ГРУППЫ, КОЛЬЦА И ПОЛЯ

Понятия абстрактных алгебраических объектов (групп, полей, колец, а также и других, которые здесь не рассматриваются) возникли в математике исследовании общих свойств операций сложения и умножения.

1. Основные определения и примеры

Определение 1. Множество G, снабжённое операцией «$\cdot$», условно называемой умножением[1], называется *группой*, если эта операция обладает следующими свойствами:

1) для любых трёх элементов выполняется равенство $f \cdot (g \cdot h) = (f \cdot g) \cdot h$ (*ассоциативность*);
2) существует такой элемент $e \in G$, что $e \cdot g = g \cdot e = g$ для любого $g \in G$ (существование *единицы*)[2];
3) для любого элемента $g \in G$ существует такой элемент $g^{-1} \in G$, что $g \cdot g^{-1} = g^{-1} \cdot g = e$ (существование *обратного элемента*).

Группа называется *коммутативной* (или *абелевой*), если $f \cdot g = g \cdot f$ для всех $f, g \in G$.

Подмножество $H \subset G$ называется *подгруппой* в G, если из $f, g \in G$ следует, что $f \cdot g \in G$.

Очевидно, если множество H — подгруппа, то оно само является группой.

Пример 1. В любой группе, содержащей более одного элемента, есть по крайней мере одна подгруппа, не совпадающая с самой группой, — это подгруппа состоящая из единичного элемента. Она же является самой простой из существующих групп. Ниже мы, конечно, рассмотрим более сложные и интересные примеры.

Пример 2. Множество рациональных чисел, отличных от нуля, образует группу относительно операции умножения, а подмножество положительных рациональных чисел является подгруппой. Точно так же группу по умножению образует множество всех действительных чисел, а подмножество положительных чисел — её подгруппа.

Пример 3. Множество $\mathbb{Z}$ всех целых чисел является группой относительно сложения, а все чётные числа образуют подгруппу (в отличие от нечётных). Заметим, что пока все рассмотренные нами группы были коммутативными.

Определение 2. Отображение $\varphi\colon G \to H$ группы G в группу H называется *гомоморфизмом*, если $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g)$ для всех $f, g \in G$. Гомоморфизм называется *эпиморфизмом*, если он является сюръекцией, и *мономорфизмом*, если он — инъекция. Если гомоморфизм является одновременно и эпиморфизмом, и мономорфизмом, то он называется *изоморфизмом*. Группы, между которыми существует изоморфизм, называются *изоморфными*, и с алгебраической точки зрения они неразличимы.

Пример 4. Сопоставим каждому целому числу n число $2n$. Это сопоставление — гомоморфизм группы целых чисел в группу чётных чисел, являющееся изоморфизмом.

Пример 5. Множество всех $\mathbb{R}$ действительных чисел является коммутативной группой относительно сложения, а множество $\mathbb{R}^+$ всех положительных чисел — коммутативной группой относительно умножения. Отображение

$$\exp\colon \mathbb{R} \to \mathbb{R}^+, \quad x \mapsto \mathrm{e}^x$$

[1]Это название действительно условно: в конкретных примерах в качестве группового умножения может выступать и умножение, и сложение, и операции иного характера.

[2]Как будет видно из примеров, этот элемент, в зависимости от операции в группе, может действительно быть единицей, может совпадать с нулём, а может быть ни тем и не другим.

— изоморфизм этих групп. Обратным к нему является отображение

$$\ln\colon \mathbb{R}^+ \to \mathbb{R}, \quad x \mapsto \ln x.$$

Рассмотрим ещё несколько примеров.

Пример 6 (группы подстановок). Пусть $\mathbb{N}_2 = \{1, 2\}$ — множество, состоящее из первых двух натуральных чисел. Существуют два отображения $\mathbb{N}_2 \to \mathbb{N}_2$, являющиеся взаимно-однозначными соответствиями:

$$\sigma_{12}\colon \begin{cases} 1 \to 1, \\ 2 \to 2 \end{cases} \quad \text{и} \quad \sigma_{21}\colon \begin{cases} 1 \to 2, \\ 2 \to 1. \end{cases}$$

Обозначим множество этих отображений через Σ_2 и в качестве групповой операции рассмотрим композицию отображений. Тогда произведение элементов будет задаваться следующей таблицей

$\circ$	σ_{12}	σ_{21}
σ_{12}	σ_{12}	σ_{21}
σ_{21}	σ_{21}	σ_{12}

Легко проверить, что относительно введённой операции Σ_2 является группой, единицей которой служит отображение σ_{12}, и $\sigma_{21}^{-1} = \sigma_{21}$.

Точно так же можно рассмотреть множество $\mathbb{N}_3 = \{1, 2, 3\}$ и всевозможные взаимно-однозначные отображения этого множества в себя. Их будет шесть:

$$\sigma_{123}\colon \begin{cases} 1 \to 1, \\ 2 \to 2, \\ 3 \to 3, \end{cases} \quad \sigma_{132}\colon \begin{cases} 1 \to 1, \\ 2 \to 3, \\ 3 \to 2, \end{cases} \quad \sigma_{213}\colon \begin{cases} 1 \to 2, \\ 2 \to 1, \\ 3 \to 3, \end{cases} \quad \sigma_{231}\colon \begin{cases} 1 \to 2, \\ 2 \to 3, \\ 3 \to 1, \end{cases} \quad \sigma_{312}\colon \begin{cases} 1 \to 3, \\ 2 \to 1, \\ 3 \to 2, \end{cases} \quad \sigma_{321}\colon \begin{cases} 1 \to 3, \\ 2 \to 2, \\ 3 \to 1. \end{cases}$$

Вновь взяв за групповую операцию композицию отображений, мы получим следующую таблицу умножения:

$\circ$	σ_{123}	σ_{132}	σ_{213}	σ_{231}	σ_{312}	σ_{321}
σ_{123}	σ_{123}	σ_{132}	σ_{213}	σ_{231}	σ_{312}	σ_{321}
σ_{132}	σ_{132}	σ_{123}	σ_{231}	σ_{213}	σ_{321}	σ_{312}
σ_{213}	σ_{213}	σ_{312}	σ_{123}	σ_{321}	σ_{132}	σ_{231}
σ_{231}	σ_{231}	σ_{321}	σ_{132}	σ_{312}	σ_{123}	σ_{213}
σ_{312}	σ_{312}	σ_{213}	σ_{321}	σ_{123}	σ_{231}	σ_{132}
σ_{321}	σ_{321}	σ_{231}	σ_{312}	σ_{132}	σ_{213}	σ_{123}

Эта таблица тоже задаёт группу, обозначаемую через Σ_3. Эта группа не коммутативна.

Вообще, рассмотрев множество $\mathbb{N}_k = \{1, 2, \ldots, k\}$ и все его взаимно-однозначные отображения в себя, мы получим группу Σ_k, называемую *группой подстановок* порядка k; она содержит $k!$ элементов. Если в Σ_k рассмотреть такие подстановки σ, что $\sigma(k) = k$, то они образуют подгруппу, изоморфную Σ_{k-1}.

Пример 7. Множество $\mathrm{GL}(n)$ всех невырожденных (т.е. обратимых) матриц размера $n \times n$ является группой по отношению к произведению матриц, называемой *полной линейной группой* (обратите внимание на то, что в $\mathrm{GL}(n)$ матрицы можно перемножать, но нельзя складывать). Отображение $\Delta\colon \mathrm{GL}(n) \to \mathbb{R} \setminus \{0\}$, сопоставляющее каждой матрице её определитель, является эпиморфизмом полной линейной группы в группу ненулевых действительных чисел.

Матрицы с положительным определителем образуют подгруппу полной линейной группы. Матрицы, чей определитель равен 1, также образуют подгруппу в $\mathrm{GL}(n)$.

Пример 8. Рассмотрим в группе $\mathrm{GL}(2)$ матрицы $A_{12} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ и $A_{21} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Они образуют подгруппу, изоморфную группе Σ_2. Аналогичным образом, в $\mathrm{GL}(3)$ можно рассмотреть матрицы

$$A_{123} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_{132} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_{213} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$A_{231} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_{312} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad A_{321} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

и они образуют подгруппу, изоморфную Σ_3.

Вообще, если в $\mathrm{GL}(n)$ рассмотреть все матрицы, в каждой строке и столбце которых будет стоять ровно по одной единице, а остальные элементы будут нулевыми, то множество этих матриц (их будет ровно $n!$) будет являться подгруппой, изоморфной Σ_n. Матрицы этого вида, определитель которых равен единице (таких матриц $\frac{n!}{2}$), также образует группу, называемую *группой чётных подстановок* и обозначаемую через Σ_n^+. Например, группа Σ_3^+ состоит из матриц A_{123}, A_{231} и A_{312} (или, что то же самое, из подстановок σ_{123}, σ_{231} и σ_{312}).

Рассмотрим последний пример группы.

Пример 9. Пусть $\mathrm{SO}(2)$ — множество поворотов плоскости вокруг некоторой выбранной точки. Композиция двух поворотов является поворотом и, поскольку поворот — отображение плоскости в себя, композиция является ассоциативной. Поворот на 0 градусов выполняет роль единичного элемента. Таким образом, $\mathrm{SO}(2)$ — группа.

Сопоставим повороту на угол φ матрицу $A_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$. Очевидно, $A_\varphi \circ A_\psi = A_{\varphi+\psi}$. Это означает, что композиции поворотов соответствует композиция матриц, т.е. мы построили гомоморфизм группы $\mathrm{SO}(2)$ в группу $\mathrm{GL}(2)$. Этот гомоморфизм является мономорфизмом.

Изучим теперь абстрактные алгебраические объекты, снабжённые двумя операциями.

Определение 3. Множество R, наделённое операциями *сложения* «$+$» и *умножения* «$\cdot$», называется *кольцом*, если эти операции обладают следующими свойствами:

1) для любых элементов a и $b \in R$ имеет место равенство $a + b = b + a$ (сложение *коммутативно*);
2) если $c \in R$, то $(a + b) + c = a + (b + c)$ (сложение *ассоциативно*);
3) существует такой элемент $0 \in R$, что $0 + a = a + 0 = a$ для любого $a \in R$ (существование *нуля*);
4) для любого $a \in R$ существует такой элемент $-a \in R$, что $(-a) + a = a + (-a) = 0$ (существование *противоположного элемента*);
5) для любых элементов a, b и $c \in R$ выполняются равенства $a(b+c) = ab+ac$, $(a+b)c = ac+bc$ (*дистрибутивность* умножения относительно сложения).

Замечание 1. Из определения 3 следует, что всякое кольцо является коммутативной группой относительно умножения.

Определение 4. Кольцо R называется *кольцом с единицей*, если существует такой элемент $1 \in R$ (*единица* кольца), что $1 \cdot a = a \cdot 1$ для всех $a \in R$.

Определение 5. Кольцо R называется *ассоциативным*, если $a(bc) = (ab)c$ для любых элементов a, b и $c \in R$ (то есть если определённое в нём *умножение ассоциативно*).

Определение 6. Кольцо R называется *коммутативным*, если $ab = ba$ для любых элементов a и $b \in R$ (то есть если определённое в нём *умножение коммутативно*).

Определение 7. Коммутативное и ассоциативное кольцо R с единицей называется *полем*, если каждый ненулевой элемент $a \in R$ обладает *обратным*, то есть существует такой элемент a^{-1}, что $a^{-1}a = aa^{-1} = 1$.

Замечание 2. Для всякого поля R множество $R \setminus \{0\}$ его ненулевых элементов является коммутативной группой относительно умножения.

Рассмотрим примеры колец и полей.

Пример 10. Множество $\mathbb{Z}$ *целых чисел* образует кольцо относительно обычных операций сложения и умножения. Это кольцо коммутативно, ассоциативно и обладает единицей.

Пример 11. Подмножество $2\mathbb{Z} \subset \mathbb{Z}$, состоящее из всех *чётных* целых чисел, то есть чисел вида $2k$, $k \in \mathbb{Z}$, также является коммутативным и ассоциативным кольцом, но в этом кольце нет единицы.

Пример 12. Множество *нечётных* чисел не образует кольца, поскольку оно не замкнуто относительно сложения — сумма двух нечётных чисел чётна.

Пример 13. Множество $\mathbb{N} \subset \mathbb{Z}$ *натуральных чисел* также не является кольцом, поскольку число, противоположное натуральному, уже не является натуральным.

Пример 14. Множество $\mathrm{Mat}(n,n)$ *квадратных матриц* размера $n \times n$ является ассоциативным кольцом с единицей относительно сложения и композиции матриц. Однако это кольцо не коммутативно.

Пример 15. То же самое множество можно наделить другим умножение, взяв в качестве такового *коммутатор матриц*. Это тоже будет кольцом, но ни ассоциативным, ни коммутативным и без единицы.

Пример 16. Если V — векторное пространство размерности n, то можно рассмотреть множество $\mathrm{Lin}(V,V)$ *линейных операторов*, действующих в этом пространстве. Оно является ассоциативным кольцом с единицей относительно сложения и композиции операторов. Аналогично примеру 15 в этом множестве можно ввести другое умножение, рассмотрев коммутатор линейных операторов.

Пример 17. Множества $\mathbb{Q}$ рациональных чисел и $\mathbb{R}$ действительных чисел являются полями относительно обычных операций сложения и умножения чисел.

Пример 18. Множество $C(\mathbb{R})$, состоящее из функций, непрерывных на прямой, является кольцом, если сложение и умножение определить следующим образом:

$$(f+g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x)g(x), \qquad f, g \in C'(\mathbb{R}), \quad x \in \mathbb{R}. \tag{1}$$

Определение 8. Элементы a и b кольца R называются *делителями нуля*, если

1) сами они отличны от нуля, $a \neq 0$, $b \neq 0$,
2) их произведение равно нулю, $ab = 0$.

Пример 19. Функции

$$f(x) = |x| + x, \qquad g(x) = |x| - x$$

являются делителями нуля в кольце непрерывных функций на прямой.

Пример 20. Матрицы $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ и $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ являются делителями нуля в кольце $\mathrm{Mat}(2,2)$.

Определение 9. Пусть R и R' — кольца. Отображение $f\colon R \to R'$ называется *гомоморфизмом* колец, если

$$f(a+b) = f(a) + f(b), \quad f(ab) = f(a)f(b)$$

для любых элементов a, $b \in R$.

Определение 10. Пусть $f\colon R \to R'$ — гомоморфизм колец. Множество

$$\ker f = \{\, a \in R \mid f(a) = 0 \,\}$$

называется *ядром* гомоморфизма f. Множество

$$\mathrm{im}\, f = \{\, a' \in R' \mid a = f(a), a \in R \,\}$$

называется *образом* гомоморфизма f.

Определение 11. Пусть $f\colon R \to R'$ гомоморфизм колец.

1) f называется *мономорфизмом*, если $\ker f = 0$;
2) f называется *эпиморфизмом*, если $\mathrm{im}\, f = R'$;
3) f называется *изоморфизмом*, если он одновременно и эпиморфизм, и мономорфизм.

Пример 21. Сопоставим каждому действительному числу $r \in \mathbb{R}$ скалярную матрицу $r \cdot \mathbf{E}$ размера $n \times n$. Это определяет мономорфизм $\mathbb{R} \to \mathrm{Mat}(n, n)$.

Пример 22. Зафиксируем точку $x_0 \in \mathbb{R}$ и сопоставим каждой непрерывной функции $f \in C(\mathbb{R})$ её значение в точке x_0. Это — эпиморфизм $C(\mathbb{R}) \to \mathbb{R}$. Его ядро состоит из функций, обращающихся в нуль в точке x_0.

Пример 23. Рассмотрим n-мерное векторное пространство V и некоторый его базис $e_1, \ldots, e_n \in V$. Сопоставим каждому линейному оператору $A\colon V \to V$ его матрицу в этом базисе. Это сопоставление определяет изоморфизм $\mathrm{Lin}(V, V) \to \mathrm{Mat}(n, n)$. Заметим, что этот изоморфизм зависит от выбора базиса!

Предложение 1. *Пусть $f\colon R \to R'$ — гомоморфизм колец. Тогда*:

1) *если $a, b \in \operatorname{im} f$, то $a + b \in \operatorname{im} f$ и $ab \in \operatorname{im} f$;*
2) *если $a, b \in \ker f$, то $a + b \in \ker f$, а также $ac \in \ker f$ и $ca \in \ker f$ для любого $c \in R$.*

Определение 12. Подмножество $S \subset R$ называется *подкольцом*, если оно обладает свойствами, описанными в п. 1 предложения 1. Оно называется *идеалом*, если оно обладает свойствами, описанными в п. 2 этого предложения.

Пример 24. Множество скалярных матриц является подкольцом кольца диагональных матриц, а диагональные матрицы, в свою очередь, образуют подкольцо кольца *верхних треугольных матриц*[3].

Пример 25. Множество $2\mathbb{Z} \subset \mathbb{Z}$ чётных чисел является идеалом кольца целых чисел.

Пример 26. Множество $\mu(x_0) \subset C(\mathbb{R})$, состоящее из функций, обращающихся в нуль в точке $x_0 \in \mathbb{R}$, является идеалом кольца непрерывных функций.

2. Кольцо целых чисел

Главное свойство целых чисел — это свойство *делимости*.

Предложение 2. *Пусть m и n — целые числа и $n \neq 0$. Тогда существует единственная пара таких целых чисел q и r, что*

$$m = qn + r, \qquad 0 \leqslant r < |n|. \tag{2}$$

Число q называется (*неполным*) *частным* от деления m на n, а r — *остатком*.

Если в равенстве (2) $r = 0$, то говорят, что m *делится* на n (или *кратно* n). В этом случае n называется *делителем* числа m.

Определение 13. Целое число $p > 1$ называется *простым*, если оно делится только на себя и единицу.

Пример 27 (первые 10 простых чисел). Вот первые 10 простых чисел: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Теорема 1 (теорема Евклида). *Множество простых чисел бесконечно.*

Теорема 2 (основная теорема арифметики). *Любое натуральное число $n > 1$ единственным образом разлагается на простые множители. Точнее, существует единственный набор таких простых чисел $p_1 < p_2 < \cdots < p_k$, что*

$$n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}, \tag{3}$$

где $i_1, \ldots, i_k > 0$.

Определение 14. Пусть m и n — целые числа.

[3]Квадратная матрица (a_{ij}) называется *верхней треугольной*, если $a_{ij} = 0$ при $i > j$.

1) *Наибольшим общим делителем* (НОД) чисел m и n называется такой положительный общий делитель[4] этих чисел, на который делится любой другой их общий делитель.
2) Числа m и n называются *взаимно простыми*, если их НОД равен единице.
3) *Наименьшим общим кратным* (НОК) чисел m и n называется такое их положительное общее кратное, которое делит любое другое общее кратное этих чисел.

Предложение 3. *У любых двух ненулевых целых чисел существуют НОД и НОК.*

Нахождение НОД и НОК. Чтобы найти НОД и НОК чисел m и n, нужно:

1) Найти разложение (3) для чисел m и n.
2) Записать числа m и n в виде
$$m = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k},$$
$$n = p_1^{j_1} p_2^{j_2} \dots p_k^{j_k}.$$
Если какое-нибудь из чисел p_α не является делителем m или n, то соответствующий показатель степени равен нулю.
3) Взять числа $l_\alpha = \min(i_\alpha, j_\alpha)$. Тогда
$$\text{НОД} = p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}.$$
4) Взять числа $s_\alpha = \max(i_\alpha, j_\alpha)$. Тогда
$$\text{НОК} = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}.$$

Пример 28. Пусть $m = 72$, $n = 75$. Тогда
$$72 = 2^3 \cdot 3^2, \qquad 75 = 3 \cdot 5^2.$$
Значит,
$$72 = 2^3 \cdot 3^2 \cdot 5^0,$$
$$75 = 2^0 \cdot 3^1 \cdot 5^2.$$
Поэтому $l_1 = \min(3,0) = 0$, $l_2 = \min(2,1) = 1$, $l_3 = \min(0,2) = 0$, а $s_1 = \max(3,0) = 3$, $s_2 = \max(2,1) = 2$, $l_3 = \max(0,2) = 2$. Значит,
$$\text{НОД} = 2^0 \cdot 3^1 \cdot 5^0 = 3, \qquad \text{НОК} = 2^3 \cdot 3^2 \cdot 5^2 = 1800.$$

Алгоритм Евклида. Ещё один способ находить НОД двух чисел основан на следующем результате (который вытекает из равенства (2)).

Теорема 3 (алгоритм Евклида). *Пусть m_0 и m_1 — натуральные числа, $m_0 > m_1$ и m_1 не является делителем числа m_0. Тогда существуют такие целые числа q_0, $q_1, \dots, q_{k-1}$, q_k и m_2, $m_3, \dots, m_k$, что $m_0 > m_1 > \dots > m_k$, $a_k > 1$ и*
$$\begin{cases} m_0 = m_1 q_0 + m_2, \\ m_1 = m_2 q_1 + m_3, \\ \dots. \\ m_{k-2} = m_{k-1} q_{k-1} + m_k, \\ m_{k-1} = m_k q_k. \end{cases}$$
При этом m_k является наибольшим общим делителем чисел m_0 и m_1.

[4] То есть число, которое является делителем и m, и n.

Пример 29. Для чисел из примера 28 имеем

$$\begin{cases} 75 = 72 \cdot 1 + 3, \\ 72 = \boxed{3} \cdot 24. \end{cases}$$

Ещё один пример: пусть $m_0 = 165$, $m_1 = 35$. Тогда

$$\begin{cases} 165 = 35 \cdot 4 + 25, \\ 35 = 25 \cdot 1 + 10, \\ 25 = 10 \cdot 2 + 5, \\ 10 = \boxed{5} \cdot 2. \end{cases}$$

Позиционные системы счисления. Зафиксируем какое-нибудь натуральное число $n \neq 1$ рассмотрим произвольное целое m. Тогда, в силу (2), m можно представить в виде

$$m = q_1 n + r_0.$$

Если $q_1 \geqslant n$, то $q_1 = q_2 n + r_1$ и, следовательно,

$$m = q_2 n^2 + r_1 n + r_0.$$

Продолжая этот процесс, мы придём к представлению

$$m = q_k n^k + q_{k-1} n^{k-1} + \cdots + q_1 n + q_0, \tag{4}$$

где все числа q_i удовлетворяют неравенствам $0 \leqslant q_i < n$. Представление (4) называется записью числа n в *n-ичной системе счисления*, а числа q_i *n-ичными цифрами*. В этом случае пишут

$$m = (q_k q_{k-1} \dots q_1 q_0)_n.$$

Например, в двоичной системе имеются всего две цифры — 0 и 1 — и всякое число записывается в этой системе в виде

$$m = q_k \cdot 2^k + q_{k-1} \cdot 2^{k-1} + \cdots + q_1 \cdot 2 + q_0, \qquad q_0, q_1, \dots, q_k = 0, 1,$$

или $m = (q_k q_{k-1} \dots q_1 q_0)_2$.

Пример 30. Имеем,

$$1 = 1_2,\ 2 = 10_2,\ 3 = 11_2,\ 4 = 100_2,\ 5 = 101_2,\ 6 = 110_2, \dots$$

и

$$1 = 1_3,\ 2 = 2_3,\ 3 = 10_3,\ 4 = 11_3,\ 5 = 12_3,\ 6 = 200_2, \dots$$

Замечание 3. Если требуется перевести из десятичной в иную систему счисления дробное число, то его представляют в виде суммы целой и дробной частей, целую часть переводят так, как было описано выше, а для перевода дробной части используют алгоритм, который мы проиллюстрируем на примерах. Он состоит в последовательном умножении исходного числа на основание новой системы счисления и выписывании получающихся целых частей результатов.

Пример 31. Перевести число $0,125$ в двоичную систему. Имеем

$$\begin{array}{r} 0,125 \\ \times\ \ 2 \\ \hline \boxed{0},250 \\ \times\ \ 2 \\ \hline \boxed{0},500 \\ \times\ \ 2 \\ \hline \boxed{1},000 \end{array}$$

Значит, $(0,125)_{10} = (0,001)_2$.

Пример 32. Перевести число $0,3$ в двоичную систему. Имеем

$$
\begin{array}{r}
0,3 \\
\hline
\boxed{0},6 \\
\hline
\boxed{1},2 \\
\hline
\boxed{0},4 \\
\hline
\boxed{0},8 \\
\hline
\boxed{1},6 \\
\hline
\boxed{1},2 \\
\hline
\ldots
\end{array}
\qquad
\begin{array}{r}
2 \\
\hline
2 \\
\hline
2 \\
\hline
2 \\
\hline
2 \\
\hline
2 \\
\hline
2 \\
\hline
\end{array}
$$

Значит, $(0,3)_{10} = (0,0100110011001...)_2$. В правой части этого равенства стоит периодическая дробь с периодом 1001.

Пример 33. Перевести число $0,2$ в троичную систему. Имеем

$$
\begin{array}{r}
0,2 \\
\hline
\boxed{0},6 \\
\hline
\boxed{1},8 \\
\hline
\boxed{2},4 \\
\hline
\boxed{1},2 \\
\hline
\boxed{0},6 \\
\hline
\boxed{1},8 \\
\hline
\ldots
\end{array}
\qquad
\begin{array}{r}
3 \\
\hline
3 \\
\hline
3 \\
\hline
3 \\
\hline
3 \\
\hline
3 \\
\hline
3 \\
\hline
\end{array}
$$

Значит, $(0,3)_{10} = (0,012101210121...)_3$. В правой части этого равенства стоит периодическая дробь с периодом 0121.

3. Кольца и поля вычетов

Зафиксируем натуральное число $k \neq 1$ и рассмотрим множество

$$\mathbb{Z}_n = \{\, 0, 1, \ldots, k-1 \,\} \tag{5}$$

всевозможных остатков от деления на k. Определим на множестве $\mathbb{Z}_k$ операции *сложения* и *умножения* следующим образом

$$a + b = \text{остаток от деления суммы } a \text{ и } b \text{ на } k \tag{6}$$

и

$$ab = \text{остаток от деления произведения } a \text{ и } b \text{ на } k. \tag{7}$$

Теорема 4. *Относительно операций* (6) *и* (7) *множество* $\mathbb{Z}_k$ *является коммутативным и ассоциативным кольцом с единицей. Это кольцо является полем тогда и только тогда, когда* k *— простое число.*

Определение 15. Множество $\mathbb{Z}_k$, снабжённое операцией сложения (6) и умножения (7) называется *кольцом вычетов по модулю* k. Если k — простое число, то оно называется *полем вычетов*.

Пример 34. Структура кольца (поля) в $\mathbb{Z}_k$ задаётся *таблицами сложения и умножения*. Например, для поля $\mathbb{Z}_2$ эти таблицы имеют вид

$+$	0	1
0	0	1
1	1	0

,

$\cdot$	0	1
0	0	0
1	0	1

,

в поле $\mathbb{Z}_3$ —

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

,

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

,

а в кольце $\mathbb{Z}_6$ таблицы таковы:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	1	4

,

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

.

Кольца и поля вычетов являются частным случаем очень важной для алгебры конструкции. Пусть $S \subset R$ — идеал кольца R. Рассмотрим элемент $a \in R$ и подмножество $[a] \subset R$ всех таких элементов $a' \in R$, что $a' - a \in S$. Можно показать, что любые два таких подмножества либо совпадают, либо не пересекаются[5]. Обозначим через R/S множество таких подмножеств и положим

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [a \cdot b], \quad a, b \in R. \tag{8}$$

Предложение 4. *Относительно операций* (8) *множество* R/S *является кольцом, а отображение* $S \to R/S$*, сопоставляющее каждому элементу* $a \in S$ *подмножество* $[a] \subset S$*, — эпиморфизмом колец. Ядром этого эпиморфизма является идеал* S.

Определение 16. Кольцо R/S называется *факторкольцом* кольца R по идеалу S.

Пример 35. Пусть $R = \mathbb{Z}$ и

$$S = k \cdot \mathbb{Z} = \{\, kn \mid n \in \mathbb{Z} \,\}.$$

Тогда $S = k \cdot \mathbb{Z}$ — идеал кольца целых чисел, а факторкольцо $\mathbb{Z}/S$ изоморфно кольцу вычетов $\mathbb{Z}_k$.

4. Поле комплексных чисел

Мнимые числа — это прекрасное и чудесное убежище божественного духа, почти что амфибия бытия с небытием.
Готфрид Вильгельм Лейбниц

Комплексные числа возникли как обобщение чисел вещественных при попытках решать произвольные квадратные (и более общие) уравнения.

[5]Причина состоит в том, что отношение $a \sim a' \Leftrightarrow a' - a \in S$ является отношением эквивалентности.

Матричное представление. Рассмотрим матрицы вида

$$M(x,y)=\begin{pmatrix}x & -y\\ y & x\end{pmatrix}=x\cdot\mathbf{E}+y\cdot\mathbf{I},\ \text{где}\ \mathbf{E}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \mathbf{I}=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\quad x,y\in\mathbb{R}.$$

Имеют место равенства

$$\begin{pmatrix}x & -y\\ y & x\end{pmatrix}+\begin{pmatrix}x' & -y'\\ y' & x'\end{pmatrix}=\begin{pmatrix}x+x' & -y-y'\\ y+y' & x+x'\end{pmatrix},\quad \begin{pmatrix}x & -y\\ y & x\end{pmatrix}\cdot\begin{pmatrix}x' & -y'\\ y' & x'\end{pmatrix}=\begin{pmatrix}xx'-yy' & -xy'-x'y\\ xy'+x'y & xx'-yy'\end{pmatrix},$$

то есть

$$M(x,y)+M(x',y')=M(x+x',y+y'),\quad M(x,y)\cdot M(x',y')=M(xx'-yy',xy'+x'y).$$

В частности, $\mathbf{I}^2=\mathbf{I}\cdot\mathbf{I}=-\mathbf{E}$. При этом

$$\begin{vmatrix}x & -y\\ y & x\end{vmatrix}=x^2+y^2$$

и

$$\begin{pmatrix}x & -y\\ y & x\end{pmatrix}\cdot\begin{pmatrix}\frac{x}{x^2+y^2} & \frac{y}{x^2+y^2}\\ \frac{-y}{x^2+y^2} & \frac{x}{x^2+y^2}\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad x^2+y^2\neq 0,$$

то есть $M(x,y)\cdot M\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)=\mathbf{E}$.

Изучим, как действует матрица $\mathbf{I}$ в пространстве $\mathbb{R}^2$. Рассмотрим произвольный вектор $\bar v=(x,y)\in\mathbb{R}^2$. Тогда $\mathbf{I}\cdot\bar v=(-y,x)$ и поэтому

$$|\mathbf{I}\cdot\bar v|=|\bar v|,\quad(\bar v,\mathbf{I}\cdot\bar v)=0.$$

Значит, вектор $\mathbf{I}\cdot\bar v$ имеет ту же длину, что и $\bar v$, и перпендикулярен ему. *Действие матрицы* $\mathbf{I}$ *— это поворот плоскости на* 90° *против часовой стрелки.*

Поле комплексных чисел. Сопоставим матрице $M(x,y)$ точку $(x,y)\in\mathbb{R}^2$ и обозначим эту точку через $z=x+iy$. Операции сложения и умножения матриц перейдут в следующие:

$$z+z'=(x+x')+i(y+y'),\qquad zz'=(xx'-yy')+i(xy'+x'y).$$

Свойства:

$$z+z'=z'+z,\qquad z+(z'+z'')=(z+z')+z'',$$
$$z+0=z,\qquad z+(-z)=0,$$

где

$$0=0+i\cdot 0,\qquad -z=-x+i(-y),$$
$$zz'=z'z,\qquad z(z'z'')=(zz')z'',$$

и

$$z\cdot 1=z,\qquad zz^{-1}=1$$

где

$$1=1+i\cdot 0,\qquad z^{-1}=\frac{x}{x^2+y^2}-i\frac{y}{x^2+y^2},z\neq 0.$$

Величи́ны $z=x+iy$, которые складывают и умножают по указанным правилам, называются *компле́кснымu числами.* Множество всех комплексных чисел образует поле, которое обозначается через $\mathbb{C}$ и называется *полем комплексных чисел.* Частным от деления двух комплексных чисел z и z', $z'\neq 0$, называется комплексное число $\frac{z}{z'}=zz^{-1}$.

Если $z=x+iy$, то действительное число x называется *вещественной частью* комплексного числа z и обозначается через $\operatorname{Re}z$; число y называется *мнимой частью* комплексного числа z и обозначается через $\operatorname{Im}z$. Если $\operatorname{Im}z=0$, то есть $z=x$, то это действительное число. Числа,

у которых $\operatorname{Re} z = 0$, называются *чисто мнимыми*. Комплексное число $i = 0 + i \cdot 1$ называется *мнимой единицей*. При этом $i^2 = -1$.

Для всякого комплексного числа $z = x + iy$ число $\bar{z} = x - iy$ называется *комплексно сопряжённым* данному. Операция комплексного сопряжения $z \mapsto \bar{z}$ обладает следующими свойствами:

$$\overline{z + z'} = \bar{z} + \bar{z}', \quad \overline{zz'} = \bar{z}\bar{z}', \quad \bar{\bar{z}} = z, \quad z + \bar{z} = 2\operatorname{Re} z, \quad z - \bar{z} = 2i \operatorname{Im} z.$$

Комплексное число является действительным тогда и только тогда, когда $z = \bar{z}$, и чисто мнимым тогда и только тогда, когда $z = -\bar{z}$.

Замечание 4. Операция комплексного сопряжения является изоморфизмом поля комплексных чисел а себя.

Модуль и аргумент. Для любого комплексного числа z произведение $z\bar{z} = x^2 + y^2$ является действительным числом. Число

$$\rho = |z| = \sqrt{x^2 + y^2}$$

называется *модулем* числа z. Угол φ, для которого справедливы равенства

$$\sin\varphi = \frac{\operatorname{Im} z}{\rho}, \quad \cos\varphi = \frac{\operatorname{Re} z}{\rho},$$

называется *аргументом* комплексного числа z. Аргумент определён с точностью до 2π и обозначается через $\operatorname{Arg} z$. Значение аргумента, выбранное в интервале $(-\pi, \pi]$, называется *главным* и обозначается через $\arg z$.

Таким образом, любое комплексное число можно записать виде

$$z = \rho(\cos\varphi + i\sin\varphi).$$

Эта форма записи называется *тригонометрической*. Эта форма удобна для умножения и деления комплексных чисел:

$$zz' = \rho\rho'(\cos(\varphi + \varphi') + i\sin(\varphi + \varphi'))$$

и

$$\frac{z}{z'} = \frac{\rho}{\rho'}(\sin(\varphi - \varphi') + i\cos(\varphi - \varphi')),$$

а также

$$z^n = \rho^n(\sin(n\varphi) + i\cos(n\varphi)).$$

Последняя формула называется *формулой Муавра*.

Числа $\cos\varphi + i\sin\varphi$ записывают также в виде $\mathrm{e}^{i\varphi}$, или $\exp(i\varphi)$. Таким образом, каждое комплексное число можно представить как

$$z = \rho\mathrm{e}^{i\varphi} \equiv \exp(i\varphi).$$

Это называется *экспоненциальной*, или *показательной* формой записи. Имеют место равенства

$$\rho\mathrm{e}^{i\varphi}\rho'\mathrm{e}^{i\varphi'} = \rho\rho'\mathrm{e}^{i(\varphi+\varphi')}, \quad \frac{\rho\mathrm{e}^{i\varphi}}{\rho'\mathrm{e}^{i\varphi'}} = \frac{\rho}{\rho'}\mathrm{e}^{i(\varphi-\varphi')}$$

(в последнем случае $\rho \neq 0$).

Решение уравнений в комплексных числах. В 1799 году Карл Фридрих Гаусс доказал следующий фундаментальный результат:

Теорема 5 (основная теорема алгебры). *Любое уравнение вида*

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0 = 0, \quad a_n \neq 0, \tag{9}$$

где $a_0, \ldots, a_n$ — комплексные числа, имеет ровно n комплексных корней, если каждый корень считать с учётом его кратности.

Например, квадратные уравнения *всегда* имеют два корня (возможно, совпадающие), кубические — три и т.д.

Вычисление корней. Рассмотрим уравнение

$$z^n = x + iy.$$

Его решения — корни n-й степени из числа, стоящего в правой части. Представляя это число в тригонометрической форме и используя формулу Муавра, получаем n различных корней

$$z_k = \sqrt[n]{\rho}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right), \quad k = 0, 1, \ldots, n-1.$$

Таким образом, каждое комплексное (и, в частности, действительное!) число имеет n различных корней степени n. Например, корнями 4-й степени из единицы являются числа

$$1, i, -1, -i.$$

Выпишем выражение для *квадратного корня* из комплексного числа $p + iq$, не используя формулу Муавра. Пусть $z = x_i y$ — такое число, что $z^2 = p_i q$. Тогда

$$x^2 - y^2 = p, \qquad 2xy = q. \tag{10}$$

Следовательно, $y = \frac{q}{2p}$ и, значит,

$$x^2 - \frac{q^2}{4x^2} = p,$$

то есть

$$4x^4 - 4px^2 - q^2 = 0.$$

Это — биквадратное уравнении, и его вещественными корнями являются

$$x_{1,2} = \pm\sqrt{\frac{\sqrt{p^2+q^2}+p}{2}}, \qquad y_{1,2} = \pm\sqrt{\frac{\sqrt{p^2+q^2}-p}{2}}.$$

Из четырёх возможных комбинаций только две при возведении в квадрат дают исходное число:

$$\begin{cases} \pm\sqrt{\frac{\sqrt{p^2+q^2}+p}{2}} \pm i\sqrt{\frac{\sqrt{p^2+q^2}-p}{2}}, & \text{если } p \geqslant 0, \\ \pm\sqrt{\frac{\sqrt{p^2+q^2}+p}{2}} \mp i\sqrt{\frac{\sqrt{p^2+q^2}-p}{2}}, & \text{если } p < 0, \end{cases} \tag{11}$$

и именно они являются квадратными корнями из комплексного числа $p + iq$.

Решение квадратных уравнений. Рассмотрим уравнение

$$az^2 + bz + c = 0, \qquad a, b, c \in \mathbb{R}, \quad a \neq 0.$$

Его решениями являются

$$z_{1,2} = \begin{cases} \dfrac{-b \pm \sqrt{D}}{2a}, & D \geqslant 0, \\ \dfrac{-b \pm i\sqrt{-D}}{2a}, & D < 0, \end{cases}$$

где $D = b^2 - 4ac$. Заметим, что если корни комплексные (случай $D < 0$), то они комплексно сопряжены. Таким же свойством обладают решения любого уравнения (9) с действительными коэффициентами: если число z — его решение, то $\bar{z}$ также является решением.

Если уравнение имеет комплексные коэффициенты, то его решения имеют вид

$$z_{1,2} = \frac{-b + \sqrt{D}}{2a},$$

где $\sqrt{D}$ вычисляется по формулам (11).

Как и для уравнений с действительными коэффициентами, для произвольных квадратных уравнений справедлива

Теорема 6 (теорема Виета). *Пусть*

$$az^2 + bz + c = 0, \qquad a, b, c \in \mathbb{Z}, \quad a \neq 0,$$

и z_1, z_2 — *его корни. Тогда*

$$z_1 z_2 = \frac{c}{a}, \qquad z_1 + z_2 = -\frac{b}{a}. \tag{12}$$

5. Кольцо полиномов

Определение 17. Выражение вида

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \quad a_0, a_1, a_2, \ldots, a_n \in \mathbb{R},$$

называется *многочленом* (или *полиномом*) от переменной x. Числа $a_0, \ldots, a_n$ называются *коэффициентами* многочлена, а число n — его *степенью*, если $a_n \neq 0$.

Степень многочлена $P(x)$ обозначается через $\deg P(x)$. Многочлены можно складывать и перемножать, причём

$$\deg(P(x) + Q(x)) \leqslant \deg P(x) + \deg Q(x), \qquad \deg(P(x)Q(x)) = \deg P(x) + \deg Q(x). \tag{13}$$

Предложение 5. *Множество многочленов является ассоциативным и коммутативным кольцом с единицей.*

Кольцо многочленов обозначается через $\mathbb{R}[x]$.

Замечание 5. Вместо поля $\mathbb{R}$ в качестве коэффициентов можно взять поле комплексных чисел $\mathbb{C}$. Мы тоже получим кольцо, которое обозначается через $\mathbb{C}[x]$.

Замечание 6. Точно так же, как из кольца целых чисел было получено поле рациональных чисел, из кольца многочленов можно получить *поле рациональных дробей*. Оно состоит из отношений $\frac{P(x)}{Q(x)}$, где $P(x)$ и $Q(x)$ — многочлены и $Q(x) \neq 0$.

Благодаря соотношениям (13) кольцо многочленов обладает многими свойствами кольца целых чисел.

Предложение 6. *Пусть* $M(x)$ *и* $N(x)$ — *многочлены и* $N(x) \neq 0$. *Тогда существует единственная пара таких многочленов* $Q(x)$ *и* $R(x)$, *что*

$$M(x) = Q(x)N(x) + R(x), \qquad 0 \leqslant \deg R(x) < \deg N(x). \tag{14}$$

Многочлен $Q(x)$ называется (*неполным*) *частным* от деления $M(x)$ на $N(x)$, а $R(x)$ — *остатком*.

Если в равенстве (14) $R(x) = 0$, то говорят, что $M(x)$ *делится* на $N(x)$ (или *кратен* $N(x)$). В этом случае $N(x)$ называется *делителем* многочлена $M(x)$.

Теорема 7 (теорема Безу). *Остаток от деления любого многочлена* $M(x)$ *на многочлен* $N(x) = x - c$, $c \in \mathbb{R}$, *равен значению* $M(x)$ *при* $x = c$. *В частности,* $M(x)$ *делится на* $x - c$ *тогда и только тогда, когда* $M(c) = 0$.

Мы будем говорить, что c — *корень многочлена* $M(x)$, если $M(c) = 0$.

Замечание 7. Как и в кольце целых чисел, в кольце многочленов выполняется *алгоритм Евклида* (ср. с теоремой 3). Для них также можно определить понятия *наибольшего общего делителя* и *наименьшего общего кратного* (см. определение 14).

Роль простых чисел в кольце многочленов играют *неразложимые многочлены*.

Определение 18. Многочлен $P(x)$ называется *неразложимым*, если $\deg P(x) > 0$ и его нельзя представить в виде

$$P(x) = S(x)Q(x), \qquad \deg S(x) > 0, \quad \deg Q(x) > 0.$$

Из основной теоремы алгебры (теорема 5) и теоремы Безу (теорема 7) следует, что любой многочлен степени n однозначно представляется в виде

$$P(x) = a_n(x - c_1)^{n_1}(x - c_2)^{n_2} \dots (x - c_k)^{n_k}, \tag{15}$$

где $c_1 < \dots < c_k$ — различные комплексные корни уравнения $P(x) = 0$, а $n_1, \dots, n_k$, $n_i \neq 0$ — их кратности. При этом представление (15) единственно. Таким образом, справедлив следующий результат.

Предложение 7. *Над полем комплексных чисел неприводимыми являются многочлены первой степени и только они.*

Если же мы хотим оставаться внутри поля действительных чисел, то есть не рассматривать комплексные корни, то в этом случае предложение 7 становится неверным и результат более сложен. Именно, во-первых, заметим следующее. Пусть $P(x) \in \mathbb{R}[x]$ — многочлен с действительными коэффициентами и c — его (комплексный) корень. Тогда число $\bar{c}$, комплексно сопряжённое к c, также является его корнем. Отсюда следует описание неразложимых многочленов над полем действительных чисел.

Теорема 8. *В кольце $\mathbb{R}[x]$ неразложимыми являются многочлены первой степени, а также квадратные трёхчлены $\alpha x^2 + \beta x + \gamma$, для которых $D = \beta^2 - 4\alpha\gamma < 0$. При этом любой многочлен разлагается в произведение неприводимых*:

$$P(x) = a_n(x - c_1)^{n_1} \dots (x - c_k)^{n_k}(x^2 + p_1x + q_1)^{m_1} \dots (x^2 + p_sx + q_s)^{m_s}, \tag{16}$$

где все сомножители попарно различны, $p_i^2 - 4q_i < 0$, c_j — различные действительные корни многочлена $P(x)$ и

$$\deg P(x) = n_1 + \dots + n_k + 2(m_1 + \dots + m_s).$$

Факторкольца. Пусть $P(x) \in \mathbb{R}[x]$. Рассмотрим множество

$$(P) = \{\, Q(x)P(x) \mid Q(x) \in \mathbb{R}[x] \,\} \subset \mathbb{R}[x].$$

Предложение 8. *Множество (P) является идеалом кольца $\mathbb{R}[x]$. Более того, любой идеал этого кольца имеет вид (P) для некоторого многочлена $P(x) \in \mathbb{R}[x]$.*

Следовательно, для любого $P(x) \in \mathbb{R}[x]$ можно рассмотреть факторкольцо $\mathbb{R}[x]/(P)$.

Предложение 9. *Пусть $P(x) \in \mathbb{R}[x]$. Тогда*:

1) *если $P(x) = \alpha x + \beta$, $\alpha \neq 0$, то факторкольцо $\mathbb{R}[x]/(P)$ изоморфно полю действительных чисел $\mathbb{R}$;*
2) *если $P(x) = \alpha x^2 + \beta x + \gamma$, $\alpha \neq 0$ и $D = \beta^2 - 4\alpha\gamma < 0$, то факторкольцо $\mathbb{R}[x]/(P)$ изоморфно полю комплексных чисел $\mathbb{C}$;*
3) *если $P(x) = \alpha x^2 + \beta x + \gamma$, $\alpha \neq 0$ и $D = \beta^2 - 4\alpha\gamma \geqslant 0$, то факторкольцо $\mathbb{R}[x]/(P)$ является некоторым кольцом с делителями нуля.*

Чтобы описать умножение в кольце $\mathbb{R}[x]/(P)$, где $P(x) = \alpha x^2 + \beta x + \gamma$, заметим, что любой элемент $L \in \mathbb{R}[x]/(P)$ однозначно представляется в виде

$$L = ax + b, \qquad a, b \in \mathbb{R}.$$

Чтобы перемножить два элемента L_1 и L_2, нужно перемножить их как многочлены, а потом вычислить остаток от деления результата на $P(x) = \alpha x^2 + \beta x + \gamma$. Поэтому

$$(a_1x + b_1)(a_2x + b_2) = (a_1b_2 + a_2b_1 - \frac{\beta}{\alpha}a_1a_2)x + (b_1b_2 - \frac{\gamma}{\alpha}a_1a_2) \tag{17}$$

в факторкольце $\mathbb{R}[x]/(P)$.