

Лекции по курсу "Алгебра"

Белоусов Григорий Николаевич

Оглавление

Глава 1. Группы	3
1. Перестановки	3
2. Группы	7
3. Действия групп на множествах	11
4. Гомоморфизм групп	13
5. Прямое произведение групп	16
6. Конечные абелевы группы	18
7. Свободные группы	19
Глава 2. Кольца, модули, поля и алгебры	25
1. Определение и основные свойства колец	25
2. Коммутативные кольца	28
3. Локализация	34
4. Многочлены	35
5. Модули	42
6. Алгебры	44
Глава 3. 2-й семестр	50
1. Расширение полей	50
2. Конечные поля	54
3. Нетеровы кольца	55
4. Артиновы кольца	60
5. Многочлены	64
6. Симметрические многочлены	69
7. Теорема Штурма	71
8. Результант	73
9. Алгоритм Кронекера	74
10. Алгоритм Берлекэмпа	75
11. Представление групп	79
Литература	92

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 $\Omega = \{1, 2, \dots, n\}$. Рассмотрим взаимно однозначные (биективные) отображения $\sigma: \Omega \rightarrow \Omega$. 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 $\sigma(1) = i_1, \sigma(2) = i_2, \dots, \sigma(n) = i_n$.

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

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

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

$$i_1 \rightarrow i_2 \rightarrow \cdots \rightarrow i_k \rightarrow i_1.$$

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 $(j_1 j_2 \dots j_m)$. 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 перестановки 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. $x \notin \tau_{p+1}, \tau_{p+2}, \dots, \tau_k$. 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

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

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

$$\sigma = (i_1 i_2 \cdots i_k)(j_1 j_2 \cdots j_l) \cdots.$$

Согласно замечанию 1.10 все циклы четной длины можно разбить на пары. Пусть $(i_1 i_2 \cdots i_k)(j_1 j_2 \cdots j_l)$ 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

$$\begin{aligned} & (i_1 i_2)(i_2 i_3) \cdots (i_{k-1} i_k)(j_1 j_2)(j_2 j_3) \cdots (j_{l-1} j_l) = \\ & = ((i_1 i_2)(j_1 j_2))((i_2 i_3)(j_2 j_3)) \cdots ((i_{k-1} i_k)(j_{k-1} j_k))(j_k j_{k+1}) \cdots (j_{l-1} j_l). \end{aligned}$$

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. \square

2. Группы

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

$$S \times S \rightarrow S.$$

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) (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 $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ — 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 $e = ee' = e'$. \square

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

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

\square

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, $g_1h_3 \in g_2H$. \square

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

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,

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

\square

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 $g = s_1^{i_1} \dots s_j^{i_j}$, где $s_1, \dots, s_j \in S$ и $i_1, \dots, i_j \in \mathbb{Z}$. 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 произведение циклов длины i_1, i_2, \dots, i_k . Пусть $\sigma' \in S_n$ — сопряженный элемент к σ . Тогда σ' разлагается в произведения циклов длины i_1, i_2, \dots, i_k . Обратно, если $\sigma' \in S_n$ разлагается в произведения циклов длины i_1, i_2, \dots, 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 $\sigma = (j_1j_2 \cdots j_l)$, 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 $\sigma = (j_1j_2 \cdots j_l)$ и $\sigma' = (k_1k_2 \cdots k_l)$. Рассмотрим перестановку τ такую, что $\tau(j_1) = k_1, \tau(j_2) = k_2, \dots, \tau(j_l) = k_l$. Тогда $\sigma' = \tau\sigma\tau^{-1}$. \square

3. Действия групп на множествах

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

- (1) $et = t$ для любого $t \in M$
- (2) $g_1(g_2t) = (g_1g_2)t$ для любых $g_1, g_2 \in G$ и $t \in M$.

ОПРЕДЕЛЕНИЕ 1.33. Пусть группа G действует на множестве M . Стабилизатором элемента $t \in M$ называется множество $\text{St}(t) = \{g \in G \mid gt = t\}$.

Легко проверить, что $\text{St}(t)$ — является подгруппой группы G .

ОПРЕДЕЛЕНИЕ 1.34. Пусть группа G действует на множестве M . Орбитой элемента $t \in M$ называется множество $\text{Orb}(t) = \{gt \mid g \in G\}$.

УТВЕРЖДЕНИЕ 1.35. Имеется взаимно однозначное соответствие между элементами орбиты $\text{Orb}(t)$ и левыми смежными классами по подгруппе $\text{St}(t)$.

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

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

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

ДОКАЗАТЕЛЬСТВО. Пусть $m_1 = g m_2$ и $a \in \text{St}(m_1)$. Тогда $g^{-1} a g \in \text{St}(m_2)$. Отсюда, $g^{-1} \text{St}(m_1) g \subseteq \text{St}(m_2)$. Пусть $b \in \text{St}(m_2)$. Тогда $g b g^{-1} = c \in \text{St}(m_1)$. Отсюда, $g^{-1} \text{St}(m_1) g = \text{St}(m_2)$. \square

ТЕОРЕМА 1.38 (Формула Бернсайда). Пусть G — конечная группа, действующая на конечном множестве M . Пусть M^g — множество элементов m таких, что $g m = m$. 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 $\sum_{g \in G} |M^g|$. Заметим, что эта сумма равна количеству пар (g, m) таких, что $g m = m$. Таким образом,

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

Теперь применим следствие 1.36. Получаем

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

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

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

Заметим, что

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

Таким образом, $\sum_{m \in M} \frac{1}{|\text{Orb}(m)|} = N$. 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. Докажем 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,

$$a'b'h = ah_1bh_2h = ab(h'_1h_2h) = ab\tilde{h},$$

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

Группа определенная в утверждении 1.40 называется *фактор-группой* 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 $f: G \rightarrow G'$, 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 инъективный гомоморфизм называется *изоморфизмом*. Две группы G и G' называются *изоморфными*, если существует изоморфизм $f: G \rightarrow G'$ (для краткости будем писать $G \cong G'$).

УТВЕРЖДЕНИЕ 1.42. Пусть $f: G \rightarrow G'$ — 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 $f(a)^{-1} = f(a^{-1})$. \square

ПРЕДЛОЖЕНИЕ 1.43. Пусть $f: G \rightarrow G'$ — 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. \square

ТЕОРЕМА 1.44 (1-я теорема о гомоморфизме). Пусть $f: G \rightarrow G'$ — сюръективный гомоморфизм групп. Тогда существует естественный изоморфизм $G/\ker(f) \cong G'$. Обратно, если $H \triangleleft G$, то

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

ДОКАЗАТЕЛЬСТВО. Пусть $\bar{f}: G/\ker(f) \rightarrow G'$ — 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

$$\begin{aligned}\bar{f}(g_1\ker(f) \cdot g_2\ker(f)) &= \bar{f}(g_1g_2\ker(f)) = f(g_1g_2) = \\ &= f(g_1)f(g_2) = \bar{f}(g_1\ker(f))\bar{f}(g_2\ker(f)).\end{aligned}$$

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. \square

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, $h_1k_1h_2k_2 = h_1h_2k'_1k_2$, где $h_1, h_2 \in H$, $k_1, k'_1k_2 \in K$. Следовательно, $HK = KH$ — подгруппа группы G . Очевидно, что $K \triangleleft HK$ и $H \cap K \triangleleft H$.

Пусть $f: H \rightarrow HK/K$ — 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. \square

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 $f: G/K \rightarrow G/H$, 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. \square

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. \square

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 $f: G \rightarrow H \times K$, 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

$$G \cong H_1 \times H_2 \times \cdots \times H_n.$$

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 $H_1 \times H_2 \triangleleft G_1 \times G_2$ и $G/H_1 \times H_2 \cong (G_1/H_1) \times (G_2/H_2)$.

ДОКАЗАТЕЛЬСТВО. Пусть $\alpha: G_1 \rightarrow G_1/H_1$ и $\beta: G_2 \rightarrow G_2/H_2$ — естественные гомоморфизмы. Определим гомоморфизм $f: G \rightarrow (G_1/H_1) \times (G_2/H_2)$ 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 $(H_1 \times H_2 \times \cdots \times H_n) \triangleleft G$ 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 группы \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. \square

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 $f: G \rightarrow G_1 = G/\langle a \rangle$, 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 $|G_2| = p^{n_2} m$. Продолжая этот процесс, мы получим $|G_i| = m$. Согласно следствию 1.24 порядок любого элемента группы G_i является делителем m . Отсюда, $m = 1$. \square

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 $q = p_1^{r_1} \cdot p_2^{r_2} \cdot \dots \cdot p_n^{r_n}$. Пусть $t_i = p_1^{r_1} \cdot \dots \cdot p_{i-1}^{r_{i-1}} \cdot p_{i+1}^{r_{i+1}} \cdot \dots \cdot p_n^{r_n}$. 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 $t = p_1^{s_1} \cdot \dots \cdot p_{i-1}^{s_{i-1}} \cdot p_{i+1}^{s_{i+1}} \cdot \dots \cdot p_n^{s_n}$. 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. \square

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 максимальной порядка p^{s_1} , мы получаем $p^{s_1-1}a + lp^{s_1-1}g = 0$. Поскольку $A \cap \langle g \rangle = \{0\}$, то $p^{s_1-1}a = 0$ и $lp^{s_1-1}g = 0$. Следовательно, $l = jp$. Отсюда, $p(b - jg) = a \in A$. Пусть $c = b - jg$ и пусть C — подгруппа, порожденная $A \cup c$. В силу максимальной 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. \square

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. \square

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

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

ДОКАЗАТЕЛЬСТВО. Пусть

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

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

$$r_1 B_1 + r_2 B_2 + \dots + r_n B_n = 0.$$

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

$$s_1 B_1 + s_2 B_2 + \dots + s_n B_n = 0,$$

где $s_i \in \mathbb{Z}$. Отсюда,

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

Тогда

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

Противоречие. □

ЗАМЕЧАНИЕ 1.64. Если $a_1, a_2, \dots, a_k \in A$ — базис группы A и $b_1, b_2, \dots, b_k \in A$ независимы, то далеко не всегда b_1, b_2, \dots, 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 $a_1, a_2, \dots, a_n \in A$ порождают группу A . Если a_1, a_2, \dots, a_n независимы, то это базис. Следовательно, мы можем считать, что существуют $s_1, s_2, \dots, s_n \in \mathbb{Z}$, что $s_1 a_1 + s_2 a_2 + \dots + s_n a_n = 0$. 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 $s_1a_1 + s_2a_2 + \dots + s_na_n = 0$ — минимальное соотношение, то наименьший общий делитель s_1, s_2, \dots, s_n равен единице. Действительно, если $s_i = ds'_i$ для всех i , то

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

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

Рассмотрим минимальное соотношение $s_1a_1 + s_2a_2 + \dots + s_na_n = 0$. 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,

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

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

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

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

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

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

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.

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

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. \square

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 $f: A \rightarrow \bar{A}$ — 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 $\bar{a}_1, \bar{a}_1, \dots, \bar{a}_n$ — базис \bar{A} , и a_1, a_1, \dots, a_n — прообразы $\bar{a}_1, \bar{a}_1, \dots, \bar{a}_n$ в A . Заметим, что a_1, a_1, \dots, a_n независимы. Пусть M — свободная абелева группа порожденная a_1, a_1, \dots, 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 $\bar{g} = s_1\bar{a}_1 + s_2\bar{a}_1 + \dots + s_n\bar{a}_n$. Рассмотрим $b = g - (s_1a_1 + s_2a_1 + \dots + s_na_n)$. Заметим, что $f(b) = 0$. Тогда $b \in B$, и

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

Таким образом, $B \oplus M = A$. \square

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 $x_i x_i^{-1}$ или $x_i^{-1} x_i$. Слово u называется *несократимым*, если в нем нет последовательностей вида $x_i x_i^{-1}$ 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, редуцируется к единственному несократимому слову. \square

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

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

\square

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 из одного элемента, а свободная абелева группа имеет ранг 1).

ТЕОРЕМА 1.74. Пусть G — группа, порожденная элементами g_1, g_2, \dots, g_n . Рассмотрим алфавит X , состоящий из x_1, x_2, \dots, x_n . Тогда отображение $f: X \rightarrow M$ по правилу $f(x_i) = g_i$ единственным образом продолжается до гомоморфизма групп $f: F(X) \rightarrow G$.

ДОКАЗАТЕЛЬСТВО. Определим $\bar{f}: F(X) \rightarrow G$ 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 $\bar{f}: F(X) \rightarrow G$ 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, \dots, 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.

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, $0 \cdot a = 0$. \square

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 $f: A \rightarrow B$ 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 $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ — 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 деления 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. \square

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 отличие 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 $f: A \rightarrow B$ — 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 . \square

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 умножения 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 $f: A \rightarrow B$ — 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 $\varphi: A \rightarrow A/\mathfrak{a}$ такое, что φ — сюръекция и $\ker(\varphi) = \mathfrak{a}$.

ДОКАЗАТЕЛЬСТВО. В силу аналогичного утверждения для групп (см. 1.44) мы уже имеем изоморфизм групп $\bar{f}: A/\ker(f) \rightarrow B$. 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 множество 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 будут 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 $\mathfrak{a}\mathfrak{b}$, как множество элементов $x = ab$, где $a \in \mathfrak{a}$, $b \in \mathfrak{b}$. Заметим, что $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$.

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. \square

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 $y \in \mathfrak{m}$. \square

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, $\mathfrak{m}' = A$. \square

ТЕОРЕМА 2.18. Пусть $f: A \rightarrow B$ — 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 $y \in \mathfrak{p}$. \square

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 $x \equiv y \pmod{\mathfrak{a}}$.

ТЕОРЕМА 2.19 (китайская теорема об остатках). Пусть A — коммутативное кольцо, и пусть $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n$ — идеалы кольца A . Предположим, что $\mathfrak{a}_i + \mathfrak{a}_j = A$ для всех $i \neq j$. Тогда для любого семейства $x_1, x_2, \dots, x_n \in A$ существует $x \in A$ такой, что $x \equiv x_i \pmod{\mathfrak{a}_i}$ 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 $a_1 \equiv 1 \pmod{\mathfrak{a}_2}$ и $a_2 \equiv 1 \pmod{\mathfrak{a}_1}$. Рассмотрим $x = x_2 a_1 + x_1 a_2$. Получаем $x \equiv x_1 \pmod{\mathfrak{a}_1}$, $x \equiv x_2 \pmod{\mathfrak{a}_2}$.

Предположим, что теорема доказана для семейства из $n - 1$ идеалов. Заметим, что существуют $a_1 \in \mathfrak{a}_1, a_2 \in \mathfrak{a}_2, \dots, a_{n-1} \in \mathfrak{a}_{n-1}$ и $b_1, b_2, \dots, b_{n-1} \in \mathfrak{a}_n$ 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 $y_n \equiv 1 \pmod{\mathfrak{a}_n}$, $y_n \equiv 0 \pmod{\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_{n-1}}$. Следовательно, $y_n \equiv 1 \pmod{\mathfrak{a}_n}$ и $y_n \equiv 0 \pmod{\mathfrak{a}_i}$ для любого $i = 1, 2, \dots, n-1$. Аналогично, существуют y_1, \dots, y_{n-1} такие, что $y_i \equiv 1 \pmod{\mathfrak{a}_i}$, $y_i \equiv 0 \pmod{\mathfrak{a}_j}$, где $i \neq j$. Тогда элемент $x = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$ удовлетворяет требованиям теоремы. \square

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

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

— 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. \square

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. \square

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

Теперь запишем китайскую теорему об остатках для кольца целых чисел.

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

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

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 . \square

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, \dots, 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, $q_i = u_i p_i$, 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,

$$s_1s_2(as's'' - sa's'') = 0, \quad s_1s_2(a's''s - s'a''s) = 0.$$

Складывая эти уравнения, получаем

$$s_1s_2(as''s' - a''ss') = s_1s_2s'(as'' - a''s) = 0.$$

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

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

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

$$t_1(as_1 - a_1s) = 0,$$

$$t_2(a's'_1 - a'_1s') = 0.$$

Умножим первое на $t_2s's'_1$, второе на t_3ss_1 и сложим. Получаем

$$\begin{aligned} 0 &= t_1t_2(s's'_1(as_1 - a_1s) + ss_1(a's'_1 - a'_1s')) = \\ &= t_1t_2(s_1s'_1(as' + a's) - ss'(a_1s'_1 + a'_1s_1)). \end{aligned}$$

Таким образом,

$$\frac{as' + a's}{ss'} = \frac{a_1s'_1 + a'_1s_1}{s_1s'_1}.$$

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

Рассмотрим отображение $\varphi_S A \rightarrow S^{-1}A$, 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. \square

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

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

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

$$\begin{aligned} f + g &= (a_0, a_1, \dots, a_n, \dots) + (b_0, b_1, \dots, b_n, \dots) = \\ &= (a_0 + b_0, a_1 + b_1, \dots, a_n + b_n, \dots), \\ f \cdot g &= (a_0, a_1, \dots, a_n, \dots) \cdot (b_0, b_1, \dots, b_n, \dots) = (h_0, h_1, \dots, h_n, \dots), \end{aligned}$$

где

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

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

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

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

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n.$$

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

$$g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m.$$

Тогда

$$f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \dots + a_n b_m x^{n+m}.$$

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 $\varphi_\alpha: A[x] \rightarrow K$, 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. \square

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

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

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 $f_2 = f_1 - \frac{a'_1}{b_m} x^{\deg f_1 - m} g$, где a'_1 — 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. \square

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

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

Подставим $r_1 = f - q_1g$ в $g = q_2r_1 + r_2$, получим $r_2 = (1 + q_1q_2)g - q_2f$. 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 $r_{n-2} = q_nr_{n-1} + r_n$ 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 $d(x)$. \square

Рассмотрим еще один класс колец. Пусть A — целостное кольцо и определено отображение $\delta: A \setminus \{0\} \rightarrow \mathbb{N} \cup \{0\}$, 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. \square

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 . \square

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. \square

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 $K[x] \rightarrow K[x]/(f)$ 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 $\alpha_1, \alpha_2, \dots, \alpha_n \in E$.

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, $f = af'_1f'_2 \cdots f'_{m'}$ 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. \square

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

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

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

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

Отсюда,

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

Рассмотрим

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

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 $|f(x_0 + h)| < |f(x_0)|$. \square

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

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

Теперь утверждение следует из известного факта из математического анализа. \square

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 *фактормодулем*. Пусть M и M' — A -модули. *Гомоморфизмом* модулей $f: M \rightarrow M'$ 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* $\text{Im} f$ называется множество $N' = \{y \mid y \in M' \ \exists x f(x) = y\}$. Легко заметить, что N' — подмодуль M' .

Как и в случае групп имеем теоремы о гомоморфизме.

ТЕОРЕМА 2.59 (1-я теорема о гомоморфизме). Пусть $f: M \rightarrow M'$ — сюръективный гомоморфизм модулей. Тогда существует естественный изоморфизм $M/\ker(f) \cong M'$.

ДОКАЗАТЕЛЬСТВО. Пусть $\bar{f}: M/\ker(f) \rightarrow M'$ — 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. \square

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 $f: N \rightarrow (N + N')/N'$ — 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. \square

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 $f: M/N' \rightarrow M/N$, 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. \square

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 $x_1, x_2, \dots, x_n \in M$ такие, что любой $x \in M$ имеет представление

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

ОПРЕДЕЛЕНИЕ 2.62. Аннулятором A -модуля M называется множество

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

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

ТЕОРЕМА 2.63. $\text{Ann}(M)$ — двусторонний идеал кольца A .

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

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

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

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

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

Полагая $(a + \text{Ann}(M))x = ax$ для $x \in M$, $(a + \text{Ann}(M)) \in A/\text{Ann}(M)$, мы определяем на M структуру $A/\text{Ann}(M)$ -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 $f: K \rightarrow A$ — 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 $a^*: A \rightarrow A$ 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 $J: A \rightarrow M_n(K)$, отображающий элемент $a \in A$ в матрицу линейного оператора a^* . Докажем, что гомоморфизм инъективен. Пусть $J(a) = 0$. Тогда $a = a \cdot 1 = a^*(1) = 0$. \square

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 $1, a, a^2, \dots, a^n$ линейно зависимы. Тогда существуют $\alpha_0, \alpha_1, \dots, \alpha_n \in K$ такие, что $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \dots + \alpha_n a^n = 0$. \square

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

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

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

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

Таким образом, a обратим. \square

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, \dots, 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

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

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

$$\begin{aligned} x\bar{x} &= (a + bi + cj + dk)(a - bi - cj - dk) = \\ &= a^2 - abi - acj - adk + abi + b^2 - bck + bdj + acj + bck + \\ &\quad + c^2 - cdi + adk - bdj + cdi + d^2 = a^2 + b^2 + c^2 + d^2. \end{aligned}$$

Следовательно,

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

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 $f(x)$. \square

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, $a \in \mathbb{C}$. \square

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

$$\begin{aligned} f(\bar{\alpha}) &= a_n \bar{\alpha}^n + a_{n-1} \bar{\alpha}^{n-1} + \cdots + a_1 \bar{\alpha} + a_0 = \overline{a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0} \\ &= \overline{a_n \alpha^n + a_{n-1} \alpha^{n-1} + \cdots + a_1 \alpha + a_0} = 0. \end{aligned}$$

□

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 стороны,

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

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 $d: A \rightarrow A$, 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 пространство над k . Другими словами, E конечно над k , если существуют $a_1, a_2, \dots, a_n \in E$ такие, что $\forall x \in E$, $x = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$, где $\alpha_1, \alpha_2, \dots, \alpha_n \in k$. *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, \dots, x_n — базис E над полем k , y_1, y_2, \dots, y_m — базис F над полем E . Тогда для любого элемента $a \in F$ существует разложение

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

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

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

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 $\sum_{j=1}^n c_{ij} x_j \in E$. Поскольку y_1, y_2, \dots, y_m линейно независимы, то все $\sum_{j=1}^n c_{ij} x_j = 0$. Поскольку x_1, x_2, \dots, x_n линейно независимы, то все $c_{ij} = 0$. \square

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 $\alpha_0, \alpha_1, \dots, \alpha_n \in k$ 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 $1, a, a^2, \dots, a^n, \dots$. Поскольку E — конечное расширение поля k , то существует n такое, что элементы $1, a, a^2, \dots, a^n$ линейно зависимы. Тогда существуют $\alpha_0, \alpha_1, \dots, \alpha_n \in k$ такие, что $\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_n a^n = 0$. \square

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

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

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

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 $f(x)$. \square

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 $\text{Ит}(a, k, x)$.

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

ДОКАЗАТЕЛЬСТВО. Заметим, что

$$k \subset k(a_1) \subset k(a_1, a_2) \subset \dots \subset k(a_1, a_2, \dots, a_n).$$

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

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

$$a_0 + a_1x + \dots + a_nx^n = 0,$$

где $a_0, a_1, \dots, a_n \in E$. Рассмотрим $E_0 = k(a_0, a_1, \dots, a_n)$. 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. \square

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 $\sigma: k[x] \rightarrow k[x]/(p(x))$ — 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.

$$\underbrace{1 + 1 + \dots + 1}_p = 0.$$

Пусть p — минимальное из таких чисел. Тогда говорят, что p — характеристика поля k . Обозначается $\text{char}(k)$. 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

$$\underbrace{1 + 1 + \dots + 1}_p = \underbrace{(1 + 1 + \dots + 1)}_m \cdot \underbrace{(1 + 1 + \dots + 1)}_n = 0.$$

Отсюда, либо

$$\underbrace{1 + 1 + \dots + 1}_m = 0,$$

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 $f: k \rightarrow k^p$ 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 $\text{char}(k) = p > 0$. 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, \dots, e_n — базис k как векторного пространства над \mathbb{Z}_p , $a_1, a_2, \dots, a_n \in \mathbb{Z}_p$. 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 умножения. 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

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

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

$$M_1 \subset M_2 \subset \dots \subset M_n \subset \dots$$

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 $M_1 \subset M_2 \subset \dots$ — возрастающая последовательность подмодулей. Положим $N = \bigcup_{n=1}^{\infty} M_n$. Тогда N — подмодуль. По предположению, N конечно порожден. Следовательно, существуют элементы x_1, x_2, \dots, x_m , порождающие N . Тогда существует модуль M_j такой, что $x_1, x_2, \dots, x_m \in M_j$. Отсюда,

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

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

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \dots$$

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

(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 $f: M \rightarrow M/N$ — канонический гомоморфизм. Пусть $\bar{M}_1 \subset \bar{M}_2 \subset \dots \subset \bar{M}_n \subset \dots$ — возрастающая последовательность подмодулей в M/N . Положим $M_i = f^{-1}(\bar{M}_i)$. Тогда $M_1 \subset M_2 \subset \dots \subset M_n \subset \dots$ — 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 $M_1 \subset M_2 \subset \dots$ — возрастающая последовательность подмодулей в M . Тогда $M_1 \cap N \subset M_2 \cap N \subset \dots$ и $(M_1 + N)/N \subset (M_2 + N)/N \subset \dots$ — 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 $M_i = M_n$. \square

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 $f: M_1 \oplus M_2 \rightarrow M$. Тогда $M \cong (M_1 \oplus M_2)/\ker f$. Теперь наше утверждение следует из теоремы 3.21. \square

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 $f: A \rightarrow B$ — сюръективный гомоморфизм колец. Тогда B нетерово.

ДОКАЗАТЕЛЬСТВО. Пусть $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \dots$ — 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 $i > n$. \square

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

ДОКАЗАТЕЛЬСТВО. Пусть x_1, x_2, \dots, x_n — образующие M . Тогда существует гомоморфизм модулей

$$f: \underbrace{A \times A \times \dots \times A}_n \rightarrow M$$

при котором

$$f(a_1, a_2, \dots, a_n) = a_1 x_1 + a_2 x_2 + \dots + a_n x_n.$$

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

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 $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \dots$ — 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

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

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

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

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 $a_{i1}, a_{i2}, \dots, a_{in_i}$ — образующие идеала \mathfrak{a}_i , и $f_{i1}, f_{i2}, \dots, f_{in_i} \in \mathfrak{A}$ — многочлены степени i со старшими коэффициентами $a_{i1}, a_{i2}, \dots, a_{in_i}$.

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 $x^{d-r} f_{r1}, x^{d-r} f_{r2}, \dots, x^{d-r} f_{rn_r}$ порождают \mathfrak{a}_d . Следовательно, существуют $c_1, c_2, \dots, c_{n_r} \in A$ такие, что многочлен

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

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, \dots, c_{n_d} такие, что многочлен

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

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

СЛЕДСТВИЕ 3.33. Пусть A — коммутативное нетерово кольцо. Тогда кольцо многочленов $A[x_1, x_2, \dots, x_n]$ 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 $y_1, y_2, \dots, y_n \in B$ — элементы, порождающие B над A . Рассмотрим кольцо многочленов $A[x_1, x_2, \dots, x_n]$. Согласно 3.33 оно нетерово. Заметим, что существует сюръективный гомоморфизм $f: A[x_1, x_2, \dots, x_n] \rightarrow B$ такой, что $f(x_i) = y_i$. Тогда, согласно 3.28, B также нетерово. \square

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. \square

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

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

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

$\text{Ann}(x^i) = \text{Ann}(x^n)$ 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, $b \in \text{Ann}(x^{n+1}) = \text{Ann}(x^n)$. Таким образом, $bx^n = 0$, т.е. $a = 0$. \square

Из теорем 3.36 и 3.38 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 nilьпотентных элементов является идеалом.*

ДОКАЗАТЕЛЬСТВО. Пусть R — множество nilьпотентных 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 $x + y \in R$. \square

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 — nilьпотент. Тогда $x^n = 0 \in \mathfrak{p}$. Следовательно, $x \in \mathfrak{p}$. Таким образом nilьрадикал 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 максимальной \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. \square

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. \square

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

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

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 $f: M \rightarrow M/N$ — канонический гомоморфизм. Пусть $\bar{M}_1 \supset \bar{M}_2 \supset \dots \supset \bar{M}_n \supset \dots$ — убывающая последовательность подмодулей в M/N . Положим $M_i = f^{-1}(\bar{M}_i)$. Тогда $M_1 \supset M_2 \supset \dots \supset M_n \supset \dots$ — 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 $i > n$. \square

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

ДОКАЗАТЕЛЬСТВО. Пусть $M_1 \supset M_2 \supset \dots$ — убывающая последовательность подмодулей в M . Тогда $M_1 \cap N \subset M_2 \cap N \subset \dots$ и $(M_1 + N)/N \subset (M_2 + N)/N \subset \dots$ — 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 $M_i = M_n$. \square

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 $f: A \rightarrow B$ — сюръективный гомоморфизм колец. Тогда B артиново.

ДОКАЗАТЕЛЬСТВО. Пусть $\mathfrak{b}_1 \supset \mathfrak{b}_2 \supset \dots$ — 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 $i > n$. \square

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 артиново кольцо. Пусть $x \in B$. Поскольку B артиново, 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). \square

СЛЕДСТВИЕ 3.53. В артиновом кольце нильрадикал совпадает с радикалом Джекобсона.

ЛЕММА 3.54. Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_n$ — 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, \dots, 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, $x_1, x_2, \dots, x_n \notin \mathfrak{p}$. Противоречие. Если $\bigcap_{i=1}^n \mathfrak{a}_i = \mathfrak{p}$, то $\mathfrak{p} \subset \mathfrak{a}_i$ для всех i . Отсюда, $\mathfrak{a}_i = \mathfrak{p}$ для некоторого i . \square

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

ДОКАЗАТЕЛЬСТВО. Пусть $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_n, \dots$ — 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 — артиново, 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 $\mathfrak{m}_i = \mathfrak{m}_{n+1}$. \square

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, $V_{i+1} \neq V_{i+2}$ тогда и только тогда, когда $\dim V_i > \dim V_{i+1}$.

Пусть V — бесконечномерное пространство. Тогда существует бесконечная последовательность $x_1, x_2, \dots, x_n, \dots$ линейно независимых элементов из V . Пусть $V_i = L(x_{i+1}, x_{i+2}, \dots)$ — линейная оболочка натянутая на элементы x_{i+1}, x_{i+2}, \dots , 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. \square

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. \square

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 — артиново 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. \square

ТЕОРЕМА 3.59. Любое артиново кольцо является нетеровым.

ДОКАЗАТЕЛЬСТВО. Пусть A — артиново кольцо. Пусть $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_n$ — 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. \square

5. Многочлены

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

натуральные числа j_1, j_2, \dots, j_n такие, что

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

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

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

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

ДОКАЗАТЕЛЬСТВО. Согласно теореме 3.60 существует представление

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

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 $r = \text{ord}_p \alpha$. Будем считать $\text{ord}_p 0 = -\infty$.

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

$$\begin{aligned}\text{ord}_p(\alpha\beta) &= \text{ord}_p \alpha + \text{ord}_p \beta, \\ \text{ord}_p(\alpha + \beta) &\geq \min(\text{ord}_p \alpha, \text{ord}_p \beta).\end{aligned}$$

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

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

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

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

□

Пусть

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

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

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

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

УТВЕРЖДЕНИЕ 3.64. Пусть $\text{cont}(f) = 1$. 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 $c = c \text{cont}(f) = \text{cont}(cf)$. Противоречие. □

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

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

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

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

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

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

Предположим, что $\text{cont}(fg)$ 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

$$h(x) = f(x)g(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0.$$

Тогда

$$c_{r+s} = a_r b_s + \sum a_i b_{r+s-i}.$$

Заметим, что $a_r b_s$ не делится на p , но любое $a_i b_{r+s-i}$ делится на p . Отсюда, c_{r+s} не делится на p . Таким образом, $\text{cont}(fg)$ не делится на p . Противоречие. \square

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 $c_1 = \text{cont}(g)$, $c_2 = \text{cont}(h)$. Тогда $c_1 c_2 = \text{cont}(f) \in A$. С другой стороны, $g(x) = c_1 g_1(x)$, $h(x) = c_2 h_1(x)$, где $\text{cont}(g_1) = \text{cont}(h_1) = 1$. Тогда $g_1(x), h_1(x) \in A[x]$ (см. 3.64). Пусть $\hat{g}(x) = c_1 c_2 g_1(x) \in A[x]$, $\hat{h}(x) = h_1(x) \in A[x]$. Тогда $f(x) = \hat{g}(x)\hat{h}(x)$. \square

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 $c_i = \text{cont}(p_i)$ и $\text{cont}(\hat{p}_i) = 1$. Отсюда,

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

где $c = c_1 c_2 \cdots c_n = \text{cont}(f) \in A$. Поскольку $\text{cont}(\hat{p}_i) = 1$, 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 . \square

СЛЕДСТВИЕ 3.68. Пусть A — факториальное кольцо. Тогда $A[x_1, x_2, \dots, x_n]$ 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

$$a_n \not\equiv 0 \pmod{p}, \quad a_i \equiv 0 \pmod{p}, \quad \forall i < n, \quad a_0 \not\equiv 0 \pmod{p^2}.$$

Тогда $f(x)$ неприводим в $K[x]$.

ДОКАЗАТЕЛЬСТВО. Заметим, что мы можем считать $\text{cont}(f) = 1$. 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

$$\begin{aligned} \sigma(a_n)x^n &= \sigma(f(x)) = \sigma(g(x)h(x)) = \sigma(g(x))\sigma(h(x)) = \\ &= \sigma(b_m)\sigma(c_k)x^n + \cdots + \sigma(b_r)\sigma(c_s)x^{r+s}. \end{aligned}$$

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 $b_0 \equiv 0 \pmod{p}$ и $c_0 \equiv 0 \pmod{p}$. Следовательно, $a_0 = b_0c_0 \equiv 0 \pmod{p^2}$. Противоречие. \square

ТЕОРЕМА 3.70. Пусть A и B — целостные кольца, $\sigma: A \rightarrow B$ — 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 . \square

6. Симметрические многочлены

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

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

Элементарными симметрическими многочленами будем называть многочлены

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

где $k = 1, 2, \dots, n$.

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

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

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 $s_1, s_2, \dots, s_{n-1}, s_n$, то мы получим $(s_1)_0, (s_2)_0, \dots, (s_{n-1})_0$ — элементарные симметрические многочлены от x_1, x_2, \dots, x_{n-1} .

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

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

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

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 $f(x_1, x_2, \dots, x_n)$ имеет степень d . Подставим $x_n = 0$. По индуктивному предположению существует многочлен $g_1(y_1, y_2, \dots, y_{n-1})$ такой, что

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

Тогда многочлен

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

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

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

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

ПРИМЕР 3.76. Пусть

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

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

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

Отсюда,

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

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

Рассмотрим симметрический многочлен

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

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

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

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

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

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

ТЕОРЕМА 3.78 (теорема Штурма). Пусть $f(x) \in \mathbb{R}[x]$ и $f(x) = f_0(x), f_1(x), \dots, f_n(x)$ — 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 $f_0(x), f_1(x), \dots, f_n(x)$ на отрезке $[a; b]$ задает разбиение

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

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 случаи

- (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. \square

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

$$\begin{aligned} f(x) &= q_1(x)f_1(x) - f_2(x), \\ f_1(x) &= q_2(x)f_2(x) - f_3(x), \\ &\dots\dots\dots \\ f_{n-2}(x) &= q_{n-1}(x)f_{n-1}(x) - f_n(x), \\ f_{n-1}(x) &= q_n(x)f_n(x). \end{aligned}$$

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). \square

8. Результат

Пусть

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

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

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

ТЕОРЕМА 3.80. *Результант $\text{Res}(f, g) = 0$ тогда и только тогда, когда f и g имеют 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, \dots, C_{n+m} — столбцы матрицы (1). Рассмотрим

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

Тогда

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

Отсюда, $\text{Res}(f, g) = 0$.

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

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

Рассмотрим многочлены

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

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

Из (2) следует

$$f g_1 + g f_1 = 0.$$

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 $\lfloor \frac{n}{2} \rfloor$;
- (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 $\lfloor \frac{n}{2} \rfloor + 1$ точке.

Таким образом, мы можем выбрать любые целые $\lfloor \frac{n}{2} \rfloor + 1$ точки, например, $0, 1, 2, \dots, \lfloor \frac{n}{2} \rfloor$. 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 $f(0), f(1), \dots, f(\lfloor \frac{n}{2} \rfloor)$. Для каждого набора существует многочлен $f_1(x)$. Далее проверяем делится ли $f(x)$ на $f_1(x)$.

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

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

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

$$S^{-1}(y^{a_1 + a_2 d + a_3 d^2 + \dots + a_n d^{n-1}}) = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}.$$

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

10. Алгоритм Берлекэмпса

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

$f_1(x) = \prod_{k_i: p \nmid k_i} (p_i(x))^{k_i}$. 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 $(h(x))^q \equiv h(x) \pmod{f(x)}$. 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,

$$(h(x))^q - h(x) = \prod_{a \in F_q} (h(x) - a) \equiv 0 \pmod{f(x)}.$$

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 $\prod_{a \in F_q} \text{НОД}(f(x), h(x) - a)$ взаимно просты. Поскольку $\deg(h(x) - a) < \deg f$, то это разложение нетривиально. \square

ОПРЕДЕЛЕНИЕ 3.82. Многочлен $h(x) \in F_q[x]$ такой, что $\deg h(x) < \deg f(x)$ и $(h(x))^q \equiv h(x) \pmod{f(x)}$ 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

$$x^{iq} \equiv \sum_{j=0}^{n-1} b_{ij} x^j \pmod{f(x)}, \quad i = 0, 1, \dots, n-1.$$

Многочлен

$$h(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in F_q[x]$$

будет удовлетворять условию $(h(x))^q \equiv h(x) \pmod{f(x)}$ тогда и только тогда, когда

$$(a_0, a_1, \dots, a_{n-1})B = (a_0, a_1, \dots, a_{n-1}),$$

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

$$(h(x))^q \equiv h(x) \pmod{f(x)}$$

равносильно условию

$$(a_0 + a_1x + \cdots + a_{n-1}x^{n-1})^q = \sum_{i=0}^{n-1} a_i x^{iq} \equiv \sum_{i=0}^{n-1} a_i x^i \pmod{f(x)}.$$

Заметим, что

$$\sum_{i=0}^{n-1} a_i x^{iq} \equiv \sum_{i=0}^{n-1} a_i \left(\sum_{j=0}^{n-1} b_{ij} x^j \right) = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} a_i b_{ij} \right) x^j \pmod{f(x)}.$$

Отсюда следует утверждение теоремы. \square

ЗАМЕЧАНИЕ 3.84. Поскольку $x^0 = 1 \equiv 1 \pmod{f(x)}$, то первая строчка матрицы B равна $(1, 0, 0, \dots, 0)$.

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, $c_1, c_2, \dots, c_m \in F_q$. Тогда существует единственный многочлен $h(x)$ такой, что $\deg h(x) < n$ и $h(x) \equiv c_i \pmod{p_i(x)}$ для всех $i = 1, 2, \dots, m$.

ДОКАЗАТЕЛЬСТВО. Пусть $c_1, c_2, \dots, c_m \in F_q$. Согласно китайской теореме об остатках существует $h(x)$ такой, что $h(x) \equiv c_i \pmod{p_i(x)}$ для всех $i = 1, 2, \dots, m$. 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 $h(x) \equiv \bar{h}(x) \pmod{f(x)}$. Следовательно, $h(x) \equiv \bar{h}(x) \pmod{p_i(x)}$ для всех $i = 1, 2, \dots, m$. 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

$h_1(x) - h_2(x) \equiv 0 \pmod{p_i(x)}$ для всех $i = 1, 2, \dots, m$. Следовательно, $h_1(x) - h_2(x) \equiv 0 \pmod{f(x)}$, 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. \square

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 $f(x) = \prod_{a \in F_q} \text{НОД}(f(x), h(x) - a)$. Заметим, что $p_i(x)$ делит $\prod_{a \in F_q} \text{НОД}(f(x), h(x) - a)$ тогда и только тогда, когда существует $c_i \in F_q$ такое, что $h(x) \equiv c_i \pmod{p_i(x)}$. Выберем $c_1, c_2, \dots, c_m \in F_q$. Согласно лемме 3.85 существует единственный многочлен $h(x)$ такой, что $\deg h(x) < n$ и $h(x) \equiv c_i \pmod{p_i(x)}$ для всех $i = 1, 2, \dots, m$. Таким образом, мы получили взаимно однозначное соответствие между наборами $c_1, c_2, \dots, c_m \in F_q$ и f -разлагающими многочленами $h(x)$. Отсюда видно, что таких многочленов q^m штук. С другой стороны, каждое решение системы

$$B_1 \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix}$$

также задает f -разлагающий многочлен. Таких многочленов q^r , где r — размерность подпространства векторов v таких, что $B_1 v = 0$. Следовательно, $r = m$. \square

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 $\text{НОД}(f(x), f'(x)) = 1$ 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 $e_1 = (1, 0, 0, \dots, 0)$, e_2, \dots, e_k — искомый базис.

- (4) Если $k = 1$, многочлен $f(x)$ неприводим. Если $k > 1$, то $e_2 = (a_{2,0}, a_{2,1}, \dots, a_{2,n-1})$. Тогда

$$h_2(x) = a_{2,0} + a_{2,1}x + \dots + a_{2,n-1}x^{n-1}$$

— f -разлагающий многочлен. Рассмотрим НОД $(f(x), h_2(x) - a)$ для всех $a \in F_q$. Найдем разложение $f(x) = g_1(x)g_2(x) \dots g_l(x)$. Если $l = k$, то алгоритм останавливается. Если $l < k$, то берем $e_3 = (a_{3,0}, a_{3,1}, \dots, a_{3,n-1})$ и

$$h_3(x) = a_{3,0} + a_{3,1}x + \dots + a_{3,n-1}x^{n-1}.$$

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 $f(x) = p_1(x)p_2(x) \dots p_m(x)$, $h_1(x), h_2(x), \dots, h_m(x)$ — f -разлагающие многочлены, векторы коэффициентов которых образуют базис пространства решений системы

$$B_1 \begin{pmatrix} a_0 \\ a_1 \\ \dots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \dots \\ 0 \end{pmatrix},$$

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 $h_r(x) \equiv c \pmod{p_i(x)}$, но $h_r(x) \not\equiv c \pmod{p_j(x)}$. Предположим противное, т.е. для всех $r = 1, 2, \dots, m$ существуют $c_r \in F_q$ такие, что $h_r(x) \equiv c_r \pmod{p_i(x)}$ и $h_r(x) \equiv c_r \pmod{p_j(x)}$. Поскольку любой f -разлагающий многочлен $h(x)$ есть линейная комбинация $h_1(x), h_2(x), \dots, h_m(x)$, то $h(x) \equiv c \pmod{p_i(x)}$ и $h(x) \equiv c \pmod{p_j(x)}$. С другой стороны, существует f -разлагающий многочлен $h(x)$ такой, что $h(x) \equiv 0 \pmod{p_i(x)}$ и $h(x) \equiv 1 \pmod{p_j(x)}$. Противоречие. \square

11. Представление групп

Пусть V — конечномерное векторное пространство над полем k . Пусть $\text{GL}(V)$ — группа обратимых линейных операторов на пространстве V .

ОПРЕДЕЛЕНИЕ 3.90. Пусть G — группа. Всякий гомоморфизм $\varphi: G \rightarrow \text{GL}(V)$ 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 $\varphi: G \rightarrow I$, 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 $f: V \rightarrow W$, делающий диаграмму

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ \varphi(g) \downarrow & & \downarrow \psi(g) \\ V & \xrightarrow{f} & W \end{array}$$

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 $\{e_1, e_2, \dots, e_n\}$ пространства V так, что $\{e_1, e_2, \dots, e_k\}$ будет базисом подпространства U . Пусть A_g — матрица линейного оператора $\varphi(g)$ в базисе $\{e_1, e_2, \dots, e_n\}$. 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 $g \rightarrow A'_g$ определяет представление на пространстве U . Оно называется *подпредставлением*. Отображение

$g \rightarrow A_g''$ определяет представление на факторпространстве 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 $(\ , \) : V \times V \rightarrow \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, \dots, e_n) — базис пространства V . Пусть

$$u = u_1 e_1 + u_2 e_2 + \dots + u_n e_n,$$

$$v = v_1 e_1 + v_2 e_2 + \dots + v_n e_n.$$

Тогда

$$(u, v) = \sum_{i,j=1}^n h_{ij} u_i \bar{v}_j.$$

Положим

$$H = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1n} \\ h_{21} & h_{22} & \dots & h_{2n} \\ \dots & \dots & \dots & \dots \\ h_{n1} & h_{n2} & \dots & h_{nn} \end{pmatrix}.$$

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, \dots, e_n) такой, что $(e_i, e_j) = 0$ для всех $i \neq j$ и $(e_i, e_i) = 1$. В этом базисе

$$(u, v) = u_1 \bar{v}_1 + u_2 \bar{v}_2 + \dots + u_n \bar{v}_n.$$

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 $U(n) \subset \text{GL}_n(\mathbb{C})$. 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

$$\begin{aligned} (u, v) &= \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u, \varphi(g)v) = \frac{1}{|G|} \sum_{g \in G} \overline{H(\varphi(g)v, \varphi(g)u)} = \\ &= \overline{\frac{1}{|G|} \sum_{g \in G} H(\varphi(g)v, \varphi(g)u)} = \overline{(v, u)}. \end{aligned}$$

Таким образом, выполнено первое условие эрмитовости (u, v) . Аналогично,

$$\begin{aligned} (u_1 + u_2, v) &= \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)(u_1 + u_2), \varphi(g)v) = \\ &= \frac{1}{|G|} \sum_{g \in G} (H(\varphi(g)u_1, \varphi(g)v) + H(\varphi(g)u_2, \varphi(g)v)) = \\ &= \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u_1, \varphi(g)v) + \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u_2, \varphi(g)v) = (u_1, v) + (u_2, v), \\ (\alpha u, v) &= \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)(\alpha u), \varphi(g)v) = \alpha \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u, \varphi(g)v) = \alpha(u, v), \\ (u, u) &= \frac{1}{|G|} \sum_{g \in G} H(\varphi(g)u, \varphi(g)u) > 0. \end{aligned}$$

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 $h \in G$. \square

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 $\varphi = \varphi' + \varphi''$. \square

ТЕОРЕМА 3.95 (лемма Шура). *Пусть (φ, V) и (ψ, W) — два неприводимых представления над полем \mathbb{C} , и $f: V \rightarrow W$ — 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 $W_0 = \text{Im } f$. 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, $f: V \rightarrow W$ — изоморфизм пространств. Из условия

$\psi(g)f = f\varphi(g)$, $\forall g \in G$ получаем, что f определяет изоморфизм представлений. Таким образом, мы доказали (1).

По условию $f: V \rightarrow V$ — 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 $\text{tr}(A)$ мы будем называть сумму элементов, стоящих на главной диагонали, т.е.

$$\text{tr}(A) = a_{11} + a_{22} + \dots + a_{nn}.$$

УТВЕРЖДЕНИЕ 3.96. (1) $\text{tr}(A + B) = \text{tr} A + \text{tr} B$ для любых двух матриц A и B ;
(2) $\text{tr}(\alpha A) = \alpha \text{tr} A$ для любого $\alpha \in \mathbb{C}$ и A .

УТВЕРЖДЕНИЕ 3.97. Пусть C — невырожденная матрица. Тогда $\text{tr}(C^{-1}AC) = \text{tr}(A)$.

ДОКАЗАТЕЛЬСТВО. Пусть A — матрица $n \times n$. Рассмотрим A , как линейный оператор. Его характеристический многочлен равен

$$\det(A - \lambda E) = (-1)^n \lambda^n + (-1)^{n-1} \lambda^{n-1} + \dots.$$

Поскольку характеристический многочлен не меняется при переходе к новому базису, то и след не изменяется (следует из того, что

$$\begin{aligned} \det(C^{-1}AC - \lambda E) &= \det(C^{-1}AC - \lambda C^{-1}EC) = \\ &= \det(C^{-1}(A - \lambda E)C) = \det(C^{-1}) \det(A - \lambda E) \det(C) = \det(A - \lambda E). \end{aligned}$$

\square

ТЕОРЕМА 3.98. Пусть (φ, V) и (ψ, W) — два неприводимых представлений над полем \mathbb{C} конечной группы G порядка $|G|$, и $f: V \rightarrow W$ — 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 $\tilde{f} = \lambda I$, $\lambda = \frac{\text{tr} f}{\dim V}$.

ДОКАЗАТЕЛЬСТВО. Заметим, что

$$\begin{aligned}\psi(g)\tilde{f}\varphi(g)^{-1} &= \frac{1}{|G|} \sum_{h \in G} \psi(g)\psi(h)f\varphi(h)^{-1}\varphi(g)^{-1} = \\ &= \frac{1}{|G|} \sum_{h \in G} \psi(gh)f\varphi(gh)^{-1} = \frac{1}{|G|} \sum_{g' \in G} \psi(g')f\varphi(g')^{-1} = \tilde{f}.\end{aligned}$$

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, \dots, e_n и e'_1, e'_2, \dots, 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 $f_{j_0 i_0} = 1$. Применим теорему 3.98 (1), получаем

$$\frac{1}{|G|} \sum_{g \in G} \psi_{jj_0}(g) \varphi_{i_0 i}(g^{-1}) = 0. \quad (1)$$

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

$$\operatorname{tr} f = \sum_{i=1}^n f_{ii} = \sum_{i', j'} \delta_{j'}^{i'} f_{j'i'},$$

где

$$\delta_{j'}^{i'} = \begin{cases} 1, & j' = i' \\ 0, & j' \neq i' \end{cases}$$

— символ Кронекера. Поскольку $\tilde{f} = \frac{\text{tr } f}{\dim V}$, то

$$\tilde{f}_{ji} = \delta_j^i \frac{\text{tr } f}{\dim V} = \frac{\delta_j^i}{\dim V} \sum_{i', j'} \delta_{j'}^{i'} f_{j'i'}.$$

Отсюда,

$$\frac{1}{|G|} \sum_{g \in G} \sum_{i'=1}^n \sum_{j'=1}^n \varphi_{jj'}(g) f_{j'i'} \varphi_{i'i}(g^{-1}) = \frac{1}{\dim V} \sum_{i'=1}^n \sum_{j'=1}^n \delta_j^i \delta_{j'}^{i'} f_{j'i'}.$$

Подставляя в качестве f матричные единицы, получаем

$$\frac{1}{|G|} \sum_{g \in G} \varphi_{jj_0}(g) \varphi_{i_0 i}(g^{-1}) = \begin{cases} \frac{\delta_j^{i_0}}{\dim V}, & j_0 = i_0 \\ 0, & j_0 \neq i_0 \end{cases}. \quad (2)$$

Пусть (φ, V) — представление группы G . Определим функцию $\chi_\varphi: G \rightarrow k$ соотношением $\chi_\varphi(g) = \text{tr } \varphi(g)$. 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) $\chi_\varphi(e) = \text{tr } \varphi(e) = \text{tr } E = \dim V$.

(2) $\chi_\varphi(hgh^{-1}) = \text{tr } \varphi(hgh^{-1}) = \text{tr}(\varphi(h)\varphi(g)\varphi(h)^{-1}) = \text{tr } \varphi(g) = \chi_\varphi(g)$.

(3) Пусть g имеет порядок m , т.е. $g^m = e$. Тогда $\varphi(g)^m = E$. Пусть $\lambda_1, \lambda_2, \dots, \lambda_n$ — собственные значения оператора $\varphi(g)$. Заметим, что $\lambda_i^m = 1$. Отсюда, $|\lambda_i| = 1$ и $\lambda_i^{-1} = \overline{\lambda_i}$. Тогда

$$\chi_\varphi(g^{-1}) = \text{tr } \varphi(g^{-1}) = \sum_{i=1}^n \lambda_i^{-1} = \sum_{i=1}^n \overline{\lambda_i} = \overline{\sum_{i=1}^n \lambda_i} = \overline{\chi_\varphi(g)}.$$

(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 $\text{tr } A_g = \text{tr } A'_g + \text{tr } A''_g$. Отсюда, $\chi_\varphi = \chi_{\varphi'} + \chi_{\varphi''}$. \square

Заметим, что если $\dim V = 1$, то $\chi_\varphi(g) = \varphi(g)$.

Рассмотрим множество функций $f: G \rightarrow \mathbb{C}$ 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 $f: G \rightarrow \mathbb{C}$ 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

$$\chi_\varphi(g) = \sum_{i=1}^n \varphi_{ii}(g), \quad \chi_\psi(g) = \sum_{j=1}^m \psi_{jj}(g).$$

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

$$\frac{1}{|G|} \sum_{g \in G} \varphi_{jj}(g) \varphi_{ii}(g^{-1}) = \frac{\delta_j^i}{\dim V}.$$

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. \square

СЛЕДСТВИЕ 3.101. Пусть (φ, V) — комплексное представление конечной группы и $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$ — разложение V в прямую сумму неприводимых инвариантных подпространств. Пусть $\varphi_1, \varphi_2, \dots, \varphi_k$ — соответствующие представления на V_1, V_2, \dots, V_k (т.е. ограничения φ на V_1, V_2, \dots, 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)

$$\chi_\varphi = \chi_{\varphi_1} + \chi_{\varphi_2} + \dots + \chi_{\varphi_k}.$$

Тогда

$$(\chi_\varphi, \chi_\psi) = (\chi_{\varphi_1}, \chi_\psi) + (\chi_{\varphi_2}, \chi_\psi) + \dots + (\chi_{\varphi_k}, \chi_\psi).$$

Согласно теореме 3.100 эта сумма состоит из нулей и единиц, причем число единиц совпадает с числом представлений (φ_i, V_i) изоморфных (ψ, W) . \square

СЛЕДСТВИЕ 3.102. Два представления с одним и тем же характером изоморфны.

ДОКАЗАТЕЛЬСТВО. Пусть (φ, V) и (ψ, W) — два представления над полем \mathbb{C} конечной группы. Пусть $V = V_1 \oplus V_2 \oplus \dots \oplus V_k$ и $W = W_1 \oplus W_2 \oplus \dots \oplus W_l$ — 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. \square

Пусть (φ, V) — комплексное представление конечной группы. Тогда

$$\chi_\varphi = m_1 \chi_{\varphi_1} + m_2 \chi_{\varphi_2} + \dots + m_k \chi_{\varphi_k},$$

где m_i — кратность с которой входит неприводимое представление (φ_i, V_i) в разложение (φ, V) . Тогда

$$(\chi_\varphi, \chi_\varphi) = m_1^2 + m_2^2 + \dots + m_k^2.$$

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 $\rho: G \rightarrow \text{GL}(W)$ 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, $\text{tr } R_a = 0$ 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, каждое неприводимое представление входит в регулярное с кратностью равной своей размерности. В частности, число различных неприводимых представлений у конечной группы, конечно. Пусть $(\varphi_1, V_1), (\varphi_2, V_2), \dots, (\varphi_s, V_s)$ — попарно неизоморфные неприводимые представления. Пусть $\chi_1, \chi_2, \dots, \chi_s$ — их характеры. Тогда

$$\chi_\rho = n_1 \chi_1 + n_2 \chi_2 + \dots + n_s \chi_s,$$

где $n_i = \dim V_i$. Отсюда

$$|G| = \chi_\rho(e) = n_1 \chi_1(e) + n_2 \chi_2(e) + \dots + n_s \chi_s(e) = n_1^2 + n_2^2 + \dots + n_s^2.$$

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, \dots, n_s пространств неприводимых линейных представлений связаны соотношением

$$|G| = n_1^2 + n_2^2 + \dots + n_s^2.$$

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

$$\begin{aligned} \varphi(h) \Phi_\Gamma \varphi(h)^{-1} &= \sum_{g \in G} \bar{\Gamma}(g) \varphi(h) \varphi(g) \varphi(h)^{-1} = \sum_{g \in G} \bar{\Gamma}(hgh^{-1}) \varphi(hgh^{-1}) = \\ &= \sum_{g' \in G} \bar{\Gamma}(g') \varphi(g') = \Phi_\Gamma. \end{aligned}$$

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

$$\begin{aligned} \lambda \chi_\varphi(e) &= \lambda \dim V = \text{tr}(\lambda I) = \sum_{g \in G} \bar{\Gamma}(g) \text{tr} \varphi(g) = \\ &= |G| \left(\frac{1}{|G|} \sum_{g \in G} \chi_\varphi(g) \bar{\Gamma}(g) \right) = |G| (\chi_\varphi, \Gamma). \end{aligned}$$

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 $\chi_1, \chi_2, \dots, \chi_s$ всех попарно неизоморфных неприводимых представлений конечной группы G образуют ортонормированный базис в X .

ДОКАЗАТЕЛЬСТВО. По теореме 3.100 система $\chi_1, \chi_2, \dots, \chi_s$ ортонормирована. Пусть Γ — центральная функция, ортогональная ко всем $\chi_1, \chi_2, \dots, \chi_s$, т.е. $(\chi_i, \Gamma) = 0$. Рассмотрим

$$\Phi_\Gamma^i = \sum_{g \in G} \bar{\Gamma}(g) \varphi_i(g),$$

где φ_i — представление с характером χ_i . Согласно лемме 3.106 $\Phi_\Gamma^i = 0$. Пусть φ — произвольное комплексное представление. Тогда по теореме Машке (см. 3.94)

$$\varphi = m_1 \varphi_1 + m_2 \varphi_2 + \dots + m_s \varphi_s.$$

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, $\Gamma = 0$. \square

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, \dots, f_r также образуют базис. По известной теореме из линейной алгебры, число векторов базиса инвариантно, т.е. $r = s$. \square

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.*