Министерство образования Российской Федерации

Санкт-Петербургский государственный институт точной механики и оптики (технический университет)

А. Г. Коробейников

Математические основы криптографии

Учебное пособие

Санкт-Петербург 2002

УДК 511
Коробейников А. Г. Математические основы криптографии. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002. 41 с

В учебном пособии представлен материал, необходимый для начального введения в теорию криптографичесих алгоритмов. Это в первую очередь теория групп, теория колец, теория полей и прикладная теория чисел. В каждом разделе рассмотрены примеры на соответствующие темы.

Предназначено для студентов, обучающихся по специальности 0754 "Комплексная защита объектов информатизации".

Илл. – 3, список литературы – 9 наим.

ВВЕДЕНИЕ

Математические методы, используемые в криптографии, невозможно успешно освоить без знания таких алгебраических структур, как группы, кольца и поля. Поэтому знание и умение работать с этими объектами является необходимым условием для подготовки специалистов в области защиты информации.

В силу присущей методам криптографии специфики, большой интерес представляет множество целых чисел и различные алгебраические структуры на его базе. Поэтому основное внимание будет уделено работе с целыми числами.

В первой части введены базовые определения и понятия теории множеств, рассмотрено понятие "отображение" и определены бинарные отношения.

Во второй части изучаются основные свойства, присущие целым числам.

В третьей части рассмотрены различные множества с последующим определением на них бинарных операций. Определены понятия полугрупп и моноидов.

В четвертой части определены и рассмотрены основные положения теории групп. Кратко изучены симметрическая и знакопеременная группа.

В пятой части рассмотрены основные правила взаимодействия между группами.

В шестой части определено понятие математического кольца, рассмотрены общие свойства колец. Построено кольцо классов вычетов. Определены правила отображений из одного кольца в другое. Рассмотрены различные типы колец.

В седьмой части определено понятие математического поля, рассмотрены его общие свойства. Кратко изучены поля Галуа.

В восьмой части определено понятие кольца многочленов, рассмотрены его общие свойства, получены правила разложения в кольце многочленов и признаки факториальности колец, рассмотрен критерий неприводимости многочлена.

Каждая часть сопровождается соответствующими примерами.

1. МНОЖЕСТВА И ОТОБРАЖЕНИЯ

1.1. МНОЖЕСТВА

Математическое понятие *множество* является одним из центральных во всей математике. Оно определяется в зависимости от задач. Примером может служить группа аксиом, известная как система NGB (по имени авторов – Джона фон Нейман, Поля Бернайса, Курта Геделя). Главная идея, положенная в основу NGB, заключается в различении понятий множества и класса. Все объекты NGB являются классами. Класс соответствует нашему интуитивному пониманию совокупности. Множеством являются те классы, которые являются элементами других классов. Классы, не являющиеся множествами, называются *собственными классами*.

Существует другая группа аксиом – система ZF (по имени авторов – Эрнста Цермело и Абрахама Френкеля). Это теория *построимых множеств*, т.е. множество строится из некоторых простых, с помощью таких операций, как пересечение, объединение, дополнение и т.д.

Мы будем понимать под множеством любую совокупность объектов, называемых *элементами* множества. Множества с конечным числом различных элементов могут быть описаны путем явного перечисления всех элементов. Обычно эти элементы заключаются в фигурные скобки. Например, {16,32,64} – множество степеней двойки, заключенных между 10 и 100. Множество обозначается прописной буквой какого-либо алфавита, а его элементы – строчными буквами того же или другого алфавита. Для некоторых особо важных множеств приняты стандартные обозначения, которых следует придерживаться. Так, буквами **N, Z, Q, R** обозначают соответственно множество натуральных чисел, множество целых чисел, множество рациональных чисел и множество вещественных чисел. При заданном множестве **S** *включение* $\mathbf{a}\in\mathbf{S}$ указывает на то, что **a** – элемент множества. В противном случае записывают $\mathbf{a}\notin\mathbf{S}$. Говорят, что **S** – *подмножество* **T** или $\mathbf{S}\subset\mathbf{T}$ (**S** содержится в **T**), когда имеет место импликация:

$$\mathbf{x}\in\mathbf{S},\ \forall\mathbf{x} \Rightarrow \mathbf{x}\in\mathbf{T}.$$

Два множества совпадают (или равны), если у них одни и те же элементы. Символически это записывается в виде:

$$\mathbf{S}=\mathbf{T} \Leftrightarrow \mathbf{S}\subset\mathbf{T} \text{ и } \mathbf{T}\subset\mathbf{S}.$$

Пустое множество $\varnothing$, т.е. множество, не содержащее ни одного элемента, по определению входит в число подмножеств любого множества.

Под *пересечением* двух множеств **S** и **T** понимают множество

$$\mathbf{S}\cap\mathbf{T}=\{\mathbf{x}|\ \mathbf{x}\in\mathbf{S} \text{ и } \mathbf{x}\in\mathbf{T}\},$$

а под их объединением – множество

$$\mathbf{S}\cup\mathbf{T}=\{\mathbf{x}|\ \mathbf{x}\in\mathbf{S} \text{ или } \mathbf{x}\in\mathbf{T}\}.$$

Пусть **X** и **Y** – произвольные множества. Пару (x,y) элементов $\mathbf{x\in X,\ y\in Y}$, взятых в данном порядке, называют *упорядоченной парой*, считая при этом, что $(x_1,y_1)=(x_2,y_2)$ тогда и только тогда, когда $x_1=x_2$, $y_1=y_2$. *Декартовым произведением* двух множеств **X** и **Y** называется множество всех упорядоченных пар (x,y):

$$\mathbf{X\times Y=\{(x,y)|x\in X,\ y\in Y\}}.$$

Пример 1. Пусть, **R** – множество всех вещественных чисел. Тогда декартов квадрат $\mathbf{R^2=R\times R}$ есть просто множество всех декартовых координат на плоскости относительно заданных координатных осей. ♦

Аналогично можно ввести декартово произведение $\mathbf{X_1\times X_2\times X_3}$ трех, четырех и т.д. множеств. При $\mathbf{X_1=X_2=X_3=\ldots=X_k=X}$ сокращенно пишут $\mathbf{X^k=X_1\times X_2\times X_3\times\ldots\times X_k}$ и говорят о k-й декартовой степени множества **X**. Элементами $\mathbf{X^k}$ являются последовательности, или строки $(x_1,x_2,\ldots x_k)$ длины k.

1.2. ОТОБРАЖЕНИЯ

Понятие *отображения* или *функции* также является одним из центральных в математике. При заданных **X** и **Y** отображение **f** с *областью определения* **X** и *областью значений* **Y** сопоставляет каждому элементу $\mathbf{x\in X}$ элемент $\mathbf{f(x)\in Y}$. Символически отображение записывается в виде $\mathbf{f:X\to Y}$. *Образом* при отображении **f** называется множество всех элементов вида **f(x)**:

$$\mathrm{Im}\ \mathbf{f=\{f(x)|x\in X\}=f(X)\subset Y}.$$

Множество

$$\mathbf{f^{-1}(y)=\{x\in X|f(x)=y\}}$$

называется *прообразом* элемента $\mathbf{y\in Y}$.

Отображение $\mathbf{f:X\to Y}$ называется *сюръективным,* или *отображением на*, когда $\mathrm{Im}\ \mathbf{f=Y}$.

Отображение $\mathbf{f:X\to Y}$ называется *инъективным,* когда из $\mathbf{x\neq x'}$ следует $\mathbf{f(x)\neq f(x')}$.

Отображение $\mathbf{f:X\to Y}$ называется *биективным,* или взаимно однозначным, если оно одновременно сюръективно и инъективно.

Равенство **f=g** двух отображений означает по определению, что их соответствующие области совпадают.

Пример 2. Пусть $\mathbf{R_+}$ – множество положительных вещественных чисел. Тогда отображения $\mathbf{f:R\to R}$, $\mathbf{g:R\to R_+}$, $\mathbf{h:R_+\to R_+}$, определенные одним и тем же правилом $\mathbf{x\to x^2}$, все различны: **f** – ни сюръективно, ни инъективно, **g** – сюръективно, но не инъективно, а отображение **h** – биективно. Таким образом, задание области определения и области значений – важная часть определения отображения. ♦

Единичным или *тождественным* отображением $\mathbf{e_X: X \to X}$ называется отображение, переводящее каждый элемент $\mathbf{x \in X}$ в себя.

Отображение $\mathbf{f^{-1}}$ является обратным к **f**, если $\mathbf{f(x)=y \Leftrightarrow f^{-1}(y)=x}$.

1.3. БИНАРНЫЕ ОТНОШЕНИЯ

Для любых двух множеств **X** и **Y** всякое подмножество $\mathbf{O \subset X \times Y}$ называется *бинарным отношением* между **X** и **Y** (или просто на **X**, если **X=Y**).

Бинарное отношение ~ на **X** называется отношением эквивалентности, если для всех $\mathbf{x}$, $\mathbf{x_1}$, $\mathbf{x_2 \in X}$ выполнены условия:

i. $\mathbf{x \sim x}$ (рефлексивность);
ii. $\mathbf{x \sim x_1 \Rightarrow x_1 \sim x}$ (симметричность);
iii. $\mathbf{x \sim x_1}$, $\mathbf{x_1 \sim x_2 \Rightarrow x_2 \sim x}$ (транзитивность).

Подмножество

$$\mathbf{H=\{x' \in X | x' \sim x\} \subset X}$$

всех элементов, эквивалентных данному **x**, называется классом эквивалентности, содержащим **x**.

Так как $\mathbf{x \sim x}$ (i), то $\mathbf{x' \in H}$. Любой элемент $\mathbf{x' \in H}$ называется *представителем класса* **H**.

Справедливо следующая теорема.

Теорема 1. Множество классов эквивалентности по отношению ~ является разбиением множества **X** в том смысле, что **X** является объединением непересекающихся подмножеств.

Доказательство. В самом деле, так как $\mathbf{x \in H}$, то $\mathbf{X=\cup H_i}$. Далее, класс **H** однозначно определяется любым своим представителем, т.е. $\mathbf{H_i=H_j \Leftrightarrow\ x_i \sim x_j}$. В одну сторону: $\mathbf{x_i \sim x_j}$ и $\mathbf{x \in H_i \Rightarrow x \sim x_i \Rightarrow x \sim x_j \Rightarrow x \in H_j \Rightarrow H_i \subset H_j}$. Но $\mathbf{x_i \sim x_j \Rightarrow x_j \sim x_i}$ (ii). Поэтому выполнено и обратное включение $\mathbf{H_j \subset H_i}$. Значит $\mathbf{H_j=H_i}$. В другую сторону: так как $\mathbf{x \in H}$, то $\mathbf{H_i=H \Rightarrow x \in H_i \Rightarrow x \sim x_i}$.

Если теперь $\mathbf{H_j \cap H_i \neq \varnothing}$ и $\mathbf{x \in H_j \cap H_i}$, то $\mathbf{x \sim x_i}$ и $\mathbf{x \sim x_j}$, откуда в силу транзитивности (iii) имеем $\mathbf{x_i \sim x_j}$ и $\mathbf{H_j=H_i}$. Значит, различные классы не пересекаются. Теорема доказана. ♦

Пример 3. Пусть $\mathbf{V=R^2}$ – вещественная плоскость с прямоугольной системой координат. Тогда, взяв за свойство ~ принадлежность точек **P**, $\mathbf{P' \in V}$ одной горизонтальной прямой, получим отношение эквивалентности с классами – горизонтальными прямыми (рис. 1).

Гиперболы $\mathbf{\Gamma}_p$ (рис. 2) вида $\boldsymbol{xy=p>0}$ определяют отношение эквивалентности в области $\mathbf{V_+ \subset V}$ точек $\mathbf{P}(x,y)$ с координатами $\boldsymbol{x>0}$, $\boldsymbol{y>0}$.

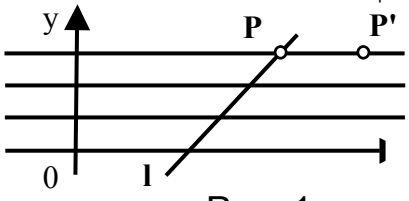

Рис. 1.

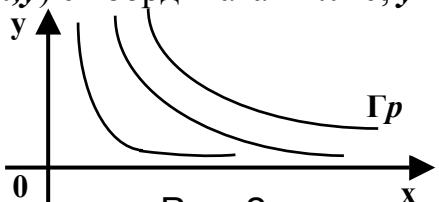

Рис. 2.

2. ОСНОВНЫЕ СВОЙСТВА ЦЕЛЫХ ЧИСЕЛ

Задачей этой части является краткое описание тех простейших свойств делимости целых чисел, на которые по разным поводам будем ссылаться в дальнейшем.

2.1. ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

Целое число s называется *делителем* (или *множителем*) целого числа n, если $n=st$ для некоторого $t\in\mathbf{Z}$. В свою очередь n называется *кратным* s. Делимость n на s обозначается символом |. Делимость – транзитивное свойство на $\mathbf{Z}$. Целое число p, делители которого исчерпываются числами $\pm p$, ± 1 (*несобственные делители*), называется *простым*. Обычно в качестве простых берутся положительные простые числа > 1.

Фундаментальную роль простых чисел вскрывает так называемая основная теорема арифметики.

Теорема 2. Каждое положительное целое число $n\neq 1$ может быть записано в виде произведения простых чисел: $n=p_1p_2p_3\ldots p_S$. Эта запись единственна с точностью до порядка сомножителей.(Без доказательства)♦

Собрав вместе одинаковые простые множители и изменив обозначения, получим запись n в виде: $n=p_1^{1}p_2^{2}p_3^{3}\ldots p_S^{S}$.

Теорема 3 (Евклида) гласит, что множество

$$\mathbf{P}=\{2,3,5,11,13,\ldots\}$$

всех простых чисел бесконечно. Действительно, если бы существовало бы лишь конечное число простых чисел, например $p_1p_2\ldots p_k$, то по основной теореме число $c=p_1p_2\ldots p_k+1$ делилось бы по крайней мере на одно из p_i. Без ограничения общности считаем $c=p_ic'$. Тогда $p_1(c'-p_2\ldots p_k)=1$, а это невозможно, поскольку делителями единицы в $\mathbf{Z}$ являются лишь ± 1, что и требовалось доказать. ♦

2.2. АЛГОРИТМ ДЕЛЕНИЯ В Z

При заданных $a,b\in\mathbf{Z}$, $b>0$, всегда найдутся $q,r\in\mathbf{Z}$ такие, что

$$a=bq+r,\quad 0\le r<b$$

(если считать лишь $b\neq 0$, то будет выполнено неравенство $0\le r<|b|$).

В самом деле, множество $\mathbf{S}=\{a-bs\,|\,s\in\mathbf{Z}, a-bs\ge 0\}$, очевидно, не пусто (например, $a-b(-a^2)\ge 0$). Стало быть, $\mathbf{S}$ содержит наименьший элемент. Обозначим его $r=a-bq$. По условию $r\ge 0$. Предположив $r\ge b$, мы получили бы элемент $r-b=a-b(q+1)\in\mathbf{S}$, меньший, чем r. Это противоречие устраняется лишь при $r<b$.

Проведенное несложное рассуждение дает алгоритм для нахождения частного b и остатка r за конечное число шагов.

Алгоритм деления в $\mathbf{Z}$ можно также использовать для определения *наибольшего общего делителя* (НОД), известного из школьного курса математики. Именно, при заданных целых числах n, m, одновременно не равных нулю, положим

$$\mathbf{J}=\{nu+mv|u,v\in\mathbf{Z}\}.$$

Выберем в **J** наименьший положительный элемент $d=nu_0+mv_0$. Используя алгоритм деления, запишем $n=dq+r$, $0\le r<d$. Ввиду выбора d включение

$$r=n-dq=n-(nu_0+mv_0)q=n(1-u_0q)+m(-v_0q)\in\mathbf{J}$$

влечет равенство $r=0$. Стало быть, $d|n$. Аналогично доказывается, что $d|m$.

Пусть теперь d' – любой делитель чисел n и m. Тогда

$$d'|n,\ d'|m\ \Rightarrow d'|nu_0,\ d'|mv_0\ \Rightarrow d'|(nu_0+mv_0)\ \Rightarrow d'|d.$$

Итак, d обладает всеми свойствами НОД, и поэтому $d=$НОД$(|n,m)$. Мы пришли к следующему утверждению.

Наибольший общий делитель двух целых чисел n,m, *не равных одновременно нулю, всегда записывается в виде*

$$\text{НОД}(n,m)=nu+mv;\ u,v\in\mathbf{Z}.$$

В частности, целые числа n,m *взаимно просты тогда и только тогда, когда* $nu+mv=1$ *при некоторых* $u,v\in\mathbf{Z}$.

Для доказательства этого утверждения нужно взять любой положительный элемент из множества **J**, а затем уменьшать его при помощи алгоритма деления до тех пор, пока не получится наименьший элемент, который и будет наибольшим общим делителем.

В дальнейшем нам понадобится так называемая *функция Эйлера* ($\varphi:\mathbf{N}\to\mathbf{N}$). Она определяется следующим образом. Если натуральное число n делится в точности на k различных простых чисел $p_1,p_2,\dots p_k$, то количество чисел, меньших n и взаимно простых с n, равно

$$\varphi(n)=n(1-1/p_1)(1-1/p_2)\dots(1-1/p_k).$$

Пример 4. $n=1155$; $p_1=3$; $p_2=5$; $p_3=7$; $p_4=11$.

$\varphi(n)=1155(1-1/3)(1-1/5)(1-1/7)(1-1/11)=480$. ♦

3. МНОЖЕСТВА С АЛГЕБРАИЧЕСКИМИ ОПЕРАЦИЯМИ

3.1. БИНАРНЫЕ ОПЕРАЦИИ

Пусть **X** – произвольное множество. *Бинарной алгебраической операцией* (или *законом композиции*) на **X** называется произвольное (но фиксированное) отображение $\tau:\mathbf{X}\times\mathbf{X}\to\mathbf{X}$ декартова квадрата $\mathbf{X}^2=\mathbf{X}\times\mathbf{X}$ в **X**. Таким образом, любой упорядоченной паре (a,b) элементов $a,b\in\mathbf{X}$ ставится в соответствие определенный элемент $\tau(a,b)$ того же множества **X**. Иногда вместо $\tau(a,b)$ пишут $a\tau b$, а еще чаще бинарную операцию на **X** обозначают каким-нибудь специальным символом: *, °, · или +.

На **X** может быть задано, вообще говоря, много различных операций. Желая выделить одну из них, используют скобки (**X**,*) и говорят, что операция * определяет на **X** *алгебраическую структуру* или что (**X**,*) – *алгебраическая система*.

Пример 5. В множестве **Z** целых чисел, помимо естественных операций +, · (сложения и умножения), легко указать получающиеся при помощи + (или -) и · "производные" операции: $n\circ m=n+m-nm$, $n*m=-n-m$ и т.д. Мы приходим к различным алгебраическим структурам (**Z**,+),(**Z**,-), (**Z**,°) и (**Z**,*). ♦

Наряду с бинарными алгебраическими операциями не лишены интереса гораздно более общие n-арные операции (унарные при $n=1$, тернарные при $n=3$ и т.д.), равно как и их комбинации. Связанные с ними алгебраические структуры составляют специальную теорию универсальных алгебр.

В направлении конструирования разных бинарных операций на множестве **X** также, очевидно, открывается неограниченный простор фантазии. Но задача изучения произвольных алгебраических структур слишком обща, чтобы она представляла реальную ценность. По этой причине ее рассматривают при различных естественных ограничениях.

3.2. ПОЛУГРУППЫ И МОНОИДЫ

Бинарная операция * на множестве **X** называется *ассоциативной*, если $(a*b)*c=a*(b*c)$ всех $a,b,c\in\mathbf{X}$. Она также называется *коммутативной*, если $a*b=b*a$. Те же названия присваиваются и соответствующей алгебраической структуре (**X**,*). Требования ассоциативности и коммутативности независимы. В самом деле, операция * на **Z**, заданная правилом $n*m=-n-m$, очевидно, коммутативна. Но $(1*2)*3=(-1-2)*3=-(1-2)-1=0\neq 1*(1*3)$. Так что условие ассоциативности не выполняется.

Элемент $e \in \mathbf{X}$ называется *единичным* (или *нейтральным*) относительно рассматриваемой бинарной операции *, если $e*x=x*e$ для всех $x \in \mathbf{X}$. Если e' – еще один единичный элемент, то, как следует из определения, $e'=e'*e=e$. Следовательно, в алгебраической структуре $(\mathbf{X},*)$ может существовать не более одного единичного элемента.

Множество $\mathbf{X}$ с заданной на нем бинарной ассоциативной операций называется *полугруппой*. Полугруппу с единичным (нейтральным) элементом принято называть *моноидом*.

Элемент a моноида $(\mathbf{M},\cdot,e)$ называется *обратимым*, если найдется элемент $b \in \mathbf{M}$, для которого $a \cdot b = b \cdot a = e$ (понятно, что элемент b тоже обратим). Если еще и $a \cdot b' = e = b' \cdot a$, то $b' = e \cdot b' = (b \cdot a) \cdot b' = b \cdot (a \cdot b') = b \cdot e = b$. Это дает основание говорить просто об *обратном элементе* a^{-1} к (обратимому) элементу $a \in \mathbf{M}: a \cdot a^{-1} = e = a^{-1} \cdot a$. Разумеется, $(a^{-1})^{-1} = a$.

Пример 6. Пусть Ω – произвольное множество, $\mathbf{M}(\Omega)$ – множество всех отображений Ω в себя. Тогда $(\mathbf{M}(\Omega),\bullet,e_\Omega)$ – моноид, где $\bullet$ – естественная композиция отображений, а e_Ω – тождественное отображение. ♦

Пример 7. Пусть $\mathbf{M_n}(\mathbf{R})$ – множество квадратных матриц n×n с вещественными коэффициентами. Тогда $(\mathbf{M_n}(\mathbf{R}),*,\mathbf{E})$ – моноид, где $*$ – операция умножения матриц, $\mathbf{E}$ – единичная матрица n×n. ♦

Пример 8. Пусть $n\mathbf{Z}=\{nm \mid m \in \mathbf{Z}\}$ – множество целых чисел, делящихся на n. Тогда $(n\mathbf{Z},+,0)$ – коммутативный моноид, а $(n\mathbf{Z},\cdot)$ – коммутативная полугруппа без единицы ($n > 1$). ♦

4. ГРУППЫ

4.1. ПОНЯТИЕ ГРУППЫ

Моноид **G**, все элементы которого обратимы, называется *группой*. Другими словами, предполагается выполнение следующих аксиом:

(**G**1) на множестве **G** определена бинарная операция $(x,y)\to xy$;

(**G**2) операция ассоциативна: $(xy)z=x(yz)$ для всех $x,y,z\in\mathbf{G}$;

(**G3**) **G** обладает нейтральным (единичным) элементом e: $e*x=x*e$ для всех $x\in\mathbf{G}$;

(**G4**) для каждого элемента $x\in\mathbf{G}$ существует обратный x^{-1}: $x^{-1}*x = x*x^{-1}=e$.

Для обозначения числа элементов в группе **G** (точнее, мощности группы) используются равноправные символы Card**G**, |**G**| и (**G**:e).

Пример 9. GL(n,**R**) – множество квадратных матриц n×n с вещественными коэффициентами с ненулевым определителем. Тогда **GL**(n,**R**) – полная линейная группа по операции умножения матриц. ♦

Пример 10. Используя рациональные числа вместо вещественных, мы приходим к полной линейной группе **GL**(n,**Q**) степени n над **Q**. ♦

Подмножество $\mathbf{H}\subset\mathbf{G}$ называется подгруппой **G**, если $e\in\mathbf{H}$; $h_1,h_2\in\mathbf{H}\Rightarrow h_1h_2\in\mathbf{H}$ и $h\in\mathbf{H}\Rightarrow h^{-1}\in\mathbf{H}$. Подгруппа $\mathbf{H}\subset\mathbf{G}$ – собственная, если $\mathbf{H}\neq e$ и $\mathbf{H}\neq\mathbf{G}$.

Пример 11. Рассмотрим в группе **GL**(n,**R**) подмножество **SL**(n,**R**) матриц с определителем, равным 1:

$$\mathbf{SL}(n,\mathbf{R})=\{\mathbf{A}\in\mathbf{GL}(n,\mathbf{R})|\det\mathbf{A}=1\}.$$

Очевидно, что $\mathbf{E}\in\mathbf{SL}(n,\mathbf{R})$. Кроме того, $\det\mathbf{A}=1$, $\det\mathbf{B}=1\Rightarrow\det\mathbf{AB}=1$ и $\det\mathbf{A}^{-1}=1$. Поэтому **SL**(*n*,**R**) – подгруппа в **GL**(*n*,**R**). Она носит название *специальной линейной группы степени* ***n*** над **R**. Ее называют еще *унимодулярной*. ♦

Пример 12. Подгруппа **SL**(*n*, **R**) содержит подгруппу **SL**(*n*, **Q**), которая, в свою очередь, содержит интересную подгруппу **SL**(*n*,**Z**) целочисленных матриц с единичным определителем. ♦

Пример 13. Положим в примерах 9 и 10 $n=1$. Тогда мы приходим к мультипликативным группам $\mathbf{R}^*=\mathbf{R}\backslash\{0\}=\mathbf{GL}(1,\mathbf{R})$ и $\mathbf{Q}^*=\mathbf{Q}\backslash\{0\}=\mathbf{GL}(1,\mathbf{Q})$ вещественных и рациональных чисел. Эти группы, очевидно, бесконечны. ♦

Пример 14. Так как в (**Z**,*,1) обратимыми элементами являются только –1 и 1, то $\mathbf{GL}(1,\mathbf{Z})=\{\pm1\}$. ♦

Пример 15. SL(1, **R**)=**SL**(1, **Q**)=**SL**(1,**Z**)=1. Но уже при $n=2$ группа **SL**(2,**Z**) бесконечна. Ей принадлежат, в частности, все матрицы

$$\begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix},\begin{pmatrix}1 & 0\\ m & 1\end{pmatrix},\begin{pmatrix}m & m-1\\ 1 & 1\end{pmatrix},\ m\in\mathbf{Z}.$$

♦

4.2. СИММЕТРИЧЕСКАЯ И ЗНАКОПЕРЕМЕННАЯ ГРУППЫ

Пусть Ω – конечное множество из n элементов. Поскольку природа этих элементов для нас несущественна, удобно считать, что $\Omega=\{1,2,\ldots n\}$. Группа $S(\Omega)$ всех взаимно однозначных отображений $\Omega\to\Omega$ называется *симметрической группой степени* n (иначе: *симметрической группой на* n *символах* или *на* n *точках*) и чаще обозначается через S_n. Ее элементы, обычно обозначаемые строчными буквами греческого алфавита, называются *перестановками* (или *подстановками*).

В развернутой и наглядной форме перестановку σ: $i\to\sigma(i)$, $i=1,2,\ldots n$, изображают двухрядным символом

$$\sigma=\begin{pmatrix}1 & 2 & . & . & . & n\\ i_1 & i_2 & . & . & . & i_n\end{pmatrix},$$

полностью указывая все образы:

$$\sigma:\ \begin{matrix}1 & 2 & \ldots & n\\ \downarrow & \downarrow & & \downarrow\\ i_1 & i_2 & \ldots & i_n\end{matrix}$$

где $i_k=\sigma(k)$, $k=1,2,\ldots n$, – переставленные символы $1,2,\ldots n$. Как всегда, e – единичная перестановка $e(i)=i$ для любых i.

Более коротко перестановки будем записывать в виде $\sigma=(i_1 i_2 \ldots i_n)$.

Перестановки $\sigma,\tau\in S_n$ перемножаются в соответствии с общим правилом композиции отображений: $(\sigma\tau)(i)=\sigma(\tau(i))$.

Пример 16. Пусть

$$\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 6 & 1 & 5 & 3 & 2\end{pmatrix},\ \tau=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 4 & 3 & 2 & 1\end{pmatrix}.$$

Тогда

$$\sigma\tau=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 4 & 3 & 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 6 & 1 & 5 & 3 & 2\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 3 & 5 & 1 & 6 & 4\end{pmatrix}.$$

В то же время

$$\tau\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 6 & 1 & 5 & 3 & 2\end{pmatrix}\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 4 & 3 & 2 & 1\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 6 & 2 & 4 & 5\end{pmatrix}.$$

т.е. $\sigma\tau\neq\tau\sigma$. ♦

Найдем порядок группы S_n. Перестановкой σ символ 1 можно перевести в любой $\sigma(1)$, для чего существует ровно n различных возможностей. Но, зафиксировав $\sigma(1)$, мы можем брать в качестве $\sigma(2)$ лишь один из оставшихся n-1 символов, в качестве $\sigma(3)$ – соответственно n-2 символа, и т.д. Всего имеется $\sigma(1),\sigma(2),\ldots\sigma(n)$ возможностей выбора, а стало быть, и всех различных перестановок получается $n\cdot(n-1)\ldots2\cdot1=n!$. Таким образом,

$$\mathrm{Card}S_n=|S_n|=(S_n:e)=n!$$

Разложим теперь перестановки из $\mathbf{S_n}$ в произведения более простых перестановок. Идея разложения поясняется на перестановках из примера 16. Короткая запись примера σ=(1 4 5 3)(2 6); τ=(1 6)(2 5)(3 4),

$\alpha=\sigma\tau$=(1 3 6 5 4 2); $\tau\sigma$=(1 2 3 5 6 4). Перестановка α=(1 3 6 5 4 2), или, что то же самое, α=(3 6 5 4 2 1) =(6 5 4 2 1 3)=(5 4 2 1 3 6)=(4 2 1 3 6 5)=(2 1 3 6 5 4) носит название цикла длины 6, а перестановка σ=(1 4 5 3)(2 6) – произведения двух независимых (непересекающихся) циклов длины 4 и 2.

Цикл длины 2 называется *транспозицией*.

Любая транспозиция имеет вид $\tau=(\boldsymbol{j}\ \boldsymbol{i})$ и оставляет на месте все символы, отличные от $\boldsymbol{j}$, $\boldsymbol{i}$.

Для транспозиций справедлива следующая теорема.

Теорема 4. Любая перестановка $\tau\in\mathbf{S_n}$ является произведением транспозиций.

Доказательство. В самом деле, любой цикл можно записать в виде транспозиций следующим образом:

$(1\ 2\ \ldots\ \boldsymbol{l}\text{-}1\ \boldsymbol{l})=(1\ \boldsymbol{l})(1\ \boldsymbol{l}\text{-}1)\ldots(1\ 3)(1\ 2)$

что и является доказательством. ♦

Но надо отметить, что ни о какой единственности записи перестановки через транспозиции не может быть и речи. Транспозиции, вообще говоря, не коммутируют, а их число не является инвариантом перестановки.

Пример 17. В $\mathbf{S_4}$ имеем:

$(1\ 2\ 3)=(1\ 3)(1\ 2)=(2\ 3)(1\ 3)=(1\ 3)(2\ 4)(1\ 2)(1\ 4)$. ♦

Впрочем, неединственность разложения видна из равенства $\sigma\tau^2=\sigma$ для любых транспозиций σ и τ. Тем не менее, один инвариант разложения перестановки через транспозиции все-таки существует. Чтобы обнаружить его по возможности естественным способом, рассмотрим действие $\mathbf{S_n}$ на функциях.

Пусть $\sigma\in\mathbf{S_n}$ и $\boldsymbol{f}(\mathbf{X_1},\ldots\mathbf{X_n})$ – функция от любых $\boldsymbol{n}$ аргументов. Полагаем:

$$(\sigma\circ f)=(X_1,\ldots X_n)=f\left(X_{\sigma^{-1}(1)},\ldots X_{\sigma^{-1}(n)}\right).$$

Говорят, что функция $\boldsymbol{g}=\sigma\circ\boldsymbol{f}$ *получается действием* σ на $\boldsymbol{f}$.

Пример 18. Пусть σ=(1 2 3) и $\boldsymbol{f}(\mathbf{X_1},\mathbf{X_2},\mathbf{X_3})=\mathbf{X_1}+2\mathbf{X_2}^2+3\mathbf{X_3}^3$. Тогда $\boldsymbol{g}=\sigma\circ\boldsymbol{f}=\mathbf{X_3}+2\mathbf{X_1}^2+3\mathbf{X_2}^3$. ♦

Говорят, что функция $\boldsymbol{f}$ называется *кососимметрической*, если $\sigma\circ\boldsymbol{f}=-\boldsymbol{f}$ для любой транспозиции $\sigma\in\mathbf{S_n}$, т.е.

$$\boldsymbol{f}(\mathbf{X_1},\mathbf{X_2},\ldots\mathbf{X_j},\ldots\mathbf{X_i},\ldots)=-(\mathbf{X_1},\mathbf{X_2},\ldots\mathbf{X_i}\ldots\mathbf{X_j}\ldots).$$

Лемма 1. Пусть $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$ – любые перестановки из $\mathbf{S_n}$. Тогда

$$(\alpha\beta)\circ\boldsymbol{f}=\alpha\circ(\beta\circ\boldsymbol{f}).$$

Доказательство. В соответствии с определением $\boldsymbol{g}=\sigma\circ\boldsymbol{f}$ имеем:

$$((\alpha\beta)\circ f)(X_1,\ldots X_n)=f\left(X_{(\alpha\beta)^{-1}(1)},\ldots X_{(\alpha\beta)^{-1}(n)}\right)=$$

$$f\left(X_{\left(\beta^{-1}\alpha^{-1}\right)(1)},\ldots X_{\left(\beta^{-1}\alpha^{-1}\right)(n)}\right)=f\left(X_{\left(\beta^{-1}\left(\alpha^{-1}(1)\right)\right)},\ldots X_{\left(\beta^{-1}\left(\alpha^{-1}(n)\right)\right)}\right)=$$

$$(\beta\circ f)\left(X_{(\alpha)^{-1}(1)},\ldots X_{(\alpha)^{-1}(n)}\right)=(\alpha\circ(\beta\circ f))(X_1,\ldots X_n)$$

что и требовалось доказать. ♦

Справедлива следующая теорема.

Теорема 5. Пусть π – перестановка из $\mathbf{S_n}$, $\pi=\tau_1\tau_2\ldots\tau_k$ – какое-нибудь разложение π в произведение транспозиций. Тогда число

$$\varepsilon_\pi=(-1)^k,$$

называемое *четностью* π(иначе *сигнатурой* или *знаком* π) полностью определяется перестановкой π и не зависит от способа разложения, т.е. четность целого числа k для данной перестановки π всегда одна и та же. Кроме того, $\varepsilon_{\alpha\beta}=\varepsilon_\alpha\varepsilon_\beta$ для всех $\alpha,\beta\in\mathbf{S_n}$.

Доказательство. Возьмем произвольную кососимметрическую функцию f от n аргументов $\mathbf{X_1},\ldots\mathbf{X_n}$. По лемме действие π на f сводится к последовательному применению транспозиций τ_k, τ_{k-1},…τ_1, т.е. к k – кратному умножению f на –1:

$$\pi\circ f=(\tau_1\tau_2\ldots\tau_{k-1})\circ(\tau_k\circ f)=-(\tau_1\tau_2\ldots\tau_{k-1})\circ f=\ldots=(-1)^k f=\varepsilon_\pi f.$$

Так как левая часть этого соотношения зависит от π, но не от какого-либо его разложения, то и отображение $\varepsilon:\pi\to\varepsilon_\pi$, заданное правилом $\varepsilon_\pi=(-1)^k$, должно полностью определятся перестановкой π при условии, конечно, что f – не тождественно равная нулю функция. Но мы знаем, что существуют кососимметрические функции, не равные нулю, например, определитель Вандермонда $\Delta_n(\mathbf{X_1},\ldots\mathbf{X_n})$ порядка n.

Применение к такой функции f перестановки $\alpha\beta$ по правилу, изложенному в лемме, дает:

$$\varepsilon_{\alpha\beta}f=(\alpha\beta)\circ f=\alpha\circ(\beta\circ f)=\alpha\circ(\varepsilon_\beta f)=\varepsilon_\beta(\alpha\circ f)=\varepsilon_\beta(\varepsilon_\alpha f)=(\varepsilon_\alpha\varepsilon_\beta)f,$$

откуда и следует соотношение $\varepsilon_{\alpha\beta}=\varepsilon_\alpha\varepsilon_\beta$. Теорема доказана. ♦

Перестановка $\beta\in\mathbf{S_n}$ называется *четной*, если $\varepsilon_\beta=1$, и *нечетной*, если $\varepsilon_\beta=-1$.

Из определения четной и нечетной перестановки следует, что все транспозиции – нечетные перестановки. В связи с этим справедливо следующее

Утверждение. Все четные перестановки степени n образуют подгруппу $\mathbf{A_n}\in\mathbf{S_n}$ порядка $n!/2$ (она называется знакопеременной группой степени n).

Доказательство. Так как $\varepsilon_{\alpha\beta}=\varepsilon_\alpha\varepsilon_\beta$, то $\varepsilon_{\alpha\beta}=1$, если $\varepsilon_\alpha=\varepsilon_\beta=1$, и $\varepsilon_{\pi^{-1}}=\varepsilon_\pi$, поскольку $\varepsilon_e=1$. Так как $\mathbf{A_n}$ – подмножество в $\mathbf{S_n}$, то все аксиомы группы выполнены.

Запишем $\mathbf{S_n}$ в виде $\mathbf{A_n}\cup\underline{\mathbf{A_n}}$, где $\underline{\mathbf{A_n}}$ – множество всех нечетных перестановок степени n. Отображение $\mathbf{S_n}$ в себя, определенное правилом

$$\rho_{(12)}: \pi \to (12)\pi,$$

биективно. (Оно инъективно: $(12)\alpha=(12)\beta \Rightarrow \alpha=\beta$. Далее можно просто заметить, что $(\rho_{(12)})^2$ – единичное отображение). Так как $\varepsilon_{(12)\pi}=\varepsilon_{(12)}\varepsilon_{\pi}=-\varepsilon_{\pi}$, то $\rho_{(12)}\mathbf{A_n}=\underline{\mathbf{A_n}}$, $\rho_{(12)}\underline{\mathbf{A_n}}=\mathbf{A_n}$. Значит, число четных перестановок в $\mathbf{S_n}$ совпадает с числом нечетных перестановок. Отсюда $|\mathbf{A_n}|=0.5|\mathbf{S_n}|=\boldsymbol{n}!/2$. Утверждение доказано. ♦

5. МОРФИЗМЫ ГРУПП

5.1. ИЗОМОРФИЗМЫ

Известно, что три вращения φ_0, φ_1, φ_2 против часовой стрелки на углы 0°, 120°, 240° переводят правильный треугольник P_3 в себя. Но имеются еще три *осевых преобразования симметрии* (*отражения*) ψ_1, ψ_2, ψ_3 с указанными на рис. 3 осями симметрии 1—1', 2—2', 3—3'. Всем шести преобразованиям симметрии соответствуют перестановки на множестве вершин треугольника. Получаем: φ_0~e,φ_1~(123),φ_2~(132),ψ_1,~(23), ψ_2~(13), ψ_3~(12). Так как других перестановок степени 3 нет, то можно утверждать, что группа D_3 всех преобразований симметрии правильного треугольника обнаруживает большое сходство с симметрической группой $\mathbf{S_3}$. Отсюда следует, что нам необходимо каким-то образом сравнивать группы. Для этого вводится понятие изоморфизма. Дадим его определение: две группы **G** и **G'** с операциями * и ○ называются *изоморфными*, если существует отображение $\mathbf{f:G\to G'}$ такое, что:

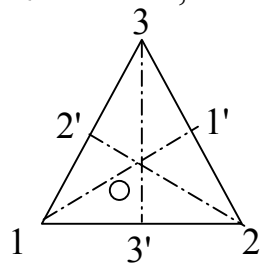

Рис. 3.

(i) $\mathbf{f}(\boldsymbol{a}*\boldsymbol{b})=\mathbf{f}(\boldsymbol{a})\circ\mathbf{f}(\boldsymbol{b})$ для всех $\boldsymbol{a},\boldsymbol{b}\in\mathbf{G}$;

(ii) **f** – биективно.

Факт изоморфизма групп обозначается символически ≅.

Отметим простейшие свойства изоморфизма.

1. Единица переходит в единицу. Действительно, если $\boldsymbol{e}$ – единица группы **G**, то $\boldsymbol{e}*\boldsymbol{a}=\boldsymbol{a}*\boldsymbol{e}=\boldsymbol{a}$, и значит $\mathbf{f}(\boldsymbol{e})\circ\mathbf{f}(\boldsymbol{a})=\mathbf{f}(\boldsymbol{a})\circ\mathbf{f}(\boldsymbol{e})=\mathbf{f}(\boldsymbol{a})$, откуда следует, что $\mathbf{f}(\boldsymbol{e})=\boldsymbol{e}'$ – единица группы **G'**. В этом рассуждении использованы, хотя и частично, оба свойства **f**. Для (i) это очевидно, а свойство (ii) обеспечивает сюръективность **f**, так что элементами $\mathbf{f}(\boldsymbol{g})$ исчерпывается вся группа **G'**.
2. $\mathbf{f}(\boldsymbol{a}^{-1})=\mathbf{f}(\boldsymbol{a})^{-1}$. В самом деле, согласно 1, $\mathbf{f}(\boldsymbol{a})\circ\mathbf{f}(\boldsymbol{a}^{-1})=\mathbf{f}(\boldsymbol{a}*\boldsymbol{a}^{-1})=\mathbf{f}(\boldsymbol{e})=\boldsymbol{e}'$ – единица группы **G'**, откуда $\mathbf{f}(\boldsymbol{a})^{-1}=\mathbf{f}(\boldsymbol{a})^{-1}\circ\boldsymbol{e}'=\mathbf{f}(\boldsymbol{a})^{-1}\circ(\mathbf{f}(\boldsymbol{a})\circ\mathbf{f}(\boldsymbol{a}^{-1}))=(\mathbf{f}(\boldsymbol{a})^{-1}\circ\mathbf{f}(\boldsymbol{a}))\circ\mathbf{f}(\boldsymbol{a}^{-1})=\boldsymbol{e}'\circ\mathbf{f}(\boldsymbol{a}^{-1})=\mathbf{f}(\boldsymbol{a}^{-1})$.
3. Обратное отображение $\mathbf{f^{-1}:G\to G'}$ (существующее в силу свойства (ii)) тоже является изоморфизмом. Для этого надо убедиться лишь в справедливости свойства (i) для $\mathbf{f^{-1}}$. Пусть $\boldsymbol{a}',\boldsymbol{b}'\in\mathbf{G}'$. Тогда ввиду биективности **f** имеем $\boldsymbol{a}'=\mathbf{f}(\boldsymbol{a})$, $\boldsymbol{b}'=\mathbf{f}(\boldsymbol{b})$ для каких-то $\boldsymbol{a},\boldsymbol{b}\in\mathbf{G}$. Поскольку **f** – изоморфизм, $\boldsymbol{a}'\circ\boldsymbol{b}'=\mathbf{f}(\boldsymbol{a})\circ\mathbf{f}(\boldsymbol{b})=\mathbf{f}(\boldsymbol{a}*\boldsymbol{b})$. Отсюда имеем $\boldsymbol{a}*\boldsymbol{b}=\mathbf{f^{-1}}(\boldsymbol{a}'\circ\boldsymbol{b}')$, а так как, в свою очередь, $\boldsymbol{a}=\mathbf{f^{-1}}(\boldsymbol{a}')$, $\boldsymbol{b}=\mathbf{f^{-1}}(\boldsymbol{b}')$, то $\mathbf{f^{-1}}(\boldsymbol{a}'\circ\boldsymbol{b}')=\mathbf{f^{-1}}(\boldsymbol{a}')*\mathbf{f^{-1}}(\boldsymbol{b}')$.

Пример 19. В качестве изоморфного отображения **f** мультипликативной группы $(R_+,*,1)$ положительных чисел на аддитивную группу $(R,+,0)$ всех вещественных чисел может служить **f=ln**. Известное свойство логарифма $\ln ab=\ln a+\ln b$ как раз моделирует свойство (i) в определении изоморфизма. Обратным к **f** служит отображение $x\to e^x$. ♦

Рассмотрим теперь теорему, иллюстрирующую роль изоморфизма в теории групп.

Теорема 6 (Кэли). Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы $\mathbf{S_n}$.

Доказательство. Пусть **G** – наша группа, $n=|\mathbf{G}|$. Можно считать,что $\mathbf{S_n}$ – группа всех биективных отображений множества **G** на себя, так как природа элементов, представляемых элементами из $\mathbf{S_n}$, несущественна.

Для любого элемента $a\in\mathbf{G}$ рассмотрим отображение $\mathbf{L_a}:\mathbf{G}\to\mathbf{G}$, определенное формулой:

$$\mathbf{L_a}(g)=ag.$$

Если $e=g_1$, то $g_1,g_2,\dots g_n$ – все элементы группы **G**. Тогда $ag_1,\dots ag_n$ – те же элементы, но расположенные в каком-то другом порядке. Это и понятно, поскольку

$$ag_i = ag_k \Rightarrow a^{-1}(ag_i)=a^{-1}(ag_k)\Rightarrow(a^{-1}a)g_i=(a^{-1}a)g_k\Rightarrow g_i=g_k.$$

Значит, $\mathbf{L_a}$ – биективное отображение (перестановка), обратным к которому будет $\mathbf{L_a}^{-1}=L_{a^{-1}}$. Единичным отображением является $\mathbf{L_e}$.

Используя вновь ассоциативность умножения в **G**, получаем $\mathbf{L_{ab}}(g)=(ab)g=a(bg)=\mathbf{L_a}(\mathbf{L_b}g)$, т.е. $\mathbf{L_{ab}}=\mathbf{L_a}\circ\mathbf{L_b}$.

Итак, множество $\mathbf{L_e}, L_{g_2},\dots L_{g_n}$ образует подгруппу, скажем **H**, в группе **S**(**G**) всех биективных отображений множества **G** на себя, т.е. в $\mathbf{S_n}$. Мы имеем включение $\mathbf{H}\subset\mathbf{S_n}$ и имеем соответствие $\mathbf{L}:a\to\mathbf{L_a}\in\mathbf{H}$, обладающее по вышесказанному всеми свойствами изоморфизма. ♦.

Теорема Кэли, несмотря на свою простоту, имеет важное значение в теории групп. Она выделяет некий универсальный объект (семейство $\{\mathbf{S_n}|n=1,2,\dots\}$ симметрических групп) – вместилище всех вообще конечных групп, рассматриваемых с точностью до изоморфизма. Фраза "с точностью до изоморфизма" отражает сущность не только теории групп, стремящейся объединить в один класс все изоморфные группы, но математики в целом, которая без таких обобщений была бы лишена смысла.

Положив **G=G'** в определении изоморфизма, мы получим изоморфное отображение $\varphi:\mathbf{G}\to\mathbf{G}$ группы **G** на себя. Оно называется *автоморфизмом* группы **G**.

Пример 20. Единичное отображение $e_g:g\to g$ – автоморфизм. ♦

Но, как правило, **G** обладает и нетривиальными автоморфизмами. Свойство 3 изоморфных отображений показывает, что отображение, обратное к автоморфизму, тоже будет автоморфизмом. Если, далее, φ,ψ – автоморфизмы группы **G**, то $(\varphi\circ\psi)(ab)=\varphi(\psi(ab))=\varphi(\psi(a)\psi(b))=$

$(\varphi\circ\psi)(a)*(\varphi\circ\psi)(b)$ для любых $a,b\in\mathbf{G}$. Стало быть множество Aut(**G**) всех автоморфизмов группы **G** образует группу – подгруппу группы всех биективных **S**(**G**) отображений $\mathbf{G}\to\mathbf{G}$.

Пример 21. Посмотрим, как можно изменить операцию на группе, не меняя, в смысле изоморфизма, самой группы. Пусть **G** – произвольная группа, t – ее какой-то фиксированный элемент. Введем на множестве **G** новую операцию:

$$(g, h)\to g*h=gth.$$

Непосредственная проверка показывает, что $(g_1*g_2)*g_3=g_1*(g_2*g_3)$, т.е. операция $*$ ассоциативна. Кроме того, $g*t^{-1}=t^{-1}*g=g$ и $g*(t^{-1}g^{-1}t^{-1}) = (t^{-1}g^{-1}t^{-1})*g=t^{-1}$, а это значит, что $\{\mathbf{G},*\}$ – группа с единичным элементом $e_*=t^{-1}$. Элементом обратным к g_* в $\{\mathbf{G},*\}$, служит $g_*^{-1}=t^{-1}g^{-1}t^{-1}$. Отображение $f:g\to gt^{-1}$ устанавливает изоморфизм групп $\{\mathbf{G},\bullet\}$ и $\{\mathbf{G},*\}$, т.е. $f(gh)= f(g)*f(h)$. ♦

5.2. ГОМОМОРФИЗМЫ

В группе автоморфизмов Aut(**G**) группы **G** содержится одна особая подгруппа. Она обозначается Inn(**G**) и называется *группой внутренних автоморфизмов*. Ее элементами являются отображения $I_a:g\to aga^{-1}$. Небольшое упражнение показывает, что I_a действительно удовлетворяет свойствам, требуемым от автоморфизмов, причем $I_a^{-1} = I_{a^{-1}}$, I_e – единичный автоморфизм, $I_a\circ I_b=I_{ab}$ (потому что $(I_a\circ I_b)(g)=I_a(I_b)(g))=I_a(bgb^{-1})=abgb^{-1}a^{-1}= abg(b^{-1}a^{-1})=abg(ab)^{-1}=I_{ab}(g)$. Последнее соотношение показывает, что отображение $f:\mathbf{G}\to\mathrm{Inn}(\mathbf{G})$ группы **G** на группу Inn(**G**) ее внутренних автоморфизмов, определенное формулой $f(a)=I_a$, $a\in\mathbf{G}$, обладает свойством (i) изоморфного отображения: $f(a)\circ f(b)=f(ab)$. однако свойство (ii) при этом не обязано выполняться. Если, например, **G** – абелева группа, то $aga^{-1}=g$ для всех $a\in\mathbf{G}$, так что $I_a=I_e$, и вся группа Inn(**G**) состоит из одного единичного элемента I_e. Это обстоятельство делает естественным следующее определение:

Отображение $f:\mathbf{G}\to\mathbf{G}'$ группы $(\mathbf{G},*)$ в $(\mathbf{G}',\circ)$ называется *гомоморфизмом*, если $f(a*b)=f(a)\circ f(b)$, для любых $a,b\in\mathbf{G}$ (другими словами, в определении изоморфизма опущено свойство (ii)).

Ядром гомоморфизма f называется множество

$\mathrm{Ker}\, f = \{g\in\mathbf{G} \mid f(g) = e'$– единица группы $\mathbf{G}'\}$.

Гомоморфное отображение группы в себя называется еще ее *эндоморфизмом*.

В этом определении от f не требуется не только биективности, но и сюръективности, что, впрочем, не очень существенно, поскольку всегда можно ограничиться рассмотрением образа $\mathrm{Im}\, f\subset\mathbf{G}'$, являющегося, очевидно, подгруппой в $\mathbf{G}'$. Главное отличие гомоморфизма f от изоморфиз-

ма заключается в наличии нетривиального ядра Ker f, являющегося мерой неинъективности f. Если же Ker f = $\{e\}$, то f:**G**→Im f – изоморфизм. Заметим, что $f(a) = e'$, $f(b) = e'$,⇒$f(a*b) = f(a)\circ f(b) = e'\circ e' = e'$ и $f(a^{-1})=f(a)^{-1}=(e)^{-1}=e'$. Поэтому ядро Ker f – подгруппа в **G**.

Пусть **H**=Ker $f\subset$**G**. Тогда (опуская знаки $*$ и $\circ$) $f(ghg^{-1})=f(g)f(h)f(g^{-1})=f(g)e'f(g^{-1})=e'$, $\forall h\in$**H**, $g\in$**G**, т.е. $ghg^{-1}\in$**H** и, значит, g**H**$g^{-1}\subset$**H**. Заменив здесь g на g^{-1}, получим g^{-1}**H**$g\subset$**H**, откуда **H**$\subset g$**H**g^{-1}. Стало быть, **H**=g**H**g^{-1}, $\forall g\in$**G**. Подгруппы, обладающие этим свойством, называются *нормальными*. Еще их называют *инвариантными подгруппами* или *нормальными делителями*. Итак, нами доказана

Теорема 7. Ядра гомоморфизмов всегда являются нормальными подгруппами. ♦

Значение этого факта мы оценим в должной мере позднее. Заметим пока, что далеко не всякая подгруппа нормальна в **G**.

Пример 22. Отображение f:**R**→**T**=**SO**(2) аддитивной группы вещественных чисел на группу **T** вращений плоскости с неподвижной точкой 0, задаваемое формулой $f(\lambda)=\Phi_\lambda$ (Φ_λ – вращение против часовой стрелки на угол $2\pi\lambda$), гомоморфно. Так как $\Phi_\lambda\circ\Phi_\mu=\Phi_{\lambda+\mu}$, а вращение на угол, целочисленно кратный 2π, совпадает с единичным вращением (на нулевой угол), то Ker f =$\{2\pi n \mid n\in$**Z**$\}$. Говорят также, что f – гомоморфизм **R** на окружность $\mathbf{S}^1$ единичного радиуса, поскольку имеется взаимно однозначное соответствие между Φ_λ и точкой на $\mathbf{S}^1$ с полярными координатами $(1,2\pi\lambda)$, $0\le\lambda<1$. ♦

Пример 23. Полная линейная группа **GL**(n,**R**) вещественных матриц **A** (т.е. матриц с коэффициентами в **R**) с не равным нулю определителем det**A** гомоморфно отображается на мультипликативную группу $\mathbf{R}^*$ отличных от нуля вещественных чисел, если положить f=det. Условие гомоморфизма f(**AB**)=f(**A**)f(**B**) выполнено. Здесь **SL**(n,**R**)=Ker f. ♦

Пример 24. Группа Aut(**G**) и даже отдельный неединичный элемент $\varphi\in$Aut(**G**) могут служить источником важных сведений о группе **G**. Вот яркий пример такого рода. Пусть **G** – конечная группа, на которой действует автоморфизм порядка 2 ($\varphi^2=\varphi_e=1$) без неподвижных точек:

$$a\ne e \Rightarrow \varphi(a)\ne a.$$

Предположим, что $\varphi(a)a^{-1}=\varphi(b)b^{-1}$ для каких-то $a,b\in$**G**. Тогда после умножения этого равенства на слева на $\varphi(b)^{-1}$ и справа на a получим $\varphi(b)^{-1}\varphi(a)=b^{-1}a$, т.е. $\varphi(b^{-1}a)=b^{-1}a$, откуда $b^{-1}a=e$ и $b^{-1}=a$. Итак, $\varphi(a)a^{-1}$ пробегает вместе с a все элементы группы **G**, или, что равносильно, любой элемент $g\in$**G** записывается в виде $g=\varphi(a)a^{-1}$. Но в таком случае $\varphi(g)$ = $\varphi(\varphi(a))\varphi(a^{-1})=\varphi^2(a)\varphi(a^{-1})=a\varphi(a)^{-1}=(\varphi(a)a^{-1})^{-1}=g^{-1}$. Итак, φ совпадает с отображением $g\to g^{-1}$. Зная это, получаем $ab=\varphi(a^{-1})\varphi(b^{-1})=\varphi(a^{-1}b^{-1})=(a^{-1}b^{-1})^{-1}=ba$, т.е. группа **G** оказывается абелевой. Кроме того, (**G**:e) – нечетное число, ибо **G** состоит из e и непересекающихся пар элементов g_i: $g_i^{-1}=\varphi(g_i)$. ♦

6. КОЛЬЦА

6.1. ОПРЕДЕЛЕНИЕ И ОБЩИЕ СВОЙСТВА КОЛЕЦ

Алгебраические структуры $(\mathbf{Z},+)$, $(\mathbf{Z},\bullet)$ выступали у нас в качестве самых первых примеров моноидов, причем на $(\mathbf{Z},+)$ мы смотрели позднее как на аддитивную абелеву группу. В повседневной жизни, однако, эти структуры чаще всего объединяются, и получается то, что в математике называется кольцом. Важный элемент элементарной арифметики заключен в дистрибутивном (или сочетательном) законе $(\boldsymbol{a}+\boldsymbol{b})\boldsymbol{c}=\boldsymbol{ac}+\boldsymbol{bc}$, кажущимся тривиальным только в силу приобретенной привычки. Попытавшись, например, объединить алгебраические структуры $(\mathbf{Z},+)$, $(\mathbf{Z},\circ)$, где $\boldsymbol{n}\circ\boldsymbol{m}=\boldsymbol{n}+\boldsymbol{m}+\boldsymbol{nm}$, мы уже не заметим столь хорошей согласованности между двумя бинарными операциями. А сейчас дадим определение кольца.

Пусть $\mathbf{K}$ – непустое множество, на котором заданы две бинарные алгебраические операции + (сложение) и × (умножение), удовлетворяющие следующим условиям:

К1 $(\mathbf{K},+)$ – коммутативная (*абелева*) группа;

К2 $(\mathbf{K},\times)$ – полугруппа;

К3 операции сложения и умножения связаны дистрибутивными законами (другими словами, умножение дистрибутивно по сложению):

$$(\boldsymbol{a}+\boldsymbol{b})\times\boldsymbol{c}=\boldsymbol{a}\times\boldsymbol{c}+\boldsymbol{b}\times\boldsymbol{c},\ \boldsymbol{c}\times(\boldsymbol{a}+\boldsymbol{b})=\boldsymbol{c}\times\boldsymbol{a}+\boldsymbol{c}\times\boldsymbol{b},\quad \boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\in\mathbf{K}.$$

Тогда $(\mathbf{K},+,\times)$ называется *кольцом*.

Структура $(\mathbf{K},+)$ называется *аддитивной группой кольца*, а $(\mathbf{K},\times)$ – его *мультипликативной полугруппой*. Если $(\mathbf{K},\times)$ – моноид, то говорят, что $(\mathbf{K},+,\times)$ – *кольцо с единицей*.

Подмножество $\mathbf{L}$ кольца $\mathbf{K}$ называется *подкольцом*, если

$$\boldsymbol{x},\boldsymbol{y}\in\mathbf{L}\Rightarrow\boldsymbol{x}+\boldsymbol{y}\in\mathbf{L}\text{ и }\boldsymbol{x}\times\boldsymbol{y}\in\mathbf{L},$$

т.е. если $\mathbf{L}$ – подгруппа аддитивной группы и подполугруппа мультипликативной полугруппы кольца.

Кольцо называется *коммутативным*, если $\boldsymbol{x}\times\boldsymbol{y}=\boldsymbol{y}\times\boldsymbol{x}$ для всех $\boldsymbol{x},\boldsymbol{y}\in\mathbf{K}$ (в отличие от групп, коммутативное кольцо не принято называть абелевым).

Пример 25. $(\mathbf{Z},+,\bullet)$ – кольцо целых чисел с обычными операциями сложения и умножения. Множество $\boldsymbol{m}\mathbf{Z}$ целых чисел, делящихся на $\boldsymbol{m}$, будет в $\mathbf{Z}$ подкольцом (без единицы при $\boldsymbol{m}>1$). Аналогично кольцами с единицей являются $\mathbf{Q}$ и $\mathbf{R}$, причем естественные включения $\mathbf{Z}\subset\mathbf{Q}\subset\mathbf{R}$ определяют цепочки подколец кольца $\mathbf{R}$. ♦

Пример 26. Свойства операций сложения и умножения в $\mathbf{M}_n(\mathbf{R})$ показывают, что $\mathbf{M}_n(\mathbf{R})$ – кольцо, называемое *кольцом квадратных матриц порядка* $\boldsymbol{n}$ *над* $\mathbf{R}$. ♦

Пример 27. Можно рассматривать кольцо квадратных матриц $\mathbf{M}_n(\mathbf{K})$ над произвольным коммутативным кольцом $\mathbf{K}$, поскольку при

сложении и умножении двух матриц $\mathbf{A},\mathbf{B}\in\mathbf{M_n(K)}$ будет снова получаться матрица с коэффициентами из **K**. Все это прямо вытекает из формальных действий с матрицами. ♦

Пример 28. Пусть **X** – произвольное множество, **K** – произвольное кольцо, $\mathbf{K^X}=\{\mathbf{X}\to\mathbf{K}\}$ – множество всех функций $\mathbf{f:X}\to\mathbf{K}$, рассматриваемое вместе с двумя бинарными операциями – *поточечной суммой* $f+g$ и *поточечным произведением* fg, определяемыми следующим образом:

$$(f+g)(x)=f(x)\oplus g(x),$$
$$(fg)(x)=f(x)\otimes g(x).$$

($\oplus$ и $\otimes$ – операции сложения и умножения в **K**).

Без труда проверяется, что $\mathbf{K^X}$ удовлетворяет всем аксиомам кольца. Так, ввиду дистрибутивности операций в **K**, имеем

$$[f(x)\oplus g(x)]\otimes h(x)=f(x)\otimes h(x)\oplus g(x)\otimes h(x)$$

для любых $f,g,h\in\mathbf{K^X}$ и любого $x\in\mathbf{X}$, а это по определению поточечных операций дает $(f+g)h=fh+gh$. Справедливость второго дистрибутивного закона устанавливается аналогично.

Если 0,1 – нулевой и единичный элементы в **K**, то $\mathbf{0_X}:x\to 0$ и $\mathbf{1_X}:x\to 1$ – постоянные функции, играющие роль нуля и единицы в $\mathbf{K^X}$. В случае коммутативности **K** кольцо функций $\mathbf{K^X}$ также коммутативно. ♦

Пример 29. Кольцо $\mathbf{K^X}$ содержит разнообразные подкольца, определяемые специальными свойствами функций. Пусть $\mathbf{X}=[0,1]$ – замкнутый интервал в **R** и $\mathbf{K}=\mathbf{R}$. Тогда кольцо $\mathbf{R}^{[0,1]}$ всех вещественных функций, определенных на [0,1], содержит в качестве подколец кольцо $\mathbf{R_{огр}}^{[0,1]}$ всех ограниченных функций, кольцо $\mathbf{R_{непр}}^{[0,1]}$ всех непрерывных функций, кольцо $\mathbf{R_{диф}}^{[0,1]}$ всех непрерывно дифференцируемых функций и т.д., поскольку все отмеченные свойства сохраняются при сложении (вычитании) и умножении функций. ♦

Пример 30. Каждому $a\in\mathbf{R}$ отвечает *постоянная функция* $a_{\mathbf{X}}:x\to a$ и отображение вложения $a\to a_{\mathbf{X}}$ позволяет рассматривать **R** как подкольцо в $\mathbf{R^X}$, т.е. почти каждому естественному классу функций соответствует свое подкольцо в $\mathbf{R^X}$. ♦

Многие свойства колец являются переформулировками соответствующих свойств групп и вообще – множеств с одной ассоциативной операцией. Например, $a^m a^n=a^{m+n}$, $(a^m)^n=a^{mn}$ для всех неотрицательных целых m, n и всех $a\in\mathbf{K}$. Другие свойства, более специфические для колец и вытекающие прямо из аксиом кольца, моделируют, по существу, свойства **Z**. Отметим некоторые из них.

1. $a0=0a=0$ для всех $a\in\mathbf{K}$. Действительно, $a+0=a \Rightarrow a(a+0)=aa \Rightarrow a^2+a0=a^2 \Rightarrow a^2+a0=a^2+0 \Rightarrow a0=0$ (аналогично $0a=0$).
2. Предположим, что 0=1. Тогда получаем, что $a=a1=a0=0$ для всех $a\in\mathbf{K}$, т.е. **K** состоит только из нуля. Стало быть, в нетривиальном кольце **K** всегда $0\neq 1$.

3. $(-a)b=a(-b)=-(ab)$. Действительно, $0 = a0 = a(b-b)=ab+a(-b) \Rightarrow a(-b) = -(ab)$. ♦

Аналогично моделируются и некоторые другие свойства.

6.2. СРАВНЕНИЯ. КОЛЬЦО КЛАССОВ ВЫЧЕТОВ

Множество $m\mathbf{Z}$, очевидно, замкнуто относительно операций сложения и умножения, удовлетворяя при этом всем аксиомам кольца. Таким образом, верно следующее утверждение: каждое ненулевое подкольцо кольца $m\mathbf{Z}$ имеет вид $m\mathbf{Z}$, где $m \in \mathbf{N}$.

Теперь, используя подкольцо $m\mathbf{Z} \subset \mathbf{Z}$, построим ненулевое кольцо, состоящее из конечного числа элементов. С этой целью введем следующее **определение**.

Два целых числа **n** и **n'** называются *сравнимыми по модулю* **m**, если при делении на **m** они дают одинаковые остатки. Пишут $\mathbf{n} \equiv \mathbf{n'}(\mathbf{m})$ или $\mathbf{n} \equiv \mathbf{n'}(\mathrm{mod}\ \mathbf{m})$, а число **m** называют модулем сравнения.

Таким образом, получается разбиение **Z** на классы чисел, сравнимых между собой по mod **m** и называемых *классами вычетов* по mod **m**. Каждый класс вычетов имеет вид:

$$\{r\}_{\mathbf{m}} = r + m\mathbf{Z} = \{r + mk \mid k \in \mathbf{Z}\},$$

так что

$$\mathbf{Z} = \{0\}_{\mathbf{m}} \cup \{1\}_{\mathbf{m}} \cup \ldots \cup \{m-1\}_{\mathbf{m}}.$$

Таким образом, каждым двум классам $\{k\}_{\mathbf{m}}$ и $\{l\}_{\mathbf{m}}$, независимо от выбора в них представителей k, l, можно сопоставить классы, являющиеся их суммой, разностью или произведением, т.е. на множестве $\mathbf{Z}_{\mathbf{m}} = \mathbf{Z}/m\mathbf{Z}$ классов вычетов по модулю m однозначным образом индуцируются операции $\oplus$ и $\otimes$:

$$\{k\}_{\mathbf{m}} \oplus \{l\}_{\mathbf{m}} = \{k+l\}_{\mathbf{m}},\ \{k\}_{\mathbf{m}} \otimes \{l\}_{\mathbf{m}} = \{kl\}_{\mathbf{m}}.$$

Так как определение этих операций сводится к соответствующим операциям над числами из классов вычетов, т.е. над элементами из **Z**, то $\{\mathbf{Z}_{\mathbf{m}}, \oplus, \otimes\}$ будет также коммутативным кольцом с единицей $\{1\}_{\mathbf{m}} = 1 + m\mathbf{Z}$. Оно называется кольцом классов вычетов по модулю m. При небольшом навыке (и фиксированном модуле) отказываются от кружочков и оперируют с каким-нибудь фиксированным множеством представителей по модулю m, чаще всего – с множеством $\{0, 1, 2, \ldots m-1\}$ (оно называется приведенной системой вычетов по модулю m). В соответствии с этим соглашением $-k = m-k$, $2(m-1) = -2 = m-2$.

Итак, конечные кольца существуют. Приведем два простейших примера, указывая отдельно таблицы сложения и умножения:

$\mathbf{Z_2}$:

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	0

$\mathbf{Z_3}$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

6.3. ГОМОМОРФИЗМЫ И ИДЕАЛЫ КОЛЕЦ

Отображение $f: n \to \{n\}_m$ обладает следующими свойствами:

$$f(k+l)=f(k)\oplus f(l);\ f(kl)=f(k)\otimes f(l).$$

Это дает основание говорить о гомоморфизме колец $\mathbf{Z}$ и $\mathbf{Z_m}$ в соответствии с общим определением.

Пусть $\{\mathbf{K}, +, \cdot\}$ и $\{\mathbf{K'},\oplus,\otimes\}$ – кольца. Отображение $f: \mathbf{K}\to\mathbf{K'}$ называется *гомоморфизмом*, если оно сохраняет все операции, т.е. если

$$f(a+b)=f(a)\oplus f(b);\ f(ab)=f(a)\otimes f(b).$$

При этом, конечно, $f(0)=0'$; $f(na)=nf(a)$, $n\in\mathbf{Z}$.

Ядром гомоморфизма f называется множество

$$\operatorname{Ker} f = \{a\in\mathbf{K} \mid f(a) = 0'\}.$$

Ясно, что $\operatorname{Ker} f$ – подкольцо в $\mathbf{K}$. Но это не произвольное подкольцо. Действительно, если $\mathbf{L}=\operatorname{Ker} f\subset\mathbf{K}$, то $\mathbf{L}\cdot x\subseteq\mathbf{L}$ (поскольку $f(lx)=f(l)\otimes f(x) = 0\otimes f(x) = 0'$ для всех $l\in\mathbf{L}$) и $x\cdot\mathbf{L}\subseteq\mathbf{L}$ для всех $x\in\mathbf{K}$. Стало быть, $\mathbf{L}\cdot\mathbf{K}\subseteq\mathbf{L}$ и $\mathbf{K}\cdot\mathbf{L}\subseteq\mathbf{L}$. Подкольцо $\mathbf{L}$, обладающее этими свойствами, называется *идеалом* кольца $\mathbf{K}$. Итак, ядра гомоморфизмов всегда являются идеалами.

Пример 31. При построении $\mathbf{Z_m}$ неявным образом как раз и использовался тот факт, что $m\mathbf{Z}$ – идеал кольца $\mathbf{Z}$. ♦

Мы видим, что в кольце $\mathbf{Z}$ каждое ненулевое подкольцо является идеалом – случайное обстоятельство, которому нет места, скажем, уже в матричном кольце $\mathbf{M_2}(\mathbf{Z})$: множество

$$\left\{\begin{pmatrix}\alpha & \beta\\ 0 & \delta\end{pmatrix} \mid \alpha,\beta,\delta\in Z\right\}$$

является подкольцом, но не идеалом в $\mathbf{M_2}(\mathbf{Z})$.

Пример $m\mathbf{Z}$ подсказывает способ построения идеалов (возможно, не всех) в произвольном коммутативном кольце $\mathbf{K}$: если a – какой-то элемент $\mathbf{K}$, то множество $a\mathbf{K}$ всегда является идеалом в $\mathbf{K}$. Действительно,

$$ax+ay=a(x+y),\ (ax)y=a(xy).$$

Говорят, что $a\mathbf{K}$ – *главный идеал*, порожденный элементом $a\in\mathbf{K}$.

6.4. ТИПЫ КОЛЕЦ

В хорошо известных нам числовых кольцах $\mathbf{Z}$, $\mathbf{Q}$ и $\mathbf{R}$ из того, что $ab=0$, следует, что либо $a=0$, либо $b=0$. Но кольцо квадратных матриц $\mathbf{M_n}$ этим свойством уже не обладает. Используя матрицы $\mathbf{E_{ij}}$, состоящие из нулей всюду, кроме элемента, стоящего на пересечении i–строки и j-го

столбца (равного 1), получаем что $\mathbf{E_{ij}E_{kl}}=0$ при $\mathbf{j}\neq\mathbf{k}$, хотя, конечно, $\mathbf{E_{ij}}\neq 0$ и $\mathbf{E_{kl}}\neq 0$. Заметим, что $\mathbf{E_{ik}E_{kl}}\neq 0$. Можно было бы приписать столь необычный для элементарной арифметики феномен некоммутативности кольца $\mathbf{M_n}$, но это не так. Рассмотрим еще несколько примеров.

Пример 32. Числовые пары (a,b) ($a,b\in\mathbf{Z}$, **Q** или **R**) со сложением и умножением, определенными формулами

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2),$$
$$(a_1,b_1)(a_2,b_2)=(a_1a_2,\ b_1b_2),$$

образуют, очевидно, коммутативное кольцо с единицей (1,1), в котором мы снова встречаемся с тем же явлением: (1,0)(0,1)=(0,0)=0. ♦

Пример 33. В кольце $\mathbf{R^R}$ вещественных функций (примеры 28-30), функции $f:x\to|x|+x$ и $g:x\to|x|-x$ таковы, что $f(x)=0$ для $x\leq 0$ и $g(x)=0$ для $x\geq 0$, а поэтому их поточечным произведением fg будет нулевая функция, хотя $f\neq 0$ и $g\neq 0$. ♦

Пример 34. Если кольцо состоит из 3 и менее элементов, то это кольцо коммутативное.

a) Если элемент один, тогда он равен нулю.
b) Если два элемента, тогда $aa=a\neq 0$.
c) Если три элемента, тогда $a+b=0$, так как третий элемент не совпадает ни с a, ни с b. Следовательно, $ab=-aa$. Это следует из такого рассуждения:

$a(a+b)=aa+ab=0 \Rightarrow aa=-ab$; Но с другой стороны: $(a+b)a=aa+ba$; $\Rightarrow aa=-ba$ $\Rightarrow ab=ba$. ♦

Пример 35. Покажем, что кольцо из четырех элементов может быть не коммутативным. Введем группу по сложению, состоящую из двух элементов 0 и 1. Нейтральным элементом является 0. Следовательно 1+1=0.

Теперь рассмотрим множество из четырех элементов – прямое произведение такой группы на себя. Оно состоит из пар (a,b), где каждая из компонент может принимать значение 0 или 1: (0,0),(0,1),(1,0),(1,1).

Зададим операцию умножения: $(a+b)(c+d)=((a+b)c,(a+b)d)$.

Покажем ассоциативность:

$(a+b)((c+d)(e+f))=(a+b)((c+d)e,(c+d)f)=((a+b)(c+d)e,(a+b)(c+d)f)$.

С другой стороны,

$((a+b)(c+d))(e+f)=((a+b)c,(a+b)d)(e,f)=(((a+b)c+(a+b)d)e,((a+b)c+(a+b)d)f)=((a+b)(c+d)e,(a+b)(c+d)f)$.

Аналогично показывается выполнение двух законов дистрибутивности.

Но это кольцо не коммутативно. Действительно:

(1,0)(1,1)=((1+0)1,(1+0)1)=(1,1)

(1,1)(1,0)=((1+1)1,(1+1)0)=(0,0). ♦

В связи с вышеизложенным, возникает необходимость в следующем **определении**. Если $ab=0$ при $a\neq 0$ и $b\neq 0$ в кольце **K**, то a называется

левым, а b – *правым делителем нуля* (в коммутативных кольцах говорят просто о делителях нуля). Сам нуль в кольце $\mathbf{K}\neq 0$ – тривиальный делитель нуля. Если других делителей нуля нет, то $\mathbf{K}$ называется *кольцом без делителей нуля*. Коммутативное кольцо с единицей $1\neq 0$ и без делителей нуля называют *целостным кольцом* (*кольцом целостности* или *областью целостности*).

Справедлива следующая теорема.

Теорема 8. Нетривиальное коммутативное кольцо $\mathbf{K}$ с единицей является целостным тогда и только тогда, когда в нем выполнен закон сокращения:

$ab=ac,\ a\neq 0 \Rightarrow b=c$

для всех $a,b,c\in\mathbf{K}$.

Доказательство. В самом деле, если в $\mathbf{K}$ имеет место закон сокращения, то из $ab=0=a0$ следует, что либо $a=0$, либо $a\neq 0$, но $b=0$. Обратно, если $\mathbf{K}$ – область целостности, то $ab=ac$, $a\neq 0 \Rightarrow a(b-c)=0 \Rightarrow b-c=0 \Rightarrow b=c$. Теорема доказана. ♦

В кольце $\mathbf{K}$ с единицей естественно рассматривать множество обратимых элементов, т.е. $aa^{-1}=a^{-1}a=1$. Точнее следовало бы говорить об элементах обратимых справа или слева, но в коммутативных кольцах, а также в кольцах без делителей нуля эти понятия совпадают. Действительно, из $ab=1$ следует $aba=a$, откуда $a(ba-1)=0$. Так как $a\neq 0$, то $ba-1=0$, т.е. $ba=1$.

Пример 36. В кольце $\mathbf{M_n}$ обратимые элементы – это в точности матрицы с отличным от нуля определителем. ♦

Обратимый элемент a не может быть делителем нуля. Действительно, если $ab=0$ тогда $a^{-1}(ab)=0 \Rightarrow (a^{-1}a)b=0 \Rightarrow 1b=0 \Rightarrow b=0$ (аналогично $ba=0 \Rightarrow b=0$). Неудивительно, поэтому, что имеет место

Теорема 9. Все обратимые элементы кольца $\mathbf{K}$ с единицей составляют группу $\mathbf{U}(\mathbf{K})$ по умножению.

Доказательство. Действительно, так как множество $\mathbf{U}(\mathbf{K})$ содержит единицу, а ассоциативность по умножению в $\mathbf{K}$ выполнена, то нам нужно убедиться в замкнутости множества $\mathbf{U}(\mathbf{K})$, т. е. проверить, что произведение ab любых двух элементов a и b из $\mathbf{U}(\mathbf{K})$ будет снова принадлежать $\mathbf{U}(\mathbf{K})$. Но это очевидно, поскольку $(ab)^{-1}=b^{-1}a^{-1}$, $(abb^{-1}a^{-1}=a(bb^{-1})a^{-1}=aa^{-1}=1)$, и, значит, ab обратим. Теорема доказана. ♦

7. ПОЛЕ

7.1. ПОНЯТИЕ ПОЛЯ

В предыдущем разделе мы получили весьма интересный класс колец – так называемые *кольца с делением*, или *тела*, заменив в определении кольца аксиому (К2) на существенно более сильное условие (К2'): относительно операции умножения множество $\mathbf{K}^*=\mathbf{K}\setminus\{0\}$ является группой. Кольцо с делением, стало быть, всегда будет без делителей нуля, и каждый ненулевой элемент в нем обратим. Операции сложения и умножения в коммутативном кольце становятся почти полностью симметричными. В математике такая структура носит специальное название – поле. Итак, дадим его **определение**.

Поле **P** – это коммутативное кольцо с единицей $1\neq0$, в котором каждый элемент $\boldsymbol{a}\neq0$ обратим. Группа $\mathbf{P}^*=\mathbf{U}(\mathbf{K})$ называется *мультипликативной группой поля*.

Поле представляет собой гибрид двух абелевых групп – аддитивной и мультипликативной, связанных законом дистрибутивности (теперь уже одним ввиду коммутативности). Произведение $\boldsymbol{ab}^{-1}$ записывается обычно в виде дроби (или отношения) $\boldsymbol{a}/\boldsymbol{b}$. Следовательно, дробь $\boldsymbol{a}/\boldsymbol{b}$, имеющая смысл только при $\boldsymbol{b}\neq0$, является решением уравнения $\boldsymbol{bx}=\boldsymbol{a}$. Действия с дробями подчиняются нескольким правилам:

$$\boldsymbol{a}/\boldsymbol{b}=\boldsymbol{c}/\boldsymbol{d} \Leftrightarrow \boldsymbol{ad}=\boldsymbol{bc},\ \boldsymbol{b},\boldsymbol{d}\neq0,$$
$$\boldsymbol{a}/\boldsymbol{b}+\boldsymbol{c}/\boldsymbol{d}=(\boldsymbol{ad}+\boldsymbol{bc})/\boldsymbol{bd},\ \boldsymbol{b},\boldsymbol{d}\neq0,$$
$$-(\boldsymbol{a}/\boldsymbol{b})=(-\boldsymbol{a}/\boldsymbol{b})=(\boldsymbol{a}/-\boldsymbol{b}),\ \boldsymbol{b}\neq0,$$
$$(\boldsymbol{a}/\boldsymbol{b})(\boldsymbol{c}/\boldsymbol{d})=(\boldsymbol{ac}/\boldsymbol{bd})\quad \boldsymbol{b},\boldsymbol{d}\neq0,$$
$$(\boldsymbol{a}/\boldsymbol{b})^{-1}=\boldsymbol{b}/\boldsymbol{a},\quad \boldsymbol{a},\boldsymbol{b}\neq0.$$

Это обычные школьные правила, но их надо не запоминать, а выводить из аксиом поля. Посмотрим, как это делается для второго правила. Пусть $\boldsymbol{x}=\boldsymbol{a}/\boldsymbol{b}$ и $\boldsymbol{y}=\boldsymbol{c}/\boldsymbol{d}$ – решения уравнений $\boldsymbol{bx}=\boldsymbol{a}$ и $\boldsymbol{dy}=\boldsymbol{c}$. Из этого следует: $\boldsymbol{dbx}=\boldsymbol{da}$ и $\boldsymbol{bdy}=\boldsymbol{bc} \Rightarrow \boldsymbol{bd}(\boldsymbol{x}+\boldsymbol{y})=\boldsymbol{da}+\boldsymbol{bc} \Rightarrow \boldsymbol{t}=\boldsymbol{x}+\boldsymbol{y}=(\boldsymbol{da}+\boldsymbol{bc})/\boldsymbol{bd}$ – единственное решение уравнения $\boldsymbol{bdt}=\boldsymbol{da}+\boldsymbol{bc}$.

Подполем **F** поля **P** называется подкольцо в **P**, само являющееся полем.

Пример 37. Поле рациональных чисел **Q** – подполе поля вещественных чисел **R**. ♦

В случае $\mathbf{F}\subset\mathbf{P}$ говорят также, что поле **P** является *расширением* своего подполя **F**. Из определения подполя следует, что ноль и единица поля **P** будут содержаться также в **F** и служить для **F** нулем и единицей. Если взять в **P** пересечение $\mathbf{F_1}$ всех подполей, содержащих **F** и некоторый элемент $\boldsymbol{a}\in\mathbf{P}$, не принадлежащий **F**, то $\mathbf{F_1}$ будет минимальным полем, содержащим множество $\{\mathbf{F},\boldsymbol{a}\}$. Говорят, что расширение $\mathbf{F_1}$ поля **F** получено

присоединением к **F** элемента a, и отражают этот факт в записи $\mathbf{F_1}=\mathbf{F}(a)$. Аналогично можно говорить о подполе $\mathbf{F_1}=\mathbf{F}(a_1,\ldots a_n)$ поля **P**, полученном присоединением к **F** n элементов $a_1,\ldots a_n$ поля **P**.

Пример 38. Небольшая проверка показывает, что $\mathbf{Q}(\sqrt{2})$ совпадает с множеством чисел $a+b\sqrt{2}$ $a,b\in\mathbf{Q}$, поскольку $\left(\sqrt{2}\right)^2=2$ и $1/(a+b\sqrt{2}) = (a/(a^2-2b^2))-(b/(a^2-2b^2))\sqrt{2}$ при $a+b\sqrt{2}\neq 0$. То же самое относится к $\mathbf{Q}(\sqrt{3})$, $\mathbf{Q}(\sqrt{5})$ и т.д. ♦

Поля **P** и **P'** называются изоморфными, если они изоморфны как кольца. По определению $f(0)=0'$ и $f(1)=1'$ для любого изоморфного отображения f. Не имеет смысла говорить о гомоморфизмах полей, так как $\mathrm{Ker}\, f \neq 0 \Rightarrow f(a)=0$, $a\neq 0 \Rightarrow f(1)=f(aa^{-1})=f(a)f(a^{-1})=0f(a^{-1})=0 \Rightarrow f(b)=f(1b)=0f(b)=0$ $\forall b \Rightarrow \mathrm{Ker}\, f = \mathbf{P}$. Напротив, автоморфизмы, т.е. изоморфные отображения поля **P** на себя, связаны с самыми глубокими свойствами полей и являются мощным инструментом для изучения этих свойств.

7.2. ПОЛЯ ГАЛУА

В 6.2 было построено конечное кольцо классов вычетов $\mathbf{Z_m}$ с элементами $0,1,\ldots m-1$ и операциями сложения и умножения. Если $m=st$, $s>1$, $t>1$, то $st=m=0$, т.е. s и t – делители нуля в $\mathbf{Z_m}$. Если $m=p$ – простое число, то справедлива

Теорема 10. Кольцо классов вычетов $\mathbf{Z_m}$ является полем тогда и только тогда, когда $m=p$ – простое число.

Доказательство. Нам достаточно установить существование для каждого $s\in\mathbf{Z_p}$ обратного элемента $s'\in\mathbf{Z_p}$ (целые числа s и s' не должны, очевидно, делится на p).

Рассмотрим элементы s, $2s$, …, $(p-1)s$. Они все отличны от нуля, так как $s\neq 0 \pmod m \Rightarrow ks\neq 0 \pmod m$ при $k=1,2,\ldots,p-1$. Здесь используется простота p. По этой же причине элементы s, $2s$, …, $(p-1)s$ все различны: из $ks=ls$, $k<l$ следовало бы $(l-k)s=0$, что неверно. Итак, последовательность элементов s, $2s$, …, $(p-1)s$ совпадает с последовательностью переставленных каким-то образом элементов $1,2,\ldots,p-1$. В частности, найдется s', $1\le s'\le p-1$, для которого $s's=1$, т.е. s' – обратный к s элемент. Теорема доказана. ♦

Следствие (малая теорема Ферма). Для любого целого числа m, не делящегося на простое число p, имеет место сравнение:

$$m^{p-1}\equiv 1 \pmod m.$$

Доказательство. Мультипликативная группа $\mathbf{Z}^*_{\mathbf{p}}$ имеет порядок $p-1$. Из теоремы Лагранжа, утверждающей, что порядок конечной группы делится на порядок каждой своей подгруппы, следует, что $p-1$ делится на порядок любого элемента из $\mathbf{Z}^*_{\mathbf{p}}$. Таким образом, $1=(m)^{p-1}=m^{p-1}$, т.е. $m^{p-1}-1=0$. Следствие доказано. ♦

8. КОЛЬЦО МНОГОЧЛЕНОВ

8.1. ПОНЯТИЕ КОЛЬЦА МНОГОЧЛЕНОВ

Многочлены составляют старый и хорошо изученный раздел традиционной алгебры. На языке многочленов формулируются или решаются самые различные задачи математики. Тому есть множество причин, и одна из них заключается в свойстве универсальности кольца многочленов.

Пусть **K** – коммутативное кольцо с единицей 1, **A –** некоторое его подкольцо, содержащее 1. Если $t\in\mathbf{K}$, то наименьшее подкольцо в **K**, содержащее **A** и t, будет, очевидно, состоять из элементов вида:

$$a(t)=a_0+a_1t+a_2t^2+\ldots+a_nt^n, \qquad (*)$$

где $a_i\in\mathbf{A}$, $n\in\mathbf{Z}$, $n\in\geq 0$. Мы обозначим его символом $\mathbf{A}[t]$ и назовем кольцом, полученным из **A** присоединением элемента t, а выражение (*) – многочленом от t с коэффициентами в **A**. Что понимать под суммой и произведением многочленов, видно из простейшего примера.

Пример 39.

$a(t)+b(t)=(a_0+a_1t+a_2t^2)+(b_0+b_1t+b_2t^2)=(a_0+b_0)+(a_1+b_1)t+(a_2+b_2)t^2$.

$a(t)b(t)=ab_0+(a_0b_1+a_1b_0)t+(a_0b_2+a_1b_1+a_2b_0)t^2+(a_1b_2+a_2b_1)t^3+a_2b_2t^4$. ♦

Очевидно, что приведение подобных членов в $\mathbf{A}[t]$ основано на попарной перестановочности всех элементов a_i, b_j, t^k.

Теперь самое время вспомнить, что t – наугад взятый элемент кольца **K**, и поэтому внешне различные выражения (*) могут на самом деле совпадать. Если, скажем, **A**=**Q**, $t=\sqrt{2}$, то $t^2=2$ и $t^3=2t$ – соотношения, которые никоим образом не вытекают из формальных правил. Чтобы прийти к привычному понятию многочлена, необходимо освободится от всех таких побочных соотношений, для чего под t следует понимать произвольный элемент, не обязательно содержащийся в **K**. Он призван играть чисто вспомогательную роль. Гораздо большее значение имеют правила, по которым составляются коэффициенты выражений $a(t)+b(t)$, $a(t)b(t)$. Имея в виду эти предварительные замечания, перейдем к точному определению алгебраического объекта, называемого многочленом, и собрания таких объектов – кольца многочленов.

Пусть **A** – произвольное коммутативное кольцо с единицей. Построим новое кольцо **B**, элементами которого являются бесконечные упорядоченные последовательности:

$$f=(f_0, f_1, f_2, \ldots),\ f\in\mathbf{A}, \qquad (8.1)$$

такие, что все f_i, кроме конечного их числа, равны нулю. Определим на множестве **B** операции сложения и умножения, полагая

$$f+g=(f_0, f_1, f_2, \ldots)+(g_0, g_1, g_2, \ldots)=(f_0+g_0,\ f_1+g_1,\ f_2+g_2, \ldots),$$

$$fg=h=(h_0, h_1, h_2, \ldots),$$

где $h_k=\sum_{i+j=k} f_ig_j$, $k=0,1,2,\ldots$

Ясно, что в результате сложения и умножения получится снова последовательность вида (8.1) с конечным числом отличных от нуля членов, т.е. элементов из **B**. Проверка всех аксиом кольца, кроме, разве, аксиомы ассоциативности, очевидна. В самом деле, поскольку сложение двух элементов из **B** сводится к сложению конечного числа элементов из кольца **A**, (**B**,+) является абелевой группой с нулевым элементом (0, 0, …) и элементом $-\boldsymbol{f}=(-\boldsymbol{f}_0, -\boldsymbol{f}_1, -\boldsymbol{f}_2, \ldots)$ обратным к произвольному $\boldsymbol{f}=(\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2, \ldots)$. Далее, коммутативность умножения следует непосредственно из симметричности выражения элементов $\boldsymbol{h}_k$ через $\boldsymbol{f}_i$ и $\boldsymbol{g}_j$. Это же выражение показывает, что в **B** выполнен закон дистрибутивности $(\boldsymbol{f}+\boldsymbol{g})\boldsymbol{h}=\boldsymbol{f}\boldsymbol{h}+\boldsymbol{g}\boldsymbol{h}$. Что касается ассоциативности операции умножения, то пусть $\boldsymbol{f}=(\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2, \ldots)$, $\boldsymbol{g}=(\boldsymbol{g}_0, \boldsymbol{g}_1, \boldsymbol{g}_2, \ldots)$, $\boldsymbol{h}=(\boldsymbol{h}_0, \boldsymbol{h}_1, \boldsymbol{h}_2, \ldots)$ – три произвольных элемента множества **B**. Тогда $\boldsymbol{f}\boldsymbol{g}=\boldsymbol{d}=(\boldsymbol{d}_0, \boldsymbol{d}_1, \boldsymbol{d}_2, \ldots)$, где $\boldsymbol{d}_l=\sum_{i+j=l} f_i g_j$, $l=0,1,2,\ldots$, а $(\boldsymbol{f}\boldsymbol{g})\boldsymbol{h}=\boldsymbol{d}\boldsymbol{h}=\boldsymbol{e}=(\boldsymbol{e}_0, \boldsymbol{e}_1, \boldsymbol{e}_2, \ldots)$, где $\boldsymbol{e}_s=\sum_{l+k=s} d_l h_k=\sum_{l+k=s}\left(\sum_{i+j=l} f_i g_j\right)h_k=\sum_{i+j+k=s} f_i g_j h_k$. Вычисление $\boldsymbol{f}(\boldsymbol{g}\boldsymbol{h})$ дает тот же результат. Итак, **B** – коммутативное кольцо с единицей (1,0,0,…).

Последовательности $(\boldsymbol{a}, 0, 0, \ldots)$ складываются и умножаются так же, как элементы кольца **A**. Это позволяет отождествить такие последовательности с соответствующими элементами из **A**, т.е. положить $\boldsymbol{a}=(\boldsymbol{a}, 0, 0, \ldots)$ для всех $\boldsymbol{a}\in\mathbf{A}$. Тем самым **A** становится подкольцом кольца **B**. Обозначим далее (0, 1, 0, 0,…) через **X** и назовем **X** *переменной* (или *неизвестной*) над **A**. Используя введенную на **B** операцию умножения, получим:

$$\begin{aligned}&\mathbf{X}=(0, 1, 0, 0,\ldots),\\ &\mathbf{X}^2=(0, 0, 1, 0,\ldots),\\ &\ldots\ \ldots\ldots\ldots\\ &\mathbf{X}^n=(0, 0, 0, 0,\ldots 0, 1, 0, \ldots).\end{aligned}\qquad (8.2)$$

Кроме того, ввиду (8.2) и включения $\mathbf{A}\subset\mathbf{B}$, имеем:

$$(0, 0, \ldots 0, \boldsymbol{a}, 0, \ldots)=\boldsymbol{a}\mathbf{X}^n=\mathbf{X}^n\boldsymbol{a}.$$

Итак, если $\boldsymbol{f}_n$ – последний отличный от нуля член последовательности $\boldsymbol{f}=(\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2, \ldots \boldsymbol{f}_n, 0,\ldots)$, то в новых обозначениях:

$$\boldsymbol{f}=(\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2,\ldots \boldsymbol{f}_{n-1},0,\ldots)+\boldsymbol{f}_n\mathbf{X}^n=(\boldsymbol{f}_0, \boldsymbol{f}_1, \boldsymbol{f}_2,\ldots \boldsymbol{f}_{n-2},0,\ldots)+\boldsymbol{f}_{n-1}\mathbf{X}^{n-1}+\boldsymbol{f}_n\mathbf{X}^n=$$
$$\boldsymbol{f}_0+\boldsymbol{f}_1\mathbf{X}^1+\boldsymbol{f}_2\mathbf{X}^2+\ldots+\boldsymbol{f}_n\mathbf{X}^n. \qquad (8.3)$$

Такое представление элемента $\boldsymbol{f}$ однозначно, поскольку $\boldsymbol{f}_0, \boldsymbol{f}_1, \ldots \boldsymbol{f}_n$ в правой части (8.3) – это члены последовательности $(\boldsymbol{f}_0, \boldsymbol{f}_1, \ldots \boldsymbol{f}_n, 0,\ldots)$, которая равна нулю тогда и только тогда, когда $\boldsymbol{f}_0=\boldsymbol{f}_1=\ldots=\boldsymbol{f}_n=0$.

Введенное таким образом кольцо **B** обозначается через **A**[**X**] и называется *кольцом многочленов над* **A** *от одной переменной* **X**, а его элементы – *многочленами* (или *полиномами*).

Введение заглавной буквы **X** – намеренное, чтобы отличить наш специально выделенный многочлен $\boldsymbol{f}=\mathbf{X}$ от теоретико-функциональной переменной $\boldsymbol{x}$, пробегающей какое-то множество значений. Это чисто вре-

менное соглашение, придерживаться которого в будущем не обязательно. Более привычной является запись многочлена f в виде:

$$f(\mathbf{X})=a_0 + a_1x^1 + a_2x^2+\ldots+a_nx^n,$$

или

$$f(\mathbf{X})=a_0x^n + a_1x^{n-1} + a_2x^{n-2}+\ldots+a_{n-1}x+ a_n.$$

Элементы a_i называются *коэффициентами* многочлена f. Многочлен f – нулевой, когда все его коэффициенты равны нулю. Коэффициент при x в нулевой степени называется еще постоянным членом. Если $a_n\neq0$ ($a_0\neq0$), то a_n (a_0) называют *старшим* коэффициентом, а n – *степенью* многочлена и пишут $n=\deg f$. Нулевому многочлену приписывают степень $-\infty$ ($\infty+(-\infty)=-\infty$, $-\infty+n=-\infty$, $-\infty<n$ для каждого $n\in\mathbf{N}$).

Роль единицы кольца $\mathbf{A}[\mathbf{X}]$ играет единичный элемент 1 кольца $\mathbf{A}$, рассматриваемый как многочлен нулевой степени. Непосредственно из определения операций сложения и умножения в $\mathbf{A}[\mathbf{X}]$ следует, что для любых двух многочленов

$$f=f_0+f_1x^1+f_2x^2+\ldots+f_nx^n,\ \ g=g_0+g_1x^1+g_2x^2+\ldots+g_mx^m, \qquad (8.4)$$

степеней n и m соответственно имеют место неравенства:

$$\deg(f+g)\le\max(\deg f, \deg g), \qquad \deg(fg)\le\deg f+\deg g. \qquad (8.5)$$

Второе из неравенств (8.5) заменяется равенством

$$\deg(fg)=\deg f+\deg g$$

всякий раз, когда произведение f_ng_m старших многочленов (8.4) отлично от нуля, поскольку

$$fg=f_0g_0+(f_0g_1+f_1g_0)x+\ldots+(f_ng_m)x^{n+m}.$$

Но это значит, что верна

Теорема 11. Если $\mathbf{A}$ – целостное кольцо, то и $\mathbf{A}[\mathbf{X}]$ является целостным. ♦

8.2. АЛГОРИТМ ДЕЛЕНИЯ В A[X]

В $\mathbf{A}[\mathbf{X}]$ над целостным кольцом $\mathbf{A}$ имеет место алгоритм деления с остатком, аналогичный рассмотренному в 2.2.

Теорема 12. Пусть $\mathbf{A}$ – целостное кольцо и g – многочлен в $\mathbf{A}[\mathbf{X}]$ со старшим коэффициентом, обратимым в $\mathbf{A}$. Тогда каждому многочлену $f\in\mathbf{A}[\mathbf{X}]$ сопоставляется одна и только одна пара многочленов q, $r\in\mathbf{A}[\mathbf{X}]$, для которых

$$f=qg+r, \quad \deg r < \deg g. \qquad (8.6)$$

Доказательство. Пусть

$$f=a_0x^n + a_1x^{n-1} + a_2x^{n-2}+\ldots+ a_n,$$
$$g=b_0x^m + b_1x^{m-1} + b_2x^{m-2}+\ldots+ b_m,$$

где $a_0b_0\neq0$ и $b_0|1$. Применим индукцию по n. Если $n=0$ и $m=\deg g>\deg f=0$, то положим $q=0$, $r=f$, а если $n=m=0$, то $r=0$ и $q=a_0b_0^{-1}$. Допустим, что теорема доказана для всех полиномов степени $<n$ ($n>0$). Без ограничения

общности считаем, что $m \le n$, поскольку в противном случае возьмем $q=0$ и $r=f$. Раз это так, то

$$f = a_0 b_0^{-1} x^{n-m} g + f',$$

где $\deg f' < n$. По индукции мы можем найти q' и r', для которых $f' = q'g + r$, причем $\deg r < m$. Положив

$$q = a_0 b_0^{-1} x^{n-m} g + q',$$

мы придем к паре многочленов с нужными свойствами.

Обращаясь к свойству единственности частного q и остатка r, предположим, что

$$qg + r = f = q'g + r'.$$

Тогда $(q'-q)g = r-r'$. По теореме 11 имеем: $\deg (r-r') = \deg (q'-q) + \deg g$, что в наших условиях возможно только при $r'=r$ и $q'=q$.

Наконец, приведенные рассуждения показывают, что коэффициенты частного q и остатка r принадлежат тому же целостному кольцу **A**, т.е. $f, g \in \mathbf{A}[\mathbf{X}]$. Теорема полностью доказана. ♦

Замечание. Процесс евклидова деления многочлена f на g упрощается, если g – *унитарный многочлен*, т.е. его старший коэффициент равен единице. Делимость f на унитарный многочлен g эквивалентна равенству нулю остатка r при евклидовом деления f на g. ♦

Следствие. Все идеалы кольца многочленов $\mathbf{P}[\mathbf{X}]$ над полем **P** – главные.

Доказательство. Пусть **T** – какой-то ненулевой идеал в $\mathbf{P}[\mathbf{X}]$. Выберем многочлен $t = t(\mathbf{X})$ минимальный степени, содержащийся в **T**. Если f – любой многочлен из **T**, то деление с остатком на t (**P** – поле, поэтому нет нужды заботится об обратимости старшего коэффициента у $t(\mathbf{X})$) даст нам равенство $f = qt + r$, $\deg r < \deg t$. Из него следует, что $r \in \mathbf{T}$, поскольку f , t, qt – элементы идеала. Ввиду выбора t нам остается заключить, что $r=0$. Значит, $f(\mathbf{X})$ делится на $t(\mathbf{X})$ и $\mathbf{T} = t\mathbf{P}[\mathbf{X}]$, т.е. **T** состоит из многочленов, делящихся на $t(\mathbf{X})$, что и требовалось доказать. ♦

8.3. РАЗЛОЖЕНИЕ В КОЛЬЦЕ МНОГОЧЛЕНОВ

В произвольном целостном кольце **K** обратимые элементы называются *делителями единицы*, или *регулярными элементами*. Совершенно очевидно, что многочлен $f \in \mathbf{A}[\mathbf{X}]$ обратим (регулярен) в точности тогда, когда $\deg f = 0$ и $f = f_0$ – обратимый элемент кольца **A**, поскольку $fg = 1 \Rightarrow \deg f + \deg g = \deg 1 = 0$.

Говорят, что элемент $b \in \mathbf{K}$ *делится* на $a \in \mathbf{K}$ (или b *кратен* a), если существует такой элемент $c \in \mathbf{K}$, что $b = ac$ (обозначается $a|b$). Если $a|b$ и $b|a$, то a и b называются *ассоциированными* элементами. Тогда $b = ua$, где $u|1$. В силу сделанного выше замечания ассоциированность многочленов $f, g \in \mathbf{A}[\mathbf{X}]$ означает, что они отличаются обратимым множителем из **A**.

Элемент $p \in \mathbf{K}$ называется *простым* (или *неразложимым*), если p необратим и его нельзя представить в виде $p=ab$, где a, b – необратимые элементы. В поле $\mathbf{P}$ каждый ненулевой элемент обратим, и в $\mathbf{P}$ нет простых элементов. Простой элемент кольца $\mathbf{A}[X]$ называется чаще *неприводимым многочленом*.

Отметим следующие основные свойства отношения делимости в целостном кольце $\mathbf{K}$.

1) Если $a|b$ и $b|c$, то $a|c$. Действительно, мы имеем $b=ab'$, $c=bc'$, где $b',c' \in \mathbf{K}$. Поэтому $c=(ab')c'=a(b'c')$.
2) Если $c|a$ и $c|b$, то $c|(a \pm b)$. В самом деле, по условию $a=ca'$, $b=cb'$ для некоторых $a',b' \in \mathbf{K}$, и ввиду дистрибутивности $a \pm b=c(a' \pm b')$.
3) Если $a|b$, то $a|bc$. Ясно, что $b=ab' \Rightarrow bc=(ab')c=a(b'c)$.
4) Комбинируя 2) и 3), получаем, что, если каждый из элементов $b_1,b_2,\ldots, b_m \in \mathbf{K}$ делится на $a \in \mathbf{K}$, то на a будет делиться также элемент $b_1c_1+b_2c_2+\ldots+b_mc_m$, где $c_1,c_2,\ldots c_m$ – произвольные элементы.

Теперь введем понятие, которое нам понадобится в дальнейшем. Говорят, что целостное кольцо $\mathbf{K}$ – *кольцо с однозначным разложением на простые множители* (или $\mathbf{K}$ – *факториальное кольцо*), если любой элемент $a \neq 0$ из $\mathbf{K}$ можно представить в виде

$$a=up_1p_2\ldots p_r,$$

где u – обратимый элемент, а $p_1,p_2,\ldots p_r$ – простые элементы (не обязательно попарно различные), причем из существования другого такого разложения $a=vq_1q_2\ldots q_s$ следует, что $r=s$, и при надлежащей нумерации элементов p_i и q_j будет

$$q_1=u_1p_1, \ \ldots q_r=u_rp_r.,$$

где $u_1,u_2,\ldots u_r$ – обратимые элементы.

Допуская в равенстве $a=up_1p_2\ldots p_r$ значение $r=0$, мы принимаем соглашение, что обратимые элементы в $\mathbf{K}$ тоже имеют разложение на простые множители. Ясно, что если p – простой, а u – обратимый элемент, то ассоциированный с p элемент up – тоже простой. В кольце $\mathbf{Z}$ с обратимыми элементами 1 и –1 отношение порядка ($a<b$) дает возможность выделить *положительное* простое число p из двух возможных простых элементов $\pm p$. В кольце $\mathbf{P}[X]$ удобно рассматривать *унитарные* (с равным единице старшим коэффициентом) неприводимые многочлены.

Справедлива следующая общая

Теорема 13. Пусть $\mathbf{K}$ – произвольное целостное кольцо с разложением на простые множители. Однозначность разложения в $\mathbf{K}$ (факториальность $\mathbf{K}$) имеет место тогда и только тогда, когда любой простой элемент $p \in \mathbf{K}$, делящий произведение $ab \in \mathbf{K}$, делит по крайней мере один из множителей a, b.

Без доказательства. ♦

В произвольном целостном кольце **K** элемент $a\neq 0$ вообще не обязан допускать разложение типа $a=up_1p_2\ldots p_r$. Что более интересно, имеются целостные кольца, в которых разложение на простые множители хотя и возможно, но не является однозначным, т.е. условие теоремы 13, кажущиеся тривиальным, не всегда выполняется.

Пример 40. Рассмотрим мнимое квадратичное поле $Q(\sqrt{-5})$, в нем – целостное кольцо $\mathbf{K}=\{a+b\sqrt{-5}\,|\,a, b\in\mathbf{Z}\}$. Норма $\mathbf{N}(a+b\sqrt{-5})=a^2+5b^2$ каждого отличного от нуля элемента $\chi\in\mathbf{K}$– целое положительное число. Если χ в **K**, то $\mathbf{N}(\chi)^{-1}=\mathbf{N}(\chi^{-1})\in\mathbf{Z}$, откуда $\mathbf{N}(\chi)=1$. Это возможно лишь при $b=0$, $a=\pm 1$. Таким образом, в **K**, как и **Z**, обратимыми элементами являются только ± 1. Если $\chi=\varepsilon\chi_1\chi_2\ldots\chi_r\neq 0$, $\varepsilon=\pm 1$, то $\mathbf{N}(\chi)=\mathbf{N}(\chi_1)\ldots\mathbf{N}(\chi_r)$. Так как $1<\mathbf{N}(\chi_i)\in\mathbf{Z}$, то при заданном χ число множителей r не может неограниченно расти. Стало быть, разложение на простые множители в **K** возможно.

Вместе с тем число 9 (да и не только оно) допускает два существенно различных разложения на простые множители:

$$9=3\cdot 3=(2+\sqrt{-5})\cdot(2-\sqrt{-5}).$$

Неассоциированность элементов 3 и $2\pm\sqrt{-5}$ очевидна. Далее, $\mathbf{N}(3)=\mathbf{N}(2\pm\sqrt{-5})=9$. Поэтому из разложения $\chi=\chi_1\chi_2$ для $\chi=3$ или $2\pm\sqrt{-5}$ с необратимыми χ_1,χ_2 следовало бы $9=\mathbf{N}(\chi)=\mathbf{N}(\chi_1)\mathbf{N}(\chi_2)$, т.е. $\mathbf{N}(\chi_i)=3$, i=1,2, что невозможно, поскольку уравнение $x^2+5y^2=3$ с $x,y\in\mathbf{Z}$ неразрешимо. Этим доказана простата элементов 3 и $2\pm\sqrt{-5}$. ♦

8.4. ФАКТОРИАЛЬНОСТЬ ЕВКЛИДОВЫХ КОЛЕЦ

Алгоритм деления с остатком в **Z** и **P**[**X**] делает естественным рассмотрение целостного кольца **K**, в котором каждому элементу $a\neq 0$ поставлено в соответствие неотрицательное целое число $\delta(a)$, т.е. определено отображение

$$\delta:\ \mathbf{K}\backslash\{0\}=\mathbf{K}^*\to\mathbf{N}\cup\{0\}$$

так, что при этом выполняются условия:

(E1) $\delta(ab)\geq\delta(a)$ для всех $a,b\neq 0$ из **K**;

(E2) Каковы бы ни были $a,b\in\mathbf{K}$, $b\neq 0$, найдутся $q,r\in\mathbf{K}$ (q – *частное*, r – *остаток*), для которых

$$a=qb+r;\qquad \delta(r)<\delta(b)\ \text{или}\ r=0. \tag{8.7}$$

Целостное кольцо **K** с этими свойствами называется *евклидовым кольцом*.

Пример 41. Полагая $\delta(a)=|a|$ для $a\in\mathbf{Z}$ и $\delta(a)=\deg a$ для $a\in\mathbf{P}[\mathbf{X}]$, мы приходим к выводу, что **Z** и **P**[**X**] – евклидовы кольца. ♦

В евклидовых кольцах существует способ нахождения НОД(a,b), называемый *алгоритмом последовательного деления* или *алгоритмом Евклида* и заключающийся в следующем.

Пусть даны ненулевые элементы $\boldsymbol{a},\boldsymbol{b}$ евклидова кольца **K**. Применяя достаточно большое (но конечное) число раз предписание (E2), мы получим систему равенств типа (8.7) с последним нулевым остатком:

$$\begin{aligned}
&\boldsymbol{a}=\boldsymbol{q}_1\boldsymbol{b}+\boldsymbol{r}_1, && \delta(\boldsymbol{r}_1)<\delta(\boldsymbol{b})\\
&\boldsymbol{b}=\boldsymbol{q}_2\boldsymbol{r}_1+\boldsymbol{r}_2, && \delta(\boldsymbol{r}_2)<\delta(\boldsymbol{r}_1)\\
&\boldsymbol{r}_1=\boldsymbol{q}_3\boldsymbol{r}_2+\boldsymbol{r}_3, && \delta(\boldsymbol{r}_3)<\delta(\boldsymbol{r}_2)\\
&\ldots\ldots\ldots\ldots\ldots\ldots && \\
&\boldsymbol{r}_{k-2}=\boldsymbol{q}_k\boldsymbol{r}_{k-1}+\boldsymbol{r}_k, && \delta(\boldsymbol{r}_k)<\delta(\boldsymbol{r}_{k-1})\\
&\boldsymbol{r}_{k-1}=\boldsymbol{q}_{k+1}\boldsymbol{r}_k, && \boldsymbol{r}_{k+1}=0.
\end{aligned} \qquad (8.8)$$

Это действительно так, поскольку убывающая цепочка неотрицательных целых чисел $\delta(\boldsymbol{b}) > \delta(\boldsymbol{r}_1) > \delta(\boldsymbol{r}_2) > \ldots$ должна оборваться, а обрыв может произойти только за счет обращения в нуль одного из остатков. Последний отличный от нуля остаток $\boldsymbol{r}_k = \text{НОД}(\boldsymbol{a},\boldsymbol{b})$.

Непосредственным шагом к установлению факториальности евклидова кольца служит

Лемма 2. Всякое евклидово кольца **K** является кольцом с разложением (т.е. любой элемент $\boldsymbol{a}\neq 0$ из **K** записывается в виде $\boldsymbol{a}=\boldsymbol{u}\boldsymbol{p}_1\boldsymbol{p}_2\ldots\boldsymbol{p}_r$).

Доказательство. Пусть элемент $\boldsymbol{a}\in\mathbf{K}$ обладает собственным делителем $\boldsymbol{b}$: $\boldsymbol{a}=\boldsymbol{b}\boldsymbol{c}$, где $\boldsymbol{b}$ и $\boldsymbol{c}$ – необратимые элементы (другими словами, $\boldsymbol{a}$ и $\boldsymbol{b}$ не ассоциированы). Докажем, что $\delta(\boldsymbol{b})<\delta(\boldsymbol{a})$.

В самом деле, согласно (E1), непосредственно имеем $\delta(\boldsymbol{b})\le\delta(\boldsymbol{b}\boldsymbol{c})=\delta(\boldsymbol{a})$. Предположив выполнение равенства $\delta(\boldsymbol{b})=\delta(\boldsymbol{a})$, воспользуемся условием (E2) и найдем $\boldsymbol{q},\boldsymbol{r}$ с $\boldsymbol{b}=\boldsymbol{q}\boldsymbol{a}+\boldsymbol{r}$, где $\delta(\boldsymbol{r})<\delta(\boldsymbol{a})$ или же $\boldsymbol{r}=0$. Случай $\boldsymbol{r}=0$ отпадает ввиду неассоциированности $\boldsymbol{a}$ и $\boldsymbol{b}$. По той же причине $1-\boldsymbol{q}\boldsymbol{c}\neq 0$. Стало быть, снова по (E2) (с заменой $\boldsymbol{a}$ на $\boldsymbol{b}$) имеем:

$$\delta(\boldsymbol{a})=\delta(\boldsymbol{b})\le\delta(\boldsymbol{b}(1-\boldsymbol{q}\boldsymbol{c}))=\delta(\boldsymbol{b}-\boldsymbol{q}\boldsymbol{a})=\delta(\boldsymbol{r})<\delta(\boldsymbol{a})$$

– противоречие. Итак, $\delta(\boldsymbol{b})<\delta(\boldsymbol{a})$.

Если теперь $\boldsymbol{a}=\boldsymbol{a}_1\boldsymbol{a}_2\ldots\boldsymbol{a}_n$, где все $\boldsymbol{a}_i$ необратимы, то $\boldsymbol{a}_{m+1}\boldsymbol{a}_{m+2}\ldots\boldsymbol{a}_n$ – собственный делитель $\boldsymbol{a}_m\boldsymbol{a}_{m+1}\boldsymbol{a}_{m+2}\ldots\boldsymbol{a}_n$, и по доказанному:

$$\delta(\boldsymbol{a})=\delta(\boldsymbol{a}_1\boldsymbol{a}_2\ldots\boldsymbol{a}_n)>\delta(\boldsymbol{a}_2\ldots\boldsymbol{a}_n)>\ldots>\delta(\boldsymbol{a}_n)>\delta(1).$$

Эта строго убывающая цепочка неотрицательных чисел имеет длину $\boldsymbol{n}\le\delta(\boldsymbol{a})$. Значит, имеется максимальное разложение $\boldsymbol{a}$ на простые множители. Лемма доказана. ♦

Теорема 14. Всякое евклидово кольцо **K** факториально (**K** обладает свойством однозначности разложения на простые множители).

Доказательство. С учетом леммы и критерия факториальности, содержащегося в теореме 13, нам остается показать, что если $\boldsymbol{p}$ – простой кольца **K**, делящий произведение $\boldsymbol{b}\boldsymbol{c}$ каких-то элементов $\boldsymbol{b},\boldsymbol{c}\in\mathbf{K}$, то $\boldsymbol{p}$ делит либо $\boldsymbol{b}$, либо $\boldsymbol{c}$.

Действительно, при $\boldsymbol{b}=0$ или $\boldsymbol{c}=0$ доказывать нечего. Если же $\boldsymbol{b}\boldsymbol{c}\neq 0$ и $\boldsymbol{d}=\text{НОД}(\boldsymbol{b},\boldsymbol{c})$, то $\boldsymbol{d}$, будучи делителем простого элемента $\boldsymbol{p}$, либо равен 1 (точнее, является делителем 1), либо ассоциирован с $\boldsymbol{p}$. В первом случае $\boldsymbol{b}$

и p оказываются взаимно простыми, и поэтому $p|c$. Во втором случае $d=up$, $u|1$ и, значит, $p|b$. Теорема доказана. ♦

Следствие. Кольца **Z** и **P**[**X**] – факториальны (**P** – произвольное поле). ♦

8.5. НЕПРИВОДИМЫЕ МНОГОЧЛЕНЫ

Специализируя данное ранее определение простого элемента, еще раз подчеркнем, что многочлен f ненулевой степени из кольца **P**[**X**] называется неприводимым в **P**[**X**] (или неприводимым над полем **P**), если он не делится ни на какой многочлен $g\in$**P**[**X**], у которого $0 < \deg g < \deg f$. В частности, всякий многочлен первой степени неприводим. Совершенно очевидно, что неприводимость многочлена степени >1 или разложение его на простые множители – понятия, тесно связанные с основным полем **P**, как это показывает многочлен в поле комплексных чисел **C** – $x^2+1=(x-i)(x+i)$. Многочлен x^4+4 приводим над **Q**, хотя об этом нелегко догадаться:

$$x^4+4=(x^2-2x+2)(x^2+2x+2).$$

Оба множителя справа неприводимы не только над **Q**, но и над **R**, будучи приводимы, однако, над **C**.

Как простых чисел в **Z**, так и унитарных *неприводимых многочленов над произвольным полем* **P** *бесконечно много*.

В случае бесконечного поля **P** это ясно: достаточно рассмотреть неприводимые многочлены вида $x-c, c\in$**P**.

Если же поле **P** конечно, то годится рассуждение Евклида. Именно, пусть уже найдены n неприводимых многочленов $p_1,p_2,\ldots p_n$. Многочлен $f=p_1p_2\ldots p_n+1$ имеет хотя бы один унитарный простой делитель, поскольку $\deg f \geq n$. Обозначим его через p_{n+1}. Он отличен от $p_1,p_2,\ldots p_n$, поскольку из $p_{n+1}=p_s$ для какого-то $s\leq n$ следовало бы $p_s|(f-p_1p_2\ldots p_n)$, т.е. $p_s|1$, что и требовалось доказать.

Так как над конечным полем количество многочленов заданной степени ограничено, то можно сделать следующее полезное **заключение**:

Над любым конечным полем существуют неприводимые многочлены сколь угодно высокой степени.

А теперь приведем (без доказательства)

Критерий неприводимости (Эйзенштейн).

Пусть

$$f(x)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n\in Z[x]$$

– унитарный многочлен над **Z**, все коэффициенты $a_1,\ldots,a_n$ которого делятся на некоторое простое число p, но a_n не делится на p^2. Тогда $f[x]$ неприводим над **Q**. ♦

Примечание. Критерий действует и в том случае, когда старший коэффициент отличен от 1, но не делится на p. ♦

Пример 42. Многочлен $f(x)=x^{p-1}+x^{p-2}+\ldots+x+1$ неприводим над **Q** при любом простом p. Для этого достаточно заметить, что вопрос о неприводимости $f(x)$ эквивалентен вопросу о неприводимости многочлена

$$f(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=x^{p-1}+C_1^p x^{p-2}+\ldots+C_{p-2}^p x+C_{p-1}^p,$$

где $C_m^n=\frac{n!}{m!(n-m)!}$, и коэффициенты, кроме старшего, делятся на p в первой степени, и, следовательно, применим критерий Эйзенштейна. ♦

ЗАКЛЮЧЕНИЕ

Для профессионального понимания криптографических алгоритмов и умения оценивать их сильные и слабые стороны необходима соответствующая математическая подготовка. Это объясняется тем, что современная криптография основана на глубоких результатах таких разделов математики, как теория сложности вычислений, теория чисел, алгебра и т.д. Представленный материал содержит основные сведения теории чисел, алгебры, необходимые для понимания основ современной криптографии. Желающие более глубоко ознакомиться с этими математическими дисциплинами могут обратится к рекомендуемой литературе.

ЛИТЕРАТУРА

1. Ван дер Ваден Б.Л. Алгебра, пер. с нем. 2–изд.– М.: Наука, 1979. 352 с.
2. Воеводин В.В. Линейная алгебра. – М.:Наука, 1980. 348 с.
3. Гантмахер Ф.Р. Теория матриц. – М.:Наука, 1966. 576 с.
4. Гельфанд И.М., Райков Д.А., Шилов Г.Е. Коммутативные нормированные кольца. – М.:Физматгиз, 1959. 356 с
5. Ибрагимов Н.Х. Группы преобразований в математической физике. М.:Наука, 1983. 280 с.
6. Кон П. Универсальная алгебра. - М.:Мир. - 1968. 351 с
7. Левин М. Криптография. Руководство пользователя. - М.: Познавательная книга плюс, 2001, - 320 с.
8. Смирнов В.И. Курс высшей математики, том III, часть I – М:. Наука, Главная редакция физико-математической литературы, 1974. 324 с.
9. Фрид Э. Элементарное введение в абстрактную алгебру. Пер. с венгер.– М.:Мир, 1979. 260 с.

ОГЛАВЛЕНИЕ

ИСТОРИЯ КАФЕДРЫ

1945-1966 гг. РЛПУ (кафедра радиолокационных приборов и устройств). Решением Советского правительства в августе 1945 г. в ЛИТМО был открыт факультет электроприборостроения.

Приказом по институту от 17 сентября 1945 г. на этом факультете была организована кафедра радиолокационных приборов и устройств, которая стала готовить инженеров, специализирующихся в новых направлениях радиоэлектронной техники, таких как радиолокация, радиоуправление, теленаведение и др. Организатором и первым заведующим кафедрой был д.т.н., профессор С. И. Зилитинкевич (до 1951 г.). Выпускникам кафедры присваивалась квалификация инженер-радиомеханик, а с 1956 г. – радиоинженер (специальность 0705).

В разные годы кафедрой заведовали доцент Б.С. Мишин, доцент И.П. Захаров, доцент А.Н. Иванов.

1966–1970 гг. КиПРЭА (кафедра конструирования и производства радиоэлектронной аппаратуры). Каждый учебный план специальности 0705 коренным образом отличался от предыдущих планов радиотехнической специальности своей четко выраженной конструкторско–технологической направленностью. Оканчивающим институт по этой специальности присваивалась квалификация инженер–конструктор–технолог РЭА.

Заведовал кафедрой доцент А.Н. Иванов.

1970–1988 гг. КиПЭВА (кафедра конструирования и производства электронной вычислительной аппаратуры). Бурное развитие электронной вычислительной техники и внедрение ее во все отрасли народного хозяйства потребовали от отечественной радиоэлектронной промышленности решения новых ответственных задач. Кафедра стала готовить инженеров по специальности 0648. Подготовка проводилась по двум направлениям– автоматизация конструирования ЭВА и технология микроэлектронных устройств ЭВА.

Заведовали кафедрой д.т.н., проф. В.В. Новиков (до 1976 г.), затем проф. Г.А. Петухов.

1988–1997 гг. МАП (кафедра микроэлектроники и автоматизации проектирования). Кафедра выпускала инженеров–конструкторов–технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность 2205). Выпускники этой кафедры имеют хорошую технологическую подготовку и успешно работают как в производстве полупроводниковых интегральных микросхем, так и при их проектировании, используя современные методы автоматизации проектирования. Инженеры специальности 2205 требуются микроэлектронной промышленности и предприятиям–разработчикам вычислительных систем.

Кафедрой с 1988 г. по 1992 г. руководил проф. С.А. Арустамов, затем снова проф. Г.А. Петухов.

С **1997 г. ПКС** (кафедра проектирования компьютерных систем). Кафедра выпускает инженеров по специальности 220500 "Проектирование и технология электронно-вычислительных средств". Область профессиональной деятельности выпускников включает в себя проектирование, конструирование и технологию электронных вычислительных средств, отвечающих целям их функционирования, требованиям надежности, дизайна и условиям эксплуатации. Кафедра готовит также специалистов по специальности 075400 – "Комплексная защита объектов информатизации". Область профессиональной деятельности включает в себя методы, средства и системы обеспечения защиты всех видов конфиденциальной информации.

С 1996 г. кафедрой заведует доктор технических наук, доцент Ю.А. Гатчин.

За время своего существования кафедра выпустила 4037 инженера, из них по специальности 0705 – 2472 чел. и по специальности 0648 (2205) – 1565 чел. На кафедре защищено 50 кандидатских и 9 докторских диссертаций.