получается из отношения строгого неравенства простой логической операцией: $n \leq m$ означает, что либо $n = m$, либо $n < m$. Например, $5 \leq 5$ – верное высказывание. Отметим фундаментальные свойства неравенств.

- Если $n > m$, то $n + k > m + k$ для любого k. То же свойство справедливо для нестрогого неравенства.
- Если $n > m$, то $n \cdot k > m \cdot k$ для любого $k \in \mathbb{N}$. Если $n \geq m$, то $n \cdot k \geq m \cdot k$ для любого $k \in \mathbb{N}_0$.

Натуральные числа, а также множество $\mathbb{N}_0$ среди других числовых систем обладают свойством полной упорядоченности: любое непустое подмножество натуральных чисел M имеет наименьший элемент min M. Докажем это утверждение.

Пусть $M \subseteq \mathbb{N}_0$ и $M \neq \emptyset$. Обозначим через $[0, n]$ множество целых неотрицательных чисел больше либо равных 0 и меньше либо равных n. Вначале индукцией по n установим, что если пересечение $M \cap [0, n]$ не пусто, то существует min M. База индукции – случай $n = 0$. Тогда min M = 0. Пусть утверждение доказано для n, проверим, что тогда оно справедливо и для $n + 1$. Имеем $M \cap [0, n + 1] \neq \emptyset$. Если, кроме того, $M \cap [0, n] = \emptyset$, то min M = $n + 1$, иначе $M \cap [0, n] \neq \emptyset$, и можно воспользоваться предположением индукции. Итак, принцип индукции позволяет утверждать, что если $M \cap [0, n] \neq \emptyset$ для какого-либо $n \in \mathbb{N}_0$, то существует min M. Но для непустого множества M это условие заведомо выполняется, достаточно выбрать $m \in M$ и тогда $m \in M \cap [0, m]$, откуда $M \cap [0, m] \neq \emptyset$.

Принцип полной упорядоченности эквивалентен принципу индукции. Сформулируем и докажем принцип индукции в другой редакции.

Пусть мы имеем серию утверждений $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, ... Известно, что утверждение $\mathcal{P}_1$ справедливо, а также известно, что если $\mathcal{P}_k$ справедливо для всех $k < n$, то и $\mathcal{P}_n$ тоже истинно. Тогда все утверждения $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, ... верны.

Для обоснования этого утверждения рассмотрим множество M всех натуральных чисел m таких, что $\mathcal{P}_m$ не верно. Если M непусто, то существует m = min M. Число m не равно 1 в силу истинности $\mathcal{P}_1$. Кроме того, для любого $k < m$ утверждение $\mathcal{P}_k$ справедливо, ибо $k \notin M$. Но тогда и $\mathcal{P}_m$ верно. Получаем противоречие с тем, что $\mathcal{P}_m$ ложно в силу того, что $m \in M$. Противоречие показывает, что $M = \emptyset$, тем самым нет ни одного натурального k такого, что $\mathcal{P}_k$ ложно. Значит все утверждения $\mathcal{P}_k$ истинны.

3.3. Делимость натуральных чисел

Операция деления не всегда возможна в области натуральных чисел. Это дает нам право ввести отношение делимости: скажем, что число n делит число m, если $m = nk$ для какого-либо подходящего $k \in \mathbb{N}$. Обозначается это отношение так: $n \mid m$. Среди всех натуральных чисел особо выделяются простые числа – это числа n, имеющие ровно два делителя, – единицу и само число n. Тем самым единица не будет простым числом – она имеет один делитель. Но по существу единица не причисляется к простым числам в силу своей обратимости: $1^{-1} = 1 \in \mathbb{N}$. Вот первые 99 простых чисел:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523.

Число, не являющееся простым, называется составным. Пусть k – составное натуральное число. Тогда $k = a \cdot b$ для некоторых натуральных чисел a и b, больших единицы. При этом получаем $a, b < k$. Число a (так же, как и b) либо простое, либо составное. Во втором случае снова раскладываем $a = pq$, где p, q>1, и поэтому $p, q < a$. Ввиду уменьшения делителей этот процесс не может продолжаться бесконечно (см. свойство полной упорядоченности). Следовательно, в итоге получаем разложение числа k в произведение простых чисел. Тот факт, что такое разложение единственно с точностью до перестановки сомножителей, мы докажем позже, а пока сформулируем теорему.

Теорема 1 (основная теорема арифметики). Любое натуральное число k, большее единицы, разложимо в произведение простых чисел:

$$k = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}, \qquad p_1 < p_2 < \dots < p_s \ - \text{ простые числа } (*)$$

(здесь $n_j \in \mathbb{N}$). Такое разложение единственно.

Теорема 2. Множество простых чисел бесконечно.

Доказательство. Предположим противное: множество простых чисел исчерпывается числами $q_1, q_2, \dots, q_n$. Образуем число

$$M := q_1 \cdot q_2 \cdot \dots \cdot q_n + 1.$$

Это число по основной теореме арифметики имеет простой множитель p. Тем самым $p = q_i$ для какого-либо i. Тогда из соотношений $p \mid M$ и $p \mid q_1 \cdot q_2 \cdot \ldots \cdot q_n$ вытекает, что p делит их разность, т.е. число 1 и, следовательно, $p \leq 1$. Это противоречие показывает, что предположение о конечности множества простых чисел неверно. Следовательно, верно отрицание этого утверждения, т.е. верно то, что утверждается в формулировке теоремы. □

4. ДЕЛИМОСТЬ ЦЕЛЫХ ЧИСЕЛ

Обозначим через $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ – кольцо целых чисел. Термин «кольцо» означает, что мы имеем дело с множеством R, на котором заданы две операции – сложение и умножение, подчиняющиеся известным правилам – переместительному, сочетательному и распределительному законам.

Кольцо $\mathbb{Z}$ – евклидово, т.е. в нем имеется возможность деления с остатком, отмеченная в первом разделе. Заметим, что $\mathbb{Z}$ – не единственное евклидово кольцо. Таковым будет и кольцо многочленов, которое будем изучать далее.

Как практически решается задача о разложении натурального числа в произведение простых? Для начала надо научиться отличать простые числа от составных. Возьмем число m = 27 489. Нетрудно догадаться, что оно делится на 3, так как сумма цифр этого числа – 2 + 7 + + 4 + 8 + 9 – делится на 3. Получаем m = 3· 9 163. А далее? Ничего не поделаешь, придется решать задачу лобовым способом: перебирать все простые числа из списка простых чисел и каждый раз пробовать – делит ли оно 9 163 или нет. При этом достаточно перебрать простые числа, не превосходящие корень квадратный из 9 163, т.е. 95,7. Действительно, если число m составное и $m = a \cdot b$, то либо a, либо b не превосходят $\sqrt{m}$. Потрудившись, получим 27 489 = 3· 7· 7· 11· 17.

4.1. Алгоритм Евклида

Дана пара целых чисел (m, n). Первый шаг алгоритма Евклида – делим m на n с остатком, а далее делим остаток на вновь получившийся остаток до тех пор, пока этот вновь получившийся остаток не станет равным 0. Этот момент обязательно наступит, так как модули остатков строго убывают. Более точно: обозначим $r_1 = n$ и образуем последовательность делений с остатком:

$$\text{если } r_1 \neq 0, \text{то } m = r_1 q_1 + r_2, \text{где } |r_2| < |r_1|,$$
$$\text{если } r_2 \neq 0, \text{то } r_1 = r_2 q_2 + r_3, \text{где } |r_3| < |r_2|,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\text{если } r_k \neq 0, \text{то } r_{k-1} = r_k q_k + r_{k+1}, \text{где } r_{k+1} = 0.$$

Для чего предназначен этот алгоритм? Например, для вычисления наибольшего общего делителя (НОД) пары чисел m и n. Обозначим через НОД (m, n) наибольшее натуральное число, делящее как m, так и и n. Дополнительно по определению полагаем НОД (0, 0) = 0.

Если $d \mid n, m$, то $d \mid m - nq_1$, т.е. $d \mid r_2$ согласно первой строке алгоритма. Но тогда d делит и $r_3 = r_1 - r_2 q_2$ и так далее, вплоть до $d \mid r_k$. Эту цепочку импликаций можно обратить: если $d \mid r_k$, то d делит $r_{k-1} = r_k q_k$, а затем делит $r_{k-2} = r_{k-1} q_{k-1} + r_k$ и так далее, вплоть до n и m. Доказано, что НОД $(m, n) = r_k$ совпадет с последним ненулевым остатком в алгоритме Евклида. Попробуем на практике, взяв m = 900 и n = 1155:

$$900 = 1155 \cdot 0 + 900;$$
$$1155 = 900 \cdot 1 + 255;$$
$$900 = 255 \cdot 3 + 135;$$
$$255 = 135 \cdot 1 + 120;$$
$$135 = 120 \cdot 1 + 15;$$
$$120 = 15 \cdot 8 + 0.$$

Итог: НОД (900, 1155) = 15. Мы могли бы уменьшить числа, пользуясь правилом

$$\text{НОД } (km, kn) = k \cdot \text{НОД } (m, n). \qquad (1)$$

Тогда НОД (900, 1155) = 5 · НОД (180, 231) = 15 · НОД (60, 77). Но далее, применяя алгоритм Евклида, мы записали бы опять шесть строк и пришли к выводу, что НОД (60, 77) = 1.

Числа m и n, наибольший общий делитель которых равен 1, называются взаимно простыми.

Оказывается, число d = НОД (m, n) можно записать в виде линейной комбинации своих аргументов:

$$d = m \cdot m' + n \cdot n'. \qquad (2)$$

Это важное соотношение позволяет доказать известное правило для простых чисел p:

$$\text{если } p \mid ab, \text{то либо } p \mid a, \text{либо } p \mid b, \qquad (3)$$

из которого, в свою очередь, вытекает единственность разложения на простые множители. Однако, все по порядку: докажем сначала (2).

Проходим еще раз по строкам алгоритма Евклида сверху вниз: $r_2 = m + n \cdot (-q_1)$ выражается в виде линейной комбинации, тогда и

$$r_3 = r_1 - r_2 q_2 = n - (m + n \cdot (-q_1))q_2 = m \cdot (-q_2) + n \cdot (1 + q_1 q_2)$$

также выражается через m и n в виде линейной комбинации. Дойдя до последней строки, видим, что и $d = r_k = r_{k-1} q_{k-1}$ выражается через m и n в виде линейной комбинации. Заметим, что если выполняется соотношение (2), то $|d|$ заведомо есть НОД чисел m и n. Для чисел $m = 900, n = 1155$ получаем:

$$255 = 1155 - 900 \cdot 1;$$

$$135 = 900 - 225 \cdot 3 = 900 - (1155 - 900 \cdot 1) \cdot 3 = \\ = 900 \cdot 4 - 1155 \cdot 3;$$

$$120 = 255 - 135 \cdot 1 = 1155 - 900 \cdot 1 - (900 \cdot 4 - 1155 \cdot 3) = \\ = 900 \cdot (-5) + 1155 \cdot 4;$$

$$15 = 135 - 120 = 900 \cdot 4 - 1155 \cdot 3 - (900 \cdot (-5) + 1155 \cdot 4) = \\ = 900 \cdot 9 - 1155 \cdot 7.$$

Докажем теперь правило (3). Пусть $p \mid ab$, т.е. $ab = pk$ для некоторого k. Если $p \mid a$, то все доказано. Иначе НОД (p, k) = 1, ибо p – простой элемент. Следовательно, найдутся числа s, t такие, что $1 = ps + at$. Тогда

$$b = 1 \cdot b = (ps + at)b = psb + abt = pst + pkt = p(sb + kt),$$

откуда $p \mid b$.

Предположим теперь, что

$$p_1^{n_1} p_2^{n_2} \dots p_s^{n_s} = q_1^{n_1} q_2^{n_2} \dots q_t^{n_t} - \qquad (4)$$

два разложения в произведение простых чисел: простые числа $p_1, p_2, \dots, p_s$, а также $q_1, q_2, \dots, q_t$ попарно различны. Доказательство ведем индукцией по числу $s + t$. База индукции – случай, когда $s = t = 1$, очевиден. Так как q_1 делит произведение $p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, то q_1 делит один из сомножителей p_i. Но этот сомножитель также есть простой элемент, и поэтому $q_1 = p_i$.

Сокращая левую и правую части соотношения (4) на q_1, получаем аналогичное равенство, но с меньшим числом сомножителей. Продолжая этот процесс, дойдем до равенства $p_s = q_t$ и, в частности, до равенства $s = t$. Этим и завершается доказательство основной теоремы арифметики.

4.2. Матричная трактовка алгоритма Евклида

Придадим матричную трактовку алгоритму Евклида (о матрицах см. разд. 7). Перепишем последовательность делений с остатком в матричном виде:

$$\begin{pmatrix}0 & 1\\ 1 & -q_1\end{pmatrix}\begin{pmatrix}m\\ n\end{pmatrix}=\begin{pmatrix}r_1\\ r_2\end{pmatrix};\ \begin{pmatrix}0 & 1\\ 1 & -q_2\end{pmatrix}\begin{pmatrix}r_1\\ r_2\end{pmatrix}=\begin{pmatrix}r_2\\ r_3\end{pmatrix};\ \dots;$$
$$\begin{pmatrix}0 & 1\\ 1 & -q_k\end{pmatrix}\begin{pmatrix}r_{k-1}\\ r_k\end{pmatrix}=\begin{pmatrix}r_k\\ 0\end{pmatrix}.$$

Подставляя в каждое последующее равенство вместо столбца в левой части левую часть предыдущего равенства, получим:

$$\begin{pmatrix}0 & 1\\ 1 & -q_k\end{pmatrix}\dots\begin{pmatrix}0 & 1\\ 1 & -q_2\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & -q_1\end{pmatrix}\begin{pmatrix}m\\ n\end{pmatrix}=\begin{pmatrix}r_k\\ 0\end{pmatrix}.$$

Заметим, что слева стоят матрицы с определителем –1, поэтому их произведение, обозначим его $\begin{pmatrix}t & s\\ u & v\end{pmatrix}$, имеет определитель $(-1)^k=\pm 1$ и, значит, оно обратимо в кольце целочисленных 2×2-матриц.

Доказана

Теорема. Для любой пары целых чисел (m,n) с $d\coloneqq \text{НОД}(m,n)$ найдется обратимая 2×2-матрица Q над $\mathbb{Z}$ такая, что

$$Q\cdot\begin{pmatrix}m\\ n\end{pmatrix}=\begin{pmatrix}d\\ 0\end{pmatrix}.$$

В частности, найдутся числа $m'=t, n'=s$ такие, что $m\cdot m'+n\times$ $\times n'=d$.

В нашем численном примере

$$\begin{pmatrix}9 & -7\\ -77 & 60\end{pmatrix}\cdot\begin{pmatrix}900\\ 1155\end{pmatrix}=\begin{pmatrix}15\\ 0\end{pmatrix}.$$

Вторую строку матрицы Q можно найти с помощью НОК (m, n) – наименьшего общего кратного чисел m и n, т.е. наименьшего натурального числа, кратного как m, так и n. Оно связано с НОД соотношением

$$\text{НОД}(a,b)\cdot\text{НОК}(a,b)=|ab| \qquad (5)$$

и в нашем числовом примере равно НОК (900, 1 155) = 900 · 1 155 / 15 = = 69 300. Тогда 69 300 = $900\cdot 77=1\,155\cdot 60$ и поэтому

$$-77\cdot\ 900+60\cdot\ 1\,155=0.$$

Вот отсюда и берется вторая строка (-77, 60). Определитель матрицы Q, полученной таким образом, будет заведомо ± 1 (мы его сделали +1 за счет корректировки знаков второй строки).

Фактически выше указан алгоритм, позволяющий вычислить матрицу Q. Основная идея алгоритма заключается в том, что по мере продвижения по строкам алгоритма Евклида мы сначала от единичной матрицы переходим к матрице $\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$, затем к матрице $\begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} = \begin{pmatrix} 1 & -q_1 \\ -q_2 & 1+q_1q_2 \end{pmatrix}$ и т.д., пока не дойдем до итоговой матрицы $Q = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \ldots \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$.

5. РАЦИОНАЛЬНЫЕ ЧИСЛА

Уравнение $xa = b$ не всегда разрешимо в области целых чисел. Для того чтобы исправить это, вводят дробные (рациональные) числа b/a как формальную запись решения этого уравнения. Число b называют числителем, а a – знаменателем дроби b/a. Заметим, что случай $a = 0$ исключается, так как уравнение $xa = b$ в этом случае либо не имеет решений ($b \neq 0$), либо имеет множество решений ($b = 0$). Кроме того, из интерпретации дроби b/a как решения уравнения $xa = b$ вытекает правило равенства дробей

$$\frac{b}{a} = \frac{b'}{a'} \underset{\text{опр}}{\Leftrightarrow} ba' = b'a.$$

Определим операции сложения и умножения дробей:

$$\frac{b_1}{a_1} + \frac{b_2}{a_2} = \frac{b_1a_2 + b_2a_1}{a_1a_2};\ \frac{b_1}{a_1} \cdot \frac{b_2}{a_2} = \frac{b_1b_2}{a_1a_2}.$$

Относительно этих операций множество рациональных чисел $\mathbb{Q}$ образует поле. Это значит, что наряду с операциями сложения и умножения, подчиняющимися тождествам ассоциативности, коммутативности и дистрибутивности, любое уравнение вида $x \cdot \left(\frac{a_1}{a_2}\right) = \frac{b_1}{b_2}$, где $\frac{a_1}{a_2} \neq 0$ имеет (единственное) решение $\frac{b_1a_2}{b_2a_1}$. Отношение линейного порядка продолжается с целых чисел на рациональные. Для ненулевой дроби $q = b/a$ определим знак $\operatorname{sgn} q$ как число 1 в том случае, когда числитель и знаменатель имеют одинаковые знаки, и полагаем $\operatorname{sgn} q = -1$ в противном случае. Итак, считаем дробь q положительной, если $\operatorname{sgn} q = 1$, и считаем ее отрицательной, если $\operatorname{sgn} q = -1$. Тогда полагаем, что $q_1 > q_2$ для двух дробей q_1, q_2, если

и только если, разность $q_1 - q_2$ – положительное число. Как и ранее считаем, что $q_1 \geq q_2$ эквивалентно тому, что либо $q_1 = q_2$, либо $q_1 > q_2$.

Заметим, кольцо целых чисел вкладывается в поле рациональных чисел посредством отображения $m \to \frac{m}{1}$. Допуская вольность, мы отождествляем целое число m и рациональное число $\frac{m}{1}$. Компьютер такую вольность допустить не может, и в его памяти целые числа и рациональные числа записываются в разных форматах. Другое дело, что методы работы с рациональными числами можно организовать так, что происходит автоматическое переформатирование там, где это возможно. Приведем пример – поручим компьютеру умножить 3 на дробь $7/3$. Вначале 3 записано как целое число, а дробь $7/3$ – как рациональное число (фактически как пара целых чисел (7,3)). «Увидев это», компьютер первым делом переведет число 3 в рациональное число $3/1$. Затем перемножит $\frac{3}{1} \cdot \frac{7}{3} = \frac{3 \cdot 7}{1 \cdot 3} = \frac{21}{3}$, после сократит – $\frac{21}{3} = \frac{7}{1}$. Наконец, усмотрев в последней дроби единичный знаменатель, выдаст ответ в виде целого числа 7.

Теорема 1 (иррациональность корня из 2). Уравнение $x^2 = 2$ неразрешимо в области рациональных чисел.

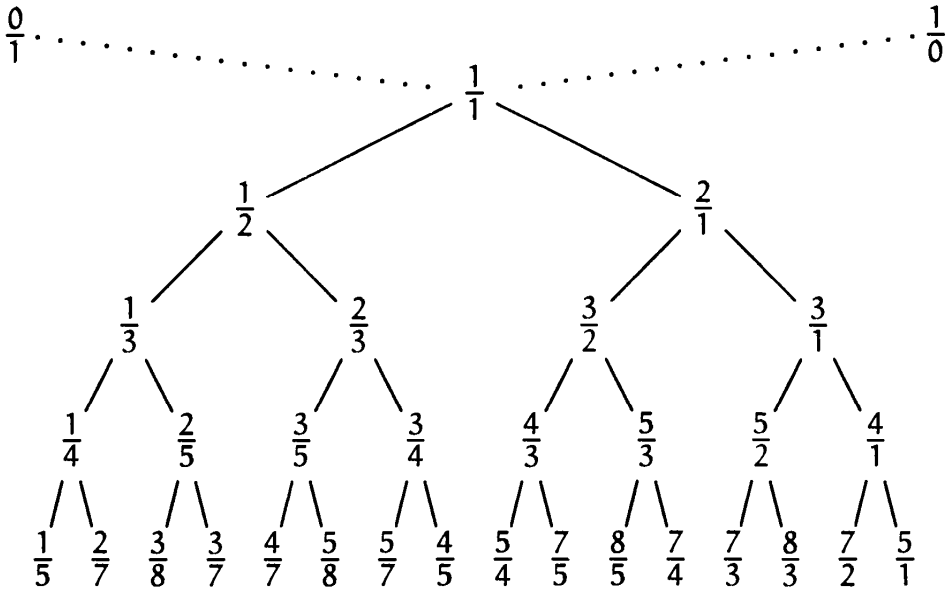
Доказательство. Предположим противное: дробь $q = b / a$ есть решение этого уравнения, т.е. $b^2/a^2 = 2$. Считаем дробь q несократимой. Так как $b^2 = 2a^2$, то по основной теореме арифметики получаем $2 \mid b$, т.е. $b = 2\,b'$. Тогда $4b'^2 = 2a^2$, т.е. $2b'^2 = a^2$ и снова $2 \mid a$. Следовательно, дробь b/a сократима на 2 – противоречие. Противоречие показывает, что наше предположение было неверным. Тем самым справедливо отрицание этого предположения: нет рациональных решений у уравнения $x^2 = 2$:

5.1. Дерево Штерна – Броко

Как перечислить все несократимые дроби от 0 до бесконечности, т.е. дроби вида m/n, где $m, n \in \mathbb{N}$ и НОД $(m, n) = 1$? Для этого рассмотрим бинарную операцию $Median\left(\frac{m}{n}, \frac{m'}{n'}\right)$, применимую к любым двум дробям

$$Median\left(\frac{m}{n}, \frac{m'}{n'}\right) = \frac{m + m'}{n + n'}. \qquad (1)$$

Обозначим совокупность несократимых положительных дробей вида, указанного выше, вместе с двумя дробями $\frac{0}{1}$ и $\frac{1}{0}$ (вторая из них несобственная, изображающая бесконечность в несократимом виде) через $\mathcal{R}$. Начиная именно с пары $\frac{0}{1}$; $\frac{1}{0}$ будем применять операцию (1) называя результат $\frac{m+m'}{n+n'}$ потомком дробей $\frac{m}{n}, \frac{m'}{n'}$. Получим следующее дерево Штерна – Брокко.



Заметим, что если $\frac{m}{n} < \frac{m'}{n'}$, то $\frac{m}{n} < \frac{m+m'}{n+n'} < \frac{m'}{n'}$. Действительно,

$$\frac{m+m'}{n+n'} - \frac{m}{n} = \frac{nm+nm'-mn-mn'}{(n+n')n} = \frac{nm'-mn'}{(n+n')n} > 0,$$

так как $\frac{m'}{n'} - \frac{m}{n} > 0$. Аналогично проверяется, что $\frac{m'}{n'} > \frac{m+m'}{n+n'}$.

Лемма. Если $\frac{m}{n}, \frac{m'}{n'}$ – последовательные дроби на любом шаге построения дерева Штерна – Брокко, то $m'n - n'm = 1$.

Доказательство. Предполагая верным равенство $m'n - n'm = 1$, достаточно проверить, что $m'(n+n') - n'(m+m') = 1$ и $(m'+m)n - (n'+n)m = 1$. Это так ввиду сокращения слагаемых $n'm'$ и $-n'm'$ в первом случае и $nm;\ -nm$ – во втором. □

Вывод: операция $Median$, примененная к двум дробям из $\mathcal{R}$, снова дает дробь из $\mathcal{R}$. Может ли какая-либо несократимая дробь a/b быть пропущенной в дереве Штерна – Брокко? Заведомо $\frac{0}{1} < \frac{a}{b} < \frac{1}{0}$. Пусть $\frac{m}{n}, \frac{m'}{n'}$ – последовательные дроби из $\mathcal{R}$ такие, что $\frac{m}{n} < \frac{a}{b} < \frac{m'}{n'}$ и тем самым

$$an - bm \geq 1; \;\; bm' - an' \geq 1. \qquad (2)$$

Для медианы $\frac{m+m\prime}{n+n\prime}$ возможны три случая. Во-первых, может быть, она совпадает a/b, и мы тогда удовлетворены. Во-вторых, она может быть меньше, чем a/b, и тогда дробь $\frac{m}{n}$ можно заменить на медиану и, в-третьих, медиана может быть больше, чем a/b, и тогда уже дробь m'/n' заменяем на медиану. Этот процесс не может продолжаться до бесконечности, так как из неравенств (2) вытекает

$$\begin{aligned} a + b = a(m'n - n'm) + b(m'n - n'm) = \\ = (m' + n')(an - bm) + (m + n)(bm' - an') \geq \\ \geq m' + n' + m + n. \end{aligned}$$

С каждым шагом либо n, либо m возрастает и мы достигнем совпадения с дробью из $\mathcal{R}$ самое большее за $a + b - 1$ шагов применения операции Median.

Можно указать алгоритм, который по заданной константе N выписывает в порядке возрастания все первые (точнее, верхние) $2^N + 1$ дроби из $\left[\frac{0}{1}; \frac{1}{1}\right] \cap \mathcal{R}$. Идея этого алгоритма состоит в том, что имея на каком-то этапе последовательность непосредственно следующих дробей из дерева Штерна – Брокко

$$q(0) = \frac{0}{1} < q(1) < q(2) \ldots < q(2^j),$$

мы «разрежаем» эту последовательность до новой последовательности

$$q(0) = \frac{0}{1} < q'^{(1)} < q'(2) < q'(3) < q'(4) \ldots < q'(2^{j+1})$$

так, что $q'(2 * i) = q(i)$, и далее полагаем

$$q'(2i + 1) = Median\big(q'(2i), q'(2i + 2)\big).$$

Результат для K = 6, т.е. для 64 + 1 = 65 дробей левой половины дерева, следующий:

0/1; 1/7; 1/6; 2/11; 1/5; 3/14; 2/9; 3/13; **1/4**; 4/15; 3/11; 5/18; 2/7; 5/17; 3/10; 4/13; 1/3; 5/14; 4/11; 7/19; 3/8; 8/21; 5/13; 7/18; 2/5; 7/17; 5/12; 8/19; 3/7; 7/16; 4/9; 5/11; **1/2**; 6/11; 5/9; 9/16; 4/7; 11/19; 7/12; 10/17; 3/5; 11/18; 8/13; 13/21; 5/8; 12/19; 7/11; 9/14; 2/3; 9/13; 7/10; 12/17; 5/7; 13/18; 8/11; 11/15; 3/4; 10/13; 7/9; 11/14; 4/5; 9/11; 5/6; 6/7; **1/1** (максимум знаменателя равен 21).

6. АЛГЕБРА ВЫСКАЗЫВАНИЙ

Высказывание есть некоторое повествовательное предложение, подлежащим в котором является математический объект и про которое можно в принципе сказать верно оно или ложно. Приведем примеры высказываний.

1. Прямая $y = 0.01$ пересекает ось Оx.
2. Число «пи» больше 3.14.
3. Отношение $\frac{0}{0}$ равно 1.
4. Число $\sqrt{3}$ есть корень уравнения $x^4 + x^2 - 12 = 0$.
5. Число $\sqrt{3}$ составляет все множество корней уравнения $x^4 + x^2 - 12 = 0$.
6. Корень из 2 не будет корнем никакого многочлена с целыми коэффициентами.
7. Число e (основание натуральных логарифмов) не будет корнем никакого многочлена с целыми коэффициентами.

Здесь утверждения 2, 4, 7 справедливы, утверждения 1, 5, 6 ложны, а 3 не является утверждением, поскольку нет такого объекта-числа как 0/0.

Пусть A и B – высказывания. Из них можно образовать более сложные высказывания путем применения логических операций.

а. «A или B». Это называется дизъюнкцией высказываний A, B и по-другому обозначается как A∨B (в компьютерной алгебре “A or B”).

б. «A и B». Это называется конъюнкцией высказываний A, B и по-другому обозначается как A ∧ B (в компьютерной алгебре “A and B”). Еще одно название этой операции – логическое умножение, в связи с чем она иногда обозначается точкой (а порой и точка не пишется).

в. «А либо В» – исключающее «либо», или, иначе, логическое сложение. В связи с этим другое обозначение операции А + В. В компьютерной алгебре эта операция обозначается “ xor ” .

г. «не А» – отрицание. В фундаментальной алгебре будем ее обозначать ⅂ А, а в компьютерной – not (А).

д. «из А следует В» – импликация. В фундаментальной алгебре будем ее обозначать А⇒ В, а в компьютерной – А Imp В.

е. «А эквивалентно В» – эквивалентность. В фундаментальной алгебре будем ее обозначать А⇔В , а в компьютерной – А Equ В.

Если известна истинностная оценка высказываний А и В, то она однозначно продолжается на перечисленные выше конструкции в соответствии с табл. 1.

Таблица 1

А	Ложь	Истина	Ложь	Истина
В	Ложь	Ложь	Истина	Истина
А ∨ В	Ложь	Истина	Истина	Истина
АВ	Ложь	Ложь	Ложь	Истина
А + В	Ложь	Истина	Истина	Ложь
⅂ А (= Истина + А)	Истина	Ложь	Истина	Ложь
А⇒ В	Истина	Ложь	Истина	Истина
$A \Leftrightarrow B$	Истина	Ложь	Ложь	Истина

Чтобы напомнить житейский смысл логических операций, попытайтесь оценить истинность следующих высказываний в зависимости от разных истинностных оценок компонент этих высказываний.

а. Не верно, что Васька – плут и мошенник.

б. Не верно, что Фигаро здесь или Фигаро там.

в. Ветер дует, потому (= из-за того), что деревья качаются.

г. Мы победим, либо все вместе погибнем.

д. Ты, и ты, и ты не можете сравниться с Матильдой моей.

В алгебре высказываний есть два «крайних»: 0 (= Ложь = False) и 1 (= Истина = True). Первое всегда верно, а второе всегда ложно. Пусть $F(A_1, \dots, A_n)$ – ложное высказывание, построенное из высказываний-переменных $A_1, \dots, A_{n,}$, а также «крайних» высказываний 0 и 1 путем многократного применения логических операций $\vee, \wedge, +, ⅂, \Rightarrow, \Leftrightarrow$. То-

гда, зная истинностную оценку переменных $A_1, \dots, A_n$, можно оценить и F, многократно пользуясь табл. 2.

Таблица 2

A	0	1	0	1
B	0	0	1	1
A ∨ B	0	1	1	1
$A \Rightarrow (A \vee B)$	1	1	1	1

Пример 1. Пусть $F(A, B)$ есть $A \Rightarrow (A \vee B)$.

Мы видим, что высказывание F равносильно 1.

Заметим, что множество $\mathrm{Boolean} = \{0,1\}$, называемое булеаном, образует подалгебру в алгебре высказываний. Это означает, что результат применения логических операций к элементам булеана есть снова элемент булеана. Тем самым табл. 1 можно упростить так (табл. 3).

Таблица 3

x	0	1	0	1
y	0	0	1	1
$x \vee y$	0	1	1	1
xy	0	0	0	1
$x + y$	0	1	1	0
$\bar{x}=1+x$	1	0	1	0
$x \Rightarrow y$	1	0	1	1
$x \Leftrightarrow y$	1	0	0	1

Предпоследняя строка таблицы определяется в соответствии с принципом «солгавши раз, да кто тебе поверит!». Если некто ложное утверждение объявляет истинным, и тем самым его собственное мировоззрение становится противоречивым, то далее он может объявлять, что угодно – в своих глазах он будет прав. Еще раз объясним импликацию на математическом языке: ложность посылки x влечет истинность импликации $x \Rightarrow y$ вне зависимости от y. В компьютерных языках операции импликации и эквивалентности используют крайне редко. Частично это объясняется тем, что высказывание $A \,\mathrm{Imp}\, B$ эквивалентно $(not\ A) or\ B$.

На битовые строки $\left\{ (\nu_1, \dots, \nu_n) \mid \text{все } \nu_j \in \{0,1\} \right\}$ логические операции распространяются покомпонентно:

$$(\nu_1, \dots, \nu_n) * (\mu_1, \dots, \mu_n) = (\nu_1 * \mu_1, \dots, \nu_n * \mu_n),$$
$$(\nu_1, \dots, \nu_n)^u = (\nu_1^u, \dots, \nu_n^u),$$

где $*$ – какая-либо бинарная операция, а $(\dots)^u$ – унарная операция (она у нас пока одна – отрицание, но все впереди).

Пример 2. Логические вычисления на строках длины 4 (полубайт):

$$(1100)\ \text{and}\ (0110) = (0100) \leftrightarrow 12\ and\ 6 = 4;$$

$$(1100)\ or\ (0110) = (1110) \leftrightarrow 12 or\ 6 = 14;$$

$$(1100)\ \text{xor}\ (0110) = (1010) \leftrightarrow 12\ xor\ 6 = 10;$$

$$not(1100) = (0011) \leftrightarrow not(12) = 3.$$

В среде VBA под True и False отводится два байта (16 бит), столько же, сколько и под тип целого числа Integer. При этом True представляется строкой из единиц (1, 1, …, 1), а False – строкой из нулей. Система представления целых чисел типа Integer такова, что первый бит указывает на знак числа (см. разд. 1) и строка из 16 единиц представляет целое число –1. Поэтому ничего удивительного нет в том, что на вопросы к VBA “True = – 1”; “True < False” он ответит утвердительно.

Для краткости обозначим булеан символом E, а множество бинарных строк длины n через E^n. Истинностная оценка упорядоченного набора высказываний $A_1, \dots, A_n$ есть строка $\boldsymbol{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n) \in E^n$. Таким образом, на сложное высказывание $F(A_1, \dots, A_n)$ можно смотреть как на отображение $E^n \to E$. Такое отображение называется булевой функцией n переменных. Совокупность всех булевых функций n переменных обозначим $\mathbb{L}_n$.

Теорема 1. Количество булевых функций n переменных равно 2^{2^n}.

Например, получаем $2^{2^2} = 16$ булевых функций двух переменных. Один из способов их перечисления следующий:

$$\mathbb{L}_2 = \left\{ \varepsilon_0 + \varepsilon_1 x + \varepsilon_2 y + \varepsilon_3 xy \mid \ \varepsilon_j \in E \right\}.$$

Таблица истинности высказывания F выглядит так же, как табл. 2, с той лишь разницей, что в случае n переменных у неё 2^n столбцов, кроме первого.

Две булевых функции n переменных эквивалентны или равны, если они совпадают как функции, т.е. имеют одинаковые булевы значения при подстановке любой строки $\boldsymbol{\varepsilon} \in E^n$ вместо переменных.

В примере 2 показано, что функция $A \Rightarrow (A \vee B)$ эквивалентна 1.

Приведение высказывания к эквивалентному, но более просто устроенному есть одна из важных задач в алгебре высказываний $\mathbb{L}_n$. Хорошо бы иметь некоторый класс высказываний $K \subseteq \mathbb{L}_n$, обладающий следующими свойствами:

- любая булева функция эквивалентна некоторой функции из K;
- если $F, F' \in K$ эквивалентны, то они совпадают как записи.

Опишем три таких класса.

6.1. Дизъюнктивная совершенная нормальная форма

Булевы переменные будем обозначать $x_1, \dots, x_n$. Строку булевых переменных обозначаем $\boldsymbol{x} = (x_1, \dots, x_n)$**.** Для $\varepsilon, x \in E$ обозначим

$$x^{\varepsilon} = \begin{cases} 1, & \text{если } x = \varepsilon, \\ 0, & \text{если } x \neq \varepsilon. \end{cases} \qquad (1)$$

Мы видим, что это просто другое обозначение операции эквивалентности. Если x, ε – булевы строки длины n, как и выше, то обозначим

$$\boldsymbol{x}^{\boldsymbol{\varepsilon}} = x_1^{\varepsilon_1} \cdot \dots \cdot x_n^{\varepsilon_n}. \qquad (2)$$

Для подмножества $B \subseteq E^n$ обозначим через χ_B ее характеристическую функцию $E^n \to E$, принимающую значение 1 на строках из B и 0 на строках из дополнения $E^n \backslash B$.

Лемма. $\boldsymbol{x}^{\boldsymbol{\varepsilon}} = \mathbf{1}$ тогда и только тогда, когда $\boldsymbol{x} = \boldsymbol{\varepsilon}$**.**

Теорема 2

А. Имеет место равенство

$$\chi_B = \bigvee_{\boldsymbol{\varepsilon} \in B} \boldsymbol{x}^{\boldsymbol{\varepsilon}}. \qquad (3)$$

В. Для любой булевой функции $F: E^n \to E$, не тождественно равной 0, обозначим через $B(F)$ множество $\{\boldsymbol{\varepsilon} \in E^n \mid F(\boldsymbol{\varepsilon}) = 1\}$. Тогда $F = \chi_{B(F)}$.

Представление функции F в виде (3) называется дизъюнктивной нормальной совершенной формой функции F (сокращенно ДСНФ). Заметим, что ДСНФ не всегда экономна. Например, обозначая операцию отрицания штрихом, будем иметь

$a'b'c' \vee a'bc' \vee a'b'c \vee a'bc \vee abc = a'c' \vee a'b'c \vee \ bc = a' \vee bc.$

Первое равенство объясняется так: $a'bc \vee abc = (a' \vee a)bc = 1bc = bc$. Второе можно проверить непосредственно, подставляя $a = 0{,}1$.

6.2. Конъюнктивная нормальная совершенная форма

Для булевой функции $F: E^n \to E$ обозначим

$$Z(F) = \{\, \varepsilon \in E^n \mid F(\neg\varepsilon) = 0 \,\}.$$

Теорема 3. Пусть F не тождественно равна 1. Тогда:

А. Имеет место равенство

$$F = \bigwedge_{\boldsymbol{\varepsilon} \in Z(F)} \left(x_1^{\varepsilon_1} \vee \ldots \vee x_n^{\varepsilon_n}\right). \qquad (4)$$

Б. Две различные формы вида (4) задают различные булевы функции.

Доказательство. А. Проверим, что F равна 0 тогда и только тогда, когда правая часть в (4) равна 0. Пусть $F(\boldsymbol{\tau}) = 0$ и тем самым $\boldsymbol{\nu} := \neg\boldsymbol{\tau} \in Z(F)$. Тогда для $\boldsymbol{\varepsilon} = \boldsymbol{\nu}$ выполняется равенство $\tau_1^{\varepsilon_1} \vee \ldots \vee \tau_n^{\varepsilon_n} = \tau_1^{\neg\tau_1} \vee \ldots \vee \tau_n^{\neg\tau_n} = = 0$, ибо каждая компонента равна 0. Следовательно, значение конъюнкции в (4) равно 0.

Наоборот, пусть значение правой части в (4) при $\boldsymbol{x} = \boldsymbol{\tau}$ равно 0. Это значит, что для некоторого $\boldsymbol{\varepsilon} \in Z(F)$ сомножитель $\tau_1^{\varepsilon_1} \vee \ldots \vee \tau_n^{\varepsilon_n}$ равен 0. Это может быть, только если $\varepsilon_j = \neg\tau_j$ для любого j. Тогда $\boldsymbol{\tau} = \neg\boldsymbol{\varepsilon}$ и $F(\boldsymbol{\tau}) = F(\neg\boldsymbol{\varepsilon}) = 0$ по определению множества $Z(F)$.

Б. Пусть две формы $\bigwedge_{\boldsymbol{\varepsilon} \in Z}(x_1^{\varepsilon_1} \vee \ldots \vee x_n^{\varepsilon_n})$ и $\bigwedge_{\boldsymbol{\varepsilon} \in Z'}(x_1^{\varepsilon_1} \vee \ldots \vee x_n^{\varepsilon_n})$ задают одинаковую булеву функцию. Первая форма принимает значение 0 только для строк $\boldsymbol{\tau}$ таких, что $\neg\boldsymbol{\tau} \in Z$, а вторая – для тех $\boldsymbol{\tau}$, что $\neg\boldsymbol{\tau} \in Z'$. Отсюда $\neg Z = \neg Z'$. Так как отображение $\boldsymbol{x} \to \neg\boldsymbol{x}$ – биекция на множестве строк, то $Z = Z'$.

По-другому можно рассуждать так: форм вида (4) столько же, сколько подмножеств в E^n, т.е. 2^{2^n}. Это число совпадает с множе-

ством различных булевых функций с n переменными. В силу утверждения А, если две формы вида (4) дают одинаковые функции, то получается, что число разных булевых функций будет строго меньше 2^{2^n}. Это противоречит теореме 1. □

Разложение (4) называют конъюнктивной нормальной совершенной формой.

6.3. Многочлены Жегалкина

Предложение

А. Эквивалентность $A \Leftrightarrow B$ равна булевой функции $(A \Rightarrow B) \times$ $\times (B \Rightarrow A)$.

Б. Импликация $A \Rightarrow B$ эквивалентна $\neg A \vee B$.

В. Дизъюнкция $A \vee B$ есть то же самое, что и $A + B + AB$.

Г. Отрицание $\neg A$ по-другому выражается как $1 + A$.

Проверить справедливость этих утверждений можно с помощью таблиц истинности.

Теорема 4

А. Любая булева функция n переменных может быть записана в виде

$$F = a_0 + \sum_{1 \le j \le n} a_j x_j + \sum_{1 \le j < k \le n} a_{jk} x_j x_k + \cdots + a_{12\ldots n} x_1 x_2 \ldots x_n, \quad (5)$$

где $a_j,\ a_{jk} \in E$.

Б. Количество слагаемых в суммах (5) суть биномиальные коэффициенты $C_n^0, C_n^1, C_n^2, \ldots, C_n^n$ (включая первое и последнее слагаемые).

В. Набор коэффициентов $a_{j\ldots k}$ (их $C_n^0, +C_n^1 + C_n^2 + \cdots + C_n^n = 2^n$ штук) однозначно определяется функцией F.

Доказательство. Учитываем, что $x^2 = x$ для булевой переменной x, а также учитываем предложение.

Множество булевых функций $\mathbb{L}_n$ относительно операций умножения, сложения, отрицания ($\mathrm{not}(x) = 1 + x$) назовем алгеброй Жегалкина.

Иван Иванович Жегалкин (22 июля 1869, г. Мценск, Российская империя – 28 марта 1947 г., Москва, СССР) – российский и советский математик и логик. Из его открытий наибольшую известность получил так называемый полином Жегалкина.

7. МАТРИЧНАЯ АЛГЕБРА

Матричная алгебра над кольцом R (R – кольцо целых чисел, поле рациональных чисел, поле вещественных чисел и т.п.) – наиболее широко используемая алгебраическая система с множеством операций как внутренних, так и внешних (сложение, умножение на элементы кольца R и умножение матрицы на матрицу, транспонирование, определитель, след, характеристический многочлен, собственные числа и т.д.). В любом языке программирования имеется возможность определять матрицы как двумерные массивы чисел. В VBA строка

$$\text{Dim M(2,2) as Long} \qquad (1)$$

задает массив-матрицу из трех строк и трех столбцов, компоненты которой – целые числа:

$$\begin{pmatrix} M(0,0) & M(0,1) & M(0,2) \\ M(1,0) & M(1,1) & M(1,2) \\ M(2,0) & M(2,1) & M(2,2) \end{pmatrix}.$$

Если мы хотим, чтобы нумерация компонент начиналась с единицы, а не с нуля, то вместо (1) надо записать

$$\text{Dim M (1 to 3, 1 to 3) as Long.} \qquad (2)$$

В математическом тексте матрицы записывают так: $A = (a_{ij}), 1 \leq \leq i \leq m, 1 \leq j \leq n$. Тем самым задана матрица, состоящая из m строк и n столбцов, (i, j)-й компонент которой, стоящий на пересечении i-й строки и j-го столбца, есть a_{ij}.

Матрица, у которой число строк и число столбцов совпадают, называется квадратной. Элементы $a_{11}, a_{22}, a_{33}, \ldots$ называются главной диагональю матрицы (a_{ij}). Единичная матрица E есть квадратная матрица, у которой на главной диагонали единицы, а остальные все коэффициенты нули.

Заметим, что две матрицы равны, если, во-первых, совпадают их размеры, а во-вторых, на одинаковых местах стоят равные друг другу числа. Матрицы

$$(a_{i1}, a_{i2}, \ldots, a_{in}); \quad \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

называются i-й строкой и j-м столбцом матрицы $A = (a_{ij})$.

Если $B = (b_{ij})$ – еще одна матрица того же размера $m \times n$, то

$$A + B = (a_{ij} + b_{ij}); \quad \lambda \cdot A = (\lambda a_{ij}). \tag{3}$$

Соотношение (3) определяет линейные операции над матрицами – сложение и умножение на элементы кольца R. Как видно из (3), сложение для матриц разных размеров не определено. Умножение матриц – более сложная операция. Чтобы понять это определение, лучше сначала обратиться к интерпретации матриц как линейных преобразований. Пусть

$$\begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}; \begin{pmatrix} c_1 & c_2 \\ d_1 & d_2 \end{pmatrix}$$

– две 2 × 2-матрицы. Они задают линейные преобразования пары переменных. Пусть первая матрица преобразует пару x_1, x_2 в пару y_1, y_2, а вторая матрица преобразует пару y_1, y_2 в пару z_1, z_2 по следующему правилу

$$\begin{cases} y_1 = a_1 x_1 + a_2 x_2 \\ y_2 = b_1 x_1 + b_2 x_2 \end{cases}; \quad \begin{cases} z_1 = c_1 y_1 + c_2 y_2 \\ z_2 = d_1 y_1 + d_2 y_2 \end{cases}.$$

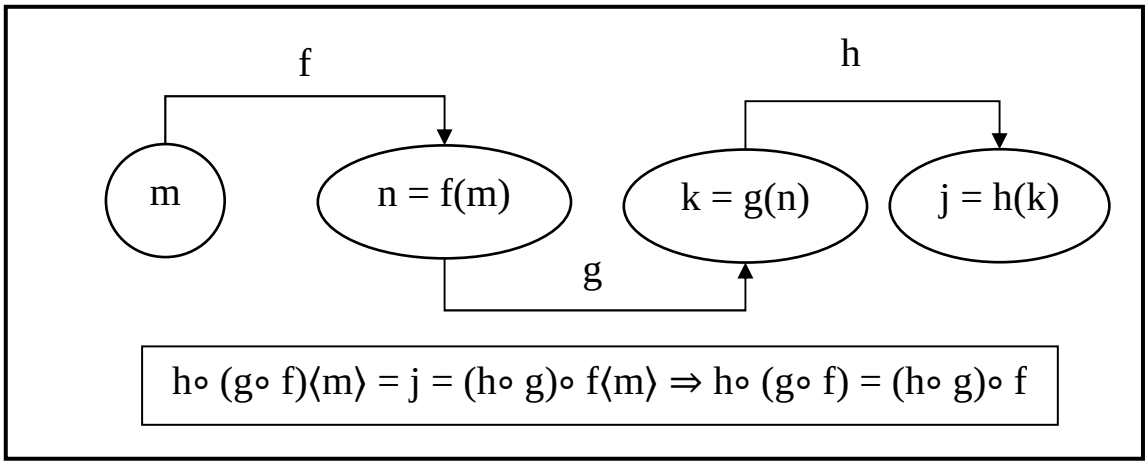
Подставим во второе соотношение вместо y_1, y_2 их линейные выражения через x_1, x_2:

$$\begin{cases} z_1 = (c_1 a_1 + c_2 b_1) x_1 + (c_1 a_2 + c_2 b_2) x_2 \\ z_2 = (d_1 a_1 + d_2 b_1) x_1 + (d_1 a_2 + d_2 b_2) x_2 \end{cases}.$$

Эта процедура называется композицией преобразований. В результате мы получили линейное преобразование, задающееся матрицей

$$\begin{pmatrix} c_1 & c_2 \\ d_1 & d_2 \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} := \begin{pmatrix} c_1 a_1 + c_2 b_1 & c_1 a_2 + c_2 b_2 \\ d_1 a_1 + d_2 b_1 & d_1 a_2 + d_2 b_2 \end{pmatrix}.$$

В произведении на месте (i, j) стоит скалярное произведение i-й строки первой матрицы на j-й столбец второй матрицы. Из интерпретации произведения матриц как последовательного выполнения преобразований немедленно вытекает ассоциативность произведения матриц (еще до формального определения произведения!), ибо композиция преобразований для любых множеств подчиняется ассоциативному закону. Доказательство этого факта смотри на диаграмме.



Формальное определение произведения матриц следующее. Произведение строки $(a_1, \dots, a_n)$ на столбец $(b_1, \dots, b_n)^\top$ определяется как число – матрица 1 × 1, равная $a_1b_1 + \dots + a_nb_n$. Произведением $m \times n$-матрицы $A = (a_{ij})$ на $n \times k$-матрицу $B = (b_{ij})$ называется $m \times k$-матрица $C = (c_{ij})$ такая, что

$$c_{ij} = a_{i1}b_{1j} + \cdots + a_{in}b_{nj} \qquad (4)$$

Единичная матрица – нейтральный элемент по отношению к произведению матриц, т.е. $E_mA = AE_n = A$ для любой $m \times n$-матрицы A.

Матрица называется нулевой, если все ее компоненты нули. Она играет роль нейтрального элемента по отношению к сложению (A + 0= = 0 + A = A) и поглощающего элемента по отношению к умножению (0 · A = 0).

Как уже сказано, произведение матриц ассоциативно, т.е. матричное равенство $(AB)C = A(BC)$ имеет место всякий раз, когда операции умножения определены. Кроме того, произведение дистрибутивно относительно сложения

$$A(B + C) = AB + AC;\ (B + C)D = BD + CD.$$

Следствие. Совокупность $n \times n$-матриц над кольцом R образует кольцо.

Обозначим это кольцо Mat ($n \times n$, R). Заметим, что это кольцо не коммутативно при $n > 1$, т.е. произведение матриц, как правило, зависит от порядка сомножителей. Мы уже имели дело с кольцом Mat (2 × 2, $\mathbb{Z}$) в разд. 4.

Транспонирование матрицы – операция над $m \times n$-матрицей A, превращающая ее в $n \times m$-матрицу $A^\top$, у которой $(i,\ j)$-й коэффици-

ент равен (j,i)-му коэффициенту матрицы A. Свойства операции транспонирования следующие:

T1. $(A+B)^{\top} = A^{\top} + B^{\top}$;

T2. $(rA)^{\top} = A^{\top} r$;

T3. Инволютивность операции транспонирования: $(A^{\top})^{\top} = A$.

Относительно транспонирования произведение матриц обладает следующим свойством антигомоморфности:

T4. $(A \cdot B)^{\top} = B^{\top} \cdot A^{\top}$.

Матрица A называется верхнетреугольной, если ниже главной диагонали матрицы A стоят нули. Аналогично A – нижнетреугольная матрица, если выше главной диагонали матрицы A стоят нули. Матрица A треугольная, если она либо верхнетреугольная, либо нижнетреугольная. Треугольная матрица с нулями на главной диагонали называется строго треугольной. Матрица называется диагональной, если вне главной диагонали стоят нули. Диагональную $n \times n$-матрицу обозначаем так: $\mathrm{diag}\,(a_1, \ldots, a_n)$. Заметим, что

$$\mathrm{diag}\,(a_1, \ldots, a_n) + \mathrm{diag}\,(b_1, \ldots, b_n) = \mathrm{diag}\,(a_1 + b_1, \ldots, a_n + b_n);$$

$$\mathrm{diag}\,(a_1, \ldots, a_n) \cdot \mathrm{diag}\,(b_1, \ldots, b_n) = \mathrm{diag}\,(a_1 \cdot b_1, \ldots, a_n \cdot b_n);$$

$$E = \mathrm{diag}\,(1, \ldots, 1).$$

Эти соотношения показывают, что множество диагональных матриц замкнуто относительно сложения и умножения, а также содержит нейтральный элемент умножения – единичную матрицу E. В этом случае в алгебре употребляется термин «подкольцо». Подкольцом будет также совокупность верхнетреугольных (нижнетреугольных) матриц.

Алгебра матриц содержит делители нуля, например

$$\mathrm{diag}\,(1,0) \cdot \mathrm{diag}\,(0,1) = 0,$$

а также нильпотентные элементы (которые в какой-либо степени обращаются в нулевой элемент):

$$\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}^3 = 0.$$

Над строками (столбцами) матрицы можно совершать элементарные преобразования трех типов.

1-й тип. Прибавление к строке (столбцу) другой строки (столбца), предварительно умноженной на какой-либо элемент кольца R.

2-й тип. Перестановка двух строк (столбцов).

3-й тип. Умножение строки (столбца) на обратимый элемент кольца R.

7.1. Определители

Определитель квадратной матрицы A есть ее числовая характеристика, обозначаемая $\det A$ или $|A|$. Начнем с определителей матриц малых размерностей 1, 2, 3:

$$\det a := a;\ \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc;$$

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} = a_1b_2c_3 + a_2b_3c_1 + a_3b_1c_2 - a_3b_2c_1 - a_1b_3c_2 - a_2b_1c_3. \quad (5)$$

Определение 1. Пусть $A = (a_{ij})$ – n×n-матрица ($n \geq 3$). Определителем матрицы A называется число, которое вычисляется по следующему правилу:

$$det\ A = \sum_{1 \leq j \leq n} (-1)^{j+1}\ a_{j1} \cdot M_{j1}, \quad (6)$$

где M_{j1} – определитель матицы, полученной из A вычеркиванием первого столбца и j-й строки.

Теорема 1. Определитель треугольной матрицы равен произведению элементов на главной диагонали. В частности, $\det E = 1$.

Доказательство – индукция по n с разложением по первому столбцу.

Перечислим свойства определителей (все они проверяются непосредственно для 2×2- и 3×3-матриц).

Свойство 1. Определитель матрицы равен определителю транспонированной матрицы.

Функция n переменных вида $f(\boldsymbol{x}) = B_1x_1 + B_2x_2 + \cdots + B_nx_n$ называется линейной. Она обладает свойством

$$f(\boldsymbol{x} + \boldsymbol{x}') = f(\boldsymbol{x}) + f(\boldsymbol{x}');\ f(\lambda\boldsymbol{x}) = \lambda f(\boldsymbol{x}). \quad (7)$$

Наоборот, любая функция n переменных, обладающая свойством (7), линейна. Здесь $\boldsymbol{x} = (x_1, \dots, x_n)$.

Свойство 2 (полилинейность). Определитель – линейная функция от каждой строки (каждого столбца) матрицы.

Свойство 3 (кососимметричность). Определитель меняет знак при перемене местами двух строк (двух столбцов).

Свойство 4. Определитель равен нулю, если какие-либо две строки (два столбца) совпадают.

Свойство 5. Определитель с нулевой строкой (столбцом) равен нулю.

Свойство 6. Определитель не изменится, если над строками совершить элементарное преобразование первого типа, т.е. к одной строке прибавить другую, умноженную на какое-либо число. То же верно и для столбцов.

Определение 2. (i, j)-м минором матрицы A называется определитель матрицы, получающейся из A вычеркиванием i-й строки и j-го столбца. Обозначаем этот минор M_{ij}. Алгебраическим дополнением (i, j)-го элемента матрицы A называется величина $A_{ij} = (-1)^{i+j} M_{ij}$.

Свойство 7. Разложение определителя по j-му столбцу и i-й строке:

$$det\ A = a_{1j}A_{1j} + a_{2j}A_{2j} + \cdots + a_{nj}A_{nj};$$
$$det\ A = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}.$$

Имеют место также ложные разложения по r-й строке и r-му столбцу; если $r \neq i$ и $r \neq j$, то

$$0 = a_{r1}A_{i1} + a_{r2}A_{i2} + \cdots + a_{rn}A_{in},$$
$$0 = a_{1r}A_{1j} + a_{2r}A_{2j} + \cdots + a_{nr}A_{nj}.$$

Теорема 2. Определитель произведения матриц равен произведению определителей: $\det(AB) = \det A \det B$ (для любых $n \times n$-матриц A и B).

7.2. Обратная матрица

Определение 3. $n \times n$-матрица D называется обратной к $n \times n$-матрице A, если $AD = DA = E$. Обратная матрица единственна и обозначается как A^{-1}.

Теорема 3. Обратная матрица к $n \times n$-матрице A существует тогда и только тогда, когда матрица A невырождена (т.е. $\det A \neq 0$). В этом случае

$$A^{-1} = \frac{1}{\det A}\left(A_{ij}\right)^{\top}, \qquad (8)$$

где A_{ij} – алгебраическое дополнение к (i, j)-му элементу матрицы A. В частности, для 2×2-матрицы

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

7.3. Линейные преобразования плоскости

Известно, что любое преобразование плоскости ϕ, сохраняющее расстояния, есть либо параллельный перенос T_a на вектор $\boldsymbol{a}$, либо поворот $R_{O,\alpha}$ вокруг точки O на угол α, либо симметрия относительно прямой S_ℓ, либо композиция двух из перечисленных преобразований. Если же наложить дополнительное условие неподвижности одной из точек (ее удобно взять в качестве начала координат – точки O), то ϕ может быть либо поворотом вокруг O, либо симметрией относительно прямой, проходящей через O. Как аналитически описать эти важнейшие геометрические преобразования? На помощь приходит матричная алгебра Mat (2 × 2, ℝ). Сопоставим точке P (x, y) на плоскости столбец координат $(x, y)^\top$. Тогда отображение

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

задает поворот на угол α . Отражение относительно оси Ox задается матрицей diag (1, –1). Давайте ослабим требование сохранения расстояний и будем следить лишь за сохранением углов. Такое преобразование может быть устроено весьма сложно, но мы ограничимся случаем линейных преобразований и, кроме того, полагаем, что начало координат остается на месте. Запишем такое преобразование в общем виде

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}. \qquad (9)$$

Из условия сохранения углов следует, что вектор $a\boldsymbol{i} + b\boldsymbol{j}$ перпендикулярен вектору $c\boldsymbol{i} + d\boldsymbol{j}$, т.е. $ac + bd = 0$. Тогда $(c, d) = t\,(-b, a)$ для некоторого числа t. Треугольник с вершинами O (0, 0); A (1, 0); B (0, 1) должен перейти в равнобедренный прямоугольный треугольник, значит длины векторов $a\boldsymbol{i} + b\boldsymbol{j}$, $c\boldsymbol{i} + d\boldsymbol{j}$ должны быть равны. Отсюда получаем $t = \pm 1$. Случай t = 1 дает матрицу $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, а случай $t = -1$ дает матрицу $\begin{pmatrix} a & b \\ b & -a \end{pmatrix}$, описывающую симметрию относительно прямой $y = \dfrac{b}{a+1}\,x$ (если $a = -1$, то относительно оси Oy). Что собой представляет преобразование, заданное первой матрицей? Для этого обозначим $r = \sqrt{a^2 + b^2}$ и найдем угол α такой, что $\cos\alpha = \dfrac{a}{r}$;

$\sin\alpha = -\frac{b}{r}$. Тогда первая матрица примет вид $r \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$. Такая матрица отвечает за композицию двух преобразований: поворот на угол α и гомотетия с коэффициентом r.

Рассмотрим подробнее совокупность всех матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, в том числе и с нулевыми a и b. Эта совокупность (обозначим ее C) замкнута относительно сложения и умножения:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ -b-b' & a+a' \end{pmatrix};$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ -b' & a' \end{pmatrix} = \begin{pmatrix} aa'-bb' & ab'+ba' \\ -(ab'+ba') & aa'-bb' \end{pmatrix} \qquad (10)$$

Кроме того, E ∈ C. Следовательно, C – подкольцо кольца матриц. Но более того, умножение в кольце C коммутативно, что сразу видно из (10). Если a и b одновременно не равны 0, то $\begin{vmatrix} a & b \\ -b & a \end{vmatrix} = a^2 + b^2 \neq 0$ и поэтому матрица $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ обратима, а обратная матрица

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

снова принадлежит C.

Следствие. Совокупность всех матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ (a,b∈ $\mathbb{R}$) образует поле.

Это одно из важнейших «классических» полей – поле комплексных чисел.

8. КОМПЛЕКСНЫЕ ЧИСЛА

В разд. 9 изучается лишь одно поле – поле комплексных чисел $\mathbb{C}$. С геометрической точки зрения оно представляет собой плоскость, а с алгебраической точки зрения в этом поле любой неконстантный полином разложим в произведение линейных множителей. В этом смысле поле комплексных чисел проще устроено, чем поле действительных чисел и тем более чем поле рациональных чисел. На базе этого поля строится теория функций комплексного переменного, ко-

торая богата своими приложениями к инженерным наукам. К полю комплексных чисел приводит, казалось бы, весьма частная задача – извлечение квадратного корня из –1. Если единицу трактовать как тождественное преобразование плоскости, то –1 будет поворотом плоскости на 180°. Ясно, что в этой ситуации корень из –1 есть поворот на 90°. Такой поворот описывается матрицей $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, квадрат которой равен –E (см. предыдущий раздел). В этих двух фразах изложена идея построения комплексной плоскости. Решив одно уравнение $z^2 = -1$, мы получаем принципиальную возможность решить любое полиномиальное уравнение (см. п. 8.7).

Определение. Полем комплексных чисел называется наименьшее расширение поля действительных чисел, содержащее корень уравнения $z^2 + 1 = 0$.

8.1. Конструкция поля комплексных чисел

Мы фактически уже построили поле комплексных чисел в предыдущем разделе. Из-за исключительной важности поля комплексных чисел приведем его непосредственную конструкцию. Рассмотрим пространство строк длины два над полем $\mathbb{R}$ с операциями покомпонентного сложения и умножения на действительные числа. Определим умножение двух строк $z_1 = (x_1, y_1)$ и $z_2 = (x_2, y_2)$ так:

$$z_1 z_2 = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1).$$

Теорема 1. Пространство строк длины два с определенным выше умножением есть поле комплексных чисел (обозначим его $\mathbb{C}$). В нем единичным элементом будет строка (1,0), а множество (1,0)$\mathbb{R}$ ={(x,0)} образует подполе поля $\mathbb{C}$, изоморфное поле действительных чисел (тем самым отображение x→ (x, 0) (x∈ $\mathbb{R}$) есть вложение $\mathbb{R}$ в $\mathbb{C}$). Строка $i := (0,1)$ (называемая далее комплексной единицей) будет корнем уравнения $z^2 + 1 = 0$.

Доказательство. Сопоставим паре $(x, y) \in \mathbb{C}$ матрицу $\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \in C$. Это отображение обозначим Ф и убедимся, что отображение Ф есть

изоморфизм алгебраической системы $\mathbb{C}$ на поле C. Это означает, что Ф – биективное отображение и

$$\Phi\,(z_1 + z_2) = \Phi\,(z_1) + \Phi\,(z_2);\ \Phi\,(z_1 \cdot z_2) = \Phi\,(z_1) \cdot \Phi\,(z_2)$$

для любых комплексных чисел z_1, z_2. Тем самым, нам нет нужды проверять аксиомы поля для $\mathbb{C}$ – они автоматически выполнены в силу изоморфизма Ф.

Отображение x→ (x,0) есть гомоморфное вложение поля действительных чисел в $\mathbb{C}$ и, более того, имеет место равенство

$$x(x', y') = (xx', xy') = (x, 0) \cdot\ (x', y')$$

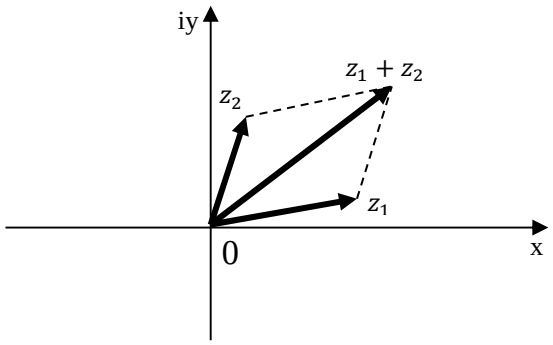
для любых $x, x', y' \in\ \mathbb{R}$. Теперь мы имеем возможность отождествить действительное число a и $(a, 0)$. Далее, равенство

$$i^2 = (0 + 1i)(0 + 1i) = (0 \cdot\ 0 - 1 \cdot\ 1) + (0 \cdot\ 1 + 1 \cdot\ 0)i = -1 + 0i = -1$$

показывает, что i есть корень уравнения $z^2 + 1 = 0$.

Вычислив обратную матрицу $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}^{-1}$ и учтя изоморфизм Ф, получаем

$$(x + iy)^{-1} = \frac{x}{x^2+y^2} - \frac{iy}{x^2+y^2}.$$



Комплексная плоскость

Любой элемент поля комплексных чисел единственным образом записывается в виде $z = x + + iy$, где x, y – действительные числа. Число x называется действительной частью комплексного числа z и обозначается Re z, а y называется мнимой частью комплексного числа z и обозначается Im z. Комплексное число z полностью определяется своей действительной и мнимой частью, т.е.

$$x + iy = x' + iy' \Leftrightarrow\ x = x' \text{ и } y = y'.$$

Комплексные числа вида iy называем чисто мнимыми. Комплексные числа изображаются точками на плоскости Oxy или векторами с начальной точкой в начале координат (см. рисунок). Горизонтальная ось Ox называется действительной осью, а вертикальная ось Oy – мнимой осью и обозначается как iy, ибо по ней откладываются чисто мнимые числа $\pm i, \pm 2i, \pm 3i$ и.т.д. При этом сложение двух комплекс-

ных чисел можно рассматривать как сложение двух векторов по правилу параллелограмма. Геометрическая интерпретация умножения будет указана позже.

8.2. Сопряжение комплексных чисел

Поле комплексных чисел доставляет нам новое свойство – наличие нетождественного непрерывного автоморфизма (изоморфизма на себя).

Комплексное число $\bar{z} = x - iy$ называется сопряженным к $z = x + iy$, а отображение $z \to \bar{z}$ – сопряжением. С геометрической точки зрения операция сопряжение есть не что иное, как отражение относительно действительной оси. Если реализовать поле комплексных чисел как подкольцо в алгебре матриц $Mat(2 \times 2, \mathbb{R})$, то сопряжение совпадает с транспонированием матрицы.

Равенство $z = \bar{z}$ имеет место тогда и только тогда, когда z – действительное число. Кроме этого сопряжение обладает свойством гомоморфности по отношению к сложению и умножению:

$$\overline{z_1 + z_2} = \bar{z_1} + \bar{z_2}, \ \ \overline{z_1 z_2} = \bar{z_1} \cdot \bar{z_2}.$$

Эти свойства проверяются непосредственно. Как и всякая симметрия, сопряжение обладает свойством инволютивности: $\bar{\bar{z}} = z$ для любого z.

Отметим также свойство $z \cdot \bar{z} = (x + iy)(x - iy) = x^2 + y^2$, которое приводит к следующему правилу деления комплексных чисел: для того чтобы разделить одно комплексное число на другое, надо числитель и знаменатель дроби умножить на величину, сопряженную знаменателю.

8.3. Тригонометрическая форма записи комплексных чисел

Изобразим комплексное число $z = x + iy$ вектором. Длина этого вектора, т.е. величина $\sqrt{x^2 + y^2}$, называется модулем комплексного числа z и обозначается $|z|$. Величину $\|z\| = x^2 + y^2 = z \cdot \bar{z}$ назовем нормой числа z, иногда удобнее пользоваться ею. Если $z = x$ – действительное число, то приходим к модулю действительного числа, ибо $\sqrt{x^2} = |x|$. Если $z \neq 0$, то угол, который образует вектор z с действительной осью, называется аргументом комплексного числа z и

обозначается $\arg z$. Пусть r и φ – модуль и аргумент ненулевого комплексного числа. Тогда

$$z = x + iy = r\cos\varphi + i\,r\sin\varphi = r(\cos\varphi + i\sin\varphi)\,. \qquad (1)$$

Выражение $r(\cos\varphi + i\sin\varphi)$ называется тригонометрической формой записи комплексного числа.

Теорема 2 (свойства модуля). Для любых комплексных чисел z_1, z_2 имеют место соотношения:

а) $|z_1 z_2| = |z_1||z_2|, \left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|}$;

б) $|z_1 + z_2| \le |z_1| + |z_2|$ (неравенство треугольника);

в) (непрерывность модуля) $|z_1 - z_2| \ge \big||z_1| - |z_2|\big|$.

Докажем первое равенство:

$$|z_1 z_2|^2 = (z_1 z_2)\overline{z_1 z_2} = z_1 z_2 \bar{z}_1 \bar{z}_2 = (z_1\bar{z}_1)(z_2\bar{z}_2) = |z_1|^2|z_2|^2.$$

Извлекая квадратный корень, получим равенство $|z_1 z_2| = |z_1||z_2|$. Второе равенство следует из первого, ибо оно эквивалентно следующему соотношению: $\left|\frac{z_1}{z_2}\right| \cdot |z_2| = \left|\frac{z_1}{z_2} \cdot z_2\right| = |z_1|$.

Неравенство треугольника следует из того, что сумма двух сторон треугольника больше третьей стороны либо равна ей, (см. рисунок). Равенство достигается, только если треугольник вырожден, т.е. представляет собой отрезок прямой. Свойство ,,в" следует из неравенства треугольника (сторона треугольника больше модуля разности двух других сторон).

Следствие. Множество комплексных чисел с единичным модулем (обозначим $\mathbb{S}$ – комплексная единичная окружность) замкнуто относительно умножения и обращения и образует подгруппу в мультипликативной группе поля $\mathbb{C}$.

Перемножим два комплексных числа в тригонометрической форме записи:

$$\begin{aligned}[r_1(\cos\varphi_1 + i\sin\varphi_1)][r_2(\cos\varphi_2 + i\sin\varphi_2)] &= \\ = r_1 r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 &+ \\ + i(\cos\varphi_1\sin\varphi_2 + \sin\ \varphi_1\cos\varphi_2).&\end{aligned}$$

Применяя тригонометрические формулы «косинус суммы» и «синус суммы», приходим к следующему правилу: при перемножении комплексных чисел модули умножаются, а аргументы складываются:

$$[r_1(\cos\varphi_1 + i\sin\varphi_1)][r_2(\cos\varphi_2 + i\sin\varphi_2)] = \\ = r_1r_2(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)). \quad (2)$$

В частности, перемножая число $\cos\varphi + i\sin\varphi$ на себя n раз, получаем **формулу Муавра:**

$$(\cos\varphi + i\sin\varphi)^{\boldsymbol{n}} = \cos n\varphi + i\sin n\varphi. \quad (3)$$

Умножая произвольное комплексное число-вектор z на комплексное число вида $\cos\varphi + i\sin\varphi$, увеличиваем аргумент у комплексного числа z на величину φ, не меняя модуля. Это преобразование соответствует повороту комплексной плоскости на угол φ. Умножение на положительное действительное число r есть гомотетия комплексной плоскости (растяжение в r раз, если $r > 1$, и сжатие в $\frac{1}{r}$ раз, если $r < 1$). Впрочем, мы это знали и ранее, имея в виду интерпретацию $\mathbb{C}$ матрицами 2×2. Итак, отображение

$$z \to z \cdot z_0,$$

где $z_0 = r(\cos\varphi + i\sin\varphi)$, представляет из себя последовательное выполнение двух геометрических преобразований над вектором z – поворота и гомотетии. В этом и заключается геометрический смысл умножения комплексных чисел.

Пример 1. Вычислим $(1+i)^{12}$. Для этого сначала найдем модуль и аргумент числа $1+i$:

$$|1+i| = \sqrt{1^2+1^2} = \sqrt{2}; \arg(1+i) = \pi/4.$$

Для того чтобы найти аргумент, изобразим комплексное число $1+i$ вектором, лежащим на биссектрисе первого квадранта, и ответ $\pi/4$, или по-другому 45^0, станет понятен. Далее

$$(1+i)^{12} = \left(\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)\right)^{12} = 2^6\left(\cos\frac{12\pi}{4} + i\sin\frac{12\pi}{4}\right) = \\ = 64(-1+0i) = -64.$$

8.4. Комплексная экспонента

Правило (2) дает нам право определить экспоненту чисто мнимого числа

$$e^{i\varphi} \coloneqq \cos\varphi + i\sin\varphi. \quad (4)$$

Действительно, таким образом определенная функция $e^{i\varphi}$ обладает следующими свойствами:

$$e^{i(\varphi+\psi)} = e^{i\varphi} \cdot e^{i\psi};\ \left(e^{i\varphi}\right)^n = e^{in\varphi};\ e^{i(\varphi+2\pi)} = e^{i\varphi}.$$

Здесь первое равенство есть частный случай (2), когда $r_1 = r_2 = 1$, второе равенство есть не что иное, как формула Муавра, а третье равенство вытекает из периодичности гармоник. Заметим, что никакой коллизии в обозначении в связи с известной экспонентой e^x действительной переменной не возникает; равенство аргументов $x = i\varphi$ возможно, лишь если $x = \varphi = 0$. Но тогда определение (4) комплексной экспоненты дает нам значение $1 + 0i = 1$, что совпадает с известным равенством $e^0 = 1$.

Определение (1) позволяет записать ненулевое комплексное число в показательной форме

$$z = re^{i\varphi}. \qquad (5)$$

В таком виде легче оперировать с комплексными числами, когда речь идет об умножении, делении и возведении в степень. Например,

$$\frac{3e^{\frac{\pi i}{5}} \cdot 6e^{\frac{\pi i}{3}}}{4e^{\frac{\pi i}{6}}} = \frac{9}{2}e^{\left(\frac{\pi}{5}+\frac{\pi}{3}-\frac{\pi}{6}\right)i} = 4.5e^{\frac{11\pi}{30}i}.$$

8.5. Извлечение корней из комплексных чисел

С помощью комплексной экспоненты легко извлекаются корни из комплексных чисел. Решим уравнение $z^n = w$. Если $w = 0$, то имеется только один нулевой корень кратности n. Пусть $w \neq 0$. Запишем его в показательном виде $w = r \cdot e^{i\varphi}$. Найдем арифметический корень n-й степени из r и обозначим его $\rho = \sqrt[n]{r}$. Тогда уравнение $z^n = w$ имеет n корней, расположенных на окружности радиуса ρ в вершинах правильного n-угольника

$$z_1 = \rho e^{i\frac{\varphi}{n}}, z_2 = \rho e^{i\frac{\varphi+2\pi}{n}}, z_3 = \rho e^{i\frac{\varphi+4\pi}{n}}, \ldots, z_n = \rho e^{i\frac{\varphi+2(n-1)\pi}{n}}.$$

8.6. Решение квадратных уравнений

Линейный многочлен $ax + b$ при $a \neq 0$ всегда имеет корень $-\frac{b}{a}$. Квадратный трехчлен уже не всегда имеет корни над полем действительных чисел.

Пусть $az^2 + bz + c$ – квадратный трехчлен над полем комплексных чисел ($a, b, c \in \mathbb{C}$ и $a \neq 0$). Обозначим через $\sqrt{D}$ какой-либо комплексный квадратный корень из дискриминанта $D = b^2 - 4ac$. Тогда

$$z_{1,2} = \frac{-b \pm \sqrt{D}}{2a} \qquad (6)$$

суть комплексные корни квадратного трехчлена. Действительно, уравнение $az^2 + bz + c = 0$ равносильно уравнению $\left(z + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$, откуда и следует формула (6).

Пример 2. Решим уравнение $z^2 + 6z + 13 = 0$:

$$z_{1,2} = \frac{-6 \pm \sqrt{6^2 - 4 \cdot 13}}{2} = \frac{-6 \pm 4i}{2} = -3 \pm 2i.$$

Заметим, что как и положено по теореме Виета, сумма корней равна -6, а произведение равно 13.

8.7. Основная теорема алгебры комплексных чисел

Поле называется алгебраически замкнутым, если любой многочлен над этим полем, не равный константе, имеет хотя бы один корень. Из теоремы Безу (см. п. «Алгебра многочленов») сразу следует, что над таким полем любой неконстантный многочлен разложим в произведение линейных множителей. В этом смысле алгебраически замкнутые поля устроены проще, чем не алгебраически замкнутые. Мы знаем, что над полем действительных чисел не всякий квадратный трехчлен имеет корень, тем самым поле $\mathbb{R}$ не является алгебраически замкнутым. Оказывается, ему чуть-чуть не хватает до алгебраической замкнутости. Другими словами: решив, казалось бы, частную задачу – уравнение $z^2 + 1 = 0$, мы одновременно справились со всеми остальными полиномиальными уравнениями.

Теорема 3 (основная теорема алгебры). Любой многочлен над полем $\mathbb{C}$, не равный константе, имеет хотя бы один комплексный корень.

Следствие. Любой многочлен, не равный константе, над полем комплексных чисел разложим в произведение линейных множителей

$$P(z) = a(z - z_1)^{k_1} \ldots (z - z_m).^{k_m}$$

Здесь $a \neq 0$ – старший коэффициент многочлена, $z_1, \ldots, z_m$ – все различные комплексные корни многочлена, $k_1, \ldots, k_m$ – их кратности.

Должно выполняться равенство

$$k_1 + k_2 + \cdots + k_m = \deg P.$$

Доказательство следствия представляет собой несложную индукцию по степени многочлена с применением теоремы Безу (см. разд. «Алгебра многочленов»).

9. АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

Алгебраическая система – это множество с семейством операций, заданным на нем. Операции должны удовлетворять некоторым аксиомам. Цели исследования алгебраической системы могут быть разными: а) получение результата применения операций к какому-либо элементу; б) ответы на качественные вопросы типа «Будет ли данная алгебраическая система удовлетворять интересующему нас тождеству?»; в) разложение данной системы на более простые алгебраические системы того же вида. Один из важнейших вопросов, касающийся двух алгебраических систем – одинаковы (т.е. изоморфны) они или нет.

9.1. Операции и отношения на множестве

Бинарной операцией на непустом множестве G называется правило, в силу которого паре элементов $a, b \in G$ сопоставляется третий элемент $c = a * b \in G$. Эта операция называется ассоциативной, если $a * (b * c) = (a * b) * c$ для любых $a, b, c \in G$. Операция * называется коммутативной, если $a * b = b * a$ для любых $a, b \in G$. Операция * называется идемпотентной, если $a * a = a$ для любого a.

Элемент $e \in G$ называется нейтральным относительно бинарной операции $*$, если $a * e = e * a = a$ для любого $a \in G$. Если e' – еще один нейтральный элемент, то $e * e' = e$, так как e' нейтрален, и $e * * e' = e'$, так как e нейтрален. Отсюда $e = e'$, чем доказана единственность нейтрального элемента.

Элемент $o \in G$ называется поглощающим относительно бинарной операции $*$, если $a * o = o * a = o$ для любого $a \in G$. Как и выше, можно доказать единственность поглощающего элемента.

В математике часто встречаются кроме бинарных операций унарные, тернарные и 0-арные операции. Для натурального числа n обо-

значим через G^n совокупность всех упорядоченных последовательностей $(g_1, \dots, g_n)$, где компоненты g_j пробегают множество G. Полагаем также по определению $G^0 = \{\emptyset\}$.

Определение 1. n-арной операцией на непустом множестве G называется отображение $G^n \to G$. 1-арная операция называется унарной, 2-арная – бинарной, 3-арная – тернарной. 0-арная операция, по сути, есть выделение некоторого элемента e в множестве G.

Иногда рассматриваются частичные операции, это тот случай, когда областью определения n-арной операции служит не все множество G^n, а лишь его собственное подмножество. Например, унарная операция – переход к обратному элементу в поле действительных чисел (как и в любом другом поле) – будет частичной операцией, поскольку обратного элемента для 0 не существует. Можно подсоединить символ ∞ к полю $\mathbb{R}$ и полагать $0^{-1} = \infty,\ \infty^{-1} = 0$, но тогда операция умножения становится частичной, так как произведение $0 \cdot \infty$ становится неопределенным.

Кроме операций на множестве могут быть заданы и отношения. Например, множество людей просто пронизано огромным числом отношений (А есть родитель Б; А есть начальник Б; А есть земляк Б и т.д. и.т.п.). Бинарное отношение $\mathcal{R}$ на множестве G есть правило, в силу которого по каждой паре g, h элементов из G мы можем узнать, находится ли g в отношении $\mathcal{R}$ к h или нет. Если g находится в отношении $\mathcal{R}$ с g, то говорим, что $g\mathcal{R}h$ верно, если нет, то говорим, что $g\mathcal{R}h$ не верно (и иногда обозначаем это, перечеркивая символ отношения $\mathcal{R}$). С точки зрения компьютерной алгебры удобно считать, что бинарное отношение – это отображение $r\colon G^2 \to \mathrm{Boolean}$, причем

$$g\mathcal{R}h \overset{\text{опр}}{\Leftrightarrow} r(g,h) = 1.$$

Важнейшие характеристики отношения таковы.

- Отношение $\mathcal{R}$ называется транзитивным, если из $g\mathcal{R}h$ и $h\mathcal{R}k$ вытекает $g\mathcal{R}k$.
- Отношение $\mathcal{R}$ называется симметричным, если $g\mathcal{R}h$ эквивалентно $h\mathcal{R}g$.
- Отношение $\mathcal{R}$ называется рефлексивным, если $g\mathcal{R}g$ для любого g.
- Отношение $\mathcal{R}$ называется антисимметричным, если из $g\mathcal{R}h$ и $h\mathcal{R}g$ вытекает $g = h$.

- Отношение $\mathcal{R}$ называется частичным порядком, если оно транзитивно, рефлексивно и антисимметрично. Если, кроме того, для любой пары $(g, h) \in G^2$ либо $g\mathcal{R}h$, либо $h\mathcal{R}g$, то $\mathcal{R}$ есть отношение линейного порядка.
- Отношение $\mathcal{R}$ называется отношением эквивалентности, если оно транзитивно, рефлексивно и симметрично.

В принципе встречаются и n-арные отношения как отображения $G^n \to \text{Boolean}$. Унарное отношение есть не что иное, как проверка какого-либо определения на множестве G. Например, унарное отношение IsPrime на множестве натуральных чисел проверяет, будет ли простым данное натуральное число. Отношения других арностей нам не встретятся в дальнейшем.

Теорема 1 (об отношении эквивалентности). Пусть "$\sim$" – отношение эквивалентности на множестве M. Для элемента $m \in M$ обозначим через $[m] = \{n \in M \mid m \sim n\}$ и назовем это множество классом эквивалентности. Тогда множество M разбивается в объединение классов эквивалентности

$$M = \bigcup_{m \in M} [m],$$

т.е. каждый элемент из M принадлежит ровно одному классу эквивалентности.

Наоборот, если $M = \bigcup_{i \in I} M_i$ есть разбиение, то отношение

$$m \sim n \Leftrightarrow \exists\, i \in I : m, n \in M_i \qquad (*)$$

есть отношение эквивалентности.

Доказательство. В силу рефлексивности $m \in [m]$, и поэтому множество M равно объединению всех классов эквивалентности. Если два класса эквивалентности $[m], [n]$ имеют общий элемент k, то для любого $m' \in [m]$ можно записать цепочку эквивалентностей $n \sim k \sim m \sim m'$ (во второй эквивалентности использована симметричность). Отсюда в силу транзитивности $n \sim m'$. Доказано включение $[m] \subseteq [n]$. Ввиду симметрии обратное включение также имеет место. Следовательно, получаем равенство $[m] = [n]$.

Докажем второе утверждение. Рефлексивность и симметричность отношения (*) ясны. Докажем транзитивность. Пусть $m \sim n$ и $n \sim k$. Это значит, что $m, n \in M_i$ и $n, k \in M_j$ для некоторых индексов i и j.

Тогда n – общий элемент подмножеств M_i, M_j. По определению разбиения получим $i = j$ и тем самым $m, k \in M_i$. Следовательно, $m \sim k$.

В алгебре обычно изучается непустое множество G с набором операций разной арности, заданными на нем и определенными отношениями типа тождества между операциями (например, ассоциативность и/или коммутативность бинарной операции).

Определение 2. Непустое множество G с набором операций $(\sigma_1, \dots, \sigma_t)$, удовлетворяющим заданным тождествам, называется алгебраической системой; сам набор операций $(\sigma_1, \dots, \sigma_t)$ вместе с их арностями называется сигнатурой алгебраической системы, а тождества называются аксиомами этой системы. Множество G называется носителем системы. Если в сигнатуру кроме операций входят также и отношения, связанные с операциями своими аксиомами, то G называют алгебраической моделью.

Пример. Приведем примеры различных алгебраических моделей без учета аксиом.

а. $\mathbb{N}(+, \cdot, 1, \leq)$ – множество натуральных чисел с двумя бинарными операциями сложения и умножения, одной 0-арной (единица) и отношением линейного порядка.

б. $\mathbb{Z}(+, \cdot, -, 0, 1, \leq)$ – кольцо целых чисел.

в. $\mathbb{Q}(+, \cdot, -, (..)^{-1}, 0, 1, \leq)$ – поле рациональных чисел; поле действительных чисел $\mathbb{R}$ с той же сигнатурой. Заметим, что унарная операция $(..)^{-1}$ частична.

г. $\mathbb{C}(+, \cdot, -, (..)^{-1}, 0, 1)$ – поле комплексных чисел.

д. $\{0,1\}(\vee, \wedge, +, \cdot, \Rightarrow, \Leftrightarrow, \neg)$ – булеан. Заметим, что на множестве из n элементов можно задать $(n^2)^n = n^{2n}$ бинарных операций. Для булеана это число равно 16. Шесть из них указаны в сигнатуре булеана. Операция отрицания $\neg$ унарна.

е. Алгебра высказываний $\mathbb{L}_n$, т.е. алгебра булевых функций n переменных относительно логических операций $\vee, +, \cdot, \neg, \Rightarrow, \Leftrightarrow$.

ж. Множество Неделя = {пн., вт., ср., чт., пт., сб., вс.} образует алгебраическую систему относительно унарных операций – «Следующий день», «Предыдущий день», имеющих очевидный смысл.

з. Фиксируем натуральное число n. Рассмотрим множество $\mathbb{Z}_n = = \{0,1, \dots, n-1\}$ остатков от деления целых чисел на n. На этом

множестве определим операции сложения и умножения, а именно, это последовательное выполнение обычных операций, а затем переход к остатку от деления на n. Получаем так называемое кольцо вычетов по модулю n. Обозначим его $\mathbb{Z}_n$.

и. Обозначим через S_n совокупность всех биекций множества натуральных чисел $\{1,2,\dots,n\}$ на себя. Рассмотрим бинарную операцию – последовательное выполнение биекций (т.е. если $\tau,\nu \in S_n$ то $\tau \circ \nu(i) := \tau\big(\nu(i)\big)$). Получаем симметрическую группу подстановок (см. п. «Группа подстановок»).

к. Пусть $\mathcal{A}$ – конечное множество, которое мы назовем алфавитом. Рассмотрим множество всех слов над этим алфавитом. Подсоединим к нему и пустое слово, не содержащее ни одной буквы. В качестве бинарной операции рассмотрим конкатенацию – приписывание к одному слову другого. Получаем свободный ассоциативный моноид с множеством порождающих $\mathcal{A}$.

л. Совокупность всех матриц над полем рациональных (действительных, комплексных) чисел образует сложнейшую алгебраическую систему относительно сложения и умножения. В данном случае это частичные операции, однако они будут всюду определены на алгебре квадратных матриц фиксированного размера.

Определим следующие алгебраические системы: полугруппы, моноиды, группы, кольца, поля, тела.

9.2. Моноиды

Непустое множество, рассматриваемое вместе с ассоциативной бинарной операцией, называется *полугруппой*. Полугруппа с нейтральным элементом называется *моноидом*. Более точно: алгебраическая система $G(*, e)$, где * – ассоциативная бинарная операция, а $e \in G$ – выделенный элемент (0-арная операция), который нейтрален относительно *, называется моноидом.

Приведем примеры. 1). $\mathbb{N}(+)$ – множество натуральных чисел со сложением. Эта полугруппа будет коммутативной, ибо сложение – коммутативная операция. Однако эта полугруппа не будет моноидом, так как в $\mathbb{N}$ нет нейтрального элемента относительно сложения. В связи с этим образуем моноид $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. 2). $\mathbb{N}(\cdot, 1)$ – моноид натуральных чисел относительно умножения. Он порожден совокупно-

стью простых чисел. 3). Множество всех целочисленных матриц второго порядка $\mathrm{Mat}(2\times 2;\mathbb{Z})$ относительно умножения будет некоммутативным моноидом, и в нем нулевая матрица будет поглощающим элементом. 4). То же самое множество $\mathrm{Mat}(2\times 2;\mathbb{Z})$ относительно сложения будет не только моноидом (нейтральный элемент – нулевая матрица), но и абелевой группой (см. далее).

В моноиде G элемент a' называется обратным (противоположным в случае, когда операция – сложение) к элементу $a\in G$, если $a*a'=$ $=e=a'*a$. Обратный элемент, если он существует, единственен. Действительно, предположив существование еще одного обратного элемента a'' к элементу a, будем иметь

$$a'=e*a'=(a''*a)*a'=a''*(a*a')=a''*e=a''.$$

Если a' обратен к a, то a обратен к a'. Это свойство сразу следует из определения обратного элемента. Если a' обратен к a, а b' обратен к b, то $b'*a'$ обратен к $a*b$. Проверка:

$$(a*b)*(b'*a')=\big((a*b)*b'\big)*a'=\big(a*(b*b')\big)*a'=$$
$$=(a*e)*a'=a*a'=e.$$

Здесь в первых двух равенствах применена ассоциативность операции *. Аналогично доказывается, что $(b'*a')*(a*b)=e$.

Заметим, что нейтральный элемент всегда обратим и обратным к нему служит сам он. Назовем элемент u моноида инволюцией, если $u*u=e$. Например, в моноиде квадратных матриц относительно умножения диагональные матрицы с элементами 0, ± 1 будут все инволюциями. В группе движений плоскости инволюциями будут отражения относительно прямой, а также повороты на 180°.

9.3. Группы

Группа – это моноид, в котором каждый элемент обратим. Более точное определение таково: алгебраическая система $G(*,(..)^{-1},e)$, где * – бинарная, $(..)^{-1}$ – унарная и $e\in G$ – 0-арная операции, называется группой, если выполнены следующие аксиомы:

Г1. $a*(b*c)=(a*b)*c$ (ассоциативность);

Г2. $e*a=a*e=a$ для любого $a\in G$ (нейтральность e);

Г3. $a*a^{-1}=a^{-1}*a=e$ (обратимость любого элемента).

Если операция $*$ к тому же и коммутативна, т.е. выполнена аксиома
Г4. $a * b = b * a$,
то группа G называется абелевой. В этом случае операция $*$ часто обозначается плюсом и называется сложением.

В группе уравнение $x * g = h$ так же, как и уравнение $g * x = h$, всегда имеют решения, а именно, первое уравнение имеет корень $x_1 = h * g^{-1}$, а второе – $x_2 = g^{-1} * h$, и эти корни не обязаны совпадать.

9.4. Кольца

Множество R с двумя бинарными операциями сложения и умножения, унарной операцией $a \to -a$ перехода к противоположному элементу, 0-арной операцией $0 \in R$ называется кольцом, если

К1. $R(+,-,0)$ является абелевой группой;

К2. $R(\cdot)$ – полугруппа;

К3. Умножение дистрибутивно относительно сложения:

$$a(b+c) = ab + ac \text{ и } (b+c)a = ba + ca.$$

Если дополнительно операция умножения коммутативна, т.е. выполняется аксиома
К4. $ab = ba$,
то R называется коммутативным кольцом. Если же дополнительно имеется единица – нейтральный элемент относительно умножения, то R называется кольцом с единицей.

Кольцо, в котором выполняется тождество
К5. $a^2 = a$,
называется булевым. Оно автоматически будет коммутативным, и в нем $a + a = 0$ для любого a. Пример булева кольца доставляет алгебра Жегалкина.

Примеры. 1). Множество, состоящее из одного нуля, является (нулевым) кольцом. 2). Кольцо целых чисел $\mathbb{Z}$ коммутативно и с единицей. 3). Все четные числа $2\mathbb{Z}$ образуют коммутативное кольцо, но уже без единицы. 4). Все десятичные рациональные дроби $\frac{m}{10^k}$ (m ∈ $\mathbb{Z}$,k ∈ $\mathbb{N}$_0) образуют коммутативное кольцо с единицей. 5). Множество квадратных $n \times n$-матриц с элементами из какого-либо кольца R (обозначение Mat ($n \times n$; R)) будет кольцом. Если R имеет единицу 1, то и Mat ($n \times n$; R) имеет единичную матрицу – E = diag (1, … ,1).

9.5. Поля и тела

Ненулевое кольцо, в котором каждый ненулевой элемент обратим, называется телом. Коммутативное тело называется полем. Более точно: алгебраическая система F с сигнатурой $(+,\cdot,-,(..)^{-1},0,1)$, где "+,·" – бинарные операции, $-,(..)^{-1}$ – унарные операции, причем вторая из них частичная, 0 и 1 – 0-арные операции, называется полем, если выполнены следующие аксиомы:

П1. (ассоциативность) $a(bc)=(ab)c;\ a+(b+c)=(a+b)+c;$

П2. (коммутативность) $ab=ba;\ \ a+b=b+a;$

П3. (дистрибутивность) $a(b+c)=ab+ac;$

П4. (нейтральность) $a+0=a;\ \ a\cdot 1=a;$

П5. $a+(-a)=0$; если $a\neq 0$, то $a\cdot a^{-1}=1;$

П6. $0\neq 1.$

Известны «классические» поля рациональных, действительных и комплексных чисел. Другие примеры полей, так же, как и пример тела, появятся позже.

9.6. Подсистемы алгебраических систем

Непустое подмножество H алгебраической системы G называется подсистемой, если оно замкнуто относительно всех операций, входящих в сигнатуру системы. Тем самым H можно рассматривать как алгебраическую систему с той же самой сигнатурой.

Если алгебраическая система имеет специальное название (моноид, группа, кольцо, поле), то название подсистемы получается прибавлением приставки «под» к этому названию: подмоноид, подгруппа, подкольцо, подполе.

Например, $\mathbb{Q}$ есть подполе поля $\mathbb{R}$. В этом случае говорят, что большее поле есть расширение меньшего.

Верхнетреугольные матрицы, так же, как и нижнетреугольные, составляют подкольцо в кольце Mat ($n \times n$; R). Вообще в алгебре матриц очень много подколец. Пусть $A \in \mathrm{Mat}(n \times n;\ \mathrm{K})$ (K – поле). Обозначим

$$K[A]=\{P(A)\mid P(x)-\text{многочлен над } K\}$$

– алгебру, порожденную над K матрицей A. Свойства этой алгебры отражают свойства матрицы A. В частности, унитарный многочлен наименьшей степени $Q(x)$ с коэффициентами из поля K такой, что $Q(A)=0$ называется минимальным многочленом матрицы A, и его степень совпадает с размерностью K[A] как линейного пространства над K.

В группе невырожденных $n \times n$-матриц над полем (или кольцом) К (обозначается GL (n, K) и называется общей линейной группой) также много подгрупп: 1). SL (n, K) – группа $n \times n$-матриц с единичным определителем, называемая специальной линейной группой. 2). UT (n, K) – группа верхнетреугольных матриц с единицами на главной диагонали. 3). Diag (n, K) – группа невырожденных диагональных матриц.

9.7. Декартово произведение алгебраических систем

Пусть $G_1, \dots, G_n$ – алгебраические системы с одной и той же сигнатурой. Определим на декартовом произведении $G_1 \times \dots \times G_n$ операции из этой сигнатуры покомпонентно:

$$(a_1, \dots, a_n) * (b_1, \dots, b_n) = (a_1 * b_1, \dots, a_n * b_n);$$
$$(a_1, \dots, a_n)^u = (a_1^u, \dots, a_n^u).$$

Получаем алгебраическую систему того же класса.

Часто употребляют эту конструкцию, когда все G_j – одна и та же алгебраическая система G. Тогда $G_1 \times \dots \times G_n$ обозначают G^n и называют декартовой степенью.

9.8. Фактор системы

Пусть ~ – отношение эквивалентности на алгебраической системе G. Скажем, что оно согласовано с операциями этой системы, если

$$a \sim a' \text{ и } b \sim b' \Rightarrow a * b \sim a' * b', \qquad a^u \sim (a')^u$$

для любой бинарной операции $*$ и любой унарной операции $(..)^u$. Аналогично определяется согласованность отношения ~ с любой n-арной операцией. Обозначим через $G/\sim$ множество классов эквивалентности. Определим на этом множестве те же самые операции:

$$[a] * [b] = [a * b]; \quad [a]^u := [a^u].$$

Эти определения корректны, т.е. результат в правой части не зависит от представителей классов эквивалентности в левой части.

Полученная таким образом алгебраическая система называется фактор-системой.

Если алгебраическая система имеет специальное название (моноид, группа, кольцо), то название фактор-системы получается прибавлением слова «фактор» к этому названию (фактор-моноид, фактор-группа, фактор-кольцо).

Выше мы уже отмечали одну фактор-систему, точнее, фактор-кольцо $\mathbb{Z}_n$ кольца целых чисел (пример «к» в п. 9.1). Отношение эквивалентности в этом случае задается так: $k \sim m \Leftrightarrow k \bmod n = m \bmod n$. Из свойств делимости вытекает его согласованность с операциями сложения и умножения.

9.9. Изоморфизм алгебраических систем

Пусть $G(*), G'(\circ)$ – две алгебраические системы с одной бинарной операцией, а $\phi: G \to G'$ – отображение. Отображение ϕ называется гомоморфным относительно пары бинарных операций $(*, \circ)$, если

$$\phi(a * b) = \phi(a) \circ \phi(b)$$

для любых $a, b \in G$. Аналогично определяется гомоморфность относительно пары унарных операций $((..)^u, (..)^v)$:

$$\phi(a^u) = \big(\phi(a)\big)^v.$$

Гомоморфность относительно пары 0-арных операций $e \in G, e' \in G'$ означает просто, что $\phi(e) = e'$.

Если G, G' – алгебраические системы с одной и той же сигнатурой, то отображение $\phi: G \to G'$ называется гомоморфизмом, если оно гомоморфно относительно всех пар соответствующих операций, входящих в сигнатуру этих систем. Если ϕ, кроме того, сюръективно, то оно называется эпиморфизмом. Инъективный гомоморфизм называется мономорфизмом. В том случае, когда ϕ одновременно есть мономорфизм и эпиморфизм и тем самым ϕ – биекция, то ϕ называется изоморфизмом. Изоморфизм алгебраической системы на себя называется автоморфизмом. Таковым, например, будет тождественное отображение $Id: G \to G$.

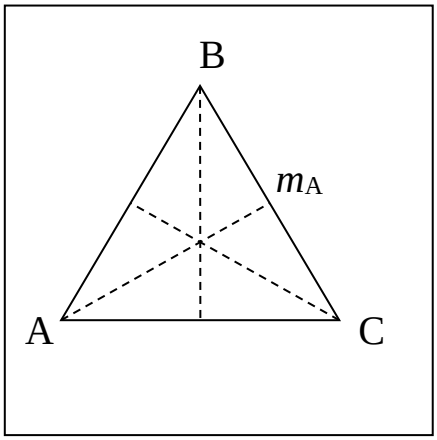
Если существует изоморфизм между алгебраическими системами, то такие системы называются изоморфными, и они в этом случае неразличимы с точки зрения алгебры. Класс всех алгебраических систем фиксированной сигнатуры распадается на классы изоморфных между собой систем, ибо изоморфизм есть отношение эквивалентности.

Пример. Группы $\mathbb{R}^+(\cdot)$ и $\mathbb{R}(+)$ изоморфны. Изоморфизм задается хорошо известным отображением $y = \ln x$, обратный к которому будет $x = e^y$. Ранее мы рассматривали две различные реализации поля комплексных чисел: одну – матрицами вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, где $a, b \in \mathbb{R}$, а другую – парами (a, b) действительных чисел. Это будут изоморфные копии одного и того же поля комплексных чисел.

10. ГРУППЫ

Группы исторические появились как семейства преобразований множества, удовлетворяющие следующим положениям: 1) вместе с любыми двумя преобразованиями в это семейство входит и их композиция, т.е. последовательное выполнение данных преобразований; 2) любое преобразование из этого семейства биективно, и обратная биекция также принадлежит семейству; 3) тождественное преобразование обязательно входит в любую группу преобразований.

Заметим, что в этом случае фундаментальный алгебраический закон ассоциативности автоматически выполняется (см. диаграмму в разд. «Матричная алгебра»). Таким условиям удовлетворяет, например, совокупность всех движений евклидовой плоскости, оставляющих данный равносторонний треугольник ABC на месте (см. рисунок). Обозначим эту совокупность движений Sym(Δ) и назовем ее группой симметрий треугольника. В этой группе шесть элементов – тождественное преобразование Id, два вращения R_{120}, R_{240} на углы 120° и 240° относительно центра O треугольника и три симметрии S_A, S_B, S_C относительно медиан этого треугольника. Имеют место равенства



$$S_A^2 = R_{120}^3 = Id,\ R_{120}^2 = R_{240},\ S_A \circ R_{120} = S_C,\ R_{120} \circ S_A = S_B.$$

В частности, из этих равенств следует, что в группа Sym(Δ) не абелева. Обратным преобразованием к симметрии является эта же симметрия, обратное преобразование к повороту на 120° есть поворот на 240°, и наоборот.

Другой пример группы преобразований множества – совокупность всех биекций конечного множества из *n* элементов на себя. Получается так называемая группа подстановок, которая отдельно изучается.

Примеры абелевых числовых групп. 1. Единичная группа {1} относительно умножения или нулевая группа {0} относительно сложения. 2. Группа ($\mathbb{Z}$,+) целых чисел по сложению. 3. Группа положительных рациональных $\mathbb{Q}^+$ (действительных $\mathbb{R}^+$) чисел по умножению. 4. Группа всех ненулевых рациональных $\mathbb{Q}^*$ (действительных $\mathbb{R}^*$) чисел по умножению. 5. Группа знаков {± 1} по умножению.

Подмножество H группы G будет подгруппой, если оно содержит нейтральный элемент e и вместе с каждыми двумя элементами $a, b \in H$ содержит ab и a^{-1}. Например, подмножество положительных действительных чисел $\mathbb{R}^+$ будет подгруппой в мультипликативной группе $\mathbb{R}^*$. Подгруппа есть сама по себе группа относительно индуцированного закона умножения. Множество, состоящее из одного нейтрального элемента, а также вся группа заведомо будут подгруппами; остальные подгруппы называются собственными.

Если фиксировать элемент g группы G и рассмотреть все его степени $\{ g^m \mid m \in \mathbb{Z} \}$, то это множество образует подгруппу в силу свойств и определений

$$g^{n+m} = g^n * g^m;\ g^0 := e;\ g^{-n} := (g^{-1})^n \text{ (здесь } n \in \mathbb{N}).$$

Она обозначается $gr\langle g\rangle$ и называется циклической подгруппой, порожденной элементом g. Если G = gr$\langle g\rangle$, то группа G целиком состоит из степеней элемента g. Тогда группа G называется циклической.

Пример 1. Обозначим через U семейство всех поворотов декартовой плоскости относительно начала координат. Относительно композиции U будет абелевой группой. Поворот на угол α обозначим R_α. Рассмотрим поворот на 90° и порожденную им подгруппу: $R_{180} = R_{90}^2,\ R_{270} = R_{90}^3, Id = R_{360} = R_{90}^4$. Она содержит четыре элемента. В этом случае будем говорить, что элемент R_{90} имеет порядок четыре. Итак, $G = \{Id,\ R_{90},\ R_{180},\ R_{270}\}$ есть циклическая группа из четырех элементов (по-другому – порядка четыре) относительно последовательного выполнения поворотов. Если вместо 90° взять угол в один радиан, то $R_{1rad}^m \neq Id$ для любого натурального, а значит, и для любого целого числа m. Это неравенство вытекает из иррациональности числа π. Получаем бесконечную циклическую группу gr $\langle R_{1rad}\rangle$. Бесконечной циклической группой будет и группа целых чисел по сложению, в ней вместо степеней g^m мы пишем $mg := g + g + \cdots + g$ (m раз). Группа ($\mathbb{Z}$, +) порождается как элементом 1, так и элементом –1; другие ненулевые элементы порождают собственные подгруппы.

11. АБЕЛЕВЫ ГРУППЫ

Теорема 1. Подгруппа циклической группы циклична.

Доказательство. Пусть $G = gr\langle\alpha\rangle$ – циклическая группа порядка N ($N \in \mathbb{N} \cup \{+\infty\}$ и H – ее подгруппа. Рассмотрим отображение $\Pi: \mathbb{Z} \to G$ переводящее целое число m в степень α^m. Проверим, что прообраз, $\Pi^{-1}(H)$, есть подгруппа в аддитивной группе целых чисел. Если $\Pi^{-1}(H) = \{0\}$, то $H = \{e_G\} = gr\langle e_G\rangle$ – циклическая (единичная) подгруппа. Иначе, рассмотрим наименьшее натуральное число n, принадлежащее $\Pi^{-1}(H)$. Ясно, что $n\mathbb{Z} \subseteq \Pi^{-1}(H)$. Докажем обратное включение. Пусть $m \in \Pi^{-1}(H)$. Поделим m на n с остатком: $m = nq + r, 0 \le r < n$. Тогда $r = m - nr \in \Pi^{-1}(H)$. В силу минимальности n должно выполняться равенство $r = 0$, тем самым $m = nq \in n\,\mathbb{Z}$. Следовательно, равенство $n\mathbb{Z} = \Pi^{-1}(H)$ доказано. Тогда $H = \mathrm{gr}\,\langle\Pi(n)\rangle$ – циклическая группа.

Следствие. Все подгруппы аддитивной группы целых чисел имеют вид $n\mathbb{Z}$, где $n = 0,1,2, \ldots$

Определение 1. Группа $(G,\cdot)$ называется конечно порожденной, если существует конечный набор элементов $g_1, \ldots, g_n \in G$, называемый порождающими элементами, который порождает группу G. Это значит, что всякий элемент $h \in G$ представим в виде $h = b_1 \cdot b_2 \cdot \ldots \cdot b_m$, где каждый из b_j либо порождающий элемент, либо обратен к порождающему элементу. Для абелевой группы $A(+)$ набор $\boldsymbol{a_1}, \ldots \boldsymbol{a_n}$ будет порождающим, если и только если выполняется равенство

$$A = \boldsymbol{a_1}\mathbb{Z} + \cdots + \boldsymbol{a_n}\mathbb{Z}. \qquad (1)$$

Далее мы будем иметь дело с группой целочисленных строк фиксированной длины n:

$$\mathbb{Z}^n = \{\,(z_1, \ldots, z_n) \mid z_j \in \mathbb{Z}\,\}. \qquad (2)$$

Заметим, что она порождается элементами

$$\boldsymbol{e_1} = (1,0, \ldots,0); \boldsymbol{e_2} = (0,1,0, \ldots,0); \ldots; \boldsymbol{e_n} = (0,0, \ldots,1), \qquad (3)$$

набор которых называется стандартным базисом. Вообще же элементы $\boldsymbol{b_1}, \ldots, \boldsymbol{b_n}$ называются базисом абелевой группы, если любая другая строка $\boldsymbol{d} \in \mathbb{Z}^n$ может быть единственным образом записана в виде $\boldsymbol{d} = \boldsymbol{b_1}z_1 + \cdots + \boldsymbol{b_n}z_n$ для некоторых целых z_j-х.

Теорема 2. Строки $\boldsymbol{b_j} = (b_{j1}, \dots, b_{jn}) \in \mathbb{Z}^n,\ 1 \le j \le m$ образуют базис в группе $\mathbb{Z}^n$ тогда и только тогда, когда $m = n$ и $\det(b_{ji}) = \pm 1$.

Доказательство. Если строки $\boldsymbol{b_j}$ образуют базис в $\mathbb{Z}^n$, то они же образуют базис линейного пространства $\mathbb{Q}^n$. Потому $m = n$. Далее выразим каждую строку стандартного базиса через $\boldsymbol{b_j}$-е:

$$\boldsymbol{e_i} = \boldsymbol{b_1} q_{1i} + \boldsymbol{b_2} q_{2i} + \dots + \boldsymbol{b_n} q_{ni} \quad (q_{ji} \in \mathbb{Z})$$

На матричном языке это значит, что $(b_{ji}) \cdot (q_{ji}) = E$ – единичная матрица. Вычисляя определитель левой и правой части, получим $\det(b_{ji}) \cdot \det(q_{ji}) = 1$. Так как слева в этом равенстве стоят целые числа, то каждое из них есть либо 1, либо –1.

Наоборот, если $m = n$ и $\det(b_{ji}) = \pm 1$, то матрица (b_{ji}) обратима над кольцом целых чисел (см. формулу обратной матрицы). Значит существует целочисленная $n \times n$-матрица (t_{ji}) такая, что $(t_{ji}) \cdot (b_{ji}) = E$. Следовательно, для любой строки $\boldsymbol{d} = (d_1, \dots, d_n) \in \mathbb{Z}^n$ выполняется равенство

$$\boldsymbol{d} = (d_1, \dots, d_n) = (d_1, \dots, d_n)E = (d_1, \dots, d_n) \cdot (t_{ji}) \cdot (b_{ji}) =$$
$$= \left[(d_1, \dots, d_n) \cdot (t_{ji})\right] \cdot (\boldsymbol{b_1}, \dots, \boldsymbol{b_n})^{\top}.$$

Разложимость доказана. Единственность разложения следует из того, что $(\boldsymbol{b_1}, \dots, \boldsymbol{b_n})$ – базис линейного пространства $\mathbb{Q}^n$. □

Рассмотрим отображение $\Pi\colon \mathbb{Z}^n \to A$ такое, что

$$\Pi(z_1, \dots, z_n) = a_1 z_1 + \dots a_n z_n \qquad (4)$$

(здесь группа A задана соотношением (1)). Определим ядро K отображения (4) как совокупность строк $(z_1, \dots, z_n)$ таких, что $a_1 z_1 + + \dots a_n z_n = 0$.

Теорема 3. Любая подгруппа H группы строк $\mathbb{Z}^n$ конечно порождена и более того, имеет базис не более чем из n элементов.

Доказательство – индукция по n. Случай $n = 1$ (база индукции) есть утверждение теоремы 1. Предположим, для размерностей меньших n утверждение теоремы 3 справедливо, и H – подгруппа группы $\mathbb{Z}^n$. Обозначим через $\rho\colon \mathbb{Z}^n \to \mathbb{Z}$ проекцию на первую координату, т.е. $\rho(z_1, \dots, z_n) = z_1$. Образ $\rho(H)$ есть подгруппа в $\mathbb{Z}$, и поэтому она имеет вид $k\mathbb{Z}$ для некоторого $k \in \mathbb{N}_0$. Выберем строку $\boldsymbol{h_1} \in H$ такую, что $\rho(\boldsymbol{h_1}) = k$ и обозначим $K = \{\boldsymbol{b} \in H \mid \rho(\boldsymbol{b}) = 0\}$. Лемма показывает (при $A = \mathbb{Z}$ и $a_1 = 1, a_j = 0, j > 1$), что K – подгруппа. При этом

$K \subseteq \boldsymbol{e_2}\mathbb{Z} + \cdots + \boldsymbol{e_n}\mathbb{Z}$. Индукционное предположение дает нам базис $\boldsymbol{h_2}, .. \boldsymbol{h_m}$ группы K, состоящий из $m-1$ элемента, и $m \leq n$. Тогда $\boldsymbol{h_1}, \boldsymbol{h_2}, \dots, \boldsymbol{h_m}$ – базис группы H. Действительно, если $\boldsymbol{b} \in H$, то найдется целое q_1 такое, что $\rho(\boldsymbol{b}) = kq_1 = \rho(\boldsymbol{h_1})q_1$. Отсюда $\rho(\boldsymbol{b} - \boldsymbol{h_1}q_1) = 0$, и поэтому $\boldsymbol{b} - \boldsymbol{h_1}q_1 \in K$. Тогда найдутся целые $q_2, \dots, q_m$ такие, что $\boldsymbol{b} - \boldsymbol{h_1}q_1 = \boldsymbol{h_2}q_2 + \cdots + \boldsymbol{h_m}q_m$, откуда

$$\boldsymbol{b} = \boldsymbol{h_1}q_1 + \boldsymbol{h_2}q_2 + \cdots + \boldsymbol{h_m}q_m. \qquad (5)$$

Разложение доказано. Единственность разложения (5) достаточно доказать для нулевого $\boldsymbol{b}$ и в предположении ненулевого k. Итак, пусть $\boldsymbol{h_1}q_1 + \boldsymbol{h_2}q_2 + \cdots + \boldsymbol{h_m}q_m = \boldsymbol{0}$. Применяя проекцию ρ к левой и правой части этого равенства, получим $kq_1 = 0$, откуда $q_1 = 0$. Равенство $\boldsymbol{h_2}q_2 + \cdots + \boldsymbol{h_m}q_m = \boldsymbol{0}$ возможно только при нулевых g_j, что показывает предположение индукции. □

Теорема 4. Пусть H – подгруппа в $\mathbb{Z}^{\boldsymbol{n}}$. Тогда в $\mathbb{Z}^{\boldsymbol{n}}$ найдется базис $\boldsymbol{b_1}, \dots, \boldsymbol{b_n}$ такой, что

$$H = \boldsymbol{b_1}t_1\mathbb{Z} + \boldsymbol{b_2}t_2\mathbb{Z} + \cdots + \boldsymbol{b_n}t_n\mathbb{Z}$$

для некоторых целых неотрицательных $t_1, \dots, t_n$ таких, что $t_j \mid t_{j+1}$ при $j < n$.

Доказательство сведем к элементарным преобразованиям целочисленных матриц. Согласно теореме 3 найдется базис $\boldsymbol{h_1}, \boldsymbol{h_2}, \dots, \boldsymbol{h_m}$ подгруппы H, состоящий не более чем из n элементов. Запишем $\boldsymbol{h_i} = (h_{i1}, \dots, h_{in}), 1 \leq i \leq m$ и составим $m \times$-матрицу $\mathcal{M}(H)$. Элементарные преобразования строк этой матрицы соответствуют замене базиса подгруппы H, а элементарные преобразования столбцов этой матрицы – замене базиса группы $\mathbb{Z}^n$.

Таким образом, на матричном языке утверждение теоремы звучит так: любую целочисленную матрицу элементарными преобразованиями строк и столбцов можно привести к диагональному виду $diag\,(t_1, t_2, \dots, t_m)$, где $t_j \mid t_{j+1}$ при $j < m$. Доказательство этого утверждения ведем индукцией по размеру матрицы $\mathcal{M}$. База индукции: $m = n = 1$ – очевидный случай. Пусть t_1 равен НОД всех элементов матрицы $\mathcal{M}$. Пользуясь алгоритмом Евклида, элементарными преобразованиями строк и столбцов поместим t_1 на место (1; 1). Все элементы получившейся матрицы (как, впрочем, и исходной матрицы $\mathcal{M}$) делятся на t_1. Тогда элементарными преобразованиями строк мы

можем занулить все элементы первого столбца, стоящие под t_1. Далее элементарными преобразованиями столбцов зануляем все элементы первой строки, стоящие правее t_1. Матрица $\mathcal{M}$ приобретает блочный вид

$$\begin{pmatrix} t_1 & 0 \dots & 0 \\ 0 & * \; * & * \\ \vdots & * \; * & * \\ 0 & * \; * & * \end{pmatrix}.$$

Остается применить индукционное предположение к подматрице, отмеченной звездочками. □

Мы готовы теперь дать описание произвольной конечно-порожденной абелевой группы (1). Пусть K – ядро отображения (4). Прямая проверка убеждает нас в справедливости следующего утверждения.

Лемма 1. Ядро K – подгруппа в группе строк $\mathbb{Z}^n$.

Отношение $\boldsymbol{z} \sim \boldsymbol{z}' \overset{\text{опр}}{\Leftrightarrow} \boldsymbol{z} - \boldsymbol{z}' \in K$ есть отношение эквивалентности на группе $\mathbb{Z}^n$, согласованное со сложением. Обозначим через $\mathbb{Z}^n/K$ совокупность всех классов эквивалентности, которыми будут смежные классы $\boldsymbol{z} + K$, где $\boldsymbol{z}$ пробегает $\mathbb{Z}^n$.

Лемма 2. Фактор-группа $\mathbb{Z}^n/K$ изоморфна А.

Доказательство. Изоморфизм $\phi: \mathbb{Z}^n/K \to A$ задается правилом $\phi(\boldsymbol{z} + K) = \Pi(\boldsymbol{z})$. □

Теорема 5. Любая конечно-порожденная абелева группа A есть прямая сумма циклических групп с порядками $(t_1, \dots, t_m, \infty, \dots, \infty)$, где $t_j \mid t_{j+1}$ при $j < m$.

Доказательство. Пусть $A = \boldsymbol{a_1}\mathbb{Z} + \cdots + \boldsymbol{a_n}\mathbb{Z}$ и K – ядро эпиморфизма (4). Тогда группа A изоморфна фактор-группе $\mathbb{Z}^n/K$. Найдем в $\mathbb{Z}^n$ и K согласованные базисы, т.е. базис $\boldsymbol{b_1}, \dots, \boldsymbol{b_n}$ пространства строк $\mathbb{Z}^n$ и натуральные числа $t_1, \dots t_m$ такие, что $t_j \mid t_{j+1}$ при $j < m$, кроме того, $m \le n$ и $\boldsymbol{b_1}t_1, \dots, \boldsymbol{b_m}t_m$ есть базис группы K. Тогда, обозначая декартово произведение символом $\oplus$, получим:

$A \cong \mathbb{Z}^n / K \cong$
$\cong (\boldsymbol{b_1}\mathbb{Z} + \cdots + \boldsymbol{b_m}\mathbb{Z} + \cdots + \boldsymbol{b_n}\mathbb{Z})/(\boldsymbol{b_1}t_1\mathbb{Z} + \cdots + \boldsymbol{b_m}t_m\mathbb{Z} + 0 + .. + 0) \cong$
$\cong \boldsymbol{b_1}\mathbb{Z}/\boldsymbol{b_1}t_1\mathbb{Z} \oplus \ldots \oplus \boldsymbol{b_m}\mathbb{Z}/\boldsymbol{b_m}t_m\mathbb{Z} \oplus \boldsymbol{b_{m+1}}\mathbb{Z}/0 \oplus \ldots \oplus \boldsymbol{b_n}\mathbb{Z}/0 \cong$
$\cong \mathbb{Z}_{\boldsymbol{t_1}} \oplus \ldots \oplus \mathbb{Z}_{\boldsymbol{t_m}} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z},$
что и требовалось доказать. □

12. ГРУППА ПОДСТАНОВОК

Биективное отображение τ чисел {1, 2, …, n} на себя называется подстановкой на n символах. Такое отображение может быть интерпретировано как перестановка чисел 1, 2, … , n, поэтому вместо термина "подстановка" можно употреблять и термин "перестановка". Полная табличная запись такого отображения следующая

$$\tau = \begin{pmatrix} 1 & 2 & \ldots n-1 & n \\ i_1 & i_2 & \ldots i_{n-1} & i_n \end{pmatrix}. \qquad (1)$$

Эта запись означает, что $\tau(k) = i_k$ для всех $1 \leq k \leq n$. В частности, от перестановки столбцов в таблице (1) перестановка τ не меняется. Короче подстановку (1) записывают так: $\tau = (i_1, i_2, \ldots, i_n)$ (не забывать ставить запятые!). Обозначим множество всех подстановок S_n и рассмотрим на этом множестве операцию композиции.

Теорема 1. Множество всех подстановок образует группу из $n!$ элементов относительно операции композиции.

Доказательство. Ассоциативность вытекает из ассоциативности операции композиции функций. Нейтральным элементом служит единичная подстановка e такая, что $e(k) \equiv k$. Обратной к подстановке (1) будет подстановка

$$\tau^{-1} = \begin{pmatrix} i_1 & i_2 & \ldots i_{n-1} & i_n \\ 1 & 2 & \ldots n-1 & n \end{pmatrix},$$

которая получается перестановкой строк таблицы, задающей элемент τ .

Подстановок на двух символах две – тождественная и меняющая местами эти два элемента. Предположим, что мы доказали равенство $|S_n| = n!$. (Здесь и далее |G| – порядок группы, т.е. количество элементов в ней). Множество подстановок $\tau \in S_{n+1}$ с фиксированным значением τ (n + 1) = k имеет ту же мощность (т.е. то же количество элементов), что и $|S_n|$, ибо и в том и другом случае это множество всех биекций одного множества из n элементов на другое множество из n элементов. Получаем, что группа S_{n+1} разбивается на n + 1 мно-

жеств, содержащих по $n!$ элементов. Тогда $|S_{n+1}| = n!\,(n+1) = (n+1)!$ Индукция показывает, что справедливо последнее утверждение теоремы. □

Подстановка вида $c = (ij \ldots k)$, которая переводит i в j, а j – в следующее справа стоящее число, а k переходит в первое число i, называется циклом, при этом множество $\{i,j,\ldots, k\}$ называется содержанием цикла c и обозначается $supp\ c$. Количество чисел в записи цикла называется его длиной. Цикл длины 2 называется транспозицией. Два цикла называются независимыми, если их содержания не пересекаются. Два независимых цикла c_1 и c_2 коммутируют, т.е. имеет место равенство $c_1c_2 = c_2c_1$. Докажем это.

Следует проверить равенство $c_1c_2(k) = c_2c_1(k)$ при любом k. Рассмотрим три возможных и исчерпывающих случая.

Случай 1. $k \notin supp\ c_1 \cup supp\ c_2$. Тогда $c_1(k) = c_2(k) = k$, поэтому и $c_1c_2(k) = c_2c_1(k)$.

Случай 2. $k \in supp\ c_1 \backslash supp\ c_2$. Пусть в цикле c_1 вслед за k стоит q. Тогда $c_1(k) = q$, причем $q \notin supp\ c_2$. Следовательно, $c_1c_2\,(k) = c_1(k) = q = c_2(q) = c_2c_1(k)$.

Случай 3. $k \in supp\ c_2 \backslash supp\ c_1$. Этот случай аналогичен случаю 2.

Поскольку циклы независимы, то $supp\ c_1 \cap supp\ c_2 = \emptyset$ и k не может принадлежать этому пересечению. Следовательно, все возможные случаи исчерпаны.

Теорема 2. Любая подстановка раскладывается в произведение независимых циклов.

Доказательство проводим индукцией по длине перестановки. Пусть τ – произвольная подстановка. Первый цикл c откроем числом 1. Носитель цикла c есть множество $\tau^k(1)$ при $k = 1,2,\ldots$ Заметим, что если $\tau^k(1) = \tau^j(1)$ при $j < k$, то $\tau^{k-j}(1) = 1$. Отсюда вытекает, что если m – наименьшеее натуральное число со свойством $\tau^m(1) = 1$, то

$$supp\ c = \{1, \tau(1), \ldots, \tau^{m-1}(1)\} \text{ и } c = \left(1\tau(1) \ldots \tau^{m-1}(1)\right).$$

Рассматривая сужение биекции τ на множество $\overline{1..n} \backslash supp\ c$ и применяя предположение индукции, получаем требуемое. □

Следствие. Любая подстановка раскладывается в произведение транспозиций.

Доказательство. Мы уже доказали, что любая подстановка раскладывается в произведение циклов. Остается убедиться, что

$$(ij\ p\ \dots\ tk) = (ij)(jp)\ \dots\ (tk). \qquad (2)$$

Пример. $\tau = (7, 1, 4, 2, 6, 9, 8, 3, 5) = (178342)(569) = (17)\ (78)\ (83)\ (34)\ (42)\ (56)\ (69)$.

Для подстановки, как и для числа, можно определить знак. Инверсией подстановки τ назовем пару натуральных чисел (j, k) с условием «$j < k$, но $\tau(j) > \tau(k)$». Подстановку τ назовем четной и будем писать $sgn\ \tau = 1$, если число всех инверсий подстановки τ четно. В противном случае подстановку τ назовем нечетной и будем писать $sgn\ \tau = -1$. Отметим, что в данном контексте sgn – отображение из группы S_n в группу знаков $\{\pm 1\}$. Докажем, что это отображение обладает свойством гомоморфности (теорема 3, Б).

Лемма. При умножении на транспозицию подстановка меняет знак.

Докажем утверждение сначала, когда подстановка (1) умножается на транспозицию $(j\ j+1)$ справа:

$$\tau\ (j\ j+1) = \begin{pmatrix} 1 & 2 & \dots\ j & j+1 \dots \\ i_1 & i_2 & \dots i_{j+1} & i_j\ \dots \end{pmatrix}.$$

Если пара $(j, j+1)$ была инверсией у перестановки τ, то она перестает ей быть у перестановки $\tau \cdot (j\ j+1)$, и наоборот. Далее пара (k, j) с $k \neq j+1$ есть инверсия подстановки τ в том и только том случае, когда пара $(k, j+1)$ есть инверсия подстановки $\tau \cdot (j\ j+1)$. Аналогично пара $(k, j+1)$ с условием $k \neq j$ есть инверсия подстановки τ в том и только том случае, когда пара (k, j) есть инверсия подстановки $\tau \cdot (j\ j+1)$.Что касается других пар (k, l) с k и l, не совпадающих ни с j, ни с $j+1$, то такая пара является инверсией в τ тогда и только тогда, когда она же есть инверсия для произведения $\tau \cdot (j\ j+1)$. Итак, число инверсий у τ отличается от числа инверсий у $\tau \cdot (j\ j+1)$ на единицу, следовательно,

$$sgn(\tau\ \cdot\ (jj+1)) = -\ sgn\ \tau\ .$$

Для транспозиции $(j\ k)$ с условием $j+1 < k$ заметим, что

$$(jk) = (k\ k-1)\ (j\ k-1)(k-1\ k).$$

Тем самым доказательство леммы завершается индукцией по числу $k - j$.

Теорема 3 (о знаке подстановки).

А. Если подстановка разложена в произведение транспозиций $\tau = t_1 t_2 \ldots t_k$, то

$$sgn\,\tau = (-1)^k.$$

В частности, любая транспозиция – нечетная перестановка.

Б. Для любых двух подстановок τ и ρ имеет место формула

$$sgn(\tau\rho) = sgn\,\tau \cdot sgn\,\rho. \qquad (3)$$

В. Для цикла *c* длины *k* справедливо равенство $sgn\,c = (-1)^{k-1}$.

С. Если $\tau = c_1 c_2 \ldots c_m$ – разложение в независимые циклы и $\overline{1\ldots n} = \bigcup_{k=1}^{m} supp\,c_k$, то

$$sgn\,\tau = (-1)^{n-m}. \qquad (4)$$

Доказательство. А. Заметим, что единичная подстановка четная, так как у неё нет инверсий вовсе. Тогда, умножая поочередно справа единичную подстановку на транспозиции $t_1, t_2, \ldots, t_k$, мы каждый раз будем менять четность на противоположную согласно лемме. Всего будет *k* смен четности единичной подстановки. Следовательно, $sgn\,\tau = sgn\,(et_1 t_2 \ldots t_k) = (-1)^k$.

Б. Пусть $\tau = t_1 t_2 \ldots t_k$ и $\rho = s_1 s_2 \ldots s_m$ – разложения в произведении транспозиций двух подстановок. Тогда, применяя утверждение А, получим

$$\mathrm{sgn}\tau\rho = \mathrm{sgn}(t_1\, t_2 \ldots t_k\, s_1 s_2 \ldots s_m) = (-1)^{k+m} = (-1)^k(-1)^m = \\ = \mathrm{sgn}\,\tau \cdot \mathrm{sgn}\rho.$$

В. Утверждение следует из А и из формулы (2)

С. Обозначим через $k_1, \ldots, k_m$ длины циклов $c_1, \ldots, c_m$. Согласно В будем иметь:

$$sgn\,\tau = (-1)^{k_1-1} \ldots (-1)^{k_m-1} = (-1)^{k_1+k_2+\cdots+k_m-m} = (-1)^{n-m}. \square$$

Следствие. Для $n > 1$ подмножество $\mathbb{A}_n$ всех четных подстановок образует подгруппу порядка *n*!/2 в группе подстановок.

Проверка: если τ, ρ $\in \mathbb{A}_n$, то *sgn* (τ ρ) = *sgn* τ· *sgn* ρ = 1 · 1 = 1, откуда вытекает τ ρ $\in \mathbb{A}_n$. Далее, $sgn\,\tau^{-1} = 1/sgn\,\tau = 1$ и $\tau^{-1} \in \mathbb{A}_n$. Так как $e \in \mathbb{A}_n$, то доказано, что $\mathbb{A}_n$ – подгруппа.

Отображение $\tau \to (12)\,\tau$ устанавливает биекцию между множеством всех четных подстановок и множеством всех нечетных подстановок. Иными словами, имеет место разбиение на смежные классы $S_n = \mathbb{A}_n \cup (12)\mathbb{A}_n$. Отсюда следует, что порядок группы $\mathbb{A}_n$ равен половине порядка группы S_n .□

Группа $\mathbb{A}_n$ называется знакопеременной группой.

Для $n = 3$ группа $\mathbb{A}_3 = \{e, (123), (132)\}$ – циклическая порядка 3. Она описывает собственные симметрии правильного треугольника (не меняющие ориентацию плоскости).

13. КОЛЬЦА

Определение кольца приведено в п. «Алгебраические системы». Подмножество S кольца R будет подкольцом, если оно, во-первых, есть подгруппа аддитивной группы $(R, +)$ и, кроме того, замкнуто относительно умножения. Подмножество S кольца с единицей R будет подкольцом с единицей, если оно будет подкольцом в смысле определения, данного выше и, кроме того, содержит единицу кольца. В этом смысле $2\mathbb{Z}$ не будет подкольцом с единицей в $\mathbb{Z}$, но будет подкольцом кольца $\mathbb{Z}$, рассматриваемого просто как кольцо. Эта процедура "забывания" операции (одной или нескольких) типична для алгебраических систем. Напомним (см. п. «Алгебраические системы»), что алгебраическая система определяется как множество с семейством операций, заданных на нем. Так, например, система $(\mathbb{Z}, +)$ есть всего лишь полугруппа, $(\mathbb{Z}, +, 0)$ – моноид, $(\mathbb{Z}, +, –, 0)$ – группа (здесь "–" – унарный минус, т.е. операция $a \to -a$). Наконец, $(\mathbb{Z}, +, \cdot, –, 0, 1)$ – кольцо с единицей; в этой системе пять операций, две из которых бинарны, одна унарная и две 0-арные. Если иногда, допуская вольность, мы пишем, что $(\mathbb{Z}, +)$ – группа, то под этим подразумевается, что операция сложения на множестве целых чисел такова, что для нее найдется нейтральный элемент, а для любого элемента найдется противоположный элемент (они единственны, см. п. «Алгебраические системы»), и существующие в силу этого операции унарного минуса и нулевой элемент мы подсоединяем к системе $(\mathbb{Z}, +)$ и таким образом получаем группу.

Подмножество I кольца R называется *идеалом*, если оно, во-первых, будет подгруппой аддитивной группы (R,+), а во-вторых, для любых $a \in I$ и $r \in R$ следует, что $ar \in I$ и $ra \in I$. Множество, состоящее из одного нуля, а также все кольцо всегда будут идеалами. Остальные идеалы называются собственными. Ясно, что всякий идеал будет подкольцом (без единицы).

Идеал коммутативного кольца с единицей R вида $aR = \{ar \mid r \in R\}$ называется главным идеалом, порожденным элементом a. Если каждый идеал главный, то R называют кольцом главных идеалов.

Кольцо R называется областью целостности, если произведение ab равно 0 лишь в том случае, когда один из сомножителей равен 0.

Теорема 1. Кольцо целых чисел есть область главных идеалов. В ней всякий идеал имеет вид $n\mathbb{Z}$ (n = 0, 1, 2, …). При n = 1 получаем все кольцо целых чисел, а при n = 0 получаем нулевой идеал.

Доказательство есть прямое следствие теоремы о подгруппах циклической группы и того факта, что всякий идеал есть прежде всего подгруппа аддитивной группы.

Пусть I – идеал кольца R. Введем на множестве R отношение сравнимости по идеалу I, считая, что два элемента $a, b \in R$ сравнимы по модулю идеала I, если и только если $a - b \in I$. Записывать это отношение будем так: $a \equiv b \ (mod\ I)$. Это отношение есть отношение эквивалентности на множестве R. Более того, это отношение согласовано с операциями сложения и умножения на кольце R в том смысле, что если $a_1 \equiv b_1$ и $a_2 \equiv b_2$, то $(a_1 + a_2) \equiv (b_1 + b_2)$ и $(a_1 \cdot a_2) \equiv$ $\equiv (b_1 \cdot b_2)$.

Действительно, из условия $a_1 \equiv b_1$ и $a_2 \equiv b_2$ вытекает, что $b_1 =$ $= a_1 + i_1$ и $b_2 = a_2 + i_2$ для некоторых $i_1, i_2 \in I$. Тогда

$(b_1 + b_2) - (a_1 + a_2) = i_1 + i_2 \in I,$

$(b_1 \cdot b_2) - (a_1 \cdot a_2) = (a_1 + i_1)(a_2 + i_2) - a_1 a_2 =$

$= i_1 a_2 + a_1 i_2 + i_1 i_2 \in I,$

что и доказывает утверждение.

Класс эквивалентности, порожденный элементом a, состоит из всех сумм $a + i$, где i пробегает идеал I. Его удобно обозначить $a + I$, называть смежным классом, а a называть представителем этого класса. Все кольцо R разбивается в объединение смежных классов. В частности, два смежных класса либо совпадают, либо не пересекаются. Обозначим через R/I фактор-множество, т.е. множество, элементами которого являются смежные классы $a + I$. Перенесем операции сложения и умножения с кольца R на этот фактор-множество

$$(a + I) + (b + I) = (a + b) + I; \ \ (a + I)(b + I) = ab + I. \qquad (*)$$

Теорема 2. А. Операции (*) определены корректно, т.е. правые части $(a + b) + I$ и $ab + I$ не зависят от представителей смежных классов.

Б. Фактор-множество R/I относительно операций (*) образует кольцо.

В. Если R – кольцо с единицей, то и R/I – кольцо с единицей $1 + I$. Если R коммутативно, то и R/I коммутативно.

Доказательство. А. Корректность операций (*) это не что иное, как уже доказанная согласованность отношения "≡ " с операциями кольца R.

Б. Ассоциативность и коммутативность сложения так же, как и ассоциативность умножения, сразу следуют из аналогичных свойств в кольце R. Например, выкладка

$$(a + I) + (b + I) = (a + b) + I = (b + a) + I = (b + I) + (a + I)$$

доказывает коммутативность сложения. Смежный класс $I = 0 + I$ будет нулем в R/I, а смежный класс $(-a) + I$ будет противоположным элементом по отношению к смежному классу $a + I$.

Утверждение В. очевидно.□

Кольцо R/I, которое построено выше, называется фактор-кольцом кольца R по идеалу I.

Применим конструкцию факторизации к кольцу целых чисел. Фиксируем натуральное число n и тем самым фиксируем идеал $n\,\mathbb{Z}$, состоящий из всех целых чисел, делящихся на n. Сравнимость по модулю этого идеала называют проще сравнимостью по модулю n и записывают как $a \equiv b \pmod{n}$. Это означает, что n делит разность $a - b$. Всего имеются n классов $n\,\mathbb{Z}$, $1 + n\,\mathbb{Z}$, … , $(n - 1) + \mathbb{Z}$. Класс $k + n\,\mathbb{Z}$ при $0 \le k \le n - 1$ можно описать как совокупность всех целых чисел, дающих при делении на n в остатке k. Получаем фактор-кольцо $\mathbb{Z} / n\,\mathbb{Z}$, которое будем обозначать как $\mathbb{Z}_n$. В нем n элементов:

$$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \dots, \widehat{n-1}\}, \quad \hat{k} := k + n\mathbb{Z}.$$

Элементы $\hat{0}, \hat{1}, \dots, \widehat{n-1}$ мыслятся как числа новой природы, и над ними можно совершать арифметические операции, пользуясь привычными законами. Например, в кольце $\mathbb{Z}_6$ справедливо соотношение $\hat{2} \cdot \hat{3} = \hat{0}$, т.е. в нем есть ненулевые делители нуля, а в кольце $\mathbb{Z}_8$ двойка в третьей степени равна нулю (нильпотентность элемента).

Кольцо $\mathbb{Z}_n$ называется кольцом вычетов по модулю n. Ранее была изложена изоморфная копия этого кольца как множества целых чисел $\{0, 1, 2, \dots, n - 1\}$ и операциями сложения и умножения по модулю n.

Элемент a кольца с единицей R называется обратимым, если он обратим в моноиде $R(\cdot)$, т.е. выполняется равенство $aa' = 1 = a'a$ для подходящего $a' \in R$.

Теорема 3. Множество обратимых элементов кольца R образует группу относительно умножения.

Это следует из свойств обратимости (см. п. «Алгебраические системы»).

Элемент $\hat{k}$ кольца вычетов $\mathbb{Z}_n$ обратим тогда и только тогда, когда НОД (k, n) = 1. Порядок группы обратимых элементов кольца $\mathbb{Z}_n$, т.е число натуральных чисел $1 \leq k \leq n-1$ взаимно простых с n, называется эйлеровой фи-функцией $\phi(n)$. Оказывается

$\phi(p^k) = p^k - p^{k-1}$; $\phi(n \cdot m) = \phi(n)\phi(m)$, если НОД $(n, m) = 1$,

что дает возможность вычислять эту характеристику натуральных чисел. Например, $\phi(12) = \phi(3)\phi(4) = (3^1 - 3^0)(4-2) = 4$.

14. ПОЛЯ

Напомним, поле – это ненулевое коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим. Структура поля как алгебраической системы более сложная, чем у кольца, и не только потому, что в понятие поля входит еще одна унарная операция – переход к обратному элементу ($k \to k^{-1}$). Сложность в том, что эта операция частичная, т.е. не всюду определенная, как известно, деление на ноль запрещено. Знакомые нам примеры полей рациональных и действительных чисел являются важнейшими, но не единственными применимыми "всюду и везде" полями. Булеан {0,1} относительно логических операций сложения и умножения образует поле из двух элементов. Обобщим этот пример.

Теорема. Кольцо вычетов по модулю простого числа является полем.

Доказательство. Пусть p – простое число, и $\hat{a} \in \mathbb{Z}_p$ – ненулевой элемент. Это значит, что $a \notin p\mathbb{Z}$, и тем самым числа p и a взаимно просты. Согласно алгоритму Евклида найдутся целые числа b и q такие, что $1 = ab + pq$. Тогда $\hat{a}\hat{b} = 1$, ибо pq = 0 (mod p). Следовательно, $\hat{a}$ обратим в кольце $\mathbb{Z}_p$. Мы проверили, что любой ненулевой элемент обратим в $\mathbb{Z}_p$. □

Заметим, что кольцо вычетов по модулю составного числа $n = km$ ($k, m > 1$) имеет делители нуля: $\hat{k} \cdot \hat{m} = 0$ и поэтому не может быть полем.

Подмножество L поля K называется подполем или, иначе, K называется расширением поля L, если L содержит ноль и единицу и замкнуто относительно операций сложения, умножения, взятия обратного и перехода к противоположному элементу.

Примеры. 1. Поле $\mathbb{R}$ есть расширение поля рациональных чисел $\mathbb{Q}$. К необходимости расширить $\mathbb{Q}$ до $\mathbb{R}$ приводит нас задача извлечения всевозможных корней из положительных действительных чисел. Если поставить более скромную задачу – извлечь корень квадратный только из одного числа – двойки, то получаем расширение

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

поля рациональных чисел. Прямая проверка показывает, что множество $\mathbb{Q}[\sqrt{2}]$ замкнуто относительно операций сложения и умножения и тем самым является кольцом. Для доказательства замкнутости относительно перехода к обратному элементу надо уметь избавляться от иррациональности в знаменателе:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

Вся тонкость заключается в том, что если $a + b\sqrt{2} \neq 0$ для рациональных a и b, то $a^2 - 2b^2 \neq 0$. Это есть следствие иррациональности числа $\sqrt{2}$.

2. Построим поле $\mathbb{Z}_7[i]$ из 49 элементов вида $a + ib$, где $a, b \in \mathbb{Z}_7$. Определим сложение и умножение так:

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

Иными словами, новое число i играет роль корня квадратного из –1 (такового нет в поле из семи элементов, что проверяется прямым вычислением всех квадратов: $2^2 = 5^2 = 4; 3^2 = 2 = 4^2; 1^2 = 6^2 = 1$). Заметим, что аналогичным образом поле из 25 элементов не построишь – в $\mathbb{Z}_5$ имеется корень квадратный из –1, а именно $2^2 = 4 = -1$.

3. Известно, что π – трансцендентное число, т.е. оно не является корнем никакого многочлена с целыми коэффициентами. Благодаря

этому наименьшее расширение поля рациональных чисел, содержащее π, состоит из всех действительных чисел вида

$$\frac{b_0+b_1\pi+\cdots+b_m\pi^m}{a_0+a_1\pi+\cdots+a_n\pi^n},$$ все a_j, b_k – целые и не все a_j-е равны 0.

Никакое упрощение по типу примера 1 здесь невозможно именно из-за трансцендентности числа π.

15. АЛГЕБРА МНОГОЧЛЕНОВ

15.1. Конструкция алгебры многочленов. Степень многочлена

Пусть K – поле. Рассмотрим бесконечномерное пространство финитных строк над этим полем:

$$(a_0, a_1, \dots a_k, \dots) \quad (1)$$

(все $a_j \in K$). Финитность означает, что лишь конечное число коэффициентов не равно нулю. Стандартным базисом в рассматриваемом пространстве служат строки e_j, у которых на j-м месте единица, а остальные коэффициенты – нули. Определим умножение базисных элементов в соответствии с правилом

$$e_j \cdot e_k = e_{j+k} \quad (2)$$

и распространим это умножение на все пространство финитных строк a по линейности, а именно для двух строк $(a_0, a_1, \dots, a_k, \dots)$ и $(b_0, b_1, \dots, b_k, \dots)$ их произведением (по-другому сверткой) будет строка $(c_0, c_1, \dots, c_k, \dots)$ такая, что

$$c_0 = a_0b_0; c_1 = a_0b_1 + a_1b_0; \dots; c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0. \quad (3)$$

Теорема 1. А. Пространство финитных строк относительно умножения (3) образует коммутативное кольцо с единицей e_0, в которое гомоморфно вкладывается поле K посредством отображения $a \to ae_0$.

Б. Строка $e_1 = (0,1,0,0, \dots)$, которую мы обозначим X, порождает кольцо финитных строк:

$$e_k = X^k;\ (a_0, a_1, \dots, a_k, \dots) = \sum_{k\geq 0} a_kX^k\ .$$

По этой причине кольцо финитных строк далее называем кольцом многочленов от одной переменной над полем K и обозначаем $K[X]$.

В. Для многочлена $P = \sum_{k\geq 0} a_kX^k$ определена степень

$$\deg P = \max\{\, k \mid a_k \neq 0 \,\}. \quad (4)$$

Если множество $\{k \mid a_k \neq 0\}$ пусто, а это может быть только для нулевого многочлена, то в соответствии с правилами логики полагаем $\deg 0 = \max \emptyset = -\infty$. Однако с точка зрения компьютерных наук это неудобно; будем считать при программировании степенью нулевого многочлена любое отрицательное целое число, например, –1. Степени обладают свойствами:

1) $\deg(P + Q) \leq \max\{\deg P, \deg Q\}$;

2) $\deg PQ = \deg P + \deg Q$.

Если $n = \deg P$, то коэффициент a_n называется старшим. Многочлен вида $aX + b$ называется линейным, а $aX^2 + bX + c$ есть общий вид квадратного трехчлена (здесь $a \neq 0$). Многочлен, у которого все коэффициенты $a_j = 0$ для $j \geq 1$ (по-другому, если $\deg P \leq 0$) называется константным.

С. Многочлен обратим тогда и только тогда, когда он имеет нулевую степень.

Пусть F – поле, содержащее K как подполе. Значением многочлена $P = \sum_{k\geq 0} a_k X^k$ на элементе $b \in F$ называется элемент $P(b) := \sum_{k\geq 0} a_k b^k \in F$. Если это значение – ноль, то b называется корнем многочлена P. Таким образом, многочлену P можно сопоставить отображение $\hat{P}: F \to F$ такое, что $\hat{P}(b) := P(b)$ для любого $b \in F$. Для полей с бесконечным числом элементов из равенства $\hat{P} = \hat{Q}$ вытекает равенство многочленов $P = Q$. Для конечных полей это неверно (пример: многочлен $X^2 + X$ над полем из двух элементов имеет только нулевые значения, но сам многочлен ненулевой). Тем не менее, допуская вольность, мы далее будем записывать X как x и мыслить x как переменную, вместо которой можно подставлять любое значение из F и, в частности, из K.

15.2. Евклидовость алгебры многочленов

В кольце многочленов существует теория делимости такая же, как и в кольце целых чисел. Причина состоит в том, что кольцо многочленов евклидово, а именно для любых многочленов $M(x), N(x) \in \in K[x]$, второй из которых не равен нулю, найдутся многочлены $Q(x)$ и $R(x)$ такие, что

$$M(x) = N(x) \cdot Q(x) + R(x), \quad \deg R < \deg Q. \qquad (5)$$

Пример 1. Разделим $x^4 - 6x^3 + x^2 + 4x + 7$ на $x^2 - x + 2$ с остатком «уголком»:

$$\begin{array}{l} x^4 - 6x^3 + x^2 + 4x + 7 \;|\; \underline{x^2 - x + 2} \\ \underline{x^4 - x^3 + 2x^2 \qquad\quad} \;|\; x^2 - 5x + 4 \\ -5x^3 - x^2 + 4x + 7 \\ \underline{-5x^3 - 5x^2 - 10x} \\ 4x^2 + 14\,x + 7 \\ \underline{4x^2 - 4x + 8} \\ 18x - 1 \end{array}$$

Итак, $x^2 - 5x + 4$ – неполное частное, а $18x - 1$ – остаток. Имеет место равенство

$$x^4 - 6x^3 + x^2 + 4x + 7 = (x^2 - x + 2)(x^2 - 5x + 4) + 18x - 1.$$

Теорема 2 (Безу). Число a есть корень многочлена $P(x)$ тогда и только тогда, когда $x - a$ делит $P(x)$ нацело, без остатка.

Доказательство. Поделим $P(x)$ на $x - a$ с остатком:

$$P(x) = D(x)(x - a) + R;\ \deg R < \deg(x - a) = 1.$$

Так как $\deg R < 1$, то R – константный многочлен. Тогда $P(a) = D(a) \cdot 0 + R = R$. Следовательно, число a – корень многочлена $P(x)$ в том и только в том случае, когда $R = 0$, а это имеет место ровно тогда, когда $x - a$ делит $P(x)$.

Следствие. Многочлен степени *n* имеет не более *n* различных корней.

Пусть a – корень многочлена $P(x)$. Тогда $P(x) = (x - a)P_2(x)$ по теореме Безу. Если a – корень многочлена $P_2(x)$, то мы можем и от него отщепить $x - a$. Будем это делать до тех пор, пока $P(x) = (x - a)^k \cdot P_{k+1}(x)$ и $P_{k+1}(a) \neq 0$. В этом случае число k называют кратностью корня a. Итак, кратностью корня a многочлена $P(x)$ называется наибольшее натуральное число k такое, что $(x - a)^k$ делит $P(x)$. Если a не является корнем многочлена $P(x)$, то удобно считать, что кратность a есть 0.

Роль простых чисел играют неприводимые многочлены. Неконстантный многочлен называется неприводимым над полем K, если его нельзя разложить в произведение многочленов с меньшими степенями. Оговорка «над полем K» существенна. Многочлен $x^2 + 1$ неприводим над полем действительных чисел, но перестает быть таковым

над полем комплексных чисел ($x^2 + 1 = (x - i)(x + i)$) . Однако, если мы сужаем поле (например, до поля рациональных чисел в примере выше), то неприводимость сохраняется.

Сформулируем аналог основной теоремы арифметики. Доказательство ее можно провести в точности так же, как и для целых чисел.

Теорема 3. Любой неконстантный многочлен разложим в произведение неприводимых многочленов. Такое разложение единственно с точностью до перестановки сомножителей и умножения их на ненулевые элементы поля.

Поле комплексных чисел алгебраически замкнуто, это и есть содержание основной теоремы алгебры. Тем самым любой неприводимый унитарный (старший коэффициент равен 1) многочлен на $\mathbb{C}$ имеет вид $z - a$ для некоторого $a \in \mathbb{C}$. Над другими полями положение дел не столь хорошее в смысле разложимости многочленов. Ясно, что всякий линейный многочлен (над любым полем) неприводим.

Разложимость квадратного трехчлена $X^2 + pX + q \in K[X]$ равносильна наличию хотя бы одного корня. Преобразуя уравнение $X^2 + pX + q = 0$ к виду $\left(X + \frac{p}{2}\right)^2 = \frac{p^2 - 4q}{4}$, заключаем, что корень квадратного трехчлена $X^2 + pX + q$ существует тогда и только тогда, когда дискриминант $D = p^2 - 4q$ есть квадрат какого-либо элемента поля K (здесь предполагаем, что $2 \neq 0$ в поле K). Отсюда получаем

Предложение. Квадратный трехчлен $X^2 + pX + q$ над полем K, в котором $2 \neq 0$, неприводим тогда и только тогда, когда он не имеет корней в поле K. Это равносильно тому, что дискриминант $p^2 - 4q$ не является квадратом никакого элемента поля K. В частности, над полем действительных чисел квадратный трехчлен $X^2 + pX + q$ неприводим, если и только если $p^2 - 4q < 0$.

15.3. Разложение многочленов над полем действительных чисел

Над полем действительных чисел существуют, по крайней мере, два вида неприводимых многочленов – линейные и квадратичные с отрицательным дискриминантом. Оказывается, что эти два случая исчерпывают множество неприводимых многочленов над $\mathbb{R}$.

Теорема 4. Любой многочлен над полем действительных чисел разложим в произведение линейных множителей и квадратичных множителей с отрицательными дискриминантами:

$P(x) = a(x - x_1)^{k_1} \dots (x - x_m)^{k_m}(x^2 + p_1x + q_1)^{h_1} \dots (x^2 + p_tx + q_t)^{h_t}$.

Здесь $x_1, \dots, x_m$ – все различные действительные корни многочлена $P(x)$, $k_1, \dots, k_m$ – их кратности, все дискриминанты $p_j^2 - 4q_j$ меньше нуля, и квадратные трехчлены $x^2 + p_jx + q_j$ все различны.

Вначале докажем лемму

Лемма. Если $f(x) \in \mathbb{R}[x]$ и $f(z) = 0$ для какого-либо $z \in \mathbb{C}$, то сопряженное число $\bar{z}$ также является корнем многочлена $f(x)$.

Доказательство. Пусть $f(x) = \sum a_j x^j$, все $a_j \in \mathbb{R}$ и z – комплексный корень многочлена $f(x)$. Тогда

$$0 = \overline{f(z)} = \sum_j \bar{a}_j \bar{z}^j = \sum_j a_j \bar{z}^j ,$$

где мы использовали свойства сопряжения. Следовательно, $f(\bar{z}) = 0$. Тем самым $\bar{z}$ – корень многочлена f. □

Доказательство теоремы. Достаточно доказать, что любой неприводимый многочлен над полем действительных чисел либо линейный, либо квадратичный с отрицательным дискриминантом. Пусть $p(x) \in$ $\in \mathbb{R}[x]$ – неприводимый многочлен с единичным старшим коэффициентом. В случае $\deg\, p(x) = 1$ сразу получаем $p(x) = x - a$ для некоторого действительного a. Предположим, что $\deg p(x) \geq 2$. Обозначим через $z = a + ib$ какой-либо комплексный корень этого многочлена, существующий по основной теореме алгебры комплексных чисел. Так как $p(x)$ неприводим, то $z \notin \mathbb{R}$ (см. теорему Безу). Тогда по лемме $\bar{z}$ будет еще одним корнем многочлена $p(x)$, отличным от z.

Многочлен $\tilde{p}\,(x) = (x - z)\,(x - \bar{z}) = x^2 - (z + \bar{z})\,x + z\bar{z} = x^2 -$ $- 2ax + a^2 + b^2$ имеет действительные коэффициенты. Кроме того, $\tilde{p}(x)$ делит $p(x)$ согласно теореме Безу. Так как $p(x)$ неприводим и имеет единичный старший коэффициент, то получаем равенство $p(x) = \tilde{p}(x)$. Дискриминант этого многочлена отрицателен, так как иначе он имел бы вещественные корни.□

Пример 2. А. Разложим многочлен $x^4 - 2x^3 + 2x^2 - 7x + 6$ на неприводимые множители. Среди делителей константного члена 6 ищем

корни многочлена. Убеждаемся, что 1 и 2 – корни. Тем самым многочлен делится на $(x-1)(x-2)$. Поделив, находим

$$x^4-2x^3+2x^2-7x+6=(x-1)(x-2)(x^2+x+3)$$

– окончательное разложение над полем $\mathbb{R}$, ибо дискриминант квадратного трехчлена x^2+x+3 отрицателен и, следовательно, он над полем действительных чисел далее неразложим. Разложение того же многочлена над полем комплексных чисел получим, если найдем комплексные корни квадратного трехчлена x^2+x+3. Они суть $-\frac{1}{2}\pm\frac{i\sqrt{11}}{2}$. Тогда

$$x^4-2x^3+2x^2-7x+6=$$
$$=(x-1)(x-2)\left(x+\frac{1}{2}-\frac{i\sqrt{11}}{2}\right)\left(x+\frac{1}{2}+\frac{i\sqrt{11}}{2}\right).$$

– разложение данного многочлена над $\mathbb{C}$.

Б. Разложим x^4+16 над полями действительных и комплексных чисел. Так как действительных корней этот многочлен не имеет, то он разложим на два квадратных трехчлена с отрицательными дискриминантами:

$$x^4+16=(x^2+px+q)(x^2+p'x+q').$$

Так как при замене x на $-x$ многочлен x^4+16 не меняется, то при такой замене квадратный трехчлен x^2+px+q должен переходить в $x^2+p'x+q'$, и наоборот. Отсюда $q=q'$ и $p=-p'$. Приравнивая коэффициенты при x^2, получаем $0=2q-p^2$. В частности, $q>0$. Тогда из соотношения $q^2=16$ (получается подстановкой $x=0$) извлекаем $q=4$ и окончательно $p=2\sqrt{2}$. Итак,

$$x^4+16=\left(x^2+2\sqrt{2}x+4\right)\left(x^2-2\sqrt{2}x+4\right)$$

– разложение над полем действительных чисел.

Для того чтобы разложить данный многочлен над комплексными числами, решим уравнение $z^4=-16$ или $z^4=16\cdot e^{i(\pi+2\pi k)}$. Ясно, что $z_k=2e^{i\left(\frac{\pi}{4}+\frac{\pi k}{2}\right)}$ будут корнями. Все различные корни мы получим при $k=0,1,2,3$. Следовательно,

$$z_0=2e^{\frac{\pi}{4}i}=\sqrt{2}+i\sqrt{2}, z_1=2e^{\frac{3\pi i}{4}}=-\sqrt{2}+i\sqrt{2};\ z_2=2e^{\frac{5\pi i}{4}}=$$
$$=-\sqrt{2}-i\sqrt{2}=\overline{z_1};$$
$$z_3=2e^{\frac{7\pi i}{4}}=\sqrt{2}-i\sqrt{2}=\overline{z_0}.$$

Тогда

$$z^4 + 16 = (z - z_1)(z - z_4)(z - z_2)(z - z_3).$$

– разложение над комплексными числами. Легко вычислить

$(z - z_1)(z - z_4) = z^2 - 2\sqrt{2}z + 4;\ (z - z_2)(z - z_3) = z^2 + 2\sqrt{2z} + 4,$

и мы получаем другое решение задачи о разложении многочлена $x^4 + 16$ над полем действительных чисел.

В. Разложим многочлен $x^4 + 1$ над полями $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ и над полем $\mathbb{Z}_2$ из двух элементов

$\mathbb{C} : x^4 + 1 = \left(x - \frac{\sqrt{2}+\sqrt{2}i}{2}\right) \cdot \left(x - \frac{\sqrt{2}-\sqrt{2}i}{2}\right) \cdot \left(x + \frac{\sqrt{2}+\sqrt{2}i}{2}\right) \cdot \left(x + \frac{\sqrt{2}-\sqrt{2}i}{2}\right),$

$\mathbb{R} : x^4 + 1 = \left(x^2 - \sqrt{2}x + 1\right)(x^2 + \sqrt{2}x + 1),$

$\mathbb{Q} : x^4 + 1$ неразложим,

$\mathbb{Z}_2 : x^4 + 1 = (x + 1)^4.$

16. НЕМНОГО КОМБИНАТОРИКИ

16.1. Биномиальные коэффициенты

Так называются комбинаторно определяемые числа C_n^k – число способов выбора k предметов из n предметов. Здесь $0 \leq k \leq n$. Ясно, что $C_n^0 = 1$ и $C_n^1 = n$. Ясно также, что

$$C_n^k = C_n^{n-k}, \qquad (1)$$

ибо выбор k предметов означает автоматический «невыбор» оставшихся $n - k$ предметов. Перейдем к выводу основного рекуррентного соотношения между биномиальными коэффициентами. Пусть у нас имеется n предметов, составляющих множество A, среди которых фиксируем один предмет a^*. Все выборы k предметов из A, т.е. все подмножества B ⊆ A, содержащие k предметов, разбиваются на два класса: те, что содержат a^*, и те, что не содержат a^*. В первом классе C_{n-1}^{k-1} подмножеств (остается выбрать k – 1 предмет из A\ {a}), а во втором классе C_{n-1}^k подмножеств (все k предметов выбираем из множества A\{a}). Получаем

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k \text{ здесь } 1 \leq k \leq n - 1. \qquad (2)$$

Вместе с граничными условиями $C_n^0 = C_n^n = 1$ это дает способ вычисления всех чисел C_n^k. Соотношения (2) также представляют собой рекуррентные формулы, только более сложные, чем те, посред-

ством которых определялось сложение и умножение натуральных чисел. Получаем так называемый треугольник Паскаля

```
                1
              1   1
            1   2   1
          1   3   3   1
        1   4   6   4   1
      1   5   10  10  5   1
    1   6   15  20  15  6   1
..... .. .. .. .. .. .. .. .. .. .. .. .. .....
```

В этом треугольнике n-я строка сверху содержит числа C_n^k при k = 0, 1, 2 ,… , n. Любое число, кроме самых крайних слева и справа, равно сумме чисел, стоящих над ним (4 = 1 + 3, 6 = 3 + 3 и т.д.) Имеется и прямая, не рекуррентная формула для чисел C_n^k

$$C_n^k = \frac{n!}{k!\,(n-k)!}\,. \qquad (3)$$

Доказательство. Обозначим пока $B_n^k = \frac{n!}{k!(n-k)!}$. Имеем

$$B_n^0 = \frac{n!}{0!\,n!} = 1 = C_n^0;\;\; B_n^n = \frac{n!}{n!\,0!} = 1 = C_n^n.$$

Иными словами, краевые условия совпадают. Докажем, что числа B_n^k удовлетворяют рекуррентному соотношению (3).

$$B_{n-1}^k + B_{n-1}^{k-1} = \frac{(n-1)!}{k!\,(n-1-k)!} + \frac{(n-1)!}{(k-1)!\,(n-k)!}$$

$$= \frac{(n-1)!\,(n-k) + (n-1)!\,k}{k!\,(n-k)!} = \frac{n!}{k!\,(n-k)!} = B_n^k.$$

Теперь очень легко индукцией по n доказать, что имеет место равенство $C_n^k = B_n^k$ для всех допустимых k. Действительно, база индукции n = 1 проверяется прямым подсчетом. Предполагая далее верным равенство $C_n^k = B_n^k$ при всех $0 \le k \le n$ докажем равенство $C_{n+1}^k = B_{n+1}^k$ для всех $0 \le k \le n + 1$. Во-первых, это так для k = 0 и для $k = n + 1$ в силу совпадения граничных условий. Для остальных k воспользуемся рекуррентным соотношением

$$C_{n+1}^k = C_n^{k-1} + C_n^k = B_n^{k-1} + B_n^k = B_{n+1}^k.$$

Теорема 1 (бином Ньютона). Для любого натурального n имеет место равенство

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k =$$

$$= a^n + \frac{n}{1} a^{n-1} b + \frac{n(n-1)}{1 \cdot 2} a^{n-2} b^2 + \cdots + b^n. \qquad (4)$$

Доказательство. Раскрывая скобки в произведении $(a + b)\,(a + b)\ldots(a + b)$ (n раз), мы видим, что количество слагаемых, у которых степень по b равна k, а степень по a равна $n – k$, совпадает с числом выборов k предметов из n предметов, т.е. с C_n^k.

Возможен и другой способ доказательства бинома Ньютона – индукцией по степени n. Тогда следует применить рекуррентную формулу (3). В связи формулой бинома Ньютона числа C_n^k называют биномиальными коэффициентами.

16.2. Числа Фибоначчи

Так называют числа, рекуррентное определение которых задается равенствами

$$F_0 = 0; F_1 = 1;\ \ F_{n+2} = F_{n+1} + F_n. \qquad (5)$$

Первые двенадцать чисел Фибоначчи таковы:

$$0;\ 1;\ 1;\ 2;\ 3;\ 5;\ 8;\ 13;\ 21;\ 34;\ 55;\ 89$$

Образуем производящую функцию

$$F(z) := \sum_{n=0}^{+\infty} F_n z^n.$$

Тогда

$$F(z) + zF(z) = \sum_{n=1}^{+\infty} (F_n + F_{n-1}) z^n = \sum_{n=1}^{+\infty} F_{n+1} z^n = \frac{1}{z} \cdot \sum_{n=1}^{+\infty} F_{n+1} z^{n+1} =$$

$$= \frac{1}{z}\left(\sum_{n=0}^{+\infty} F_n z^n - F_1 z\right) = \frac{1}{z}(F(z) - z).$$

Отсюда $zF(z) + z^2 F(z) = F(z) - z$ и

$$F(z) = \frac{z}{1 - z - z^2}. \qquad (6)$$

В этой функции скрыта вся последовательность чисел Фибоначчи. В частности, $F_n = \frac{F^{(n)}(0)}{n!}$. Однако мы пойдем другим путем. Представим $1 - z - z^2$ в виде $(1 - \alpha\, z)(1 - \beta z)$. Тогда числа α, β обратны корням квадратного уравнения $z^2 + z - 1 = 0$, и тем самым есть корни уравнения $\zeta^2 - \zeta - 1 = 0$. Его корни суть

$$\phi := \frac{\sqrt{5}+1}{2} \approx 1.61803 - \text{золотое сечение и} - 1/\phi$$

Тогда, применяя формулу суммы геометрической прогрессии, получим

$$\frac{z}{1 - z - z^2} = \frac{z}{(1 - \phi\, z)\left(1 + \frac{z}{\phi}\right)} = \frac{1}{\sqrt{5}}\left(\frac{1}{1 - \phi z} - \frac{1}{1 + \frac{z}{\phi}}\right) =$$

$$= \sum_{n=0}^{+\infty} \frac{1}{\sqrt{5}}\left(\phi^n + \frac{(-1)^{n+1}}{\phi^n}\right) z^n.$$

Как итог получаем явную формулу

$$F_n = \frac{1}{\sqrt{5}}\left(\phi^n + \frac{(-1)^{n+1}}{\phi^n}\right) =$$

$$= \frac{1}{\sqrt{5}}\left(\left(\frac{\sqrt{5}+1}{2}\right)^n + (-1)^{n+1}\left(\frac{\sqrt{5}-1}{2}\right)^n\right). \qquad (7)$$

Системой счисления Фибоначчи называется представление натурального числа n в виде суммы чисел Фибоначчи

$$n = F_{k_1} + F_{k_2} + \cdots + F_{k_r}, \text{где } k_1 \gg k_2 \gg \cdots >> k_r \qquad (8)$$

(здесь и далее $m \gg k \overset{\text{опр}}{\Leftrightarrow} m \geq k + 1$).

Теорема 2. Представление вида (8) существует и единственно.

Доказательство. Используем «жадный» алгоритм представления. Выбираем k_1 максимальное такое, что $F_{k_1} \leq n$. Если здесь равенство, то разложение (8) построено. Иначе выбираем k_2 максимальное такое, что $F_{k_2} \leq n - F_{k_1}$ и т. д. Заметим, что $k_2 << k_1$ так как в противном случае $F_{k_1 - 1} \leq F_{k_2} \leq n - F_{k_1}$ и $F_{k_1+1} = F_{k_1} + F_{k_1-1} \leq n$ – противоречие с максимальностью k_1. Понятно, что этот процесс оборвется на конечном шаге.

Единственность. Из рекуррентного задания чисел Фибоначчи следует, что

$F_m = F_{m-1} + F_{m-2} = 2F_{m-2} + F_{m-3} = F_{m-2} + 2F_{m-3} + F_{m-4} = F_{m-2} + \\ + F_{m-3} + 2F_{m-4} + F_{m-5} = \cdots = F_{m-2} + F_{m-3} + \cdots + F_2 + 2F_1 = 1 + \\ + \sum_{k=1}^{m-2} F_k.$

Отсюда просто следует единственность числа k_1, а затем применяем индукцию к $n - F_{k_1}$.

17. АЛГЕБРА КВАТЕРНИОНОВ

Кватернионы были изобретены Гамильтоном в 1843 году (Вильям Роуэн Гамильтон (1805 – 1865) – ирландский математик). Это был первый пример конечномерной некоммутативной алгебры над полем действительных чисел, в которой каждый ненулевой элемент обратим (т. е. алгебры с делением, или тела). Как потом оказалось, это был и последний пример такой алгебры, ибо конечномерная алгебра с делением над $\mathbb{R}$ есть либо само поле $\mathbb{R}$, либо поле комплексных чисел $\mathbb{C}$, либо тело кватернионов $\mathbb{H}$ согласно теореме Фробениуса (см. [В], гл. 11, § 6, теорема 4). Произвольный элемент $q \in \mathbb{H}$ однозначно записывается в виде

$$q = a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k},$$

где $a_0, a_1, a_2, a_3 \in \mathbb{R}$. Если $a_0 = 0$, то такой кватернион называется чистым. Во-первых, превратим $\mathbb{H}$ в четырехмерное линейное пространство на полем $\mathbb{R}$, складывая кватернионы и умножая их на числа покомпонентно. Таблица умножения базисных элементов такова:

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1, \qquad \boldsymbol{ijk} = -1. \tag{1}$$

Из этих равенств получаем следствия:

$$\boldsymbol{ij} = \boldsymbol{k},\ \boldsymbol{jk} = \boldsymbol{i},\ \boldsymbol{ki} = \boldsymbol{j},\ \boldsymbol{ji} = -\boldsymbol{k},\ \boldsymbol{kj} = -\boldsymbol{i},\ \boldsymbol{ik} = -\boldsymbol{j}. \tag{2}$$

Так как умножение базисных элементов ассоциативно, то и $\mathbb{H}$ – ассоциативная алгебра.

Чистые кватернионы образуют подпространство $\boldsymbol{i}\mathbb{R} + \boldsymbol{j}\mathbb{R} + \boldsymbol{k}\mathbb{R}$, которое будем отождествлять с трехмерным линейным евклидовым пространством со стандартным базисом $\boldsymbol{i}$, $\boldsymbol{j}$, $\boldsymbol{k}$. Для вычисления результата умножения двух кватернионов используем скалярное и векторное произведения. Операцию скалярного произведения между векторами $\boldsymbol{a}$ и $\boldsymbol{b}$ придется обозначать, например как $\boldsymbol{a} * \boldsymbol{b}$, оставив $\boldsymbol{a} \cdot \boldsymbol{b}$ для обозначения произведения кватернионов. Итак, если даны

два кватерниона $q = a + \boldsymbol{a}$ и $t = b + \boldsymbol{b}$, где $\boldsymbol{a}, \boldsymbol{b}$ – чистые кватернионы, а a, b – числа, то можно убедиться, что

$$q \cdot t = (a + \boldsymbol{a})(b + \boldsymbol{b}) = (ab - \boldsymbol{a} * \boldsymbol{b}) + (a\boldsymbol{b} + b\boldsymbol{a} + \boldsymbol{a} \times \boldsymbol{b}). \quad (3)$$

Записывая q и t более подробно и вспоминая записи скалярного и векторного произведений через координаты, получим:

$$(a_0 + a_1\boldsymbol{i} + a_2\boldsymbol{j} + a_3\boldsymbol{k})(b_0 + b_1\boldsymbol{i} + b_2\boldsymbol{j} + b_3\boldsymbol{k}) =$$
$$= (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + (a_0b_1 + b_0a_1 + a_2b_3 - a_3b_2)\boldsymbol{i} +$$
$$+(a_0b_2 + b_0a_2 + a_3b_1 - a_1b_3)\boldsymbol{j} + (a_0b_3 + b_0a_3 + a_1b_2 - a_2b_1)\boldsymbol{k}.$$

Кватернион $a - \boldsymbol{a}$ назовем сопряженным к кватерниону $q = a + \boldsymbol{a}$ и будем его обозначать $\bar{q}$. Нетрудно проверить, что

$$q\,\bar{q} = \bar{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

и поэтому $q\,\bar{q} = 0$ тогда и только тогда, когда $q = 0$. Величина $q\,\bar{q}$ называется нормой кватерниона q и обозначается $\|q\|$, а арифметический корень из нормы называется модулем кватерниона q и обозначается $|q|$. Имеет место следующее утверждение

Теорема. Множество кватернионов относительно определенных выше операций сложения и умножения образует алгебру с делением над полем действительных чисел. Каждый ненулевой кватернион q имеет обратный $q^{-1} = \frac{1}{\|q\|}\bar{q}$.

Уже отмечалось, что алгебра кватернионов ассоциативна. Она не коммутативна, так как, например, $\boldsymbol{ij} \neq \boldsymbol{ji}$. Проверим теперь, что кватернион $\frac{1}{\|q\|}\bar{q}$ обратен к ненулевому кватерниону q:

$$q \cdot \frac{1}{\|q\|}\bar{q} = \frac{q\bar{q}}{\|q\|} = \frac{\|q\|}{\|q\|} = 1.$$

Отображение $\mathbb{C} \to \mathbb{H}$ $(x + iy \to x + y\boldsymbol{i} + 0\boldsymbol{j} + 0\boldsymbol{k})$ будет вложением поля комплексных чисел в алгебру кватернионов. С таким же успехом подходят для вложения отображения $x + iy \to x + y\boldsymbol{j}$ и $x + iy \to x + y\boldsymbol{k}$. Однако $\mathbb{H}$ не является алгеброй над полем комплексных чисел, ибо "мнимые единицы" $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ не лежат в центре $\mathbb{H}$, т.е. не коммутируют с каждым элементом алгебры кватернионов.

Пусть $u = a + \boldsymbol{a}$ – ненулевой кватернион. Отображение сопряжения

$$r_u: h \to u^{-1}hu, \qquad h \in \mathbb{H}$$

есть автоморфизм алгебры кватернионов. Это означает, что r_u – биекция (у него есть обратное отображение $r_{u^{-1}}$) и $r_u(h_1 + h_2) = r_u(h_1) + r_u(h_2)$; $r_u(h_1h_2) = r_u(h_1)r_u(h_2)$ для любых кватернионов h_1, h_2. Проверим, что

$$r_u(\boldsymbol{i}\mathbb{R} + \boldsymbol{j}\mathbb{R} + \boldsymbol{k}\mathbb{R}) = \boldsymbol{i}\mathbb{R} + \boldsymbol{j}\mathbb{R} + \boldsymbol{k}\mathbb{R}.$$

Достаточно установить, что $r_u(\boldsymbol{i}) \in \boldsymbol{i}\mathbb{R} + \boldsymbol{j}\mathbb{R} + \boldsymbol{k}\mathbb{R}$:

$$r_u(\boldsymbol{i}) = \frac{1}{\|u\|} \cdot (a - \boldsymbol{a})\boldsymbol{i}(a + \boldsymbol{a}) = \frac{1}{\|u\|}(a - \boldsymbol{a})\left(-a_x + a\boldsymbol{i} - a_z\boldsymbol{j} + a_y\boldsymbol{k}\right) =$$

$$= \frac{1}{\|u\|}\Big(-aa_x + a_x a - a_y a_z + a_z a_y + a_x\boldsymbol{a} + a^2\boldsymbol{i} - aa_z\boldsymbol{j}$$

$$+ aa_y\boldsymbol{k} - \boldsymbol{a} \times \left(a\boldsymbol{i} - a_z\boldsymbol{j} + a_y\boldsymbol{k}\right)\Big) =$$

$$= \frac{1}{\|u\|}\left(a_x\boldsymbol{a} + a^2\boldsymbol{i} - aa_z\boldsymbol{j} + aa_y\boldsymbol{k} - \boldsymbol{a} \times \left(a\boldsymbol{i} - a_z\boldsymbol{j} + a_y\boldsymbol{k}\right)\right) \in$$

$$\in \boldsymbol{i}\mathbb{R} + \boldsymbol{j}\mathbb{R} + \boldsymbol{k}\mathbb{R}$$

Далее, $\|r_u(\boldsymbol{h})\| = \|h\|$, ибо норма произведения равна произведению норм (прямая проверка !), следовательно, это линейное преобразование пространства $\boldsymbol{i}\mathbb{R} + \boldsymbol{j}\mathbb{R} + \boldsymbol{k}\mathbb{R}$ ортогонально. Так как $r_u(\boldsymbol{a}) = \boldsymbol{a}$, то преобразование сопряжения r_u есть поворот на угол β_u относительно вектора $\boldsymbol{a}$. Как найти угол β_u? Пусть вектор $\boldsymbol{b}$ перпендикулярен вектору $\boldsymbol{a}$. Тогда

$$r_u(\boldsymbol{b}) = \frac{1}{\|u\|} \cdot (a - \boldsymbol{a})\boldsymbol{b}(a + \boldsymbol{a}) = \frac{1}{\|u\|} \cdot (a - \boldsymbol{a})(-\boldsymbol{a} * \boldsymbol{b} + \boldsymbol{b}a + \boldsymbol{b} \times \boldsymbol{a}) =$$

$$= \frac{1}{\|u\|} \cdot \left(a^2\boldsymbol{b} + a\,\boldsymbol{b} \times \boldsymbol{a} - a\,\boldsymbol{a} \times \boldsymbol{b} - \boldsymbol{a} \times (\boldsymbol{b} \times \boldsymbol{a})\right) =$$

$$= \frac{1}{\|u\|} \cdot (a^2\boldsymbol{b} - \boldsymbol{b} - 2a\,\boldsymbol{a} \times \boldsymbol{b}).$$

Пусть $\boldsymbol{a}, \boldsymbol{b}$ – вектора единичной длины. Тогда на плоскости $\boldsymbol{b}\mathbb{R} + (\boldsymbol{a} \times \boldsymbol{b})\mathbb{R}$ в базисе $(\boldsymbol{b}, \boldsymbol{a} \times \boldsymbol{b})$ поворот, индуцированный сопряжением, задается матрицей

$$\frac{1}{a^2 + 1} \cdot \begin{pmatrix} a^2 - 1 & 2a \\ -2a & a^2 - 1 \end{pmatrix}. \tag{4}$$

Отсюда следует, что

$$\cos\beta_u = \frac{a^2 - 1}{a^2 + 1}; \sin\beta_u = \frac{2a}{a^2 + 1}. \tag{5}$$

Пример. 1) $u = \boldsymbol{j}, u^{-1} = -\boldsymbol{j}$ **и** $\boldsymbol{r_u}(\boldsymbol{i}) = -\boldsymbol{jij} = -\boldsymbol{jk} = -\boldsymbol{i}$ – поворот на 180°. Это же следует из (5), в котором полагаем $a = 0$.

2) $u = 1 + \boldsymbol{j}, u^{-1} = \frac{1}{2}(1 - j)$ и

$$r_u(i) = \frac{1}{2}(1 - j)i(1 + j) = \frac{1}{2}(1 - j)(i + k) = \frac{1}{2}(i + k + k - i) = k$$

– поворот на угол 90°. Это следует также из (5), в котором полагаем $a = 1$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. [БН] *Бугров, Я. С.* Элементы линейной алгебры и аналитической геометрии / Я. С. Бугров, С. М. Никольский. – М. : Наука, 1980. – 176 с.

2. [НБ] *Бурбаки, Н.* Теория множеств / Н. Бурбаки. – М. : Мир, 1965. – 455 с.

3. [В]. *Винберг, Э. Б.* Курс алгебры / Э. Б. Винберг. – 3-е изд., перераб. и доп. – М. : Факториал Пресс, 2002. – 544 с.

4. [ДД] *Дубровина, Т. В.* Алгебра и геометрия / Т. В. Дубровина, Н. И. Дубровин. – Владимир : Изд-во ВлГУ, 2002. – 144 с.

5. [Д] *Дубровин, Н. И.* Конспект лекций по алгебре : учеб. пособие / Н. И. Дубровин. – Владимир : Изд-во ВлГУ, 1997. – 60 с.

6. [К] *Кострикин, А. И.* Введение в алгебру / А. И. Кострикин. – М. : Наука, 1977. – 495 с.

7. [КМ]. *Он же.* Линейная алгебра и геометрия / А. И. Кострикин, Ю. И. Манин. – М. : Изд-во МГУ, 1980. – 320 с.

8. [Л] *Ленг, С.* Математические беседы для студентов. Регулярная и хаотическая динамика / С. Ленг. – М. : Наука, 2000. – 159 с.

9. [КС] *Кантор, Н. Л.* Гиперкомплексные числа / Н. Л. Кантор, А. С. Солодовников. – М. : Наука, 1973. – 144 с.

Учебное издание

ДУБРОВИН Николай Иванович

ФУНДАМЕНТАЛЬНАЯ И КОМПЬЮТЕРНАЯ АЛГЕБРА

Учебное пособие

Подписано в печать 06.05.14.
Формат 60×84/16. Усл. печ. л. 5,11. Тираж 50 экз.
Заказ
Издательство
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.