Лекции по курсу "Алгебра"

Белоусов Григорий Николаевич

Оглавление

Мы будем придерживаться следующих обозначений.

Обозначения 0.1. Мы будем придерживаться следующих обозначений:

- $\mathbb{N}$ — множество натуральных чисел.
- $\mathbb{Z}$ — множество целых чисел.
- $\mathbb{Q}$ — множество рациональных чисел.
- $\mathbb{R}$ — множество вещественных чисел.
- $\forall$ — для любого.
- $\exists$ — существует.
- $\in$ — принадлежит.
- ∞ — бесконечность.

Глава 1

Группы

1. Перестановки

Рассмотрим конечное множество Ω, состоящее из n элементов. Занумеровав эти элементы, мы можем считать, что $\Omega = \{1, 2, \ldots, n\}$. Рассмотрим взаимно однозначные (биективные) отображения $\sigma\colon \Omega \to \Omega$. Такие отображения мы будем называть *перестановками* (*подстановками*). Мы можем записать перестановку в виде

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

Эта запись означает, что $\sigma(1) = i_1, \sigma(2) = i_2, \ldots, \sigma(n) = i_n$.

Пример 1.1. Вот несколько примеров подстановок.

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

Обозначим через S_n — множество всех перестановок из n элементов. Заметим, что число элементов в S_n равно $n!$.

Пусть $\sigma, \tau \in S_n$ — две перестановки. *Произведением подстановок* σ и τ мы будем называть композицию этих отображений, т.е. $(\sigma\tau) = \sigma(\tau(i))$. Заметим, что умножение производится с право на лево.

Пример 1.2. Пусть

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

Тогда

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

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

Этот пример показывает, что в общем случае $\sigma\tau \neq \tau\sigma$, т.е. умножение перестановок не коммутативно. Однако, поскольку перестановки это отображения, то их композиция ассоциативна, т.е. $(\sigma\tau)\pi = \sigma(\tau\pi)$. В множестве перестановок S_n существует единичный элемент

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

такой, что $e\sigma = \sigma e = \sigma$, для любого $\sigma \in S_n$. Поскольку любая перестановка σ это биективное отображение, то существует обратное отображение σ^{-1} такое, что $\sigma\sigma^{-1} = \sigma^{-1}\sigma = e$.

Утверждение 1.3. *Обратная перестановка единственна.*

Доказательство. Предположим противное, т.е. у σ существуют две обратные перестановки σ^{-1} и σ'. Тогда

$$\sigma' = \sigma' e = \sigma'(\sigma\sigma^{-1}) = (\sigma'\sigma)\sigma^{-1} = e\sigma^{-1} = \sigma^{-1}.$$

□

Теперь рассмотрим другую запись перестановок. Пусть $\sigma \in S_n$. Возьмем произвольный элемент $i_1 \in \Omega$. Пусть $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2)$ и т.д. Поскольку Ω — конечное множество, а отображение σ биективно (в частности инъективно), то существует i_k такое, что $i_1 = \sigma(i_k)$. Таким образом, мы получили цикл

$$i_1 \to i_2 \to \cdots \to i_k \to i_1.$$

Его можно записать как $(i_1 i_2 \dots i_k)$. Более того, мы можем считать, что цикл начинается с минимального числа, т.е. i_1 — минимальное число из $i_1, i_2, \dots, i_k$. Пусть $j_1 \in \Omega$ и $j_1 \notin \{i_1, i_2, \dots, i_k\}$. Пусть $j_2 = \sigma(j_1)$, $j_3 = \sigma(j_2)$ и т.д. Мы снова получим цикл $(j_1 j_2 \cdots j_m)$. Так как σ биективно, то множества $\{i_1, i_2, \dots, i_k\}$ и $\{j_1, j_2, \dots, j_m\}$ не пересекаются. Продолжая этот процесс, мы получим разложение $\sigma = \sigma_1\sigma_2\cdots\sigma_l$ в произведение попарно непересекающихся циклов. Количество элементов в цикле мы будем называть *длиной* цикла. При разложении перестановке в произведения циклов, мы будем опускать циклы длины один.

Пример 1.4.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34), \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{pmatrix} = (16)(243).$$

Определение 1.5. Цикл длины два называется *транспозицией*.

Заметим, что если σ — транспозиция, то $\sigma^2 = e$.

Утверждение 1.6. *Любая перестановка $\sigma \in S_n$ является произведением транспозиций.*

Доказательство. Так как любую перестановку можно представить в виде произведения непересекающихся циклов, то достаточно доказать утверждения для одного цикла. Действительно,

$$(i_1 i_2 \cdots i_k) = (i_1 i_2)(i_2 i_3) \cdots (i_{k-1} i_k).$$

□

Теорема 1.7. *Пусть $\sigma \in S_n$ — перестановка. Пусть $\sigma = \tau_1 \tau_2 \cdots \tau_m$ — разложение σ в произведение транспозиций. Тогда число $\epsilon_\sigma = (-1)^m$ не зависит от выбора разложения.*

Доказательство. Пусть существует другое разложение $\sigma = \tau'_1 \tau'_2 \cdots \tau'_l$. Тогда

$$\tau_1 \tau_2 \cdots \tau_m = \tau'_1 \tau'_2 \cdots \tau'_l.$$

Домножим это равенство на τ'_l справа. Получим

$$\tau_1 \tau_2 \cdots \tau_m \tau'_l = \tau'_1 \tau'_2 \cdots \tau'_{l-1}.$$

Продолжая этот процесс, мы получим

$$\tau_1 \tau_2 \cdots \tau_m \tau'_l \tau'_{l-1} \cdots \tau'_1 = e.$$

Таким образом, нам нужно доказать, что любое представление единичной перестановки в произведение транспозиций состоит из четного числа сомножителей. Пусть $e = \tau_1 \tau_2 \cdots \tau_k$. Пусть $x \in \Omega$ и $x \in \tau_p$, где p — максимальное число такое, что $x \in \tau_p$, т.е. $x \notin \tau_{p+1}, \tau_{p+2}, \ldots, \tau_k$. Пусть $\tau_p = (xy)$. Рассмотрим τ_{p-1}. Если τ_{p-1} не содержит ни x, ни y, то $\tau_{p-1}\tau_p = \tau_p \tau_{p-1}$. И мы можем считать p на единицу меньше. Если $\tau_{p-1} = (xy)$, то $\tau_{p-1}\tau_p = e$. И мы также уменьшаем p. Четность при этом остается прежней. Таким образом у нас осталось два случая $\tau_{p-1} = (xz)$ и $\tau_{p-1} = (yz)$. Если $\tau_{p-1} = (xz)$, то

$$\tau_{p-1}\tau_p = (xz)(xy) = (xyz) = (xy)(yz).$$

Если $\tau_{p-1} = (yz)$, то

$$\tau_{p-1}\tau_p = (yz)(xy) = (xzy) = (xz)(zy).$$

Таким образом, во всех случаях мы можем уменьшить p. Следовательно, мы можем считать, что x входит только в $\tau_1 = (xy)$. Однако, в этом случае перестановка $\tau_1 \tau_2 \cdots \tau_k$ отображает x в y, а следовательно $\tau_1 \tau_2 \cdots \tau_k \neq e$. Противоречие. □

Следствие 1.8. *Пусть* $\sigma_1, \sigma_2 \in S_n$. *Тогда*

$$\epsilon_{\sigma_1\sigma_2} = \epsilon_{\sigma_1}\epsilon_{\sigma_2}.$$

Доказательство. Пусть $\sigma_1 = \tau_1\tau_2\cdots\tau_k$, $\sigma_2 = \pi_1\pi_2\cdots\pi_m$ — разложение перестановок в произведение транспозиций. Тогда $\epsilon_{\sigma_1} = (-1)^k$, $\epsilon_{\sigma_2} = (-1)^m$. С другой стороны,

$$\sigma_1\sigma_2 = \tau_1\tau_2\cdots\tau_k\pi_1\pi_2\cdots\pi_m.$$

Следовательно,

$$\epsilon_{\sigma_1\sigma_2} = (-1)^{k+m} = (-1)^k(-1)^m = \epsilon_{\sigma_1}\epsilon_{\sigma_2}.$$

□

Определение 1.9. Перестановка $\sigma \in S_n$ называется *четной*, если $\epsilon_\sigma = 1$, и *нечетной*, если $\epsilon_\sigma = -1$. Множество четных перестановок мы будем обозначать через A_n.

Согласно следствию 1.8 произведение двух четных и двух нечетных перестановок есть четная перестановка, а произведение четной и нечетной перестановки есть нечетная перестановка.

Замечание 1.10. Заметим, что четность/нечетность перестановки мы можем определить по длине циклов в разложении. Поскольку

$$(i_1i_2\cdots i_k) = (i_1i_2)(i_2i_3)\cdots(i_{k-1}i_k),$$

то циклы четной длины нечетны, а циклы нечетной длины четны. Таким образом, четность подстановки совпадает с четностью количества циклов четной длины.

Теорема 1.11. *Пусть* $\sigma \in A_n$ *— четная перестановка. Тогда перестановку* σ *можно представить в виде произведения циклов длины три (не обязательно непересекающихся).*

Доказательство. Разложим σ в произведение непересекающихся циклов

$$\sigma = (i_1i_2\cdots i_k)(j_1j_2\cdots j_l)\cdots .$$

Согласно замечанию 1.10 все циклы четной длины можно разбить на пары. Пусть $(i_1i_2\cdots i_k)(j_1j_2\cdots j_l)$ такая пара, т.е. k и l четные. Поскольку циклы не пересекаются, а, следовательно, их можно переставлять, мы можем предполагать, что $l \geq k$. Тогда

$$(i_1i_2)(i_2i_3)\cdots(i_{k-1}i_k)(j_1j_2)(j_2j_3)\cdots(j_{l-1}j_l) =$$

$$= ((i_1i_2)(j_1j_2))((i_2i_3)(j_2j_3))\cdots((i_{k-1}i_k)(j_{k-1}j_k))(j_kj_{k+1})\cdots(j_{l-1}j_l).$$

Заметим, что $(j_k j_{k+1}) \cdots (j_{l-1} j_l) = (j_k j_{k+1} \cdots j_l)$ — цикл длины $l - k + 1$, т.е. нечетной длины. Таким образом, нам нужно получить все циклы нечетной длины и все перестановки вида $(xy)(zt)$. Все циклы нечетной длины получаются по индукции, а именно

$$(i_1 i_2 \cdots i_k)(i_k i_{k+1} i_{k+2}) = (i_1 i_2 \cdots i_k i_{k+1} i_{k+2}).$$

Аналогично,

$$(xyz)(xyt) = (xz)(yt).$$

В силу произвольности x, y, z, t, теорема доказана. □

2. Группы

Пусть S — произвольное множество. *Бинарной операцией* на множестве S мы будем называть любое отображение

$$S \times S \to S.$$

На S может быть задано, вообще говоря, много различных операций. Желая выделить одну из них, используются скобки: $(S, \circ)$, и говорят, что операция $\circ$ определена на S. Примерами множеств с заданными на них операциями, могут служить: $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$.

Определение 1.12. *Группой* называется множество G с определенной на ней операцией $\circ$ такое, что для $(G, \circ)$ выполнены следующие условия:

(1) (ассоциативность) для любых $a, b, c \in G$ имеет место $(a \circ b) \circ c = a \circ (b \circ c)$;
(2) (существование единицы) существует элемент $e \in G$ такой, что для любого $a \in G$ имеет место $a = e \circ a = a \circ e$ (элемент e называется единицей группы G);
(3) (существование обратного элемента) для любого $a \in G$ существует $a^{-1} \in G$ такой, что $a \circ a^{-1} = a^{-1} \circ a = e$.

Определение 1.13. Группа G называется *абелевой*, если для любых $a, b \in G$ имеет место $a \circ b = b \circ a$ (коммутативность).

Если группа G имеет конечное число элементов, то группа G называется конечной группой, а число элементов группы называется порядком группы G и обозначается $|G|$. Пусть $a \in G$ — элемент группы G. Минимальное целое число k, удовлетворяющее условию $a^k = e$, называется *порядком* элемента a.

Замечание 1.14. Часто, мы будем опускать символ $\circ$ и вместо $a \circ b$ писать ab. Для абелевых групп так же часто мы будем использовать аддитивную запись, т.е. вместо $a \circ b$ будем писать $a + b$.

Пример 1.15.
(1) $(\mathbb{N}, +)$ не является группой, т.к. нет обратного.
(2) $(\mathbb{N}, \cdot)$ не является группой, т.к. нет обратного.
(3) $(\mathbb{Z}, +)$ является бесконечной абелевой группой, единицей является 0, обратное к a, $-a$.
(4) $(\mathbb{Z}, \cdot)$ не является группой, т.к. нет обратного.
(5) $(\mathbb{Q}, +)$ является бесконечной абелевой группой, единицей является 0, обратное к a, $-a$.
(6) $(\mathbb{Q}, \cdot)$ не является группой, т.к. у 0 нет обратного.
(7) $(\mathbb{Q}^*, \cdot)$ (здесь $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$) является бесконечной абелевой группой, единицей является 1, обратное к a, $\frac{1}{a}$.
(8) $(\mathbb{R}, +)$ является бесконечной абелевой группой, единицей является 0, обратное к a, $-a$.
(9) $(\mathbb{R}, \cdot)$ не является группой, т.к. у 0 нет обратного.
(10) $(\mathbb{R}^*, \cdot)$ (здесь $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$) является бесконечной абелевой группой, единицей является 1, обратное к a, $\frac{1}{a}$.
(11) $(\mathbb{C}, +)$ является бесконечной абелевой группой, единицей является 0, обратное к a, $-a$.
(12) $(\mathbb{C}, \cdot)$ не является группой, т.к. у 0 нет обратного.
(13) $(\mathbb{C}^*, \cdot)$ (здесь $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$) является бесконечной абелевой группой, единицей является 1, обратное к a, $\frac{1}{a}$.
(14) $(M_{n\times m}, +)$ (здесь $M_{n\times m}$ — множество матриц размера $n \times m$) является бесконечной абелевой группой, единицей является нулевая матрица, обратное к M, $-M$.
(15) $(\mathrm{GL}_n, \cdot)$ (здесь GL_n — множество невырожденных матриц размера $n \times n$) является бесконечной некоммутативной группой, единицей является матрица E, обратное к A, A^{-1}.
(16) $(S_n, \cdot)$ является конечной некоммутативной группой, единицей является перестановка e, обратное к σ, σ^{-1}.
(17) $(A_n, \cdot)$ является конечной некоммутативной группой, единицей является перестановка e, обратное к σ, σ^{-1}.

Пример 1.16. Пусть $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ — множество остатков при делении на m. Заметим, что остатки можно складывать. Тогда множество $\mathbb{Z}_m$ образует группу относительно операции $+$. Такая группа также называется группой вычетов по модулю m.

Утверждение 1.17. *Пусть G — произвольная группа. Тогда в G существует только одна единица.*

Доказательство. Предположим противное. Пусть существуют две единицы $e, e' \in G$. Тогда $e = ee' = e'$. □

Утверждение 1.18. *Пусть G — произвольная группа и $a \in G$ — произвольный элемент. Тогда в G существует только один обратный к a элемент — a^{-1}.*

Доказательство. Предположим противное. Пусть существуют элемент $b \in G$ обратный к a. Тогда

$$b = be = b(aa^{-1}) = (ba)a^{-1} = ea^{-1} = a^{-1}.$$

□

Определение 1.19. Группа G называется p-группой, если p — простое и $|G| = p^n$.

Определение 1.20. Пусть $(G, \circ)$ — группа. Пусть H — подмножество группы G. Тогда H называется подгруппой группы G, если $e \in H$ и H является группой относительно операции $\circ$.

Определение 1.21. Пусть G — группа, и H — ее подгруппа. Тогда для любого элемента $a \in G$ множество всех элементов ah, где $h \in H$, называется левым смежным классом и обозначается aH, а множество элементов ha — правым смежным классом и обозначается Ha.

Предложение 1.22. *Пусть G — произвольная группа и H — ее подгруппа. Тогда группа G распадается на непересекающиеся левые (правые) смежные классы.*

Доказательство. Нам достаточно доказать, что если смежные классы содержат один и тот же элемент, то они совпадают. Пусть $g_1, g_2 \in G$, $h_1, h_2, h_3 \in H$. Предположим, что $g_1h_1 = g_2h_2$. Тогда $g_1 = g_2h_2h_1^{-1}$. Отсюда, $g_1h_3 = g_2h_2h_1^{-1}h_3$. Заметим, что $h_2h_1^{-1}h_3 \in H$. Следовательно, $g_1h_3 \in g_2H$. □

Число смежных классов группы G по подгруппе H мы будем обозначать $(G : H)$.

Следствие 1.23 (теорема Лагранжа). *Пусть G — конечная группа и $H \subset G$ — ее подгруппа. Пусть $|G| = n$ и $|H| = k$. Тогда $n = k(G : H)$.*

Следствие 1.24. *Пусть G — конечная группа и $a \in G$. Пусть k — порядок элемента a. Тогда k — делитель $|G|$.*

Доказательство. Пусть $H := \{e, a, a^2, \ldots, a^{k-1}\}$. Заметим, что H — подгруппа группы G. Таким образом, наше утверждение следует из теоремы 1.22. □

Определение 1.25. Группа G называется *циклической*, если существует элемент $a \in G$ такой, что для любого элемента $g \in G$ существует $k \in \mathbb{Z}$ такое, что $g = a^k$. Элемент a называется *порождающим* группы G.

Определение 1.26. Два элемента $a, b \in G$ называются *сопряженными*, если существует элемент $g \in G$ такой, что $a = g^{-1}bg$. Множество всех элементов, сопряженных элементу a, называется *классом сопряженности* элемента a. Аналогично, две подгруппы $H_1, H_2 \subset G$ называются *сопряженными*, если существует элемент $g \in G$ такой, что $H_2 = g^{-1}H_1g$.

Утверждение 1.27. *Пусть G — произвольная группа. Тогда группа G распадается на непересекающиеся классы сопряженности.*

Доказательство. Пусть C_1 и C_2 — классы сопряженности элементов a и b соответственно. Предположим, что $g_1^{-1}ag_1 = g_2^{-1}bg_2$. Тогда

$$b = g_2g_1^{-1}ag_1g_2^{-1} = (g_1g_2^{-1})^{-1}a(g_1g_2^{-1}).$$

Следовательно, $b \in C_1$. Отсюда,

$$g_3^{-1}bg_3 = g_3^{-1}g_2g_1^{-1}ag_1g_2^{-1}g_3 = (g_1g_2^{-1}g_3)^{-1}a(g_1g_2^{-1}g_3).$$

□

Следствие 1.28. *Любая группа разбивается на попарно непересекающиеся классы сопряженности.*

Замечание 1.29. Заметим, что для абелевых групп, любой класс сопряженности состоит из одного элемента. Также в любой группе есть класс сопряженности, состоящий из одного элемента e.

Определение 1.30. Пусть G и G' — две группы. Тогда *прямым произведением* этих групп $G \times G'$ называется группа из пар (a, a') с операцией $(a, a') \times (b, b') = (ab, a'b')$. Очевидно, что единицей группы $G \times G'$ является (e, e'), где e, e' — единицы групп G и G' соответственно.

Определение 1.31. Пусть $S \subset G$ — подмножество такое, что любой элемент группы $g \in G$ представляется в виде $g = s_1^{i_1} \ldots s_j^{i_j}$, где $s_1, \ldots, s_j \in S$ и $i_1, \ldots, i_j \in \mathbb{Z}$. Тогда мы будем говорить, что G порождается множеством S. Группа G — *конечнопорожденная*, если существует конечное множество S, порождающая G.

Рассмотрим группу перестановок S_n.

Теорема 1.32. *Пусть перестановка $\sigma \in S_n$ разлагается в произведения циклов длины $i_1, i_2, \ldots, i_k$. Пусть $\sigma' \in S_n$ — сопряженный элемент к σ. Тогда σ' разлагается в произведения циклов длины $i_1, i_2, \ldots, i_k$. Обратно, если $\sigma' \in S_n$ разлагается в произведения циклов длины $i_1, i_2, \ldots, i_k$, то σ' сопряжен к σ.*

Доказательство. Заметим, что $\tau\sigma\tau^{-1}(i) = i$, если $\tau^{-1}(i)$ не входит в разложение σ в произведения циклов. Поскольку

$$\tau((j_{11}j_{12}\cdots j_{1k_1})(j_{21}j_{22}\cdots j_{2k_2})\cdots(j_{l1}j_{l2}\cdots j_{lk_l}))\tau^{-1} =$$

$$(\tau(j_{11}j_{12}\cdots j_{1k_1})\tau^{-1})(\tau(j_{21}j_{22}\cdots j_{2k_2})\tau^{-1})\cdots(\tau(j_{l1}j_{l2}\cdots j_{lk_l})\tau^{-1})$$

и $\tau^{-1}(i)$ входит не более чем в один цикл, то утверждение теоремы достаточно доказать для случая, когда $\sigma = (j_1 j_2 \cdots j_l)$, т.е. σ состоит из одного цикла. Пусть $\sigma' \in S_n$ сопряжен к σ. Тогда $\sigma' = \tau\sigma\tau^{-1}$ и $\sigma = \tau^{-1}\sigma'\tau$. Отсюда, σ' — цикл длины l.

Обратно. Пусть $\sigma = (j_1 j_2 \cdots j_l)$ и $\sigma' = (k_1 k_2 \cdots k_l)$. Рассмотри перестановку τ такую, что $\tau(j_1) = k_1$, $\tau(j_2) = k_2$,..., $\tau(j_l) = k_l$. Тогда $\sigma' = \tau\sigma\tau^{-1}$. □

3. Действия групп на множествах

Пусть G — группа и M — произвольное множество. *Действием* группы G на множестве M называется отображение $G \times M \to M$ такое, что

(1) $em = m$ для любого $m \in M$
(2) $g_1(g_2 m) = (g_1 g_2)m$ для любых $g_1, g_2 \in G$ и $m \in M$.

Определение 1.33. Пусть группа G действует на множестве M. *Стабилизатором* элемента $m \in M$ называется множество $\mathrm{St}(m) = \{g \in G \mid gm = m\}$.

Легко проверить, что $\mathrm{St}(m)$ - является подгруппой группы G.

Определение 1.34. Пусть группа G действует на множестве M. *Орбитой* элемента $m \in M$ называется множество $\mathrm{Orb}(m) = \{gm \mid g \in G\}$.

Утверждение 1.35. *Имеется взаимно однозначное соответствие между элементами орбиты* $\mathrm{Orb}(m)$ *и левыми смежными классами по подгруппе* $\mathrm{St}(m)$.

Доказательство. Пусть $g_1 \operatorname{St}(m) = g_2 \operatorname{St}(m)$. Тогда $g_1 = g_2 a$, где $a \in \operatorname{St}(m)$. Отсюда, $g_1 = g_2 am = g_2 m$. Следовательно, каждому смежному классу соответствует один элемент орбиты $\operatorname{Orb}(m)$. Обратно, пусть $g_1 m = g_2 m$. Тогда $g_2^{-1} g_1 m = m$. Следовательно, $g_2^{-1} g_1 \in \operatorname{St}(m)$. Отсюда, $g_1 = g_2 a$, где $a = g_2^{-1} g_1 \in \operatorname{St}(m)$. □

Следствие 1.36. *Пусть G — конечная подгруппа и G действует на множестве M. Тогда $|G| = |\operatorname{Orb}(m)| \cdot |\operatorname{St}(m)|$ для любого $m \in M$.*

Утверждение 1.37. *Пусть m_1 и m_2 — элементы одной орбиты. Тогда подгруппы $\operatorname{St}(m_1)$ и $\operatorname{St}(m_2)$ сопряжены.*

Доказательство. Пусть $m_1 = gm_2$ и $a \in \operatorname{St}(m_1)$. Тогда $g^{-1} a g \in \operatorname{St}(m_2)$. Отсюда, $g^{-1} \operatorname{St}(m_1) g \subseteq \operatorname{St}(m_2)$. Пусть $b \in \operatorname{St}(m_2)$. Тогда $gbg^{-1} = c \in \operatorname{St}(m_1)$. Отсюда, $g^{-1} \operatorname{St}(m_1) g = \operatorname{St}(m_2)$. □

Теорема 1.38 (Формула Бернсайда). *Пусть G — конечная группа, действующая на конечном множестве M. Пусть M^g — множество элементов m таких, что $gm = m$. Тогда*

$$N = \frac{1}{|G|} \sum_{g \in G} |M^g|,$$

где N — число орбит, $|M^g|$ — число элементов M^g, $|G|$ — порядок группы.

Доказательство. Рассмотрим $\sum\limits_{g \in G} |M^g|$. Заметим, что эта сумма равна количеству пар (g, m) таких, что $gm = m$. Таким образом,

$$\sum_{g \in G} |M^g| = \sum_{m \in M} |\operatorname{St}(m)|.$$

Теперь применим следствие 1.36. Получаем

$$\sum_{g \in G} |M^g| = \sum_{m \in M} |\operatorname{St}(m)| = \sum_{m \in M} \frac{|G|}{|\operatorname{Orb}(m)|} = |G| \sum_{m \in M} \frac{1}{|\operatorname{Orb}(m)|}.$$

Пусть множество M разбивается на орбиты $\operatorname{Orb}_1, \operatorname{Orb}_2, \ldots, \operatorname{Orb}_N$. Рассмотрим сумму $\sum\limits_{m \in M} \frac{1}{|\operatorname{Orb}(m)|}$. Мы можем разбить ее на суммы по каждой орбите, т.е.

$$\sum_{m \in M} \frac{1}{|\operatorname{Orb}(m)|} = \sum_{m \in \operatorname{Orb}_1} \frac{1}{|\operatorname{Orb}_1|} + \sum_{m \in \operatorname{Orb}_2} \frac{1}{|\operatorname{Orb}_2|} + \cdots + \sum_{m \in \operatorname{Orb}_N} \frac{1}{|\operatorname{Orb}_N|}.$$

Заметим, что

$$\sum_{m\in \mathrm{Orb}_i} \frac{1}{|\,\mathrm{Orb}_i\,|} = |\,\mathrm{Orb}_i\,|\frac{1}{|\,\mathrm{Orb}_i\,|} = 1.$$

Таким образом, $\sum\limits_{m\in M} \frac{1}{|\,\mathrm{Orb}(m)|} = N$. Отсюда,

$$\sum_{g\in G} |M^g| = N|G|.$$

□

4. Гомоморфизм групп

Предложение 1.39. *Пусть G — произвольная группа и H — ее подгруппа. Тогда следующие условия эквивалентны:*

(1) $gH = Hg$ *для всех* $g \in G$;
(2) $g^{-1}Hg \subseteq H$ *для всех* $g \in G$;
(3) $g^{-1}Hg = H$ *для всех* $g \in G$.

Доказательство. (1) $\Rightarrow$ (2). Пусть $h \in H$. Поскольку $gH = Hg$, то существует $h' \in H$ такое, что $gh' = hg$. Тогда $g^{-1}hg = h' \in H$.

(2) $\Rightarrow$ (3). Пусть $(g^{-1})^{-1}hg^{-1} = h'$, где $h, h' \in H$. Тогда $h = g^{-1}(g^{-1})^{-1}hg^{-1}g = g^{-1}h'g \in g^{-1}Hg$. Следовательно, $H = g^{-1}Hg$.

(3) $\Rightarrow$ (1). Если $H = g^{-1}Hg$, то, умножая на g, $gH = Hg$. □

Подгруппа, удовлетворяющая условиям предложения 1.39, называется *нормальной подгруппой* группы G, и обозначается $H \triangleleft G$.

Утверждение 1.40. *Пусть $H \triangleleft G$ — нормальная подгруппа группы G. Пусть A — множество смежных классов по подгруппе H. Введем следующую бинарную операцию на множестве A: $aH \circ bH \mapsto abH$. Множество A образует группу относительно бинарной операции $aH \circ bH \mapsto abH$.*

Доказательство. Докажим корректность введенной операции, т.е. то что эта операция не зависит от выбора представителей a и b. Пусть a' и b' — другие представители смежных классов aH и bH. Тогда $a' = ah_1$, $b' = bh_2$. Пусть $h \in H$. Тогда $a'b'h = ah_1bh_2h$. Поскольку $bH = Hb$, то существует $h_1' \in H$ такое, что $h_1b = bh_1'$. Отсюда,

$$a'b'h = ah_1bh_2h = ab(h_1'h_2h) = ab\tilde{h},$$

где $\tilde{h} \in H$. Ассоциативность такой операции очевидна. Единицей служит сама H. Обратный элемент к aH — $a^{-1}H$. □

Группа определенная в утверждении 1.40 называется *факторгруппой* G по H и обозначается G/H.

Определение 1.41. Пусть G — группа. Тогда множество $Z(G) := \{a \in G \mid ag = ga \text{ для всех } g \in G\}$ называется центром группы G.

Из определения непосредственно следует, что $Z(G)$ — нормальная подгруппа.

Пусть G, G' — две группы. Отображение $f\colon G \to G'$, для которого $f(ab) = f(a)f(b)$ для любых $a, b \in G$, называется *гомоморфизмом*. Множество $\ker(f) = \{a \in G \mid f(a) = e\}$ называется *ядром* гомоморфизма f. Гомоморфизм f называется *инъективным*, если $\ker(f) = \{e\}$ (e' — единица группы G') и сюръективным, если для любого $g' \in G'$ существует $g \in G$ такой, что $f(g) = g'$. Сюръективный и инъективны гомоморфизм называется *изоморфизмом*. Две группы G и G' называются изоморфными, если существует изоморфизм $f : G \to G'$ (для краткости будем писать $G \cong G'$).

Утверждение 1.42. *Пусть $f\colon G \to G'$ — гомоморфизм групп. Тогда $f(e) = e'$, где e и e' — единицы групп G и G', и $f(a)^{-1} = f(a^{-1})$.*

Доказательство. Пусть $a \in G$ — элемент группы G. Тогда $f(a) = f(ae) = f(a)f(e)$. Отсюда, $f(e) = e'$. Заметим, что $f(a)f(a)^{-1} = e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$. Отсюда $f(a)^{-1} = f(a^{-1})$. □

Предложение 1.43. *Пусть $f\colon G \to G'$ — гомоморфизм групп. Тогда $\ker(f)$ — нормальная подгруппа в группе G.*

Доказательство. Докажем сначала, что $\ker(f)$ — группа. Пусть $a, b \in \ker(f)$. Тогда $f(ab) = f(a)f(b) = e' \cdot e' = e'$, т.е. $ab \in \ker(f)$. Согласно утверждению 1.42 $f(e) = e'$, где e и e' — единицы групп G и G'. Пусть $a \in \ker(f)$. Тогда, согласно утверждению 1.42 $f(a^{-1}) = f(a)^{-1} = e'$. Следовательно, $\ker(f)$ — группа. Пусть $g \in G$. Тогда $f(g^{-1}ag) = f(g^{-1})e'f(g) = e'$. Следовательно, $\ker(f)$ — нормальная подгруппа. □

Теорема 1.44 (1-я теорема о гомоморфизме). *Пусть $f\colon G \to G'$ — сюръективный гомоморфизм групп. Тогда существует естественный изоморфизм $G/\ker(f) \cong G'$. Обратно, если $H \lhd G$, то*

существует естественное отображение $\varphi\colon G \to G/H$ *такое, что* φ *— сюръекция и* $\ker(\varphi) = H$.

Доказательство. Пусть $\bar{f}\colon G/\ker(f) \to G'$ — отображение, определяемое следующим образом: $\bar{f}(g\ker(f)) = f(g)$. Докажем корректность определения $\bar{f}$. Пусть $g_1\ker(f) = g_2\ker(f)$. Тогда $g_2 = g_1\alpha$, где $\alpha \in \ker(f)$. Следовательно, $f(g_2) = f(g_1\alpha) = f(g_1)f(\alpha) = f(g_1)e' = f(g_1)$. Пусть $g_1, g_2 \in G$. Тогда

$$\bar{f}(g_1\ker(f)\cdot g_2\ker(f)) = \bar{f}(g_1g_2\ker(f)) = f(g_1g_2) = \\ = f(g_1)f(g_2) = \bar{f}(g_1\ker(f))\bar{f}(g_2\ker(f)).$$

Таким образом, $\bar{f}$ — гомоморфизм групп. Докажем, что $\bar{f}$ — инъекция. Пусть $e' = \bar{f}(g\ker(f)) = f(g)$. Тогда $g \in \ker(f)$ и $g\ker(f) = \ker(f)$. Докажем, что $\bar{f}$ — сюръекция. Пусть $a \in G'$. Тогда существует $b \in G$ такое, что $f(b) = a$. Отсюда, $\bar{f}(b\ker(f)) = a$. Таким образом, первая часть теоремы доказана.

Докажем второе утверждение. Положим $\varphi(a) = aH$. Очевидно, φ — сюръективный гомоморфизм групп. Пусть $g \in \ker(\varphi)$. Тогда $\varphi(g) = gH = H$. Следовательно, $g \in H$. Таким образом, теорема доказана. □

Теорема 1.45 (2-я теорема о гомоморфизме). *Пусть* H *и* K *подгруппы группы* G*, причем* K *— нормальная подгруппа. Тогда* $HK = KH$ *— подгруппа группы* G *и* $HK/K \cong H/(H \cap K)$.

Доказательство. Докажем, что $HK = KH$. Пусть $hk_1 \in HK$. Тогда, поскольку K — нормальная подгруппа, существует $k_2 \in K$ такое, что $hk_1 = k_2h \in KH$. Аналогично, $h_1k_1h_2k_2 = h_1h_2k_1'k_2$, где $h_1, h_2 \in H$, $k_1, k_1'k_2 \in K$. Следовательно, $HK = KH$ — подгруппа группы G. Очевидно, что $K \lhd HK$ и $H \cap K \lhd H$.

Пусть $f\colon H \to HK/K$ — гомоморфизм групп, определяемый следующим образом: $f(h) = hK$. Очевидно, что f — сюръекция. Тогда, по теореме 1.44, $HK/K \cong H/\ker(f)$. Очевидно, $H \cap K \subset \ker(f)$. Пусть $a \in \ker(f)$. Тогда $a \in K$. Следовательно, $a \in H \cap K$. Таким образом, $H \cap K = \ker(f)$ и теорема доказана. □

Теорема 1.46 (3-я теорема о гомоморфизме). *Пусть* H *и* K *— нормальные подгруппы группы* G*, причем* $K \subset H$. *Тогда*

$$G/H \cong (G/K)/(H/K).$$

Доказательство. Рассмотрим гомоморфизм $f\colon G/K \to G/H$, определяемый следующим образом: $f(gK) = gH$. Очевидно, что $\ker(f)$ состоит из всех gK таких, что $g \in H$. Следовательно, $\ker(f) \cong H/K$. Таким образом, наше утверждение следует из теоремы 1.44. □

Теорема 1.47 (теорема Кели). *Пусть G — конечная группа порядка n. Тогда существует вложение (т.е. инъективный гомоморфизм) группы G в группу S_n.*

Доказательство. Пронумеруем элементы группы G и рассмотрим действие группы G на самой себе умножением слева, т.е. $a(g) = ag$. Таким образом, мы получили гомоморфизм G в группу перестановок S_n. Заметим, что он инъективен. Действительно, если a оставляет все элементы на месте, то a — единица. □

Теорема 1.48 (лемма о бабочке). *Пусть A и B — подгруппы группы G, и пусть H и K — нормальные подгруппы в A, и в B соответственно. Тогда $H(A\cap K)$ нормальна в $H(A\cap B)$, и $(H\cap B)K$ нормальна в $(A \cap B)K$. Более того,*

$$H(A \cap B)/H(A \cap K) \cong (A \cap B)K/(H \cap B)K.$$

5. Прямое произведение групп

Рассмотрим более подробно прямое произведение групп.

Теорема 1.49. *Пусть G — группа и H, K — ее нормальные подгруппы. Предположим, что $H \cap K = \{e\}$ и $HK = G$. Тогда $G \cong H \times K$.*

Доказательство. Пусть $g \in G$. Поскольку $HK = G$, то существуют элементы $a \in H$, $b \in K$, что $g = ab$. Предположим, что существуют другие элементы $a' \in H$, $b' \in K$, что $g = a'b'$. Из $ab = a'b'$ следует $a'^{-1}a = b'b^{-1}$. Поскольку $a'^{-1}a \in H$, $b'b^{-1} \in K$, то $a'^{-1}a = b'b^{-1} \in H \cap K$. Отсюда, $a'^{-1}a = b'b^{-1} = e$ и $a = a'$, $b = b'$. Докажем, что $ab = ba$. Действительно, рассмотрим $aba^{-1}b^{-1}$. Поскольку $aba^{-1} \in K$, то $aba^{-1}b^{-1} \in K$. С другой стороны, поскольку $ba^{-1}b^{-1} \in H$, то $aba^{-1}b^{-1} \in H$. Следовательно, $aba^{-1}b^{-1} = e$. Отсюда $ab = ba$. Теперь мы можем определить гомоморфизм $f\colon G \to H \times K$, как $f(g) = (a, b)$. В силу единственности представления $g = ab$ это отображение корректно определено. Заметим, что если $g' = a'b'$, то

$$f(gg') = f(aba'b') = f(aa'bb') = (aa', bb') = (a, b)(a', b') = f(g)f(g').$$

Следовательно, f — гомоморфизм. Очевидно, что он инъективен и сюръективен. $\square$

Следствие 1.50. *Пусть G — группа и $H_1, H_2, \dots H_n$ — ее нормальные подгруппы. Предположим, что $G = H_1 H_2 \cdots H_n$ и $H_i \cap (H_1 H_2 \cdots H_{i-1} H_{i+1} \cdots H_n = \{e\}$. Тогда*

$$G \cong H_1 \times H_1 \times \cdots \times H_n.$$

Теорема 1.51. *Пусть $G = G_1 \times G_2$ и H_1, H_2 — нормальные подгруппы в G_1 и G_2 соответственно. Тогда $H_1 \times H_2 \lhd G_1 \times G_2$ и $G/H_1 \times H_2 \cong (G_1/H_1) \times (G_2/H_2)$.*

Доказательство. Пусть $\alpha\colon G_1 \to G_1/H_1$ и $\beta\colon G_2 \to G_2/H_2$ — естественные гомоморфизмы. Определим гомоморфизм $f\colon G \to (G_1/H_1) \times (G_2/H_2)$ как $f(ab) = (\alpha(a), \beta(b))$. Очевидно, что f — гомоморфизм с ядром $\ker f = H_1 \times H_2$ и образом $(G_1/H_1) \times (G_2/H_2)$. $\square$

Следствие 1.52. *Пусть $G = G_1 \times G_2 \times \cdots \times G_n$ и $H_1, H_2, \dots, H_n$ — нормальные подгруппы в $G_1, G_2, \dots, G_n$. Тогда $(H_1 \times H_2 \times \cdots \times H_n) \lhd G$ и*

$$G/(H_1 \times H_2 \times \cdots \times H_n) \cong (G_1/H_1) \times (G_2/H_2) \times \cdots \times (G_n/H_n).$$

Утверждение 1.53. *Пусть элементы $a \in G_1$, $b \in G_2$ имеют порядки n и m соответственно. Тогда порядок $(a, b) \in G_1 \times G_2$ равен наименьшему общему кратному n и m.*

Доказательство. Пусть $(a, b)^k = (a^k, b^k) = (e, e')$. Тогда k делится на n и m. $\square$

Утверждение 1.54. *Пусть порядки групп G_1 и G_2 равны n и m соответственно. Тогда порядок группы $G_1 \times G_2$ равен nm.*

Определение 1.55. Группа G называется *циклической*, если существует элемент $a \in G$ такой, что для любого элемента $g \in G$ существует $k \in \mathbb{Z}$ такое, что $g = a^k$. Элемент a называется *порождающим* группы G.

Из определения циклических групп следует, что все циклические подгруппы, порядка n, изоморфны $\mathbb{Z}_n$.

Теорема 1.56. *Пусть $\mathbb{Z}_n$ и $\mathbb{Z}_m$ — циклические группы. Тогда группа $\mathbb{Z}_n \times \mathbb{Z}_m$ циклическая тогда и только тогда, когда n и m взаимно просты.*

Доказательство. Пусть n и m взаимно просты, g_1 и g_2 — порождающие групп $\mathbb{Z}_n$ и $\mathbb{Z}_m$ соответственно. Согласно утверждению 1.53 порядок $(g_1, g_2) \in \mathbb{Z}_n \times \mathbb{Z}_m$ равен nm, и по утверждению 1.54 равен порядку группы. Таким образом, (g_1, g_2) порождает $\mathbb{Z}_n \times \mathbb{Z}_m$. Пусть $\mathbb{Z}_n \times \mathbb{Z}_m$ — циклическая группа и $(g_1, g_2) \in \mathbb{Z}_n \times \mathbb{Z}_m$ порождает эту группу. Тогда порядок (g_1, g_2) равен nm. С другой стороны, согласно утверждению 1.53, порядок (g_1, g_2) равен наименьшему общему кратному порядков g_1 и g_2, которые, в свою очередь, являются делителями n и m. Отсюда, порядок (g_1, g_2) является делителем наименьшего общего кратного n и m. Таким образом, n и m взаимно просты. □

6. Конечные абелевы группы

В этом параграфе мы рассмотрим абелевы группы. Мы будем, вместо мультипликативной записи ab, будем использовать аддитивную $a + b$, вместо a^n будем писать na, вместо e будем писать 0. Заметим, что в абелевой группе любая подгруппа нормальная. Так же прямое произведение двух абелевых групп обычно называется прямой суммой и обозначают $A \oplus B$.

Лемма 1.57. *Пусть G — абелева группа и любой элемент $a \in G$ имеет порядок p^k, для какого-то k. Тогда $|G| = p^n$.*

Доказательство. Предположим, что $|G| = p^n m$, где $(p, m) = 1$. Пусть $f\colon G \to G_1 = G/\langle a\rangle$, где $\langle a\rangle$ — циклическая группа порожденная элементом a. Поскольку порядок элемента a равен p^k, то $|G_1| = p^{n_1} m$, где $n_1 < n$. Предположим, что существует элемент $b \in G_1$ такой, что порядок b равен $p^s t$, где $(p, t) = 1$. Пусть b' прообраз b. По предположению порядок b' равен p^r. Отсюда, $0 = f(0) = f(p^r b') = p^r b$. Противоречие. Следовательно, любой элемент группы G_1 имеет порядок p^r для какого-то r. Снова $G_2 = G_1/\langle b\rangle$. Тогда $|G_2| = p^{n_3} m$. Продолжая этот процесс, мы получим $|G_i| = m$. Согласно следствию 1.24 порядок любого элемента группы G_i является делителем m. Отсюда, $m = 1$. □

Теорема 1.58. *Пусть G — абелева группа и $|G| = m = p_1^{s_1} \cdot p_2^{s_2} \dots p_n^{s_n}$. Тогда $G \cong A_{p_1} \oplus \dots \oplus A_{p_n}$, где A_{p_i} — абелева группа и $|A_{p_i}| = p_i^{s_i}$.*

Доказательство. Пусть A_{p_i} — множество элементов, порядок которых равен p_i^k, где $k = 0, 1, 2, \dots$ (возможно $A_{p_i} = \{0\}$). Заметим, что A_{p_i} — подгруппа группы G. Действительно, если $p_i^{l_1} a = 0$ и $p_i^{l_2} b = 0$, то $p_i^h (a + b) = 0$, где $h = \max\{l_1, l_2\}$. При

этом $A_{p_i} \cap A_{p_j} = \{0\}$. Пусть $g \in G$ и пусть порядок элемента g равен $q = p_1^{r_1} \cdot p_2^{r_2} \dots p_n^{r_n}$. Пусть $t_i = p_1^{r_1} \dots p_{i-1}^{r_{i-1}} \cdot p_{i+1}^{r_{i+1}} \dots p_n^{r_n}$. Тогда $t_i g \in A_{p_i}$. Поскольку $(t_1, \dots, t_n) = 1$, то существуют a_i такие, что $a_1 t_1 + \dots + a_n t_n = 1$. Тогда $a_1 t_1 g + \dots + a_n t_n g = g$. Докажем, что такое разложение единственно. Пусть существует два разложения $b_1 + \dots + b_n = g$ и $b'_1 + \dots + b'_n = g$, где $b_i, b'_i \in A_i$. Тогда $(b_1 - b'_1) + \dots + (b_n - b'_n) = 0$. Предположим, что $b_i - b'_i \neq \{0\}$. Пусть $t = p_1^{s_1} \dots p_{i-1}^{s_{i-1}} \cdot p_{i+1}^{s_{i+1}} \dots p_n^{s_n}$. Тогда $t((b_1 - b'_1) + \dots + (b_n - b'_n)) = t(b_i - b'_i) = 0$. Отсюда, $b_i = b'_i$. Теперь утверждение теоремы следует из леммы 1.57. □

Теорема 1.59. *Пусть G — абелева p-группа. Тогда $G \cong \mathbb{Z}_{p^{s_1}} \oplus \dots \oplus \mathbb{Z}_{p^{s_n}}$.*

Доказательство. Пусть g — элемент максимального порядка p^{s_1} и пусть A — максимальная подгруппа группы G такая, что $A \cap \langle g \rangle = \{0\}$, где $\langle g \rangle$ — циклическая группа порожденная g. Пусть H — подгруппа, порожденная множеством $A \cup g$. Докажем, что $H = G$. Предположим, что существует элемент $b \in G$ такой, что $b \notin H$. Можно считать, что $pb \in H$ (если $p^i b \in H$ и $p^{i-1} b \notin H$, то можно заменить b на $p^{i-1} b$). Тогда $pb = a + lg$, где $a \in A$ $l \in \mathbb{N} \cup \{0\}$. Умножим это равенство на $p^{s_1 - 1}$. В силу максимальности порядка p^{s_1}, мы получаем $p^{s_1-1} a + l p^{s_1-1} g = 0$. Поскольку $A \cap \langle g \rangle = \{0\}$, то $p^{s_1-1} a = 0$ и $l p^{s_1-1} g = 0$. Следовательно, $l = jp$. Отсюда, $p(b - jg) = a \in A$. Пусть $c = b - jg$ и пусть C — подгруппа, порожденная $A \cup c$. В силу максимальности A существуют $s, k \in \mathbb{N}$ и $a' \in A$ такие, что $a' + sc = kg$. Тогда $sc \in H$ и s не делится на p. Отсюда, $c \in H$. Следовательно, $b \in H$. Противоречие. Таким образом $G = H = A \oplus \mathbb{Z}_{p^{s_1}}$. Повторяя тоже самое рассуждение для A, мы получаем утверждение теоремы. □

Теорема 1.60. *Пусть G — абелева группа. Тогда G разлагается в прямую сумму циклических p-групп. Причем это разложение единственно с точностью до перестановки слагаемых.*

Доказательство. Из теорем 1.58 и 1.59 следует, что достаточно доказать единственность разложения для p-групп. □

7. Свободные группы

Рассмотрим сначала абелевы группы.

Определение 1.61. Пусть A — абелева группа. Мы говорим, что группа A без кручений, если в ней не существует элементов конечного порядка, т.е. таких $a \in A$, что $na = 0$ для некоторого n.

Определение 1.62. Система элементов $a_1, a_2, \ldots, a_k \in A$ называется *независимой*, если из равенства $n_1a_1 + n_2a_2 + \cdots + n_ka_k = 0$, где $n_i \in \mathbb{Z}$ следует, что $n_1 = n_2 = \cdots = n_k = 0$. Пусть A — абелева группа без кручений. Система элементов $a_1, a_2, \ldots, a_k \in A$ называется *базисом* группы A, если $a_1, a_2, \ldots, a_k$ независимы и порождают A (т.е. любой элемент $a \in A$ представляется в виде $a = n_1a_1 + n_2a_2 + \cdots + n_ka_k$).

Лемма 1.63. *Пусть A — абелева группа и $a_1, a_2, \ldots, a_k$ — базис A. Пусть $b_1, b_2, \ldots, b_n \in A$ независимы. Тогда $n \geq k$.*

Доказательство. Пусть

$$b_i = \alpha_{i1}a_1 + \alpha_{i2}a_2 + \cdots + \alpha_{ik}a_k,$$

где $\alpha_{ij} \in \mathbb{Z}$. Рассмотрим целочисленные вектора $B_i = (\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{ik})$. Предположим, что $n > k$. Тогда вектора $B_1, B_2, \ldots, B_n$ линейно зависимы. Следовательно, существуют $r_1, r_2, \ldots, r_n \in \mathbb{Q}$, что

$$r_1B_2 + r_2B_2 + \cdots + r_nB_n = 0.$$

Умножим это равенство на общий знаменатель $r_1, r_2, \ldots, r_n$, получим

$$s_1B_2 + s_2B_2 + \cdots + s_nB_n = 0,$$

где $s_i \in \mathbb{Z}$. Отсюда,

$$s_1\alpha_{1j} + s_2\alpha_{2j} + \cdots + s_n\alpha_{nj} = 0, \quad \forall j.$$

Тогда

$$\sum_{i=1}^{n} s_ib_i = \sum_{i=1}^{n} s_i \left(\sum_{j=1}^{k} \alpha_{ij}a_j \right) = \sum_{j=1}^{k} \left(\sum_{i=1}^{n} s_i\alpha_{ij} \right) a_j = 0.$$

Противоречие. □

Замечание 1.64. Если $a_1, a_2, \ldots, a_k \in A$ — базис группы A и $b_1, b_2, \ldots, b_k \in A$ независимы, то далеко не всегда $b_1, b_2, \ldots, b_k$ — базис.

Теорема 1.65. *Всякая конечно порожденная абелева группа A без кручений обладает базисом. Все базисы группы A равномощны (содержат одинаковое количество элементов).*

Доказательство. Пусть $a_1, a_2, \ldots, a_n \in A$ порождают группу A. Если $a_1, a_2, \ldots, a_n$ независимы, то это базис. Следовательно, мы можем считать, что существуют $s_1, s_2, \ldots, s_n \in \mathbb{Z}$, что $s_1a_1 + s_2a_2 + \cdots + s_na_n = 0$. Такие выражения мы будем называть

соотношениями. Число, равное $\min|s_i|$, будем называть высотой соотношения (здесь минимум берется по всем s_i не равным нулю). Соотношение, у которого высота минимальна, будем называть минимальным соотношением. Заметим, что минимальное соотношение не всегда единственно.

Если $s_1a_1 + s_2a_2 + \cdots + s_na_n = 0$ — минимальное соотношение, то наименьший общий делитель $s_1, s_2, \ldots, s_n$ равен единице. Действительно, если $s_i = ds'_i$ для всех i, то

$$s_1a_1 + s_2a_2 + \cdots + s_na_n = d(s'_1a_1 + s'_2a_2 + \cdots + s'_na_n) = 0.$$

Поскольку в A нет кручений, то $s'_1a_1 + s'_2a_2 + \cdots + s'_na_n = 0$. Противоречие.

Рассмотрим минимальное соотношение $s_1a_1+s_2a_2+\cdots+s_na_n = 0$. Пусть его высота h. Умножая на -1 и перенумеровывая образующие, мы можем считать, что $s_1 = h$. Мы знаем, что не все s_i делятся на h. Пусть s_2 не делится на h. Тогда $s_2 = qh + r$. Отсюда,

$$ha'_1 + ra'_2 + s_3a'_3 + s_4a'_4 + \cdots + s_na'_n = 0,$$

где $a'_1 = a_1 + qa_2$, $a'_i = a_i$ при $2 \leq i \leq n$. Заметим, что $a'_1, a'_2, \ldots, a'_n$ — образующие A. При этом высота минимального соотношения уменьшилась. Продолжая этот процесс, мы можем считать, что высота минимального соотношения равна 1.

Пусть $s_1a_1 + s_2a_2 + \cdots + s_na_n = 0$ — соотношение высоты 1 и $|s_k| = 1$. Тогда мы можем выразить

$$a_k = s'_1a_1 + s'_2a_2 + \cdots + s'_{k-1}a_{k-1} + s'_{k+1}a_{k+1} + \cdots + s'_na_n,$$

где $s'_i = \pm s_i$. Таким образом, элементы $\{a_1, a_2, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n\}$ будут системой образующих. Продолжая этот процесс, мы получим базис.

Теперь докажем второе утверждение. Пусть $a_1, a_2, \ldots, a_n$ и $b_1, b_2, \ldots, b_m$ — два базиса. Дважды применяя лемму 1.63, получаем $n \leq m$, $m \leq n$. □

Определение 1.66. Конечно порожденная абелева группа A без кручений называется *свободной абелевой группой*. Количество элементов в базисе называется *рангом* этой группы. Обозначается F_n^{ab}.

Замечание 1.67. Согласно теореме 1.65, свободная группа ранга n представляет собой сумму из n копий групп $\mathbb{Z}$, т.е.

$$F_n^{ab} = \underbrace{\mathbb{Z} + \mathbb{Z} + \cdots + \mathbb{Z}}_{n \text{ слагаемых}}.$$

Утверждение 1.68. *Пусть A — свободная абелева группа ранга n и B — ее подгруппа. Тогда B — свободная абелева группа ранга m, $m \leq n$.*

Доказательство. Следует из теоремы 1.65. □

Теорема 1.69. *Пусть A — конечно порожденная абелева группа. Тогда $A \cong F_n^{ab} \oplus B$, где F_n^{ab} — свободная абелева группа ранга n, B — конечная абелева группа.*

Доказательство. Пусть $B \subset A$ — множество элементов конечного порядка. Заметим, что B — конечная подгруппа. Рассмотрим факторгруппу $\bar{A} = A/B$. Пусть $f\colon A \to \bar{A}$ — естественный гомоморфизм. Заметим, что в $\bar{A}$ нет кручений. Действительно, пусть $\bar{a} \in \bar{A}$ и $k\bar{a} = 0$. Пусть a — любой прообраз $\bar{a}$ в A. Тогда $ka \in B$. Следовательно, существует m, что $mka = 0$. Противоречие. Таким образом, $\bar{A}$ свободная группа. Пусть $\bar{a}_1, \bar{a}_1, \ldots, \bar{a}_n$ — базис $\bar{A}$, и $a_1, a_1, \ldots, a_n$ — прообразы $\bar{a}_1, \bar{a}_1, \ldots, \bar{a}_n$ в A. Заметим, что $a_1, a_1, \ldots, a_n$ независимы. Пусть M — свободная абелева группа порожденная $a_1, a_1, \ldots, a_n$. Докажем, что $B \oplus M = A$. Пусть $g \in A$. Если g имеет конечный порядок, то $g \in B$. Пусть $g \notin B$, $\bar{g} = f(g)$. Тогда $\bar{g} = s_1\bar{a}_1 + s_2\bar{a}_1 + \cdots + s_n\bar{a}_n$. Рассмотрим $b = g - (s_1a_1 + s_2a_1 + \cdots + s_na_n)$. Заметим, что $f(b) = 0$. Тогда $b \in B$, и

$$g = b + s_1a_1 + s_2a_1 + \cdots + s_na_n \in B \oplus M.$$

Таким образом, $B \oplus M = A$. □

Теперь перейдем к рассмотрению не коммутативного случая.

Пусть X — некоторое множество символов x_i, будем называть его *алфавитом*. Пусть X^{-1} — множество символов, состоящее из x_i^{-1}. *Словом* в алфавите X будем называть пустую (обозначается 1) или конечную последовательность символов из $X \cup X^{-1}$. *Редукцией* слова u мы будем называть вычеркивание подслов вида $x_ix_i^{-1}$ или $x_i^{-1}x_i$. Слово u называется *несократимым*, если в нем нет последовательностей вида $x_ix_i^{-1}$ или $x_i^{-1}x_i$. Ясно, что применяя редукцию, мы можем от любого слова перейти к несократимому. Два слова u и v будем называть эквивалентными, если, применяя редукцию к обоим словам, мы получаем одно и тоже несократимое слово. Обозначим класс слов эквивалентных u через $[u]$.

Теорема 1.70. *В каждом классе слов $[u]$ существует только одно несократимое слово.*

Доказательство. Будем доказывать индукцией по длине слова. Слова длины ноль и один являются несократимыми. Предположим, что единственность несократимого слова доказана для всех слов, длины меньшей n. Предположим, что слово v, длины n, редуцируется к двум несократимым словам v' и v''. Если первая редукция применялась к одному подслову $x_i x_i^{-1}$ или $x_i^{-1} x_i$, то мы можем воспользоваться индуктивным предположением. Рассмотрим случай, когда первые редукции не пересекаются т.е.

$$v = a x_i x_i^{-1} b x_j^{-1} x_j c,$$

где a, b, c — подслова (заметим, что возможны варианты — вместо $x_i x_i^{-1}$ может стоять $x_i^{-1} x_i$, вместо $x_j^{-1} x_j$ может стоять $x_j x_j^{-1}$, доказательство не меняется). После первой редукции, мы получаем слова $v_1 = a b x_j^{-1} x_j c$ и $v_2 = a x_i x_i^{-1} b c$. Оба эти слова редуцируются к слову abc. Следовательно, по индуктивному предположению, редуцируются к единственному несократимому слову. Рассмотрим случай, когда первые редукции пересекаются, т.е.

$$v = a x_i x_i^{-1} x_i b,$$

где a, b — подслова. Тогда обе редукции приводят в слову $v_1 = a x_i b$, которое, по индуктивному предположению, редуцируются к единственному несократимому слову. □

Теорема 1.71. *Пусть $X = \{x_i\}$ — некоторое множество символов, $F(X)$ — множество классов эквивалентных слов. На $F(X)$ введем операцию умножения $[u][v] = [uv]$. Эта операция не зависит от выбора представителей в классах, и $F(X)$ является группой относительно этой операции.*

Доказательство. Корректность этой операции и ее ассоциативность следуют из теоремы 1.70. Единицей служит пустое слово, т.е. 1. Обратный элемент строится по следующему правилу. Пусть дано слово

$$v = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n},$$

где $x_1, x_2, \ldots, x_n \in X$, $\epsilon_i = \pm 1$. Тогда

$$v^{-1} = x_n^{-\epsilon_n} x_{n-1}^{-\epsilon_{n-1}} \cdots x_2^{-\epsilon_2} x_1^{-\epsilon_1}.$$

□

Определение 1.72. Группа $F(X)$ называется *свободной группой*. Если X — конечное множество, то $F(X)$ конечно порожденная свободная группа. Количество элементов в X называется *степенью свободы* группы $F(X)$.

Замечание 1.73. Не нужно путать свободную группу и свободную абелеву группу. Свободная абелева группа не является свободной группой и наоборот (исключением является случай, когда X состоит их одного элемента, а свободная абелева группа имеет ранг 1).

Теорема 1.74. *Пусть G — группа, порожденная элементами $g_1, g_2, \ldots, g_n$. Рассмотрим алфавит X, состоящий из $x_1, x_2, \ldots, x_n$. Тогда отображение $f\colon X \to M$ по правилу $f(x_i) = g_i$ единственным образом продолжается до гомоморфизма групп $\bar{f}\colon F(X) \to G$.*

Доказательство. Определим $\bar{f}\colon F(X) \to G$ по правилу

$$\bar{f}(x_{i_1}^{\epsilon_{i_1}} x_{i_2}^{\epsilon_{i_2}} \cdots x_{i_m}^{\epsilon_{i_m}}) = g_{i_1}^{\epsilon_{i_1}} g_{i_2}^{\epsilon_{i_2}} \cdots g_{i_m}^{\epsilon_{i_m}}.$$

□

Определение 1.75. Элементы ядра гомоморфизма $\bar{f}\colon F(X) \to G$ называются *соотношениями* группы G в алфавите X. Если множество соотношений H' такого, что минимальная нормальная подгруппа в $F(X)$, содержащая H', совпадает с H, то H' называется *определяющим множеством соотношений.*

Пример 1.76. Пусть алфавит X состоит из $x_1, x_2, \ldots, x_n$. Тогда соотношения

$$H' = \{x_i x_j x_i^{-1} x_j^{-1} \mid 1 \leq i < j \leq n\}$$

определяют свободную абелеву группу.

Глава 2

Кольца, модули, поля и алгебры

В этой главе мы рассмотрим еще несколько важных алгебраических структур.

1. Определение и основные свойства колец

Пусть на множестве A заданы две бинарные операции — умножение и сложение $(+, \cdot)$ — такие, что

(1) $(A, +)$ — является абелевой группой.
(2) Умножение ассоциативно и имеется единичный элемент.
(3) Для всех $x, y, z \in A$

$$(x + y)z = xz + yz \text{ и } z(x + y) = zx + zy.$$

(Эти соотношения называются *дистрибутивностью*).

Тогда A называется *кольцом*.

Если для любых двух элементов $a, b \in A$ выполнено $ab = ba$, то кольцо A называется *коммутативным*. Если для любого ненулевого элемента $a \in A$ существует a^{-1} такое что $aa^{-1} = a^{-1}a = 1$, то кольцо A называется *телом*. Тело, в котором выполнено $ab = ba$ для любых двух элементов $a, b \in A$, называется *полем*.

Утверждение 2.1. *Пусть A — кольцо. Тогда $a \cdot 0 = 0 \cdot a = 0$ для любого $a \in A$.*

Доказательство. Заметим, что

$$a = a \cdot 1 = a(1 + 0) = a \cdot 1 + a \cdot 0 = a + a \cdot 0.$$

Прибавим к обеим частям равенства $-a$, получим $0 = a \cdot 0$. Аналогично, $0 \cdot a = 0$. □

Утверждение 2.2. *Пусть A — кольцо. Тогда, для любых $a, b \in A$, выполнено $(-a)b = a(-b) = -(ab)$, $(-a)(-b) = ab$.*

Доказательство. Поскольку, согласно 2.1, $0b = 0$, то

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

Отсюда, $(-a)b = -(ab)$. Аналогично, $a(-b) = -(ab)$. Теперь

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$$

□

Определение 2.3. Пусть A и B — два кольца. *Гомоморфизмом* колец называется отображение $f\colon A \to B$ такое что $f(a+b) = f(a) + f(b)$ и $f(ab) = f(a)f(b)$ для любых $a, b \in A$. *Ядром* гомоморфизма f называется множество элементов $a \in A$, отображающихся в 0, т.е.

$$\ker f = \{a \mid f(a) = 0\}.$$

Пусть $f(a) \neq 0$. Не трудно убедиться, что $f(0) = 0$, $f(1) = 1$. Действительно,

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

Отсюда, $f(0) = 0$. Аналогично, $f(a) = f(a1) = f(a)f(1)$. Если $f(a) \neq 0$, то $f(1) = 1$. Аналогично $f(-a) = -f(a)$.

Пример 2.4.
(1) $\mathbb{Z}$ является коммутативным кольцом (не является полем, поскольку обратимы только 1 и -1).
(2) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ являются полями.
(3) $M_{n\times m}$ (здесь $M_{n\times m}$ — множество матриц размера $n \times m$) является некоммутативным кольцом (единицей является единичная матрица E). Заметим, что $M_{n\times m}$ не является телом, поскольку матрицы, с определителем равным нулю, необратимы.

Рассмотрим еще один важный пример.

Пример 2.5. Пусть $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ — множество остатков при делении на m. Тогда $\mathbb{Z}_m$ — коммутативное кольцо.

Утверждение 2.6. *Кольцо $\mathbb{Z}_m$ является полем тогда и только тогда, когда m — простое число.*

Доказательство. Пусть m не является простым числом, т.е. $m = m_1 m_2$. Тогда $m_1 m_2 = 0$ в кольце $\mathbb{Z}_m$. Предположим, что m_2 обратим, т.е. существует m_2^{-1} такой что $m_2^{-1} m_2 = 1$. С другой стороны,

$$m_1 = m_1 1 = m_1 m_2 m_2^{-1} = 0 m_2^{-1} = 0.$$

Противоречие.

Пусть m — простое число. Рассмотрим остаток $k \in \mathbb{Z}_m$. Поскольку $(k, m) = 1$, то существуют целые числа a, b такие что $ak + bm = 1$. Пусть $\bar{a}$ — остаток от деление a на m. Поскольку bm делится на m,

то $\bar{a}k = 1$ в $\mathbb{Z}_m$. Следовательно, любой элемент в $\mathbb{Z}_m$ обратим. Тогда $\mathbb{Z}_m$ — поле. □

Замечание 2.7. Заметим, что мы фактически доказали, что если в кольце существуют два элемента a, b такие, что $ab = 0$, то кольцо не является полем. Коммутативные кольца, в которых не существует таких элементов, называются *кольцом без делителей нуля* или *целостным кольцом*.

Определение 2.8. Множество $\mathfrak{a} \subset A$ называется *левым идеалом* (*правым идеалом*) кольца A, если $\mathfrak{a}$ является подгруппой относительно операции сложения и $ax \in \mathfrak{a}$ ($xa \in \mathfrak{a}$) для любых $a \in A, x \in \mathfrak{a}$, т.е. $A\mathfrak{a} \subset \mathfrak{a}$ ($\mathfrak{a}A \subset \mathfrak{a}$). Если $\mathfrak{a}$ является одновременно правым и левым идеалом, то говорят, что $\mathfrak{a}$ *двусторонней идеал* или просто *идеал*.

Замечание 2.9. Заметим, что в отличии от групп и нормальных подгрупп, идеал не является кольцом (за исключением тривиального случая $\mathfrak{a} = A$). Действительно, если $1 \in \mathfrak{a}$, то из $a1 \in \mathfrak{a}$ ($1a \in \mathfrak{a}$) для любых $a \in A$, следует $A = \mathfrak{a}$. Следовательно, $1 \notin \mathfrak{a}$ для нетривиального идеала. Тогда $\mathfrak{a}$ не является кольцом. Очевидно, что если $\mathfrak{a}$ и $\mathfrak{b}$ — два идеала (левых, правых или двусторонних), то их пересечение $\mathfrak{a} \cap \mathfrak{b}$ также будет идеалом.

Теорема 2.10. *Пусть $f\colon A \to B$ — гомоморфизм колец. Тогда $\ker f$ является идеалом.*

Доказательство. Заметим, что $f(a) = f(a+0) = f(a)+f(0)$. Отсюда, $0 \in \ker f$. Пусть $a, b \in \ker f$. Тогда $f(a + b) = f(a) + f(b) = 0 + 0 = 0$. Отсюда, $a + b \in \ker f$. Заметим, что

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

Таким образом, $-a \in \ker f$. Следовательно, $\ker f$ — группа относительно операции сложения. Пусть $x \in A$. Тогда $f(ax) = f(a)f(x) = 0f(x) = 0$, $f(xa) = f(x)f(a) = f(x)0 = 0$. Следовательно, $xa, ax \in \ker f$. Таким образом, $\ker f$ — идеал кольца A. □

Аналогично, как в случае групп, мы можем определить факторструктуру $A/\mathfrak{a}$, где A — кольцо, $\mathfrak{a}$ — идеал кольца A. Элементами $A/\mathfrak{a}$ будут являться смежные классы $x + \mathfrak{a}$. Операции сложения и умножение осуществляются по правилам $(x+\mathfrak{a})+(y+\mathfrak{a}) = (x+y)+\mathfrak{a}$, $(x + \mathfrak{a})(y + \mathfrak{a}) = xy + \mathfrak{a}$. Поскольку $\mathfrak{a}$ — подгруппа по сложению, то

мы уже знаем, что операция сложения определена корректно. Докажем корректность операции умножения. Выберем по два представителя x, x' и y, y' в двух смежных классах $x + \mathfrak{a}$ и $y + \mathfrak{a}$. Тогда $x' = x + a$, $y' = y + b$, где $a, b \in \mathfrak{a}$. Отсюда,

$$x'y' = (x + a)(y + b) = xy + ay + xb + ab.$$

Поскольку $\mathfrak{a}$ — идеал кольца A, то $ay, xb \in \mathfrak{a}$. Следовательно, $x'y'$ и xy принадлежат одному и тому же смежному классу.

Теорема 2.11 (теорема о гомоморфизме). *Пусть $f\colon A \to B$ — сюръективный гомоморфизм колец. Тогда существует естественный изоморфизм $A/\ker(f) \cong B$. Обратно, если $\mathfrak{a} \subset A$ — идеал кольца A, то существует естественное отображение $\varphi\colon A \to A/\mathfrak{a}$ такое, что φ — сюръекция и $\ker(\varphi) = \mathfrak{a}$.*

Доказательство. В силу аналогичного утверждения для групп (см. 1.44) мы уже имеем изоморфизм групп $\bar{f}\colon A/\ker(f) \to B$. Осталось проверить его корректность для операции умножения. Пусть $\bar{a}, \bar{b}$ — два смежных класса, и пусть $a \in \bar{a}$, $b \in \bar{b}$. Тогда, по определению,

$$\bar{f}(\bar{a}\bar{b}) = f(ab) = f(a)f(b) = \bar{f}(\bar{a})\bar{f}(\bar{b}).$$

□

Пусть A и B — два кольца. Тогда мы можем определить прямое произведение $A \times B$, как множемтво пар (a, b), $a \in A$, $b \in B$ с операциями $(a_1, b_1)+(a_2, b_2) = (a_1+a_2, b_1+b_2)$, $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$. Нулем будет элемент $(0, 0)$, единицей элемент $(1, 1)$.

Замечание 2.12. Заметим, что если мы возьмем прямое произведение двух полей (тел) A и B, то $A \times B$ не будет полем (телом). Действительно, элементы $(a, 0)$ и $(0, b)$ не обратимы.

Пусть $U \subset A$ — множество обратимых элементов, т.е. множество элементов, имеющих одновременно правый и левый обратный. Тогда U — группа. Действительно, если $a, b \in U$, то обратным к ab будет элемент $b^{-1}a^{-1}$. Группа U называется *группой единиц* кольца A, а элементы этой группы *единицами* кольца A.

2. Коммутативные кольца

В этом параграфе все кольца будут предполагаться коммутативными.

Замечание 2.13. В коммутативных кольцах понятия левого, правого и двустороннего идеала совпадают.

Пусть $\mathfrak{a}$ и $\mathfrak{b}$ — идеалы кольца A. Тогда мы можем определить произведение идеалов $\mathfrak{ab}$, как множество элементов $x = ab$, где $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Заметим, что $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$.

Определение 2.14. Пусть A — кольцо. Идеал $\mathfrak{p} \subset A$ называется *простым*, если из $xy \in \mathfrak{p}$ следует, что либо $x \in \mathfrak{p}$, либо $y \in \mathfrak{p}$. Идеал $\mathfrak{m} \subset A$ называется *максимальным*, если не существует идеала $\mathfrak{a} \neq A$ такого, что $\mathfrak{m} \subset \mathfrak{a}$ и $\mathfrak{m} \neq \mathfrak{a}$.

Утверждение 2.15. *Идеал $\mathfrak{p} \subset A$ простой тогда и только тогда, когда $A/\mathfrak{p}$ целостно.*

Доказательство. Предположим, что идеал $\mathfrak{p} \subset A$ не прост. Тогда существуют $x, y \notin \mathfrak{p}$ такие, что $xy \in \mathfrak{p}$. Пусть $\bar{x}, \bar{y} \in A/\mathfrak{p}$ — образы x, y при естественном гомоморфизме. Тогда $\bar{x}\bar{y} = 0$. Следовательно, кольцо $A/\mathfrak{p}$ целостно не целостно. Пусть $\mathfrak{p} \subset A$ — простой идеал. Предположим, что существуют элементы $\bar{x}, \bar{y} \in A/\mathfrak{p}$ такие, что $\bar{x}\bar{y} = 0$. Пусть x, y — их прообразы при естественном гомоморфизме. Тогда $x, y \notin \mathfrak{p}$, но $xy \in \mathfrak{p}$. Противоречие. □

Утверждение 2.16. *Всякий максимальный идеал — простой.*

Доказательство. Пусть $\mathfrak{m}$ — максимальный идеал. Пусть $x, y \in A$ такие, что $xy \in \mathfrak{m}$ и $x \notin \mathfrak{m}$. Тогда $\mathfrak{m} + Ax$ — идеал, содержащий $\mathfrak{m}$. Поскольку $\mathfrak{m}$ — максимальный идеал, то $\mathfrak{m} + Ax = A$. Следовательно, существуют $m \in \mathfrak{m}$ и $a \in A$ такие, что $1 = m + ax$. Умножая на y, получаем $y = my + axy$. Поскольку $my, axy \in \mathfrak{m}$, то $y \in \mathfrak{m}$. □

Теорема 2.17. *Кольцо $A/\mathfrak{m}$ является полем тогда и только тогда, когда $\mathfrak{m}$ — максимальный идеал кольца A.*

Доказательство. Пусть $\mathfrak{m}$ — максимальный идеал кольца A. Поскольку $\mathfrak{m} \neq A$, то в $A/\mathfrak{m}$ существует единичный элемент. Пусть $x \in A$. Обозначим через $\bar{x}$ — образ x при естественном гомоморфизме. Заметим, что всякий ненулевой элемент $A/\mathfrak{m}$ может быть записан, как $\bar{x}$ для некоторого $x \in A, x \notin \mathfrak{m}$. Заметим, что $\mathfrak{m} + xA$ — идеал кольца A, содержащий $\mathfrak{m}$. Тогда $\mathfrak{m} + xA = A$. Отсюда, существуют $a \in \mathfrak{m}$ и $y \in A$ такие, что $1 = a + xy$. Следовательно, $\bar{x}\bar{y} = \bar{1}$. Таким образом, всякий элемент $A/\mathfrak{m}$ обратим, и $A/\mathfrak{m}$ — поле.

Пусть $A/\mathfrak{m}$ — поле. Предположим, что существует идеал $\mathfrak{m}'$, который содержит $\mathfrak{m}$ и $\mathfrak{m} \neq \mathfrak{m}'$. Пусть $x \in \mathfrak{m}'$ и $x \notin \mathfrak{m}$. Обозначим через $\bar{x}$

— образ x при естественном гомоморфизме. Поскольку $A/\mathfrak{m}$ — поле, то $\bar{x}$ обратим, т.е. существует элемент $\bar{y} \in A/\mathfrak{m}$ такой, что $\bar{x}\bar{y} = \bar{1}$. Пусть y — прообраз $\bar{y}$. Поскольку образ xy при естественном гомоморфизме есть $\bar{1}$, то $xy = 1 + m$, где $m \in \mathfrak{m}$. Тогда $1 = xy - m \in \mathfrak{m}'$. Следовательно, $\mathfrak{m}' = A$. □

Теорема 2.18. *Пусть $f\colon A \to B$ — гомоморфизм колец. Пусть $\mathfrak{p}'$ — простой идеал кольца B. Тогда $\mathfrak{p} = f^{-1}(\mathfrak{p}')$ — простой идеал кольца A.*

Доказательство. Пусть $x, y \in A$ такие, что $xy \in \mathfrak{p}$. Тогда $f(xy) = f(x)f(y) \in \mathfrak{p}'$. Следовательно, либо $f(x) \in \mathfrak{p}'$, либо $f(y) \in \mathfrak{p}'$. Отсюда, либо $x \in \mathfrak{p}$, либо $y \in \mathfrak{p}$. □

Пусть A — кольцо, и $\mathfrak{a}$ — идеал этого кольца. Мы говорим, что элементы $x, y \in A$ *сравнимы по модулю* $\mathfrak{a}$, если $x - y \in \mathfrak{a}$. Записываем $x \equiv y(\mod \mathfrak{a})$.

Теорема 2.19 (китайская теорема об остатках). *Пусть A — коммутативное кольцо, и пусть $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ — идеалы кольца A. Предположим, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ для всех $i \neq j$. Тогда для любого семейства $x_1, x_2, \ldots, x_n \in A$ существует $x \in A$ такой, что $x \equiv x_i(\mod \mathfrak{a}_i)$ для всех i.*

Доказательство. Докажем по индукции. Пусть $n = 2$. Тогда существуют $a_1 \in \mathfrak{a}_1$ и $a_2 \in \mathfrak{a}_2$ такие, что $1 = a_1 + a_2$. Заметим, что $a_1 \equiv 1(\mod \mathfrak{a}_2)$ и $a_2 \equiv 1(\mod \mathfrak{a}_1)$. Рассмотрим $x = x_2a_1 + x_1a_2$. Получаем $x \equiv x_1(\mod \mathfrak{a}_1)$, $x \equiv x_2(\mod \mathfrak{a}_2)$.

Предположим, что теорема доказана для семейства из $n-1$ идеалов. Заметим, что существуют $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2, \ldots, a_{n-1} \in \mathfrak{a}_{n-1}$ и $b_1, b_2, \ldots, b_{n-1} \in \mathfrak{a}_n$ такие, что $a_i + b_i = 1$ для всех i. Тогда

$$(a_1 + b_1)(a_2 + b_2)\cdots(a_{n-1} + b_{n-1}) = 1.$$

С другой стороны,

$$(a_1 + b_1)(a_2 + b_2)\cdots(a_{n-1} + b_{n-1}) \in \mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_{n-1} + \mathfrak{a}_n.$$

Следовательно, $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_{n-1} + \mathfrak{a}_n = A$. Тогда существует $y_n \in A$ такой, что $y_n \equiv 1(\mod \mathfrak{a}_n)$, $y_n \equiv 0(\mod \mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_{n-1})$. Следовательно, $y_n \equiv 1(\mod \mathfrak{a}_n)$ и $y_n \equiv 0(\mod \mathfrak{a}_i)$ для любого $i = 1, 2, \ldots, n-1$. Аналогично, существуют $y_1, \ldots, y_{n-1}$ такие, что $y_i \equiv 1(\mod \mathfrak{a}_i)$, $y_i \equiv 0(\mod \mathfrak{a}_j)$, где $i \neq j$. Тогда элемент $x = x_1y_1 + x_2y_2 + \cdots + x_ny_n$ удовлетворяет требованиям теоремы. □

Следствие 2.20. *Пусть A — коммутативное кольцо, и пусть $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ — идеалы кольца A. Предположим, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ для всех $i \neq j$. Пусть*

$$f\colon A \to (A/\mathfrak{a}_1) \times (A/\mathfrak{a}_2) \times \cdots \times (A/\mathfrak{a}_n)$$

— отображение, индуцированное каноническими отображениями A в $A/\mathfrak{a}_i$ для каждого множителя. Тогда $\ker f = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n$ *и*

$$A/(\mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n) \cong (A/\mathfrak{a}_1) \times (A/\mathfrak{a}_2) \times \cdots \times (A/\mathfrak{a}_n).$$

Доказательство. Утверждение о ядре очевидно. Изоморфизм

$$A/(= \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \cdots \cap \mathfrak{a}_n) \cong (A/\mathfrak{a}_1) \times (A/\mathfrak{a}_2) \times \cdots \times (A/\mathfrak{a}_n)$$

следует из сюръективности f, которая следует из теоремы 2.19. □

Теперь рассмотрим приложение китайской теоремы об остатках к целым числам. Для этого нам потребуется несколько определений и вспомогательных фактов.

Определение 2.21. Идеал $\mathfrak{a}$ кольца A называется *главным*, если существует $a \in A$ такое, что $\mathfrak{a} = aA$. Если в кольце A все идеалы главные, то оно называется *кольцом главных идеалов*.

Утверждение 2.22. *Кольцо $\mathbb{Z}$ является кольцом главных идеалов.*

Доказательство. Пусть $\mathfrak{a} \subset \mathbb{Z}$ — идеал кольца $\mathbb{Z}$. Пусть $a \in \mathfrak{a}$ — минимальное положительное число в идеале $\mathfrak{a}$. Докажем, что все элементы идеала $\mathfrak{a}$ делятся на a. Предположим, что существует элемент $b \in \mathfrak{a}$, который не делится на a. Тогда $b = aq + r$, где $r < a$. Поскольку $a, b \in \mathfrak{a}$, то $r \in \mathfrak{a}$. Противоречие. □

Если $\mathfrak{a} = aA$ — главный идеал, то часто пишут $\mathfrak{a} = (a)$. Поскольку кольцо $\mathbb{Z}$ является кольцом главных идеалов, то мы будем писать $a \equiv b(\mod m)$ вместо $a \equiv b(\mod (m))$ (здесь a, b, m — целые числа).

Теперь запишем китайскую теорему об остатках для кольца целых чисел.

Теорема 2.23. *Пусть $m_1, m_2, \ldots, m_n$ — попарно взаимно простые целые числа. Тогда для любого семейства остатков $x_1, x_2, \ldots, x_n$ существует $x \in \mathbb{Z}$ такой, что $x \equiv x_i(\mod m_i)$ для всех i.*

Замечание 2.24. Пусть (m) — идеал кольца $\mathbb{Z}$. Тогда $\mathbb{Z}/(m) = \mathbb{Z}_m$. Таким образом, существует естественное отображение $f\colon \mathbb{Z} \to \mathbb{Z}_m$.

Замечание 2.25. Не трудно увидеть, что максимальными идеалами в кольце $\mathbb{Z}$ являются идеалы (p), где p — простое число. Из теоремы 2.17 следует, что $\mathbb{Z}_p$ является полем, если p — простое число.

Определение 2.26. Пусть A — целостное кольцо. Элемент $a \neq 0$ называется *неприводимым*, если он не является единицей и из равенства $a = bc$ следует, что либо b, либо c единица.

Утверждение 2.27. *Пусть $a \neq 0$ — элемент целостного кольца A, и главный идеал (a) простой. Тогда a неприводим.*

Доказательство. Пусть $a = bc$. Поскольку идеал (a) простой, то либо $b \in (a)$, либо $c \in (a)$. Пусть $b \in (a)$. Тогда $b = da$. Отсюда, $a = adc$. Следовательно, $cd = 1$, т.е. c — единица кольца A. □

Определение 2.28. Говорят, что элемент $a \in A$, $a \neq 0$, обладает *однозначным разложением на неприводимые элементы*, если существует единица u и неприводимые элементы $p_1, p_2 \ldots, p_k$ такие, что

$$a = up_1p_2 \cdots p_k,$$

причем для двух таких разложений

$$a = up_1p_2 \cdots p_k = u'q_1q_2 \cdots q_m$$

мы имеем $m = k$ и, с точностью до перестановки, $q_i = u_ip_i$, где u_i — единицы в A. Кольцо A называется *факториальным*, если оно целостное и всякий элемент имеет однозначное разложение на неприводимые элементы.

Определение 2.29. Мы говорим, что элемент a *делит* b, если существует элемент $c \in A$ такой, что $b = ac$. Мы говорим, что элемент d является *наибольшим общим делителем* (сокращенно НОД) элементов a и b, если d делит одновременно a и b, и если любой элемент c, делящий a и b, делит также d.

Замечание 2.30. Наибольший общий делитель не всегда определен однозначно.

Теорема 2.31. *Пусть A — целостное кольцо главных идеалов, и $a, b \in A$ — ненулевые элементы. Если $(a, b) = (c)$, то c — наибольший общий делитель элементов a и b.*

Доказательство. Поскольку $a, b \in (c)$, то существуют $x, y \in A$ такие, что $a = xc$, $b = yc$. Таким образом, c делит и a, и b. Пусть d делит и a, и b. Тогда $a = zd$, $b = td$, где $z, t \in A$. С другой стороны, поскольку $c \in (a, b)$, то $c = ua + vb$, где $u, v \in A$. Тогда

$$c = ua + vb = uzd + vtd = (uz + vt)d.$$

Таким образом, d делит c. □

Теорема 2.32. *Всякое целостное кольцо главных идеалов факториально.*

Доказательство. Пусть A — целостное кольцо главных идеалов. Докажем, что любой ненулевой элемент в A разложим на неприводимые множители. Пусть S — множество главных идеалов, образующие которых не имеют разложение на неприводимые множители. Предположим, что S не пусто, и $(a_1) \in S$. Рассмотрим произвольную возрастающую цепочку

$$(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_n) \subsetneq \cdots$$

идеалов из S. Докажем, что она обрывается. Действительно, объединение идеалов этой цепочки есть идеал в A, который порожден a. Тогда $a \in (a_n)$ для какого-то n. Следовательно цепочка обрывается на (a_n). Заметим, что a_n не может быть неприводимым элементом (иначе он имел бы разложение). Следовательно, существуют b и c не являющиеся единицами кольца A такие, что $a_n = bc$. Тогда $(a_n) \subsetneq (b)$ и $(a_n) \subsetneq (c)$. Следовательно, b и c разложимы на неприводимые множители. Тогда произведение их разложений будет разложением a_n. Таким образом, мы доказали, что любой ненулевой элемент в A разложим на неприводимые множители. Докажем единственность этого разложения. Заметим, что если неприводимый элемент p делит ab, то либо p делит a, либо p делит b. Действительно, если p не делит a. Тогда, согласно теореме 2.31, $(a, p) = A$. Следовательно, существуют $x, y \in A$ такие, что $xp + ya = 1$. Тогда $b = bpx + bay$. Поскольку p делит ab, то p делит b. Предположим, что существует два разложения

$$a = u_1 p_1 p_2 \cdots p_r = u_2 q_1 q_2 \cdots q_s.$$

Поскольку p_1 делит произведение, стоящее справа, то существует q_i и единица u такие, что $q_i = up_1$. Без ограничения общности можно считать, что $i = 1$. Сократим на p_1, получаем

$$u_1 p_2 \cdots p_r = u_3 q_2 \cdots q_s.$$

Далее доказательство завершается по индукции. □

Пример 2.33. Кольцо $\mathbb{Z}$ — кольцо главных идеалов, а, следовательно факториально. Группа единиц состоит из 1 и -1. Неприводимыми элементами являются простые числа.

Пример 2.34. Пусть $\mathbb{R}[x]$ — кольцо многочленов с вещественными коэффициентами. Пусть I — идеал этого кольца. Если $f, g \in I$, то $(f, g) = h \in I$. Таким образом, $\mathbb{R}[x]$ — кольцо главных идеалов, а, следовательно, факториально. Группа единиц состоит из вещественных чисел. Неприводимыми элементами являются неприводимые многочлены. Аналогично, $\mathbb{Q}[x]$ — кольцо главных идеалов.

3. Локализация

В этом параграфе все кольца будут предполагаться коммутативными.

Пусть A — кольцо. Множество $S \subset A$ называется *мультипликативным подмножеством*, если $1 \in S$ и если $x, y \in S$, то $xy \in S$. Рассмотрим пары (a, s), где $a \in A$, $s \in S$. Определим отношение эквивалентности. Две пары (a, s), (a', s') эквивалентны, если существует $s'' \in S$ такое, что

$$s''(as' - sa') = 0.$$

Рефлексивность и симметричность очевидна. Проверим транзитивность. Пусть $(a, s) \sim (a', s')$ и $(a', s') \sim (a'', s'')$. Тогда существуют $s_1, s_2 \in S$ такие, что

$$s_1(as' - sa') = 0, \quad s_2(a's'' - s'a'') = 0.$$

Следовательно,

$$s_1 s_2(as's'' - sa's'') = 0, \quad s_1 s_2(a's''s - s'a''s) = 0.$$

Складывая эти уравнения, получаем

$$s_1 s_2(as''s' - a''ss') = s_1 s_2 s'(as'' - a''s) = 0.$$

Множество классов эквивалентности будем обозначать $S^{-1}A$, элементы (a, s) этого множества будем обозначать $\frac{a}{s}$. На множестве $S^{-1}A$ можно ввести операции сложения и умножения. Умножение осуществляется по правилу

$$(\frac{a}{s})(\frac{a'}{s'}) = \frac{aa'}{ss'}.$$

Сложение осуществляется по правилу

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}.$$

Проверим корректность этих операций. Пусть $\frac{a}{s} = \frac{a_1}{s_1}$, $\frac{a'}{s'} = \frac{a'_1}{s'_1}$. Тогда существуют $t_1, t_2 \in S$ такие, что

$$t_1(as_1 - a_1 s) = 0,$$

$$t_2(a's'_1 - a'_1 s') = 0.$$

Умножим первое на $t_2 s' s'_1$, второе на $t_3 s s_1$ и сложим. Получаем

$$0 = t_1 t_2 (s' s'_1 (as_1 - a_1 s) + s s_1 (a' s'_1 - a'_1 s')) =$$

$$= t_1 t_2 (s_1 s'_1 (as' + a's) - s s' (a_1 s'_1 + a'_1 s_1)).$$

Таким образом,

$$\frac{as' + a's}{ss'} = \frac{a_1 s'_1 + a'_1 s_1}{s_1 s'_1}.$$

Следовательно, $S^{-1}A$ является кольцом. Единицей служит класс s/s.

Рассмотрим отображение $\varphi_S A \to S^{-1}A$, осуществляемое по правилу $\varphi_S(a) = a/1$.

Утверждение 2.35. *Пусть A — целостное кольцо и S — мультипликативное множество, не содержащее нуля. Тогда φ_S инъективен.*

Доказательство. Предположим, что существует $a \in A$ такой, что $\varphi_S(a) = a/1 = 0$. Тогда существует $s \in S$, что $sa = 0$. Противоречие. □

Заметим, что множество $S \subset S^{-1}A$ обратимо. Обратным к $s/1$ служит $1/s$.

Пример 2.36. Пусть A — целостное кольцо. Если S состоит из обратимых элементов, то $S^{-1}A = A$.

Пример 2.37. Пусть A — целостное кольцо, и S — множество всех его ненулевых элементов. Тогда S — мультипликативное множество, и $S^{-1}A$ — поле. Оно называется *полем частных* кольца A. Например, $\mathbb{Q}$ — поле частных кольца $\mathbb{Z}$.

4. Многочлены

Пусть A — коммутативное кольцо (в этом параграфе слово "кольцо"означает "коммутативное кольцо"). Построим новое кольцо B, элементами которого будут последовательности

$$f = (a_0, a_1, a_2, \ldots, a_n, \ldots), \quad a_i \in A$$

такие, что все a_i за исключением конечного числа равны нулю. Определим на этом множестве операции сложения и умножения, полагая

$$f+g=(a_0,a_1,\ldots,a_n,\ldots)+(b_0,b_1,\ldots,b_n,\ldots)=$$
$$=(a_0+b_0,a_1+b_1,\ldots,a_n+b_n,\ldots),$$
$$f\cdot g=(a_0,a_1,\ldots,a_n,\ldots)\cdot(b_0,b_1,\ldots,b_n,\ldots)=(h_0,h_1,\ldots,h_n,\ldots),$$

где

$$h_m=\sum_{i+j=m}a_ib_j.$$

Очевидно, что B — кольцо. Нулем будет элемент $(0,0,0,\ldots)$, единицей $(1,0,0,\ldots)$. Обратным к $f=(a_0,a_1,\ldots,a_n,\ldots)$ будет $f=(-a_0,-a_1,\ldots-,a_n,\ldots)$. Рассмотрим гомоморфизм, $\varphi A\to B$ заданный по правилу $\varphi(a)=(a,0,0,\ldots)$. Очевидно, что φ инъективен. Таким образом, мы можем рассматривать кольцо A, как подкольцо кольца B. Пусть $x=(0,1,0,0,\ldots)$. Тогда $x^2=(0,0,1,0,\ldots)$, $x^3=(0,0,0,1,0\ldots)$ и т.д. Поскольку $A\subset B$, то

$$a\cdot x^n=a\cdot(0,0,\ldots,0,1,0,\ldots)=(0,0,\ldots,0,a,0,\ldots),$$

где $a\in A$. Таким образом, любой элемент из B может быть записан в виде

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n.$$

Кольцо B называется *кольцом многочленов* от одной переменной и обозначается $A[x]$. Элементы $a_0,a_1,\ldots,a_n$ называются *коэффициентами* многочлена $f(x)$, максимальное n для которого $a_n\neq 0$ называется *степенью* многочлена и обозначается $\deg(f)$. Пусть

$$g(x)=b_0+b_1x+b_2x^2+\cdots+b_mx^m.$$

Тогда

$$f(x)g(x)=a_0b_0+(a_0b_1+a_1b_0)x+\cdots+a_nb_mx^{n+m}.$$

Отсюда следует следующие утверждения.

Утверждение 2.38. *Пусть A — целостное кольцо. Тогда* $\deg(f+g)\leq\max(\deg(f),\deg(g))$, $\deg(fg)=\deg(f)+\deg(g)$.

Теорема 2.39. *Пусть A — целостное кольцо. Тогда $A[x]$ также является целостным.*

Теорема 2.40. *Пусть A — подкольцо коммутативного кольца K, и $\alpha\in K$. Тогда существует единственный гомоморфизм $\varphi_\alpha\colon A[x]\to K$, такой, что $\varphi_\alpha(a)=a$ для любого $a\in A$ и $\varphi_\alpha(x)=\alpha$.*

Доказательство. Предположим, что такой гомоморфизм существует. Поскольку $\varphi_\alpha(a) = a$ и $\varphi_\alpha(x) = \alpha$, то

$$\varphi_\alpha(f) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n.$$

Таким образом, φ_α определен однозначно. Обратно, мы можем задать φ_α, как

$$\varphi_\alpha(f) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n.$$

Легко проверяется, что данное отображение будет гомоморфизмом. □

Элемент α называется *алгебраическим* над A, если существует $f \in A[x]$ такой, что $\varphi_\alpha(f) = 0$. Если φ_α инъективно, то α называется *трансцендентным* над A. Если $A = \mathbb{Q}$, $K = \mathbb{C}$, то говорят об *алгебраических* и *трансцендентных* числах. Если $\varphi_\alpha(f) = 0$, то α называется *корнем* многочлена f, будем писать $f(\alpha) = 0$.

Рассмотрим алгоритм деления в кольце многочленов.

Теорема 2.41. *Пусть K — поле и $f, g \in K[x]$. Тогда существуют многочлены $q, r \in K[x]$, причем $\deg r < \deg g$, что $f = qg + r$.*

Доказательство. Пусть

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

Если $m > n$, то $q = 0$, $r = f$. Предположим, что $n \geq m$. Пусть $f_1 = f - \frac{a_n}{b_m}x^{n-m}g$. Тогда $\deg f_1 \leq n - 1$. Если $\deg f_1 < \deg g$, то все доказано. Предположим, что $\deg f_1 \geq \deg g$. Пусть $f_2 = f_1 - \frac{a'}{b_m}x^{\deg f_1 - m}g$, где a' — коэффициент при старшей степени. Снова, $\deg f_2 \leq \deg f_1 - 1$. Если $\deg f_2 < \deg g$, то все доказано. Продолжая этот процесс, мы получим нужное представление. □

Пусть K — поле и $f, g \in K[x]$. Запишем $f = q_1 g + r_1$. Поскольку $\deg r_1 < \deg g$, то существуют $q_2, r_2 \in K[x]$ такие, что $g = q_2 r_1 + r_2$. Аналогично, $r_1 = q_3 r_2 + r_3$ и т.д. Поскольку $\deg r_{i+1} < \deg r_i$, мы получим

$$\begin{cases} f = q_1 g + r_1 \\ g = q_2 r_1 + r_2 \\ r_1 = q_3 r_2 + r_3 \\ \cdots \quad \cdots \\ r_{n-2} = q_n r_{n-1} + r_n \\ r_{n-1} = q_{n+1} r_n. \end{cases}$$

Подставим $r_1 = f - q_1 g$ в $g = q_2 r_1 + r_2$, получим $r_2 = (1 + q_1 q_2) g - q_2 f$. Затем выразим r_3. Продолжая этот процесс, мы получим $r_n = Pf + Qg$.

Утверждение 2.42. *Многочлен r_n является наибольшим общим делителем f и g.*

Доказательство. Поскольку $r_{n-1} = q_{n+1} r_n$, то r_{n-1} делится на r_n. В силу $r_{n-2} = q_n r_{n-1} + r_n$ видим, что r_{n-2} делится на r_n. Таким образом, f и g делится на r_n. Пусть делится f и g делится на $d(x)$. Из равенства $r_n = Pf + Qg$ следует, что и r_n делится на $d(x)$. □

Рассмотрим еще один класс колец. Пусть A — целостное кольцо и определено отображение $\delta\colon A \setminus \{0\} \to \mathbb{N} \cup \{0\}$, обладающее следующими свойствами.

(1) $\delta(ab) \geq \delta(a)$ $\forall a, b \in A \setminus \{0\}$;
(2) для любых $a, b \in A$, $b \neq 0$ существуют $q, r \in A$ такие, что $a = qb + r$, $\delta(r) < \delta(b)$ или $r = 0$.

Такие кольца называются *евклидовыми кольцами.*

Теорема 2.43. *Всякое евклидово кольцо является кольцом главных идеалов.*

Доказательство. Пусть A — евклидово кольцо, $\mathfrak{a}$ — идеал в A. Пусть $a \in \mathfrak{a}$ — элемент для которого $\delta(a)$ минимально. Пусть $b \in \mathfrak{a}$. Тогда $b = qa + r$, где $\delta(r) < \delta(a)$ или $r = 0$. Поскольку $qa \in \mathfrak{a}$, то $r \in \mathfrak{a}$. В силу минимальности $\delta(a)$, $r = 0$. Тогда $b = qa$. Следовательно, $\mathfrak{a} = (a)$ — главный идеал. □

Следствие 2.44. *Всякое евклидово кольцо является факториальным.*

Заметим, что кольцо многочленов над полем евклидово. Возьмем $\delta(f) = \deg f$. Таким образом, $A[x]$ — кольцо главных идеалов, а следовательно, и факториально.

Лемма 2.45 (лемма Гаусса). *Пусть $f(x)$ и $g(x)$ — многочлены с целыми коэффициентами. Пусть a — наибольший общий делитель коэффициентов многочлена $f(x)$, b — наибольший общий делитель коэффициентов многочлена $g(x)$, c — наибольший общий делитель коэффициентов многочлена $f(x)g(x)$. Тогда $c = ba$.*

Доказательство. Достаточно доказать, что если $a = b = 1$, то $c = 1$. Предположим, что c делится на простое число p. Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0.$$

Пусть r — наименьшее число такое, что a_r не делится на p, s — наименьшее число такое, что b_s не делится на p. Рассмотрим коэффициент при x^{r+s} в $f(x)g(x)$. Он равен

$$c_{r+s} = a_r b_s + a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots + a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \cdots .$$

Заметим, что все слагаемые, кроме $a_r b_s$ делятся на p, а $a_r b_s$ не делится на p. Тогда c_{r+s} также не делится на p. □

Пусть K — поле. Многочлен $f \in K[x]$ ненулевой степени называется *неприводимым* над полем K, если он не делится ни на какой многочлен $g \in K[x]$, у которого $1 \leq \deg g < \deg f$.

Теорема 2.46. *Пусть $f(x) \in K[x]$ и $\alpha \in K$ — корень $f(x)$. Тогда $f = g(x - \alpha)$ для некоторого $g \in K$.*

Доказательство. Предположим, что f не делится на $x - \alpha$. Тогда наибольший общий делитель этих многочленов равен 1. Следовательно, существуют $h, g \in K[x]$ такие, что $fh + g(x - \alpha) = 1$. Заметим, что $\varphi_\alpha(x - \alpha) = 0$ и $\varphi_\alpha(1) = 1$. Применяя φ_α к равенству $fh + g(x - \alpha) = 1$, получаем $0 = 1$. Противоречие. □

Пусть f — неприводимый многочлен над K. Из теоремы 2.46 следует, что если $\deg f \geq 2$, то f не имеет корней в K. Докажем, что $\mathfrak{a} = (f)$ — максимальный идеал. Действительно, если существует $\mathfrak{a}' \supset \mathfrak{a}$, то $\mathfrak{a}' = (g)$. Следовательно, $f = gh$. Если $\deg h \geq 1$, то f приводим. Отсюда, $\deg h = 0$, т.е. $h \in K$. Тогда $g = h^{-1} f$ и $\mathfrak{a}' = \mathfrak{a}$. Согласно теореме 2.17 $K[x]/(f)$ является полем. Заметим, что естественный гомоморфизм $K[x] \to K[x]/(f)$ задает инъективный гомоморфизм K в $K[x]/(f)$. Таким образом, мы можем рассматривать K как подполе $K[x]/(f)$. Заметим, что образ элемента x в $K[x]/(f)$ является корнем многочлена f. Поле $K[x]/(f)$ называется расширением поля K.

Теорема 2.47. *Пусть $f(x) \in K[x]$. Тогда существует расширение E поля K, в котором $f(x)$ разлагается на линейные множители, т.е.*

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

где $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$.

Доказательство. Пусть $f = af_1f_2\cdots f_m$ — разложение на неприводимые множители, причем коэффициент при старшей степени во всех f_i равен 1. Если все f_i линейны, то все доказано. Пусть $\deg f_i \geq 2$. Рассмотрим расширение $E_1 = K[x]/(f_i)$. Поскольку $K[x] \subset E_1[x]$, то $f = af_1f_2\cdots f_m$ над E_1. Более того, f_i имеет разложение в поле E_1. Таким образом, $f = af_1'f_2'\cdots f_{m'}'$ над E_1, где $m' > m$. Если все f_i' линейны, то все доказано. Если существует f_j' такой, что $\deg f_j' \geq 2$, рассмотрим расширение $E_2 = E_1[x]/(f_j')$. Продолжая этот процесс, мы получаем необходимое разложение. □

Заметим, что число α_i совпадает со степенью многочлена (возможно не все α_i различны. Число s называется *кратностью* корня α, если $f(x) = g(x)(x-\alpha)^s$ и $g(\alpha) \neq 0$.

Определение 2.48. Поле K называется *алгебраически замкнутым*, если любой многочлен $f(x) \in K[x]$ имеет корень.

Теорема 2.49. *Для любого поля K существует поле $\bar{K}$, содержащее поле K, такое, что $\bar{K}$ алгебраически замкнуто.*

Если все элементы поля $\bar{K}$ алгебраичны над K, то $\bar{K}$ называется *алгебраическим замыканием* поля K.

Теорема 2.50 (основная теорема алгебры). *Поле $\mathbb{C}$ алгебраически замкнуто.*

Для доказательства этой теоремы нам потребуется некоторые вспомогательные утверждения.

Лемма 2.51 (лемма Даламбера). *Пусть $f(x)$ — многочлен над полем комплексных чисел, и $f(x_0) \neq 0$. Тогда существует $h \in \mathbb{C}$ такое, что $|f(x_0+h)| < |f(x_0)|$.*

Доказательство. Рассмотрим разложение в ряд Тейлора в точке x_0, получаем

$$f(x) = f(x_0)+f'(x_0)(x-x_0)+\frac{f''(x_0)}{2}(x-x_0)^2+\cdots+\frac{f^{(n)}(x_0)}{n!}(x-x_0)^n.$$

Обозначим $h = x - x_0$. Пусть

$$f'(x_0) = f''(x_0) = \cdots = f^{(k-1)}(x_0) = 0, \quad f^{(k)}(x_0) \neq 0.$$

Тогда

$$f(x_0+h) = f(x_0) + \frac{f^{(k)}(x_0)}{k!}h^k + \cdots + \frac{f^{(n)}(x_0)}{n!}h^n.$$

Поделим на $f(x_0)$, получим

$$\frac{f(x_0+h)}{f(x_0)} = 1 + c_k h^k + c_{k+1} h^{k+1} + \cdots + c_n h^n,$$

где $c_i = \frac{f^{(i)}(x_0)}{i! f(x_0)}$. Получаем

$$\frac{f(x_0+h)}{f(x_0)} = 1 + c_k h^k + c_k h^k \left(\frac{c_{k+1}}{c_k} h + \cdots + \frac{c_n}{c_k} h^{n-k} \right).$$

Отсюда,

$$\left| \frac{f(x_0+h)}{f(x_0)} \right| \leq |1 + c_k h^k| + |c_k h^k| \left| \frac{c_{k+1}}{c_k} h + \cdots + \frac{c_n}{c_k} h^{n-k} \right|.$$

Рассмотрим

$$g(h) = \frac{c_{k+1}}{c_k} h + \cdots + \frac{c_n}{c_k} h^{n-k}.$$

Заметим, что g непрерывна и $g(0) = 0$. Следовательно, для любого $\varepsilon > 0$ существует δ такое, что для любого h с условием $|h| < \delta$ выполнено $|g(h)| < \varepsilon$. Возьмем $\varepsilon = \frac{1}{2}$. Тогда для любого h с условием $|h| < \delta$ выполнено

$$\left| \frac{f(x_0+h)}{f(x_0)} \right| \leq |1 + c_k h^k| + \frac{1}{2} |c_k h^k|.$$

Рассмотрим h с $\arg h^k = \pi - \arg c_k$. Тогда $c_k h^k = -|c_k||h|^k$. Отсюда,

$$\left| \frac{f(x_0+h)}{f(x_0)} \right| \leq |1 + c_k h^k| + \frac{1}{2} |c_k h^k| = 1 - |c_k||h|^k + \frac{1}{2} |c_k||h|^k = 1 - \frac{1}{2} |c_k||h|^k.$$

Получаем $|f(x_0+h)| < |f(x_0)|$. □

Лемма 2.52. *Для любого $K \in \mathbb{R}$ существует $M \in \mathbb{R}$ такое, что для любого x с условием $|x| > M$ выполнено $|f(x)| > K$.*

Доказательство. Имеем

$$\begin{gathered} |f(x)| = |a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0| \geq \\ \geq |a_n x^n| - |a_{n-1} x^{n-1} + \cdots + a_1 x + a_0| \geq \\ \geq |a_n||x|^n - (|a_{n-1}||x|^{n-1} + \cdots + |a_1||x| + |a_0|). \end{gathered}$$

Теперь утверждение следует из известного факта из математического анализа. □

Теперь докажем теорему. Нам необходимо доказать, что любой многочлен имеет корень в $\mathbb{C}$. Мы можем считать, что $a_0 \neq 0$. Пусть $M \in \mathbb{R}$ такое, что $|f(x)| > 2|a_0|$ для любого x с условием $|x| > M$. Рассмотрим замкнутый круг R радиуса M. Заметим, что функция $|f(x)|$ непрерывна. Следовательно, $|f(x)|$ достигает минимума в R.

Этот минимум достигается во внутренней точке круга R. Пусть x_0 — точка минимума. Согласно лемме 2.52 x_0 — точка минимума $|f(x)|$ на всем $\mathbb{C}$. С другой стороны, согласно лемме Даламбера если $|f(x_0)| \neq 0$, то существует h такое, что $|f(x_0+h)| < |f(x_0)|$. Таким образом, $f(x)$ имеет корень в $\mathbb{C}$.

5. Модули

Определение 2.53. Пусть A — кольцо. *Левым модулем* над A (или *левым A-модулем*) называется абелева группа M с действием кольца A на M, удовлетворяющим следующим свойствам.

(1) $(a+b)x = ax + bx \ \forall a, b \in A, x \in M$;
(2) $a(x+y) = ax + ay \ \forall a \in A, x, y \in M$;
(3) $(ab)x = a(bx) \ \forall a, b \in A, x \in M$;
(4) $1 \cdot x = x \ \forall x \in M$.

Аналогично можно определить *правый A-модуль*. Далее мы будем иметь дело только с левыми модулями над кольцом A, поэтому будем называть их просто "модуль"(A-модуль).

Пример 2.54. Любой левый идеал в A есть модуль.

Пример 2.55. Любая коммутативная группа есть $\mathbb{Z}$-модуль.

Пример 2.56. Кольцо многочленов $A[x]$ есть A-модуль.

Определение 2.57. Пусть M — модуль. Подгруппа $N \subset M$ называется *подмодулем*, если $AN \subset N$.

Пример 2.58. Пусть M — модуль над A и $\mathfrak{a} \subset A$ — левый идеал в A. Тогда множество $\mathfrak{a}M$ всех элементов вида

$$a_1x_1 + a_2x_2 + \cdots a_nx_n,$$

где $a_i \in \mathfrak{a}$, $x_i \in M$ будет подмодулем в M.

Пусть M — модуль над A и N — его подмодуль. Определим структуру модуля на факторгруппе M/N. Пусть $x+N$ — смежный класс. Тогда $a(x+N) = ax + N$. Модуль M/N называется *факторомодулем*. Пусть M и M' — A-модули. *Гомоморфизмом* модулей $f\colon M \to M'$ называется гомоморфизм групп такой, что $f(ax) = af(x)$ для любых $a \in A$, $x \in M$. *Ядром* $\ker f$ называется множество $N = \{x \mid f(x) = 0\}$. Легко заметить, что N — подмодуль M. *Образом* Imf называется множество $N' = \{y \mid y \in M' \quad \exists x f(x) = y\}$. Легко заметить, что N' — подмодуль M'.

Как и в случае групп имеем теоремы о гомоморфизме.

Теорема 2.59 (1-я теорема о гомоморфизме). *Пусть* $f\colon M \to M'$ *— сюръективный гомоморфизм модулей. Тогда существует естественный изоморфизм* $M/\ker(f) \cong M'$.

Доказательство. Пусть $\bar{f}\colon M/\ker(f) \to M'$ — отображение, определяемое следующим образом: $\bar{f}(x + \ker(f)) = f(x)$. Докажем корректность определения $\bar{f}$. Пусть $x + \ker(f) \in M/\ker(f)$, $a \in A$. Тогда

$$\bar{f}(a(x + \ker(f))) = \bar{f}(ax + \ker(f)) = f(ax) = af(x) = af(x + N).$$

Изоморфизм $M/\ker(f) \cong M'$ следует из аналогичного утверждения для групп. □

Теорема 2.60 (2-я теорема о гомоморфизме). *Пусть* N *и* N' *— подмодули модуля* M. *Тогда* $(N + N')/N' \cong N/(N \cap N')$.

Доказательство. Пусть $f\colon N \to (N+N')/N'$ — гомоморфизм групп, определяемый следующим образом: $f(h) = h+N'$. Очевидно, что f — сюръекция. Тогда, по теореме 2.59, $(N+N')/N' \cong N/\ker(f)$. Очевидно, $N \cap N' \subset \ker(f)$. Пусть $a \in \ker(f)$. Тогда $a \in N'$. Следовательно, $a \in N \cap N'$. Таким образом, $N \cap N' = \ker(f)$ и теорема доказана. □

Теорема 2.61 (3-я теорема о гомоморфизме). *Пусть* N *и* N' *— подмодули модуля* M, *причем* $N' \subset N$. *Тогда*

$$M/N \cong (M/N')/(N/N').$$

Доказательство. Рассмотрим гомоморфизм $f\colon M/N' \to M/N$, определяемый следующим образом: $f(x + N') = x + N$. Очевидно, что $\ker(f)$ состоит из всех $x + N'$ таких, что $x \in N$. Следовательно, $\ker(f) \cong N/N'$. Таким образом, наше утверждение следует из теоремы 2.59. □

Пусть M и M' — A-модули. *Прямой суммой* $M \oplus M'$ этих модулей называется прямая сумма абелевых групп, на которой определена структура модуля $a(x, y) = (ax, ay)$, где $x \in M$, $y \in M'$, $a \in A$. Модуль M называется *конечно порожденным* или модулем *конечного типа*, если он имеет конечную систему образующих, т.е. существуют элементы $x_1, x)2, \ldots, x_n \in M$ такие, что любой $x \in M$ имеет представление

$$x = a_1x_1 + a_2x_2 + \cdots a_nx_n.$$

Определение 2.62. *Аннулятором* A-модуля M называется множество

$$\mathrm{Ann}(M) = \{a \mid a \in A, ax = 0, \forall x \in M\}.$$

Модуль M называется *точным*, если $\operatorname{Ann}(M) = 0$.

Теорема 2.63. $\operatorname{Ann}(M)$ — *двусторонний идеал кольца* A.

Доказательство. Очевидно, что $0 \in \operatorname{Ann}(M)$. Пусть $b, c \in \operatorname{Ann}(M)$. Тогда $(b+c)x = bx + cx = 0$ для любого $x \in M$. Из равенства

$$0 = (b-b)x = bx + (-bx) = (-bx)$$

следует, что $-b \in \operatorname{Ann}(M)$. Таким образом, $\operatorname{Ann}(M)$ — абелева группа. Пусть $a \in A$. Тогда

$$(ab)x = a(bx) = a \cdot 0 = 0, \quad (ba)x = b(ax) = by = 0.$$

Таким образом, $\operatorname{Ann}(M)$ — двусторонний идеал кольца A. □

Полагая $(a + \operatorname{Ann}(M))x = ax$ для $x \in M$, $(a + \operatorname{Ann}(M) \in A/\operatorname{Ann}(M)$, мы определяем на M структуру $A/\operatorname{Ann}(M)$-модуля.

Модуль M над полем называется *векторным пространством*. Если M конечно порожден, то M *конечномерное векторное пространство*.

6. Алгебры

Определение 2.64. Пусть K — поле. Будем говорить, что A является *алгеброй* над полем K или K-*алгеброй*, если A является векторным пространством над K и на A есть операция умножения, удовлетворяющая следующим свойствам

(1) $x(y+z) = xy + xz$, $\forall x, y, z \in A$;
(2) $(x+y)z = xz + yz$, $\forall x, y, z \in A$;
(3) $(ax)y = x(ay) = a(xy)$, $\forall x, y \in A$, $a \in K$.

Если умножение в A обладает свойством ассоциативности, то A называется *ассоциативной алгеброй*. Если в A существует единица, т.е. элемент $1 \in A$ такой, что $x = 1 \cdot x = x \cdot 1$ для любого $x \in A$, то A называется *алгеброй с единицей*.

В этом параграфе все алгебры будут предполагаться ассоциативными алгебрами с единицей. Заметим, что в таких алгебрах $K \cong K \cdot 1$. Действительно, пусть $f\colon K \to A$ — отображение, заданное $f(a) = a \cdot 1$. Заметим, что $\ker f \neq K$. Поскольку K — поле, то $\ker f = 0$. Таким образом, мы можем считать, что $K \subset A$.

Алгебра A над полем K называется *конечномерной*, если конечномерно векторное пространство A над K. Алгебра A над полем K

называется *конечно порожденной*, если существует конечное множество элементов порождающих A.

Пример 2.65. Поле $\mathbb{C}$ является алгеброй над $\mathbb{R}$.

Пример 2.66. Пусть K — поле. Кольцо многочленов $K[x]$ есть K-алгебра. Эта алгебра конечно порождена, но не конечномерна.

Пример 2.67. Кольцо матриц $M_n(K)$ является конечномерной K-алгеброй.

Теорема 2.68. *Пусть A — n-мерная алгебра над полем K. Тогда A изоморфна некоторой подалгебре в $M_n(K)$.*

Доказательство. Пусть $a \in A$. Тогда a определяет отображение $a^*\colon A \to A$ по правилу $a^*(x) = ax$. Заметим, что для любых $x, y \in A$, $\alpha \in K$ выполнено

$$a^*(x+y) = a(x+y) = ax + ay = a^*(x) + a^*(y),$$

$$a^*(\alpha x) = a(\alpha x) = \alpha ax = \alpha a^*(x).$$

Таким образом, a — линейный оператор на пространстве A. Более того, для $a, b \in A$ выполнено

$$(a+b)^*(x) = (a+b)x = ax + bx = a^*(x) + b^*(x) = (a^* + b^*)(x),$$

$$(ab)^*(x) = (ab)x = a(bx) = ab^*(x) = a^*(b^*(x)) = (a^*b^*)(x).$$

Зафиксируем базис $e_1, e_2, \dots e_n$ пространства A. Мы получили гомоморфизм $J\colon A \to M_n(K)$, отображающий элемент $a \in A$ в матрицу линейного оператора a^*. Докажем, что гомоморфизм инъективен. Пусть $J(a) = 0$. Тогда $a = a \cdot 1 = a^*(1) = 0$. □

Теорема 2.69. *Пусть A — n-мерная алгебра над полем K. Тогда для любого $a \in A$ существует многочлен $f(x) \in K[x]$ такой, что $f(a) = 0$ и $\deg f \leq n$.*

Доказательство. Поскольку A — n-мерная алгебра над полем K, то элементы $1, a, a^2 \cdots a^n$ линейно зависимы. Тогда существуют $\alpha_0, \alpha_1 \dots, \alpha_n \in K$ такие, что $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots \alpha_n a^n = 0$. □

Многочлен $f(x) \in K[x]$ для которого $f(a) = 0$ называется *аннулирующим* элемент a.

Теорема 2.70. *Пусть A — конечномерная алгебра над полем K. Тогда любой элемент $a \in A$ либо обратим, либо является делителем нуля.*

Доказательство. Рассмотрим многочлен $f(x) = \alpha_n x^n + \cdots + \alpha_1 x + \alpha_0$ минимальной степени, аннулирующий a. Предположим, что $\alpha_0 = 0$. Тогда

$$0 = f(a) = \alpha_n a^n + \cdots + \alpha_1 a = a(\alpha_n a^{n-1} + \cdots + \alpha_1).$$

Поскольку $f(x)$ имеет минимальную степень из всех многочленов, аннулирующих a, то a — делитель нуля. Предположим, что $\alpha_0 \neq 0$. Тогда

$$1 = \alpha_0^{-1}(\alpha_n a^{n-1} + \cdots + \alpha_1)a.$$

Таким образом, a обратим. □

Следствие 2.71. *Пусть A — конечномерная алгебра над полем K. Если в A нет делителей нуля, то A — тело.*

Если в K-алгебре A (необязательно ассоциативной) есть единичный элемент и любой элемент обратим, то такая алгебра называется *алгеброй с делением*. Пусть A — конечномерная алгебра над полем K и $e_1, e_2, \ldots, e_n$ — базис A над K. Тогда соотношения

$$e_i e_j = \sum_{k=1}^{n} g_{ij}^k e_k$$

задают структуру K-алгебры на A. Действительно, пусть

$$a = a_1 e_1 + a_2 e_2 + \cdots + a_n e_n, \quad b = b_1 e_1 + b_2 e_2 + \cdots + b_n e_n,$$

тогда

$$ab = \left(\sum_{i=1}^{n} a_i e_i\right)\left(\sum_{j=1}^{n} b_j e_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i b_j e_i e_j = \sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} a_i b_j g_{ij}^k e_k.$$

Пример 2.72. Рассмотрим четырехмерное векторное пространство $\mathbb{H}$ над $\mathbb{R}$ с базисом $1, i, j, k$, т.е. $\mathbb{H}$ — множество $x = a + bi + cj + dk$, где $a, b, c, d \in \mathbb{R}$. Положим $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$. Эти соотношения определяют $\mathbb{R}$-алгебру на $\mathbb{H}$. Не трудно убедиться, что элементы $\pm 1, \pm i, \pm j, \pm k$ образуют группу (это группа кватернионов). Таким образом, $\mathbb{H}$ ассоциативная $\mathbb{R}$-алгебра с единицей. Пусть $x = a + bi + cj + dk$. Положим $\bar{x} = a - bi - cj - dk$. Тогда

$$x\bar{x} = (a + bi + cj + dk)(a - bi - cj - dk) =$$

$$= a^2 - abi - acj - adk + abi + b^2 - bck + bdj + acj + bck +$$

$$+ c^2 - cdi + adk - bdj + cdi + d^2 = a^2 + b^2 + c^2 + d^2.$$

Следовательно,

$$(a+bi+cj+dk)(\frac{a}{|x|}-\frac{b}{|x|}i-\frac{c}{|x|}j-\frac{d}{|x|}k)=1,$$

где $|x| = a^2+b^2+c^2+d^2$. Таким образом, любой элемент в $\mathbb{H}$ обратим. Мы получили, что $\mathbb{H}$ — тело. Это тело называется *телом кватернионов*. Легко увидеть, что $\mathbb{H}$ не является полем.

Определение 2.73. Пусть A — конечномерная алгебра над полем K и $a \in A$. Тогда многочлен $f(x)$, аннулирующий a, степень которого минимальна и старший коэффициент равен 1, называется *минимальным многочленом элемента* a над K.

Теорема 2.74. *Пусть A — конечномерная алгебра с делением над полем K и $a \in A$. Тогда минимальный многочлен $f(x)$ элемента a неприводим и единственен. Более того, любой многочлен $g(x)$, аннулирующий a, делится на $f(x)$.*

Доказательство. Пусть $f(x)$ — минимальный многочлен элемента a. Предположим, что он приводим, т.е. $f(x) = g(x)h(x)$ и $\deg f > \deg g \geq \deg h \geq 1$. Тогда $0 = f(a) = g(a)h(a)$. Поскольку A — алгебра с делением, то либо $g(a) = 0$, либо $h(a) = 0$. Противоречие с минимальностью $f(x)$. Пусть $g(x)$ — другой многочлен, аннулирующий a. Заметим, что $\deg g \geq \deg f$. Тогда $g(x) = q(x)f(x)+r(x)$, где $\deg r < \deg f$. Поскольку $f(a) = g(a) = 0$, то $r(a) = 0$. Следовательно, $r(x) = 0$. Таким образом, $g(x)$ делится на $f(x)$. Если $\deg f = \deg g$, то $f = \alpha g$, где $\alpha \in K$. Отсюда следует единственность $f(x)$. □

Теорема 2.75. *Пусть A — конечномерная алгебра с делением над полем $\mathbb{C}$. Тогда $A = \mathbb{C}$.*

Доказательство. Пусть $a \in A$, и $f(x)$ — его минимальный многочлен. Тогда $f(x)$ неприводим (см. 2.74). Тогда $f(x) = x - a$ (см. 2.50). Отсюда, $a \in \mathbb{C}$. □

Теорема 2.76 (Фробениус). *Пусть A — конечномерная ассоциативная алгебра с делением над полем $\mathbb{R}$. Тогда либо $A = \mathbb{R}$, либо $A = \mathbb{C}$, либо $A = \mathbb{H}$.*

Лемма 2.77. *Пусть $f(x) \in \mathbb{R}[x]$, и α — комплексный корень $f(x)$. Тогда $\bar{\alpha}$ — тоже корень $f(x)$.*

Доказательство. Пусть

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

где все $a_i \in \mathbb{R}$. Заметим, что $\bar{a}_i = a_i$. Тогда

$$f(\bar{\alpha}) = a_n\bar{\alpha}^n + a_{n-1}\bar{\alpha}^{n-1} + \cdots + a_1\bar{\alpha} + a_0 = \bar{a}_n\overline{\alpha^n} + \bar{a}_{n-1}\overline{\alpha^{n-1}} + \cdots + \bar{a}_1\bar{\alpha} + \bar{a}_0$$
$$= \overline{a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0} = 0.$$

□

Следствие 2.78. *Любой многочлен $f(x) \in \mathbb{R}[x]$ степени больше 2 приводим.*

Доказательство. Пусть $f(x) \in \mathbb{R}[x]$ и $\deg f > 2$. Пусть α — комплексный корень многочлена $f(x)$. Согласно 2.77 $\bar{\alpha}$ — тоже корень $f(x)$. Тогда $f(x)$ делится на $x-\alpha$ и $x-\bar{\alpha}$ над $\mathbb{C}$. Следовательно, $f(x)$ делится на $(x-\alpha)(x-\bar{\alpha})$. С другой строны,

$$(x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha+\bar{\alpha})x + \bar{\alpha}\alpha \in \mathbb{R}[x].$$

Таким образом, $f(x)$ приводим. □

Теперь докажем более слабый вариант теоремы Фробениуса.

Теорема 2.79. *Пусть A — конечномерная ассоциативная коммутативная алгебра с делением над полем $\mathbb{R}$ (т.е. A — поле). Тогда либо $A = \mathbb{R}$, либо $A = \mathbb{C}$.*

Доказательство. Если размерность A над $\mathbb{R}$ равна единице, то $A = \mathbb{R}$. Предположим, что $\dim A \geq 2$. Тогда существует $a \in A$ такое, что $a \notin \mathbb{R}$. Пусть $f(x)$ — минимальный многочлен элемента a. Согласно теореме 2.74 и следствию 2.78, либо $\deg f = 1$, либо $\deg f = 2$. Если $\deg f = 1$, то $f(x) = x - a$ и $a \in \mathbb{R}$. Следовательно, $\deg f = 2$, т.е. $f(x) = x^2 + \alpha x + \beta$, $\alpha, \beta \in \mathbb{R}$. Представим $f(x)$ в виде

$$f(x) = (x + \frac{\alpha}{2})^2 + (\beta - \frac{\alpha^2}{4}).$$

Отсюда, $(a + \frac{\alpha}{2})^2 = D$, где $D = \frac{\alpha^2}{4} - \beta$. Если $D \geq 0$, то многочлен $f(x)$ приводим, что противоречит теореме 2.74. Положим $i = \frac{a+\frac{\alpha}{2}}{\sqrt{|D|}}$. Тогда $i^2 = -1$. Таким образом, в A есть подалгебра $\mathbb{R} + \mathbb{R}i$, которая изоморфна полю комплексных чисел. Поскольку A поле, содержащее $\mathbb{C}$, то A является $\mathbb{C}$-алгеброй. Заметим, что размерность A над $\mathbb{C}$ меньше размерности A над $\mathbb{R}$. Следовательно, A — конечномерная алгебра с делением над полем $\mathbb{C}$. Тогда, согласно 2.75, $A = \mathbb{C}$. □

Пример 2.80. Пусть G — конечная группа и K — поле. Пусть

$$KG = \{\sum k_g g \mid g \in G, k_g \in K\}$$

— совокупность формальных линейных комбинаций элементов группы G с коэффициентами из поля K. Мы можем задать умножение на KG как

$$\left(\sum_{g\in G} k_g g\right)\left(\sum_{g'\in G} l_{g'} g'\right) = \left(\sum_{h\in G}\left(\sum_{g,g'\in G, gg'=h} k_g l_{g'}\right) h\right).$$

Таким образом мы получили ассоциативную алгебру с единицей. Эта алгебра называется *групповой алгеброй* группы G над полем K.

Определение 2.81. Пусть A — алгебра над полем K. *Дифференцированием* алгебры A называется отображение $d\colon A \to A$, удовлетворяющее условиям.

(1) $d(ax) = adx$, $\forall a \in K, x \in A$;
(2) $d(x + y) = dx + dy$, $\forall x, y \in A$;
(3) $d(xy) = (dx)y + x(dy)$, $\forall x, y \in A$.

Глава 3

2-й семестр

1. Расширение полей

Пусть E, k — два поля, причем $k \subset E$. Тогда поле E называется *расширением* поля k.

Определение 3.1. Расширение E поля k называется *конечным* (*бесконечным*), если E конечномерно (бесконечномерно), как линейное пространства над k. Другими словами, E конечно над k, если существуют $a_1, a_2, \ldots, a_n \in E$ такие, что $\forall x \in E$, $x = \alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n$, где $\alpha_1, \alpha_2 \ldots, \alpha_n \in k$. *Степенью* E над k мы будем называть размерность E как линейного пространства и обозначать $[E : k]$.

Теорема 3.2. *Пусть E — конечное расширение поля k, F — конечное расширение поля E. Тогда F — конечное расширение поля k и $[F : k] = [E : k][F : E]$.*

Доказательство. Пусть $x_1, x_2, \ldots, x_n$ — базис E над полем k, $y_1, y_2, \ldots, y_m$ — базис F над полем E. Тогда для любого элемента $a \in F$ существует разложение

$$a = \alpha_1 y_1 + \cdots + \alpha_m y_m,$$

где $\alpha_1, \ldots \alpha_m \in E$. Поскольку E — конечное расширение поля k, то

$$\alpha_i = \beta_{i1} x_1 + \cdots \beta_{in} x_n,$$

где $\beta_{ij} \in k$. Таким образом,

$$a = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} x_j y_i.$$

Следовательно, $\{x_j y_i\}$ порождают F над k. Таким образом, F — конечное расширение поля k. Осталось доказать равенство $[F : k] = [E : k][F : E]$. Для этого докажем линейную независимость $\{x_j y_i\}$. Предположим противное, т.е. существуют элементы

c_{ij} такие, что

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_j y_i = 0.$$

С другой стороны,

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_j y_i = \left(\sum_{j=1}^{n} c_{1j}x_j\right) y_1 + \left(\sum_{j=1}^{n} c_{2j}x_j\right) y_2 + \cdots + \left(\sum_{j=1}^{n} c_{mj}x_j\right) y_m.$$

Заметим, что $\sum\limits_{j=1}^{n} c_{ij}x_j \in E$. Поскольку $y_1, y_2, \ldots, y_m$ линейно независимы, то все $\sum\limits_{j=1}^{n} c_{ij}x_j = 0$. Поскольку $x_1, x_2, \ldots, x_n$ линейно независимы, то все $c_{ij} = 0$. □

Замечание 3.3. Если $k \subset E \subset F$ и F — конечное расширение поля k, то очевидно, что E — конечное расширение поля k, а F — конечное расширение поля E.

Определение 3.4. Элемент $x \in E$ называется *алгебраическим*, если он является корнем многочлена с коэффициентами из k, т.е. существуют $\alpha_0, \alpha_1 \ldots, \alpha_n \in k$ такие, что $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots \alpha_n x^n = 0$. Расширение E поля k называется *алгебраическим*, если любой элемент E является алгебраическим.

Теорема 3.5. *Любое конечное расширение является алгебраическим.*

Доказательство. Пусть E — конечное расширение поля k, и пусть $a \in E$. Если $a \in k$, то он алгебраичен. Предположим, что $a \notin k$. Рассмотрим $1, a, a^2 \cdots a^n \cdots$. Поскольку E — конечное расширение поля k, то существует n такое, что элементы $1, a, a^2 \cdots a^n$ линейно зависимы. Тогда существуют $\alpha_0, \alpha_1 \ldots, \alpha_n \in k$ такие, что $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots \alpha_n a^n = 0$. □

Пусть E — расширение поля k, и $a_1, a_2, \ldots, a_n \in E$ обозначим через $k(a_1, a_2, \ldots, a_n)$ наименьшее подполе поля E, содержащее $a_1, a_2, \ldots, a_n$. Очевидно оно состоит из элементов вида

$$\frac{f(a_1, a_2, \ldots, a_n)}{g(a_1, a_2, \ldots, a_n)},$$

где f, g — многочлены с коэффициентами из k и $g(a_1, a_2, \ldots, a_n) \neq 0$.

Теорема 3.6. *Пусть E — расширение поля k и $a \in E$ алгебраичен над k. Тогда $k(a)$ — конечное расширение поля k.*

Доказательство. Пусть $f(x)$ — многочлен с коэффициентами из k такой, что $f(a) = 0$. Предположим, что $f(x)$ приводим над k, т.е. $f(x) = f_1(x)f_2(x)$, где $f_1(x), f_2(x)$ — многочлены над k, степени меньше степени $f(x)$. Тогда либо $f_1(a) = 0$, либо $f_2(a) = 0$. Таким образом, последовательно заменяя $f(x)$ на многочлены меньшей степени, мы можем считать, что $f(x)$ неприводим. Рассмотрим $k[x]$ — множество многочленов от x с коэффициентами из k. Пусть $g(x) \in k[x]$ такой, что $g(a) \neq 0$. Тогда $g(x)$ взаимно прост с $f(x)$. Следовательно, существуют многочлены $p(x), q(x)$ такие, что $f(x)p(x) + g(x)q(x) = 1$. Подставляя a, получаем $g(a)q(a) = 1$. Таким образом, $k[a]$ не только кольцо, но и поле. Очевидно, что размерность $k[a]$ как векторного пространства над k не превышает степени многочлена $f(x)$. □

Замечание 3.7. Заметим, что многочлен $f(x)$ единственен с точностью до умножения на константу. Мы можем считать, что коэффициент при старшей степени у этого многочлена равен 1. Действительно, пусть существует другой неприводимый многочлен $f'(x)$ такой, что $f'(a) = 0$. Поскольку они оба неприводимы, то они взаимно просты. Тогда существуют многочлены $p(x), q(x)$ такие, что $f(x)p(x) + f'(x)q(x) = 1$. Подставляем a, получаем противоречие. Таким образом, мы можем считать, что старший коэффициент многочлена $f(x)$ равен 1. Такой многочлен мы будем называть *минимальным многочленом элемента* a над k, и обозначать $\mathrm{Irr}(a, k, x)$.

Следствие 3.8. *Пусть E — расширение поля k и $a_1, a_2, \ldots, a_n \in E$ алгебраичны над k. Тогда $k(a_1, a_2, \ldots, a_n)$ — конечное расширение поля k.*

Доказательство. Заметим, что

$$k \subset k(a_1) \subset k(a_1, a_2) \subset \cdots \subset k(a_1, a_2, \ldots, a_n).$$

Поскольку $k(a_1, a_2, \ldots, a_i, a_{i+1}) = k(a_1, a_2, \ldots, a_i)(a_{i+1})$, то согласно теореме 3.6 каждое вложение является конечным расширением. Теперь утверждение следует из теоремы 3.2. □

Теорема 3.9. *Пусть E — алгебраическое расширение поля k и F — алгебраическое расширение поля E. Тогда F — алгебраическое расширение поля k.*

Доказательство. Пусть $x \in F$. Тогда

$$a_0 + a_1 x + \cdots + a_n x^n = 0,$$

где $a_0, a_1, \ldots, a_n \in E$. Рассмотрим $E_0 = k(a_0, a_1, \ldots, a_n)$. Согласно следствию 3.8 E_0 — конечное расширение k. Рассмотрим $F_0 = E_0(x)$. Аналогично, F_0 — конечное расширение E_0. Следовательно, по теореме 3.2, F_0 — конечное расширение k. Заметим, что $x \in F_0$. С другой стороны, согласно теореме 3.5, F_0 — алгебраическое расширение поля k. Следовательно, x алгебраичен. □

Замечание 3.10. Если $k \subset E \subset F$ и F — алгебраическое расширение поля k, то очевидно, что E — алгебраическое расширение поля k, а F — алгебраическое расширение поля E.

Пусть $p(x)$ — неприводимый многочлен над полем k. Рассмотрим кольцо многочленов $k[x]$. Тогда многочлен $p(x)$ порождает главный идеал $(p(x))$. Поскольку $p(x)$ неприводим, то $(p(x))$ — максимальный идеал. Следовательно, $k[x]/(p(x))$ — поле. Пусть $\sigma\colon k[x] \to k[x]/(p(x))$ — естественный гомоморфизм. Заметим, что σ сюръективен на k. Тогда $\sigma(k)$ — подполе поля $k[x]/(p(x))$ изоморфное k. Мы можем отождествить его с k. Тогда $E = k[x]/(p(x))$ является расширением поля k. Рассмотрим $\xi = \sigma(x)$. Заметим, что ξ является корнем многочлена $p(x)$ в E. Таким образом, мы получили следующее утверждение.

Утверждение 3.11. *Для любого многочлена $p(x) \in k[x]$ существует расширение поля k в котором $p(x)$ имеет корень.*

Определение 3.12. Пусть k — поле. Предположим, что существует такое число p, что $p \cdot 1 = 0$, т.е.

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ слагаемых}} = 0.$$

Пусть p — минимальное из таких чисел. Тогда говорят, что p — *характеристика поля k*. Обозначается $char(k)$. Если не существует такого положительного числа p, то говорим, что поле имеет характеристику ноль.

Утверждение 3.13. *Характеристика поля либо ноль, либо простое число.*

Доказательство. Предположим, что характеристика поля $p = mn$. Тогда

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ слагаемых}} = \underbrace{(1 + 1 + \cdots + 1)}_{m \text{ слагаемых}} \cdot \underbrace{(1 + 1 + \cdots + 1)}_{n \text{ слагаемых}} = 0.$$

Отсюда, либо

$$\underbrace{1 + 1 + \cdots + 1}_{m \text{ слагаемых}} = 0,$$

либо

$$\underbrace{1+1+\cdots+1}_{n \text{ слагаемых}} = 0.$$

□

Рассмотрим поле k характеристики p.

Утверждение 3.14. *Пусть k — поле характеристики p. Тогда $(a+b)^p = a^p + b^p$.*

Доказательство. Следует из формулы Бинома–Ньютона и того, что C_p^i делится на p для любого $i \neq 0, p$. □

Определение 3.15. Поскольку $(a+b)^p = a^p + b^p$ и $(ab)^p = a^p b^p$, то отображение $f\colon k \to k^p$ заданное $f(x) = x^p$ является гомоморфизмом. Он называется *морфизмом Фробениуса.*

Определение 3.16. Поле k называется совершенным, если либо k характеристики ноль, либо k характеристики p и совпадает с k^p.

Теорема 3.17. *Пусть k — конечное поле. Тогда k совершенно.*

Доказательство. Заметим, что k^p — подполе в k и k^p изоморфно k. Следовательно, k^p и k имеют одинаковое количество элементов. Тогда они совпадают. □

2. Конечные поля

В этом параграфе мы рассмотрим конечные поля. Пусть k — поле из q элементов. Очевидно, что $char(k) = p > 0$. Следовательно, поле k содержит $\mathbb{Z}_p$ в качестве подполя. Тогда k является конечным расширением поля $\mathbb{Z}_p$, т.е. $[k : \mathbb{Z}_p] = n$. Таким образом, любой элемент $\alpha \in k$ имеет единственное представление в виде

$$\alpha = a_1 e_1 + a_2 e_2 + \cdots + a_n e_n,$$

где $e_1, e_2, \ldots, e_n$ — базис k как векторного пространства над $\mathbb{Z}_p$, $a_1, a_2, \ldots, a_n \in \mathbb{Z}_p$. Отсюда, число элементов в поле k равно p^n.

Теорема 3.18. *Пусть k^* — мультипликативная группа поля k, т.е. множество $k \setminus \{0\}$ с операцией умножение. Тогда k^* — циклическая группа порядка $p^n - 1$.*

Доказательство. Предположим, что k^* не является циклической группой. Тогда существует $r < p^n - 1$ такое, что $\alpha^r = 1$ для любого $\alpha \in k^*$. Таким образом, все элементы k^* являются корнями многочлена $x^r - 1 = 0$, но этот многочлен имеет не более r корней. Противоречие. □

Замечание 3.19. Фактически мы доказали, что любая конечная мультипликативная группа в поле циклическая.

Рассмотрим поле разложения многочлена $f(x) = x^{p^n} - x$ над полем $\mathbb{Z}_p$. Мы утверждаем, что это поле состоит из корней $f(x)$. Действительно, если α, β — корни $f(x)$, то

$$(\alpha+\beta)^{p^n} - (\alpha+\beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta = 0,$$
$$(\alpha\beta)^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0,$$
$$(\alpha^{-1})^{p^n} - \alpha^{-1} = (\alpha^{p^n})^{-1} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0,$$
$$(-\alpha)^{p^n} - (-\alpha) = -\alpha + \alpha = 0.$$

Заметим, что 0 и 1 — корни $f(x)$. Следовательно, поле разложение многочлена $f(x) = x^{p^n} - x$ состоит из его корней. С другой стороны, $f'(x) = -1$. Следовательно, все корни $f(x)$ различные. Таким образом, мы получили поле состоящее из p^n элементов.

3. Нетеровы кольца

Теорема 3.20. *Пусть A — кольцо и M — A-модуль. Тогда следующие условия эквивалентны:*

(1) *всякий подмодуль в M конечно порожден;*
(2) *всякая возрастающая последовательность подмодулей*

$$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$$

в M, такая, что $M_i \neq M_{i+1}$ для любого i, конечна;
(3) *всякое непустое множество подмодулей в M содержит максимальный элемент.*

Доказательство. (1) $\Rightarrow$ (2). Пусть $M_1 \subset M_2 \subset \cdots$ — возрастающая последовательность подмодулей. Положим $N = \bigcup\limits_{n=1}^{\infty} M_n$. Тогда N — подмодуль. По предположению, N конечно порожден. Следовательно, существуют элементы $x_1, x_2, \ldots x_m$, порождающие N. Тогда существует модуль M_j такой, что $x_1, x_2, \ldots x_m \in M_j$. Отсюда,

$$(x_1, x_2, \ldots x_m) \subset M_j \subset N = (x_1, x_2, \ldots x_m).$$

Следовательно, $M_j = N$. Тогда $M_p = N$ для любого $p > j$.

(2) $\Rightarrow$ (1). Пусть N — подмодуль в M. Пусть $a_1 \in N$. Если $(a_1) \neq N$, то существует $a_2 \in N$ такой, что $a_2 \notin (a_1)$. Если $(a_1, a_2) \neq N$, то существует $a_3 \in N$ такой, что $a_3 \notin (a_1, a_2)$ и т.д. Таким образом, мы получили возрастающую последовательность

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots .$$

Согласно предположению, эта последовательность конечна. Тогда $N = (a_1, a_2, \ldots, a_n)$.

(2) $\Rightarrow$ (3). Пусть $N_1 \in S$. Предположим, что N_1 не максимален. Тогда существует $N_2 \in S$ такой, что $N_1 \subset N_2$ и $N_1 \neq N_2$. Предположим, что N_2 не максимален. Тогда существует $N_3 \in S$ такой, что $N_2 \subset N_3$ и $N_2 \neq N_3$ и т.д. Таким образом, мы либо получим максимальный элемент, содержащий N_1, либо бесконечную возрастающую последовательность подмодулей, что невозможно по предположению.

(3) $\Rightarrow$ (2). Очевидно. $\square$

Теорема 3.21. *Пусть M — нетеров A-модуль. Тогда всякий подмодуль и всякий фактормодуль модуля M нетеровы.*

Доказательство. Пусть N — подмодуль M. Тогда любая возрастающая последовательность подмодулей в N является возрастающей последовательностью подмодулей в M. Отсюда, N — нетеров A-модуль. Докажем утверждение для фактормодулей. Пусть $f\colon M \to M/N$ — канонический гомоморфизм. Пусть $\bar{M}_1 \subset \bar{M}_2 \subset \cdots \subset \bar{M}_n \subset \cdots$ — возрастающая последовательность подмодулей в M/N. Положим $M_i = f^{-1}(\bar{M}_i)$. Тогда $M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots$ — возрастающая последовательность подмодулей в M, которая должна иметь максимальный элемент M_n, т.е. $M_i = M_n$ для любого $i > n$. Тогда $\bar{M}_n = f(M_n) = f(M_i) = \bar{M}_i$ для любого $i > n$. $\square$

Лемма 3.22. *Пусть M — A-модуль, N — его подмодуль. Пусть $K \subset L$ — два подмодуля M. Более того $K \cap N = L \cap N$ и $(K + N)/N = (L + N)/N$. Тогда $K = L$.*

Доказательство. Пусть $x \in L$. Поскольку $(K + N)/N = (L + N)/N$, то существуют элементы $u, v \in N$, $y \in K$ такие, что $y + u = x + v$. Отсюда,

$$x - y = u - v \in L \cap N = K \cap N.$$

Тогда $x = y + u - v \in K$. $\square$

Теорема 3.23. *Пусть M — A-модуль, N — его подмодуль. Предположим, что N и M/N нетеровы. Тогда M тоже нетеров.*

Доказательство. Пусть $M_1 \subset M_2 \subset \cdots$ — возрастающая последовательность подмодулей в M. Тогда $M_1 \cap N \subset M_2 \cap N \subset \cdots$ и $(M_1 + N)/N \subset (M_2 + N)/N \subset \cdots$ — возрастающие последовательности в N и M/N соответственно. Поскольку N и M/N — нетеровы

модули, то эти последовательности конечны, т.е. существует n такое, что $M_i \cap N = M_n \cap N$ и $(M_i + N)/N = (M_n + N)/N$ для любых $i > n$. Согласно лемме 3.22 $M_i = M_n$. □

Следствие 3.24. *Пусть M_1 и M_2 — нетеровы A-модули. Тогда $M_1 \oplus M_2$ тоже нетеров.*

Следствие 3.25. *Пусть M — A-модуль и $M = M_1 + M_2$. Предположим, что M_1 и M_2 нетеровы. Тогда M тоже нетеров.*

Доказательство. Согласно 3.24 $M_1 \oplus M_2$ — нетеров A-модуль. Заметим, что существует канонический гомоморфизм $f\colon M_1 \oplus M_2 \to M$. Тогда $M \cong (M_1 \oplus M_2)/\ker f$. Теперь наше утверждение следует из теоремы 3.21. □

Определение 3.26. Кольцо называется *нетеровым*, если оно нетерово как левый модуль над собой, т.е. любой левый идеал конечно порожден.

Утверждение 3.27. *Пусть A, B — нетеровы кольца. Тогда $A \times B$ — нетерово кольцо.*

Теорема 3.28. *Пусть A — нетерово кольцо и $f\colon A \to B$ — сюръективный гомоморфизм колец. Тогда B нетерово.*

Доказательство. Пусть $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \cdots$ — возрастающая цепочка левых идеалов в B. Положим $\mathfrak{a}_i = f^{-1}(\mathfrak{b}_i)$. Тогда $\mathfrak{a}_i$ образуют возрастающую цепочку левых идеалов в A, которая должна стабилизироваться, т.е. существует $\mathfrak{a}_n$ такой, что $\mathfrak{a}_i = \mathfrak{a}_n$ для любого $i > n$. Тогда $\mathfrak{b}_i = f(\mathfrak{a}_i) = f(\mathfrak{a}_n) = \mathfrak{b}_n$ для любого $i > n$. □

Теорема 3.29. *Пусть A — нетерово кольцо, M — конечно порожденный A-модуль. Тогда M нетеров.*

Доказательство. Пусть $x_1, x_2, \ldots, x_n$ — образующие M. Тогда существует гомоморфизм модулей

$$f\colon \underbrace{A \times A \times \cdots \times A}_{n} \to M$$

при котором

$$f(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

Этот гомоморфизм сюръективен. Согласно 3.21 и теореме о гомоморфизме для модулей M нетеров. □

Следствие 3.30. *Линейное пространство является нетеровым модулем тогда и только тогда, когда оно конечномерно.*

Теорема 3.31. *Пусть A — коммутативное нетерово кольцо, S — его мультипликативное подмножество. Тогда $S^{-1}A$ нетерово.*

Доказательство. Замети, что A можно считать подкольцом $S^{-1}A$. Пусть $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \cdots$ — возрастающая цепочка левых идеалов в $S^{-1}A$. Положим $\mathfrak{a}_i = \mathfrak{b}_i \cap A$. Тогда $\mathfrak{a}_i$ образуют возрастающую цепочку левых идеалов в A, которая должна стабилизироваться, т.е. существует $\mathfrak{a}_n$ такой, что $\mathfrak{a}_i = \mathfrak{a}_n$ для любого $i > n$. Предположим, что существует элемент $\frac{a}{s} \in \mathfrak{b}_i$ такой, что $\frac{a}{s} \notin \mathfrak{b}_n$, где $a \in A$, $s \in S$, $i > n$. Умножая на s, мы видим, что $a \in \mathfrak{b}_i$, а следовательно, $a \in \mathfrak{a}_i$. Отсюда, $a \in \mathfrak{a}_n$. Умножая на $\frac{1}{s}$, получаем $\frac{a}{s} \in \mathfrak{b}_n$. Противоречие. $\square$

Теорема 3.32 (теорема Гильберта о базисе). *Пусть A — коммутативное нетерово кольцо. Тогда кольцо многочленов $A[x]$ также нетерово.*

Доказательство. Пусть $\mathfrak{A}$ — идеал в $A[x]$. Обозначим через $\mathfrak{a}_n$ — множество элементов из A, являющимися коэффициентами при старшей степени в многочленах

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathfrak{A}.$$

Заметим, что $\mathfrak{a}_n$ — идеал кольца A. Поскольку умножая элемент $f \in \mathfrak{A}$ на x мы получаем многочлен степени на единицу больше, но с тем же коэффициентом при старшей степени, то имеем

$$\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \mathfrak{a}_n \subseteq \cdots .$$

Поскольку A нетерово, то эта последовательность стабилизируется, т.е. существует $\mathfrak{a}_r$ такой, что $\mathfrak{a}_i = \mathfrak{a}_r$ для любого $i > r$. Пусть $a_{i1}, a_{i2}, \ldots, a_{in_i}$ — образующие идеала $\mathfrak{a}_i$, и $f_{i1}, f_{i2}, \ldots, f_{in_i} \in \mathfrak{A}$ — многочлены степени i со старшими коэффициентами $a_{i1}, a_{i2}, \ldots, a_{in_i}$.

Докажем, что $\{f_{ij}\}$ — образующие идеала $\mathfrak{A}$. Пусть $f \in \mathfrak{A}$ — многочлен степени d. Предположим, что $d \geq r$. Поскольку $\mathfrak{a}_d = \mathfrak{a}_r$, то старшие коэффициенты многочленов $x^{d-r}f_{r1}, x^{d-r}f_{r2}, \ldots, x^{d-r}f_{rn_r}$ порождают $\mathfrak{a}_d$. Следовательно, существуют $c_1, c_2, \ldots, c_{n_r} \in A$ такие, что многочлен

$$f - c_1 x^{d-r} f_{r1} - c_2 x^{d-r} f_{r2} - \cdots - c_{n_r} x^{d-r} f_{rn_r}$$

имеет степень меньшую d, причем этот многочлен также лежит в $\mathfrak{A}$. Таким образом, мы можем считать, что $d < r$. Поскольку старший коэффициент лежит в $\mathfrak{a}_d$, то существуют $c_1, c_2, \ldots, c_{n_d}$ такие, что многочлен

$$f - c_1 f_{d1} - c_2 f_{d2} - \cdots - c_{n_d} f_{dn_d}$$

имеет степень меньшую d. Таким образом, f можно выразить, как линейную комбинацию $\{f_{ij}\}$. □

Следствие 3.33. *Пусть A — коммутативное нетерово кольцо. Тогда кольцо многочленов $A[x_1, x_2, \ldots, x_n]$ также нетерово.*

Следствие 3.34. *Пусть A — коммутативное нетерово кольцо, B — кольцо, содержащее A. Предположим, что B конечно порождено над A. Тогда B также нетерово.*

Доказательство. Пусть $y_1, y_2, \ldots y_n \in B$ — элементы, порождающие B над A. Рассмотрим кольцо многочленов $A[x_1, x_2, \ldots, x_n]$. Согласно 3.33 оно нетерово. Заметим, что существует сюръективный гомоморфизм $f\colon A[x_1, x_2, \ldots, x_n] \to B$ такой, что $f(x_i) = y_i$. Тогда, согласно 3.28, B также нетерово. □

Далее мы будем предполагать, что все кольца коммутативны.

Определение 3.35. Идеал $\mathfrak{a}$ называется *неприводимым*, если из $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$ следует, что либо $\mathfrak{a} = \mathfrak{a}_1$, либо $\mathfrak{a} = \mathfrak{a}_2$.

Теорема 3.36. *В нетеровом кольце любой идеал является пересечением конечного числа неприводимых идеалов.*

Доказательство. Предположим противное. Тогда множество идеалов, которые не являются пересечением неприводимых идеалов, содержит максимальный элемент $\mathfrak{a}$. Поскольку $\mathfrak{a}$ приводим, то $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$, где $\mathfrak{a} \subset \mathfrak{a}_1$ и $\mathfrak{a} \subset \mathfrak{a}_2$. Поскольку $\mathfrak{a}$ — максимальный идеал из тех, которые не являются пересечением неприводимых идеалов, то $\mathfrak{a}_1$ и $\mathfrak{a}_2$ можно представить в виде пересечения неприводимых идеалов. Следовательно, $\mathfrak{a}$ также можно представить в виде пересечения неприводимых идеалов. Противоречие. □

Определение 3.37. Идеал $\mathfrak{a}$ называется *примарным*, если из $xy \in \mathfrak{a}$ следует, что либо $x \in \mathfrak{a}$, либо $y^n \in \mathfrak{a}$ для некоторого n.

Теорема 3.38. *В нетеровом кольце любой неприводимый идеал примарен.*

Доказательство. Пусть $\mathfrak{a}$ — неприводимый идеал в кольце A. Рассматривая факторкольцо $A/\mathfrak{a}$, мы должны проверить, что если нулевой идеал неприводим, то он примарен. Пусть $xy = 0$. Рассмотрим

$$\mathrm{Ann}(x) = \{a \mid ax = 0\}.$$

Заметим, что $\mathrm{Ann}(x)$ является идеалом в кольце. Рассмотрим цепочку идеалов $\mathrm{Ann}(x) \subset \mathrm{Ann}(x^2) \subset \cdots$. Поскольку кольцо A нетерово, то эта цепочка стабилизируется, т.е. существует n такое, что

$\mathrm{Ann}(x^i) = \mathrm{Ann}(x^n)$ для любого $i > n$. Отсюда, $(x^n) \cap (y) = 0$. Действительно, пусть $a \in (x^n) \cap (y)$. Из $a \in (y)$ следует, что $ax = 0$. Поскольку $a \in (x^n)$, то $a = bx^n$. Тогда $0 = ax = bx^{n+1}$. Отсюда, $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$. Таким образом, $bx^n = 0$, т.е. $a = 0$. □

Из теорем 3.36 и 3.39 следует

Теорема 3.39. *В нетеровом кольце любой идеал можно представить в виде пересечения конечного числа примарных идеалов.*

4. Артиновы кольца

В этом параграфе мы будем предполагать, что все кольца коммутативные.

Элемент $a \in A$ называется *нильпотентным* (*нильпотентом*), если существует n такое, что $a^n = 0$.

Теорема 3.40. *Множество всех нильпотентных элементов является идеалом.*

Доказательство. Пусть R — множесво нильпотентных элементов в кольце A, $x, y \in R$, т.е. $x^n = 0$, $y^m = 0$. Тогда $(ax)^n = a^n x^n = a^n 0 = 0$, т.е. $ax \in R$. Проверим, что $x + y \in R$. Рассмотрим $(x + y)^{n+m}$. По формуле бинома, получаем

$$(x + y)^{n+m} = \sum_{i=0}^{n+m} C_{n+m}^i x^i y^{n+m-i}.$$

Заметим, что либо $i > n$, либо $m + n - i > m$. Таким образом, все слагаемые этой суммы обращаются в ноль. Следовательно, $(x + y)^{n+m} = 0$ и $x + y \in R$. □

Идеал R называется *нильрадикалом*.

Теорема 3.41. *Нильрадикал кольца A совпадает с пересечением всех простых идеалов в A.*

Доказательство. Пусть $\mathfrak{p}$ — простой идеал и x — нильпотент. Тогда $x^n = 0 \in \mathfrak{p}$. Следовательно, $x \in \mathfrak{p}$. Таким образом нильрадикал лежит в пересечение всех простых идеалов в A.

Обратно. Пусть a лежит в пересечение всех простых идеалов в A. Пусть $\mathfrak{m}$ — максимальный идеал такой, что $a^n \notin \mathfrak{m}$ для любого n. Докажем, что $\mathfrak{m}$ — простой идеал. Пусть $xy \in \mathfrak{m}$, но $x \notin \mathfrak{m}$ и $y \notin \mathfrak{m}$. Тогда идеалы $\mathfrak{m} + (x)$ и $\mathfrak{m} + (y)$ содержат $\mathfrak{m}$. В силу максимальности $\mathfrak{m}$ имеем $a^n \in \mathfrak{m} + (x)$ и $a^m \in \mathfrak{m} + (y)$. Отсюда, $a^{n+m} \in \mathfrak{m} + (xy) = \mathfrak{m}$. Противоречие. □

Определение 3.42. *Радикалом Джекобсона* кольца A называется пересечение всех его максимальных идеалов.

Из теоремы 3.41 следует

Утверждение 3.43. *Радикал Джекобсона содержит нильрадикал.*

Теорема 3.44. *Пусть R — радикал Джекобсона кольца A. Тогда $x \in R \Leftrightarrow 1 - xy$ является единицей в A для всех $y \in A$.*

Доказательство. Пусть $x \in R$. Предположим, что $1 - xy$ не является единицей. Тогда существует максимальный идеал $\mathfrak{m}$, содержащий $1 - xy$. Заметим, что $x \in \mathfrak{m}$. Отсюда, $1 \in \mathfrak{m}$. Противоречие.

Пусть $1 - xy$ является единицей для всех y. Предположим, что $x \notin \mathfrak{m}$ для некоторого максимального идеала $\mathfrak{m}$. Тогда $(x, \mathfrak{m}) = A$. Отсюда, $xy + m = 1$, где $y \in A$, $m \in \mathfrak{m}$. Следовательно, $1 - xy \in \mathfrak{m}$, т.е. $1 - xy$ не является единицей. Противоречие. □

Определение 3.45. Модуль M над кольцом A *артиновым*, если всякая последовательность его подмодулей $M_1 \supset M_2 \supset \cdots \subset M_n \subset \cdots$ стабилизируется, т.е. существует n такое, что $M_i = M_n$ для любого $i > n$. Кольцо A называется *артиновым*, если оно артиного как модуль над собой, или (равносильно) всякая последовательность идеалов

$$\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n \supset \cdots$$

стабилизируется.

Теорема 3.46. *Пусть M — артинов A-модуль. Тогда всякий подмодуль и всякий фактормодуль модуля M артиновы.*

Доказательство. Пусть N — подмодуль M. Тогда любая убывающая последовательность подмодулей в N является убывающей последовательностью подмодулей в M. Отсюда, N — артинов A-модуль. Докажем утверждение для фактормодулей. Пусть $f\colon M \to M/N$ — канонический гомоморфизм. Пусть $\bar{M}_1 \supset \bar{M}_2 \supset \cdots \supset \bar{M}_n \supset \cdots$ — убывающая последовательность подмодулей в M/N. Положим $M_i = f^{-1}(\bar{M}_i)$. Тогда $M_1 \supset M_2 \supset \cdots \supset M_n \supset \cdots$ — убывающая последовательность подмодулей в M, которая должна стабилизироваться, т.е. $M_i = M_n$ для любого $i > n$. Тогда $\bar{M}_n = f(M_n) = f(M_i) = \bar{M}_i$ для любого $i > n$. □

Теорема 3.47. *Пусть M — A-модуль, N — его подмодуль. Предположим, что N и M/N артиновы. Тогда M тоже артинов.*

Доказательство. Пусть $M_1 \supset M_2 \supset \cdots$ — убывающая последовательность подмодулей в M. Тогда $M_1 \cap N \subset M_2 \cap N \subset \cdots$ и $(M_1 + N)/N \subset (M_2 + N)/N \subset \cdots$ — убывающие последовательности в N и M/N соответственно. Поскольку N и M/N — артиновы модули, то эти последовательности конечны, т.е. существует n такое, что $M_i \cap N = M_n \cap N$ и $(M_i + N)/N = (M_n + N)/N$ для любых $i > n$. Согласно лемме 3.22 $M_i = M_n$. □

Следствие 3.48. *Пусть M_1 и M_2 — артиновы A-модули. Тогда $M_1 \oplus M_2$ тоже артинов.*

Следствие 3.49. *Пусть M — A-модуль и $M = M_1 + M_2$. Предположим, что M_1 и M_2 артиновы. Тогда M тоже артинов.*

Утверждение 3.50. *Пусть A, B — артиновы кольца. Тогда $A \times B$ — артиново кольцо.*

Теорема 3.51. *Пусть A — артиново кольцо и $f\colon A \to B$ — сюръективный гомоморфизм колец. Тогда B артиново.*

Доказательство. Пусть $\mathfrak{b}_1 \supset \mathfrak{b}_2 \supset \cdots$ — убывающая цепочка идеалов в B. Положим $\mathfrak{a}_i = f^{-1}(\mathfrak{b}_i)$. Тогда $\mathfrak{a}_i$ образуют убывающую цепочку идеалов в A, которая должна стабилизироваться, т.е. существует $\mathfrak{a}_n$ такой, что $\mathfrak{a}_i = \mathfrak{a}_n$ для любого $i > n$. Тогда $\mathfrak{b}_i = f(\mathfrak{a}_i) = f(\mathfrak{a}_n) = \mathfrak{b}_n$ для любого $i > n$. □

Теорема 3.52. *В артиновом кольце любой простой идеал максимален.*

Доказательство. Пусть $\mathfrak{p}$ — простой идеал в артиновом кольце A. Положим $B = A/\mathfrak{p}$. Заметим, что B — целостное артиного кольцо. Пусть $x \in B$. Поскольку B артиного, то существует n такое, что $(x^n) = (x^{n+1})$. Тогда $x^n = x^{n+1}y$, $y \in B$. Отсюда, $x^n(1 - xy) = 0$. Поскольку B — целостное кольцо, то $1 - xy = 0$. Отсюда, $xy = 1$, т.е. x обратим. Таким образом B — поле. Следовательно, $\mathfrak{p}$ — максимальный идеал (см. 2.17). □

Следствие 3.53. *В артиновом кольце нильрадикал совпадает с радикалом Джекобсона.*

Лемма 3.54. *Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ — идеалы кольца A, $\mathfrak{p}$ — простой идеал в A. Предположим, что $\bigcap_{i=1}^{n} \mathfrak{a}_i \subset \mathfrak{p}$. Тогда $\mathfrak{a}_i \subset \mathfrak{p}$ для некоторого i. Если $\bigcap_{i=1}^{n} \mathfrak{a}_i = \mathfrak{p}$, то $\mathfrak{a}_i = \mathfrak{p}$ для некоторого i.*

Доказательство. Предположим, что $\mathfrak{a}_i \not\subset \mathfrak{p}$ для всех i. Тогда существуют элементы $x_1, x_2, \ldots, x_n$ такие, что $x_i \in \mathfrak{a}_i$, $x_i \notin \mathfrak{p}$. Заметим, что

$$x_1 x_2 \cdots x_n \in \prod_{i=1}^{n} \mathfrak{a}_i \subset \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

С другой стороны, $x_1, x_2, \ldots, x_n \notin \mathfrak{p}$. Противоречие. Если $\bigcap\limits_{i=1}^{n} \mathfrak{a}_i = \mathfrak{p}$, то $\mathfrak{p} \subset \mathfrak{a}_i$ для всех i. Отсюда, $\mathfrak{a}_i = \mathfrak{p}$ для некоторого i. □

Теорема 3.55. *В артиновом кольце множество максимальных идеалов конечно.*

Доказательство. Пусть $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n, \ldots$ — последовательность максимальных идеалов в A. Рассмотрим последовательность

$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_k \supset \cdots .$$

Поскольку A — артиного, то $\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_{n+1}$ для некоторого n. Тогда $\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n \subset \mathfrak{m}_{n+1}$. Отсюда, $\mathfrak{m}_i \subset \mathfrak{m}_{n+1}$ для некоторого i. Поскольку $\mathfrak{m}_i$ максимален, то $\mathfrak{m}_i = \mathfrak{m}_{n+1}$. □

Утверждение 3.56. *Пусть V — векторное пространство над полем k. Тогда V — артинов модуль тогда и только тогда, когда V конечномерно.*

Доказательство. Пусть V — конечномерное пространство. Рассмотрим убывающую цепочку

$$V_1 \supset V_2 \supset \cdots \supseteq V_m \supset \cdots$$

подпространств в V. Заметим, что $\dim V_i \geq \dim V_{i+1}$. Более того, $V +_i \neq V_{i+1}$ тогда и только тогда, когда $\dim V_i > \dim V_{i+1}$.

Пусть V — бесконечномерное пространство. Тогда существует бесконечная последовательность $x_1, x_2, \ldots, x_n, \ldots$ линейно независимых элементов из V. Пусть $V_i = L(x_{i+1}, x_{i+2}, \ldots)$ — линейная оболочка натянутая на элементы $x_{i+1}, x_{i+2}, \ldots$, т.е. множество линейных комбинаций $a_1 x_{k_1} + a_2 x_{k_2} + \cdots + a_m x_{k_m}$, где $a_j \in k$, $k_j > i$. Тогда V_i — линейные подпространства в V. Мы получили убывающую цепочку подпространств

$$V_1 \supset V_2 \supset \cdots \supset V_n \supset \cdots ,$$

которая не стабилизируется. □

Теорема 3.57. *Пусть A — кольцо, в котором нулевой идеал является произведением (не обязательно различных) максимальных*

идеалов $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n$. *Тогда нетеровость* A *равносильно его артиновости.*

Доказательство. Рассмотрим цепочку идеалов

$$A \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n = 0.$$

Заметим, что фактор $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{i-1}/\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_i$ является векторным пространством над $A/\mathfrak{m}_i$. Тогда его артиновость равносильна его нетеровости. Тогда нетеровость A равносильно его артиновости. □

Лемма 3.58. *В артиновом кольце* A *нильрадикал* R *нильпотентен, т.е. существует* k *такое, что* $R^k = 0$.

Доказательство. Рассмотрим

$$R \supset R^2 \supset \cdots \supset R^n \supset R^{n+1} \supset \cdots.$$

Поскольку A — артиного кольцо, то существует k такое, что $R^k = R^i$ для любого $i > k$. Обозначим $\mathfrak{a} = R^k$. Рассмотрим множество идеалов $\mathfrak{b}$ таких, что $\mathfrak{b}\mathfrak{a} \neq 0$. Пусть $\mathfrak{b}_0$ — его минимальный элемент. Заметим, что существует элемент $x \in \mathfrak{b}_0$ такой, что $x\mathfrak{a} \neq 0$. Поскольку $(x) \subset \mathfrak{b}_0$, то $\mathfrak{b}_0 = (x)$. С другой стороны, $(x\mathfrak{a})\mathfrak{a} = x\mathfrak{a}^2 = x\mathfrak{a} \neq 0$ и $x\mathfrak{a} \subset (x)$. Отсюда, $x\mathfrak{a} = (x)$. Таким образом, существует $y \in \mathfrak{a}$ такой, что $x = xy$. Тогда $x = xy = xy^2 = \cdots = xy^n = \cdots$. Поскольку $y \in R^k \subset R$, то существует n такое, что $y^n = 0$. Следовательно, $x = 0$. Противоречие. □

Теорема 3.59. *Любое артиного кольцо является нетеровым.*

Доказательство. Пусть A — артиного кольцо. Пусть $\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_n$ — множество максимальных идеалов. Тогда нильрадикал $R = \bigcap \mathfrak{m}_i$ (см. 3.41, 3.52 и 3.55). Согласно лемме 3.58, существует k такое, что $R^k = 0$. Отсюда,

$$\prod_{i=1}^{n} \mathfrak{m}_i^k \subset \left(\bigcap_{i=1}^{n} \mathfrak{m}_i\right)^k = R^k = 0.$$

Согласно теореме 3.57, A — нетерого кольцо. □

5. Многочлены

Теорема 3.60. *Пусть* A *— целостное кольцо главных идеалов,* K *— его поле частных. Пусть* $\alpha \in K$. *Тогда существуют неприводимые элементы* $p_1, p_2, \ldots, p_n \in A$, *элементы* $a_1, a_2, \ldots, a_n \in A$ *и*

натуральные числа $j_1, j_2, \ldots, j_n$ *такие, что*

$$\alpha = \frac{a_1}{p_1^{j_1}} + \frac{a_2}{p_2^{j_2}} + \cdots + \frac{a_n}{p_n^{j_n}}.$$

Доказательство. Пусть $a, b \in A$ — взаимно простые ненулевые элементы. Тогда существуют $x, y \in A$ такие, что $ax + by = 1$. Отсюда,

$$\frac{1}{ab} = \frac{y}{a} + \frac{x}{b}.$$

Таким образом,

$$\frac{c}{ab} = \frac{yc}{a} + \frac{xc}{b}.$$

Далее требуемое представление получается по индукции. □

Замечание 3.61. Сокращая на наибольший общий делитель, мы можем считать, что a_i не делится на p_i.

Теорема 3.62. *Пусть* k *— поле,* $k(x)$ *— поле частных кольца многочленов* $k[x]$*. Пусть* $R(x) = \frac{P(x)}{Q(x)} \in k(x)$*. Тогда существует представление*

$$R(x) = f(x) + \frac{f_1(x)}{(p_1(x))^{j_1}} + \frac{f_2(x)}{(p_2(x))^{j_2}} + \cdots + \frac{f_n(x)}{(p_n(x))^{j_n}},$$

где $f(x), f_1(x), \ldots, f_n(x) \in k[x]$*,* $p_1(x), \ldots, p_n(x) \in k[x]$ *— неприводимые (не обязательно различные) многочлены. Более того* $\deg f_i(x) < \deg p_i(x)$*.*

Доказательство. Согласно теореме 3.60 существует представление

$$R(x) = \frac{f_1(x)}{(p_1(x))^{j_1}} + \frac{f_2(x)}{(p_2(x))^{j_2}} + \cdots + \frac{f_m(x)}{(p_n(x))^{j_m}},$$

где $p_i(x)$ — неприводимые над полем k многочлены. Предположим, что $\deg f_i(x) \geq \deg p_i(x)$. Тогда $f_i(x) = q(x)p_i(x) + r(x)$, $\deg r(x) < \deg p_i(x)$. Отсюда, $\frac{f_i(x)}{(p_i(x))^{j_i}} = \frac{q(x)}{(p_i(x))^{j_i-1}} + \frac{r(x)}{(p_i(x))^{j_i}}$, где $\deg q(x) < \deg f_i(x)$. □

Пусть A — факториальное кольцо, K — его поле частных. Пусть $\alpha \in K$. Тогда мы можем представить в виде несократимой дроби $\alpha = \frac{a}{b}$, где a, b — элементы A, не имеющие общих простых множителей. Пусть $p \in A$ — простой элемент. Тогда $\alpha = p^r\beta$, где $\beta \in K$, при этом p не делит ни числитель, ни знаменатель β (в его несократимом представлении), $r \in \mathbb{Z}$. Будем называть число $r \in \mathbb{Z}$ *порядком* p в α, и записывать $r = \operatorname{ord}_p \alpha$. Будем считать $\operatorname{ord}_p 0 = -\infty$.

Утверждение 3.63. *Пусть $\alpha, \beta \in K$, $p \in A$ — простой элемент. Тогда*

$$\operatorname{ord}_p(\alpha\beta) = \operatorname{ord}_p \alpha + \operatorname{ord}_p \beta,$$
$$\operatorname{ord}_p(\alpha + \beta) \geq \min(\operatorname{ord}_p \alpha, \operatorname{ord}_p \beta).$$

Доказательство. Пусть $\alpha = p^r \frac{a}{b}$, $\beta = p^s \frac{c}{d}$, при этом a, b, c, d не делятся на p. Тогда $\alpha\beta = p^{r+s} \frac{ac}{bd}$. Поскольку ac и bd не делятся на p, то

$$\operatorname{ord}_p(\alpha\beta) = \operatorname{ord}_p \alpha + \operatorname{ord}_p \beta.$$

Предположим, что $r \geq s$. Тогда

$$\alpha + \beta = p^r \frac{a}{b} + p^s \frac{c}{d} = p^s \left(\frac{p^{r-s} a}{b} + \frac{c}{d} \right) = p^s \frac{p^{r-s} ad + bc}{bd}.$$

Поскольку bd не делится на p и $r - s > 0$, то

$$\operatorname{ord}_p(\alpha + \beta) \geq \min(\operatorname{ord}_p \alpha, \operatorname{ord}_p \beta).$$

□

Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in K[x].$$

Положим $\operatorname{ord}_p f = \min \operatorname{ord}_p a_i$. *Содержанием* многочлена $f(x)$ называется выражение

$$\operatorname{cont}(f) = u \prod_{p:\ \operatorname{ord}_p f \neq 0} p^{\operatorname{ord}_p f},$$

где u — любая единица кольца A. По определению $\operatorname{cont}(0) = -\infty$. Заметим, что содержание определено с точностью до умножения на единицу. Пусть $b \in K$. Тогда $\operatorname{cont}(bf) = b \operatorname{cont}(f)$. Таким образом, $f(x) = c f_1(x)$, где $c = \operatorname{cont}(f)$ и $\operatorname{cont}(f_1) = 1$.

Утверждение 3.64. *Пусть* $\operatorname{cont}(f) = 1$. *Тогда все коэффициенты $f(x)$ принадлежат A.*

Доказательство. Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in K[x].$$

Пусть c — наименьшее общее кратное знаменателей a_i. Тогда ca_i не имеют общих делителей. С другой стороны, $cf(x) \in A[x]$ и $c = c \operatorname{cont}(f) = \operatorname{cont}(cf)$. Противоречие. □

Теорема 3.65 (лемма Гаусса). *Пусть A — факториальное кольцо, K — его поле частных. Пусть $f(x), g(x) \in K[x]$. Тогда* $\operatorname{cont}(fg) = \operatorname{cont}(f) \operatorname{cont}(g)$.

Доказательство. Пусть $f(x) = cf_1(x)$, $g(x) = dg_1(x)$, где $c = \mathrm{cont}(f)$, $d = \mathrm{cont}(g)$ и $\mathrm{cont}(f_1) = \mathrm{cont}(g_1) = 1$. Тогда

$$\mathrm{cont}(fg) = \mathrm{cont}(cdf_1g_1) = cd\,\mathrm{cont}(f_1g_1).$$

Таким образом, достаточно доказать, что если $\mathrm{cont}(f) = \mathrm{cont}(g) = 1$, то $\mathrm{cont}(fg) = 1$. Более того, согласно 3.64, $f(x), g(x) \in A[x]$. Пусть

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$
$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0.$$

Предположим, что $\mathrm{cont}(fg)$ делится на простой элемент $p \in A$. Пусть r — минимальное число такое, что a_r не делит p, s — минимальное число такое, что b_s не делит p. Положим

$$h(x) = f(x)g(x) = c_{n+m}x^{n+m} + \cdots + c_1x + c_0.$$

Тогда

$$c_{r+s} = a_rb_s + \sum a_ib_{r+s-i}.$$

Заметим, что a_rb_s не делится на p, но любое a_ib_{r+s-i} делится на p. Отсюда, c_{r+s} не делится на p. Таким образом, $\mathrm{cont}(fg)$ не делится на p. Противоречие. □

Следствие 3.66. *Пусть $f(x) \in A[x]$ и существует разложение $f(x) = g(x)h(x)$ в $K[x]$, т.е. $g(x), h(x) \in K[x]$. Тогда существует разложение $f(x) = \hat{g}(x)\hat{h}(x)$ в $A[x]$, т.е. $\hat{g}(x), \hat{h}(x) \in A[x]$.*

Доказательство. Пусть $f(x) = g(x)h(x)$, где $g(x), h(x) \in K[x]$. Положим $c_1 = \mathrm{cont}(g)$, $c_2 = \mathrm{cont}(h)$. Тогда $c_1c_2 = \mathrm{cont}(f) \in A$. С другой стороны, $g(x) = c_1g_1(x)$, $h(x) = c_2h_1(x)$, где $\mathrm{cont}(g_1) = \mathrm{cont}(h_1) = 1$. Тогда $g_1(x), h_1(x) \in A[x]$ (см. 3.64). Пусть $\hat{g}(x) = c_1c_2g_1(x) \in A[x]$, $\hat{h}(x) = h_1(x) \in A[x]$. Тогда $f(x) = \hat{g}(x)\hat{h}(x)$. □

Теорема 3.67. *Пусть A — факториальное кольцо, K — его поле частных. Тогда $A[x]$ тоже факториально, его простыми элементами являются простые элементы из A и многочлены, неприводимые над $K[x]$ и имеющие содержание* 1.

Доказательство. Пусть $f(x) \in A[x]$. Поскольку $K[x]$ факториально, то

$$f(x) = p_1(x)p_2(x)\cdots p_n(x),$$

где $p_i(x)$ — неприводимые в $K[x]$ многочлены. Заметим, что $p_i(x) = c_i\hat{p}_i(x)$, где $c_i = \mathrm{cont}(p_i)$ и $\mathrm{cont}(\hat{p}_i) = 1$. Отсюда,

$$f(x) = c\hat{p}_1(x)\hat{p}_2(x)\cdots\hat{p}_n(x),$$

где $c = c_1 c_2 \cdots c_n = \mathrm{cont}(f) \in A$. Поскольку $\mathrm{cont}(\hat{p}_i) = 1$, то $\hat{p}_i(x) \in A[x]$. Очевидно, что $\hat{p}_i(x)$ неприводимы в $A[x]$. Поскольку A факториально, то существует разложение c на простые множители. Таким образом, осталось доказать единственность разложения. Пусть существует другое разложение

$$f(x) = dq_1(x)q_2(x)\cdots q_m(x).$$

В силу однозначности разложения на множители в $K[x]$ получаем $n = m$ и $p_1(x) = a_i q_i(x)$, где $a_i \in K$. Поскольку $p_1(x)$ и $q_i(x)$ имеют содержание 1, то a_i является единицей в A. □

Следствие 3.68. *Пусть A — факториальное кольцо. Тогда $A[x_1, x_2, \ldots, x_n]$ тоже факториально.*

Теорема 3.69. *Пусть A — факториальное кольцо, K — его поле частных,*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in A[x].$$

Пусть p — простой элемент в A. Предположим, что

$$a_n \not\equiv 0(\mod p), \quad a_i \equiv 0(\mod p), \forall i < n, \quad a_0 \not\equiv 0(\mod p^2).$$

Тогда $f(x)$ неприводим в $K[x]$.

Доказательство. Заметим, что мы можем считать $\mathrm{cont}(f) = 1$. Если $f(x)$ разлагается в $K[x]$, то $f(x)$ разлагается в $A[x]$ (см. 3.66). Пусть $f(x) = g(x)h(x)$, где $g, h \in A[x]$. Положим

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

$$h(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0.$$

Заметим, что $m + k = n$ и $b_m c_k \neq 0$. Пусть σ — канонический гомоморфизм A в $A/(p)$. Заметим, что σ индуцирует гомоморфизм $A[x]$ в $A/(p)[x]$. Тогда $\sigma(f(x)) = \sigma(a_n)x^n$. Докажем, что $\sigma(g(x)) = \sigma(b_m)x^m$, $\sigma(h(x)) = \sigma(c_k)x^k$. Предположим, что

$$\sigma(g(x)) = \sigma(b_m)x^m + \sigma(b_{m-1})x^{m-1} + \cdots + \sigma(b_r)x^r,$$

$$\sigma(h(x)) = \sigma(c_k)x^k + \sigma(c_{k-1})x^{k-1} + \cdots + \sigma(c_s)x^s,$$

где $\sigma(b_r) \neq 0$, $\sigma(c_s) \neq 0$ в $A/(p)[x]$. Тогда

$$\sigma(a_n)x^n = \sigma(f(x)) = \sigma(g(x)h(x)) = \sigma(g(x))\sigma(h(x)) =$$

$$= \sigma(b_m)\sigma(c_k)x^n + \cdots + \sigma(b_r)\sigma(c_s)x^{r+s}.$$

Поскольку p — простой элемент, то (p) — простой идеал. Тогда $\sigma(b_r)\sigma(c_s) \neq 0$. Противоречие. Таким образом, $\sigma(g(x)) = \sigma(b_m)x^m$,

$\sigma(h(x)) = \sigma(c_k)x^k$. Тогда $b_0 \equiv 0(\mod p)$ и $c_0 \equiv 0(\mod p)$. Следовательно, $a_0 = b_0c_0 \equiv 0(\mod p^2)$. Противоречие. □

Теорема 3.70. *Пусть A и B — целостные кольца, $\sigma\colon A \to B$ — гомоморфизм, K и L — поля частных для A и B соответственно. Пусть $f(x) \in A[x]$ и $\deg f(x) = \deg \sigma(f(x))$. Предположим, что $\sigma(f(x))$ неприводим в $L[x]$. Тогда $f(x)$ не обладает разложением $f(x) = g(x)h(x)$ в котором $g(x), h(x) \in A[x]$ и $\deg g(x) \geq 1$, $\deg h(x) \geq 1$.*

Доказательство. Предположим, что $f(x)$ имеет такое разложение, т.е. $f(x) = g(x)h(x)$, где $g(x), h(x) \in A[x]$. Поскольку A — целостное, то $\deg f = \deg g + \deg h$. Тогда $\sigma(f(x)) = \sigma(g(x))\sigma(h(x))$. Заметим, что $\deg \sigma(g(x)) \leq \deg g(x)$, $\deg \sigma(h(x)) \leq \deg h(x)$. Поскольку $\deg f(x) = \deg \sigma(f(x))$ и B целостное, то $\deg \sigma(g(x)) = \deg g(x)$, $\deg \sigma(h(x)) = \deg h(x)$. Поскольку $\sigma(f(x))$ неприводим в $L[x]$, то либо $g(x)$, либо $h(x)$ есть элемент из A. □

6. Симметрические многочлены

Определение 3.71. Пусть A — целостное кольцо и $f(x_1, x_2, \ldots, x_n) \in A[x_1, x_2, \ldots, x_n]$. Будем говорить, что $f(x_1, x_2, \ldots, x_n)$ *симметрический многочлен*, если для любой перестановки $\sigma \in S_n$ выполнено

$$f(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Элементарными симметрическими многочленами будем называть многочлены

$$s_k(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k},$$

где $k = 1, 2, \ldots, n$.

Замечание 3.72. Заметим, что элементарные симметрические многочлены можно определить следующим образом. Рассмотрим $A[x_1, x_2, \ldots, x_n][y]$. Пусть

$$f(y) = (y - x_1)(y - x_2) \cdots (y - x_n) \in A[x_1, x_2, \ldots, x_n][y].$$

Тогда

$$f(y) = y^n - s_1 y^{n-1} + s_2 y^{n-2} - s_3 y^{n-3} + \cdots + (-1)^n s_n.$$

Замечание 3.73. Если мы подставим $x_n = 0$ в $s_1, s_2, \ldots, s_{n-1}, s_n$, то мы получим $(s_1)_0, (s_2)_0, \ldots, (s_{n-1})_0$ — элементарные симметрические многочлены от $x_1, x_2, \ldots, x_{n-1}$.

Определение 3.74. Пусть $x_1, x_2, \ldots, x_n$ — переменные. Будем называть *весом* одночлена $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ число $k_1 + 2k_2 + \cdots + nk_n$. *Весом* многочлена $f(x_1, x_2, \ldots, x_n)$ будем называть максимум весов одночленов, встречающихся в $f(x_1, x_2, \ldots, x_n)$.

Теорема 3.75. *Пусть $f(x_1, x_2, \ldots, x_n) \in A[x_1, x_2, \ldots, x_n]$ — симметрический многочлен степени d. Тогда существует многочлен $g(y_1, y_2, \ldots, y_n)$ веса, не превышающего d, такой, что*

$$f(x_1, x_2, \ldots, x_n) = g(s_1, s_2, \ldots, s_n).$$

Доказательство. Докажем индукцией по n. Если $n = 1$ (т.е. $f(x) \in A[x]$), то утверждение очевидно. Предположим мы доказали для любого $m < n$. Проведем теперь индукцию по d. Если $d = 0$, то наше утверждение очевидно. Предположим утверждение доказано для многочленов степени меньше d. Пусть $f(x_1, x_2, \ldots, x_n)$ имеет степень d. Подставим $x_n = 0$. По индуктивному предположению существует многочлен $g_1(y_1, y_2, \ldots, y_{n-1})$ такой, что

$$f(x_1, x_2, \ldots, x_{n-1}, 0) = g_1((s_1)_0, (s_2)_0, \ldots, (s_{n-1})_0).$$

Тогда многочлен

$$f_1(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n) - g_1(s_1, s_2, \ldots, s_{n-1})$$

имеет степень $\leq d$ и является симметрическим. Более того, $f_1(x_1, x_2, \ldots, x_{n-1}, 0) = 0$. Следовательно, $f_1(x_1, x_2, \ldots, x_n)$ делится на x_n. Поскольку $f_1(x_1, x_2, \ldots, x_n)$ симметрический, то $f_1(x_1, x_2, \ldots, x_n)$ делится на $x_1 x_2 \cdots x_n$. Таким образом, $f_1(x_1, x_2, \ldots, x_n) = s_n f_2(x_1, x_2, \ldots, x_n)$, где $f_2(x_1, x_2, \ldots, x_n)$ — симметрический многочлен, степени $\leq d - n$. По индуктивному предположению существует многочлен g_2 такой, что $f_2(x_1, x_2, \ldots, x_n) = g_2(s_1, s_2, \ldots, s_n)$. Отсюда,

$$f(x_1, x_2, \ldots, x_n) = g_1(s_1, s_2, \ldots, s_{n-1}) + s_n g_2(s_1, s_2, \ldots, s_n).$$

Заметим, что каждый член справа имеет вес $\leq d$. □

Пример 3.76. Пусть

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \in \mathbb{C}[x]$$

— многочлен над полем $\mathbb{C}$. Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — его корни (необязательно различные). Тогда

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Отсюда,

$$a_1 = -s_1(\alpha_1, \alpha_2, \ldots, \alpha_n), \quad a_2 = s_2(\alpha_1, \alpha_2, \ldots, \alpha_n), \ldots,$$

$$a_n = (-1)^n s_n(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Рассмотрим симметрический многочлен

$$D(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)^2.$$

Выражение $D(\alpha_1, \alpha_2, \ldots, \alpha_n)$ называется *дискриминантом* многочлена $f(x)$. Заметим, что многочлен $f(x)$ имеет кратные корни тогда и только тогда, когда $D(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$. Поскольку $D(x_1, x_2, \ldots, x_n)$ — симметрический многочлен, то существует многочлен $g(y_1, y_2, \ldots, y_n)$ такой, что

$$D(\alpha_1, \alpha_2, \ldots, \alpha_n) = g(a_1, a_2, \ldots, a_n).$$

Таким образом, мы можем определять наличие кратных корней не находя их.

7. Теорема Штурма

Определение 3.77. Пусть $f(x)$ — многочлен с вещественными коэффициентами. Конечная упорядоченная система многочленов

$$f(x) = f_0(x), f_1(x), \ldots, f_n(x)$$

с вещественными коэффициентами называется *системой Штурма* многочлена $f(x)$ на отрезке $[a; b]$, если

(1) $f_n(x)$ не имеет корней на $[a; b]$;
(2) $f(a) \neq 0$, $f(b) \neq 0$;
(3) если $f_k(c) = 0$, то $f_{k-1}(c) f_{k+1}(c) < 0$;
(4) если $f(c) = 0$, то $f_0(x) f_1(x)$ меняет знак с минуса на плюс при переходе через точку c, т.е. существует $\delta > 0$ такое, что $f_0(x) f_1(x) < 0$ при $x \in [c - \delta; c]$ и $f_0(x) f_1(x) > 0$ при $x \in [c; c + \delta]$.

Пусть $V_c = V_c(f_0, f_1, \ldots, f_n)$ — число перемен знаков в последовательности $f_0(c), f_1(c), \ldots, f_n(c)$ (если эта последовательность содержит нули, то их просто вычеркиваем).

Теорема 3.78 (теорема Штурма). *Пусть $f(x) \in \mathbb{R}[x]$ и $f(x) = f_0(x), f_1(x), \ldots, f_n(x)$ — последовательность Штурма для $f(x)$. Тогда число вещественных корней многочлена $f(x)$ на отрезке $[a; b]$ равно $V_a - V_b$.*

Доказательство. Совокупность корней многочленов $f_0(x), f_1(x), \ldots, f_n(x)$ на отрезке $[a; b]$ задает разбиение

$$a = t_0 < t_1 < \cdots < t_m = b.$$

Заметим, что на интервале $(t_{i-1}; t_i)$ многочлены $f_j(x)$ не имеют корней. Следовательно, $V_{x_1} = V_{x_2}$ для любых $x_1, x_2 \in (t_{i-1}; t_i)$. Из (3) следует, что соседние многочлены не имеют общих корней на $[a; b]$. Тогда $V_a = V_c$ для любого $c \in (t_0; t_1)$. Рассмотрим точку t_1. Предположим, что $f(t_1) \neq 0$. Пусть $f_j(t_1) = 0$. Тогда из (3) $f_{j-1}(t_1) \neq 0$ и $f_{j+1}(t_1) \neq 0$. Имеют место следующие случае

(1) $f_{j-1}(x) > 0$, $f_{j+1}(x) < 0$ в окрестности t_1, и $f_j(x)$ меняет знак с плюса на минус;
(2) $f_{j-1}(x) > 0$, $f_{j+1}(x) < 0$ в окрестности t_1, и $f_j(x)$ меняет знак с минуса на плюс;
(3) $f_{j-1}(x) > 0$, $f_{j+1}(x) < 0$ в окрестности t_1, и $f_j(x)$ не меняет знак;
(4) $f_{j-1}(x) < 0$, $f_{j+1}(x) > 0$ в окрестности t_1, и $f_j(x)$ меняет знак с плюса на минус;
(5) $f_{j-1}(x) < 0$, $f_{j+1}(x) > 0$ в окрестности t_1, и $f_j(x)$ меняет знак с минуса на плюс;
(6) $f_{j-1}(x) < 0$, $f_{j+1}(x) > 0$ в окрестности t_1, и $f_j(x)$ не меняет знак.

Во всех случаях число перемен знака в последовательности $f_{j-1}(x), f_j(x), f_{j+1}(x)$ не меняется. Таким образом, $V_a = V_c$ для любого $c \in (t_1; t_2)$. Предположим, что $f(t_1) = 0$. Поскольку $f_0(x)f_1(x)$ меняет знак с минуса на плюс при переходе через точку t_1, то $V_a = V_c + 1$ для любого $c \in (t_1; t_2)$. Последовательно рассматривая точки t_i получаем необходимое утверждение. □

Пусть $f(x) \in \mathbb{R}[x]$. Положим $f_1(x) = f'(x)$ и применим алгоритм Евклида. Получаем

$$f(x) = q_1(x)f_1(x) - f_2(x),$$

$$f_1(x) = q_2(x)f_2(x) - f_3(x),$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$f_{n-2}(x) = q_{n-1}(x)f_{n-1}(x) - f_n(x),$$

$$f_{n-1}(x) = q_n(x)f_n(x).$$

Теорема 3.79. *Предположим, что $f(x)$ не имеет кратных корней на $[a; b]$ и $f(a) \neq 0$, $f(b) \neq 0$. Тогда только что полученная последовательность является системой Штурма.*

Доказательство. Поскольку $f_n(x)$ — наибольший общий делитель $f(x)$ и $f'(x)$ и $f(x)$ не имеет кратных корней на $[a; b]$, то

$f_n(x)$ не имеет корней на $[a;b]$. Второе свойство выполнено по предположению. Если $f_k(c) = 0$, то $f_{k-1}(c) = -f_{k+1}(c)$. Следовательно, $f_{k-1}(c)f_{k+1}(c) \leq 0$. Предположим, что $f_{k+1}(c) = 0$. Поскольку $f_k(c) = q_{k+1}(c)f_{k+1}(c) + f_{k+2}(c)$, то $f_{k+2}(c) = 0$. Следовательно, $f_n(c) = 0$. Противоречие. Таким образом, $f_{k-1}(c)f_{k+1}(c) < 0$, т.е. выполнено свойство (3). Пусть $f(c) = 0$ для некоторой точки $c \in [a;b]$. Тогда $f(x) = (x-c)g(x)$, где $g(c) \neq 0$. Заметим, что $f'(x) = g(x) + (x-c)g'(x)$. Тогда $f(x)f'(x) = (x-c)h(x)$, где

$$h(x) = g^2(x) + (x-c)g(x)g'(x).$$

Заметим, что $h(c) = g^2(c) > 0$. Следовательно, $h(x)$ принимает положительные значения в достаточно малой окрестности c. Поскольку $x - c$ меняет знак с минуса на плюс при переходе через точку c, то $f(x)f'(x) = (x-c)h(x)$ также меняет знак с минуса на плюс при переходе через точку c. Таким образом, выполнено свойство (4). □

8. Результант

Пусть

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

— два многочлена с коэффициентами в поле k. *Результантом* многочленов $f(x)$ и $g(x)$ называется

$$\operatorname{Res}(f,g) = \begin{vmatrix} a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_n & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 \end{vmatrix} \quad (1).$$

Теорема 3.80. *Результант* $\operatorname{Res}(f,g) = 0$ *тогда и только тогда, когда* f *и* g *имеет общий множитель в* $k[x]$ *степени* > 0.

Доказательство. Пусть h — наибольший общий делитель f и g. Предположим, что $\deg h > 0$. Тогда существует расширение E поля k такое, что $h(x)$ имеет корень в E. Обозначим этот корень ξ. Пусть $C_1, C_2, \ldots, C_{n+m}$ — столбцы матрицы (1). Рассмотрим

$$C_1\xi^{n+m-1} + C_2\xi^{n+m-2} + \cdots + C_{n+m-1}\xi + C_{n+m} = C.$$

Тогда

$$C = \begin{pmatrix} \xi^{m-1}f(\xi) \\ \xi^{m-2}f(\xi) \\ \cdots \\ f(\xi) \\ \xi^{n-1}g(\xi) \\ \xi^{n-2}g(\xi) \\ \cdots \\ g(\xi) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ \cdots \\ \cdots \\ 0 \end{pmatrix}.$$

Отсюда, $\mathrm{Res}(f,g) = 0$.

Обратно. Пусть $\mathrm{Res}(f,g) = 0$. Положим $D_1, D_2, \ldots, D_{n+m}$ — строки матрицы (1). Тогда существуют ненулевые $\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n$ такие, что

$$\alpha_1 D_1 + \alpha_2 D_2 + \cdots + \alpha_m D_m + \beta_1 D_{m+1} + \cdots + \beta_n D_{m+n} = (0, 0, \ldots, 0). \quad (2)$$

Рассмотрим многочлены

$$f_1(x) = \beta_1 x^{n-1} + \beta_2 x^{n-2} + \cdots + \beta_{n-1}x + \beta_n,$$

$$g_1(x) = \alpha_1 x^{m-1} + \alpha_2 x^{m-2} + \cdots + \alpha_{m-1}x + \alpha_m.$$

Из (2) следует

$$fg_1 + gf_1 = 0.$$

Предположим, что f и g не имеют общих делителей степени > 0. Поскольку $k[x]$ факториально, то существует разложение на простые множители $f(x) = p_1(x) \cdots p_k(x)$. Заметим, что $g(x)$ не делится ни на один $p_i(x)$. Тогда $f_1(x)$ делится на все $p_i(x)$. Следовательно, $f_1(x)$ делится на $f(x)$, но $\deg f_1(x) < \deg f(x)$. Противоречие. $\square$

9. Алгоритм Кронекера

Пусть $f(x) \in \mathbb{Z}[x]$. Нужно найти $f_1(x) \in \mathbb{Z}[x]$ такой, что $f(x)$ делится на $f_1(x)$ или доказать, что таких нет. Алгоритм Кронекера основан на следующих соображениях:

(1) если степень многочлена $f(x)$ равна n, то степень хотя бы одного множителя $f_1(x)$ многочлена $f(x)$ не превосходит $[\frac{n}{2}]$;
(2) значения многочленов $f(x)$ и $f_1(x)$ в целых точках — целые числа;
(3) пусть $k \in \mathbb{Z}$ и $f(k) \neq 0$ тогда $f_1(x)$ может принимать только конечное число значений, состоящее из делителей числа $f(k)$;

(4) многочлен $f_1(x)$ однозначно восстанавливается по его значению в $[\frac{n}{2}]+1$ точке.

Таким образом, мы можем выбрать любые целые $[\frac{n}{2}]+1$ точки, например, $0, 1, 2, \ldots, [\frac{n}{2}]$. Посчитать значение в них. Если существует k такое, что $f(k) = 0$, то $f(x)$ делится на $x - k$. Если таких точек нет, то мы можем рассмотреть все возможные наборы делителей $f(0), f(1), \ldots, f([\frac{n}{2}])$. Для каждого набора существует многочлен $f_1(x)$. Далее проверяем делится ли $f(x)$ на $f_1(x)$.

Пусть $f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$. Для того, чтобы разложить $f(x_1, x_2, \ldots, x_n)$ в $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ выберем достаточно большое d (например большее степени $f(x_1, x_2, \ldots, x_n)$). Рассмотри $g(y) = f(y, y^d, y^{d^2}, \ldots, y^{d^{n-1}})$. Разложим его на множители $g(y) = g_1(y)g_2(y)\cdots g_m(y)$. Рассмотрим всевозможные наборы $\{i_1, \ldots, i_k\} \subset \{1, 2, \ldots, m\}$. Для каждого набора определим

$$g_{i_1,\ldots,i_k}(y) = g_{i_1}(y)g_{i_2}(y)\cdots g_{i_k}(y).$$

Найдем $f_{i_1,\ldots,i_k}(x_1, x_2, \ldots, x_n) = S^{-1}(g_{i_1,\ldots,i_k}(y))$, где S^{-1} определяется на одночленах по формуле

$$S^{-1}(y^{a_1+a_2d+a_3d^2+\cdots+a_nd^{n-1}}) = x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}.$$

Проверяем делится ли $f(x_1, x_2, \ldots, x_n)$ на $f_{i_1,\ldots,i_k}(x_1, x_2, \ldots, x_n)$.

10. Алгоритм Берлекэмпа

Пусть F_q — поле из $q = p^n$ элементов. Пусть $f(x) \in F_q[x]$ — многочлен со старшим коэффициентом 1. Рассмотрим алгоритм разложения $f(x) \in F_q[x]$ на неприводимые множители. Пусть

$$f(x) = (p_1(x))^{k_1}(p_2(x))^{k_2}\cdots(p_m(x))^{k_m}$$

— разложение $f(x)$ на различные неприводимые множители со старшим коэффициентом 1. Сначала избавимся от кратностей. Рассмотрим производную $f'(x)$. Если $f'(x) = 0$, то $f(x) = g(x^p)$. Отсюда, $f(x) = (g(x))^p$. Таким образом, мы можем считать, что $f'(x) \neq 0$. Тогда вычислим $h(x) = \text{НОД}\,(f(x), f'(x))$. Очевидно, что

$$h(x) = (p_1(x))^{j_1}(p_2(x))^{j_2}\cdots(p_m(x))^{j_m},$$

где $j_i = k_i - 1$, если k_i не делится на p, и $j_i = k_i$, если k_i делится на p. Рассмотрим $\tilde{f}(x) = \frac{f(x)}{h(x)}$. Заметим, у $\tilde{f}(x)$ нет кратных неприводимых множителей. Если мы найдем разложение $\tilde{f}(x)$, то, последовательно поделив на неприводимые множители $f(x)$, мы найдем все множители $p_i(x)$, у которых k_i не делится на p. Пусть

$f_1(x) = \prod\limits_{k_i : p \nmid k_i} (p_i(x))^{k_i}$. Тогда многочлен $\frac{f(x)}{f_1(x)}$ имеет нулевую производную. Таким образом, мы можем считать, что

$$f(x) = p_1(x)p_2(x)\cdots p_m(x).$$

Теорема 3.81. *Пусть* $h(x) \in F_q[x]$ *и* $\deg h(x) < \deg f(x)$. *Предположим, что* $(h(x))^q \equiv h(x)(\mod f(x))$. *Тогда*

$$f(x) = \prod_{a \in F_q} \text{НОД } (f(x), h(x) - a).$$

Более того, правая часть этого равенства представляет собой нетривиальное разложение $f(x)$ *на взаимно простые множители.*

Доказательство. Мы знаем, что $y^q - y = 0$ для любого $y \in F_q$. Таким образом,

$$y^q - y = \prod_{a \in F_q} (y - a).$$

Следовательно,

$$(h(x))^q - h(x) = \prod_{a \in F_q} (h(x) - a) \equiv 0(\mod f(x)).$$

Заметим, что $h(x) - a_1$ и $h(x) - a_2$ взаимно просты при $a_1 \neq a_2$. Следовательно,

$$f(x) = \prod_{a \in F_q} \text{НОД } (f(x), h(x) - a)$$

и все множители $\prod\limits_{a \in F_q} \text{НОД } (f(x), h(x) - a)$ взаимно просты. Поскольку $\deg(h(x) - a) < \deg f$, то это разложение нетривиально. □

Определение 3.82. Многочлен $h(x) \in F_q[x]$ такой, что $\deg h(x) < \deg f(x)$ и $(h(x))^q \equiv h(x)(\mod f(x))$ называется *f-разлагающим* многочленом.

Из теоремы 3.81 следует, что если мы найдем какой-нибудь f-разлагающий многочлен, то сможем с его помощью разложить $f(x)$ на нетривиальные множители.

Теорема 3.83. *Пусть* $\deg f(x) = n$ *и*

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j (\mod f(x)), \quad i = 0, 1, \ldots, n-1.$$

Многочлен

$$h(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in F_q[x]$$

будет удовлетворять условию $(h(x))^q \equiv h(x)(\mod f(x))$ *тогда и только тогда, когда*

$$(a_0, a_1, \ldots, a_{n-1})B = (a_0, a_1, \ldots, a_{n-1}),$$

где

$$B = \begin{pmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,n-1} \\ b_{1,0} & b_{1,1} & \cdots & b_{1,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ b_{n-1,0} & b_{n-1,1} & \cdots & b_{n-1,n-1} \end{pmatrix}.$$

Доказательство. Заметим, что условие

$$(h(x))^q \equiv h(x)(\mod f(x))$$

равносильно условию

$$(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1})^q = \sum_{i=0}^{n-1} a_i x^{iq} \equiv \sum_{i=0}^{n-1} a_i x^i (\mod f(x)).$$

Заметим, что

$$\sum_{i=0}^{n-1} a_i x^{iq} \equiv \sum_{i=0}^{n-1} a_i \left(\sum_{j=0}^{n-1} b_{ij} x^j \right) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_i b_{ij} \right) x^j (\mod f(x)).$$

Отсюда следует утверждение теоремы. □

Замечание 3.84. Поскольку $x^0 = 1 \equiv 1(\mod f(x))$, то первая строчка матрицы B равна $(1, 0, 0, \ldots, 0)$.

Лемма 3.85. *Пусть* $\deg f(x) = n$ *и* $f(x) = p_1(x)p_2(x)\cdots p_m(x)$ *— разложение на неприводимые множители,* $c_1, c_2, \ldots, c_m \in F_q$. *Тогда существует единственный многочлен* $h(x)$ *такой, что* $\deg h(x) < n$ *и* $h(x) \equiv c_i(\mod p_i(x))$ *для всех* $i = 1, 2, \ldots, m$.

Доказательство. Пусть $c_1, c_2, \ldots, c_m \in F_q$. Согласно китайской теореме об остатках существует $h(x)$ такой, что $h(x) \equiv c_i(\mod p_i(x))$ для всех $i = 1, 2, \ldots, m$. Если $\deg h(x) \geq n$, то применив алгоритм Евклида, получаем $h(x) = g(x)f(x) + \bar{h}(x)$, где $\deg(\bar{h}(x)) < n$. При этом $h(x) \equiv \bar{h}(x)(\mod f(x))$. Следовательно, $h(x) \equiv \bar{h}(x)(\mod p_i(x))$ для всех $i = 1, 2, \ldots, m$. Заменив $h(x)$ на $\bar{h}(x)$, мы можем считать, что $\deg h(x) < n$. Осталось доказать единственность. Пусть есть два таких многочлена $h_1(x)$ и $h_2(x)$. Рассмотрим $h_1(x) - h_2(x)$. Заметим, что $\deg(h_1(x) - h_2(x)) < n$ и

$h_1(x) - h_2(x) \equiv 0(\mod p_i(x))$ для всех $i = 1, 2, \ldots, m$. Следовательно, $h_1(x) - h_2(x) \equiv 0(\mod f(x))$, т.е. $h_1(x) - h_2(x)$ делится на $f(x)$, но $\deg(f(x)) = n > \deg(h_1(x) - h_2(x))$. Противоречие. □

Теорема 3.86. *Пусть* $\deg f(x) = n$ *и* $f(x) = p_1(x)p_2(x)\cdots p_m(x)$ *— разложение на неприводимые множители,* $B_1 = (B - E)^T$*, где* B *— матрица из теоремы 3.83,* E *— единичная матрица. Тогда* m *равно размерности ядра матрицы* B_1*, т.е. размерности подпространства векторов* v *таких, что* $B_1 v = 0$*.*

Доказательство. Согласно теореме 3.81 $f(x) = \prod\limits_{a \in F_q} \text{НОД}\ (f(x), h(x) - a)$. Заметим, что $p_i(x)$ делит $\prod\limits_{a \in F_q} \text{НОД}\ (f(x), h(x) - a)$ тогда и только тогда, когда существует $c_i \in F_q$ такое, что $h(x) \equiv c_i(\mod p_i(x))$. Выберем $c_1, c_2, \ldots, c_m \in F_q$. Согласно лемме 3.85 существует единственный многочлен $h(x)$ такой, что $\deg h(x) < n$ и $h(x) \equiv c_i(\mod p_i(x))$ для всех $i = 1, 2, \ldots, m$. Таким образом, мы получили взаимно однозначное соответствие между наборами $c_1, c_2, \ldots, c_m \in F_q$ и f-разлагающими многочленами $h(x)$. Отсюда видно, что таких многочленов q^m штук. С другой стороны, каждое решение системы

$$B_1 \begin{pmatrix} a_0 \\ a_1 \\ \cdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix}$$

также задает f-разлагающий многочлен. Таких многочленов q^r, где r — размерность подпространства векторов v таких, что $B_1 v = 0$. Следовательно, $r = m$. □

Замечание 3.87. Заметим, что размерность ядра матрицы B_1 равна $n - s$, где s — ранг матрицы B_1.

Таким образом, мы получили следующий критерий неразложимости.

Следствие 3.88. *Многочлен* $f(x)$ *неприводим тогда и только тогда, когда* НОД $(f(x), f'(x)) = 1$ *и ранг матрицы* B_1 *равен* $n - 1$*.*

Теперь перейдем к алгоритму Берлекемпа.

(1) Избавимся от кратностей в разложении многочлена $f(x)$.
(2) Вычислим матрицу B.
(3) Найдем базис ядра B_1. Пусть $e_1 = (1, 0, 0, \ldots, 0)$, $e_2, \ldots, e_k$ — искомый базис.

(4) Если $k = 1$, многочлен $f(x)$ неприводим. Если $k > 1$, то $e_2 = (a_{2,0}, a_{2,1}, \ldots, a_{2,n-1})$. Тогда

$$h_2(x) = a_{2,0} + a_{2,1}x + \cdots + a_{2,n-1}x^{n-1}$$

— f-разлагающий многочлен. Рассмотрим НОД $(f(x), h_2(x) - a)$ для всех $a \in F_q$. Найдем разложение $f(x) = g_1(x)g_2(x)\cdots g_l(x)$. Если $l = k$, то алгоритм останавливается. Если $l < k$, то берем $e_3 = (a_{3,0}, a_{3,1}, \ldots, a_{3,n-1})$ и

$$h_3(x) = a_{3,0} + a_{3,1}x + \cdots + a_{3,n-1}x^{n-1}.$$

Вычисляя НОД $(g_i(x), h_3(x) - a)$ для всех $g_i(x)$ и $a \in F_q$, мы получаем дальнейшее разложение $f(x)$.

Теорема 3.89. *Алгоритм Берлекэмпа разлагает $f(x)$ на неприводимые множители.*

Доказательство. Пусть $f(x) = p_1(x)p_2(x)\cdots p_m(x)$, $h_1(x), h_2(x), \ldots, h_m(x)$ — f-разлагающие многочлены, векторы коэффициентов которых образуют базис пространства решений системы

$$B_1 \begin{pmatrix} a_0 \\ a_1 \\ \cdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \cdots \\ 0 \end{pmatrix},$$

мы считаем, что $h_1(x) = 1$. Нам нужно показать, что для любых двух $p_i(x)$ и $p_j(x)$ существуют $h_r(x)$ и $c \in F_q$ такие, что $h_r(x) \equiv c(\mod p_i(x))$, но $h_r(x) \not\equiv c(\mod p_j(x))$. Предположим противное, т.е. для всех $r = 1, 2, \ldots, m$ существуют $c_r \in F_q$ такие, что $h_r(x) \equiv c_r(\mod p_i(x))$ и $h_r(x) \equiv c_r(\mod p_j(x))$. Поскольку любой f-разлагающий многочлен $h(x)$ есть линейная комбинация $h_1(x), h_2(x), \ldots, h_m(x)$, то $h(x) \equiv c(\mod p_i(x))$ и $h(x) \equiv c(\mod p_j(x))$. С другой стороны, существует f-разлагающий многочлен $h(x)$ такой, что $h(x) \equiv 0(\mod p_i(x))$ и $h(x) \equiv 1(\mod p_j(x))$. Противоречие. □

11. Представление групп

Пусть V — конечномерное векторное пространство над полем k. Пусть $\mathrm{GL}(V)$ — группа обратимых линейных операторов на пространстве V.

Определение 3.90. Пусть G — группа. Всякий гомоморфизм $\varphi\colon G \to \mathrm{GL}(V)$ называется *линейным представлением* группы G в пространстве V.

Таким образом, линейное представление это пара (φ, V), состоящая из пространства V и гомоморфизма φ. Очевидно, что всегда существует гомоморфизм $\varphi\colon G \to I$, где I — единичный оператор. Такое представление называется *тривиальным*.

Определение 3.91. Два линейных представления (φ, V) и (ψ, W) называются *эквивалентными*(*изоморфными*), если существует изоморфизм $f\colon V \to W$, делающий диаграмму

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \varphi(g)}\downarrow & & \downarrow{\scriptstyle \psi(g)} \\ V & \xrightarrow{f} & W \end{array}$$

коммутативной для всех $g \in G$.

Заметим, что если мы выберем базис в пространстве V, то любой обратимый оператор представляется невырожденной матрицей A. Таким образом, мы получили гомоморфизм из группы G в группу невырожденных матриц, размера $n \times n$, где n — размерность пространства.

Определение 3.92. Пусть (φ, V) — линейное представление группы G. Подпространство $U \subset V$ называется *инвариантным* относительно (φ, V), если $\varphi(g)u \in U$ для любых $g \in G$, $u \in U$. Очевидно, что V и $\{0\}$ являются инвариантными. Если представление (φ, V) не имеет других инвариантных подпространств, то оно называется *неприводимым*. Представление (φ, V) *приводимо*, если у него есть нетривиальное (т.е. не равное V и $\{0\}$) инвариантное подпространство.

Пусть (φ, V) — линейное представление группы G и $U \subset V$ — нетривиальное инвариантное подпространство. Выберем базис $\{e_1, e_2, \ldots, e_n\}$ пространство V так, что $\{e_1, e_2, \ldots, e_k\}$ будет базисом подпространства U. Пусть A_g — матрица линейного оператора $\varphi(g)$ в базисе $\{e_1, e_2, \ldots, e_n\}$. Тогда

$$A_g = \begin{pmatrix} A'_g & B \\ 0 & A''_g \end{pmatrix}$$

для всех $g \in G$. Заметим, что

$$A_{gh} = A_g A_h = \begin{pmatrix} A'_g & B \\ 0 & A''_g \end{pmatrix} \begin{pmatrix} A'_h & C \\ 0 & A''_h \end{pmatrix} = \begin{pmatrix} A'_g A'_h & D \\ 0 & A''_g A''_h \end{pmatrix}.$$

Таким образом, отображение $g \to A'_g$ определяет представление на пространстве U. Оно называется *подпредставлением*. Отображение

$g \to A''_g$ определяет представление на фаткорпространстве V/U. Оно называется *факторпредставлением*. Если в V можно выбрать базис так, что

$$A_g = \begin{pmatrix} A'_g & 0 \\ 0 & A''_g \end{pmatrix}$$

для всех $g \in G$, то φ можно представить в виде прямой суммы представлений $\varphi = \varphi' + \varphi''$. Разложение в прямую сумму возможно тогда и только тогда, когда инвариантное подпространство $U \subset V$ имеет инвариантное дополнение W такое, что $V = U \oplus W$. Линейное представление (φ, V) называется *неразложимым*, если его нельзя представить в виде суммы двух нетривиальных подпредставлений. Если линейное представление (φ, V) можно разложить в прямую сумму неприводимых представлений, то это представление называется *вполне приводимым*.

Пусть теперь $k = \mathbb{C}$. Группу $\mathrm{GL}(V)$ в этом случае мы будем обозначать $\mathrm{GL}_n(\mathbb{C})$, где $n = \dim V$. Пусть на V задана функция $(\ \ ,\ \ ) \colon V \times V \to \mathbb{C}$. Эта функция называется *эрмитовой формой* (*эрмитовым произведением*), если

(1) $(u, v) = \overline{(v, u)}$ для всех $u, v \in V$;
(2) $(u_1 + u_2, v) = (u_1, v) + (u_2, v)$ для всех $u_1, u_2, v \in V$;
(3) $(\alpha u, v) = (u, \bar{\alpha} v) = \alpha (u, v)$ для всех $u, v \in V$, $\alpha \in \mathbb{C}$;
(4) $(u, u) \in \mathbb{R}$ и $(u, u) > 0$ для всех $u \in V$, $u \neq 0$.

Пусть $(e_1, e_2, \ldots, e_n)$ — базис пространства V. Пусть

$$u = u_1 e_1 + u_2 e_2 + \cdots + u_n e_n,$$

$$v = v_1 e_1 + v_2 e_2 + \cdots + v_n e_n.$$

Тогда

$$(u, v) = \sum_{i,j=1}^{n} h_{ij} u_i \bar{v}_j.$$

Положим

$$H = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ h_{n1} & h_{n2} & \cdots & h_{nn} \end{pmatrix}.$$

Заметим, что $h_{ij} = \bar{h}_{ji}$. Матрица H называется *эрмитовой*. У любой эрмитовой формы существует ортонормированный базис, т.е. базис $(e_1, e_2, \ldots, e_n)$ такой, что $(e_i, e_j) = 0$ для всех $i \neq j$ и $(e_i, e_i) = 1$. В этом базисе

$$(u, v) = u_1 \bar{v}_1 + u_2 \bar{v}_2 + \cdots + u_n \bar{v}_n.$$

Линейный оператор A называется *унитарным*, если $(Au, Av) = (u, v)$. Если матрица A (мы опускаем различие между оператором и его матрицей) задана в ортонормированном базисе, то условие унитарности записывается в виде $A\bar{A}^T = E$. Заметим, что унитарные матрицы (операторы) образуют группу. Мы будем обозначать ее через $U(n)$. Ясно, что $U(n) \subset \mathrm{GL}_n(\mathbb{C})$. Представление (φ, V) называется *унитарным*, если $\varphi(g) \in U(n)$ для любого $g \in G$.

Теорема 3.93. *Любое линейное представление (φ, V) конечной группы G изоморфно унитарному представлению.*

Доказательство. Выберем в пространстве V эрмитову форму $H(u, v)$. Рассмотрим форму

$$(u, v) = \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u, \varphi(g)v).$$

Заметим, что

$$(u, v) = \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u, \varphi(g)v) = \frac{1}{|G|} \sum_{g \in G} \overline{H(\varphi(g)v, \varphi(g)u)} =$$

$$= \overline{\frac{1}{|G|} \sum_{g \in G} H(\varphi(g)v, \varphi(g)u)} = \overline{(v, u)}.$$

Таким образом, выполнено первое условие эрмитовости (u, v). Аналогично,

$$(u_1 + u_2, v) = \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)(u_1 + u_2), \varphi(g)v) =$$

$$= \frac{1}{|G|} \sum_{g \in G} (H(\varphi(g)u_1, v) + H(\varphi(g)u_2, \varphi(g)v)) =$$

$$= \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u_1, \varphi(g)v) + \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u_2, \varphi(g)v) = (u_1, v) + (u_2, v),$$

$$(\alpha u, v) = \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)(\alpha u), \varphi(g)v) = \alpha \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u, \varphi(g)v) = \alpha(u, v),$$

$$(u, u) = \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u, \varphi(g)u) > 0.$$

Таким образом, (u, v) — эрмитова форма. С другой стороны,

$$(\varphi(h)u, \varphi(h)v) = \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)\varphi(h)u, \varphi(g)\varphi(h)v) =$$

$$= \frac{1}{|G|} \sum_{g \in G} H(\varphi(gh)u, \varphi(gh)v) = \frac{1}{|G|} \sum_{s \in G} H(\varphi(s)u, \varphi(s)v) = (u, v).$$

Таким образом, $\varphi(h)$ унитарен для любого $h \in G$. □

Теорема 3.94 (теорема Машке). *Каждое линейное представление конечной группы G над полем $\mathbb{C}$ вполне приводимо.*

Доказательство. Пусть (φ, V) — линейное представление над полем $\mathbb{C}$. Согласно теореме 3.93 существует эрмитова форма (u, v) на пространстве V, инвариантная относительно линейных операторов $\varphi(g)$ для всех $g \in G$. Пусть U — инвариантное подпространство. Тогда существует ортогональное дополнение

$$U^{\perp} = \{v \in V \mid (u, v) = 0, \quad \forall u \in U\}.$$

Заметим, что $V = U \oplus U^{\perp}$. Поскольку $\varphi(g)$ автоморфизм подпространства U, то для любого $u \in U$ существует $u' \in U$ такой, что $u = \varphi(g)u'$. Тогда для любого $v \in U^{\perp}$

$$(u, \varphi(g)v) = (\varphi(g)u', \varphi(g)v) = (u', v) = 0.$$

Таким образом, $U^{\perp}$ — инвариантное подпространство, и мы получаем разложение $\varphi = \varphi' + \varphi''$. □

Теорема 3.95 (лемма Шура). *Пусть (φ, V) и (ψ, W) — два неприводимых представлений над полем $\mathbb{C}$, и $f\colon V \to W$ — линейное отображение такое, что*

$$\psi(g)f = f\varphi(g), \quad \forall g \in G.$$

Тогда

(1) *если эти представления неизоморфны, то $f = 0$;*
(2) *если $V = W$ и $\varphi = \psi$, то $f = \lambda I$.*

Доказательство. Если $f = 0$, то все доказано. Пусть $V_0 = \ker f$ и $V_0 \neq V$. Поскольку

$$f(\varphi(g)v_0) = \psi(g)f(v_0) = 0,$$

то $\varphi(g)v_0 \in V_0$ для любого $g \in G$. Таким образом, V_0 — инвариантное подпространство. Отсюда, $V_0 = 0$. Пусть $W_0 = \operatorname{Im} f$. Для любого $w_0 \in W_0$ имеем

$$\psi(g)w_0 = \psi(g)f(u_0) = f(\varphi(g)u_0) = w_0' \in W_0,$$

для любого $g \in G$. Таким образом, W_0 — инвариантное подпространство W. Поскольку $f \neq 0$ и (ψ, W) неприводимо, то $W_0 = W$. Отсюда, $f\colon V \to W$ — изоморфизм пространств. Из условия

$\psi(g)f = f\varphi(g), \quad \forall g \in G$ получаем, что f определяет изоморфизм представлений. Таким образом, мы доказали (1).

По условию $f\colon V \to V$ — линейный оператор. Пусть λ — его собственное значение. Линейный оператор $f_0 = f - \lambda I$ имеет нетривиальное ядро и

$$\psi(g)f_0 = \psi(g)(f - \lambda I) = \psi(g)f - \lambda\psi(g) = f\varphi(g) - \lambda\varphi(g) = f_0\varphi(g).$$

Из утверждения (1) следует, что $f_0 = 0$. Таким образом, $f = \lambda I$. $\square$

Пусть A — матрица, размера $n \times n$. *Следом* этой матрицы $\operatorname{tr}(A)$ мы будем называть сумму элементов, стоящих на главной диагонали, т.е.

$$\operatorname{tr}(A) = a_{11} + a_{22} + \cdots + a_{nn}.$$

Утверждение 3.96. (1) $\operatorname{tr}(A + B) = \operatorname{tr} A + \operatorname{tr} B$ *для любых двух матриц* A *и* B*;*
(2) $\operatorname{tr}(\alpha A) = \alpha \operatorname{tr} A$ *для любого* $\alpha \in \mathbb{C}$ *и* A*.*

Утверждение 3.97. *Пусть* C *— невырожденная матрица. Тогда* $\operatorname{tr}(C^{-1}AC) = \operatorname{tr}(A)$*.*

Доказательство. Пусть A — матрица $n \times n$. Рассмотрим A, как линейный оператор. Его характеристический многочлен равен

$$\det(A - \lambda E) = (-1)^n\lambda^n + (-1)^{n-1}\lambda^{n-1} + \cdots .$$

Поскольку характеристический многочлен не меняется при переходе к новому базису, то и след не изменяется (следует из того, что

$$\det(C^{-1}AC - \lambda E) = \det(C^{-1}AC - \lambda C^{-1}EC) =$$

$$= \det(C^{-1}(A - \lambda E)C) = \det(C^{-1})\det(A - \lambda E)\det(C) = \det(A - \lambda E).)$$

$\square$

Теорема 3.98. *Пусть* (φ, V) *и* (ψ, W) *— два неприводимых представлений над полем* $\mathbb{C}$ *конечной группы* G *порядка* $|G|$*, и* $f\colon V \to W$ *— линейное отображение. Пусть*

$$\tilde{f} = \frac{1}{|G|}\sum_{g \in G} \psi(g) f \varphi(g)^{-1}.$$

Тогда

(1) *если* (φ, V) *и* (ψ, W) *неизоморфны, то* $\tilde{f} = 0$*;*
(2) *если* $V = W$ *и* $\varphi = \psi$*, то* $\tilde{f} = \lambda I$*,* $\lambda = \frac{\operatorname{tr} f}{\dim V}$*.*

Доказательство. Заметим, что

$$\psi(g)\tilde{f}\varphi(g)^{-1} = \frac{1}{|G|}\sum_{h\in G}\psi(g)\psi(h)f\varphi(h)^{-1}\varphi(g)^{-1} =$$

$$= \frac{1}{|G|}\sum_{h\in G}\psi(gh)f\varphi(gh)^{-1} = \frac{1}{|G|}\sum_{g'\in G}\psi(g')f\varphi(g')^{-1} = \tilde{f}.$$

Таким образом,

$$\psi(g)\tilde{f} = \tilde{f}\varphi(g), \quad \forall g \in G.$$

Теперь утверждение теоремы следует из леммы Шура (см. 3.95). Осталось проверить выражение для λ. Заметим, что

$$(\dim V)\lambda = \operatorname{tr}(\lambda E) = \operatorname{tr}\tilde{f} = \frac{1}{|G|}\sum_{g\in G}\operatorname{tr}(\varphi(g)f\varphi(g)^{-1}) = \frac{1}{|G|}\sum_{g\in G}\operatorname{tr} f = \operatorname{tr} f.$$

□

Выберем в пространствах V и W базисы $e_1, e_2, \ldots, e_n$ и $e'_1, e'_2, \ldots, e'_m$ соответственно. Запишем наши отображения в этих базисах. Получаем

$$\varphi(g) = (\varphi_{ii'}(g)), \quad \psi(g) = (\psi_{jj'}(g)), \quad f = (f_{ji}), \quad \tilde{f} = (\tilde{f}_{ji}).$$

Тогда

$$\tilde{f}_{ji} = \frac{1}{|G|}\sum_{g\in G}\sum_{i'=1}^{n}\sum_{j'=1}^{m}\psi_{jj'}(g)f_{j'i'}\varphi_{i'i}(g^{-1}).$$

Пусть f задается матричной единицей, т.е. $f_{ji} = 0$, для всех $(j,i) \neq (j_0,i_0)$ и $f_{j_0i_0} = 1$. Применим теорему 3.98 (1), получаем

$$\frac{1}{|G|}\sum_{g\in G}\psi_{jj_0}(g)\varphi_{i_0i}(g^{-1}) = 0. \tag{1}$$

Заметим, что это равенство выполнено для всех i, i_0, j, j_0. (Мы считаем, что представления (φ, V) и (ψ, W) неизоморфны).

Пусть теперь $(\varphi, V) = (\psi, W)$. Заметим, что

$$\operatorname{tr} f = \sum_{i=1}^{n} f_{ii} = \sum_{i',j'}\delta^{i'}_{j'}f_{j'i'},$$

где

$$\delta^{i'}_{j'} = \begin{cases} 1, & j' = i' \\ 0, & j' \neq i' \end{cases}$$

— символ Кронекера. Поскольку $\tilde{f} = \frac{\operatorname{tr} f}{\dim V}$, то

$$\tilde{f}_{ji} = \delta^i_j \frac{\operatorname{tr} f}{\dim V} = \frac{\delta^i_j}{\dim V} \sum_{i',j'} \delta^{i'}_{j'} f_{j'i'}.$$

Отсюда,

$$\frac{1}{|G|} \sum_{g\in G} \sum_{i'=1}^{n} \sum_{j'=1}^{n} \varphi_{jj'}(g) f_{j'i'} \varphi_{i'i}(g^{-1}) = \frac{1}{\dim V} \sum_{i'=1}^{n} \sum_{j'=1}^{n} \delta^i_j \delta^{i'}_{j'} f_{j'i'}.$$

Подставляя в качестве f матричные единицы, получаем

$$\frac{1}{|G|} \sum_{g\in G} \varphi_{jj_0}(g) \varphi_{i_0 i}(g^{-1}) = \begin{cases} \frac{\delta^i_j}{\dim V}, & j_0 = i_0 \\ 0, & j_0 \neq i_0 \end{cases} . \tag{2}$$

Пусть (φ, V) — представление группы G. Определим функцию $\chi_\varphi \colon G \to k$ соотношением $\chi_\varphi(g) = \operatorname{tr} \varphi(g)$. Эта функция называется *характером представления*. Поскольку при переходе к новому базису матрица $\varphi(g)$ переходит в матрицу $C^{-1}\varphi(g)C$, то характер не зависит от выбора базиса.

Теорема 3.99. *Пусть χ_φ — характер комплексного линейного представления (φ, V) (т.е. $k = \mathbb{C}$) группы G. Тогда*

(1) $\chi_\varphi(e) = \dim V$;
(2) $\chi_\varphi(hgh^{-1}) = \chi_\varphi(g)$ *для любых* $g, h \in G$;
(3) *если* $g \in G$ *имеет конечный порядок, то* $\chi_\varphi(g^{-1}) = \overline{\chi_\varphi(g)}$;
(4) *если* $\varphi = \varphi' + \varphi''$, *то* $\chi_\varphi = \chi_{\varphi'} + \chi_{\varphi''}$.

Доказательство. (1) $\chi_\varphi(e) = \operatorname{tr} \varphi(e) = \operatorname{tr} E = \dim V$.

(2) $\chi_\varphi(hgh^{-1}) = \operatorname{tr} \varphi(hgh^{-1}) = \operatorname{tr}(\varphi(h)\varphi(g)\varphi(h)^{-1}) = \operatorname{tr} \varphi(g) = \chi_\varphi(g)$.

(3) Пусть g имеет порядок m, т.е. $g^m = e$. Тогда $\varphi(g)^m = E$. Пусть $\lambda_1, \lambda_2, \ldots, \lambda_n$ — собственные значения оператора $\varphi(g)$. Заметим, что $\lambda_i^m = 1$. Отсюда, $|\lambda_i| = 1$ и $\lambda_i^{-1} = \overline{\lambda_i}$. Тогда

$$\chi_\varphi(g^{-1}) = \operatorname{tr} \varphi(g^{-1}) = \sum_{i=1}^{n} \lambda_i^{-1} = \sum_{i=1}^{n} \overline{\lambda_i} = \overline{\sum_{i=1}^{n} \lambda_i} = \overline{\chi_\varphi(g)}.$$

(4) Пусть $\varphi = \varphi' + \varphi''$. Тогда

$$A_g = \begin{pmatrix} A'_g & 0 \\ 0 & A''_g \end{pmatrix},$$

где A_g, A'_g, A''_g — матрицы операторов $\varphi(g), \varphi'(g), \varphi''(g)$ соответственно. Тогда $\operatorname{tr} A_g = \operatorname{tr} A'_g + \operatorname{tr} A''_g$. Отсюда, $\chi_\varphi = \chi_{\varphi'} + \chi_{\varphi''}$. □

Заметим, что если $\dim V = 1$, то $\chi_\varphi(g) = \varphi(g)$.

Рассмотрим множество функций $f\colon G \to \mathbb{C}$ из группы G в поле комплексных чисел. Очевидно, что мы можем определить суммы двух функций $f_1 + f_2$ как $(f_1 + f_2)(g) = f_1(g) + f_2(g)$. Аналогично, $(\alpha f)(g) = \alpha f(g)$. Таким образом, на этом множестве естественно определена структура линейного пространства. Функция $f\colon G \to \mathbb{C}$ называется *центральной*, если она постоянна на классах сопряженности. Заметим, что согласно теореме 3.99 (2), характеры являются центральными функциями.

Далее будем предполагать, что группа G конечна. Тогда на пространстве функций мы можем задать эрмитово произведение

$$(f_1, f_2) = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

Теорема 3.100. *Пусть φ, ψ — неприводимые комплексные представления конечной группы G. Тогда*

$$(\chi_\varphi, \chi_\psi) = \begin{cases} 1, & \text{если } \varphi \text{ изоморфно } \psi \\ 0, & \text{если } \varphi \text{ неизоморфно } \psi \end{cases}.$$

Доказательство. Предположим, что представления φ и ψ неизоморфны. Положим

$$\chi_\varphi(g) = \sum_{i=1}^{n} \varphi_{ii}(g), \quad \chi_\psi(g) = \sum_{j=1}^{m} \psi_{ii}(g).$$

Подставив в (1) $j_0 = j$, $i_0 = i$, получим

$$\frac{1}{|G|} \sum_{g \in G} \psi_{jj}(g)\varphi_{ii}(g^{-1}) = 0.$$

Просуммируем это равенство по всем i и j. Получаем

$$\frac{1}{|G|} \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{g \in G} \psi_{jj}(g)\varphi_{ii}(g^{-1}) = 0.$$

Поскольку группа конечна, то $\varphi_{ii}(g^{-1}) = \overline{\varphi_{ii}(g)}$. Таким образом, $(\chi_\varphi, \chi_\psi) = 0$, если представления неизоморфны.

Пусть $\varphi = \psi$. Подставим в (2) $j_0 = j$, $i_0 = i$. Получаем

$$\frac{1}{|G|} \sum_{g \in G} \varphi_{jj}(g)\varphi_{ii}(g^{-1}) = \frac{\delta^i_j}{\dim V}.$$

Просуммируем это равенство по всем i и j. Получаем

$$\frac{1}{|G|}\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{g\in G}\varphi_{jj}(g)\varphi_{ii}(g^{-1}) = \frac{\delta_j^i}{\dim V} = \sum_{i=1}^{n}\sum_{j=1}^{n}\frac{\delta_j^i}{\dim V} = 1.$$

Используя $\varphi_{ii}(g^{-1}) = \overline{\varphi_{ii}(g)}$, получаем $(\chi_\varphi, \chi_\psi) = 1$, если представления изоморфны. □

Следствие 3.101. *Пусть (φ, V) — комплексное представление конечной группы и $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ — разложение V в прямую сумму неприводимых инвариантных подпространств. Пусть $\varphi_1, \varphi_2, \ldots, \varphi_k$ — соответствующие представление на $V_1, V_2, \ldots, V_k$ (т.е. ограничения φ на $V_1, V_2, \ldots, V_k$). Пусть (ψ, W) — неприводимое представление. Тогда число представлений (φ_i, V_i) изоморфных (ψ, W) равно $(\chi_\varphi, \chi_\psi)$.*

Доказательство. Согласно теореме 3.99 (4)

$$\chi_\varphi = \chi_{\varphi_1} + \chi_{\varphi_2} + \cdots + \chi_{\varphi_k}.$$

Тогда

$$(\chi_\varphi, \chi_\psi) = (\chi_{\varphi_1}, \chi_\psi) + (\chi_{\varphi_2}, \chi_\psi) + \cdots + (\chi_{\varphi_k}, \chi_\psi).$$

Согласно теореме 3.100 эта сумму состоит из нулей и единиц, причем число единиц совпадает с числом представлений (φ_i, V_i) изоморфных (ψ, W). □

Следствие 3.102. *Два представления с одним и тем же характером изоморфны.*

Доказательство. Пусть (φ, V) и (ψ, W) — два представлений над полем $\mathbb{C}$ конечной группы. Пусть $V = V_1 \oplus V_2 \oplus \cdots \oplus V_k$ и $W = W_1 \oplus W_2 \oplus \cdots \oplus W_l$ — разложения V и W в прямую сумму неприводимых инвариантных подпространств. Рассмотрим представление (φ_i, V_i). Заметим, что $(\chi_\varphi, \chi_{\varphi_i}) = s$, где s — число подпредставлений в (φ, V), изоморфных (φ_i, V_i). С другой стороны, $(\chi_\psi, \chi_{\varphi_i}) = s$. Таким образом, число подпредставлений в (ψ, W), изоморфных (φ_i, V_i) также равно s. Следовательно, представления (φ, V) и (ψ, W) изоморфны. □

Пусть (φ, V) — комплексное представление конечной группы. Тогда

$$\chi_\varphi = m_1\chi_{\varphi_1} + m_2\chi_{\varphi_2} + \cdots + m_k\chi_{\varphi_k},$$

где m_i — кратность с которой входит неприводимое представление (φ_i, V_i) в разложение (φ, V). Тогда

$$(\chi_\varphi, \chi_\varphi) = m_1^2 + m_2^2 + \cdots + m_k^2.$$

Определение 3.103. Представление (φ, V) называется *точным*, если $\ker \varphi = e$.

Рассмотрим один важный пример.

Пример 3.104. Пусть G — конечная группа. Рассмотрим групповую алгебру $W = \mathbb{C}G$ над полем $\mathbb{C}$. Как векторное пространство W порождено множеством $\{e_g \mid g \in G\}$. Таким образом, $\dim W = |G|$. Определим представление $\rho\colon G \to \mathrm{GL}(W)$ группы G, как $\rho(a)e_g = e_{ag}$ для любых $a, g \in G$. Такое представление называется *регулярным*. Заметим, что регулярное представление является точным. Пусть R_a — матрица линейного оператора $\rho(a)$ в базисе $\{e_g \mid g \in G\}$. Заметим, что все матрицы R_a состоят из нулей и единиц. Более того, для любого $a \neq e$ $\rho(a)e_g \neq e_g$, т.е. все диагональные элементы матрицы R_a равны нулю. Таким образом, $\operatorname{tr} R_a = 0$ для любого $a \in G$, $a \neq e$. Тогда

$$\chi_\rho(e) = |G|, \quad \chi_\rho(g) = 0, \quad \forall g \neq e.$$

Пусть (φ, V) — любое неприводимое представление конечной группы G над $\mathbb{C}$. Тогда

$$(\chi_\rho, \chi_\varphi) = \frac{1}{|G|}\sum_{g\in G} \chi_\rho(g)\overline{\chi_\varphi(g)} = \frac{1}{|G|}\chi_\rho(e)\overline{\chi_\varphi(e)} = \frac{1}{|G|}|G|\chi_\varphi(e) = \dim V.$$

Согласно следствию 3.101, аждое неприводимое представление входит в регулярное с кратностью равной своей размерности. В частности, число различных неприводимых представлений у конечной группы, конечно. Пусть $(\varphi_1, V_1), (\varphi_2, V_2), \ldots, (\varphi_s, V_s)$ — попарно неизоморфные неприводимые представления. Пусть $\chi_1, \chi_2, \ldots, \chi_s$ — их характеры. Тогда

$$\chi_\rho = n_1\chi_1 + n_2\chi_2 + \cdots + n_s\chi_s,$$

где $n_i = \dim V_i$. Отсюда

$$|G| = \chi_\rho(e) = n_1\chi_1(e) + n_2\chi_2(e) + \cdots + n_s\chi_s(e) = n_1^2 + n_2^2 + \cdots + n_s^2.$$

Таким образом, мы доказали следующую теорему.

Теорема 3.105. *Каждое неприводимое представление конечной группы G входит в разложение регулярного представления с кратностью, равной размерности пространства этого представления. Порядок $|G|$ и размерности $n_1, n_2, \ldots, n_s$ пространств неприводимых линейных представлений связаны соотношением*

$$|G| = n_1^2 + n_2^2 + \cdots + n_s^2.$$

Лемма 3.106. *Пусть* Γ *— центральная функция на конечной группе* G *и* (φ, V) *— неприводимое комплексное представление этой группы с характером* χ_φ*. Рассмотрим линейный оператор*

$$\Phi_\Gamma = \sum_{g\in G} \bar{\Gamma}(g)\varphi(g).$$

Тогда $\Phi_\Gamma = \lambda I$*, где* $\lambda = \frac{|G|}{\chi_\varphi(e)}(\chi_\varphi, \Gamma)$.

Доказательство. Поскольку Γ — центральная функция, то $\Gamma(hgh^{-1}) = \Gamma(g)$, а следовательно и $\bar{\Gamma}(hgh^{-1}) = \bar{\Gamma}(g)$. Тогда

$$\varphi(h)\Phi_\Gamma\varphi(h)^{-1} = \sum_{g\in G} \bar{\Gamma}(g)\varphi(h)\varphi(g)\varphi(h)^{-1} = \sum_{g\in G} \bar{\Gamma}(hgh^{-1})\varphi(hgh^{-1}) =$$

$$= \sum_{g'\in G} \bar{\Gamma}(g')\varphi(g') = \Phi_\Gamma.$$

Отсюда, $\varphi(h)\Phi_\Gamma = \Phi_\Gamma\varphi(h)$ для любого $h \in G$. Согласно лемме Шура (см. 3.95) $\Phi_\Gamma = \lambda I$. Вычислим след этих операторов. Получаем

$$\lambda\chi_\varphi(e) = \lambda \dim V = \operatorname{tr}(\lambda I) = \sum_{g\in G} \bar{\Gamma}(g) \operatorname{tr}\varphi(g) =$$

$$= |G| \left(\frac{1}{|G|} \sum_{g\in G} \chi_\varphi(g)\bar{\Gamma}(g) \right) = |G|(\chi_\varphi, \Gamma).$$

Отсюда, $\lambda = \frac{|G|}{\chi_\varphi(e)}(\chi_\varphi, \Gamma)$. □

Заметим, что множество всех центральных функций образуют подпространство в множестве всех функций на группе G. Обозначим это подпространство через X.

Лемма 3.107. *Характеры* $\chi_1, \chi_2, \ldots, \chi_s$ *всех попарно неизоморфных неприводимых представлений конечной группы* G *образуют ортонормированный базис в* X.

Доказательство. По теореме 3.100 система $\chi_1, \chi_2, \ldots, \chi_s$ ортонормирована. Пусть Γ — центральная функция, ортогональная ко всем $\chi_1, \chi_2, \ldots, \chi_s$, т.е. $(\chi_i, \Gamma) = 0$. Рассмотрим

$$\Phi^i_\Gamma = \sum_{g\in G} \bar{\Gamma}(g)\varphi_i(g),$$

где φ_i — представление с характером χ_i. Согласно лемме 3.106 $\Phi^i_\Gamma = 0$. Пусть φ — произвольное комплексное представление. Тогда по теореме Машке (см. 3.94)

$$\varphi = m_1\varphi_1 + m_2\varphi_2 + \cdots + m_s\varphi_s.$$

Пусть

$$\Phi_\Gamma = \sum_{g \in G} \bar{\Gamma}(g)\varphi(g).$$

Тогда

$$\Phi_\Gamma = m_1\Phi_\Gamma^1 + m_2\Phi_\Gamma^2 + \cdots + m_s\Phi_\Gamma^s = 0.$$

Таким образом, $\Phi_\Gamma = 0$ для любого представления φ. В частности и для регулярного представления ρ имеем $\rho_\Gamma = 0$. С другой стороны, применим ρ_Γ к вектору e_e (вектор, соответствующий единицы группы). Получаем

$$0 = \rho_\Gamma(e_e) = \sum_{g \in G} \bar{\Gamma}(g)\rho(g)e_e = \sum_{g \in G} \bar{\Gamma}(g)e_g.$$

Отсюда, $\bar{\Gamma}(g) = 0$ для любого $g \in G$. Следовательно, $\Gamma = 0$. □

Теорема 3.108. *Число неприводимых попарно неизоморфных представлений конечной группы G над полем $\mathbb{C}$ равно числу ее классов сопряженности.*

Доказательство. Согласно лемме 3.107 характеры всех попарно неизоморфных неприводимых представлений образуют базис в пространстве центральных функций. С другой стороны, каждому классу сопряженности $C_i \subset G$ мы можем сопоставить функцию

$$f_i(g) = \begin{cases} 1, & g \in C_i \\ 0, & g \notin C_i \end{cases}.$$

Заметим, что $f_1, f_2, \ldots, f_r$ также образуют базис. По известной теореме из линейной алгебры, число векторов базиса инвариантно, т.е. $r = s$. □

Литература

[1] Атья М., Макдональд И. *Введение в коммутативную алгебру.*
[2] Ленг С. *Алгебра.*
[3] Каргополов М.И., Мерзляков Ю.И. *Основы теории групп.*
[4] Кострикин А.И. *Основы алгебры.*
[5] Курош А.Г., *Курс высшей алгебры.*
[6] Панкратьев Е.В., *Элементы компьютерной алгебры.*
[7] Прасолов В.В., *Многочлены.*