

12-1. № задача № 12 (Б) (Б)

KB № 12 (Б) (Б) (19 окт 2011 г.)

1) $O(a) = n < \infty$

$$a^k = e \Leftrightarrow k = nq$$

2) $k = nq + r, 0 < r < n \Rightarrow$

$$a^k = (a^n)^q \cdot a^r \neq e$$

(но имеем, что $\{e = a^0, a, \dots, a^{n-1}\}$ все элементы различны).

2) $\Rightarrow 1.4.14$

3) $\Rightarrow 1.4.15$

4) $\Rightarrow 1.4.16$

5) $\Rightarrow 1.4.28$ Т(6), 6-адреса

6) $\Rightarrow 1.4.29 \equiv 1.4.20.$

2) Найдите все элементы наибольшего порядка в S_{10} , S_{11} , S_{12} и в A_{10} .

3) Найти порядки элементов 2, 3 и 7 в мультипликативной группе $\mathbb{Z}_{11}^* = \mathbb{Z}_{11} \setminus \{0\}$ поля вычетов \mathbb{Z}_{11} .

KB 1 Теорема 1.4.14. Пусть G — конечная абелева группа. Тогда:

- 1) произведение всех элементов группы G , порядки которых отличны от 2, равно единичному элементу;
- 2) если группа G содержит элемент порядка 2, то произведение всех элементов группы G равно произведению всех элементов порядка 2 группы G .

Доказательство. Если $e \neq x \in G$, то $O(x) = 2$ тогда и только тогда, когда $x = x^{-1}$. Если $O(x) > 2$, то $O(x^{-1}) = O(x) > 2$, и $x \neq x^{-1}$. Так как G — абелева группа, то:

$$\prod_{\substack{g \in G \\ O(g) \neq 2}} g = \prod_{\substack{\{x, x^{-1}\} \\ O(x) \neq 2}} x \cdot x^{-1} = e;$$

$$\prod_{g \in G} g = \left(\prod_{\substack{x \in G \\ O(x)=2}} x \right) \cdot \left(\prod_{\substack{y \in G \\ O(y) \neq 2}} y \right) = \prod_{\substack{x \in G \\ O(x)=2}} x. \quad \square$$

KB 3 Теорема 1.4.15 (теорема Вилсона). Если $p \in \mathbb{N}$, то p — простое число тогда и только тогда, когда:

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказательство.

1) Пусть $G = (\mathbb{Z}_p \setminus \{0\}, \cdot) = \mathbb{Z}_p^*$ — мультипликативная группа поля вычетов \mathbb{Z}_p . Если $a \in \mathbb{Z}_p^*$ и $O(a) = 2$, то $a^2 \equiv 1 \pmod{p}$, следовательно, $a^2 - 1 = (a-1)(a+1)$ делится на p , поэтому или $a \equiv 1 \pmod{p}$, или $a \equiv -1 \pmod{p}$. В силу теоремы 1.4.14 в \mathbb{Z}_p

$$1 \cdot 2 \cdot \dots \cdot (p-1) \equiv 1 \cdot (-1) \equiv -1 \pmod{p}.$$

KB 4 2) Если $p = k \cdot l$, $k, l \in \mathbb{N}$, $1 < k < p$, $1 < l < p$, то $(p-1)! \equiv 0 \pmod{k}$. Если $(p-1)! \equiv -1 \pmod{p}$, то $(p-1)! + 1 = p \cdot q = k \cdot l \cdot q$, что приводит к противоречию. □

KB 4 Теорема 1.4.16. Пусть G — группа, $|G| = 2k$. Тогда G содержит элемент g порядка $O(g) = 2$.

Доказательство. Пусть для всех $e \neq g \in G$ имеем $O(g) > 2$. Тогда $g \neq g^{-1}$, $O(g^{-1}) = O(g)$, поэтому число неединичных элементов группы G чётно, а $|G|$ — нечётное число. Получили противоречие. □

Замечание 1.4.17. В дальнейшем мы рассмотрим глубокое развитие этого утверждения: случаи, когда верно обращение теоремы Лагранжа, а именно теоремы Коши и Силова.

Доказательство.

1) Если $a, b \in T(G)$, $O(a) = k < \infty$, $O(b) = l < \infty$, то

$$(ab)^{kl} = a^{kl}b^{kl} = (a^k)^l(b^l)^k = e \cdot e = e.$$

Поэтому $O(ab) < \infty$, и следовательно, $ab \in T(G)$.

2) Так как $O(a^{-1}) = O(a) < \infty$ для $a \in T(G)$, то $a^{-1} \in T(G)$. \square

Замечание 1.4.29. Как мы видели в примере 1.4.20 1) совокупность элементов конечного порядка $T(G)$ некоммутативной группы G может не быть подгруппой группы G .

Замечание 1.4.30. Важным инвариантом конечной группы G является её *спектр*

$$\omega(G) = \{n \in \mathbb{N} \mid \exists x \in G, O(x) = n\},$$

другими словами, множество порядков её элементов.

Конечная группа G называется *распознаваемой по спектру*, если любая конечная группа H с условием равенства спектров $\omega(H) = \omega(G)$ изоморфна группе G . В задаче о характеризации распознаваемых по спектру конечных групп одна из интересных проблем заключается в выяснении распознаваемости по спектру конечных простых групп.

Группа G называется *периодической*, если каждый элемент g группы G имеет конечный порядок $O(g) < \infty$, и *группой без кручения*, если каждый элемент $e \neq g \in G$ имеет бесконечный порядок, $O(g) = \infty$.

1.5. Подгруппы группы

Конец лекции 11

Лемма 1.5.1. Для непустого подмножества H группы G следующие условия эквивалентны:

- 1) H является группой относительно исходной операции в группе G ;
- 2) подмножество H удовлетворяет следующим двум условиям:
 - а) если $h_1, h_2 \in H$, то $h_1h_2 \in H$;
 - б) если $h \in H$, то $h^{-1} \in H$.

Непустое подмножество H группы G , удовлетворяющее эквивалентным условиям 1) и 2), называется *подгруппой группы G* .

Доказательство.

1) \Rightarrow 2). Если $h_1, h_2 \in H$, то, поскольку операция определена на H (т. е. не выводится из H), имеем $h_1h_2 \in H$, т. е. 2а).

Если e' — нейтральный элемент группы H , то $e' \cdot e' = e'$. Умножая в группе обе стороны этого равенства на $(e')^{-1}$, получаем $e' = e$ (здесь e — нейтральный элемент группы G).

Если \underline{h}^{-1} — обратный элемент для элемента $\underline{h} \in H$ в группе H , то $\underline{h}^{-1} \cdot \underline{h} = e' = e = \underline{h} \cdot \underline{h}^{-1}$, т. е. $\underline{h}^{-1} = \underline{h}^{-1} \in H$ (условие 2б)).

2) \Rightarrow 1). Условие 2а) показывает, что операция определена на множестве H . Конечно, она ассоциативна. Далее, для $\underline{h} \in H$ в силу 2б) $\underline{h}^{-1} \in H$, и поэтому в силу 2а) $e = \underline{h} \cdot \underline{h}^{-1} \in H$. Ясно, что e — нейтральный элемент в H , а \underline{h}^{-1} — обратный элемент для \underline{h} в H . Итак, H — группа относительно операции, индуцированной операцией группы G . \square

М-4

Лекция №12 (13)

(19 октября 2011 г.)

1.4. Порядок элемента группы

33

Замечание 1.4.26. Для различных разложений

$$n = O(a) = rs = r's', \quad (r, s) = 1 = (r', s'),$$

канонические представления

$$\begin{aligned} a &= bc = b'c', \quad bc = cb, \quad b'c' = c'b', \\ O(b) &= r, \quad O(c) = s, \quad O(b') = r', \quad O(c') = s', \end{aligned}$$

различны. Действительно, для

$$\begin{aligned} O(a) &= 30 = (2 \cdot 3) \cdot 5 = 2 \cdot (3 \cdot 5), \\ r &= 2 \cdot 3, \quad s = 5, \quad (r, s) = 1, \quad r' = 2, \quad s' = 3 \cdot 5, \quad (r', s') = 1, \end{aligned}$$

имеем для $b = a^5$, $c = a^{24}$, $b' = a^{15}$, $c' = a^{28}$: $n = rs = r's'$, $a = bc = b'c'$, $bc = cb$, $b'c' = c'b'$, $O(b) = r = 6$, $O(c) = s = 5$, $O(b') = r' = 2$, $O(c') = s' = 15$. \square

Упражнение 1.4.27. Пусть G — группа, $a, b \in G$, $ab = ba$, $O(a) = m$, $O(b) = n$. Тогда группа G содержит такой элемент c , что $O(c) = \text{НОК}(m, n)$. Действительно, $H = \langle a, b \rangle$ — конечная абелева группа. Пусть $H = \bigoplus_p H_p$ — разложение конечной абелевой группы в прямую сумму конечного числа p -примарных компонент, p — простое число. Если

$$\begin{aligned} a &= \sum_p a_p, \quad a_p \in H_p, \quad O(a_p) = p^{i_p}, \\ b &= \sum_p b_p, \quad b_p \in H_p, \quad O(b_p) = p^{j_p}. \end{aligned}$$

Так как

$$(O(a_p), O(a_q)) = 1 = (O(b_p), O(b_q))$$

для различных простых чисел p и q , то

$$m = O(a) = \prod_p p^{i_p}, \quad n = O(b) = \prod_p p^{j_p}.$$

Тогда

$$\text{НОК}(m, n) = \prod_p p^{\max(i_p, j_p)}.$$

Выберем

$$c_p = \begin{cases} a_p, & \text{если } i_p \geq j_p, \\ b_p, & \text{если } j_p > i_p. \end{cases}$$

Тогда $c_p \in H_p$ и $O(c_p) = p^{\max(i_p, j_p)}$. Если $c = \sum_p c_p \in \bigoplus_p H_p = H \subset G$, $O(c) = \prod_p p^{\max(i_p, j_p)} = \text{НОК}(m, n)$. \square

Теорема 1.4.28. В любой коммутативной группе G совокупность всех элементов конечного порядка

$$T(G) = \{g \in G \mid O(g) < \infty\}$$

образует подгруппу, называемую периодической частью $T(G)$ абелевой группы G .

Доказательство.

1) Если $a, b \in T(G)$, $O(a) = k < \infty$, $O(b) = l < \infty$, то

$$(ab)^{kl} = a^{kl}b^{kl} = (a^k)^l(b^l)^k = e \cdot e = e.$$

Поэтому $O(ab) < \infty$, и следовательно, $ab \in T(G)$.

2) Так как $O(a^{-1}) = O(a) < \infty$ для $a \in T(G)$, то $a^{-1} \in T(G)$. \square

Замечание 1.4.29. Как мы видели в примере 1.4.20 1) совокупность элементов конечного порядка $T(G)$ некоммутативной группы G может не быть подгруппой группы G .

Замечание 1.4.30. Важным инвариантом конечной группы G является её *спектр*

$$\omega(G) = \{n \in \mathbb{N} \mid \exists x \in G, O(x) = n\},$$

другими словами, множество порядков её элементов.

Конечная группа G называется *распознаваемой по спектру*, если любая конечная группа H с условием равенства спектров $\omega(H) = \omega(G)$ изоморфна группе G . В задаче о характеризации распознаваемых по спектру конечных групп одна из интересных проблем заключается в выяснении распознаваемости по спектру конечных простых групп.

Группа G называется *периодической*, если каждый элемент g группы G имеет конечный порядок $O(g) < \infty$, и *группой без кручения*, если каждый элемент $e \neq g \in G$ имеет бесконечный порядок, $O(g) = \infty$.

1.5. Подгруппы группы

Лемма 1.5.1. Для непустого подмножества H группы G следующие условия эквивалентны:

- 1) H является группой относительно исходной операции в группе G ;
- 2) подмножество H удовлетворяет следующим двум условиям:
 - a) если $h_1, h_2 \in H$, то $h_1h_2 \in H$;
 - б) если $h \in H$, то $h^{-1} \in H$.

Непустое подмножество H группы G удовлетворяющее эквивалентным условиям 1) и 2), называется *подгруппой группы G* .

Доказательство.

1) \Rightarrow 2). Если $h_1, h_2 \in H$, то, поскольку операция определена на H (т. е. не выводит из H), имеем $h_1h_2 \in H$, т. е. 2a).

Если e' — нейтральный элемент группы H , то $e' \cdot e' = e'$. Умножая в группе обе стороны этого равенства на $(e')^{-1}$, получаем $e' = e$ (здесь e — нейтральный элемент группы G).

Если \tilde{h}^{-1} — обратный элемент для элемента $\tilde{h} \in H$ в группе H , то $\tilde{h}^{-1} \cdot \tilde{h} = e' = e = \tilde{h} \cdot \tilde{h}^{-1}$, т. е. $\tilde{h}^{-1} = \tilde{h} \in H$ (условие 2б)).

2) \Rightarrow 1). Условие 2а) показывает, что операция определена на множестве H . Конечно, она ассоциативна. Далее, для $h \in H$ в силу 2б) $h^{-1} \in H$, и поэтому в силу 2а) $e = h \cdot h^{-1} \in H$. Ясно, что e — нейтральный элемент в H , а h^{-1} — обратный элемент для h в H . Итак, H — группа относительно операции, индуцированной операцией группы G .

Замечание 1.5.2. Так как подгруппа H группы G содержит единицу e группы G , то из $|H| = 1$ следует, что $H = \{e\}$. Если же G — конечная группа, $H \subseteq G$, $|H| = |G|$, то $H = G$. \square

Замечание 1.5.3. Пусть G — группа и $\emptyset \neq H \subseteq G$.

1) H — подгруппа тогда и только тогда, когда $h_1 h_2^{-1} \in H$ для всех $h_1, h_2 \in H$. Действительно, если H — подгруппа и $h_1, h_2 \in H$, то $h_2^{-1} \in H$ и поэтому $h_1 h_2^{-1} \in H$. Если же $h_1 h_2^{-1} \in H$ для всех $h_1, h_2 \in H$, то $e = h_1(h_1)^{-1} \in H$, $h_2^{-1} = e h_2^{-1} \in H$, $h_1 h_2 = h_1(h_2^{-1})^{-1} \in H$. Итак, H — подгруппа. \square

2) Если подмножество H в группе G конечно, $|H| < \infty$, и замкнуто относительно операции в группе G , то H является подгруппой. Действительно, если $h \in H$, то $\{h^i \mid i \in \mathbb{N}\} \subseteq H$, $|H| < \infty$, и поэтому $h^i = h^j$ для некоторых $j > i$. Тогда $e = h^{j-i}$. Итак, H — конечный подмонOID группы G . В силу следствия 1.2.15 H — подгруппа. \square

Следствие 1.5.4. Если G — группа, $\emptyset \neq F \subset H \subset G$, H — подгруппа группы G , F — подгруппа группы H , то F — подгруппа группы G . \square

Теорема 1.5.5. Пусть G — группа, $\{H_i \mid i \in I\}$ — любое семейство подгрупп группы G . Тогда их пересечение $H = \bigcap_{i \in I} H_i$ также является подгруппой.

Доказательство.

1) Если $h_1, h_2 \in H = \bigcap_{i \in I} H_i$, то $h_1, h_2 \in H_i$ для каждого i . Так как H_i — подгруппа, то $h_1 h_2 \in H_i$ для каждого i , и поэтому $h_1 h_2 \in \bigcap_{i \in I} H_i = H$.

2) Если $h \in H = \bigcap_{i \in I} H_i$, то $h \in H_i$ для каждого i . Так как H_i — подгруппа, то $h^{-1} \in H_i$ для каждого i , и поэтому $h^{-1} \in \bigcap_{i \in I} H_i = H$.

Итак, $H = \bigcap_{i \in I} H_i$ — подгруппа группы G . \square

Следствие 1.5.6. Пусть X — непустое подмножество группы G . Тогда:

- 1) существует подгруппа H , являющаяся наименьшей среди подгрупп, содержащих подмножество X (эта подгруппа называется подгруппой, порождённой подмножеством X , она обозначается через $\langle X \rangle$);
- 2) подгруппа $\langle X \rangle$ состоит из всех элементов группы G , имеющих вид $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$, где $x_i \in X$, $k_i = \pm 1$, $n \geq 0$.

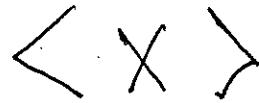
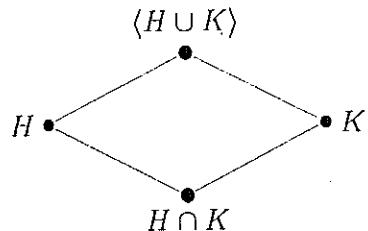
Доказательство.

1) Множество всех подгрупп H_i , $i \in I$, содержащих подмножество X , не пусто, ему принадлежит сама группа G . Ясно, что $X \subseteq H = \bigcap_{i \in I} H_i$ и H — наименьшая подгруппа среди всех H_i , $i \in I$.

2) Указанные элементы лежат в $\langle X \rangle$, в то же время они сами образуют подгруппу, содержащую подмножество X . \square

10-7

Следствие 1.5.7 (решётка подгрупп). Пусть G — группа, $\mathcal{L}(G)$ — частично упорядоченное множество (с отношением включения) всех её подгрупп. Тогда $\mathcal{L}(G)$ является решёткой, т. е. для любых подгрупп $H, K \in \mathcal{L}(G)$ их пересечение $H \cap K$ является точной нижней гранью для пары H и K , а $\langle H \cup K \rangle$ (подгруппа, порождённая объединением H и K) является точной верхней гранью пары H и K :



Примеры 1.5.8.

1. Чётные числа $2\mathbb{Z}$ — подгруппа в группе целых чисел $(\mathbb{Z}, +)$.
2. $\mathbb{Z} \subset (\mathbb{Q}, +)$, $\mathbb{Q} \subset (\mathbb{R}, +)$, $\mathbb{R} \subset (\mathbb{C}, +)$ — подгруппы.
3. $A_n \subset S_n$ (чётные подстановки являются подгруппой в группе всех подстановок).
4. Если K — поле, то через $K^* = \{k \in K \mid k \neq 0\}$ обозначим его мультипликативную группу. Тогда $\mathbb{Q}^* \subset (\mathbb{R}^*, \cdot)$, $\mathbb{R}^* \subset (\mathbb{C}^*, \cdot)$, $\{1, -1\} \subset (\mathbb{Q}^*, \cdot)$, $T = \{z \in \mathbb{C} \mid |z| = 1\} \subset (\mathbb{C}^*, \cdot)$, $G = \sqrt[n]{1} \subset T \subset C^*$ — подгруппы.
5. $SL_n(K) \subset GL_n(K)$, $O_n(K) \subset GL_n(K)$ — подгруппы линейной группы $GL_n(K)$.
6. Если R — кольцо,

$$T_n(R) = \{A = (a_{ij}) \in GL_n(R) \mid a_{ij} = 0 \text{ для } i > j\} —$$

совокупность обратимых верхнетреугольных матриц, то $T(R)$ — подгруппа линейной группы $GL_n(R)$.

7. В любой группе G имеем наименьшую подгруппу $H = \{e\}$ (и наибольшую подгруппу $H = G$). Если $H < G$, то подгруппа H называется *собственной*.
8. $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$.
9. $\mathbb{Q}^* = \left\langle \left\{ \frac{1}{p} \mid p \text{ — простое} \right\} \cup \{-1\} \right\rangle$.
10. $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle = \langle (1\ 2), (1\ 3) \rangle$.

Kb!

Задача 1.5.9. Группа, имеющая лишь конечное число подгрупп, конечна.

Упражнение 1.5.10.

- 1) Пусть H и K — подгруппы группы G . Тогда $H \cup K$ — подгруппа в том и только в том случае, если либо $H \subseteq K$, либо $K \subseteq H$.
- 2) Никакая группа G не является объединением $H \cup K$ двух собственных подгрупп $H \subset G$, $K \subset G$.

- 3) Привести пример группы G , являющейся объединением трёх собственных подгрупп.
- 4) Если H — подгруппа группы G , $x \in G$, то
- $x^{-1}Hx$ — подгруппа группы G (подгруппы H и $x^{-1}Hx$ называются *сопряжёнными*);
 - подгруппы H и $x^{-1}Hx$ равномощны.
- 5) Если H — подгруппа группы G , $g \in G$, $O(g) = n$, $g^m \in H$, $(m, n) = 1$, то $g \in H$. Действительно, пусть $1 = mu + nv$, $u, v \in \mathbb{Z}$, тогда $g = g^{mu+nv} = (g^m)^u(g^n)^v = (g^m)^u \in H$. \square

Циклические подгруппы

Рассмотрим строение подгрупп, порождённых одним элементом.

Пусть a — элемент группы G . Рассмотрим в G следующее подмножество:

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

$\langle a \rangle$

(т. е. совокупность всех целых степеней элемента a).

Лемма 1.5.11.

- 1) $\langle a \rangle$ является коммутативной подгруппой группы G , называемой циклической подгруппой, порождённой элементом a ;
- 2) $|\langle a \rangle| = O(a)$ (т. е. число элементов в подгруппе $\langle a \rangle$ равно порядку элемента a).

Доказательство.

1) Для $m, n \in \mathbb{Z}$

$$a^m a^n = a^{m+n} \in \langle a \rangle; \quad (a^n)^{-1} = a^{-n} \in \langle a \rangle.$$

Таким образом, для $\langle a \rangle$ выполнены условия предыдущей леммы, т. е. $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ — подгруппа группы G . Так как

$$a^m a^n = a^{m+n} = a^n a^m,$$

то $\langle a \rangle$ — коммутативная группа.

2) Если $O(a) = \infty$, то

$$\langle a \rangle = \{\dots, a^{-1}, e, a, \dots\},$$

при этом в ряду целых степеней элемента a все элементы различны, т. е. $|\langle a \rangle| = \infty$. Если же $O(a) = n < \infty$, то, как мы отметили ранее,

$$\langle a \rangle = \{e, a, \dots, a^{n-1}\}$$

и

$$|\langle a \rangle| = n = O(a). \quad \square$$

Примеры 1.5.12 (примеры циклических групп). *ноги*

1. Если $G = \mathbb{Z}$ и $a = 2$, то

$$\langle a \rangle = \{n2 \mid n \in \mathbb{Z}\} = 2\mathbb{Z}$$

(все чётные числа).

2. Если $G = \mathrm{GL}_2(\mathbb{R})$ и

$$a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

то

$$\langle a \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

3. Если $G = \{1, i, -1, -i\}$ — группа комплексных корней четвёртой степени из 1, то $\langle i \rangle = G$, $\langle -1 \rangle = \{1, -1\}$, $\langle -i \rangle = G$.

4. Если $G = S_3$ и

$$a = (1 \ 2 \ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

то

$$\langle a \rangle = \left\{ e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

1.6. Циклические группы

Группа G называется *циклической*, если найдётся такой элемент $a \in G$, что $\langle a \rangle = G$, т. е. все элементы группы G являются (целыми) степенями этого элемента a , называемого в этом случае *циклическим образующим* группы G . Если $O(a) = n < \infty$, то $G = \langle a \rangle$ — *циклическая группа из n элементов*; если же $O(a) = \infty$, то $G = \langle a \rangle$ — *бесконечная (счётная!) циклическая группа*.

Замечание 1.6.1. Любая циклическая группа $G = \langle a \rangle$ является конечной или счётной коммутативной группой. Поэтому любая некоммутативная группа не является циклической и любая несчётная группа не является циклической группой.

Примеры 1.6.2 (примеры циклических групп).

- $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ (это показывает, что циклических образующих может быть много!).
- Группа подстановок S_n является циклической тогда и только тогда, когда $n < 3$. Действительно, $S_1 = \langle e \rangle$, $S_2 = \langle (1 \ 2) \rangle$, при $n \geq 3$ группа S_n некоммутативна, поэтому она не может быть циклической.
- Группа действительных чисел $(\mathbb{R}, +)$ не является счётной, поэтому она не является циклической.
- Показать, что счётная группа $(\mathbb{Q}, +)$ рациональных чисел не является циклической, однако является *локально циклической группой* (это означает, что каждое конечное подмножество порождает циклическую группу).
- Группа $G = \sqrt[n]{1}$ комплексных корней из 1 является циклической группой из n элементов. Действительно,

$$G = \sqrt[n]{1} = \left\{ \varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \mid k = 0, 1, \dots, n-1 \right\}$$

и $G = \langle a \rangle$ для $a = \varepsilon_1 = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$, поскольку $\varepsilon_k = a^k$ для $k = 0, 1, \dots, n-1$.

1.6. Циклические группы

Упражнение 1.6.3.

- ✓ 1. Пусть $G = \mathbb{Z}_{11} \setminus \{0\} = \{1, 2, \dots, 10\}$ — ненулевые вычеты в кольце \mathbb{Z}_{11} . Тогда: (G, \cdot) — группа, при этом $G = \langle 2 \rangle$.
2. Пусть $1 < m \in \mathbb{N}$. При каких условиях на m ненулевые элементы $(G, \cdot) = \{1, 2, \dots, m-1\} \subset \mathbb{Z}_m$ в кольце вычетов по модулю m образуют циклическую группу?

Лемма 1.6.4. Если $G = \langle a \rangle$ — конечная циклическая группа порядка n (т. е. $O(a) = n$), $b = a^k \in G$, $k \in \mathbb{Z}$, то элемент b является образующим группы G (т. е. $G = \langle a \rangle = \langle b \rangle$) тогда и только тогда, когда числа k и n взаимно просты.

Доказательство. Так как $|\langle b \rangle| = O(b)$, то $G = \langle a \rangle = \langle b \rangle$ тогда и только тогда, когда

$$O(b) = |\langle b \rangle| = |\langle a \rangle| = O(a).$$

Учитывая, что $O(b) = \frac{n}{d}$, где $d = \text{НОД}(k, n)$, мы видим, что $O(b) = O(a) = n$ тогда и только тогда, когда $d = 1$, т. е. числа k и n взаимно просты. \square

Замечание 1.6.5. Пусть $G = \langle a \rangle$, $|G| = O(a) = n < \infty$. Если мы знаем какой-нибудь образующий a конечной циклической группы G из n элементов, то все циклические образующие группы G имеют вид $b = a^k$, где $1 \leq k \leq n-1$ и k взаимно просто с n . Число таких чисел k обозначается через $\varphi(n)$ (функция Эйлера $\varphi(n)$ часто возникает в теории чисел и в комбинаторике, см. с. 22).

Задача 1.6.6. Показать, что при $n > 30$ число $\varphi(n)$ строго больше числа делителей числа n .

Указание. Пусть $\tau(n)$ — число делителей числа n . Для простого числа p рассмотрим отношение

$$\frac{\tau(p^k)}{\varphi(p^k)} = \frac{k+1}{p^{k-1}(p-1)}$$

и воспользуемся тем, что $\frac{\tau(n)}{\varphi(n)}$ — мультипликативная функция.

Теорема 1.6.7 (о первообразных комплексных корнях из 1). Пусть

$$G = \{e = \varepsilon_0, \varepsilon_1 = \varepsilon, \varepsilon_2 = \varepsilon^2, \dots, \varepsilon_{n-1} = \varepsilon^{n-1}\} —$$

группа комплексных корней n -й степени из 1,

$$\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}, \quad \varepsilon_k = \varepsilon^k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}.$$

Так как $G = \langle \varepsilon \rangle$ — циклическая группа с образующим ε , то $\varepsilon_k = \varepsilon^k$ является образующим группы G (такой корень называется первообразным: все другие корни являются его степенями) тогда и только тогда, когда k взаимно просто с n . Число первообразных корней из 1 степени n равно $\varphi(n)$.

Доказательство вытекает из предыдущего следствия, применённого к группе комплексных корней n -й степени из 1. \square

Пример 1.6.8.

- 1) Для $n = 4$ все первообразные корни 4-й степени из 1: $i, -i$.
 2) Для $n = 8$ из всех комплексных корней 8-й степени из 1

$$1, \varepsilon, \varepsilon^2, \dots, \varepsilon^7,$$

где

$$\varepsilon = \cos \frac{2\pi}{8} + i \sin \frac{2\pi}{8} = e^{\frac{\pi}{4}i},$$

первообразными корнями являются

$$\varepsilon, \varepsilon^3, \varepsilon^5, \varepsilon^7.$$

- 3) Для $n = 12$ все первообразные корни 12-й степени из 1:

$$\varepsilon, \varepsilon^5, \varepsilon^7, \dots, \varepsilon^{11},$$

где

$$\varepsilon = \cos \frac{2\pi}{12} + i \sin \frac{2\pi}{12} = e^{\frac{\pi}{6}i}.$$

Теорема 1.6.9 (о цикличности подгрупп циклической группы). Пусть $G = \langle a \rangle$ — циклическая группа, a — один из её циклических образующих. Любая подгруппа H циклической группы G является циклической, $H = \langle b \rangle$ (при этом образующий в подгруппе H можно выбрать в виде $b = a^k$, где $k \geq 0$).

Доказательство. Пусть $G = \langle a \rangle$ — циклическая группа, a — её циклический образующий, $\emptyset \neq H \subseteq G$ — подгруппа.

Случай 1. $|H| = 1$, т. е. $H = \{e = a^0\} = \langle e \rangle$.

Случай 2. $|H| > 1$. Пусть $e \neq a^t \in H$, т. е. $0 \neq t \in \mathbb{Z}$. Тогда

$$a^{-t} = (a^t)^{-1} \in H.$$

Поэтому или $t > 0$, или $-t > 0$, т. е. в H содержится некоторая натуральная степень элемента a . Таким образом, среди положительных степеней $a^t \in H$, $t > 0$,

$$\{t \in \mathbb{N} \mid a^t \in H\} \subset \mathbb{N},$$

есть наименьшая степень $k > 0$. Так как $a^k \in H$, то $\langle a^k \rangle \subseteq H$.

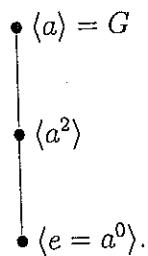
Для любого элемента $h \in H$, поскольку $H \subseteq G = \langle a \rangle$, имеем $h = a^l$, $l \in \mathbb{Z}$. Пусть $l = kq + r$, $0 \leq r < k$. Тогда $h = a^l = (a^k)^q a^r$, т. е. $a^r = a^l (a^k)^{-q} \in H$, поскольку $a^l \in H$, $a^k \in H$ (а тогда и $(a^k)^{-q} \in H$). В силу выбора числа k остаётся возможность $r = 0$, т. е. $l = kq$. Но тогда $h = a^l = (a^k)^q$, т. е. H является циклической группой с образующим a^k , $H = \langle a^k \rangle$. \square

Замечание 1.6.10.

1. Несколько позже (имея в своём распоряжении теорему Лагранжа) мы дадим (см. ??) явное описание решётки подгрупп циклической группы.

1.7. Смежные классы по подгруппе

- ✓ 2. Все подгруппы группы $(\mathbb{Z}, +)$ имеют вид $\mathbb{Z}n$, где $n \in \mathbb{N} \cup \{0\}$.
3. Диаграмма Хассе (решётка) подгрупп циклической группы $G = \langle a \rangle$ ($\cong \mathbb{Z}_4$) порядка $4 = |G| = O(a)$ имеет вид



4. Число элементов порядка p^m в циклической группе порядка p^n ($1 \leq m \leq n$, p — простое число) равно $p^m - p^{m-1}$.

Задача 1.6.11 (утверждение, весьма полезное в алгебраической теории кодирования). Пусть K — любое конечное поле. Тогда его мультипликативная группа $K^* = (K \setminus \{0\}, \cdot)$ — циклическая группа.

Упражнение 1.6.12. Привести пример неабелевой группы, в которой каждая из собственных подгрупп циклическая: рассмотрите группу S_3 .

Упражнение 1.6.13. В группе рациональных чисел $(\mathbb{Q}, +)$ каждая конечно порождённая подгруппа является циклической (такая группа называется локально циклической), при этом группа \mathbb{Q} не является циклической: если $\mathbb{Q} = \left\langle q = \frac{m}{n} \right\rangle$, то $\frac{1}{2n} = rq$, $r \in \mathbb{Z}$, поэтому $\frac{1}{2n} = \frac{rm}{n}$, и тогда $1 = 2rm$ для $r, m \in \mathbb{Z}$, что приводит к противоречию.

Упражнение 1.6.14. Пусть p — простое число, \mathbb{Z}_{p^∞} — группа всех комплексных корней из 1 степени p^n для всех натуральных n . Покажите, что любая собственная подгруппа группы \mathbb{Z}_{p^∞} — конечная циклическая группа, а также что любая нетривиальная фактор-группа группы \mathbb{Z}_{p^∞} изоморфна \mathbb{Z}_{p^∞} . В группе \mathbb{Z}_{p^∞} любое конечное подмножество порождает циклическую группу.

Указание. $\{e\} \subseteq C_p \subseteq C_{p^2} \subseteq \dots \subseteq C_{p^n} \subseteq \dots \subseteq \mathbb{Z}_{p^\infty}$, где $C_{p^n} = \mathbb{Z}_{p^n}$ — циклическая группа всех корней степени p^n из 1, $\mathbb{Z}_{p^\infty} = \bigcup_{n \geq 1} C_{p^n}$.

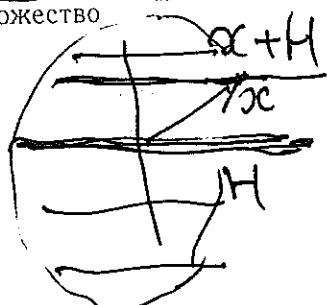
1.7. Смежные классы по подгруппе

Пусть G — группа, H — подгруппа группы G , $x \in G$. Левым смежным классом группы G по подгруппе H , порождённым элементом x , называется множество

$$xH = \{xh \mid h \in H\}.$$

Аналогично, правый смежный класс определяется как

$$Hx = \{hx \mid h \in H\}.$$



12-13

Пример 1.7.1. Пусть $G = \mathbb{R}^2$ с операцией сложения, $H = \{(a, 0) \mid a \in \mathbb{R}\}$, $x = (1, 1)$. Тогда

$$x + H = \{(a, b) \in \mathbb{R}^2 \mid b = 1\}.$$

Все смежные классы группы \mathbb{R}^2 по H — это все прямые, параллельные прямой H .

Пример 1.7.2. Пусть $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ — группа всех комплексных чисел, отличных от нуля, с операцией умножения, $H \equiv T = \{z \in \mathbb{C} \mid |z| = 1\}$, $x = 1+i$. Тогда

$$xH = \{w \in \mathbb{C} \mid |w| = \sqrt{2}\}.$$

Все смежные классы группы G по H в этом случае — это подмножества вида $\{w \in \mathbb{C} \mid |w| = r \neq 0\}$, т. е. концентрические окружности положительного радиуса с центром в нуле.

Пример 1.7.3. Пусть $G = S_3$,

$$H = \langle(1 2)\rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\},$$

$$x = (1 3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Тогда:

$$xH = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 3), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1 2 3) \right\};$$

$$Hx = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 3), \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 3 2) \right\}.$$

Замечание 1.7.4.

1) Мы видим в этом примере, что $xH \neq Hx$ (т. е. правый и левый смежные классы по подгруппе, порождённые элементом x , могут не совпадать).

2) Если $x = e$ — нейтральный элемент группы G , то $eH = H = He$.

3) $xH = H$ тогда и только тогда, когда $x \in H$; $Hx = H$ тогда и только тогда, когда $x \in H$.

4) Пусть H и K — подгруппы группы G , $x \in G$.

a) $x(H \cap K) = xH \cap xK$; $(H \cap K)x = Hx \cap Kx$. Действительно: если $g \in H \cap K$, то $xg \in xH \cap xK$, поэтому

$$x(H \cap K) \subseteq xH \cap xK;$$

если $xh = xk \in xH \cap xK$, $h \in H$, $k \in K$, то $h = k \in H \cap K$, и поэтому $xh = xk \in x(H \cap K)$, поэтому

$$x(H \cap K) \supseteq xH \cap xK.$$

Второе равенство проверяется аналогично.



(12-14-15)

б) Постановка каждому левому смежному классу $x(H \cap K)$ в соответствие пары левых смежных классов (xH, xK) является корректным инъективным отображением. Действительно, если $x(H \cap K) = y(H \cap K)$, то $y = xd$, где $d \in H \cap K$, и поэтому

$$xH = xdH = yH, \quad xK = xdK = yK$$

(т. е. наше соответствие определено корректно). Если же $(xH, xK) = (x'H, x'K)$, $x, x' \in G$, то $xH = x'H$, $xK = x'K$, поэтому $x^{-1}x' \in H \cap K$, и следовательно,

$$x(H \cap K) = x'(H \cap K)$$

(т. е. наше отображение инъективно).

1.8. Разбиение группы на смежные классы, теорема Лагранжа

 Лемма 1.8.1 (о восстановлении подгруппы H по любому её левому смежному классу aH (или по правому смежному классу Ha) в группе G). Пусть G — группа, H — её подгруппа, $a \in G$. Тогда:

-  1) $H = (aH)^{-1}(aH) = \{u^{-1}v \mid u, v \in aH\}$;
- 2) $H = (Ha)(Ha)^{-1} = \{uv^{-1} \mid u, v \in Ha\}$.

 *Доказательство.*

1a) Если $h \in H$, то

$$h = a^{-1}(ah) \in (aH)^{-1}(aH).$$

Итак, $H \subseteq (aH)^{-1}(aH)$.

1б) Если $z = (ax)^{-1}ay \in (aH)^{-1}(aH)$, $x, y \in H$, то

$$z = (ax)^{-1}ay = x^{-1}a^{-1}ay = x^{-1}y \in H.$$

Итак, $(aH)^{-1}(aH) \subseteq H$.

2а) Если $h \in H$, то

$$h = (ha)a^{-1} \in (Ha)(Ha)^{-1}.$$

Итак, $H \subseteq (Ha)(Ha)^{-1}$.

2б) Если $z = (xa)(ya)^{-1} \in (Ha)(Ha)^{-1}$, $x, y \in H$, то

$$z = xa(ya)^{-1} = xaa^{-1}y^{-1} = xy^{-1} \in H.$$

Итак, $(Ha)(Ha)^{-1} \subseteq H$. 

 Следствие 1.8.2. Если H_1 и H_2 — подгруппы группы G , $a_1, a_2 \in G$, то

- 1) из $a_1H_1 = a_2H_2$ следует, что $H_1 = H_2$;
- 2) из $H_1a_1 = H_2a_2$ следует, что $H_1 = H_2$.

Доказательство.

- 1) $H_1 = (a_1 H_1)^{-1} (a_1 H_1) = (a_2 H_2)^{-1} (a_2 H_2) = H_2$.
- 2) $H_1 = (H_1 a_1)(H_1 a_1)^{-1} = (H_2 a_2)^{-1} (H_2 a_2) = H_2$. \square

Замечание 1.8.3.

- 1) Если H — подгруппа группы G , то $Ha = a(a^{-1}Ha)$ (т. е. левый смежный класс является правым смежным классом некоторой сопряжённой подгруппы).
- 2) Если H_1 и H_2 — подгруппы группы G , $a, b \in G$, $aH_1 = H_2b$, то $H_1 = b^{-1}H_2b$. Действительно, $aH_1 = H_2b = b(b^{-1}H_2b)$, и поэтому $H_1 = b^{-1}H_2b$. \square

Теорема 1.8.4 (о разбиении группы на левые смежные классы). Пусть G — группа и H — подгруппа группы G , тогда:

- 1) $x \in xH$ для всех $x \in G$;
- 2) если $z \in xH$, то $zH = xH$;
- 3) если $xH \cap yH \neq \emptyset$, то $xH = yH$ (т. е. два левых смежных класса либо не пересекаются, либо совпадают);
- 4) равносильны следующие условия:
 - a) $xH = yH$;
 - б) $y^{-1}x \in H$;
 - в) $x^{-1}y \in H$;
- 5) если $|H| = k < \infty$, то $|xH| = k$.

Доказательство.

- 1) $x = xe \in xH$, так как $e \in H$.
- 2) Если $z \in xH$, то $z = xh_0$, где $h_0 \in H$. Тогда $x = zh_0^{-1}$, где $h_0^{-1} \in H$.
Пусть $h \in H$. Тогда:

$$\begin{aligned} zh &= (xh_0)h = x(h_0h) \in xH, \text{ так как } h_0h \in H; \\ xh &= (zh_0^{-1})h = z(h_0^{-1}h) \in zH, \text{ так как } h_0^{-1}h \in H. \end{aligned}$$

Итак, $zH \subseteq xH$ и $xH \subseteq zH$, т. е. $zH = xH$.

- 3) Пусть $z \in xH \cap yH$. В силу 2) $xH = zH = yH$.
- 4) Если $xH = yH$, то $x \in xH = yH$, и поэтому $x = yh$, $h \in H$, т. е. $y^{-1}x = h \in H$. Аналогично, $y \in yH = xH$, $y = xh'$, $h' \in H$, т. е. $x^{-1}y = h' \in H$. Если $y^{-1}x = h \in H$, то $x = yh \in yH$. В силу 2) $xH = yH$. Если $x^{-1}y = h' \in H$, то $y = xh' \in xH$. В силу 2) $yH = xH$.
- 5) Если $xh = xh'$, то, умножая на x^{-1} , видим, что $h = h'$. \square

Следствие 1.8.5.

- 1) Группа G разбивается на непересекающиеся левые смежные классы по подгруппе H (разбиение на левые смежные классы): $G = \bigcup_{i \in I} x_i H$, $(G : H) = |I|$. Если множество I бесконечно, то для выбора в каждом смежном классе своего представителя x_i мы используем аксиому выбора (см. ??). Набор представителей $\{x_i \mid i \in I\}$ левых смежных классов называется левой трансверсалю к подгруппе H группы G . Таким образом, каждый элемент $x \in G$ однозначно определяется в терминах трансверсали и элементов подгруппы H (если $x \in x_i H$, то $x = x_i h$, где $i \in I$ и $h \in H$ определены для x однозначно).
- 2) Если $g_1, g_2 \in G$ и $g_1 H \subseteq g_2 H$, то $g_1 H = g_2 H$; если же $g_1 H \neq g_2 H$, то $g_1 H \cap g_2 H = \emptyset$.

Аналогичное утверждение имеет место для правых смежных классов.

Замечание 1.8.6.

- 1) Разбиение группы G на левые смежные классы xH по подгруппе H можно также интерпретировать как разбиение на классы эквивалентности по следующему отношению эквивалентности на множестве G :

$$x \sim y \iff x^{-1}y \in H.$$

Действительно:

- a) Проверим, что это отношение является отношением эквивалентности:

$$\begin{aligned} x^{-1}x = e \in H &\implies x \sim x \text{ для всех } x \in G; \\ x \sim y &\implies x^{-1}y = h \in H \implies y^{-1}x = h^{-1} \in H \implies y \sim x; \\ x \sim y, y \sim z &\implies x^{-1}y = h_1 \in H, y^{-1}z = h_2 \in H \implies \\ &\implies x^{-1}z = x^{-1}yy^{-1}z = h_1h_2 \in H \implies x \sim z. \end{aligned}$$

- б) Если $x \sim y$, то $x^{-1}y = h \in H$, и поэтому $y = xh \in xH$. Если $y = xh \in xH$, то $x^{-1}y = h \in H$, т. е. $x \sim y$. Итак, совокупность элементов y таких, что $x \sim y$, совпадает с левым смежным классом xH элемента x по подгруппе H . \square
- 2) Аналогично, разбиение группы G на правые смежные классы Hx по подгруппе H является разбиением на классы эквивалентности по следующему отношению эквивалентности на множестве G :

$$x \sim y \iff xy^{-1} \in H.$$

Пример 1.8.7.

- 1) Пусть $G = S_3$ — группа подстановок на множестве из трёх элементов $\{1, 2, 3\}$ и $H = \langle(1 2)\rangle$ — циклическая группа, порождённая циклом $(1 2)$. Тогда $(G : H) = |G|/|H| = 6/2 = 3$. Выпишем явно разбиения: на левые смежные классы

$$\begin{aligned} H &= \{e, (1 2)\}, \quad (1 2 3)H = \{(1 2 3), (1 3)\}, \\ (1 3 2)H &= \{(1 3 2), (2 3)\}; \end{aligned}$$

на правые смежные классы

$$H = \{e, (1 2)\}, \quad H(1 2 3) = \{(1 2 3), (2 3)\}, \\ H(1 3 2) = \{(1 3 2), (2 3)\}.$$

В этом случае разбиения на левые и правые смежные классы оказываются разными.

- 2) Пусть $G = S_n$ и $H = A_n$. Тогда $(G : H) = |G|/|H| = n!/(n!/2) = 2$, разбиение на левые смежные классы

$$H = A_n, \quad (1 2)H = S_n \setminus A_n$$

и разбиение на правые смежные классы

$$H = A_n, \quad H(1 2) = S_n \setminus A_n$$

совпадают.

Упражнение 1.8.8 (двойные смежные классы). Пусть H и M — подгруппы группы G . Для фиксированного элемента $x \in G$ множество

$$HxM = \{hxm \mid h \in H, m \in M\}$$

называется двойным смежным классом группы G . Покажите, что:

- а) два двойных смежных класса HxM и HyM либо совпадают, либо не пересекаются; группа G разлагается в объединение непересекающихся двойных смежных классов;
- б) число левых смежных классов по H в HxM равно

$$|M : (M \cap x^{-1}Hx)|;$$

- в) число правых смежных классов по M в HxM равно

$$|x^{-1}Hx : (M \cap x^{-1}Hx)|.$$

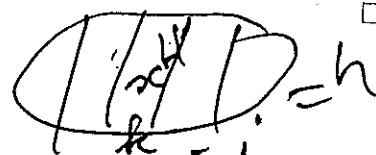
Теорема 1.8.9 (Лагранж, Joseph Louis Lagrange (1736–1813)). Если H — подгруппа группы G , $|G| = n < \infty$, $|H| = k$, то k — делитель числа n , а именно, $n = kj$, где j — число левых (правых) смежных классов, называемое индексом подгруппы H в G (обозначение: $j = (G : H)$).

Доказательство. Рассмотрим разбиение группы G на j различных левых смежных классов xH . Так как $|xH| = |H| = k$, то $n = kj$. \square

1.9. Следствия из теоремы Лагранжа

Следствие 1.9.1. Если $a \in G$, $|G| = n$, то порядок $O(a)$ элемента a является делителем числа n , порядка группы G .

Доказательство. Рассмотрим циклическую подгруппу $H = \langle a \rangle$. Тогда $|H| = O(a)$. В силу теоремы Лагранжа $n = O(a) \cdot j$. \square



Следствие 1.9.2. Если $|G| = n$ и $a \in G$, то $a^n = e$.

Доказательство. В силу следствия 1.9.1 $n = O(a) \cdot j$. Тогда $a^n = (a^{O(a)})^j = e^j = e$. \square

Следствие 1.9.3 (теорема Эйлера и малая теорема Ферма). Если $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$, то

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

где $\varphi(m) = |U(\mathbb{Z}_m)|$ — функция Эйлера. В частности, при $m = p$ получаем малую теорему Ферма: если a не делится на простое число p , то

$$a^{p-1} \equiv 1 \pmod{p}$$

(другими словами, $a^p \equiv a \pmod{p}$).

Доказательство.

1) Пусть $G = U(\mathbb{Z}_m)$ — группа обратимых элементов кольца вычетов \mathbb{Z}_m , $|G| = |\mathbb{Z}_m| = \varphi(m)$ — функция Эйлера (т. е. $\varphi(m)$ — число тех $x \in \mathbb{N}$, что $0 < x < m$, $(x, m) = 1$). Так как

$$(a, m) = 1 \iff a + \mathbb{Z}m \in U(\mathbb{Z}_m),$$

то

$$(a + \mathbb{Z}m)^{\varphi(m)} = a^{\varphi(m)} + \mathbb{Z}m = 1 + \mathbb{Z}m,$$

и поэтому

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

✓ 2) Если $m = p$, то $\varphi(p) = p - 1$. \square

Замечание 1.9.4. На применении малой теоремы Ферма основаны вероятностные алгоритмы нахождения больших простых чисел p : для достаточно большого числа случайных значений $a < p$ проверяется, что $a^{p-1} \equiv 1 \pmod{p}$.

Упражнение 1.9.5. Пусть p_1, p_2 — нечётные простые числа, при этом $\text{НОД}(p_1 - 1, p_2 - 1) = 2$ и $m = p_1 p_2$. Если $a^{m-1} \equiv 1 \pmod{m}$, то $a^2 \equiv 1 \pmod{m}$, и следовательно, имеем четыре решения для a (порядок элемента $O(a)$ делит $p_1 + p_2 - 2$, поэтому делит $(p_1 - 1)^2$ и $(p_2 - 1)^2$ и, следовательно, делит 4).

Следствие 1.9.6 (о цикличности группы простого порядка). Порядок $|G|$ конечной группы G равен простому числу p тогда и только тогда, когда $G \cong \mathbb{Z}_p$ (т. е. группа G циклическая и изоморфна группе вычетов \mathbb{Z}_p по модулю простого числа p). Итак, если $|G| = p$, то G — циклическая группа и в качестве циклического образующего группы G можно выбирать любой неединичный элемент группы G . В частности, в группе G нет подгрупп, отличных от $\{e\}$ и G .

Доказательство.

1) Если $G \cong \mathbb{Z}_p$, то $|G| = |\mathbb{Z}_p| = p$.

2) Пусть $|G| = p$ и $e \neq a \in G$. Тогда число $O(a)$ является делителем числа $p = |G|$, поэтому $O(a) = p$ и $|\langle a \rangle| = O(a) = p = |G|$. Следовательно, $\langle a \rangle = G$, т. е. G — циклическая группа порядка p . Итак, $G \cong \mathbb{Z}_p$ (см. ??). \square

Упражнение 1.9.7 (классификация групп порядка $n \leq 5$). Пусть G — группа и $|G| \leq 5$. Если $|G| = 1, 2, 3$ или 5 , то, по следствию 1.9.6 к теореме Лагранжа для $p = 2, 3$ или 5 , G — циклическая группа. Если $|G| = 4$ и в G есть элемент a порядка 4 , то $G = \langle a \rangle$ — циклическая группа, $G \cong \mathbb{Z}_4$. В противном случае $G = \{e, a, b, c\}$, $a^2 = b^2 = c^2 = e$. Если $ab = e$, то $ab = e = a^2$, и поэтому $b = a$, что противоречит тому, что $a \neq b$; аналогично, $ab \neq a$, $ab \neq b$. Итак, $ab = c$. Так же проверяем, что $ba = c$, $ac = b = ca$, $bc = a = cb$. Таким образом, G — группа Клейна (см. 1.2.9, п. 5). \square

Следствие 1.9.8. Группа S_3 является неабелевой группой наименьшего порядка.

Теорема 1.9.9 (теорема Пуанкаре о пересечении подгрупп конечного индекса). Пересечение $H \cap K$ двух подгрупп H и K конечного индекса группы G является подгруппой конечного индекса в G (оценка для индекса пересечения будет дана позже в теореме 1.9.35).

Доказательство. Если $a \in G$, то в силу 1.7.4, п. 4)

$$(H \cap K)a = Ha \cap Ka.$$

Таким образом, любой правый смежный класс $(H \cap K)a$ является пересечением правого смежного класса Ha по подгруппе H и правого смежного класса Ka по подгруппе K . Число таких пересечений конечно. Из этого следует, что индекс подгруппы $H \cap K$ конечен. \square

Упражнение 1.9.10.

1) Если A, B — подгруппы группы G , то

$$(A : A \cap B) \leq (G : B).$$

2) Если A, B, C — подгруппы группы G и $A \subseteq B$, то

$$(B \cap C : A \cap C) \leq (B : A).$$

3) Группа $(\mathbb{Q}, +)$ не содержит собственных подгрупп конечного индекса.

Следствие 1.9.11. Число левых смежных классов и число правых смежных классов группы G по подгруппе H совпадают (это число называется индексом подгруппы H в группе G и обозначается $(G : H)$).

Доказательство. Для конечной группы G , $|G| = n < \infty$, $|H| = k$, эти числа равны $j = \frac{n}{k} = \frac{|G|}{|H|}$. \square

Другое рассуждение применимо и для бесконечных групп: биекция $x \rightarrow x^{-1}$, $G \rightarrow G$, осуществляет биекцию между множествами левых и правых смежных классов: $xH \rightarrow Hx^{-1}$.

Упражнение 1.9.12. Пусть $\varphi: G_1 \rightarrow G_2$ — изоморфизм групп G_1 и G_2 , H_1 — подгруппа группы G_1 , $H_2 = \varphi(H_1)$. Тогда $(G_1 : H_1) = (G_2 : H_2)$.

Лемма 1.9.13. Пусть H и K — конечные подгруппы группы G . Тогда:

- a) если $(|H|, |K|) = 1$, то $H \cap K = e$;
- б) если $|H| = p$ — простое число, то либо $H \cap K = e$, либо $H \subseteq K$.

Доказательство.

а) Так как $H \cap K$ — подгруппа в группе H и в группе K , то $|H \cap K|$ — общий делитель чисел $|H|$ и $|K|$. Поскольку $(|H|, |K|) = 1$, имеем $|H \cap K| = 1$, и следовательно, $H \cap K = e$.

б) Если $H \cap K \neq e$, то $1 < |H \cap K|$. Так как $H \cap K$ — подгруппа в H , то $|H \cap K|$ — делитель числа $p = |H|$, отличный от 1. Поэтому $|H \cap K| = p$. Таким образом, $H \cap K \subseteq H$ и $|H \cap K| = p = |H|$. Следовательно, $H = H \cap K \subseteq K$. \square

Теорема 1.9.14. Пусть G — группа, H и K — её подгруппы, при этом $H \leq K \leq G$. Если $(G : H) < \infty$, то

$$(G : H) = (G : K) \cdot (K : H).$$

Доказательство. Пусть $(K : H) = r$, $(G : K) = s$. Зафиксируем выбор представителей левых смежных классов в разбиении:

$$K = \bigcup_{j \in J} y_j H, \quad |J| = r, \quad G = \bigcup_{i \in I} x_i K, \quad |I| = s.$$

Тогда

$$G = \bigcup_{(i,j) \in I \times J} x_i y_j H.$$

Если $x_i y_j H = x_{i'} y_{j'} H$, $i, i' \in I$, $j, j' \in J$, то $y_j H \subseteq K$, $y_{j'} H \subseteq K$, и поэтому $x_i K = x_{i'} K$, откуда следует, что $i = i'$. Тогда $y_j H = y_{j'} H$, и следовательно, $j = j'$. Итак, имеем разбиение

$$G = \bigcup_{(i,j) \in I \times J} x_i y_j H$$

на непересекающиеся смежные классы $(x_i y_j)H$ группы G по подгруппе H , $(i, j) \in I \times J$. Осталось отметить, что

$$(G : H) = |I \times J| = |I| \times |J| = rs. \quad \square$$

Замечание 1.9.15. Если $|G| < \infty$, то утверждение теоремы 1.9.14 непосредственно следует из теоремы Лагранжа:

$$(G : H) = |G|/|H| = (|G|/|K|) \cdot (|K|/|H|) = (G : K) \cdot (K : H). \quad \square$$

Следствие 1.9.16. Пусть G — конечная группа, H и K — её подгруппы, при этом $H \leq K \leq G$ и $(G : H) = p$ — простое число. Тогда $H = K$ или $K = G$.

Доказательство. Так как $p = (G : H) = (G : K) \cdot (K : H)$ — простое число, то либо $(G : K) = 1$ (и поэтому $G = K$), либо $(K : H) = 1$ (и поэтому $K = H$). \square

Замечание 1.9.17. Обращение теоремы Лагранжа не имеет места (в классе всех конечных групп), т. е. для делителя k числа $n = |G|$ может не найтись подгруппы из k элементов. *Что показывают следующие:*

Примеры 1.9.18.

Что показывают следующие:

- 1) Обращение теоремы Лагранжа не имеет места: группа A_4 чётных подстановок имеет порядок $|A_4| = 12 = 6 \cdot 2$, однако группа A_4 не содержит подгрупп из 6 элементов. Действительно, пусть

$$H \subset G = A_4 = \{e, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3), (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3)\}$$

(отсюда: любой неединичный элемент в A_4 — либо тройной цикл (их 8), либо 3 произведения двух транспозиций с непересекающимися орбитами);

$$|H| = 6; \\ V = \{e, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\} \subset S_4.$$

подгруппа Клейна. Если $H \cap V = \{e\}$, то из $h_1 v_1 = h_2 v_2$, $h_1, h_2 \in H$, $v_1, v_2 \in V$, следует, что

$$h_2^{-1} h_1 = v_2 v_1^{-1} \in H \cap V = \{e\},$$

т. е. $h_1 = h_2$ и $v_1 = v_2$. Таким образом,

$$|HV| = |H||V| = 6 \cdot 4 = 24,$$

что противоречит $HV \subseteq S_4$, $|S_4| = 12$.

Итак, $H \cap V \neq \{e\}$. Пусть $\pi = (i j)(k l) \in H$, $\{i, j, k, l\} = \{1, 2, 3, 4\}$, например $(1 2)(3 4)$. Кроме того, поскольку $|H| = 6$ и $|V| = 4$, то H содержит один из тройных циклов (их 8 в $G = A_4$), скажем $\sigma = (1 2 3) \in H$. Но тогда $\tau = \sigma \pi \sigma^{-1} = (1 4)(2 3) \in H$ и $\pi \tau = (1 3)(2 4) \in H$. Итак, $V \subset H$, но $4 = |V|$ не делит $6 = |H|$. Полученное противоречие завершает доказательство. Можно для доказательства использовать разбиение группы A_4 на классы сопряжённых элементов. \square

- 2) $|A_5| = 60 = 30 \cdot 2$, но в A_5 нет подгрупп из 30 элементов.

Указание. Можно и удобно для доказательства использовать простоту группы A_5 , которая будет установлена позже, см. ??.

Замечание 1.9.19. Для $G = \langle a \rangle$, если $|G| = n = kj$, то $H = \langle a^j \rangle$, $|H| = k$. Итак, для конечных циклических групп верно обращение теоремы Лагранжа.

Решётки подгрупп циклических групп

Следующее следствие из теоремы Лагранжа даёт описание строения решётки подгрупп циклической группы, развивая нашу теорему 1.6.9 о том, что любая подгруппа циклической группы является циклической (при этом будет существенно использован тот факт, что для класса конечных циклических групп обращение теоремы Лагранжа верно).

Теорема 1.9.20 (об описании решётки подгрупп циклической группы). Пусть $G = \langle a \rangle$ — циклическая группа, a — фиксированный один из её циклических образующих.

- 1) Если $G = \langle a \rangle$ — бесконечная циклическая группа, то:

- 1a) каждая подгруппа группы G имеет вид $H_i = \langle a^i \rangle$, $i \geq 0$; все подгруппы H_i при $i \geq 0$ различны, при этом H_i при $i > 0$ — бесконечные циклические группы, $O(a^i) = \infty$; $H_0 = \langle e = a^0 \rangle$ — единичная группа;
- 1б) $H_i = \langle a^i \rangle \subseteq \langle a^j \rangle = H_j$, $i \geq 0$, $j \geq 0$, тогда и только тогда, когда j — делитель числа i , $i = jm$;

$$H_i \wedge H_j = H_i \cap H_j = H_{\text{НОК}(i,j)},$$

$$H_i \vee H_j = \langle H_i \cup H_j \rangle = H_{\text{НОД}(i,j)};$$

- 1в) решётка подгрупп $\mathcal{L}(G)$ бесконечной циклической группы $G = \langle a \rangle$, $|G| = O(a) = \infty$, изоморфна решётке $\mathbb{N}_0 = (\mathbb{N} \cup \{0\}, \wedge, \vee)$ с отношением порядка, определяемым делимостью,

$$i \leq j \iff j \text{ — делитель числа } i$$

$$(i \wedge j = \text{НОК}(i,j); i \vee j = \text{НОД}(i,j)).$$

- 2) Если $G = \langle a \rangle$ — конечная циклическая группа порядка $n = |G| = O(a)$, $1 \leq n < \infty$, то:

- 2а) порядок d каждой подгруппы H группы G является делителем числа n , $n = dq$, $d > 0$, $q > 0$; для каждого делителя d числа n , $n = dq$, $d > 0$, существует и единственная подгруппа $K_d = \langle a^{n/d} \rangle$, $d = |K_d| = O(a^{n/d})$ элементов (циклическая подгруппа, порождённая элементом $a^{n/d} = a^q \in G$);
- 2б) для двух делителей d_1 и d_2 числа n , $n = d_1 q_1 = d_2 q_2$,

$$K_{d_1} \subseteq K_{d_2} \iff d_2 = d_1 t, \quad t \in \mathbb{N};$$

$$K_{d_1} \wedge K_{d_2} = K_{d_1} \cap K_{d_2} = K_{\text{НОД}(d_1, d_2)},$$

$$K_{d_1} \vee K_{d_2} = \langle K_{d_1} \cup K_{d_2} \rangle = K_{\text{НОК}(d_1, d_2)};$$

- 2в) решётка подгрупп $\mathcal{L}(G)$ конечной циклической группы $G = \langle a \rangle$, $|G| = O(a) = n < \infty$, изоморфна решётке делителей d числа n , $1 \leq d \leq n$, $n = dq$, с отношением порядка

$$d_1 \leq d_2 \iff d_2 = d_1 t, \quad t \in \mathbb{N}.$$

Доказательство.

1) Пусть $G = \langle a \rangle$, $|G| = O(a) = \infty$. В силу теоремы 1.6.9 каждая подгруппа H группы $G = \langle a \rangle$ имеет вид $H = \langle a^k \rangle$, где $k \geq 0$, при этом $O(a^k) = \infty$ при $k > 0$ и $a^0 = e$.

Включение $\langle a^i \rangle \subseteq \langle a^j \rangle$, $i \geq 0$, $j \geq 0$, равносильно включению $a^i \in \langle a^j \rangle$, что означает $a^i = (a^j)^m$, $m \in \mathbb{Z}$. Поскольку $O(a) = \infty$, это равенство равносильно тому, что $i = jm$.

Следовательно, $\langle a^i \rangle = \langle a^j \rangle$, $i \geq 0$, $j \geq 0$, равносильно тому, что $i = j$. Отсюда следует, что для $i \geq 0$, $j \geq 0$:

$$H_i \wedge H_j = H_i \cap H_j = \langle a^i \rangle \cap \langle a^j \rangle = \langle a^{\text{НОК}(i,j)} \rangle = H_{\text{НОК}(i,j)};$$

$$H_i \vee H_j = \langle H_i \cup H_j \rangle = \langle a^{\text{НОД}(i,j)} \rangle = H_{\text{НОД}(i,j)}.$$

В итоге мы получили сформулированное описание решётки подгрупп $\mathcal{L}(G)$ для $G = \langle a \rangle$, $|G| = O(a) = \infty$.

2) Пусть $G = \langle a \rangle$, $|G| = O(a) = n$. Если H — подгруппа группы G порядка $d = |H|$, то по теореме Лагранжа $n = dq$.

Для любого делителя d числа n , $n = dq$, мы можем предъявить подгруппу из d элементов:

$$K_d = \langle a^{n/d} \rangle, \quad |\langle a^{n/d} \rangle| = O(a^{n/d}) = \frac{n}{n/d} = d.$$

Более того, это единственная подгруппа из d элементов. Действительно, в силу теоремы 1.6.9 о подгруппах циклической группы: $H = \langle a^r \rangle$, $|H| = O(a^r) = d$. Тогда $a^{rd} = e$, поэтому rd делится на n и, следовательно, r делится на $q = n/d$. Поэтому $H = \langle a^r \rangle \subseteq \langle a^{n/d} \rangle = K_d$. Так как $|H| = d = |K_d|$, то $H = K_d$.

Если $n = d_1 q_1 = d_2 q_2$ и $K_{d_1} \subseteq K_{d_2}$, то по теореме Лагранжа $d_2 = d_1 t$. Если же $d_2 = d_1 t$, то $q_1 = n/d_1 = (d_2 q_2)/d_1 = (d_1 t q_2)/d_1 = tq_2$, и поэтому $K_{d_1} = \langle a^{q_1} \rangle \subseteq \langle a^{q_2} \rangle = K_{d_2}$. Итак,

$$K_{d_1} \subseteq K_{d_2} \iff d_2 = d_1 t.$$

Следовательно, для любых двух делителей d_1 и d_2 числа n :

$$K_{d_1} \wedge K_{d_2} = K_{d_1} \cap K_{d_2} = K_{\text{НОД}(d_1, d_2)}; \quad K_{d_1} \vee K_{d_2} = \langle K_{d_1} \cup K_{d_2} \rangle = H_{\text{НОК}(d_1, d_2)}.$$

В итоге получили сформулированное описание решётки подгрупп $\mathcal{L}(G)$ для $G = \langle a \rangle$, $|G| = O(a) = n$. \square

Примеры 1.9.21.

- Пусть $G = \langle a \rangle$, $|G| = O(a) = \infty$. Тогда для $H_4 = \langle a^4 \rangle$, $H_6 = \langle a^6 \rangle$ имеем:

$$H_4 \wedge H_6 = H_4 \cap H_6 = H_{12}; \quad H_4 \vee H_6 = \langle H_4 \cup H_6 \rangle = H_2;$$

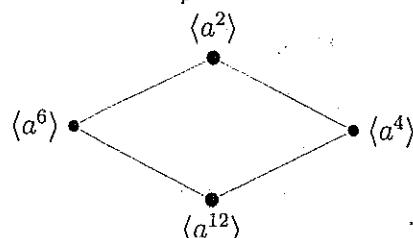
- В бесконечной циклической группе $G = \langle a \rangle$, $|G| = O(a) = \infty$, выполнено условие обрыва возрастающих цепей подгрупп, однако имеются бесконечные строго убывающие цепи подгрупп, например:

$$\langle a \rangle \supset \langle a^2 \rangle \supset \langle a^4 \rangle \supset \dots \supset \langle a^{2^n} \rangle \supset \langle a^{2^{n+1}} \rangle \supset \dots$$

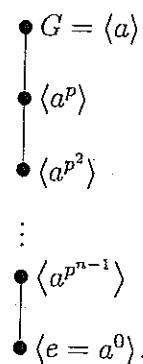
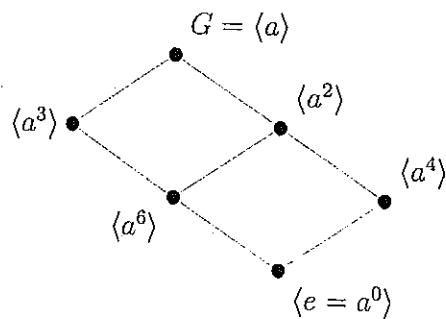
- Диаграмма Хассе (решётка) всех подгрупп $\mathcal{L}(G)$ циклической группы $G = \langle a \rangle$ порядка $12 = |G| = O(a)$ имеет вид

- Все подгруппы примарной циклической группы $G = \langle a \rangle$ порядка $p^n = |G| = O(a)$, где p — простое число, образуют цепь

Теорема 1.9.22. Группа G имеет в точности две различные подгруппы ($\{e\}$ и G) тогда и только тогда, когда G — циклическая группа порядка p , p — простое число, $G = \langle a \rangle$, $|G| = O(a) = p$, другими словами, $G = \mathbb{Z}_p$.



12-25



Доказательство. Если $G = \langle a \rangle$, $|G| = O(a) = p$, то в силу теоремы Лагранжа (или теоремы 1.9.20, п. 2а)) группа G имеет в точности две подгруппы $\{e\}$ и G .

Пусть группа G имеет в точности две различные подгруппы $\{e\}$ и G . Тогда $|G| > 1$. Если $e \neq a \in G$, то $\{e\} \neq \langle a \rangle$, и поэтому $G = \langle a \rangle$ — циклическая группа. Группа G не может быть бесконечной (поскольку тогда в силу п. 1а) теоремы 1.9.20 группа G имеет бесконечное число подгрупп). Таким образом, группа G конечна: $|G| = O(a) = n < \infty$. Если число n не является простым, $1 < d < n$, $n = dq$, то в силу п. 2а) теоремы 1.9.20 подгруппа $K = \langle a^{n/d} \rangle$ отлична от $\{e\}$ и G , что невозможно. Итак, $n = p$ — простое число. \square

Следствие 1.9.23. Каждая неабелева группа содержит собственную подгруппу.

Доказательство. В теореме показано, что все группы без собственных подгрупп, в частности, абелевы. \square

Упражнения 1.9.24.

- ✓ 1) Группа S_3 имеет шесть различных подгрупп.
- ✓ 2) Найти все подгруппы в группе Клейна $V \subseteq S_4$.
- ✓ 3) Найти все подгруппы группы кватернионов.

Теорема Коши

Одно из следствий теоремы Лагранжа утверждает, что если G — конечная группа, $n = |G| < \infty$, $g \in G$ — любой элемент группы G , то его порядок $m = O(g)$ является делителем порядка $n = |G|$ группы G . Оказывается, что обращение этого утверждения верно для простых делителей $m = p$ числа $n = |G|$. Это составляет содержание теоремы Коши, одного из первых тонких утверждений в началах теории групп, но имеющего многочисленные применения.

Замечание 1.9.25.

- 1) Для непростых делителей m порядка группы $n = |G|$ это утверждение уже не имеет места, как мы видели (см. ??) в группе Клейна $G = V_4 \subset S_4$: $n = |V_4| = 4$; все неединичные элементы имеют порядок 2; для делителя $m = 4$ числа $n = 4$ в группе $G = V_4$ нет элемента g , для которого $O(g) = 4$.
- 2) Конечно, теорема Коши является следствием глубокой теоремы Силова (которая появится у нас на более продвинутом уровне теории групп) о том, что для делителей $m = p^r$, где p — простое число, числа $n = |G|$ в группе G найдётся подгруппа $H \subseteq G$ такая, что $|H| = p^r$. Действительно, любой неединичный элемент $e \neq a \in H$ имеет порядок $O(a) = p^l$, $1 \leq l \leq r$, и тогда в его циклической подгруппе $\langle a \rangle \subseteq H \subseteq G$ найдётся элемент $b = a^{p^{l-1}}$, $O(b) = p$.

Отметим также, что во многих доказательствах теорем Силова используется теорема Коши.

Теорема 1.9.26 (теорема Коши). Пусть G — конечная группа, $n = |G| < \infty$. Если число $n = |G|$ делится на простое число p , то группа G содержит элемент порядка p .

1-е доказательство (комбинаторное).

- 1) Пусть

$$T = \left\{ (g_1, \dots, g_p) \in \underbrace{G \times \dots \times G}_p \mid g_1 \dots g_p = e \right\}.$$

Так как для любого набора $(g_1, g_2, \dots, g_{p-1})$, $g_i \in G$, $1 \leq i \leq p-1$, существует и единственный элемент $g_p = (g_1 \dots g_{p-1})^{-1} \in G$ такой, что

$$g_1 g_2 \dots g_{p-1} g_p = e,$$

то $|T| = |G|^{p-1}$. Так как в силу условия теоремы число $|G|$ делится на p , то и число $|T| = |G|^{p-1}$ делится на p .

- 2) Рассмотрим разбиение множества строк T :

$$T = S \cup T', \quad S \cap T' = \emptyset,$$

где

$$S = \{(g, \dots, g) \in T\} = \left\{ (g, \dots, g) \in \underbrace{G \times \dots \times G}_p \mid g^p = e \right\},$$

$$T' = \{(g_1, \dots, g_p) \in T \mid g_i \neq g_j \text{ для некоторых } i, j\}.$$

- 3) Если $(g_1, g_2, \dots, g_p) \in T'$, то все перестановки этой строчки по циклу также лежат в T' ,

$$(g_i, g_{i+1}, \dots, g_p, g_1, \dots, g_{i-1}) \in T'$$

для любого $1 \leq i \leq p$.

Действительно,

$$e = g_1 \dots g_p = (g_1 \dots g_{i-1})(g_i \dots g_p),$$

поэтому

$$g_i \dots g_p = (g_1 \dots g_{i-1})^{-1},$$

и следовательно,

$$g_i \dots g_p g_1 \dots g_{i-1} = (g_1 \dots g_{i-1})^{-1} g_1 \dots g_{i-1} = e.$$

4) Для любой строки $(g_1, \dots, g_p) \in T'$ все p её перестановок по циклу

$$\{(g_i, g_{i+1}, \dots, g_p, g_1, \dots, g_{i-1}) \mid 1 \leq i \leq p\}$$

являются различными строчками в T' , и поэтому число $|T'|$ делится на p .

Действительно, допустим противное: пусть при $1 \leq i < j \leq p$ ($t = j - i > 0$, $j = i + t$) имеем

$$(g_i, g_{i+1}, \dots, g_p, g_1, \dots, g_{i-1}) = (g_j, g_{j+1}, \dots, g_p, g_1, \dots, g_{j-1}).$$

Приравнивая 1-ю компоненту, получаем:

$$g_i = g_j (\equiv g_{i+t}).$$

Сравнивая $(t+1)$ -ю компоненту, получаем

$$g_j = g_{i+t} = g_r, \quad i+2t = pq+r, \quad 0 \leq r < p.$$

Удобно рассматривать наши индексы как элементы группы $\mathbb{Z}_p = (\{0 = p, 1, 2, \dots, p-1\}, +)$, тогда

$$g_i = g_{i+t} = g_{i+2t} = \dots = g_{i+(p-1)t}.$$

Так как группа $(\mathbb{Z}_p, +)$ — циклическая группа порядка p , то любой её ненулевой элемент t является образующим порядка p , $\mathbb{Z}_p = \langle t \rangle$, $O(t) = p$, и поэтому

$$\{0, t, 2t, \dots, (p-1)t\} = \{0, 1, 2, \dots, p-1\}.$$

Итак,

$$g_1 = g_2 = \dots = g_p.$$

Но это противоречит тому, что

$$(g_1, g_2, \dots, g_p) \in T' = T \setminus S.$$

Итак, множество строк T' разбито на непересекающиеся подмножества из p элементов каждое, поэтому число $|T'|$ делится на p .

5) Так как $|S| = |T| - |T'|$, при этом числа $|T|$ и $|T'|$ делятся на p , то $|S|$ делится на p , и поэтому $|S| \geq p \geq 2$.

6) Рассмотрим $\hat{S} = \{g \in G \mid g^p = e\} \subseteq G$. Тогда $e \in \hat{S}$, $|\hat{S}| = |S| \geq 2$, поэтому найдётся элемент $e \neq g \in G$ такой, что $g^p = e$. Итак, $O(g) \neq 1$ и $O(g)$ — делитель числа p , следовательно, $O(g) = p$. \square

Экспонента конечной группы

Доказанная теорема Коши позволяет нам сейчас рассмотреть понятие экспоненты конечной группы.

Пусть G — конечная группа, экспонента $\exp(G)$ конечной группы G определяется следующим образом:

$$\exp(G) = \text{НОК}\{\text{O}(g) \mid g \in G\}.$$

Лемма 1.9.27. Пусть G — конечная группа. Тогда:

- 1) экспонента $\exp(G)$ делит порядок группы $|G|$;
- 2) каждое простое число, делящее порядок группы $|G|$, делит и экспоненту $\exp(G)$;
- 3) $\exp(G)$ совпадает с наименьшим натуральным числом m таким, что $g^m = e$ для всех элементов $g \in G$ группы G .

Доказательство.

1) В силу следствия 1.9.1 к теореме Лагранжа для всякого $g \in G$ порядок $\text{O}(g)$ является делителем числа $|G|$. Поэтому порядок группы $|G|$ делится на экспоненту $\exp(G) = \text{НОК}\{\text{O}(g) \mid g \in G\}$.

2) В силу теоремы Коши 1.9.26 в группе G найдётся подгруппа H такая, что $|H| = p$. Подгруппа H циклическая, $H = \langle h \rangle$. Тогда $p = |H| = \text{O}(h)$. Поэтому простое число p делит экспоненту $\exp(G)$.

3) Так как $\exp(G)$ делится на порядок $\text{O}(g)$ любого элемента $g \in G$, то $g^{\exp(G)} = e$.

Если $m \in \mathbb{N}$ и $g^m = e$ для всех $g \in G$, то число m делится на все порядки $\text{O}(g)$, $g \in G$, и поэтому число m делится на $\text{НОК}\{\text{O}(g) \mid g \in G\} = \exp(G)$. \square

Упражнения 1.9.28.

- 1) Если $G = \langle a \rangle$ — циклическая группа, то $\exp(G) = |G|$. Действительно: $n = |G| = \text{O}(a)$; для любого $b = a^k$ имеем $\text{O}(b) = \frac{n}{(k, n)}$. Поэтому $\exp(G) = \text{НОК}\{\text{O}(g) \mid g \in G\} = n$. \square
- 2) Если $G = V_4 \subseteq S_4$, то $|V_4| = 4$, $\exp(V_4) = 2$ (таким образом, возможно, что $\exp(G) < |G|$).
- 3) Если $|G| = p^r$, где p — простое число, и $\exp(G) = |G|$, то $G = \langle a \rangle$ для некоторого $a \in G$ (т. е. G — циклическая группа). Действительно, в противном случае порядок $\text{O}(g)$ каждого элемента $g \in G$ является собственным делителем числа p^r , и поэтому p^{r-1} делится на все $\text{O}(g)$, $g \in G$, что противоречит равенству $\exp(G) = |G| = p^r$. \square
- 4) Если $|G| = p^r$, то существует элемент $g \in G$, для которого $\text{O}(g) = \exp(G)$.
- 5) Если $\exp(G) = 2$, то G — абелева группа. Действительно, для любых $a, b \in G$ имеем $e = (ab)^2 = abab$, $e = a^2 = b^2$, поэтому $ab = ba$. \square
- 6) Если p — простое число, $p \neq 2$, $G = \text{UT}_3(F_p)$ — унитреугольная группа над полем F_p из p элементов, то $|G| = p^3$, группа G некоммутативна (матрицы $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$)

Решение №12

В-1

Лекция №13

1.9. Следствия из теоремы Лагранжа

(19 октября 2011г.)

57

не перестановочны), но $x^p = e$ для всех $x \in G$, т. е. $\exp(G) = p > 2$. Действительно, если $x = A = E + N \in G$, $p \geq 3$, то $N^p = 0$, и поэтому

$$x^p = A^p = (E + N)^p = E^p + N^p = E,$$

поскольку $\{a_0 E + a_1 N + \dots + a_m N^m \mid a_i \in F_p\}$ — коммутаторное кольцо, в котором $px = 0$ для всех x .

Произведение подгрупп

Наличие бинарной операции произведения элементов в группе G позволяет определить произведение для подмножеств группы G : если $H \subseteq G$, $K \subseteq G$, то

$$HK = \{hk \mid h \in H, k \in K\}.$$

Ясно, что множество всех непустых подмножеств группы G с этой операцией умножения подмножеств образует моноид с нейтральным элементом $\{e\}$.

Ясно также, что если H — подгруппа группы G , то:

- a) $HH = H$;
- б) если $\emptyset \neq A \subseteq G$ — непустое подмножество в G , то $AH = H$ тогда и только тогда, когда $A \subseteq H$.

Полезность рассмотрения таких произведений была уже продемонстрирована при введении смежных классов по подгруппе: $H = \{h\}$, K — подгруппа группы G , в этом случае $HK = hK$ — левый смежный класс элемента h по подгруппе K .

В этом разделе мы рассмотрим произведения HK подгрупп H и K группы G . В общем случае HK может не быть подгруппой.

Примеры 1.9.29 (произведений подгрупп, не являющихся подгруппами).

- 1) Пусть $G = S_3$, $H = \langle (1 2) \rangle$, $|H| = 2$, $K = \langle (1 3) \rangle$, $|K| = 2$. Тогда

$$HK = \{e, (1 2), (1 3), (1 3 2)\}$$

не является подгруппой, поскольку $|HK| = 4$, а $|S_3| = 6$ не делится на 4 (по теореме Лагранжа в группе S_3 нет подгрупп из четырёх элементов).

- 2) Пусть $G = S_4$, $H = \langle (1 2) \rangle$, $|H| = 2$, $K = \langle (1 2 3 4) \rangle$, $|K| = 4$. Тогда $|HK| \leq 8$, $\langle H \cup K \rangle = \langle (1 2), (1 2 3 4) \rangle = S_4$, $|S_4| = 24$. Если бы подмножество HK было подгруппой, оно содержало бы подгруппы H и K , и следовательно, $S_4 = \langle H \cup K \rangle \subseteq HK$, что противоречит $|S_4| = 24$, $|HK| \leq 8$.

Следующее утверждение даёт ответ на вопрос: когда произведение подгрупп является подгруппой.

Теорема 1.9.30 (условие, при котором произведение подгрупп является подгруппой). Пусть H и K — подгруппы группы G . Тогда подмножество HK является подгруппой в том и только в том случае, если $HK = KH$ (такие подгруппы H и K , что $HK = KH$, называются *перестановочными*), в этом случае $\langle H, K \rangle = HK$.

Доказательство.

- а) Допустим, что HK является подгруппой. Тогда

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH.$$

- б) Пусть $HK = KH$. Проверим, что HK является подгруппой:

$$(HK)(HK) = HKHK = HHKK = HK;$$

$$(HK)^{-1} = K^{-1}H^{-1} = KH = HK. \quad \square$$

Модулярное тождество Дедекинда

Замечание 1.9.31.

- 1) Подгруппа $\langle A, B \rangle$, порождённая подгруппами A и B в группе G , тогда и только тогда совпадает с произведением AB , когда $AB = BA$.

Действительно, если $\langle A, B \rangle = AB$, то AB — подгруппа, и следовательно,

$$AB = BA.$$

Если же $AB = BA$, то AB — подгруппа, содержащая A и B . Итак, $\langle A, B \rangle \subseteq AB$. Так как всегда $AB \subseteq \langle A, B \rangle$, то $AB = \langle A, B \rangle$. \square

- 2) Конечные индексы подгруппы A в группе $\langle A, B \rangle$ и пересечения $A \cap B$ в подгруппе B совпадают тогда и только тогда, когда $AB = BA$. \square

Следующая теорема оказывается полезной в вычислениях с подгруппами.

Теорема 1.9.32 (модулярное тождество Дедекинда (Richard Dedekind, 1831–1916)). Пусть H, K, L — подгруппы группы G , при этом $K \subseteq L$. Тогда

$$(HK) \cap L = (H \cap L)K.$$

Доказательство.

- а) Так как $K \subseteq L$, то $(H \cap L)K \subseteq L$. Поэтому

$$(H \cap L)K \subseteq (HK) \cap L.$$

- б) Пусть $x \in (HK) \cap L$, $x = hk$, $h \in H$, $k \in K$. Тогда

$$h = xk^{-1} \in LK = L.$$

Следовательно, $h \in H \cap L$, и поэтому

$$x = hk \in (H \cap L)K.$$

Таким образом,

$$(HK) \cap L \subseteq (H \cap L)K. \quad \square$$

Замечание 1.9.33. Более сильное, чем модулярное тождество, тождество дистрибутивности

$$\langle H, K \rangle \cap L = \langle H \cap L, K \cap L \rangle$$

в общем случае не выполняется (приведите пример такой группы G).

Для конечных подгрупп H и K группы G полезно подсчитать число элементов в произведении HK .

Теорема 1.9.34. Если H и K — конечные подгруппы группы G , то

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Доказательство. Рассмотрим сюръективное отображение

$$f: H \times K \rightarrow HK, \quad f((h, k)) = hk, \quad h \in H, \quad k \in K.$$

Заметим, что $f((h_1, k_1)) = f((h_2, k_2))$, $h_1, h_2 \in H$, $k_1, k_2 \in K$, тогда и только тогда, когда $h_1k_1 = h_2k_2$, т. е. когда

$$h_2^{-1}h_1 = k_2k_1^{-1} = d \in H \cap K, \quad h_2 = h_1d^{-1}, \quad k_2 = dk_1.$$

Итак,

$$f^{-1}(h_1k_1) = \{(h_1d^{-1}, dk_1) \mid d \in H \cap K\}.$$

Следовательно,

$$|H| \cdot |K| = |H \times K| = |HK| \cdot |H \cap K|. \quad \square$$

В ряде случаев полезна следующая оценка индекса пересечения подгрупп, дополняющая теорему 1.9.9.

Теорема 1.9.35 (оценка индекса пересечения подгрупп; А. Пуанкаре (Henri Poincaré, 1854–1912)). Пусть H и K — подгруппы конечного индекса группы G , $(G : H) < \infty$, $(G : K) < \infty$. Тогда:

- a) $(G : (H \cap K)) \leq (G : H) \cdot (G : K)$;
- б) если индексы $(G : H)$ и $(G : K)$ взаимно просты, то неравенство в а) превращается в равенство $(G : (H \cap K)) = (G : H) \cdot (G : K)$, и в этом случае $G = HK$.

Доказательство.

а) Каждому левому смежному классу $x(H \cap K)$ поставим в соответствие пару левых смежных классов (xH, xK) . Как мы убедились в 1.7.4, п. 4б, это отображение определено корректно. Таким образом:

$$(G : (H \cap K)) \leq (G : H) \cdot (G : K).$$

- б) Допустим, что индексы $(G : H)$ и $(G : K)$ взаимно просты. В силу теоремы 1.9.14:

$$(G : (H \cap K)) = (G : H) \cdot (H : (H \cap K));$$

$$(G : (H \cap K)) = (G : K) \cdot (K : (H \cap K)).$$

Следовательно, индексы $(G : H)$ и $(G : K)$ являются делителями числа $(G : (H \cap K))$. Поскольку они взаимно просты, индекс $(G : (H \cap K))$ делится на их произведение $(G : H) \cdot (G : K)$, при этом, как мы показали в а), $(G : (H \cap K)) \leq (G : H) \cdot (G : K)$. Итак,

$$(G : (H \cap K)) = (G : H) \cdot (G : K).$$

Покажем, что в этом случае $G = HK$. Действительно,

$$\begin{aligned} |H| &= \frac{|G|}{(G : H)}, \quad |K| = \frac{|G|}{(G : K)}, \\ |H \cap K| &= \frac{|G|}{(G : (H \cap K))} = \frac{|G|}{(G : H) \cdot (G : K)}, \end{aligned}$$

поэтому

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{|G| \cdot |G| \cdot (G : H) \cdot (G : K)}{(G : H) \cdot (G : K) \cdot |G|} = |G|.$$

Итак, $G = HK$. □

Упражнения 1.9.36.

- 1) Если H — подгруппа группы G и $|G \setminus H| < \infty$, то либо $H = G$, либо $|G| < \infty$. *Действительно*, пусть $H < G$. Рассмотрим разбиение на левые смежные классы $G = \bigcup xH$. Тогда

$$G \setminus H = \bigcup_{xH \neq H} xH, \quad |xH| = |H|.$$

Таким образом, $|H| < \infty$, и следовательно, $|G| < \infty$.

2) ???

- 3) Пусть группа G имеет в точности три различные подгруппы: $\{e\} \subset H \subset G$. Тогда $G \cong \mathbb{Z}_{p^2}$, где p — простое число.

Действительно, покажем сначала, что G — циклическая группа. Пусть $e \neq a \in G \setminus H$, тогда $\langle a \rangle \neq \{e\}$, $\langle a \rangle \neq H$, поэтому $\langle a \rangle = G$. Из описания решётки подгрупп $\mathcal{L}(G)$ циклической группы $G = \langle a \rangle$ следует, что $|G| = n < \infty$ и, более того, n имеет ровно три положительных делителя: $1, p, n = p^2$, где p — простое число. □

- 4) Пусть G — конечная группа, H и K — подгруппы в G , порядки которых взаимно просты. Тогда $H \cap K = \{e\}$ и число $|HK|$ делит порядок подгруппы $\langle H, K \rangle$.

Действительно, по теореме Лагранжа порядок $|H \cap K|$ подгруппы $H \cap K$ делит взаимно простые числа $|H|$ и $|K|$, поэтому $|H \cap K| = 1$, т. е. $H \cap K = \{e\}$. Следовательно,

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = |H| \cdot |K|.$$

Так как $H \subseteq \langle H, K \rangle$, $K \subseteq \langle H, K \rangle$, то по теореме Лагранжа число $|\langle H, K \rangle|$ делится на взаимно простые числа $|H|$ и $|K|$, следовательно, оно делится и на их произведение $|H| \cdot |K| = |HK|$. □

- 5) Пусть G — конечная группа, $|G| = n$, d — минимальное число образующих группы G . Тогда $n \geq 2^d$, и поэтому $d \leq \lceil \log_2 n \rceil$.

Указание. Пусть $\{g_1, \dots, g_d\}$ — минимальная система образующих группы G . Рассмотрите 2^d элементов вида $g_{i_1} \dots g_{i_l}$, где $i_1 < \dots < i_l$, и покажите, что эти элементы различны.

- 6) ???

1.10. Нормальная подгруппа

Подгруппа H группы G называется *нормальной*, если $xH = Hx$ для всех $x \in G$ (т. е. если разбиения на левые и правые смежные классы совпадают). Будем использовать обозначение $H \triangleleft G$ в этом случае. Приведём ряд условий, эквивалентных условию нормальности.

Теорема 1.10.1. Пусть H — подгруппа группы G . Тогда эквивалентны следующие условия:

- 1) $gH = Hg$ для всех $g \in G$;
- 2) $g^{-1}Hg \subseteq H$ для всех $g \in G$ (т. е. $g^{-1}hg \in H$ для всех $g \in G, h \in H$);
- 3) $g^{-1}Hg = H$ для всех $g \in G$.

Доказательство.

- 1) \Rightarrow 2). Так как $Hg = gH$, то $hg = gh'$, $h' \in H$, и поэтому $g^{-1}hg = h' \in H$.
- 2) \Rightarrow 3). Так как $h = g^{-1}(ghg^{-1})g \in g^{-1}Hg$, поскольку $ghg^{-1} = (g^{-1})^{-1}h(g^{-1}) \in H$, то $H \subseteq g^{-1}Hg$, и поэтому $H = g^{-1}Hg$.
- 3) \Rightarrow 1). Если $g^{-1}Hg = H$ для всех $g \in G$, то, умножая слева на g , получаем, что $Hg = gH$. \square

Элемент $g^{-1}hg$ называется *сопряжённым с h при помощи элемента g* .

Пример 1.10.2. Ясно, что $\{e\} \triangleleft G$ и $G \triangleleft G$.

Группы G , в которых нет других нормальных подгрупп, кроме $\{e\}$ и G , называются *простыми* (например, \mathbb{Z}_p , p — простое число, A_5). Строение (конечных) простых групп весьма непросто! Это самый тонкий (простой) юмор математиков!

Упражнение 1.10.3.

- 1) Пусть H — подгруппа группы G . Тогда подгруппа H нормальная, $H \triangleleft G$, тогда и только тогда, когда

$$xy \in H \implies yx \in H \quad \forall x, y \in G. \quad (*)$$

Доказательство. а) Пусть H — нормальная подгруппа группы G . Если $xy = h \in H$, то $x = hy^{-1}$, и поэтому $yx = yhy^{-1} \in H$, поскольку $H \triangleleft G$.

б) Пусть выполнено условие $(*)$, $h \in H$, $y \in G$. Рассмотрим элемент $x = hy^{-1} \in G$. Тогда $xy = hy^{-1}y = h \in H$, и поэтому, в силу условия $(*)$, $yx = yhy^{-1} \in H$. Итак, $yhy^{-1} \in H$ для всех $h \in H$, $y \in G$. Это означает, что $H \triangleleft G$. \square

2) Если H — подгруппа группы G , для которой для любых $a, b \in G$ из $Ha \neq Hb$ следует, что $aH \neq bH$, то H — нормальная подгруппа.

Действительно, в противном случае найдём $h \in H$ и $g \in G$, для которых $ghg^{-1} \notin H$. Тогда для $a = gh$, $b = g$ имеем $ab^{-1} \notin H$, т. е. $Ha \neq Hb$, но $b^{-1}a = g^{-1}gh = h \in H$, т. е. $aH = bH$, что противоречит нашему предположению. \square

Пример 1.10.4. Как мы видели, $\langle(1\ 2)\rangle \not\triangleleft S_3$ (т. е. циклическая подгруппа $\langle(1\ 2)\rangle$ не является нормальной в группе S_3), поскольку разбиения на левые и правые смежные классы различны.

Упражнение 1.10.5. Найти все подгруппы (и среди них все нормальные подгруппы) группы подстановок S_3 .

Ясно, что $\{e\}$ и S_3 — подгруппы в S_3 . Пусть H — нетривиальная подгруппа в S_3 , $|H| = 6$. В силу теоремы Лагранжа $|H| = 2$ или 3 (как нетривиальные делители числа 6).

В силу ?? любая группа H из p элементов, где p — простое число (в частности, в нашем случае $p = 2$ или 3), является циклической группой порядка p . Наша группа S_3 имеет шесть элементов:

- один тождественный элемент e порядка 1;
- три элемента порядка 2 $\{(1\ 2), (1\ 3), (2\ 3)\}$;
- два элемента порядка 3 $\{(1\ 2\ 3), (1\ 3\ 2)\}$.

Ясно, что $(1\ 2\ 3)^2 = (1\ 3\ 2)$, $(1\ 2\ 3)^{-1} = (1\ 2\ 3)^2 = (1\ 3\ 2)$.

Следовательно, группа S_3 имеет:

- три циклические подгруппы второго порядка $T = \{e, (1\ 2)\}$, $U = \{e, (1\ 3)\}$, $V = \{e, (2\ 3)\}$;
- одну циклическую подгруппу третьего порядка $A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$.

Так как $(1\ 2) \in T$, но

$$(1\ 3)^{-1}(1\ 2)(1\ 3) = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin T,$$

то подгруппа T не является нормальной в G . Аналогично, не являются нормальными подгруппами в $G = S_3$ подгруппы U и V .

Как мы уже убедились, $A_3 \triangleleft S_3$. \square

Задача 1.10.6. Если $H \triangleleft S_n$ и $(1\ 2) \in H$, то $H = S_n$ (здесь $n \geq 2$).

Пример 1.10.7. Если G — абелева группа, то, конечно, любая подгруппа H в G нормальна (т. е. $xH = Hx$ для всех $x \in G$).

Пример 1.10.8. Если $|G| = 2|H|$, т. е. H — подгруппа индекса 2 в группе G , то H нормальна в G .

Доказательство. Разбиения на левые и правые классы совпадают, это $eH = H = He$ и $G \setminus H$. \square

Следствие 1.10.9. $A_n \triangleleft S_n$ (т. е. подгруппа чётных подстановок нормальна).

Это ясно и из непосредственного подсчёта чётности для $\pi \in A_n$:

$$\varepsilon(\sigma^{-1}\pi\sigma) = \varepsilon(\sigma^{-1})\varepsilon(\pi)\varepsilon(\sigma) = \varepsilon(\sigma)^2 = 1$$

для всех $\sigma \in S_n$.

Упражнение 1.10.10. A_n — единственная подгруппа индекса 2 в S_n . Более того, при $n \geq 5$ A_n — единственная собственная нормальная подгруппа группы S_n .

Упражнение 1.10.11. Пусть $|G| = n < \infty$ — конечная группа, p — наименьшее простое число, делящее n . Тогда любая подгруппа H индекса p в G нормальна в G .

Упражнение 1.10.12. Покажите, что A_3 — единственная собственная нормальная подгруппа группы S_3 . Найдите все нормальные подгруппы групп A_4 и D_4 .

Пример 1.10.13. $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ (специальная линейная подгруппа нормальна в линейной группе).

Доказательство. Пусть $A \in SL_n(\mathbb{R})$, т. е. $|A| = 1$, и $C \in GL_n(\mathbb{R})$, т. е. $|C| \neq 0$. Тогда

$$|C^{-1}AC| = |C^{-1}| |A| |C| = |C|^{-1} |C| = 1,$$

т. е. $C^{-1}SL_n(\mathbb{R})C \subseteq SL_n(\mathbb{R})$. □

Упражнение 1.10.14. $SO_n(\mathbb{R}) \triangleleft O_n(\mathbb{R})$; $SU_n(\mathbb{C}) \triangleleft U_n(\mathbb{C})$.

Упражнение 1.10.15. Если $K \triangleleft G$ и $K \subseteq H \subseteq G$, где H — подгруппа группы G , то $K \triangleleft H$, но H может не быть нормальной подгруппой.

Действительно, если $h \in H \subseteq G$, то $h^{-1}Kh = K$, и поэтому $K \triangleleft H$.

Если $G = S_3$, $K = \{e\}$, $H = \{e, (1 2)\}$, то $K \triangleleft G$, $K \subseteq H \subseteq G$, но $H \not\triangleleft G$. □

Пример 1.10.16. Подгруппа

$$T = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}$$

не является нормальной в линейной группе $GL_2(\mathbb{R})$. Действительно, для

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in T$$

имеем

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \notin T$$

для

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \in GL_2(\mathbb{R}).$$
□

Пример 1.10.17. Ортогональная подгруппа

$$O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A^* = A^{-1}\}$$

не является нормальной подгруппой в линейной группе $GL_n(\mathbb{R})$ при $n \geq 2$.

Доказательство. Заметим, что

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in O_2(\mathbb{R}),$$

но

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ -4 & -3 \end{pmatrix} \notin O_2(\mathbb{R}). \quad \square$$

Пример 1.10.18 (субнормальной подгруппы, не являющейся нормальной: $K \triangleleft T \triangleleft G$ не влечёт $K \triangleleft G$).

- 1) Пусть $T = \{e, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\} \subseteq S_4$ — подгруппа Клейна $T = V_4$ группы S_4 . Так как все неединичные элементы в T имеют цикловое разложение $(a b)(c d)$ и все элементы с таким цикловым разложением лежат в T , то $T \triangleleft S_4$, при этом T — абелева группа.

Пусть $K = \{e, (1 2)(3 4)\}$, тогда $K \triangleleft T$, но K не является нормальной подгруппой в S_4 , поскольку подстановка $(1 3)(2 4)$ сопряжена с подстановкой $(1 2)(3 4)$, но не лежит в K . \square

- 2) Пусть $G = S_3 \times S_3$, $L = \{e, (1 2 3), (1 3 2)\} = A_3 \triangleleft S_3$. Тогда $T = L \times L \triangleleft G = S_3 \times S_3$, при этом T — абелева группа, и поэтому любая её подгруппа в ней нормальна, в частности,

$$K = \{(e, e), ((1 2 3), (1 2 3)), ((1 3 2), (1 3 2))\} \triangleleft T = L \times L,$$

но

$$\begin{aligned} ((1 2), 1)^{-1}((1 2 3), (1 2 3))((1 2), 1) = \\ = ((1 2)(1 2 3)(1 2), (1 2 3)) = ((1 3 2), (1 2 3)). \end{aligned}$$

Итак, $K \not\triangleleft G$. \square

- 3) Пусть $G = D_4$, $K = \{e, \tau\}$, $T = \{e, \sigma^2, \tau, \sigma^2\tau\}$. Тогда $K \triangleleft T \triangleleft G$, однако $\sigma^{-1}\tau\sigma \notin K$, это означает, что $K \not\triangleleft G$.

Пример 1.10.19 (матричная реализация группы кватернионов). Матрицы

$$G = \left\{ e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, a = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\}$$

образуют подгруппу линейной группы $GL_2(\mathbb{C})$, при этом G — неабелева группа, $|G| = 8$, $a^4 = e$, $b^2 = a^2$, $b^{-1}ab = a^3$, все подгруппы группы G нормальны (действительно, единственная подгруппа порядка 2

$$\left\{ e = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\},$$

все подгруппы порядка 4 имеют индекс 2 и поэтому нормальны).

Лемма 1.10.20. Если H — нормальная подгруппа группы G , $H \triangleleft G$, и K — любая подгруппа группы G , то:

- H и K — перестановочные подгруппы, т. е. $HK = KH$;
- $H \vee K = HK$ — подгруппа группы G .

Доказательство.

- Так как $H \triangleleft G$, то для любого $k \in K$ имеем $Hk = kH$. Следовательно, $HK = KH$.
- В силу критерия 1.9.30: если $HK = KH$, то HK — подгруппа. \square

Лемма 1.10.21.

- Если $H \triangleleft G$, $K \triangleleft G$, то $H \vee K = HK = KH \triangleleft G$.
- Если $H \triangleleft G$, $K_1 \triangleleft K_2 \subseteq G$, то $H \vee K_1 = HK_1 = K_1H \triangleleft HK_2 = K_2H = H \vee K_2$.

Доказательство.

- Если $g \in G$, то

$$g(HK)g^{-1} = gHg^{-1}gKg^{-1} = HK.$$

- Пусть $g = hk_2$, $h \in H$, $k_2 \in K_2$. Тогда

$$gK_1g^{-1} = hk_2K_1k_2^{-1}h^{-1} = hK_1h^{-1},$$

и поэтому

$$gHK_1g^{-1} = gHg^{-1}gK_1g^{-1} = HhK_1h^{-1} = HK_1h^{-1} = K_1Hh^{-1} = K_1H = HK_1. \quad \square$$

Лемма 1.10.22. Если H , K , L — подгруппы группы G , $H \triangleleft K \subseteq G$, $L \subseteq G$, то $H \cap L \triangleleft K \cap L$.

Доказательство. $H \cap L$ и $K \cap L$ — подгруппы, при этом $H \cap L \subseteq K \cap L$. Если $x \in H \cap L$ и $g \in K \cap L$, то $g^{-1}xg \in L$ ($x \in L$, $g^{-1}, g \in L$), $g^{-1}xg \in H$ ($g \in K$, $x \in H$, $H \triangleleft K$), и поэтому $g^{-1}xg \in H \cap L$. Итак, $H \cap L \triangleleft K \cap L$. \square

Следствие 1.10.23 (при $K = G$). Если $H \triangleleft G$ и L — подгруппа в G , то $H \cap L \triangleleft H$.

Лемма 1.10.24. Пусть

$$H_1 \subseteq H_2 \subseteq \dots \subseteq H_i \subseteq \dots$$

возрастающая цепь подгрупп группы G , при этом

$$G = \bigcup_i H_i$$

и все H_i — простые группы. Тогда G — простая группа.

Доказательство. Допустим противное: пусть $N \triangleleft G$, $N \neq \{e\}$, $N \neq G$. Тогда $N \cap H_i \triangleleft H_i$ (по следствию 1.10.23) для всех i ,

$$N \cap H_1 \subseteq N \cap H_2 \subseteq \dots \subseteq N \cap H_i \subseteq \dots,$$

$$N = N \cap G = N \cap \left(\bigcup_i H_i \right) = \bigcup_i (N \cap H_i).$$

Для $e \neq n \in N$ найдётся такой индекс i , что $e \neq n \in N \cap H_j$ для всех $j \geq i$. Поэтому $N \cap H_j = H_j$ для всех $j \geq i$. Следовательно,

$$N = \bigcup_{j \geq i} (N \cap H_j) = \bigcup_{j \leq i} H_j = G,$$

что противоречит нашему допущению. \square

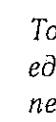
 **Теорема 1.10.25.** Пусть H, K, N — подгруппы группы G , при этом $H \subseteq K \subseteq G$, $|N \triangleleft G$. Если $H \cap N = K \cap N$ и $HN = KN$, то $H = K$.

 **Доказательство.** Пусть $k \in K$. Тогда $kN = hN$ для некоторого элемента $h \in H \subseteq K$. Поэтому $k^{-1}h \in K$ и $k^{-1}h \in N$, т. е. $k^{-1}h \in K \cap N = H \cap N$, $k^{-1}h = h' \in H$, $k = (h')^{-1}h \in H$. Итак, $K \subseteq H$, и поэтому $H = K$. \square

Нормальное ядро подгруппы

 **Лемма 1.10.26.** Пусть H — подгруппа группы G ,

$$H_G = \bigcap_{g \in G} g^{-1}Hg.$$

 Тогда $H_G \triangleleft G$, при этом если $K \subseteq H \subseteq G$, $K \triangleleft G$, то $K \subseteq H_G$ (таким образом, H_G — единственная наибольшая нормальная подгруппа группы G , содержащаяся в подгруппе H ; для H_G будем использовать название *нормальное ядро подгруппы H*).

Доказательство. 1) Так как $g^{-1}Hg$, $g \in G$, — подгруппа (сопряжённая подгруппа для H), то $H_G = \bigcap_{g \in G} g^{-1}Hg$ — подгруппа группы G ; при этом $e^{-1}He = H$, следовательно, $H_G \subseteq H$.

Если $h \in H_G \subseteq H$ и $a \in G$, то $h \in g^{-1}Hg$ для всех $g \in G$, поэтому $h = g^{-1}h_g g$ для $h_g \in H$. Тогда

$$a^{-1}ha = a^{-1}g^{-1}h_g ga = (ga)^{-1}h_g ga \in (ga)^{-1}Hga$$

для всех $g \in G$. Таким образом,

$$a^{-1}ha \in \bigcap_{ga \in G} (ga)^{-1}Hga = \bigcap_{g \in G} g^{-1}Hg = H_G,$$

поскольку $\{ga \mid g \in G\} = \{g \in G\}$ и отображение $ga \rightarrow g$ — биекция.

Итак, $H_G \triangleleft G$, $H_G \subseteq H \subseteq G$.

2) Если $K \subseteq H \subseteq G$ и $K \triangleleft G$, то $K = g^{-1}Kg \subseteq g^{-1}Hg$ для всех $g \in G$, и поэтому

$$K \subseteq \bigcap_{g \in G} g^{-1}Hg = H_G.$$

Упражнение 1.10.27.

1) Если $H = \{e\}$, то $\{e\}_G = \{e\}$.

2) Если $H = G$, то

$$G_G = \bigcap_{g \in G} g^{-1}Gg = \bigcap_{g \in G} G = G$$

(конечно, ясно, что G — единственная наибольшая нормальная подгруппа G).

3) Если $G = S_3$ и $H = \{e, (1 2)\}$, то $H_G = \{e, (1 2)\} \cap \{e, (1 3)\} \cap \{e, (2 3)\} = \{e\}$.

4) Пусть F — поле, $G = \mathrm{GL}_n(F)$ — линейная группа над полем F ,

$$H = \left\{ \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix} \middle| d_i \in F \setminus \{0\} \right\} -$$

подгруппа диагональных матриц. Тогда

$$H_G = \left\{ \begin{pmatrix} d & & 0 \\ & \ddots & \\ 0 & & d \end{pmatrix} \middle| 0 \neq d \in F \right\} -$$

подгруппа скалярных матриц ($= Z(\mathrm{GL}_n(F))$, центр линейной группы).

Действительно, если в диагональной матрице $d_i \neq d_j$, то её сопряжение с помощью элементарной матрицы $E + E_{ij}$ не является диагональной матрицей. \square

Трансверсали (системы представителей смежных классов по подгруппе)

Поскольку выбор системы представителей в разбиении группы на левые смежные классы (на правые смежные классы) по подгруппе неоднозначен (поскольку любой элемент смежного класса может быть выбран в качестве его представителя), то в ряде случаев полезно рассмотреть всевозможные выборы системы представителей смежных классов по подгруппе группы.

Пусть H — подгруппа группы G , $S \subseteq G$. Подмножество S группы G называется *левой трансверсалю подгруппы H группы G* , если S содержит один и только один элемент $s \in S$ из каждого левого смежного класса xH , $x \in G$ (в этом случае $xH = sH$, $SH = G$, $|S \cap xH| = 1$, $|S| = (G : H)$).

Соответственно подмножество T группы G называется *правой трансверсалю подгруппы H группы G* , если T содержит один и только один элемент $t \in T$ из каждого правого смежного класса Hx , $x \in G$ (в этом случае $Ht = Hx$, $HT = G$, $|T \cap Hx| = 1$, $|T| = (G : H)$).

Через $S = S_G(H)$ и $T = T_G(H)$ обозначим соответственно совокупность левых и правых трансверсалей подгруппы H группы G .

Лемма 1.10.28. Пусть H — подгруппа группы G , $|H| = m$, $(G : H) = n$. Если $S = S_G(H)$ и $T = T_G(H)$ — совокупности всех соответственно левых и правых трансверсалей подгруппы H в G , то

$$S(H) = \prod_{i=1}^n x_i H, \quad T(H) = \prod_{j=1}^n H y_j;$$

$$|x_i H| = |H| = m = |H y_j|, \quad |S| = |H|^{(G:H)} = m^n = |T|.$$

Доказательство. Это число равно числу выборок n элементов, где каждый элемент выбирается из подмножества, содержащего m элементов. \square

Предложение 1.10.29. Пусть H — подгруппа группы G , $S \subseteq G$. Тогда:

- 1a) подмножество S группы G является левой трансверсалю подгруппы H группы G тогда и только тогда, когда:

$$G = SH \text{ и } s^{-1}t \notin H \text{ для всех } s \neq t, s, t \in S;$$

- 1б) если $S \subseteq G$, то S — левая трансверсаль подгруппы H группы G тогда и только тогда, когда отображение

$$S \times H \rightarrow G, (s, h) \mapsto sh,$$

является биекцией (это означает, что каждый элемент $g \in G$ однозначно представим в виде $g = sh$, где $s \in S, h \in H$);

- 2a) подмножество T группы G является правой трансверсалю подгруппы H группы G тогда и только тогда, когда:

$$G = HT \text{ и } st^{-1} \notin H \text{ для всех } s \neq t, s, t \in T;$$

- 2б) если $T \subseteq G$, то T — правая трансверсаль подгруппы H группы G тогда и только тогда, когда отображение

$$H \times T \rightarrow G, (h, t) \mapsto ht,$$

является биекцией (это означает, что каждый элемент $g \in G$ однозначно представим в виде $g = ht$, где $h \in H, t \in T$);

- 3a) если K — подгруппа группы G такая, что

$$G = KH \text{ и } H \cap K = \{e\}$$

(в этом случае говорят, что подгруппа K является левым дополнением подгруппы H в G), то $S = K$ является левой трансверсалю подгруппы H в группе G ;

- 3б) если K — подгруппа группы G такая, что

$$G = HK \text{ и } H \cap K = \{e\}$$

(в этом случае говорят, что подгруппа K является правым дополнением подгруппы H в G), то $T = H$ является правой трансверсалю подгруппы H в группе G .

Доказательство.

1a) $sH = tH \iff s^{-1}t \in H;$

2a) $Hs = Ht \iff st^{-1} \in H;$

1б) условие $G = HS$ равносильно тому, что указанное отображение сюръективно. Если $(h, s), (h', s') \in H \times S$, $h, h' \in H$, $s, s' \in S$, при этом $hs = h's'$, то $Hs = Hs'$, и поэтому условие $s = s'$ (но тогда $h = h'$) означает инъективность указанного отображения;

2б) аналогично;

3a) если $s, t \in S = K$ и $s^{-1}t \in H$, то $s^{-1}t \in K \cap H = \{e\}$, поэтому $s = t$; в силу 2a) $S = K$ — левая трансверсаль;

3б) если $s, t \in T = K$ и $st^{-1} \in H$, то $st^{-1} \in K \cap H = \{e\}$, поэтому $s = t$; в силу 2б) $T = K$ — правая трансверсаль. \square

Замечание 1.10.30. Отметим в этом контексте один из вариантов тождества Дедекинда (см. 1.9.32): пусть $G = KL$, где K и L — подгруппы группы G , H — подгруппа группы G , содержащая подгруппу K , $K \subseteq H \subseteq G$. Тогда подгруппа H допускает следующую факторизацию:

$$H = K \cdot (L \cap H).$$

Действительно, если $h \in H \subseteq G = KL$, то $h = kl$, $k \in K$, $l \in L$; поэтому $l = k^{-1}h \in L \cap H$, поскольку $k^{-1} \in K \subseteq H$; таким образом, $H \subseteq K \cdot (L \cap H)$.

Если $k \in K$, $l \in L \cap H$, то $k \in K \subseteq H$, $l \in L \cap H \subset H$, и поэтому $kl \in H$. Итак, $K \cdot (L \cap H) \subseteq H$. \square

Упражнение 1.10.31. Пусть G — конечная группа. Допустим, что A — подгруппа группы G и $G = A \cdot A^g$ для $g \in G$, где $A^g = g^{-1}Ag$. Тогда $G = A$.

Действительно, пусть $G = \bigcup Ag_i$, $1 \leq i \leq r$, $g \in Ag_1$, $g = ag_1$, $g_1 = a_1g^{-1}a_2g$, где $g_i \in G$, $a, a_1, a_2 \in A$. Тогда $g = aa_1g^{-1}a_2g$, поэтому $g = a_2aa_1 \in A$, следовательно, $A^g = A$ и $G = A \cdot A^g = A \cdot A = A$. \square

Лемма 1.10.32.

- ✓ а) Если T — правая трансверсаль подгруппы H группы G , $g \in G$, то $Tg = \{tg \mid t \in T\}$ также является правой трансверсалю подгруппы H группы G . Таким образом, множество $T = T(H)$ всех правых трансверсалей подгруппы H группы G является правым полигоном T_G над группой G .
- ✓ б) Если T — правая трансверсаль подгруппы H группы G , $h \in H$ и $hT = \{ht \mid t \in T\}$, то hT — правая трансверсаль подгруппы H группы G . Таким образом, $T = T(H)$ является левым полигоном ${}_HT$ над группой H .
- ✓ в) Более того, $T = T(H) - H$ -биполигон ${}_HT_G$ (т. е. $(hT)g = h(Tg)$ для всех $h \in H$, $T \in T$, $g \in G$).

Доказательство.

а) Если $x \in G$, то, по предположению, $|T \cap Hxg^{-1}| = 1$, и поэтому $|Tg \cap Hx| = |(T \cap Hxg^{-1})g| = 1$. Если $T = T(H)$ — совокупность всех правых трансверсалей подгруппы H группы G , то T_G — правый G -полигон, поскольку $Te = T$, $T(g_1g_2) = (Tg_1)g_2$ (см. п. 1).

б) Если $x \in G$, то

$$|hT \cap Hx| = |T \cap h^{-1}Hx| = |T \cap Hx| = 1.$$

Так как $eT = T$ и $(h_1h_2)T = h_1(h_2T)$, то ${}_HT$ — левый H -полигон.

в) Так как для всех $h \in H$, $g \in G$, $T \in T$ имеем

$$(hT)g = hTg = h(Tg),$$

то ${}_HT_G$ — H -биполигон. \square

Связи между левыми и правыми трансверсалами подгруппы в группе

Отметим связи между совокупностью всех левых трансверсалей $S = S_G(H)$ и совокупностью всех правых трансверсалей $T = T_G(H)$ подгруппы H группы G .

Лемма 1.10.33. Пусть H — подгруппа группы G . Если $S, T \subseteq G$, то

$$S = \{s_i \mid i \in I\} —$$

левая трансверсаль подгруппы H группы G , $S \in S_G(H)$, тогда и только тогда, когда

$$T = S^{-1} = \{t_i = s_i^{-1} \mid i \in I\} —$$

правая трансверсаль подгруппы H группы G , $T \in T_G(H)$.

Таким образом: $T_G(H) = (S_G(H))^{-1}$ и, в частности, $|T_G(H)| = |S_G(H)^{-1}| = I = (G : H)$.

Доказательство. При биекции $G \rightarrow G$, $x \mapsto x^{-1}$, имеем

$$(xH)^{-1} = Hx^{-1},$$

и, как следствие, получаем биекцию $xH \mapsto Hx^{-1}$ между левыми и правыми смежными классами.

Если $S = \{s_i \mid i \in I\}$ — левая трансверсаль, то

$$G = SH \text{ и } s_i^{-1}s_j \notin H \text{ для всех } i \neq j.$$

Но тогда при биекции $x \mapsto x^{-1}$:

$$G = G^{-1} = HS^{-1} = HT$$

и $t_i = s_i^{-1}$, $i \in I$:

$$t_j t_i^{-1} = s_j^{-1} s_i = (s_i^{-1} s_j)^{-1} \in H^{-1} = H \text{ для всех } i \neq j.$$

Итак, $T = \{t_i = s_i^{-1} \mid i \in I\} = S^{-1}$ — правая трансверсаль подгруппы H группы G (см. п. 1 предложения 1.10.29). \square

Теорема Кёнига о разбиениях

Если индекс $(G : H)$ подгруппы H группы G конечен, то верен весьма любопытный факт о том, что разбиение на левые смежные классы и разбиение на правые смежные классы по подгруппе H имеют общую систему представителей (это означает, что $S_G(H) \cap T_G(H) \neq \emptyset$!). Доказательство этого факта мы выведем из элегантной теоремы Кёнига (1916 г.) об общей системе представителей для двух разбиений множества (при некоторых условиях). Это комбинаторное утверждение нашло многочисленные применения в комбинаторной математике.

Теорема 1.10.34 (теорема Кёнига о разбиениях, D. König, 1916 г.). Пусть множество M разбито на n непересекающихся подмножеств двумя способами

$$M = \bigcup_{i=1}^n A_i = \bigcup_{j=1}^n B_j,$$

при этом выполнено следующее условие:

любые r классов A_{i_1}, \dots, A_{i_r} первого разбиения содержат (в своём объединении) не более чем k классов B_{j_1}, \dots, B_{j_k} , $k \leq r$, второго разбиения. (*)

Тогда:

- 1) условие (*) симметрично;
- 2) первое и второе разбиения имеют общую систему представителей.

Доказательство. 1) Допустим противное:

$$\bigcup_{k=1}^r B_{j_k} \supseteq \bigcup_{l=1}^{r+1} A_{i_l}.$$

Тогда

$$M \setminus \bigcup_{k=1}^r B_{j_k} = \bigcup_{k=r+1}^n B_{j_k} \subseteq M \setminus \bigcup_{l=1}^{r+1} A_{i_l} = \bigcup_{l=r+2}^n A_{i_l},$$

но при этом $n - r > n - (r + 1) = (n - r) - 1$, что противоречит выполнению условия (*) для первого разбиения $M = \bigcup_{i=1}^n A_i$.

2) Рассмотрим матрицу инцидентности этих двух разбиений множества M :

$$A = (a_{ik}) \in M_n(\mathbb{Z}_2),$$

где

$$a_{ik} = \begin{cases} 1, & \text{если } A_i \cap B_k \neq \emptyset, \\ 0, & \text{если } A_i \cap B_k = \emptyset. \end{cases}$$

Эта $(n \times n)$ -матрица из 0 и 1 обладает следующими свойствами:

- i) в каждой i -й строке матрицы A найдётся хотя бы одна 1 (иначе $A_i \cap B_j = \emptyset$ для всех $1 \leq j \leq n$ и, следовательно,

$$A_i = A_i \cap M = A_i \cap \left(\bigcup_{j=1}^n B_j \right) = \bigcup_{j=1}^n (A_i \cap B_j) = \emptyset,$$

что невозможно), аналогично в каждом j -м столбце матрицы A найдётся хотя бы одна 1;

Применяя индуктивное предположение для $0 < r < n$ и $0 < n - r < n$, перестановками первых r строк и столбцов и перестановками последних $n - r$ строк и столбцов приведём угловые миноры к такому виду, что $a_{11} = \dots = a_{rr} = 1$ и $a_{r+1,r+1} = \dots = a_{nn} = 1$. Таким образом, искомый вид матрицы A достигнут.

Случай 2. Не существует нулевой $(r \times (n-r))$ -подматрицы в A , т. е. для любой нулевой (k, l) -подматрицы имеем $k + l \leq n - 1$. Тогда любая $((n-1) \times (n-1))$ -подматрица является нормальной. Поэтому перестановками строк и столбцов сначала добьёмся того, что $a_{11} = 1$ (в первой строке есть 1), а затем, по индуктивному предположению, для правого нижнего нормального $((n-1) \times (n-1))$ -минора добьёмся перестановками строк и столбцов того, что $a_{22} = \dots = a_{nn} = 1$. \square

Следствие из теоремы Кёнига

Теорема 1.10.35. Если индекс $(G : H)$ подгруппы H группы G конечен, то разбиение на левые смежные классы и разбиение на правые смежные классы по подгруппе H имеют общую систему представителей (трансверсаль), т. е. $S_G(H) \cap T_G(H) \neq \emptyset$.

Доказательство. Если G — конечная группа, то любые r правых смежных классов содержат не более чем r левых смежных классов, поскольку

$$|Hg_1 \dot{\cup} \dots \dot{\cup} Hg_r| = r|H|,$$

и если

$$\bigcup_{j=1}^k u_j H \subseteq \bigcup_{i=1}^r Hg_i,$$

то

$$k|H| = \left| \bigcup_{j=1}^k u_j H \right| \leq \left| \bigcup_{i=1}^r Hg_i \right| = r|H|,$$

и поэтому $k \leq r$.

Применяя к этим двум разбиениям группы G теорему Кёнига о разбиениях (теорема 1.10.34), получаем общую систему представителей для левых и правых смежных классов. \square

Трансверсали нормальной подгруппы

Отметим теперь, что в том случае, когда H — нормальная подгруппа группы G , $H \triangleleft G$, нет разницы между левыми и правыми смежными классами ($xH = Hx$ для всех $x \in G$ для $H \triangleleft G$), и поэтому любая левая трансверсаль является правой трансверсалью, и наоборот, которая называется просто *трансверсалью*.

Лемма 1.10.36. Пусть H — нормальная подгруппа группы G . Тогда $S_G(H) = T_G(H)$. \square

Упражнение 1.10.37. Пусть H — подгруппа группы G . Если каждая правая трансверсаль подгруппы H является левой трансверсалью, то $H \triangleleft G$.

Упражнение 1.10.38. Пусть H — нормальная подгруппа группы G . Тогда существование трансверсали к нормальной подгруппе H , являющейся подгруппой группы G , равносильно тому, что группа G расщепляется над H (т. е. $G = HK$ и $H \cap K = \{e\}$ для некоторой подгруппы K в G).

ii) матрица A *нормальна* в следующем смысле: любая её $(k \times l)$ -подматрица, состоящая целиком из нулей, имеет $k + l \leq n$.

Проверим выполнение свойства ii). Допустим противное: пусть, для простоты записи, наша нулевая $(k \times l)$ -подматрица расположена в левом верхнем углу на пересечении первых k строк и первых l столбцов (это достигается, например, соответствующими перестановками строк и столбцов): при этом $k + l > n$. Так как наше условие (*) симметрично, то можно считать, что $k \leq l$. Тогда $A_i \cap B_j = \emptyset$ для $1 \leq i \leq k, 1 \leq j \leq l$, и следовательно,

$$\left(\bigcup_{i=1}^k A_i \right) \cap \left(\bigcup_{j=1}^l B_j \right) = \emptyset.$$

Поэтому

$$\bigcup_{i=k+1}^n A_i = M \setminus \bigcup_{i=1}^k A_i \supseteq \bigcup_{j=1}^l B_j,$$

при этом $n - k < l$, поскольку $k + l > n$, что противоречит условию (*) для наших разбиений.

Итак, доказано, что $k + l \leq n$.

Нам осталось показать, что любая нормальная $(n \times n)$ -матрица $A = (a_{ik})$ с элементами из $\mathbb{Z}_2 = \{0, 1\}$ может быть приведена с помощью перестановок строк и столбцов к виду A' , в котором на диагонали стоят 1, $a'_{11} = a'_{22} = \dots = a'_{nn} = 1$. Тогда в этой новой нумерации классов разбиений система элементов

$$\{c_i \in A_i \cap B_i \neq \emptyset, i = 1, 2, \dots, n\}$$

является общей системой представителей для первого и второго разбиений.

Проведём индукцию по n . Для $n = 1$ утверждение очевидно. Пусть $n > 1$.

Случай 1. Существует нулевая $(r \times (n - r))$ -подматрица в A ; переставляя, несомненно, строки и столбцы, можно считать, что:

$$a_{ik} = 0, \text{ если } 1 \leq i \leq r < k \leq n$$

(таким образом, нулевая $(r \times (n - r))$ -подматрица занимает правый верхний угол).

Проверим теперь, что в новой матрице $(r \times r)$ -минор в левом верхнем углу $M_{1, \dots, r; 1, \dots, r}$ и $(n - r, n - r)$ -минор в правом нижнем углу $M_{r+1, \dots, n; r+1, \dots, n}$ являются нормальными матрицами, при этом $r < n, n - r < n$.

Действительно, если $(r \times r)$ -минор в левом верхнем углу не является нормальной матрицей, то после перестановки первых r строк и столбцов получим, что нулевая (s, t) -матрица с $s + t > r$ находится в правом верхнем углу $(r \times r)$ -минора, и тогда $a_{ik} = 0$ для $1 \leq i \leq s < k \leq n$, где $1 \leq s \leq r - 1$ ($s \leq r - 1$, поскольку в противном случае в матрице A будет нулевая строка). Таким образом мы получаем нулевую $s \times (t + (n - r))$ -матрицу на пересечении первых s строк и последних $t + (n - r)$ столбцов, при этом

$$s + t + (n - r) > r + (n - r) = n,$$

что противоречит нормальности матрицы A .

Аналогично проверяется, что правый нижний $((n - r) \times (n - r))$ -минор также является нормальной матрицей.

Центр группы

Определение 1.10.39. Пусть G — группа, центром группы G называется подмножество элементов

$$Z(G) = \{a \in G \mid ag = ga \forall g \in G\}.$$

Теорема 1.10.40. Центр $Z(G)$ является нормальной подгруппой группы G .

Доказательство.

1) Если $a, b \in Z(G)$ и $g \in G$, то:

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab),$$

и поэтому $ab \in Z(G)$; $ag = ga$, следовательно, $ga^{-1} = a^{-1}g$, и поэтому $a^{-1} \in Z(G)$. Таким образом, $Z(G)$ — подгруппа группы G .

2) Если $g \in G$ и $a \in Z(G)$, то $ag = ga$, поэтому

$$g^{-1}ag = g^{-1}ga = ea = a \in Z(G).$$

Итак, $Z(G) \triangleleft G$. \square

Замечание 1.10.41.

1) Группа G коммутативна тогда и только тогда, когда $Z(G) = G$.

2) $Z(S_2) = S_2$.

3) Центр $Z(G)$ группы G может быть тривиальным, $Z(G) = \{e\}$:

3а) если $n \geq 3$, то $Z(S_n) = \{e\}$;

3б) если G — некоммутативная простая группа, то $Z(G) = \{e\}$ (в противном случае $\{e\} \neq Z(G) \trianglelefteq G$, и поэтому $Z(G) = G$, т. е. G — абелева группа, что противоречит предположению).

4) Фактор-группа по центру $G/Z(G)$ может иметь нетривиальный центр: если G — группа кватернионов, то $Z(G) \cong \mathbb{Z}_2$, $G/Z(G)$ — абелева группа.

Упражнение 1.10.42. Вычислите $Z(GL_n(K))$, $Z(SL_n(K))$; покажите, в частности, что $Z(SL_2(\mathbb{Z}_p)) = \{\pm E\}$ при $p > 2$.

Упражнение 1.10.43. Если G — группа, $x, y \in G$, $z = xy \in Z(G)$, то элементы x и y коммутируют: $xy = yx$.

Доказательство. Так как $x = zy^{-1}$ и $z \in Z(G)$, то $x = zy^{-1} = y^{-1}z$,

$$xy = zy^{-1}y = ze = z = ez = yy^{-1}z = z = yx. \quad \square$$

Централизатор элемента группы

Пусть G — группа, $a \in G$, централизатором элемента $a \in G$ в группе G называется подмножество

$$C(a) = C_G(a) = \{g \in G \mid ga = ag\}$$

группы G .

Лемма 1.10.44. Централизатор $C(a)$ любого элемента a группы G является подгруппой в G .

Доказательство. Если $g, g_1, g_2 \in C(a)$, то $ga = ag$, $g_1a = ag_1$, $g_2a = ag_2$, и поэтому:

$$(g_1g_2)a = g_1(g_2a) = g_1(ag_2) = (g_1a)g_2 = (ag_1)g_2 = a(g_1g_2),$$

следовательно, $g_1g_2 \in C(a)$;

$$g^{-1}a = g^{-1}agg^{-1} = g^{-1}gag^{-1} = ag^{-1},$$

следовательно, $g^{-1} \in C(a)$.

Итак, $C(a)$ — подгруппа группы G . \square

Замечания 1.10.45.

1) $Z(G) = \bigcap_{a \in G} C(a)$;

2) $a \in Z(G)$ тогда и только тогда, когда $C(a) = G$;

3) $\langle a \rangle \triangleleft C(a)$.

Лемма 1.10.46. $C(g^{-1}ag) = g^{-1}C(a)g$ для любых элементов g и a группы G .

Доказательство. Пусть $x \in G$, тогда:

$$\begin{aligned} x \in C(g^{-1}ag) &\iff x(g^{-1}ag) = (g^{-1}ag)x \iff gxg^{-1}ag = agx \iff \\ &\iff (gxg^{-1})a = g(xg^{-1}ag)g^{-1} = g(g^{-1}agx)g^{-1} = a(gxg^{-1}) \iff \\ &\iff gxg^{-1} \in C(a) \iff x \in g^{-1}C(a)g. \end{aligned}$$
 \square

Задача 1.10.47. Найти

$$Z(S_n) = \begin{cases} S_n, & n = 2, \\ \{e\}, & n > 2, \end{cases} \quad Z(A_n) = \begin{cases} A_n, & n \leq 3, \\ \{e\}, & n > 3, \end{cases}$$

$$Z(GL_n(K)) = \{\lambda E \mid 0 \neq \lambda \in K\}, \quad Z(SL_n(K)) = E.$$

Задача 1.10.48. $|Z(GL_n(F_q))| = q - 1$; $|Z(SL_n(F_q))| = \text{НОД}(n, q - 1)$.

Задача 1.10.49. В группе S_n найдите все подстановки σ , перестановочные с циклом $(i_1 \dots i_n)$.

Коммутаторы элементов, коммутант группы, взаимный коммутант подгрупп

Пусть G — группа, $a, b \in G$. Коммутатором элементов $a, b \in G$ называется элемент

$$[a, b] = aba^{-1}b^{-1} \in G.$$

Лемма 1.10.50 (свойства коммутаторов). Пусть G — группа, $a, b \in G$. Тогда:

- 1) $[a, b]ba = ab$;
- 2) $[a, b] = e$ тогда и только тогда, когда $ab = ba$;
- 3) $[a, b]^{-1} = [b, a]$;
- 4) $g^{-1}[a, b]g = [g^{-1}ag, g^{-1}bg]$ для $g \in G$.

Доказательство.

- 1) $[a, b]ba = aba^{-1}b^{-1}ba = ab$.
- 2) $[a, b] = aba^{-1}b^{-1} = e$ тогда и только тогда, когда $ab = ba$.
- 3) $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$.
- 4)

$$\begin{aligned} g^{-1}[a, b]g &= g^{-1}aba^{-1}b^{-1}g = \\ &= (g^{-1}ag)(g^{-1}bg)(g^{-1}a^{-1}g)(g^{-1}b^{-1}g) = \\ &= (g^{-1}ag)(g^{-1}bg)(g^{-1}ag)^{-1}(g^{-1}bg)^{-1} = [g^{-1}ag, g^{-1}bg]. \end{aligned}$$

□

Упражнение 1.10.51.

1)

$$\begin{aligned} [a^{-1}, b] &= a^{-1}bab^{-1} = a^{-1}(bab^{-1}a^{-1})a = a^{-1}[b, a]a; \\ [a, b^{-1}] &= ab^{-1}a^{-1}b = b^{-1}(bab^{-1}a^{-1})b = b^{-1}[b, a]b. \end{aligned}$$

2)

$$\begin{aligned} [ab, c] &= abcb^{-1}a^{-1}c^{-1} = \\ &= a(bcb^{-1}c^{-1})a^{-1}(aca^{-1}c^{-1}) = a[b, c]a^{-1}[a, c]; \\ [a, bc] &= abc^{-1}c^{-1}b^{-1} = ab(a^{-1}b^{-1}ba)ca^{-1}c^{-1}b^{-1} = \\ &= (aba^{-1}b^{-1})b(aca^{-1}c^{-1})b^{-1} = [a, b]b[a, c]b^{-1}. \end{aligned}$$

3) Операция коммутирования не является ассоциативной. Она ассоциативна, т. е. $[[a, b], c] = [a, [b, c]]$ для всех a, b, c в группе G тогда и только тогда, когда группа G метабелева (коммутатор $[a, b]$ любой пары элементов $a, b \in G$ лежит в центре $Z(G)$); эти группы также называются *нильпотентными группами* класса 2.

4) $[a, b][b, c] = [aba^{-1}, ca^{-1}]$.

Доказательство. $[a, b][b, c] = (aba^{-1}b^{-1})(bc^{-1}c^{-1}) = (aba^{-1})(ca^{-1})(ab^{-1}a)(ac^{-1})$. □

Замечание 1.10.52 (о другом определении коммутатора). Мы выбрали в качестве определения коммутатора $[a, b] = aba^{-1}b^{-1}$ двух элементов a и b группы G решение уравнения $x(ba) = ab$, $x = ab(ba)^{-1}$. В ряде учебных пособий и монографий по теории групп в качестве исходного определения коммутатора двух элементов $a, b \in G$ берётся решение другого уравнения $(ba)y = ab$, $y = a^{-1}b^{-1}ab = (ba)^{-1}ab$. Поэтому прежде чем применять результаты, использующие коммутаторы, проверьте, что понимается в том или ином тексте под коммутатором. В частности, если положить

$$[a, b] = a^{-1}b^{-1}ab, \quad a^b = b^{-1}ab,$$

то предыдущие формулы примут другой вид:

$$\begin{aligned} [a, b][b, a] &= 1; & a^b &= a[a, b]; \\ [a, b^{-1}] &= b[b, a]b^{-1}; & [a^{-1}, b] &= a[b, a]a^{-1}; \\ [ab, c] &= [a, c]^b[b, c]; & [ab, c] &= [a, c] \cdot [[a, c], b] \cdot [b, c]; \\ [a, bc] &= [a, c][a, b]^c; & [a, bc] &= [a, c] \cdot [a, b] \cdot [[a, b], c]; \\ [[a, b], c^a] \cdot [[c, a], b^c] \cdot [[b, c], a^b] &= 1; \\ [[a, b^{-1}], c] \cdot [[b, c^{-1}], a]^c[[c, a^{-1}], b]^a &= 1; \\ [[a, b], c] \cdot [[b, c], a] \cdot [[c, a], b] &= [b, a] \cdot [c, a] \cdot [c, b]^a \cdot [a, b] \cdot [a, c]^b \cdot [b, c]^a \cdot [a, c] \cdot [c, a]^b. \end{aligned}$$

□

Коммутант группы

Коммутант группы G определим как подгруппу

$$G' = [G, G] = \langle [a, b] \mid a, b \in G \rangle$$

группы G , порождённую множеством S всех коммутаторов $[a, b]$, $a, b \in G$.

Теорема 1.10.53.

- 1) $G' = [G, G] = \{[x_1, y_1][x_2, y_2] \dots [x_k, y_k] \mid x_i, y_i \in G\}$ (т. е. коммутант состоит из всех конечных произведений коммутаторов).
- 2) $G' \triangleleft G$ (коммутант группы является нормальной подгруппой группы).

Доказательство.

1) Так как $[a, b]^{-1} = [b, a]$, то $G' = \langle S \rangle$, где S — множество всех коммутаторов, состоит из произведений конечного числа коммутаторов (см. 1.5.6).

2) Так как для $g \in G$ имеем

$$g^{-1}(xy)g = (g^{-1}xg)(g^{-1}yg), \quad g^{-1}[a, b]g = [g^{-1}ag, g^{-1}bg],$$

то

$$\begin{aligned} g^{-1}([x_1, y_1] \dots [x_k, y_k])g &= (g^{-1}[x_1, y_1]g) \dots (g^{-1}[x_k, y_k]g) = \\ &= [g^{-1}x_1g, g^{-1}y_1g] \dots [g^{-1}x_kg, g^{-1}y_kg]. \end{aligned}$$

Итак, $g^{-1}G'g \subseteq G'$ для всех $g \in G$, это означает, что $G' \triangleleft G$. □

Упражнение 1.10.54.

- 1) Группа G коммутативна тогда и только тогда, когда $G' = [G, G] = \{e\}$.
- 2) Привести пример группы G , в которой совокупность коммутаторов не является подгруппой (т. е. произведение двух коммутаторов не является коммутатором).
- 3) Покажите, что любой элемент группы A_5 является коммутатором, в частности, $[A_5, A_5] = A_5$.
- 4) Пусть G — группа, $Z(G)$ — её центр, $(G : Z(G)) = n$. Тогда группа G имеет не более n^2 различных коммутаторов, $[G, G]$ — конечная группа, $|[G, G]| \leq n^{2n^3}$.

Задача 1.10.55. Докажите, что:

$$[S_2, S_2] = \{e\};$$

$$[A_3, A_3] = \{e\};$$

$$[A_4, A_4] = \{1, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\} = V_4;$$

$$[S_n, S_n] = A_n \text{ для всех } n;$$

$$[A_n, A_n] = A_n \text{ при } n \geq 5;$$

если K — поле, то

$$[GL_n(K), GL_n(K)] = SL_n(K) \text{ (кроме } GL_2(\mathbb{Z}_2) = SL_2(\mathbb{Z}_2));$$

$$[SL_n(K), SL_n(K)] = SL_n(K) \text{ (кроме } SL_2(\mathbb{Z}_2), SL_2(\mathbb{Z}_3));$$

если

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}, a, d \neq 0 \right\},$$

то

$$[G, G] = \left\{ \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix} \mid g \in \mathbb{R} \right\}.$$

Взаимный коммутант подгрупп

Пусть A и B — подгруппы группы G и

$$[A, B] = \langle \{[a, b] \mid a \in A, b \in B\} \rangle —$$

подгруппа группы G , порождённая всеми коммутаторами

$$[a, b] = a^{-1}b^{-1}ab, \quad \forall a \in A, \quad \forall b \in B$$

(называемая *взаимным коммутантом* подгрупп A и B).

Если $A \triangleleft G$, то для $a \in A, b \in B$

$$[a, b] = a^{-1}(b^{-1}ab) \in A \cdot A = A,$$

13-23

и поэтому

$$[A, B] \subseteq A.$$

Аналогично, если $B \triangleleft G$, то

$$[a, b] = (a^{-1}b^{-1}a)b \in B \cdot B = B,$$

и поэтому

$$[A, B] \subseteq B.$$

Если же $A \triangleleft G$, $b \triangleleft G$, то

$$[A, B] \triangleleft G, \quad [A, B] \subseteq A \cap B.$$

Коммутант группы как функтор

Пусть

$$G' = [G, G] = \langle aba^{-1}b^{-1} \mid a, b \in G \rangle -$$

коммутант группы G . Если

$$\alpha: G \rightarrow H -$$

гомоморфизм, то

$$\alpha(aba^{-1}b^{-1}) = \alpha(a)\alpha(b)\alpha(a)^{-1}\alpha(b)^{-1},$$

и поэтому α индуцирует гомоморфизм

$$\alpha' = \alpha|_{G'}: G' = [G, G] \rightarrow H' = [H, H],$$

при этом: если α — инъекция, то α' — инъекция; если α — сюръекция, то α' — сюръекция; если α — изоморфизм, то α' — изоморфизм.

Соответствие

$$G \mapsto G' = [G, G], \quad \alpha \mapsto \alpha' = \alpha|_{G'},$$

очевидно, является *ковариантным функтором из категории групп в категорию групп*.

1.11. Решётка нормальных подгрупп

Предложение 1.11.1. Если $\{H_i, i \in I\}$ — совокупность нормальных подгрупп группы G , $H_i \triangleleft G$, то $H = \bigcap_{i \in I} H_i$ — нормальная подгруппа группы G .

Доказательство. Действительно, мы знаем (см. ??), что H — подгруппа. Если $h \in H$ и $g \in G$, то $h \in H_i$ для всех $i \in I$, и так как $H_i \triangleleft G$, то $g^{-1}hg \in H_i$ для всех $i \in I$. Поэтому $g^{-1}hg \in \bigcap_{i \in I} H_i = H$. Итак, $H \triangleleft G$. \square

13-24

Нормальное замыкание подмножества и подгруппы

Пусть S — непустое подмножество группы G . Рассмотрим совокупность всех нормальных подгрупп $H_i \triangleleft G$, $i \in I$, таких, что $S \subseteq H_i$ (эта совокупность непуста, поскольку она содержит саму группу G). Тогда

$$S \subseteq N(S) = \bigcap_{i \in I} H_i \triangleleft G.$$

Покажем в следующей теореме, что: $N(S)$ — наименьшая нормальная подгруппа, содержащая S ; если

$$S^G = \{g^{-1}sg \mid s \in S, g \in G\},$$

то оказывается, что подгруппа $\langle S^G \rangle$, порождённая подмножеством S^G , является наименьшей нормальной подгруппой, содержащей S , и потому она совпадает с $N(S)$.

Теорема 1.11.2 (о нормальном замыкании подмножества группы). Пусть S — непустое подмножество группы G , $\emptyset \neq S \subseteq G$. Тогда:

1) пересечение

$$N(S) = \bigcap_{S \subseteq N_i \triangleleft G} N_i$$

всех нормальных подгрупп $N_i \triangleleft G$ таких, что $S \subseteq N_i$, является наименьшей нормальной подгруппой группы G , содержащей подмножество S (таким образом, нормальное замыкание N непустого подмножества S группы G существует);

2) $N(S) = \langle S^G \rangle = \left\{ \prod_{k=1}^t g_k^{-1} s_k^{\pm 1} g_k \mid t \in \mathbb{N}, s_k \in S, g_k \in G \right\}$ (элементы нормального замыкания подмножества S в группе G — это в точности конечные произведения элементов вида $g^{-1}s^{\pm 1}g$, $s \in S, g \in G$).

Доказательство.

1) Так как пересечение нормальных подгрупп — нормальная подгруппа, то $N = \bigcap N_i \triangleleft G$. Ясно, что $S \subseteq N = \bigcap N_i$, поскольку $S \subseteq N_i$ для всех $\{N_i \triangleleft G \mid S \subseteq N_i, i \in I\}$ (это множество содержит $N_i = G$, и поэтому не является пустым). Таким образом, нормальная подгруппа N , $S \subseteq N$, сама принадлежит этому множеству, т. е. $N = N_i$ для некоторого $i \in I$, и следовательно, $N = \bigcap_{S \subseteq N_i \triangleleft G} N_i$.

2) В силу 1) из $S \subseteq N \triangleleft G$ следует, что

$$\langle S^G \rangle = \left\{ \prod_{k=1}^t g_k^{-1} s_k^{\pm 1} g_k \mid t \in \mathbb{N}, s_k \in S, g_k \in G \right\} \subseteq N.$$

Но ясно, что $\langle S^G \rangle$ — нормальная подгруппа в G , содержащая S . Таким образом, $N \subseteq \langle S^G \rangle$. Итак, $\langle S^G \rangle = N$, и мы имеем общий вид произвольного элемента нормального замыкания $N(S)$. \square

Наиболее часто рассматривается нормальное замыкание $N(H) = \langle H^G \rangle$ подгруппы H группы G , т. е. тот случай, когда $S = H$ — подгруппа в G .

Конец лекции №13.

Лекция № 14 (25 октября 2011 г.)

Гомоморфизмы групп

1.12. Свойства гомоморфизмов групп

81

1.12. Свойства гомоморфизмов групп

Пусть G и G' — группы. Напомним, что отображение $f: G \rightarrow G'$, для которого $f(ab) = f(a)f(b)$ для всех элементов $a, b \in G$, называется *гомоморфизмом*. Биективные гомоморфизмы называются *изоморфизмами* (см. 1.2.1).

Пример 1.12.1. Пусть $G = \mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$ с операцией умножения, $G' = (\mathbb{R}, +)$ с операцией сложения. Так как для отображения $\ln: \mathbb{R}^+ \rightarrow \mathbb{R}$ имеем $\ln(ab) = \ln(a) + \ln(b)$ для всех $a, b \in \mathbb{R}^+$, то \ln — гомоморфизм групп. Так как это — биекция, то \ln — изоморфизм.

Пример 1.12.2. Если $G = S_n$ — группа подстановок и $G' = \{1, -1\}$ — группа с операцией умножения, то отображение $\varepsilon: S_n \rightarrow \{1, -1\}$, для которого $\varepsilon(\sigma) = 1$, если $\sigma \in A_n$, т. е. если σ — чётная подстановка, и $\varepsilon(\sigma) = -1$ для $\sigma \in S_n \setminus A_n$, т. е. для нечётной подстановки σ , является гомоморфизмом групп, поскольку $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ для всех $\sigma, \tau \in S_n$.

Пример 1.12.3. Пусть $G = \mathrm{GL}_n(\mathbb{R})$, $G' = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ с операцией умножения. Так как $|AB| = |A||B|$ для $A, B \in \mathrm{GL}_n(\mathbb{R})$, то отображение $A \mapsto |A|$ из $\mathrm{GL}_n(\mathbb{R})$ в \mathbb{R}^* , ставящее в соответствие матрице A её определитель $|A|$, является гомоморфизмом групп.

Упражнение 1.12.4. Найти все гомоморфизмы $f: G \rightarrow G'$, где $G = \langle a \rangle$, $O(a) = m$, $G' = \langle b \rangle$, $O(b) = n$ (в частности, для $m = 12, n = 15$).

Для гомоморфизмов $f: G \rightarrow G'$ определим:

$$\mathrm{Im}\, f = \{g' \in G' \mid g' = f(g) \text{ для } g \in G\}$$

(образ гомоморфизма f);

$$\mathrm{Ker}\, f = \{g \in G \mid f(g) = e'\},$$

где e' — нейтральный элемент группы G' (ядро гомоморфизма f).

Упражнение 1.12.5. В рассмотренных выше примерах гомоморфизмов групп найти образ и ядро гомоморфизма.

Упражнение 1.12.6. Если G — группа, G' — группоид, $f: G \rightarrow G'$ — гомоморфизм группоидов, то образ

$$\mathrm{Im}(f) = f(G) = \{x = f(g) \mid g \in G\}$$

гомоморфизма f является группой.

Задача 1.12.7. Доказать, что не существует сюръективного гомоморфизма $(\mathbb{Q}, +) \rightarrow (\mathbb{Z}, +)$.

Указание. В $(\mathbb{Q}, +)$ уравнение $nx = a$ имеет (и единственное) решение для любых $n \in \mathbb{N}$, $a \in \mathbb{Q}$.

Задача 1.12.8. Пусть $f: S_n \rightarrow \mathrm{GL}_n(K)$, где $f(\sigma) = A_\sigma = (a_{ij})$ для $\sigma \in S_n$, где

$$a_{ij} = \begin{cases} 1, & \text{если } \sigma(i) = j, \\ 0 & \text{в противном случае.} \end{cases}$$

Доказать, что f — инъективный гомоморфизм, при этом $\varepsilon(\sigma) = |A_\sigma|$ (т. е. $|A_\sigma| = 1$ для чётных подстановок и $|A_\sigma| = -1$ для нечётных подстановок).

Упражнение 1.12.9. Пусть G — группа, $Z(G)$ — центр группы G , $|G : Z(G)| = m$. Покажите, что отображение

$$f: G \rightarrow Z(G), \quad f(g) = g^m \text{ для } g \in G,$$

является гомоморфизмом групп.

Теорема 1.12.10 (свойства гомоморфизма групп). Пусть G и G' — группы, e и e' соответственно — их нейтральные элементы, $f: G \rightarrow G'$ — гомоморфизм групп. Тогда:

- 1) $f(e) = e'$;
- 2) $f(x^{-1}) = (f(x))^{-1}$ для всех $x \in G$;
- 3) $H' = \text{Im } f$ — подгруппа группы G' ;
- 4) если $G = \langle a \rangle$ — циклическая группа, то $\text{Im } f = \langle f(a) \rangle$ также циклическая группа;
- 4') если $O(a) < \infty$ для $a \in G$, то $O(f(a))$ является делителем числа $O(a)$ (если f — инъективный гомоморфизм, то $O(f(a)) = O(a)$);
- 5) $f(g^{-1}hg) = (f(g))^{-1}f(h)f(g)$;
- 6) $f([g, h]) = [f(g), f(h)]$, и следовательно, $f([G, G]) = [f(G), f(G)]$;
- 7) $\text{Ker } f$ — нормальная подгруппа группы G ;
- 8) для $x, y \in G$ $f(x) = f(y)$ тогда и только тогда, когда $xy^{-1} \in \text{Ker } f$;
- 9) f — инъективное отображение тогда и только тогда, когда $\text{Ker } f = \{e\}$.

Доказательство.

- (1) Так как $u = f(e) = f(e^2) = f(e)f(e) = u^2$, то $u = e'$, т. е. $f(e) = e'$.
- (2) Так как $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e'$ и $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$, то $f(x^{-1}) = (f(x))^{-1}$.
- (3) Если $h'_1 = f(g_1)$ и $h'_2 = f(g_2)$ — элементы из $\text{Im } f$, где $g_1, g_2 \in G$, то

$$h'_1 h'_2 = f(g_1)f(g_2) = f(g_1g_2) \in \text{Im } f.$$

Если $h' = f(g) \in \text{Im } f$, $g \in G$, то

$$(h')^{-1} = (f(g))^{-1} = f(g^{-1}) \in \text{Im } f.$$

Итак, $\text{Im } f$ — подгруппа группы G' .

- (4) Если $G = \langle a \rangle$ и $h' \in \text{Im } f$, $h' = f(g)$, $g \in G$, то $g = a^n$, $n \in \mathbb{Z}$, и поэтому

$$h' = f(g) = f(a^n) = (f(a))^n.$$

Итак, $\text{Im } f = \langle f(a) \rangle$ — циклическая группа с образующим $f(a)$.

- (4') Пусть $n = O(a)$. Тогда $a^n = e$, и поэтому

$$(f(a))^n = f(a^n) = f(e) = e'.$$

Следовательно, число $O(f(a))$ является делителем числа $n = O(a)$.

Если же f — инъективный гомоморфизм и $m = O(f(a))$, то

$$e' = (f(a))^m = f(a^m),$$

поэтому $a^m = e$, и следовательно, $n = O(a)$ является делителем числа m . Таким образом, $O(a) = n = m = O(f(a))$.

5) и 6) следуют из 2).

7) Если $h_1, h_2 \in H = \text{Ker } f$, то $f(h_1) = e'$, $f(h_2) = e'$. Поэтому $f(h_1 h_2) = f(h_1)f(h_2) = e' \cdot e' = e'$, т. е. $h_1 h_2 \in \text{Ker } f$.

Если $h \in \text{Ker } f$, то $f(h) = e'$, и поэтому $f(h^{-1}) = (f(h))^{-1} = (e')^{-1} = e'$, т. е. $h^{-1} \in \text{Ker } f$. Таким образом, $\text{Ker } f$ — подгруппа группы G .

Если $h \in H = \text{Ker } f$, то $f(h) = e'$. Для любого элемента $g \in G$ имеем

$$f(g^{-1}hg) = f(g^{-1})f(h)f(g) = f(g)^{-1}e'f(g) = e'.$$

Таким образом, $g^{-1}(\text{Ker } f)g \subseteq \text{Ker } f$ для всех элементов $g \in G$, т. е. $\text{Ker } f$ — нормальная подгруппа группы G .

$$8) f(x) = f(y) \iff e' = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \iff xy^{-1} \in \text{Ker } f.$$

9) а) Если $\text{Ker } f = \{e\}$, то из $f(x) = f(y)$ следует, что $xy^{-1} = e$, т. е. что $x = y$, другими словами, f — инъективное отображение.

б) Если f — инъективное отображение, то, так как $f(e) = e'$, из $f(x) = e'$ следует, что $x = e$, т. е. $\text{Ker } f = \{e\}$. \square

Теорема 1.12.11 (теорема Кэли). Пусть G — группа, H — её подгруппа, L — множество всех левых смежных классов группы G по подгруппе H , $\varphi: G \rightarrow S(L)$, $S(L)$ — группа подстановок на множестве L , $\varphi(g)(xH) = gxH$ для $x, g \in G$. Тогда:

1) φ — гомоморфизм групп;

$$2) \text{Ker } \varphi = \bigcap_{x \in G} xHx^{-1}.$$

Доказательство.

1) Если $x, g_1, g_2 \in G$, то

$$\varphi(g_1g_2)(xH) = (g_1g_2)xH = g_1(g_2xH) = \varphi(g_1)(\varphi(g_2)(xH)),$$

поэтому $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$.

2) Ясно, что:

$$g \in \text{Ker } \varphi \iff \{xH = gxH \ \forall xH\} \iff \{g \in xHx^{-1} \ \forall x \in G\}. \quad \square$$

Следствие 1.12.12. При $H = \{e\}$, $L = G$, $S(G)$ — группа подстановок на множестве G :

а) $\varphi: G \rightarrow S(G)$, $\varphi(g)(x) = gx$ для $x, g \in G$, является левым регулярным представлением группы G , оно осуществляет вложение группы G в группу $S(G)$, поскольку $\text{Ker } \varphi = \bigcap_{x \in G} xex^{-1} = \{e\}$;

б) конечная группа G вкладывается в группу подстановок S_m , где $m = |G|$;

- в) конечная группа G вкладывается в линейную группу $\mathrm{GL}_m(F)$ над любым полем F , где $m = |G|$, если принять во внимание каноническое вложение группы S_m в $\mathrm{GL}_m(F)$, $\sigma \mapsto A_\sigma = (a_{ij})$,

$$a_{ij} = \begin{cases} 1, & \text{если } \sigma(j) = i, \\ 0, & \text{если } \sigma(j) \neq i. \end{cases}$$

Следствие 1.12.13. Если H — подгруппа конечного индекса m группы G , то H содержит нормальную подгруппу N , индекс которой делится на m и делит число $m!$.

Доказательство. Применим в этом случае теорему Кэли и рассмотрим нормальную подгруппу $N = \mathrm{Ker} \varphi \triangleleft G$, $N \subseteq H$, индекс которой в группе G равен порядку $|\mathrm{Im} \varphi|$ подгруппы $\mathrm{Im} \varphi$ группы $S(L) = S_m$, и поэтому этот индекс делит число $m! = |S_m|$.

Так как $\mathrm{Ker} \varphi \subseteq H \subseteq G$, то $(G : \mathrm{Ker} \varphi) = (G : H) \cdot (H : \mathrm{Ker} \varphi)$, то индекс $(G : \mathrm{Ker} \varphi)$ делится на $m = (G : H)$. \square

Упражнение 1.12.14. Пусть K — подгруппа группы G , H — нормальная подгруппа в K , $H \triangleleft K \subseteq G$, $f: G \rightarrow G'$ — гомоморфизм групп. Тогда

$$f(H) \triangleleft f(K) \subseteq G'.$$

Действительно, мы знаем, что $f(H)$, $f(K)$ — подгруппы группы G' . Ясно, что $f(H) \subseteq f(K)$. Если $y = f(x) \in f(K)$ для $x \in K$, то $y^{-1}f(H)y = f(y^{-1}Hy) = f(H)$. Итак, $f(H) \triangleleft f(K)$. \square

Упражнение 1.12.15. Пусть R — кольцо, I — двусторонний идеал кольца R , $G = \mathrm{GL}_n(R)$ — группа обратимых $(n \times n)$ -матриц над кольцом R . Положим

$$G_I = \{A \in \mathrm{GL}_n(R) \mid A - E \in M_n(I)\}.$$

Тогда

$$G_I \trianglelefteq G = \mathrm{GL}_n(R)$$

(нормальная подгруппа G_I в $G = \mathrm{GL}_n(R)$ называется *главной конгруэнц-подгруппой* для идеала I).

Всякий гомоморфизм колец

$$f: R \rightarrow R'$$

индуцирует гомоморфизм линейных групп

$$\begin{aligned} f_G: G = \mathrm{GL}_n(R) &\rightarrow G' = \mathrm{GL}_n(R'), \\ A = (a_{ij}) &\mapsto f_G(A) = (f(a_{ij})), \end{aligned}$$

при этом

$$\mathrm{Ker} f_G = G_{\mathrm{Ker} f}.$$

Если $I \triangleleft R$ и $\pi: R \rightarrow R/I$ — канонический гомоморфизм, $\mathrm{Ker} \pi = I$, то

$$\pi_G: G = \mathrm{GL}_n(R) \rightarrow G' = \mathrm{GL}_n(R/I) —$$

гомоморфизм линейных групп, ядро которого $\mathrm{Ker} \pi_G = G_I \trianglelefteq \mathrm{GL}_n(R)$ (обозначается также в литературе как $\mathrm{GL}_n(R, I)$).

Подгруппы группы подстановок S_n

Для любого $k < n$ группа S_k содержит подгруппу

$$\left\{ \begin{pmatrix} 1 & 2 & \dots & k & k+1 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(k) & k+1 & \dots & n \end{pmatrix} \mid \sigma \in S_k \right\},$$

изоморфную группе S_k . По теореме Кэли каждая группа G из $n = |G|$ элементов вложима в группу S_n , т. е. группа S_n среди своих подгрупп содержит все подгруппы порядка $k \leq n$.

При малых n :

$n = 2$, $|S_2| = 2$; все подгруппы в S_2 — это единичная подгруппа $\{e\}$ и вся группа S_2 ;

$n = 3$, $|S_3| = 3! = 6$, порядки собственных подгрупп могут быть 1, 2, 3, простые числа, поэтому все собственные подгруппы являются циклическими, таким образом, подгруппы

$$\begin{aligned} \langle e \rangle &= \{e\}, \quad \langle (2 \ 3) \rangle = \{e, (2 \ 3)\}, \quad \langle (1 \ 2) \rangle = \{e, (1 \ 2)\}, \\ \langle (1 \ 3) \rangle &= \{e, (1 \ 3)\}, \quad \langle (1 \ 2 \ 3) \rangle = \{e, (1 \ 2 \ 3), (1 \ 3 \ 2)\} = \langle (1 \ 3 \ 2) \rangle \end{aligned}$$

порядков 1, 2, 2, 2, 3 соответственно и, конечно, вся группа S_3 , $|S_3| = 6$.

Упражнение 1.12.16. Напишите программу для компьютера, перечисляющую все неизоморфные группы фиксированного порядка n . Проверьте работу программы для $n = 8$.

1.13. Фактор-группа по нормальной подгруппе, канонический гомоморфизм

Пусть G — группа, H — её нормальная подгруппа, $G/H = \{xH = Hx \mid x \in G\}$ — множество смежных классов по подгруппе H . Определим на множестве G/H операцию умножения, полагая $xH \cdot yH = xyH$.

Проверим корректность этого определения (т. е. что умножение смежных классов не зависит от выбора их представителей).

Действительно, пусть $xH = x'H$, $yH = y'H$. Тогда $x' = xh_1$, $y' = yh_2$, где $h_1, h_2 \in H$. Следовательно, $x'y' = xh_1yh_2 = xyh_1'h_2$, где $h_1y = yh_1'$ (поскольку $Hy = yH$) для $h_1' \in H$. Так как $h_1'h_2 \in H$, то $x'y' = xyh_1'h_2 \in xyH$, и поэтому $x'y'H = xyH$.

Для любых $x, y, z \in G$ имеем

$$(xHyH)zH = (xy)zH = x(yz)H = xH(yHzH),$$

т. е. операция умножения смежных классов ассоциативна.

Замечание 1.13.1. Если $x, y \in G$, $H \triangleleft G$, то $Hy = yH$, $HH = H$, и поэтому

$$(xH)(yH) = x(Hy)H = x(yH)H = (xy)(HH) = xyH$$

(здесь мы рассматриваем произведение подмножеств xH и yH группы G). Таким образом, выбранное нами формальное определение произведения смежных классов $xH \cdot yH = xyH$ — это, на самом деле, произведение этих смежных классов как подмножеств группы. Так как произведение подмножеств группы ассоциативно, получаем другое доказательство того факта, что операция произведения смежных классов также ассоциативна.

Ясно, что для $H = eH$ имеем

$$eHxH = exH = xH = xeH = xHeH$$

для всех $xH \in G/H$, т. е. $H = eH$ — нейтральный элемент.

Для всякого $xH \in G/H$ из

$$(xH)(x^{-1}H) = xx^{-1}H = eH = H,$$

$$(x^{-1}H)(xH) = x^{-1}xH = eH = H$$

получаем, что $(xH)^{-1} = x^{-1}H$, т. е. у каждого смежного класса xH имеется обратный элемент $(xH)^{-1} = x^{-1}H$.

Таким образом, мы доказали первое утверждение следующей теоремы.

Теорема 1.13.2. Если $H \triangleleft G$, то:

- 1) множество смежных классов $G/H = \{xH = Hx \mid x \in G\}$ группы G по её нормальной подгруппе $H \triangleleft G$ с операцией $xH \cdot yH = xyH$ является группой (называемой фактор-группой группы G по нормальной подгруппе H);
- 2) отображение $\pi = \pi_H: G \rightarrow G/H$, для которого $\pi(x) = xH$, $x \in G$, является сюръективным гомоморфизмом (называемым каноническим гомоморфизмом);
- 3) $\text{Ker } \pi_H = H$;
- 4) если $|G| < \infty$, то $|G/H| = \frac{|G|}{|H|} = (G : H)$.

Доказательство. Осталось проверить 2), 3) и 4). Действительно, для $a, b \in G$ имеем

$$\pi(ab) = abH = aH \cdot bH = \pi(a)\pi(b),$$

т. е. $\pi = \pi_H$ — гомоморфизм.

Если $g \in G$, то $gH = \pi(g)$, т. е. π — сюръекция.

Если $a \in G$, то $a \in \text{Ker } \pi_H$ тогда и только тогда, когда $\pi(a) = aH = H$. Но это равносильно тому, что $a \in H$. Итак, $\text{Ker } \pi_H = H$.

4) следует из теоремы Лагранжа. □

Следствие 1.13.3. Нормальные подгруппы H группы G и только они являются ядрами гомоморфизмов $f: G \rightarrow G'$ из группы G во все группы G' .

Примеры фактор-групп

- 1) Пусть $H = \{e\} \triangleleft G$. Тогда $x\{e\} = x$ для всех $x \in G$, т. е. все смежные классы по единичной подгруппе — это в точности одноэлементные подмножества, т. е. элементы группы G , при этом

$$x\{e\} \cdot y\{e\} = xy\{e\} = xy.$$

Таким образом, биекция $x\{e\} \mapsto x$, $G/\{e\} \rightarrow G$ является изоморфизмом групп.

- 2) Пусть $H = G \triangleleft G$. Тогда имеем один смежный класс $\bar{e} = eG = G$. Итак, $G/G = \{\bar{e}\}$, $|G/G| = 1$.

3) Группа \mathbb{Z}_n вычетов по модулю n как фактор-группа группы $(\mathbb{Z}, +)$ по подгруппе $n\mathbb{Z}$. Пусть $G = \mathbb{Z}$ — группа целых чисел с операцией сложения, n — натуральное число и $H = n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\}$ — подгруппа целых чисел, делящихся на n . Для $k \in \mathbb{Z}$ рассмотрим смежный класс

$$C_k = k + n\mathbb{Z} = \{k + nq \mid q \in \mathbb{Z}\}.$$

Ясно, что $C_k = C_l$ для $l \in \mathbb{Z}$ тогда и только тогда, когда $k - l = nq$. Так как $k = nq + r$, где $q \in \mathbb{Z}$, $0 \leq r < n$, то $C_k = C_r$. Таким образом, множество всех различных смежных классов $\mathbb{Z}_n = G/H = \mathbb{Z}/n\mathbb{Z} = \{C_0, C_1, \dots, C_{n-1}\}$ находится в биективном соответствии с остатками $\{0, 1, 2, \dots, n-1\}$ при делении на число n . Если $k, l \in \mathbb{Z}$ и $k + l = nq + r$, то

$$C_k + C_l = (k + n\mathbb{Z}) + (l + n\mathbb{Z}) = (k + l) + n\mathbb{Z} = r + n\mathbb{Z} = C_r.$$

Таким образом, операция сложения фактор-группы $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ в точности соответствует операции сложения остатков при делении на n по модулю числа n (т. е. сначала надо сложить остатки как целые числа, а затем от суммы взять остаток при её делении на n). Таким образом, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ — группа, более того, $\mathbb{Z}_n = \langle C_1 \rangle$ — циклическая группа, $|\mathbb{Z}_n| = n$. Конечно, это можно было бы проверить и непосредственно для группы остатков (вычетов) $\{0, 1, 2, \dots, n-1\}$.

Примеры таблиц сложения:

	+	0	1
+	0	1	
0	0	1	
1	1	0	

для \mathbb{Z}_2

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

для \mathbb{Z}_3

4) В фактор-группе \mathbb{Q}/\mathbb{Z} любой элемент имеет конечный порядок; для любого натурального числа n существует единственная подгруппа группы \mathbb{Q}/\mathbb{Z} порядка n .

5) Фактор-группа \mathbb{R}/\mathbb{Z} имеет естественную интерпретацию как группа $T = \{z \in \mathbb{C} \mid |z| = 1\}$ единичной окружности (или поворотов плоскости вокруг начала координат против часовой стрелки на угол φ , что равносильно умножению на комплексное число $\cos \varphi + i \sin \varphi$), а именно биекция

$$f: \mathbb{R}/\mathbb{Z} \rightarrow T, \quad f(r + \mathbb{Z}) = \cos 2\pi r + i \sin 2\pi r,$$

осуществляет изоморфизм групп \mathbb{R}/\mathbb{Z} и T , поскольку

$$\begin{aligned} f((r_1 + \mathbb{Z}) + (r_2 + \mathbb{Z})) &= f((r_1 + r_2) + \mathbb{Z}) = \\ &= \cos 2\pi(r_1 + r_2) + i \sin 2\pi(r_1 + r_2) = \\ &= (\cos 2\pi r_1 + i \sin 2\pi r_1)(\cos 2\pi r_2 + i \sin 2\pi r_2) = \\ &= f(r_1 + \mathbb{Z}) \cdot f(r_2 + \mathbb{Z}). \end{aligned}$$

6) Пусть $G = \langle a \rangle$ — конечная циклическая группа, $|G| = O(a) = n$, $d \geq 0$. Тогда

$$\tilde{G} = G/\langle a^d \rangle = \langle \bar{a} \rangle, \quad |\tilde{G}| = O(\bar{a}) = \text{НОД}(n, d).$$

Теорема 1.13.4 (о подгруппах фактор-группы). Пусть H — нормальная подгруппа группы G , $\pi: G \rightarrow G/H$ — канонический гомоморфизм. Соответствие

$$K \mapsto \bar{K} = K/H = \pi(K)$$

является биекцией между множеством всех подгрупп K группы G , содержащих нормальную подгруппу H , $K \supseteq H$, и всеми подгруппами \bar{K} фактор-группы G/H (обратное соответствие $\bar{K} \mapsto K = \pi^{-1}(\bar{K}) \supseteq H$), при этом:

- a) $L \supseteq K \supseteq H$ тогда и только тогда, когда $\bar{L} \supseteq \bar{K}$;
- b) $G \triangleright K \supseteq H$ тогда и только тогда, когда $G/H \triangleright K/H$.

Доказательство.

1) Пусть \bar{K} — подгруппа группы G и $K \supseteq H \subseteq \bar{K}$. Так как $H \triangleleft G$, то $H \triangleleft K$. Ясно, что фактор-группа $K/H = \{xH \mid x \in K\}$ является подгруппой фактор-группы G/H . Если L — подгруппа группы G , $H \subseteq L$, то из $K/H = L/H$ следует, что $K = L$. Действительно, если $k \in K$, то $kH = lH$ для $l \in L$, поэтому $k = lh$ для $h \in H \subseteq L$, следовательно, $K \subseteq L$. Симметрично $L \subseteq K$. Итак, $K = L$, что означает инъективность нашего соответствия.

2) Если \bar{K} — подгруппа фактор-группы $\bar{G} = G/H$, то рассмотрим

$$K = \pi^{-1}(\bar{K}) = \{x \in G \mid \pi(x) = xH \in \bar{K}\}.$$

Если $x, y \in K$, то $xH, yH \in \bar{K}$, поэтому

$$\pi(xy) = (xy)H = xHyH \in \bar{K},$$

$$\pi(x^{-1}) = x^{-1}H = (xH)^{-1} \in \bar{K}.$$

Таким образом, $xy, x^{-1} \in K$, следовательно, K — подгруппа группы G . Ясно, что $H = \pi^{-1}(\bar{H}) \subseteq K$ и $\pi(K) = K/H = \bar{K}$. Итак, наше соответствие сюръективно.

3) Если $L \supseteq K \supseteq H$, то $\bar{L} = \pi(L) \supseteq \pi(K) = \bar{K}$. Если $L \supseteq H$, $K \supseteq H$ и $\pi(L) \supseteq \pi(K)$, то

$$\bar{L} = \pi^{-1}(\pi(L)) \supseteq \pi^{-1}(\pi(K)) = K.$$

4) Если $g \in G$ и $k \in K$, то

$$(gH)(kH)(gH)^{-1} = (gkg^{-1})H,$$

и поэтому $K/H \triangleleft G/H$ тогда и только тогда, когда $K \triangleleft G$. □

Следствие I.13.5. Пусть $H \triangleleft G$, $\pi: G \rightarrow G/H = \bar{G}$ — канонический сюръективный гомоморфизм, \bar{S} — подгруппа группы \bar{G} индекса n , $n = (\bar{G} : \bar{S})$, тогда $S = \pi^{-1}(\bar{S})$ ($H \subseteq S$, $\pi(S) = \bar{S}$) — подгруппа группы G индекса n , $(G : S) = n$.

Доказательство. Пусть

$$\bar{G} = \bigcup_{i=1}^n \bar{S}\bar{g}_i, \quad \bar{g}_i = \pi(g_i) \in \bar{G}, \quad g_i \in G, \quad$$

разбиение группы \bar{G} на смежные классы по подгруппе \bar{S} .

Если $g \in G$, то

$$\pi(g) \in \bar{S}\bar{g}_i = \pi(S)\pi(g_i) = \pi(Sg_i)$$

для некоторого $1 \leq i \leq n$, и поэтому

$$g \in \text{Ker } \pi \cdot Sg_i = H \cdot Sg_i \subseteq Sg_i.$$

Если $Sg_i = Sg_j$, то

$$\bar{S}g_i = \pi(Sg_i) = \pi(Sg_j) = \bar{S}g_j.$$

Поэтому $G = \bigcup_{i=1}^n Sg_i$ — разбиение группы G на смежные классы по подгруппе S , $(G : S) = n$. \square

Следствие 1.13.6. Пусть $N \triangleleft G$, $N \neq G$. Тогда N — максимальная нормальная подгруппа в G (это означает, что $N \neq G$, $H \triangleleft G$, $N \subset H$ влечёт $H = N$ или $H = G$) тогда и только тогда, когда G/N — простая группа.

Следствие 1.13.7. Пусть H и K — различные максимальные нормальные подгруппы группы G . Тогда $H \cap K$ — максимальная нормальная подгруппа как группы H , так и группы K .

Доказательство. Так как

$$H/(H \cap K) \cong HK/K, \quad K \triangleleft HK \triangleleft G,$$

то или $HK = K$ (и тогда $H \subset K$, что невозможно), или $HK = G$. Поэтому $H/(H \cap K) \cong G/K$ — простая группа, следовательно, $H \cap K$ — максимальная нормальная подгруппа группы H (аналогично, группы K). \square

Предложение 1.13.8.

- 1) Пусть G — группа, $[G, G]$ — её коммутант, тогда $G/[G, G]$ — коммутативная группа.
- 2) Если $H \triangleleft G$, то G/H — коммутативная группа тогда и только тогда, когда $[G, G] \subseteq H$.

Доказательство.

- 1) $[xH, yH] = [x, y]H = H$ для $H = [G, G] \triangleleft G$.
- 2) Если $H \triangleleft G$ и $x, y \in G$, то

$$xyH = xHyH = yHxH = yxH$$

тогда и только тогда, когда

$$[x, y]H = [xH, yH] = H,$$

что эквивалентно $[x, y] \in H$. Итак, коммутативность группы G/H равносильна тому, что $[G, G] = \langle [x, y] \mid x, y \in G \rangle \subseteq H$. \square

Предложение 1.13.9. Если $Z = Z(G) < G$ (т. е. группа G не является абелевой), то фактор-группа $G/Z(G)$ не является циклической группой.

Доказательство. Допустим противное, т. е. что $G/Z = (aZ)$, $a \in G$. Пусть $b, c \in G$, тогда

$$\begin{aligned} bZ &= (aZ)^k = a^k Z \\ cZ &= (aZ)^l = a^l Z \end{aligned} \Rightarrow \begin{aligned} b &= a^k z_1, \quad z_1 \in Z \\ c &= a^l z_2, \quad z_2 \in Z. \end{aligned}$$

Тогда:

$$\begin{aligned} bc &= a^k z_1 a^l z_2 = a^k a^l z_1 z_2 = a^{k+l} z_1 z_2; \\ cb &= a^l z_2 a^k z_1 = a^l a^k z_2 z_1 = a^{k+l} z_1 z_2. \end{aligned}$$

Итак, $bc = cb$ для всех $b, c \in G$, следовательно, $Z = Z(G) = G$, что противоречит нашему предположению. \square

1.14. Умножение подмножеств группы

Для группы G через $P^*(G)$ обозначим множество всех непустых подмножеств множества G . Если $S, T \in P^*(G)$, то положим

$$ST = \{st \mid s \in S, t \in T\}.$$

Так как операция умножения в группе G ассоциативна, то и операция произведения подмножеств $(S, T) \mapsto ST$ также ассоциативна, поскольку

$$(ST)U = \{(st)u = s(tu) \mid s \in S, t \in T, u \in U\} = S(TU)$$

для любых $S, T, U \in P^*(G)$.

Если $S = \{s\}$, то $ST = \{s\} \cdot T = sT$, $Ts = T \cdot \{s\} = Ts$. В частности, для $s = e$ имеем

$$eS = S = Se,$$

поэтому $\{e\} \in P^*(G)$ — нейтральный элемент в $(P^*(G), \cdot)$. Итак, $(P^*(G), \cdot)$ — моноид.

Замечание 1.14.1. Моноид $(P^*(G), \cdot)$ является группой тогда и только тогда, когда $|G| = 1$ (для $S \in P^*(G)$ с $|S| > 1$ не существует обратный элемент).

Моноид $P^*(G)$ группы G позволяет несколько в ином ракурсе рассматривать произведения HK подгрупп H и K группы G и (левые) смежные классы $aH = \{a\} \cdot H$ как результат применения операции произведения к элементам $H, K, \{a\}$ моноида $P^*(G)$. В частности, совокупность левых смежных классов $G/H = \{aH \mid a \in G\}$ лежит в $P^*(G)$. В этом контексте моноида $P^*(G)$ отметим возможное введение фактор-группы и повторим ряд утверждений, доказанных ранее (см. 1.9.30, 1.10.20, 1.10.21).

Предложение 1.14.2. Пусть G — группа.

- 1)
 - a) Если H и K — подгруппы группы G , то их произведение HK является подгруппой тогда и только тогда, когда $HK = KH$ (т. е. когда они перестановочны в моноиде $P^*(G)$; это не означает перестановочности элементов из H с элементами из K !).
 - b) Если к тому же H — нормальная подгруппа, то HK ($= (KH)$) — подгруппа;
 - v) Если к тому же H и K — нормальные подгруппы, то HK ($= (KH)$) — нормальная подгруппа.
- 2) Пусть $a, b \in G$ и H — подгруппа группы G . Если $(aH)(bH) = cH$, где $c \in G$, то $cH = abH$ (в частности, если множество левых смежных классов $G/H = \{aH \mid a \in G\}$ замкнуто в $P^*(G)$ относительно умножения моноида $P^*(G)$, то $(aH)(bH) = abH$ для всех $a, b \in G$).
- 3) Если H — подгруппа группы G , то $(aH)(bH) = abH$ для всех $a, b \in G$ тогда и только тогда, когда $gHg^{-1} = H$ для всех $g \in G$ (такая подгруппа H была названа нормальной подгруппой, см. 1.10.1, обозначение: $H \triangleleft G$).
- 4) Если N — нормальная подгруппа группы G , то фактор-группа (множество левых смежных классов) $G/N = \{aN \mid a \in G\}$ является подгруппой моноида $P^*(G)$.

Доказательство. 1) а) Если HK — подгруппа, то

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH.$$

б) Пусть $HK = KH$. Тогда:

$$\begin{aligned}(HK)(HK) &= H(KH)K = H(HK)K = HHKK = HK; \\ (HK)^{-1} &= K^{-1}H^{-1} = KH = HK.\end{aligned}$$

Итак, HK — подгруппа группы G (см. также 1.9.30).

Доказательства п. б) и в) см. в 1.10.20 и 1.10.21.

2) Если $(aH)(bH) = cH$, то $ab \in cH$, и поэтому $cH = abH$; следовательно, $(aH)(bH) = cH = abH$.

3) Если $(aH)(bH) = abH$ для всех $a, b \in G$, то для $g \in G$ имеем

$$gHg^{-1} \subseteq gHg^{-1}H = gg^{-1}H = eH = H.$$

Заменяя g на g^{-1} , получаем $g^{-1}Hg \subseteq H$, и поэтому $H \subseteq gHg^{-1}$. Итак, $gHg^{-1} = H$ для всех $g \in G$.

4) Мы уже знаем, что G/N замкнуто относительно операции умножения в $P^*(G)$, которая ассоциативна. Так как

$$(eN)(aN) = eaN = aN = aeN = (aN)(eN),$$

то $eN = N$ — нейтральный элемент в G/N . Так как

$$(aN)(a^{-1}N) = aa^{-1}N = eN = N = a^{-1}aN = (a^{-1}N)(aN),$$

то $a^{-1}N$ является обратным элементом для aN в $G/N \subseteq P^*(G)$. Итак, G/N — подгруппа в $P^*(G)$. \square

Упражнение 1.14.3. Пусть G — группа, H — такое конечное подмножество элементов группы G , что $HH = H$. Покажите, что H — подгруппа группы G .

Предыдущее утверждение не имеет места, если X — бесконечное множество. Например, $G = \mathbb{Z}$, X — подмножество всех натуральных чисел.

Пример 1.14.4. H, K — подгруппы группы G , однако HK не является группой. Пусть $G = \text{GL}_2(\mathbb{Q})$.

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{Q} \right\}, \quad K = \left\{ \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \mid b \in \mathbb{Q} \right\}.$$

Тогда H, K — подгруппы группы G ,

$$HK = \left\{ \begin{pmatrix} 1+ab & a \\ b & 1 \end{pmatrix} \mid a, b \in \mathbb{Q} \right\},$$

при этом

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in HK,$$

однако

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \notin HK.$$

Таким образом, HK не является подгруппой группы G .

1.15. Продолжение рассмотрения свойств гомоморфизмов групп

Лемма 1.15.1. Если G, G', G'' — группы, $f: G \rightarrow G'$, $g: G' \rightarrow G''$ — гомоморфизмы, то их произведение $gf: G \rightarrow G''$ — гомоморфизм.

Доказательство. Пусть $a, b \in G$. Тогда

$$(gf)(ab) = g[f(ab)] = g[f(a)f(b)] = [(gf)(a)][(gf)(b)]. \quad \square$$

Лемма 1.15.2. Пусть G, G' — группы, $f: G \rightarrow G'$ — гомоморфизм. Тогда:

- 1) f — инъекция в том и только в том случае, когда $\text{Ker } f = \{e\}$;
- 2) f — биекция в том и только в том случае, когда $\text{Ker } f = \{e\}$, $\text{Im } f = G'$.

Доказательство. Достаточно доказать 1). Если f — инъекция, то, учитывая равенство $f(e) = e'$, видим, что $\text{Ker } f = \{e\}$. Пусть теперь $\text{Ker } f = \{e\}$. Если $f(a) = f(b)$ для $a, b \in G$, то $f(a^{-1}b) = f(a^{-1})f(b) = [f(a)]^{-1}f(b) = e'$, т. е. $a^{-1}b \in \text{Ker } f = \{e\}$. Поэтому $a^{-1}b = e$, т. е. $a = b$. Итак, f — инъекция. \square

1.16. Свойства изоморфизмов групп (продолжение)

Определение 1.16.1. Пусть G, G' — группы. Напомним, что отображение $f: G \rightarrow G'$ называем *изоморфизмом* (см. 1.2.1), если:

- 1) f — гомоморфизм;
- 2) f — биекция.

Группы G и G' называются *изоморфными*, если существует какой-либо изоморфизм $f: G \rightarrow G'$ (обозначение $G \cong G'$).

Замечание 1.16.2. Пусть G и G' — две группы, $f: G \rightarrow G'$, $f': G' \rightarrow G$ — гомоморфизмы групп. Если $f'f = 1_G$ и $ff' = 1_{G'}$, то f и f' — изоморфизмы групп ($f' = f^{-1}$, $f = (f')^{-1}$).

Действительно, из $f'f = 1_G$, $ff' = 1_{G'}$ следует, что f и f' — взаимно обратные биекции, $f' = f^{-1}$, $f = (f')^{-1}$. Так как f и f' — гомоморфизмы групп, то, следовательно, они являются взаимно обратными изоморфизмами групп. \square

Примеры 1.16.3.

- ✓ 1) $(\mathbb{R}^+, \cdot) = (\{r \in \mathbb{R} \mid r > 0\}, \cdot) \xrightarrow{\ln} (\mathbb{R}, +)$, $r \mapsto \ln(r)$, — изоморфизм групп;
- ✓ 2) $(\mathbb{R}, +) \rightarrow (\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}, \cdot)$, $x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, — изоморфизм групп;
- ✓ 3) $\mathbb{Z} \rightarrow 2\mathbb{Z}$, $n \mapsto 2n$, — изоморфизм групп;
- ✓ 4) любая группа порядка 4 изоморфна или циклической группе \mathbb{Z}_4 , или четвёртой группе Клейна $\{e, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\}$;

- 5) абелевы группы (\mathbb{Q}^+, \cdot) всех положительных рациональных чисел с операцией умножения и $(\mathbb{Q}, +)$ всех рациональных чисел с операцией сложения уже не являются изоморфными (ср. п. 1).

Указание. Группа $(\mathbb{Q}, +)$ делимая (это означает, что в ней уравнение $nx = a$ разрешимо для всех $n \in \mathbb{N}$ и для всех $a \in \mathbb{Q}$); в то же время уравнение $x^2 = 2$ в группе (\mathbb{Q}^+, \cdot) не имеет решения;

- ✓ 6) любой сюръективный гомоморфизм конечной группы на себя является автоморфизмом;

- ✓ 7) $S_3 \cong \mathrm{SL}_2(\mathbb{Z}_2) \cong \mathrm{GL}_2(\mathbb{Z}_2)$.

Указание. а) $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle$, покажите, что отображение

$$(1\ 2) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (1\ 2\ 3) \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

продолжается до изоморфизма групп

$$S_3 \cong \mathrm{GL}_2(\mathbb{Z}_2);$$

- б) в двумерном пространстве $\mathbb{Z}_2 V = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ над полем \mathbb{Z}_2 имеются ровно три базиса; каждое обратимое линейное преобразование осуществляет подстановку на множестве базисов линейного пространства, при этом $|\mathrm{GL}_2(\mathbb{Z}_2)| = 6$.

- 8) $S_m \cong S_n$ тогда и только тогда, когда $m = n$. Итак, в бесконечном семействе групп подстановок $\{S_n \mid n \in \mathbb{N}\}$ никакие две различные группы не являются изоморфными.

Действительно, если $S_m \cong S_n$, то $m! = |S_m| = |S_n| = n!$, поэтому $m = n$.

Если $m = n$, то $S_m = S_n$, и поэтому, конечно, $S_m \cong S_n$. \square

- 9) Если G — конечная группа, H — подгруппа группы G , $H \neq G$, то $H \not\cong G$. Действительно, так как $|H| < |G|$, то $|H| \neq |G|$, и поэтому $H \not\cong G$.

Однако $2\mathbb{Z} < \mathbb{Z}$, но $2\mathbb{Z} \cong \mathbb{Z}$.

Представления групп подстановками, теорема Кэли

Ещё раз вернёмся к теореме Кэли (см. 1.12.11) в несколько более упрощённом варианте.

Теорема 1.16.4 (теорема Кэли). Каждая группа изоморфна некоторой подгруппе группы подстановок (в частности, группа G , $|G| = n < \infty$, вложима как подгруппа в группу подстановок $S(G) = S_n$).

Доказательство. Пусть G — группа. Каждому элементу $a \in G$ поставим в соответствие отображение

$$f_a: G \rightarrow G, \quad f_a(x) = ax \text{ для } x \in G.$$

Так как из $ax = ax'$ следует, что $x = x'$, то f_a — инъекция. Поскольку $y = a(a^{-1}y) = f_a(a^{-1}y)$ для любого $y \in G$, отображение f_a сюръективно. Итак, f_a — биекция, $f_a \in S(G)$, где $S(G)$ — группа подстановок на множестве G .

|| Рассмотрим теперь отображение (левое регулярное представление группы G)

$$\varphi: G \rightarrow S(G), \quad \varphi(a) = f_a \text{ для } a \in G.$$

Так как для a, b, x имеем

$$f_{ab}(x) = abx = f_a(bx) = f_a(f_b(x)) = (f_a f_b)(x),$$

то

$$\varphi(ab) = f_{ab} = f_a f_b = \varphi(a)\varphi(b).$$

|| Следовательно, $\varphi: G \rightarrow S(G)$ — гомоморфизм групп.

Если $\varphi(a) = \varphi(b)$ для $a, b \in G$, то для всех $x \in G$

$$ax = \varphi(a)(x) = \varphi(b)(x) = bx,$$

и поэтому $a = b$. Таким образом, φ — инъективный гомоморфизм. Поэтому $G \cong \text{Im } \varphi \subseteq S(G)$.

Если $|G| = n$, то $S(G) = S_n$, и поэтому

$$G \cong \text{Im } \varphi \subseteq S_n, \quad |S_n| = n!.$$

Замечания 1.16.5.

- 1) Если G — конечная группа, $|G| = n < \infty$, то левое регулярное представление φ является изоморфизмом тогда и только тогда, когда $n = |G| \leq 2$ (если $n = |G| > 2$, то $n = |G| < n! = |G|! = |S(G)|$).
- 2) Теорема Кэли, несомненно, полезна с точки зрения контроля, что ничего не потеряно при рассмотрении групп данного порядка. С другой стороны, число $|S(G)| = |G|!$ так быстро растёт с ростом $|G|$, что не стоит преувеличивать роль теоремы Кэли в классификационных задачах. С этим же связаны поиски меньших групп подстановок, содержащих экземпляр группы G .

Под представлением группы G подстановками будем понимать любой гомоморфизм

$$\varphi: G \rightarrow S(X), \quad \text{где } X \text{ — некоторое множество.}$$

- || В левом регулярном представлении $\varphi: G \rightarrow S(G)$ имеем $X = G$. Если H — подгруппа группы G (не предполагается, что H — нормальная подгруппа), то продолжим (см. 1.12.11): рассмотрение представления подстановками на левых смежных классах по H :

$$\varphi_H: G \rightarrow S(G/H), \quad \varphi_H(a)(bH) = abH,$$

где

$$X = G/H = \{aH \mid a \in G\} —$$

пространство левых смежных классов группы G по подгруппе H , при этом если $|H| > 1$, то

$$|X| = |G/H| < |G|.$$

Предложение 1.16.6. Если H — подгруппа группы G ,

$$\varphi_H: G \rightarrow S(G/H) -$$

представление группы G подстановками на пространстве левых смежных классов G/H , то $\text{Ker } \varphi_H$ — наибольшая нормальная подгруппа группы G , лежащая в подгруппе H .

Доказательство. Если

$$\varphi_H(a)(bH) = abH = acH = \varphi_H(a)(cH),$$

то $bH = cH$, и следовательно, $\varphi_H(a)$ — инъекция.

Так как

$$\varphi_H(a)(a^{-1}bH) = aa^{-1}bH = bH,$$

то $\varphi_H(a)$ — сюръекция.

Итак, $\varphi_H(a) \in S(G/H)$ для всех $a \in G$.

Так как для всех $bH \in G/H$, $a_1, a_2 \in G$, то

$$\varphi_H(a_1a_2)(bH) = a_1a_2bH = \varphi_H(a_1)(a_2bH) = \varphi_H(a_1)(\varphi_H(a_2)(bH)) = (\varphi_H(a_1)\varphi_H(a_2))(bH),$$

и поэтому $\varphi_H(a_1a_2) = \varphi_H(a_1)\varphi_H(a_2)$. Следовательно,

$$\varphi_H: G \rightarrow S(G/H) -$$

гомоморфизм групп. Таким образом,

$$\text{Ker } \varphi_H \triangleleft G.$$

Если $a \in \text{Ker } \varphi_H$, то $\varphi_H(a) = 1_{G/H}$; и поэтому

$$aH = \varphi_H(a)(H) = 1_{G/H}(H) = H.$$

Следовательно, $a \in H$, и поэтому

$$\text{Ker } \varphi_H \subseteq H.$$

Пусть теперь $N \triangleleft G$ и $N \subseteq H$. Если $a \in N$, $b \in G$, то $b^{-1}ab = a' \in N \subseteq H$,

$$\varphi_H(a)(bH) = abH = ba'H = bH,$$

и поэтому $\varphi_H(a) = 1_{G/H}$, следовательно, $N \subseteq \text{Ker } \varphi_H$.

Итак, $\text{Ker } \varphi_H$ — наибольшая нормальная подгруппа группы G , лежащая в H . \square

Следствие 1.16.7. Пусть H — подгруппа конечной группы G и её порядок $|G|$ не делит $(G : H)!$, тогда существует такая неединичная нормальная подгруппа $e \neq N \triangleleft G$, что $N \subseteq H$.

Доказательство. Пусть $N = \text{Ker } \varphi_H \triangleleft G$, $N \subseteq H$, $G/N \cong \text{Im } \varphi_H \subseteq S(G/H)$. Следовательно, $|G|/|N| = |G/N| = |\text{Im } \varphi_H|$ — делитель числа $|S(G/H)| = (G : H)!$. Так как $|G|$ не делит число $(G : H)!$, то $|N| > 1$, и поэтому $N \neq \{e\}$. \square

Следствие 1.16.8. Пусть H — подгруппа конечной группы G такая, что

$$\text{НОД}(|H|, ((G : H) - 1)!) = 1.$$

Тогда $H \triangleleft G$.

Доказательство. Пусть

$$N = \text{Кер } \varphi_H.$$

Тогда $N \subseteq H$ и $G/N \cong \text{Im } \varphi_H \subseteq S(G/H)$, поэтому число

$$(|G|/|H|) \cdot (|H|/|N|) = (|G|/|N|) = |\text{Im } \varphi_H|$$

делит

$$|(G : H)|! = |G/H|! = (|G|/|H|)! = 1 \cdot 2 \cdots |G|/|H|.$$

Следовательно, $|H|/|N|$ делит $((G : H) - 1)!$. Так как $\text{НОД}(|H|, ((G : H) - 1)!) = 1$, то $|H|/|N| = 1$, т. е. $H = N$. \square

Следствие 1.16.9. Пусть p — наименьший простой делитель порядка $|G|$ конечной группы G . Тогда любая подгруппа H группы G индекса $(G : H) = p$ является нормальной, $H \triangleleft G$.

Доказательство. Пусть $r = |H| = |G|/p$. Тогда каждый простой делитель числа r больше или равен p . Поэтому

$$\text{НОД}(|H|, ((G : H) - 1)!) = (r, (p - 1)!) = 1.$$

В силу следствия 1.16.8 $H \triangleleft G$. \square

Лемма 1.16.10. Если G, G', G'' — группы, $f: G \rightarrow G'$, $g: G' \rightarrow G''$ — изоморфизмы, то gf и f^{-1} — изоморфизмы.

Доказательство.

а) По лемме 1.15.2 gf — гомоморфизм. Так как gf и биекция, то gf — изоморфизм.

б) Мы знаем, что f^{-1} — биекция. Пусть $w, z \in G'$. Тогда $w = f(x)$, $z = f(y)$, где $x, y \in G$. Следовательно, $wz = f(x)f(y) = f(xy)$. Поэтому $f^{-1}(wz) = f^{-1}(f(xy)) = xy = f^{-1}(w)f^{-1}(z)$, т. е. f^{-1} — гомоморфизм. Итак, f^{-1} — изоморфизм. \square

Следствие 1.16.11. Отношение $G \cong G'$ является отношением эквивалентности.

Замечание 1.16.12. Изоморфные группы обладают одинаковыми «алгебраическими» свойствами.

Пример 1.16.13. Если группы G и G' изоморфны и группа G — коммутативная группа, то G' также коммутативная группа. Действительно, пусть $f: G \rightarrow G'$ — некоторый изоморфизм. Если $z, w \in G'$, то $z = f(a)$, $w = f(b)$ для некоторых $a, b \in G$. Тогда

$$zw = f(a)f(b) = f(ab) = f(ba) = f(b)f(a) = wz. \quad \square$$

Лемма 1.16.14. Пусть $f: G \rightarrow G'$ — изоморфизм групп, $g \in G$. Тогда $O(g) = O(f(g))$.

Доказательство. Так как $f(g^m) = f(g)^m$ для всех $m \in \mathbb{Z}$ и f — инъективное отображение, то $f(g)^m = e'$ тогда и только тогда, когда $g^m = e$. Следовательно, $O(g) = O(f(g))$. \square

Следствие 1.16.15. Если $f \in \text{Aut}(G)$ — автоморфизм группы G , $g \in G$, то $O(g) = O(f(g))$.

Упражнение 1.16.16. Покажите, что группа $G = \{1, i, -1, -i\}$ корней четвёртой степени из 1 изоморфна группе вращений квадрата.

Упражнение 1.16.17. Покажите, что: $\text{GL}_2(\mathbb{Z}_2) = \text{SL}_2(\mathbb{Z}_2) \cong S_3 \cong D_3$; $\text{SL}_3(\mathbb{Z}_2) \cong \text{SL}_2(\mathbb{Z}_7)$.

Упражнение 1.16.18. Пусть

$$G = \left\{ e = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} = (A \ B), \right. \\ \left. \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix} = (A \ C), \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} = (A \ C)(B \ D) \right\} -$$

группа симметрий ромба с вершинами A, B, C, D . Так как $|G| = 4$ и $x^2 = e$ для всех $x \in G$, то эта группа G не является циклической и, следовательно, не является изоморфной предыдущей группе вращений квадрата.

Задача 1.16.19. Найти все гомоморфизмы $A_4 \rightarrow \mathbb{Z}_3$.

Задача 1.16.20. Пусть $M = \mathbb{R} \setminus \{0, 1\}$. Показать, что шесть функций из M в M с операцией композиции образуют группу G :

$$f_1(x) = x, \quad f_2(x) = \frac{1}{1-x}, \quad f_3(x) = \frac{x-1}{x}, \\ f_4(x) = \frac{1}{x}, \quad f_5(x) = \frac{x}{x-1}, \quad f_6(x) = 1-x.$$

Покажите, что $G \cong S_3$.

Упражнение 1.16.21 (группы вращений и симметрий правильных многоугольников и многогранников, см. также ??). Рассмотрим правильный многоугольник (многогранник) с центром в начале координат. Группа симметрий этого многоугольника (многогранника) — это подгруппа (ортогональной) группы $O_m(\mathbb{R})$ ($m = 2, 3$), оставляющая этот многоугольник (многогранник) на месте. Группа вращений — это подгруппа группы симметрий, состоящая из матриц с определителем 1 (подгруппа в $\text{SO}_m(\mathbb{R})$).

Покажите, что

1) при $m = 2$:

- a) группа вращений правильного n -угольника является циклической группой порядка n ;
- b) группа симметрий правильного n -угольника (диэдральная группа D_n) состоит из $2n$ элементов. Эта группа изоморфна группе вращений правильного диэдра ($m = 3$). При $n = 3$: $D_3 \cong S_3$. При $n \geq 3$ группа D_n некоммутативна.

Покажите, что число классов сопряжённых элементов в группе D_n при нечётном n равно $\frac{n+3}{2}$, а при чётном n равно $\frac{n}{2} + 3$; группа D_n порождается двумя элементами;

2) при $m = 3$:

- а) группа вращений правильного тетраэдра T изоморфна группе A_4 ;
- б) группа вращений куба O изоморфна группе S_4 ;
- в) группа симметрий тетраэдра изоморфна группе S_4 ;
- г) группа симметрий куба состоит из 48 элементов и имеет 10 классов сопряжённых элементов;
- д) группы вращений правильных додекаэдра и икосаэдра совпадают и изоморфны группе A_5 ;
- е) группа симметрий правильного додекаэдра (икосаэдра) состоит из 120 элементов и изоморфна прямому произведению группы A_5 и циклической группы второго порядка.

Задача 1.16.22. Пусть $G = \langle a \rangle$, $O(a) = n$, — циклическая группа порядка n . Показать, что для всякого $m \in \mathbb{Z}$ отображение

$$f_m: G \rightarrow G, \quad f_m(x) = x^m,$$

является гомоморфизмом, при этом f_m — изоморфизм тогда и только тогда, когда $(m, n) = 1$.

Лемма 1.16.23. Бесконечная группа G является циклической тогда и только тогда, когда группа G изоморфна каждой своей собственной подгруппе.

Доказательство.

- 1) Бесконечная циклическая группа G изоморфна группе $(\mathbb{Z}, +)$ целых чисел. Если $H \subseteq \mathbb{Z}$ — собственная подгруппа, то $H = \mathbb{Z}m$, $m > 0$. Ясно, что $\mathbb{Z} \cong \mathbb{Z}m$.
- 2) Пусть G — бесконечная группа, изоморфная каждой своей собственной подгруппе. Если $e \neq g \in G$, то $G \cong \langle g \rangle$, поэтому G — циклическая группа. \square

Задача 1.16.24. Если в группе G $a^2 = b^3 = e$ и $ab = b^2a$ для всех $a, b \in G$, то $G \cong S_3$.

Задача 1.16.25. Если G — неабелева группа порядка 6, то $G \cong S_3$ (см. также ??).

Задача 1.16.26. Сколько существует неизоморфных групп порядка 4? Показать, что все они абелевы. (Более сильное утверждение: если p — простое число и $|G| = p^2$, то G — абелева группа.)

Приложение:

число неизоморфных групп и абелевых групп заданного порядка

Число $N(n)$ неизоморфных групп G порядка n , $|G| = n$, всегда конечно (например, в силу теоремы Кэли, каждая группа из n элементов изоморфна некоторой подгруппе группы подстановок S_n). В ряде случаев мы вычислили некоторые из значений функции $N(n)$, используя дополнительные результаты из теории групп (алгоритм прямого перебора подмножеств из n элементов в S_n с проверкой на то, является ли это подмножество группой и изоморфны или не изоморфны найденные группы, крайне неэффективны уже при $n > 10$).

Число $N_a(n)$ неизоморфных абелевых групп из n элементов было вычислено нами по разложению числа n на простые множители (см. ??). Ясно, что всегда $N_a(n) \leq N(n)$, $N_a(p) = N(p) = 1$ для простого p .

В данном приложении мы приведём значения функций $N(n)$ и $N_a(n)$ для $n \leq 220$. Уже эти данные показывают сложность общей проблемы классификации конечных групп, а для конечных абелевых групп, где мы нашли хорошие алгоритмы классификации, приведённая таблица значений для $N_a(n)$ при малых n даёт представление о фактическом состоянии дел.

В данной таблице:

$n = |G|$ — число элементов в группе G ;

$N(n)$ — число неизоморфных групп из n элементов;

$N_a(n)$ — число неизоморфных абелевых групп из n элементов.

n	$N(n)$	$N_a(n)$	n	$N(n)$	$N_a(n)$	n	$N(n)$	$N_a(n)$
1	1	1	2	1	1	3	1	1
4	2	2	5	1	1	6	2	1
7	1	1	8	5	3	9	2	2
10	2	1	11	1	1	12	5	2
13	1	1	14	2	1	15	1	1
16	14	5	17	1	1	18	5	2
19	1	1	20	5	2	21	2	1
22	2	1	23	1	1	24	15	3
25	2	2	26	2	1	27	5	3
28	4	2	29	1	1	30	4	1
31	1	1	32	51	7	33	1	1
34	2	1	35	1	1	36	14	4
37	1	1	38	2	1	39	2	1
40	14	3	41	1	1	42	6	1
43	1	1	44	4	2	45	2	2
46	2	1	47	1	1	48	52	5
49	2	2	50	5	2	51	1	1
52	5	2	53	1	1	54	15	3
55	2	1	56	13	3	57	2	1
58	2	1	59	1	1	60	13	2
61	1	1	62	2	2	63	4	2
64	294	11	65	1	1	66	4	1
67	1	1	68	5	2	69	1	1
70	4	1	71	1	1	72	50	6
73	1	1	74	2	1	75	3	2

14-21

n	$N(n)$	$N_a(n)$	n	$N(n)$	$N_a(n)$	n	$N(n)$	$N_a(n)$
76	4	2	77	1	1	78	6	1
79	1	1	80	52	5	81	15	5
82	2	1	83	1	1	84	15	2
85	1	1	86	2	1	87	1	1
88	12	3	89	1	1	90	10	2
91	1	1	92	4	2	93	2	1
94	2	1	95	1	1	96	230	7
97	1	1	98	5	2	99	2	2
100	16	4	101	1	1	102	4	1
103	1	1	104	14	3	105	2	1
106	2	1	107	1	1	108	45	6
109	1	1	110	6	1	111	2	1
112	43	5	113	1	1	114	6	1
115	1	1	116	5	2	117	4	2
118	2	1	119	1	1	120	47	3
121	2	2	122	2	1	123	1	1
124	4	2	125	5	3	126	16	2
127	1	1	128	2328	15	129	2	1
130	4	1	131	1	1	132	10	2
133	1	1	134	2	1	135	5	3
136	15	3	137	1	1	138	4	1
139	1	1	140	11	2	141	1	1
142	2	1	143	1	1	144	197	10
145	1	1	146	2	1	147	6	2
148	5	2	149	1	1	150	13	2
151	1	1	152	12	3	153	2	2
154	4	1	155	2	1	156	18	2
157	1	1	158	2	1	159	1	1
160	238	7	161	1	1	162	55	5
163	1	1	164	5	2	165	2	1
166	2	1	167	1	1	168	57	3
169	2	2	170	4	1	171	5	2
172	4	2	173	1	1	174	4	1
175	2	2	176	42	5	177	1	5
178	2	1	179	1	1	180	37	4
181	1	1	182	4	1	183	2	1
184	12	3	185	1	1	186	6	1
187	1	1	188	4	2	189	13	3

14-22

n	$N(n)$	$N_a(n)$	n	$N(n)$	$N_a(n)$	n	$N(n)$	$N_a(n)$
190	4	1	191	1	1	192	1543	11
193	1	1	194	2	1	195	2	1
196	17	4	197	1	1	198	10	2
199	1	1	200	52	6	201	2	1
202	2	1	203	2	1	204	12	2
205	2	1	206	2	1	207	2	2
208	51	5	209	1	1	210	12	1
211	1	1	212	5	2	213	1	1
214	2	1	215	1	1	216	177	9
217	1	1	218	2	1	219	2	1
220	15	2						

Замечание 1.16.27. В настоящее время посчитаны числа $N(n)$ для всех $n \leq 2000$. Например, $N(256) = 56092$, $N(640) = 21541$, $N(864) = 4725$, $N(896) = 19349$, $N(960) = 11394$, $N(1000) = 199$, $N(2^9) = 10494213$, $N(2^9 \cdot 3) = 408641062$, $N(2^{10}) = 49487365422$.

Пусть

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

разложение числа n в произведение простых чисел (p_1, \dots, p_k — различные простые числа),

$$\mu(n) = \max\{\alpha_i \mid i \leq k\}.$$

Известно, что

$$N(n) \leq n^{\frac{2}{27}} (\mu(n))^2 + O((\mu(n))^{3/2}).$$

Если $\mu(n) = 1$, то $N(n) \leq \varphi(n)$, где $\varphi(n)$ — функция Эйлера.

Если p — простое число, то

$$N(p^n) \geq p^{\frac{2}{27}m^2(m-6)}.$$

Теорема 1.16.28 (о классификации с точностью до изоморфизма циклических групп).

- 1) Все бесконечные циклические группы изоморфны между собой (в частности, изоморфны группе $(\mathbb{Z}, +)$ целых чисел с операцией сложения).
- 2) Все конечные циклические группы одного конечного порядка n изоморфны между собой (в частности, изоморфны группе корней n -й степени из единицы или другой изоморфной реализации группы \mathbb{Z}_n вычетов по модулю n).

Доказательство.

1) Пусть $G = \langle a \rangle$, $O(a) = \infty$, $G' = \langle b \rangle$, $O(b) = \infty$. Рассмотрим биекцию $f: (a) \rightarrow (b)$, $f(a^k) = b^k$ для любого $k \in \mathbb{Z}$. Так как

$$f(a^k a^l) = f(a^{k+l}) = b^{k+l} = b^k b^l = f(a^k) f(a^l),$$

то f — биективный гомоморфизм и, следовательно, изоморфизм.

Так как $(\mathbb{Z}, +) = (1)$, то любая группа $G = \langle a \rangle$, $O(a) = \infty$, изоморфна группе $(\mathbb{Z}, +)$.

2) Пусть $G = \langle a \rangle$, $O(a) = n$, $G' = \langle b \rangle$, $O(b) = n$. Тогда $G = \langle a \rangle = \{e, a, \dots, a^{n-1}\}$, $G' = \{e', b, \dots, b^{n-1}\}$. Отображение $f: G \rightarrow G'$, для которого $f(a^k) = b^k$, $0 \leq k \leq n-1$, очевидно, является биекцией. Если $0 \leq k, l \leq n-1$ и $k+l = nq+r$, $0 \leq r \leq n-1$, то

$$f(a^k a^l) = f(a^{k+l}) = f((a^n)^q a^r) = f(a^r) = b^r = (b^n)^q b^r = b^{nq+r} = b^{k+l} = b^k b^l = f(a^k) f(a^l).$$

Таким образом, f — гомоморфизм групп и, следовательно, для нашей биекции, изоморфизм. Так как

$$(\sqrt[n]{1}, \cdot) = \left\{ \varepsilon_k = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \mid 0 \leq k \leq n-1 \right\} = (\varepsilon = \varepsilon_1)$$

и

$$(\mathbb{Z}_n, +) = \{C_k = k + n\mathbb{Z} \mid 0 \leq k \leq n-1\},$$

то

$$G = \langle a \rangle \cong (\sqrt[n]{1}, \cdot) \cong (\mathbb{Z}_n, +). \quad \square$$

1.17. Теоремы о гомоморфизмах

Теорема 1.17.1 (о гомоморфизме для групп). Пусть $f: G \rightarrow G'$ — сюръективный гомоморфизм (т. е. гомоморфизм из группы G на группу G'). Тогда существует изоморфизм $\psi: G/\text{Ker } f \rightarrow G'$ такой, что $f = \psi\pi$, где $\pi: G \rightarrow G/\text{Ker } f$ — канонический гомоморфизм из группы G на фактор-группу $G/\text{Ker } f$ по нормальной подгруппе $\text{Ker } f$ (ядро гомоморфизма f), т. е. следующая диаграмма коммутативна:

$$\begin{array}{ccc} x \in G & \xrightarrow{f} & G' \\ \pi \searrow & & \downarrow \psi \\ & G/\text{Ker } f & \end{array}$$

Доказательство. Для смежного класса $x \text{Ker } f$, $x \in G$, положим $\psi(x \text{Ker } f) = f(x)$.

Корректность отображения $\psi: G/\text{Ker } f \rightarrow G'$. Если для $y \in G$ имеем $x \text{Ker } f = y \text{Ker } f$, то $x^{-1}y \in \text{Ker } f$, поэтому $e' = f(x^{-1}y) = f(x)^{-1}f(y)$, следовательно, $f(x) = f(y)$.

Покажем, что ψ — биекция.

а) Если для $x, y \in G$ имеем $f(x) = \psi(x \text{Ker } f) = \psi(y \text{Ker } f) = f(y)$, то $f(x^{-1}y) = f(x)^{-1}f(y) = e'$, т. е. $x^{-1}y \in \text{Ker } f$. Поэтому $x \text{Ker } f = y \text{Ker } f$, т. е. ψ — инъекция.

б) Если $g' \in G'$, то $g' = f(x)$ для некоторого $x \in G$ (поскольку f — сюръекция). Тогда $g' = f(x) = \psi(x \text{Ker } f)$, т. е. ψ — сюръекция.

Проверим, что ψ — гомоморфизм групп. Действительно, для $x, y \in G$ имеем

$$\psi(x \text{Ker } f \cdot y \text{Ker } f) = \psi(xy \text{Ker } f) = f(xy) = f(x)f(y) = \psi(x \text{Ker } f)\psi(y \text{Ker } f).$$

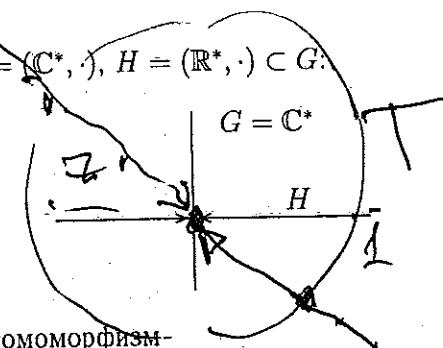
Итак, мы показали, что $\psi: G/\text{Ker } f \rightarrow G'$ — изоморфизм.

Проверим, что $f = \psi\pi$. Действительно, для $x \in G$ имеем

$$(\psi\pi)(x) = \psi(\pi(x)) = \psi(x \text{Ker } f) = f(x). \quad \square$$

Теорема о гомоморфизме является эффективным средством для вычисления фактор-групп.

Пример 1.17.2. Пусть $G = (\mathbb{C}^*, \cdot)$, $H = (\mathbb{R}^*, \cdot) \subset G$.



$$G/H = \mathbb{C}^*/H \cong T$$

Рассмотрим сюръективный гомоморфизм

$$f: G = \mathbb{C}^* \rightarrow T = \{z \in \mathbb{C} \mid |z| = 1\},$$

для которого $f(z) = \frac{z^2}{|z|^2}$ для $z \in \mathbb{C}^*$. Тогда $\text{Ker } f = H = \{\mathbb{R}^*, \cdot\}$. В силу теоремы о гомоморфизме

$$T \cong G/\text{Ker } f = \mathbb{C}^*/\mathbb{R}^*. \quad \square$$

Пример 1.17.3. Пусть K — поле, $G = \text{GL}_n(K)$, $H = \text{SL}_n(K) \triangleleft \text{GL}_n(K)$. Рассмотрим сюръективный гомоморфизм

$$f: \text{GL}_n(K) \rightarrow K^* = (K \setminus \{0\}, \cdot),$$

для которого $f(A) = |A|$ для $A \in \text{GL}_n(K)$. Так как $\text{Ker } f = \text{SL}_n(K)$, то в силу теоремы о гомоморфизме имеем

$$K^* \cong G/\text{Ker } f = \text{GL}_n(K)/\text{SL}_n(K). \quad \square$$

Замечание 1.17.4. Если G — коммутативная группа, то:

- 1) любая её подгруппа H нормальная;
- 2) любая её фактор-группа G/H коммутативна.

Пример 1.17.5 (другое доказательство теоремы о классификации циклических групп). Пусть $G = \langle a \rangle$ — циклическая группа. Рассмотрим сюръективный гомоморфизм

$$\mathbb{Z} \xrightarrow{f} G = \langle a \rangle, \quad f(n) = a^n \text{ для } n \in \mathbb{Z}.$$

Тогда

$$\text{Ker } f = \begin{cases} 0, & \text{если } O(a) = \infty, \\ \mathbb{Z}n, & \text{если } n = O(a) < \infty. \end{cases}$$

Поэтому $G \cong \mathbb{Z}/\text{Ker } f$, при этом $\mathbb{Z}/\text{Ker } f = \mathbb{Z}$, если $O(a) = \infty$; $\mathbb{Z}/\text{Ker } f = \mathbb{Z}_n$, если $n = O(a) < \infty$. \square

Пример 1.17.6. Пусть G и G' — конечные группы взаимно простых порядков, $|G| = m$, $|G'| = n$, $(m, n) = 1$, $f: G \rightarrow G'$ — гомоморфизм групп. Тогда f — тривиальный гомоморфизм, т. е. $f(x) = e'$ для всех $x \in G$.

14-25

Доказательство. Так как образ гомоморфизма $f: \text{Im } f \rightarrow G'$ — подгруппа группы G' , то $|\text{Im } f|$ — делитель числа $n = |G'|$. В то же время $\text{Im } f \cong G/\text{Ker } f$, поэтому $|\text{Im } f|$ — делитель числа $m = |G|$. Так как $(m, n) = 1$, то $\text{Im } f = \{e'\}$. \square

Задача 1.17.7. Восемь матриц

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in M_2(\mathbb{C})$$

образуют подгруппу группы $GL_2(\mathbb{C})$. Эта группа называется *группой кватернионов* и обозначается Q_8 . Показать, что любая подгруппа группы Q_8 нормальна. Центр $Z(Q_8)$ изоморчен группе

$$\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Задача 1.17.8. Нормальные подгруппы группы S_4 исчерпываются подгруппами

$$\{e\}, V_4 = \{e, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\}, A_4, S_4,$$

при этом $\{e, (1 2)\} \triangleleft V_4 \triangleleft A_4$, но $\{e, (1 2)\}$ не является нормальной подгруппой в A_4 (т. е. свойство быть нормальной подгруппой не является транзитивным). Покажите, что $S_4/V_4 \cong S_3$.

Задача 1.17.9. $A_4/V_4 \cong \mathbb{Z}_3$.

Задача 1.17.10. $GL_2(\mathbb{Z}_3)/Z(GL_2(\mathbb{Z}_3)) \cong S_4$.

Задача 1.17.11. $SO_3 = SO_3(\mathbb{R}) \cong SU_2(\mathbb{C})/\{\pm E\}$.

Упражнение 1.17.12. Определим проективную специальную группу над коммутативным кольцом K как

$$PSL_n(K) = SL_n(K)/Z(SL_n(K)).$$

Докажите, что:

$$PSL_2(\mathbb{Z}_2) \cong S_3;$$

$$PSL_2(\mathbb{Z}_3) \cong A_4;$$

$$PSL_2(\mathbb{Z}_5) \cong A_5.$$

Задача 1.17.13. Найти

$$Z(S_n) = \begin{cases} S_n, & n = 2, \\ \{e\}, & n > 2, \end{cases} \quad Z(A_n) = \begin{cases} A_n, & n \leq 3, \\ \{e\}, & n > 3. \end{cases}$$

Если K — поле, то

$$Z(GL_n(K)) = \{\lambda E \mid 0 \neq \lambda \in K\}, \quad Z(SL_n(K)) = \{\lambda E \mid \lambda^n = 1\}.$$

В частности, $Z(SL_n(\mathbb{C}))$ — циклическая группа, порождённая матрицей $\varepsilon \cdot E$, где $\varepsilon = e^{\frac{2\pi i}{n}}$.

Задача 1.17.14. Если G — некоммутативная группа, то группа $G/Z(G)$ не является циклической.

Задача 1.17.15. $(\mathrm{GL}_n(K))' = \mathrm{SL}_n(K)$ при $|K| > 3$.

Задача 1.17.16. $G/[G, G]$ — абелева группа.

Задача 1.17.17. Пусть G — циклическая группа, A, B — её подгруппы. Если $G/A \cong G/B$, то $A = B$.

Задача 1.17.18. Пусть $G = \mathbb{C}^* = \mathbb{C} \setminus \{0\}$, $A = \{r \in \mathbb{C} \mid r \in \mathbb{R}, r > 0\}$, $B = \{r \in \mathbb{C} \mid r \in \mathbb{R} \setminus \{0\}\}$. Тогда $A < B \subset G$; $G/A \cong T \cong G/B$.

Упражнение 1.17.19.

1) Пусть в группе G $(ab)^2 = a^2b^2$ для всех $a, b \in G$. Тогда G — абелева группа.

Доказательство. Так как $abab = a^2b^2$, то $ba = ab$. \square

2) Пусть в группе G $(ab)^2 = (ba)^2$ для всех $a, b \in G$ и, кроме того,

$$x^2 = e, \quad x \in G \implies x = e.$$

Тогда G — абелева группа.

Доказательство. Для $a, b \in G$ имеем:

$$a^2 = ((ab^{-1})b)^2 = (bab^{-1})^2 = ba^2b^{-1},$$

поэтому $a^2b = ba^2$ для всех $a, b \in G$. Если $c = aba^{-1}b^{-1}$, то

$$\begin{aligned} c^2 &= (aba^{-1}b^{-1})(aba^{-1}b^{-1}) = ab(a^{-1}b^{-1}a)(ba^{-1}b^{-1}) = \\ &= ab(aa^{-2}b^{-1}a)(ba^{-1}b^{-1}) = ab(ab^{-1}a^{-2}a)(ba^{-1}b^{-1}) = \\ &= ab(ab^{-1}a^{-1})(ba^{-1}b^{-1}) = ab(abb^{-2}a^{-1})(ba^{-1}b^{-1}) = \\ &= ab(aba^{-1}b^{-2})(ba^{-1}b^{-1}) = ab(aba^{-1})(b^{-1}a^{-1}b^{-1}) = \\ &= (ab)^2(a^{-1}b^{-1})^2 = (ba)^2(a^{-1}b^{-1})^2 = e. \end{aligned} \quad \square$$

3) Пусть G — группа и $(ab)^i = a^ib^i$ для $i = n, n+1, n+2$. Тогда $ab = ba$.

Доказательство.

$$(a^n b^n)(ab) = ((ab)^n)(ab) = (ab)^{n+1} = a^{n+1}b^{n+1},$$

поэтому, сокращая слева на a^n и справа на b , получаем

$$b^n a = ab^n.$$

Аналогично получаем

$$b^{n+1} a = ab^{n+1}.$$

Следовательно,

$$b^{n+1} a = b(b^n a) = b(ab^n),$$

поэтому

$$ab^{n+1} = b^{n+1} a = bab^n.$$

Итак, $ab = ba$. \square

4) Пусть G — группа, $n \in \mathbb{N}$, $(ab)^n = a^n b^n$ для всех $a, b \in G$,

$$G_n = \{a \in G \mid a^n = e\}, \quad G^n = \{a^n \mid a \in G\}.$$

Тогда:

- 1) $G_n \triangleleft G$;
- 2) $G^n \triangleleft G$;
- 3) $G/G_n \cong G^n$.

Доказательство.

1) Если $a, b \in G_n$ и $x \in G$, то:

- a) $(ab)^n = a^n b^n = e \cdot e = e$, и поэтому $ab \in G_n$;
- б) $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$, и поэтому $a^{-1} \in G_n$;
- в) $(xax^{-1})^n = x a^n x^{-1} = x e x^{-1} = e$.

Итак, $G_n \triangleleft G$.

2) Если $a, b \in G$, $a^n, b^n \in G^n$ и $x \in G$, то:

- a) $a^n b^n = (ab)^n \in G^n$;
- б) $(a^n)^{-1} = (a^{-1})^n \in G^n$;
- в) $x a^n x^{-1} = (xax^{-1})^n \in G^n$.

Итак, $G^n \triangleleft G$.

3) Если $f: G \rightarrow G^n$, $f(a) = a^n$ для $a \in G$, то

$$f(ab) = (ab)^n = a^n b^n = f(a)f(b)$$

Итак, f — сюръективный гомоморфизм,

$$\text{Ker } f = \{a \in G \mid a^n = e\} = G_n,$$

и поэтому по теореме о гомоморфизме

$$G/\text{Ker } f = G/G_n \cong \text{Im } f = G^n. \quad \square$$

Теорема 1.17.20 (вторая теорема о гомоморфизме). Пусть H — подгруппа группы G , K — нормальная подгруппа группы G (в силу леммы HK — подгруппа группы G). Тогда:

- 1) $H \cap K \triangleleft H$ и $K \triangleleft HK$;
- 2) $HK/K \cong H/H \cap K$.

Доказательство. Нас интересуют четыре подгруппы:

$$\begin{array}{ccccc} & & HK & & \\ & \triangleleft & & \supseteq & \\ K & \triangleleft & H & \supseteq & H \cap K \\ \supseteq & & \triangleleft & & \end{array}$$

1) Так как $K \triangleleft G$, то $H \cap K \triangleleft H$. Если $h \in H$, $k \in K$, то

$$(hk)^{-1}Khk = k^{-1}(h^{-1}Kh)k = k^{-1}Kk \subseteq K,$$

т. е. $K \triangleleft HK$.

2) Рассмотрим канонический эпиморфизм

$$\pi_K: G \rightarrow G/K$$

и его ограничение на H

$$\pi_K|_H: H \rightarrow \pi_K(H) \subseteq G/K.$$

Ясно, что $\text{Ker } \pi_K|_H = H \cap \text{Ker } \pi_K = H \cap K$.

Далее, для $h \in H$ и $k \in K$ имеем

$$\pi_K(h) = hK \subseteq HK/K, \quad (hk)K = hK = \pi_K(h)$$

т. е. $HK/K \subseteq \pi_K(H)$. Таким образом,

$$\text{Im}(\pi_K|_H) = \pi_K(H) = HK/K.$$

В силу первой теоремы о гомоморфизмах (её следствия)

$$HK/K = \text{Im}(\pi_K|_H) \cong H/\text{Ker}(\pi_K|_H) = H/H \cap K. \quad \square$$

Упражнение 1.17.21.

1) Пусть H — подгруппа группы S_n , $H \not\subseteq A_n$ (т. е. подгруппа H содержит нечётную подстановку). Тогда

$$H/(H \cap A_n) \cong \mathbb{Z}_2$$

(другими словами, $H \cap A_n$ — подгруппа группы H индекса 2).

Доказательство. Если $h \in H$, $h \notin A_n$, то $hA_n = S_n \setminus A_n$. Следовательно, $HA_n = S_n$. Применяя вторую теорему о гомоморфизмах для $K = A_n$, получаем

$$H/(H \cap A_n) \cong (HA_n)/A_n = S_n/A_n \cong \mathbb{Z}_2. \quad \square$$

2) Пусть $m, n \in \mathbb{Z}$, $d = \text{НОД}(m, n)$, $l = \text{НОК}(m, n)$. Тогда

$$d\mathbb{Z}/n\mathbb{Z} = (m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} \cong m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}) = m\mathbb{Z}/l\mathbb{Z}$$

($dl = mn$). \square

3) Пусть G — конечная группа, $H \triangleleft G$, $(|H|, |G/H|) = 1$. Тогда H — единственная подгруппа группы G порядка $|H|$.

Доказательство. Если $K \subseteq G$, $|K| = |H|$, то $K/K \cap H \cong KH/H \subseteq G/H$ и $|KH/H| = \frac{|KH|}{|H|} = \frac{|K|}{|K \cap H|}$, при этом $|K|/|K \cap H|$ — делитель числа $|G/H|$. Так как $(|H|, |G/H|) = 1$ и $|K| = |H|$, то $|K|/|K \cap H| = 1$, и поэтому $K = K \cap H$, следовательно, $K = H$. \square

14-26

- 4) Пусть $m, n \in \mathbb{N}$. Тогда в силу второй теоремы об изоморфизме

$$(m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} \cong m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}).$$

Проанализируем, что это означает в теоретико-числовых терминах.

Пусть $l = \text{НОК}(m, n)$, тогда $l\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$. Если $d = \text{НОД}(m, n)$, то $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$, и поэтому

$$\mathbb{Z}/(n/d)\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/l\mathbb{Z} \cong \mathbb{Z}/(l/m)\mathbb{Z},$$

$$n/d = l/m, mn = dl, \text{ т. е. } \text{НОД}(m, n) \cdot \text{НОК}(m, n) = mn.$$

- 5) Пусть K, L — нормальные подгруппы группы G , $G = KL$, $K \cap L = N$. Покажите, что $G/N \cong K/N \times L/N$.

Лемма Цассенхауза

Следующая лемма Цассенхауза вытекает из второй теоремы об изоморфизме (иногда её называют «леммой о бабочке» по виду рассматриваемой диаграммы подгрупп). В дальнейшем лемма Цассенхауза найдёт своё применение в доказательствах теоремы Шрайера об уплотнении субнормальных рядов подгрупп группы и теоремы Жордана—Гельдера о композиционных рядах группы.

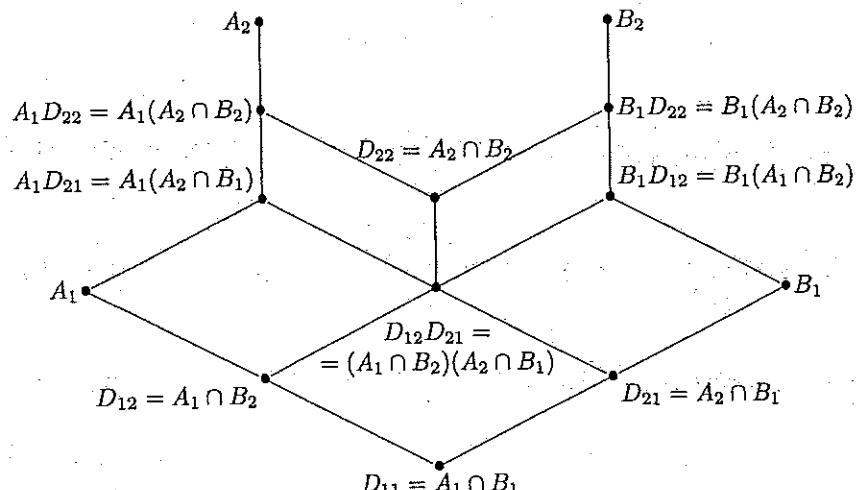
Лемма 1.17.22 (лемма Цассенхауза). Пусть A_1, A_2, B_1, B_2 — подгруппы группы G такие, что: $A_1 \triangleleft A_2$; $B_1 \triangleleft B_2$. Тогда:

- 1) $A_1(A_2 \cap B_1) \triangleleft A_1(A_2 \cap B_2)$;
- 2) $B_1(A_1 \cap B_2) \triangleleft B_1(A_2 \cap B_2)$;
- 3) $A_1(A_2 \cap B_2)/A_1(A_2 \cap B_1) \cong B_1(A_2 \cap B_2)/B_1(A_1 \cap B_2)$.

Доказательство. Пусть

$$D_{ij} = A_i \cap B_j, \quad i, j = 1, 2.$$

Рассмотрим диаграмму подгрупп:



1) Так как $B_1 \triangleleft B_2$, то

$$D_{21} = A_2 \cap B_1 \triangleleft A_2 \cap B_2 = D_{22}.$$

Применяя лемму ?? в группе A_2 , с учётом $A_1 \triangleleft A_2$ получаем, что

$$A_1 D_{21} = A_1 (A_2 \cap B_1) \triangleleft A_1 (A_2 \cap B_2) = A_1 D_{22}.$$

2) Аналогично

$$B_1 D_{12} = B_1 (A_1 \cap B_2) \triangleleft B_1 (A_2 \cap B_2) = B_1 D_{22}.$$

3) Применим вторую теорему об изоморфизме

$$HN/N = H/H \cap N$$

в ситуации $H = D_{22}$, $N = A_1 D_{21}$, $HN = D_{22} A_1 D_{21}$, $H \cap N = D_{22} \cap A_1 D_{21} = D_{12} D_{21}$ (учитывая модулярное свойство Дедекинда, см. ??), получаем, что

$$A_1 D_{22}/A_1 D_{21} \cong D_{22}/D_{12} D_{21}.$$

Аналогично

$$B_1 D_{22}/B_1 D_{12} \cong D_{22}/D_{12} D_{21}.$$

Итак,

$$A_1 D_{22}/A_1 D_{21} = A_1 (A_2 \cap B_2)/A_1 (A_2 \cap B_1) \cong B_1 D_{22}/B_1 D_{12} = B_1 (A_2 \cap B_2)/B_1 (A_1 \cap B_2). \quad \square$$

Теорема 1.17.23 (третья теорема о гомоморфизмах). Пусть $G \xrightarrow{f} G'$ — сюръективный гомоморфизм, $K = \text{Ker } f \triangleleft G$ (например, если $K \triangleleft G$, то $f = \pi_K: G \xrightarrow{\sim} G/K$), $H' \subseteq G'$ — подгруппа, $f^{-1}(H') = \{g \in G \mid f(g) \in H'\}$ — её полный прообраз при отображении f (ясно, что $H \supseteq K$, поскольку $f(K) = e'$). Тогда:

1) естественные соответствия

$$\begin{aligned} H &\mapsto f(H) = H', \\ H &= f^{-1}(H') \leftrightarrow H' \end{aligned}$$

устанавливают естественную биекцию между множеством подгрупп H группы G , содержащих нормальную подгруппу K , и множеством всех подгрупп H' группы G' ;

2) при этом соответствия $H \triangleleft G$ тогда и только тогда, когда $H' \triangleleft G'$, и $G'/H' \cong G/H$ (в частности, $(G/K)/(H/K) \cong G/H$ для $G \triangleright H \triangleright K$).

Доказательство.

1) Ясно, что в нашем случае $f(f^{-1}(H')) = H'$. Пусть теперь H — подгруппа группы G и $H \supseteq K$. Тогда $f^{-1}(f(H)) \supseteq H$. Если $g \in G$ и $f(g) \in f(H)$, т. е. $f(g) = f(h)$ для $h \in H$, то $f(h^{-1}g) = f(h)^{-1}f(g) = e'$, следовательно, $h^{-1}g \in \text{Ker } f = K \subseteq H$, т. е. $g \in hH = H$. Итак, $f^{-1}(f(H)) = H$.

2) Если $H \triangleleft G$, $H \supseteq K$, и $g' = f(g) \in G'$, и $a = g(h) \in f(H)$, $h \in H$, то $(g')^{-1}ag' = f(g)^{-1}f(h)f(g) = f(g^{-1}hg) \in f(H)$, т. е. $f(H) \triangleleft G'$.

Если $H' \triangleleft G'$, $g \in G$, $x \in H = f^{-1}(H')$, т. е. $f(x) \in H'$, то $f(g^{-1}xg) = f(g)^{-1}f(x)f(g) \in H'$, поэтому $g^{-1}xg \in f^{-1}(H')$, т. е. $f^{-1}(H') \triangleleft G$.

14-31

Рассмотрим теперь сюръективный гомоморфизм

$$\psi = \pi_{H'} \cdot f: G \xrightarrow{f} G' \xrightarrow{\pi_{H'}} G'/H'.$$

Если $g \in G$, то $\psi(g) = f(g)H' = H'$ тогда и только тогда, когда $f(g) \in H'$, т. е.

$$\text{Ker } \psi = f^{-1}(H') = H.$$

В силу первой теоремы о гомоморфизмах для ψ

$$G/H = G/\text{Ker } \psi \cong G'/H'.$$

В ситуации $G \triangleright H \triangleright K$ и $f = \pi_K: G \rightarrow G' = G/K$ $H' = f(H) = H/K \triangleleft G'/K$, имеем по доказанному $G/H \cong G'/H' = (G/K)/(H/K)$. \square

1.18. Диаграммный поиск

Диаграмма гомоморфизмов групп

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ \gamma \downarrow & & \downarrow \delta \\ C & \xrightarrow{\beta} & D \end{array}$$

называется *коммутативной*, если $\delta\alpha = \gamma\beta$ в $\text{Hom}(A, D)$. Аналогично определяется коммутативность других диаграмм.

Доказательство следующей полезной леммы хорошо иллюстрирует так называемый *диаграммный поиск*.

Лемма 1.18.1 (о пяти гомоморфизмах). Пусть строки следующей коммутативной диаграммы гомоморфизмов групп

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{f_1} & A_2 & \xrightarrow{f_2} & A_3 & \xrightarrow{f_3} & A_4 & \xrightarrow{f_4} & A_5 \\ h_1 \downarrow & & h_2 \downarrow & & h_3 \downarrow & & h_4 \downarrow & & h_5 \downarrow \\ B_1 & \xrightarrow{g_1} & B_2 & \xrightarrow{g_2} & B_3 & \xrightarrow{g_3} & B_4 & \xrightarrow{g_4} & B_5 \end{array}$$

являются точными последовательностями. Тогда:

- 1) если $\text{Im } h_1 = B_1$, $\text{Ker } h_2 = \{e_{A_2}\}$, $\text{Ker } h_4 = \{e_{A_4}\}$, то $\text{Ker } h_3 = \{e_{A_3}\}$;
 - 2) если $\text{Im } h_2 = B_2$, $\text{Im } h_4 = B_4$, $\text{Ker } h_5 = \{e_{A_5}\}$, то $\text{Im } h_3 = B_3$.
- В частности,
- 3) если h_1, h_2, h_4, h_5 — изоморфизмы, то h_3 — изоморфизм.

Доказательство.

1) Пусть $a \in \text{Ker } h_3$. Тогда

$$h_4(f_3(a)) = g_3(h_3(a)) = e_{B_4}.$$

Так как $\text{Ker } f_4 = \{e_{A_4}\}$, то $f_3(a) = e_{A_4}$. В силу точности первой строки в A_3 найдётся элемент $a' \in A_2$, для которого $a = f_2(a')$. Так как

$$g_2(h_2(a')) = h_3(f_2(a')) = h_3(a) = e_{B_3},$$

то в силу точности второй строки в B_2 найдётся элемент $b \in B_1$, для которого $h_2(a') = g_1(b)$. Так как $\text{Im } h_1 = B_1$, то $b = h_1(a'')$ для $a'' \in A_1$. Поэтому

$$h_2(f_1(a'')) = g_1(h_1(a'')) = g_1(b) = h_2(a').$$

Но $\text{Ker } h_2 = e_{A_2}$, и следовательно, $a' = f_1(a'')$. В силу точности первой строки в A_2

$$a = f_2(a') = f_2(f_1(a'')) = e_{A_3}.$$

Итак, $\text{Ker } h_3 = \{e_{A_3}\}$.

2) Пусть $x \in B_3$. В силу $\text{Im } h_4 = B_4$ $g_3(x) = h_4(y)$ для $y \in A_4$. Учитывая точность второй строки в B_4 , имеем

$$h_5(f_4(y)) = g_4(h_4(y)) = g_4(g_3(x)) = e_{B_5}.$$

Так как $\text{Ker } h_5 = \{e_{A_5}\}$, то $f_4(y) = e_{A_5}$, т. е. $y \in \text{Ker } f_4 = \text{Im } f_3$, поэтому $y = f_3(z)$ для $z \in A_3$. Тогда

$$g_3(h_3(z)) = h_4(f_3(z)) = h_4(y) = g_3(x).$$

Следовательно, $x^{-1}h_3(z) \in \text{Ker } g_3 = \text{Im } g_2$, поэтому $x^{-1}h_3(z) = g_2(w)$ для $w \in B_2$. Так как $\text{Im } h_2 = B_2$, то $w = h_2(u)$ для $u \in A_2$. Тогда

$$h_3(f_2(u)) = g_2(h_2(u)) = g_2(w) = x^{-1}h_3(z),$$

следовательно,

$$x = (h_3(f_2(u)))^{-1}h_3(z) = h_3(f_2(u^{-1}))h_3(z) = h_3(f_2(u^{-1})z)$$

для $f_2(u^{-1})z \in A_3$. Итак, $\text{Im } h_3 = B_3$. □

1.19. Субнормальные подгруппы

Как мы отметили (см. 1.10.18), нормальная подгруппа в нормальной подгруппе группы G может не быть нормальной подгруппой группы G . Поэтому целесообразно рассмотреть более широкий класс субнормальных подгрупп, чем нормальные подгруппы. А именно, подгруппа A группы G называется *субнормальной в G* , если существуют подгруппы A_1, \dots, A_t группы G , образующие *субнормальный ряд*

$$A = A_1 \trianglelefteq A_2 \trianglelefteq \dots \trianglelefteq A_{t-1} \trianglelefteq A_t = G$$

(обозначение: $A \trianglelefteq\trianglelefteq B$).

14-33

Замечание 1.19.1. Отношение «быть субнормальной подгруппой» уже транзитивно:

$$A \trianglelefteq\trianglelefteq B \trianglelefteq\trianglelefteq G \implies A \trianglelefteq\trianglelefteq G$$

(это вытекает непосредственно из определения).

Теорема 1.19.2 (свойства субнормальных подгрупп). Пусть A и B — субнормальные подгруппы группы G . Тогда:

- 1) $U \cap A \trianglelefteq\trianglelefteq U$ в любой подгруппе U группы G (т. е. пересечение субнормальной подгруппы с подгруппой даёт субнормальную подгруппу этой подгруппы);
- 2) $A \cap B \trianglelefteq\trianglelefteq G$ (пересечение субнормальных подгрупп субнормально в G);
- 3) если $f: G \rightarrow G'$ — гомоморфизм групп, то

$f(A)$ — субнормальная подгруппа в $\text{Im } f$;

полный прообраз $f^{-1}(C)$ — субнормальная подгруппа в G для любой субнормальной подгруппы в $\text{Im } f$.

Доказательство.

1) Если

$$A = A_1 \trianglelefteq A_2 \trianglelefteq \dots \trianglelefteq A_t = G$$

субнормальный ряд для A , то

$$U \cap A = U \cap A_1 \trianglelefteq A_2 \trianglelefteq \dots \trianglelefteq U \cap A_{t-1} \trianglelefteq U \cap A_t = G$$

субнормальный ряд для $U \cap A$ в U .

2) В силу 1)

$$A \cap B \trianglelefteq\trianglelefteq B \trianglelefteq\trianglelefteq G$$

и поэтому $A \cap B$ — субнормальная подгруппа в G .

3) Утверждение следует из определения субнормальности подгруппы и свойств нормальных подгрупп при гомоморфизмах. \square

1.20. Группы характеров абелевых групп

Пусть $T = (\mathbb{R}/\mathbb{Z}, +) \cong \{z \in \mathbb{C} \mid |z| = 1\}$. Если A — абелева группа, то определим её группу характеров

$$\text{Ch}(A) = \text{Hom}_{\mathbb{Z}}(A, T).$$

Если

$$\alpha: A \rightarrow B$$

гомоморфизм абелевых групп, то

$$\text{Ch}(\alpha): \text{Ch}(B) \rightarrow \text{Ch}(A),$$

где

$$\text{Ch}(\alpha)(g) = g\alpha: A \rightarrow T$$

для любого

$$g: B \rightarrow T,$$

является гомоморфизмом групп характеров,

$$\gamma = \gamma_A: A \rightarrow \text{Ch}(\text{Ch}(A)),$$

где $\gamma(a)(f) = f(a)$ для $a \in A$ и $f \in \text{Ch}(A)$, $f: A \rightarrow T$, является каноническим гомоморфизмом.

Замечание 1.20.1.

- 1) Покажите, что группа $T = \mathbb{R}/\mathbb{Z}$ содержит единственную подгруппу порядка n для любого $n \geq 1$.
- 2) Покажите, что:
 - a) $\text{Ch}(\mathbb{Z}_n) = \mathbb{Z}_n$;
 - б) $\text{Ch}(A) \cong A$ для любой конечной абелевой группы;
 - в) если A — конечная абелева группа, то канонический гомоморфизм

$$\gamma_A: A \rightarrow \text{Ch}(\text{Ch}(A))$$

является изоморфизмом.

- 3) a) Соответствие

$$A \mapsto \text{Ch}(A), \quad \alpha: A \rightarrow B \mapsto \text{Ch}(\alpha),$$

определяет контравариантный функтор из категории абелевых групп в себя;

- б) $\text{Ch}(\text{Ch}(\alpha)) \cdot \gamma_A = \gamma_B \cdot \alpha$ для любого гомоморфизма $\alpha: A \rightarrow B$;
- в) $\text{Ch}(\gamma_A) \cdot \gamma_{\text{Ch}(A)} = 1$.

- 4) a) Если

$$0 \rightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \rightarrow 0$$

короткая точная последовательность абелевых групп ($\text{Ker } \alpha = 0$, $\text{Im } \alpha = \text{Ker } \beta$, $\text{Im } \beta = C$), то последовательность

$$0 \rightarrow \text{Ch}(C) \xrightarrow{\text{Ch}(\beta)} \text{Ch}(B) \xrightarrow{\text{Ch}(\alpha)} \text{Ch}(A)$$

точна ($\text{Ker Ch}(\beta) = 0$, $\text{Im Ch}(\beta) = \text{Ker Ch}(\alpha)$);

- б) если группа B конечна, то точна и последовательность

$$\text{Ch}(B) \xrightarrow{\text{Ch}(\alpha)} \text{Ch}(A) \rightarrow 0$$

($\text{Im Ch}(\alpha) = \text{Ch}(A)$).

- 5) Если S — подгруппа абелевой группы A , $j: S \rightarrow A$ — вложение, то $\text{Ch}(j): \text{Ch}(A) \rightarrow \text{Ch}(S)$, при этом подгруппа группы характеров $\text{Ch}(A)$

$$\text{Ann}(S) = \text{Ker}(\text{Ch}(j))$$

называется *аннулятором* подгруппы S в группе $\text{Ch}(A)$.

a) Если A — конечная абелева группа, то соответствие

$$S \mapsto \text{Ann}(S)$$

задаёт антиавтоморфизм (дуальный изоморфизм) решётки всех подгрупп группы A на решётку всех подгрупп группы $\text{Ch}(A)$;

б) если A — конечная абелева группа, то

$$\text{Ann}(S) \cong \text{Ch}(A/S), \quad \text{Ch}(S) \cong \text{Ch}(A)/\text{Ann}(S).$$

1.21. Прямые произведения двух групп

Учёж Сначала рассмотрим *внутреннее прямое произведение нормальных подгрупп*: будем говорить, что группа G является *внутренним произведением своих нормальных подгрупп* H и K , $H \triangleleft G$, $K \triangleleft G$, если $G = HK$ и $H \cap K = \{e\}$ (обозначение: $G = H \times K$).

Выведем основные свойства конструкции $G = H \times K$.

Лемма 1.21.1. Если H и K — нормальные подгруппы группы G , $H \triangleleft G$, $K \triangleleft G$, и $H \cap K = \{e\}$, то $hk = kh$ для любых $h \in H$, $k \in K$.

Доказательство. Так как $H \triangleleft G$ и $K \triangleleft G$, то

$$[k, h] = (k^{-1}h^{-1}k)h = h^{-1}(h^{-1}kh) \in H \cap K = \{e\},$$

поэтому $hk = kh$. □

Так как $G = HK$, то любой элемент $g \in G$ представим в виде $g = hk$, $h \in H$, $k \in K$. Покажем единственность этого представления. Если $g = hk = h'k'$, $h' \in H$, $k' \in K$, то

$$(h')^{-1}h = k'k^{-1} \in H \cap K = \{e\},$$

и поэтому $h' = h$, $k' = k$.

Если $h_1, h_2 \in H$, $k_1, k_2 \in K$, то по лемме ?? $k_1h_2 = h_2k_1$, и поэтому

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_2k_1)k_2 = (h_1h_2)(k_1k_2).$$

Пример 1.21.2. Пусть

$$\begin{aligned} G &= V_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subseteq S_4, \\ H &= \{e, (1\ 2)(3\ 4)\}, \quad K = \{e, (1\ 3)(2\ 4)\}, \quad L = \{e, (1\ 4)(2\ 3)\}. \end{aligned}$$

Так как четверная группа Клейна V_4 абелева, то все подгруппы в ней нормальны. Ясно, что

$$H \cap K = K \cap L = H \cap L = \{e\};$$

$$HK = KL = HL = V.$$

Таким образом,

$$V = H \times K = K \times L = H \times L.$$

Замечание 1.21.3. Определение внутреннего прямого произведения можно распространить на любое конечное множество нормальных подгрупп $H_i \triangleleft G$, $1 \leq i \leq m$, где

$$G = H_1 H_2 \dots H_m$$

и

$$H_i \cap \left\langle \bigcup_j H_j, j = 1, 2, \dots, m, j \neq i \right\rangle = \{e\}$$

(обозначение: $G = H_1 \times H_2 \times \dots \times H_m$).

В этом случае: $h_i h_j = h_j h_i$ для $h_i \in H_i$, $h_j \in H_j$, $i \neq j$; каждый элемент $g \in G$ единственным образом представляется в виде $g = h_1 h_2 \dots h_m$, $h_i \in H_i$; при этом

$$(h_1 h_2 \dots h_m)(h'_1 h'_2 \dots h'_m) = (h_1 h'_1)(h_2 h'_2) \dots (h_m h'_m).$$

Перейдём к рассмотрению конструкции *внешнего прямого произведения*. Пусть нам дано конечное множество групп G_1, G_2, \dots, G_m (в отличие от внутренней конструкции, они не предполагаются подгруппами одной группы). Рассмотрим множество

$$G = G_1 \times G_2 \times \dots \times G_m = \{(g_1, g_2, \dots, g_m) \mid g_i \in G_i\}$$

с бинарной операцией

$$(g_1, g_2, \dots, g_m)(g'_1, g'_2, \dots, g'_m) = (g_1 g'_1, g_2 g'_2, \dots, g_m g'_m), \quad g_i, g'_i \in G_i.$$

Ясно, что эта операция ассоциативна, $e = (e_{G_1}, e_{G_2}, \dots, e_{G_m})$ — нейтральный элемент, $(g_1, g_2, \dots, g_m)^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_m^{-1})$.

Итак, G — группа, называемая *внешним прямым произведением групп G_1, G_2, \dots, G_m* (обозначение: $G = G_1 \times G_2 \times \dots \times G_m$).

Группа G_i не является подгруппой внешнего прямого произведения $G = G_1 \times G_2 \times \dots \times G_m$, но в G имеется подгруппа G'_i , изоморфная группе G_i , а именно

$$G'_i = \{(e_{G_1}, e_{G_2}, \dots, a_i, \dots, e_{G_m}) \mid a \in G_i\}.$$

Так как для $g_i, h_i \in G_i$ имеем

$$(g_1, g_2, \dots, g_m)^{-1}(h_1, h_2, \dots, h_m)(g_1, g_2, \dots, g_m) = (g_1^{-1}h_1g_1, g_2^{-1}h_2g_2, \dots, g_m^{-1}h_mg_m),$$

то G'_i — нормальная подгруппа в G , $G'_i \triangleleft G$. Кроме того,

$$\begin{aligned} G &= G'_1 G'_2 \dots G'_m, \\ G'_i \cap \left\langle \bigcup_j G'_j \mid j = 1, \dots, m, j \neq i \right\rangle &= \{e\}. \end{aligned}$$

Итак, внешнее прямое произведение групп G_1, G_2, \dots, G_m является внутренним прямым произведением своих подгрупп G'_i , $G'_i \cong G_i$:

$$G = G_1 \times G_2 \times \dots \times G_m = G'_1 \times G'_2 \times \dots \times G'_m.$$

Кроме того, из анализа строение внутреннего прямого произведения $G = H_1 \times H_2 \times \dots \times H_m$ нормальных подгрупп $H_i \triangleleft G$, $1 \leq i \leq m$, мы видим, что группа G изоморфна внешнему прямому произведению групп H_i , $1 \leq i \leq m$, при соответствии

$$g = h_1 h_2 \dots h_m \mapsto (h_1, h_2, \dots, h_m).$$

В дальнейшем мы будем использовать термин «прямое произведение групп» без упоминания прилагательных «внутреннее» и «внешнее», понимая, что это разные описания одной и той же конструкции.

Замечание 1.21.4.

- 1) Ясно, что прямое произведение групп $G = H_1 \times H_2 \times \dots \times H_m$ является коммутативной группой тогда и только тогда, когда все группы H_1, \dots, H_m коммутативны.
- 2) Пусть A, B, A', B' — группы, $A \cong A', B \cong B', G = A \times B, G' = A' \times B'$. Тогда $G \cong G'$.
- 3) Для прямых разложений возможно, что $G = H_1 \times H_2 = K_1 \times K_2$, но $H_i \not\cong K_j$, $i, j \in \{1, 2\}$. Действительно,

$$\mathbb{Z}_{30} = \mathbb{Z}_2 \oplus \mathbb{Z}_{15} = \mathbb{Z}_5 \oplus \mathbb{Z}_6.$$

- 4) Группа $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ не является циклической, поскольку $|\mathbb{Z}_2 \oplus \mathbb{Z}_2| = 4$, но в группе $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ нет элементов четвёртого порядка, так как $2(a, b) = (2a, 2b) = (0, 0)$ для всех $(a, b) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
- 5) Группа $G = \mathbb{Z} \oplus \mathbb{Z}$ не является циклической, поскольку её гомоморфный образ (фактор-группа) $G/2G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ не является циклической (см. 1)).
- 6) Группа $(\mathbb{Q}, +)$ неразложима в прямую сумму собственных подгрупп, поскольку в \mathbb{Q} любые две ненулевые подгруппы имеют ненулевое пересечение.
- 7) Примарная циклическая группа \mathbb{Z}_{p^l} , где p — простое число, $l \geq 1$, уже неразложима в прямое произведение собственных подгрупп (поскольку все подгруппы в \mathbb{Z}_{p^l} образуют цепь).

Теорема 1.21.5. Пусть $G_i = (a_i)$, $O(a_i) = n_i$, $i = 1, \dots, m$, — циклические группы порядка n_i . Тогда прямое произведение $G = G_1 \times G_2 \times \dots \times G_m$ является циклической группой тогда и только тогда, когда порядки n_1, n_2, \dots, n_m попарно взаимно просты.

Доказательство.

- 1) Пусть числа n_1, n_2, \dots, n_m попарно взаимно просты и $(a_1, a_2, \dots, a_m)^k = (e_1, e_2, \dots, e_m)$, $k > 0$. Тогда $a_i^k = e_i$ для всех $1 \leq i \leq m$. Поэтому $k = n_i q_i$ и k делится на число $|G| = n = n_1 n_2 \dots n_m$. Итак, $O((a_1, a_2, \dots, a_m)) = n = |G|$, и следовательно, $G = ((a_1, a_2, \dots, a_m))$ — циклическая группа с циклическим образующим (a_1, a_2, \dots, a_m) .
- 2) Если $(n_i, n_j) = d > 1$, то

$$l = \text{НОК}(n_1, n_2, \dots, n_m) < n = n_1 n_2 \dots n_m,$$

и поэтому

$$(g_1, g_2, \dots, g_m)^l = (g_1^l, g_2^l, \dots, g_m^l) = (e_1, e_2, \dots, e_m).$$

Таким образом, в группе $G = G_1 \times G_2 \times \dots \times G_m$ нет элемента порядка $n = |G|$, и следовательно, группа G не является циклической. \square

Следствие 1.21.6. Если $n = p_1^{l_1} \dots p_m^{l_m}$, где p_1, \dots, p_m — различные простые числа, $l_i > 0$, $1 \leq i \leq m$, то

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{l_1}} \times \mathbb{Z}_{p_2^{l_2}} \times \dots \times \mathbb{Z}_{p_m^{l_m}}$$

(групповой вариант китайской теоремы об остатках), при этом примарные циклические сомножители $\mathbb{Z}_{p_i^{l_i}}$ далее в прямое произведение неразложимы.

Упражнения 1.21.7.

✓ 1) $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\cong \mathbb{Z}_4$.

✓ 2) $\mathbb{Z} \times \mathbb{Z}$ не является циклической группой.

3) $(\mathbb{C} \setminus \{0\}, \cdot) \cong \mathbb{R}_+^* \times T$, где $\mathbb{R}_+^* = \{r \in \mathbb{R} \mid r > 0\}$, $T = \{z \in \mathbb{C} \mid |z| = 1\}$.

4) $\{A \in \mathrm{GL}_n(\mathbb{R}) \mid |A| > 0\} \cong \{\lambda E \mid \lambda > 0\} \times \mathrm{SL}_n(\mathbb{R})$; если $n = 2k + 1$, то $\mathrm{GL}_n(\mathbb{R}) \cong \mathrm{SL}_n(\mathbb{R}) \times \mathbb{R}^*$.

5) Пусть G_1, G_2, G_3 — любые группы. Тогда

$$G_1 \times G_2 \times G_3 \cong G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3.$$

6) Если $H \triangleleft G$, $K \triangleleft G$ и $G = H \times K$, то $G/H \cong K$, $G/K \cong H$. Действительно, если $g \in G$ и $g = hk = kh$, $h \in H$, $k \in K$, — его каноническое представление, то $gH = khH = kH$. Если $kH = k'H$, $k' \in K$, то $g = hk = kh = k'h'$, $h' \in H$, поэтому $k = k'$, $h = h'$. Таким образом, биекция $gH \mapsto k$ является изоморфизмом групп G/H и K . Аналогично $G/K \cong H$.

7) Пусть

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R}, a \neq 0, c \neq 0 \right\} \subseteq \mathrm{GL}_2(\mathbb{R}),$$

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\} \subseteq G.$$

Тогда $H \triangleleft G$ и $G/H \cong \mathbb{R}^* \times \mathbb{R}^*$.

8) Отображение $S_n \times S_n \rightarrow S_{2n}$, где

$$(\sigma, \tau) \mapsto \begin{pmatrix} 1 & \dots & n & n+1 & \dots & 2n \\ \sigma(1) & \dots & \sigma(n) & \tau(n) & \dots & \tau(2n) \end{pmatrix},$$

является инъективным гомоморфизмом из прямого произведения $S_n \times S_n$ в группу S_{2n} .

9) $D_6 \cong \mathbb{Z}_2 \times D_3$.

10) Подгруппа H абелевой группы G выделяется в G прямым слагаемым тогда и только тогда, когда существует такой эпиморфизм $\pi: G \rightarrow H$, что $\pi^2 = \pi$.

- 11) Пусть $D = \{(g, g)\} \subseteq G \times G$ — диагональная подгруппа прямого квадрата $G \times G$ группы G . Тогда: $D \triangleleft G \times G$ — нормальная подгруппа в том и только в том случае, когда G — абелева группа.

Действительно, если G — абелева группа, то $G \times G$ — также абелева группа, и поэтому $D \triangleleft G \times G$.

Если же $D \triangleleft G \times G$, $g, h \in G$, то $(e, h)^{-1} = (e, h^{-1})$, и поэтому

$$(e, h^{-1})(g, g)(e, h) = (g, h^{-1}gh) \in D,$$

следовательно, $h^{-1}gh = g$. Итак, $gh = hg$ для всех $g, h \in G$. \square

Упражнение 1.21.8. Пусть G, H — периодические группы. Тогда $G \times H$ — периодическая группа. Если G, H — группы без кручения, то $G \times H$ также группа без кручения.

Замечания 1.21.9.

- 1) Существуют абелевые группы, разложимые в прямое произведение, но не допускающие прямых разложений с неразложимыми компонентами.
- 2) Если же все убывающие (или возрастающие) цепочки прямых множителей группы G обрываются, то группа G не может быть разложена в прямое произведение бесконечного множества подгрупп, а всякое её прямое разложение с конечным числом множителей может быть продолжено до прямого разложения, все сомножители которого неразложимы.
- 3) А. Г. Курош построил пример группы G с двумя неизоморфными прямыми разложениями

$$G = A \times B = C \times D,$$

в которых подгруппы A, B, C, D неразложимы в прямое произведение.

- 4) Условия для изоморфизма любых прямых разложений группы с неразложимыми множителями или существование изоморфных продолжений для произвольных прямых разложений дают теорема Ремака—Шмидта и её обобщения (см. ??).

Выделение совершенных нормальных подгрупп прямым сомножителем

Напомним, что группа G называется *совершенной*, если её центр тривиален ($Z(G) = \{e\}$) и всякий её автоморфизм является внутренним. Таким образом, совершенная группа канонически изоморфна группе своих автоморфизмов. Новые грани совершенных групп (нормальная инъективность) открывает следующая теорема.

Теорема 1.21.10 (Бэр (R. Baer, 1946)). Следующие условия на группу G равносильны:

- 1) G — совершенная группа;
- 2) группа G выделяется прямым сомножителем в любой группе \tilde{G} , в которой она содержится в качестве нормальной подгруппы, $G \trianglelefteq \tilde{G}$.

Доказательство.

1) \Rightarrow 2). Допустим, что группа \tilde{G} содержит нормальную подгруппу G , $G \trianglelefteq \tilde{G}$, являющуюся совершенной группой. Через N обозначим централизатор подгруппы G в группе \tilde{G} , $N = C_{\tilde{G}}(G)$. Как доказано в следствии к лемме ??,

$$N = C_{\tilde{G}}(G) \trianglelefteq N_{\tilde{G}}(G) = G.$$

Так как центр совершенной группы G тривиален, $Z(G) = \{e\}$, то $\tilde{G} \cap N = \{e\}$. Если $\tilde{g} \in \tilde{G}$, то внутренний автоморфизм $x \mapsto \tilde{g}^{-1}x\tilde{g}$ группы \tilde{G} , ограниченный на нормальную подгруппу $G \trianglelefteq \tilde{G}$, являющуюся совершенной, является внутренним, т. е. сопряжением с помощью элемента $g \in G$. Тогда $n = \tilde{g}g^{-1} \in C_{\tilde{G}}(G)$. Итак, $\tilde{g} = ng \in NG$. Таким образом,

$$\tilde{G} = N \times G.$$

Оставшуюся импликацию $2) \Rightarrow 1)$ оставим читателю к качеству упражнения. \square

Центральный изоморфизм прямых дополнений подгруппы

Подгруппы A и B группы G называются *центрально изоморфными*, если между ними существует такой изоморфизм

$$\varphi: A \rightarrow B,$$

что

$$a(\varphi(a))^{-1} \in Z(G).$$

В этом случае для $b = \varphi(a)$ имеем:

$$b^{-1}a = b^{-1}(ab^{-1})b = ab^{-1} \in Z(G);$$

$$\varphi(a) = b = az = za \text{ для } z = a^{-1}b = ba^{-1} \in Z(G).$$

Лемма 1.21.11. Если G — группа и

$$G = A_1 \times B = A_2 \times B,$$

то подгруппы A_1 и A_2 центрально изоморфны.

Доказательство. Так как имеем канонические изоморфизмы

$$A_1 \cong G/B \cong A_2, \quad a_1 \mapsto a_1B = a_2B \mapsto a_2;$$

то имеем изоморфизм

$$\varphi: A_1 \rightarrow A_2,$$

для которого

$$a_1 = \varphi(a_1)b, \quad b \in B,$$

и поэтому элемент b перестановчен с любым элементом из A_2 . Кроме того, любой элемент из B перестановчен как с a_1 , так и с a_2 , а поэтому и с b . Таким образом, $b \in Z(G)$. \square

Замечание 1.21.12. Центральные изоморфизмы подгрупп существенны в развитии общей теории прямых разложений групп.

1.22. Автоморфизмы группы

Напомним, что *автоморфизмом* группы G называется биекция $f: G \rightarrow G$, являющаяся гомоморфизмом. Через $\text{Aut}(G)$ обозначим множество всех автоморфизмов группы G .

Предложение 1.22.1. Если G — группа, то $\text{Aut}(G)$ — группа, являющаяся подгруппой группы подстановок $S(G)$, $\text{Aut}(G) \subseteq S(G)$.

Доказательство. Так как произведение автоморфизмов — автоморфизм (из свойств гомоморфизмов и изоморфизмов), то операция произведения в группе подстановок $S(G)$ на множестве G не выводит нас из $\text{Aut}(G)$.

Ассоциативность этой операции на $\text{Aut}(G)$ является следствием ассоциативности операции умножения в $S(G)$. Ясно, что тождественное отображение 1_G является автоморфизмом и нейтральным элементом в $\text{Aut}(G)$. Если $f \in \text{Aut}(G)$, то f^{-1} также автоморфизм (из свойств гомоморфизмов и изоморфизмов). Итак, $\text{Aut}(G)$ — группа, являющаяся подгруппой группы подстановок $S(G)$ на множестве G . \square

Примеры 1.22.2 (автоморфизмов групп).

- 1) Как мы уже отметили, тождественное отображение 1_G является автоморфизмом любой группы G .
- 2) Если $(A, +)$ — абелева группа, то отображение $\alpha: A \rightarrow A$, где $\alpha(a) = -a$ для $a \in A$, является автоморфизмом. Действительно, α — биекция, при этом

$$\alpha(x+y) = -(x+y) = -x-y = \alpha(x) + \alpha(y),$$

т. е. α — гомоморфизм. Итак, α — автоморфизм.

- 3) Пусть G — группа, и пусть отображение $f: G \rightarrow G$, $f(x) = x^{-1}$ для $x \in G$, является гомоморфизмом (т. е. пусть биекция $x \mapsto x^{-1}$ — автоморфизм), тогда G — абелева группа (это объясняет, почему в 2) мы предполагали, что A — абелева группа). Действительно, для любых $x, y \in G$ имеем

$$y^{-1}x^{-1} = (xy)^{-1} = f(xy) = f(x)f(y) = x^{-1}y^{-1}.$$

Поэтому $xyx^{-1}y^{-1} = e$ и $xy = yx$.

Лемма 1.22.3. $\alpha \in \text{Aut} \implies O(\alpha(g)) = O(g) \forall g \in G$.

Группа автоморфизмов циклических групп

Теорема 1.22.4. Пусть $G = G(a)$ — циклическая группа с образующим элементом a . Тогда:

- 1) если $|G| = O(a) = \infty$ (т. е. если G — бесконечная циклическая группа, $G \cong (\mathbb{Z}, +)$), то $\text{Aut}((\mathbb{Z}, +)) \cong \mathbb{Z}_2$, $|\text{Aut}(G)| = 2$;
- 2) если $|G| = O(a) = n < \infty$, $G \cong \mathbb{Z}_n$, то $\text{Aut}((\mathbb{Z}_n, +)) \cong U(\mathbb{Z}_n)$, $|\text{Aut}((\mathbb{Z}_m, +))| = \varphi(m)$, где $\varphi(m)$ — функция Эйлера.

Доказательство. Пусть $G = \langle a \rangle$ — циклическая группа.

Случай 1: $G = \langle a \rangle$; $O(a) = \infty$, $G \cong (\mathbb{Z}, +)$, — бесконечная циклическая группа. Если $f: \mathbb{Z} \rightarrow \mathbb{Z}$ — автоморфизм группы $(\mathbb{Z}, +)$, то f полностью определяется целым числом $n = f(1) \in \mathbb{Z}$, поскольку

$$f(m) = f(m \cdot 1) = mf(1) = mn$$

для всех $m \in \mathbb{Z}$. Так как f — сюръекция, то $1 = f(t)$ для некоторого $t \in \mathbb{Z}$, поэтому

$$1 = f(t) = f(t \cdot 1) = tf(1) = tn.$$

Таким образом, $n = \pm 1$. Итак, либо $f = 1_{\mathbb{Z}}$ ($f(1) = 1$), либо $f(m) = -m$ для всех $m \in \mathbb{Z}$ ($f(1) = -1$). Следовательно, $|\text{Aut}(\mathbb{Z})| = 2$, т. е. $\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

Замечание 1.22.5. Пример $G = (\mathbb{Z}, +)$ показывает, что $\text{Aut}(G)$ может быть маленькой подгруппой в группе $S(G)$: $|\text{Aut}(\mathbb{Z})| = 2$, хотя группа подстановок $S(\mathbb{Z})$ на множестве \mathbb{Z} несчётна.

Случай 2: пусть $G = \langle a \rangle$, $n = |G| = O(a) < \infty$, $f: G \rightarrow G$ — автоморфизм.

а) Ясно, что f полностью определяется элементом $f(a) \in G$, поскольку $f(a^k) = f(a)^k$ для всех $k \in \mathbb{Z}$. Так как f — изоморфизм, то $O(f(a)) = O(a) = n$ (см. ??), т. е. $f(a)$ — образующий циклической группы $G = \langle a \rangle$, и поэтому (см. ??) $f(a) = a^i$, где $1 \leq i < m$, $(i, m) = 1$.

б) Если же $i \in \mathbb{Z}$, $1 \leq i < n$, $(i, n) = 1$, то отображение $f: G \rightarrow G$, $f(g) = g^i$ для всех $g \in G$, является гомоморфизмом, поскольку $G = \langle a \rangle$ — абелева группа:

$$f(g_1g_2) = (g_1g_2)^i = g_1^i g_2^i = f(g_1)f(g_2)$$

для всех $g_1, g_2 \in G$.

Так как $f(a) = a^i$ и $(i, n) = 1$, то

$$O(f(a)) = O(a^i) = \frac{n}{(i, n)} = n,$$

поэтому $f(a)$ является образующим группы $G = \langle a \rangle$, и следовательно, $\text{Im } f = G$, т. е. $f: G \rightarrow G$ — сюръективное отображение. Но G — конечное множество, поэтому (см. ??) f — биекция, т. е. $f \in \text{Aut}(G)$.

в) Итак, мы описали строение всех автоморфизмов $f \in \text{Aut}(G)$, где $G = \langle a \rangle$, $|G| = O(a) = n < \infty$, $G \cong \mathbb{Z}_n$, доказав, что $\text{Aut}(\mathbb{Z}_n) \cong U(\mathbb{Z}_n, \cdot)$. Из этого описания следует, что $|\text{Aut}(G)| = \varphi(n)$ для $G = \langle a \rangle$, $|G| = O(a) = n < \infty$, где $\varphi(n)$ — функция Эйлера. \square

Следствие 1.22.6. Если G — циклическая группа, то $\text{Aut}(G)$ — коммутативная группа, поскольку кольцо вычетов \mathbb{Z}_n коммутативно.

Упражнение 1.22.7. $\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ для простого числа p (мультиликативная группа $U(\mathbb{Z}_p)$ поля \mathbb{Z}_p циклическая); $\text{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$; $\text{Aut}(\mathbb{Z}_8) \cong V_4 \cong \text{Aut}(\mathbb{Z}_{12})$, это показывает, что группа автоморфизмов циклической группы может не быть циклической; $\text{Aut}(\mathbb{Z}_9) \cong \mathbb{Z}_6$; $\text{Aut}(\mathbb{Z}_{14}) \cong \mathbb{Z}_6$; $\text{Aut}(A_3) \cong \mathbb{Z}_2$ ($A_3 \cong \mathbb{Z}_3$).

Упражнение 1.22.8. Пусть G — конечная группа, $T \in \text{Aut}(G)$. Предположим, что $T(x) = x$ тогда и только тогда, когда $x = e$ (т. е. $\text{Ker } T = \{e\}$). Тогда:

- 1) каждый элемент $g \in G$ может быть записан в виде $g = x^{-1}T(x)$ для некоторого $x \in G$;
- 2) если к тому же $T^2 = 1_G$, то G — абелева группа.

Доказательство.

- 1) Если $x, y \in G$ и $x^{-1}T(x) = y^{-1}T(y)$, то

$$T(yx^{-1}) = T(y)T(x)^{-1} = yx^{-1}T(x)T(x)^{-1} = yx^{-1},$$

и поэтому $yx^{-1} = e$, т. е. $y = x$. Итак,

$$|\{x^{-1}T(x) \mid x \in G\}| = |G|,$$

и следовательно,

$$\{x^{-1}T(x) \mid x \in G\} = G.$$

- 2) Пусть $x \in G$. Тогда

$$x^{-1}T(x) = T^2(x^{-1}T(x)) = T(T(x^{-1}))T^2(x) = T(T(x^{-1})x) = T((x^{-1}T(x))^{-1}).$$

Итак, для всех $g \in G$ имеем $g = T(g^{-1})$, и поэтому для $a, b \in G$

$$ab = T((ab)^{-1}) = T(b^{-1}a^{-1}) = T(b^{-1})T(a^{-1}) = ba.$$

Следовательно, G — абелева группа. \square

Замечание 1.22.9. Если отображение $\varphi: G \rightarrow G$, $\varphi(a) = a^{-1}$ для $a \in G$, является автоморфизмом группы G , то группа G абелева.

Указание. $\varphi(ab) = (ab)^{-1} = b^{-1}a^{-1} = \varphi(b)\varphi(a) = \varphi(ba)$. Поэтому $ab = ba$ для всех $a, b \in G$.

Упражнение 1.22.10. Найдите все такие группы G , что $\text{Aut}(G)$ — тривиальная группа.

Указание. Для элемента $g \in G$ внутренний автоморфизм $x \mapsto g^{-1}xg$ для всех $x \in G$ является тривиальным в том и только в том случае, когда $g \in Z(G)$. Так как в нашем случае $\text{Aut}(G) = \{e\}$, получаем, что G — абелева группа. Если $g \in G$, $O(g) > 2$, то автоморфизм $x \mapsto x^{-1}$ нетривиален ($g^{-1} \neq g$). Следовательно, любой неединичный элемент группы G имеет порядок 2. Таким образом, наша абелева группа G является линейным пространством над полем \mathbb{Z}_2 . Если $\dim_{\mathbb{Z}_2} G \geq 1$, то любая нетривиальная перестановка элементов базиса задаёт нетривиальный автоморфизм группы G . Следовательно, $\dim_{\mathbb{Z}_2} G \leq 1$, т. е. $G = \{e\}$ или G — циклическая группа порядка 2.

Упражнение 1.22.11.

- 1) Пусть $G = \mathbb{Z} \times \mathbb{Z} = \{(m, n) \mid m, n \in \mathbb{Z}\}$. Тогда $\text{Aut } G \cong \text{GL}_2(\mathbb{Z})$, и эта группа не является абелевой.
- 2) Пусть $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ (группа Клейна). Тогда $\text{Aut}(V_4) \cong \text{GL}_2(\mathbb{Z}_2) \cong S_3$.

Лемма 1.22.12. Пусть G_1 и G_2 — конечные группы взаимно простых порядков, $m = |G_1|$, $n = |G_2|$, $(m, n) = 1$. Тогда

$$\text{Aut}(G_1 \times G_2) \cong \text{Aut } G_1 \times \text{Aut } G_2.$$

Доказательство. Пусть $\alpha \in \text{Aut}(G_1 \times G_2)$,

$$\alpha: G_1 \times G_2 \rightarrow G_1 \times G_2.$$

Так как α — инъективное отображение, то

$$|\alpha(G_1)| = |G'_1| = |G_1| = m, \quad |\alpha(G_2)| = |G'_2| = |G_2| = n,$$

где

$$G'_1 = \{(g_1, e_{G_2}) \mid g_1 \in G_1\}, \quad G'_2 = \{(e_{G_1}, g_2) \mid g_2 \in G_2\},$$

$$G'_1 \cong G_1, \quad G'_2 \cong G_2.$$

Если $g_1 \in G_1, g_2 \in G_2$, то $O((g_1, g_2)) = \text{НОК}(O(g_1), O(g_2))$ (см. ??), и поэтому для $g_2 \neq e_{G_2}$ из $(O(g_1), O(g_2)) = 1$ следует, что $O((g_1, g_2))$ не является делителем числа $m = |G'_1| = |G_1|$. Итак,

$$G'_1 = \{(g_1, g_2) \in G_1 \times G_2 \mid O((g_1, g_2)) \text{ — делитель числа } m\}.$$

Отсюда следует, что $\alpha(G'_1) \subseteq G'_1$. Так как $|\alpha(G'_1)| = m = |G'_1|$, то $\alpha(G'_1) = G'_1$. Таким образом,

$$\alpha_1 = \alpha|_{G'_1}: G'_1 \rightarrow G'_1 \in \text{Aut}(G'_1) \cong \text{Aut}(G_1).$$

Аналогично,

$$\alpha_2 = \alpha|_{G'_2}: G'_2 \rightarrow G'_2 \in \text{Aut}(G'_2) \cong \text{Aut}(G_2).$$

При этом отображение

$$\Delta: \text{Aut}(G_1 \times G_2) \rightarrow \text{Aut} G'_1 \times \text{Aut} G'_2, \quad \Delta(\alpha) = (\alpha_1, \alpha_2),$$

является гомоморфизмом: если $\alpha, \beta \in \text{Aut}(G_1 \times G_2)$, то

$$\Delta(\alpha\beta) = ((\alpha\beta)_1, (\alpha\beta)_2) = (\alpha_1\beta_1, \alpha_2\beta_2) = (\alpha_1, \alpha_2)(\beta_1, \beta_2) = \Delta(\alpha)\Delta(\beta).$$

Если

$$\Delta(\alpha) = (\alpha_1, \alpha_2) = (1_{G'_1}, 1_{G'_2}),$$

то

$$\alpha|_{G'_1} = \alpha_1 = 1_{G'_1}, \quad \alpha|_{G'_2} = \alpha_2 = 1_{G'_2},$$

поэтому для $(g_1, g_2) \in G_1 \times G_2$ имеем

$$\begin{aligned} \alpha((g_1, g_2)) &= \alpha((g_1, e_{G_2})(e_{G_1}, g_2)) = \alpha((g_1, g_2))\alpha((e_{G_1}, g_2)) = \\ &= \alpha_1((g_1, e_{G_2})) \cdot \alpha_2((e_{G_1}, g_2)) = (g_1, e_{G_2})(e_{G_1}, g_2) = (g_1, g_2). \end{aligned}$$

Так как $G'_1 \cong G_1, G'_2 \cong G_2$, то имеем канонический изоморфизм

$$\text{Aut} G'_1 \times \text{Aut} G'_2 \cong \text{Aut} G_1 \times \text{Aut} G_2.$$

Итак,

$$\text{Aut}(G_1 \times G_2) \cong \text{Aut} G_1 \times \text{Aut} G_2. \quad \square$$

 **Следствие 1.22.13.** Если φ — функция Эйлера, $\varphi(m) = |\text{U}(\mathbb{Z}_m)|$, то для $m, n \in \mathbb{N}$ с $(m, n) = 1$ имеем $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказательство проведём с использованием теорем о группах автоморфизмов (прямое доказательство — см. ??):

$$\begin{aligned} \varphi(mn) &= |\text{U}(\mathbb{Z}_{mn})| = |\text{Aut}(\mathbb{Z}_{mn})| = |\text{Aut}(\mathbb{Z}_m \times \mathbb{Z}_n)| = \\ &= |\text{Aut}(\mathbb{Z}_m) \times \text{Aut}(\mathbb{Z}_n)| = |\text{Aut}(\mathbb{Z}_m)| \cdot |\text{Aut}(\mathbb{Z}_n)| = \varphi(m)\varphi(n). \quad \square \end{aligned}$$

14-45

1.23. Внутренние автоморфизмы

Определение 1.23.1. Пусть G — группа, $g, x \in G$. Элемент $gxg^{-1} \in G$ называется элементом, сопряжённым с элементом x с помощью элемента g (иногда используется обозначение $gxg^{-1} = x^g$).

Лемма 1.23.2. Пусть G — группа. Для каждого элемента $g \in G$ отображение

$$\tau(g): G \rightarrow G, \quad \tau(g)(x) = gxg^{-1} \text{ для } x \in G,$$

является автоморфизмом группы G (называемым внутренним автоморфизмом группы G , индуцированным элементом $g \in G$).

Доказательство.

1) Если $x, y \in G$, то

$$\tau(g)(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = (\tau(g)x)(\tau(g)(y)),$$

т. е. $\tau(g): G \rightarrow G$ — гомоморфизм группы.

2) Так как $\tau(g^{-1}) = \tau(g)^{-1}$, то $\tau(g)$ — биекция, и поэтому $\tau(g)$ — автоморфизм группы G . \square

Соберём вместе свойства отображения $\tau: G \rightarrow \text{Aut}(G)$.

Теорема 1.23.3 (свойства внутренних автоморфизмов). Пусть G — группа. Тогда:

- 1) отображение $\tau: G \rightarrow \text{Aut}(G)$, $\tau(g)(x) = gxg^{-1}$, $g \in G$, $x \in G$, является гомоморфизмом групп (называемым гомоморфизмом сопряжения);
- 2) образ гомоморфизма $\tau: G \rightarrow \text{Aut}(G)$, т. е. совокупность $\text{Inn}(G) = \{\tau(g) \in \text{Aut}(G) \mid g \in G\} = \text{Im } \tau$ всех внутренних автоморфизмов $\tau(g)$, $g \in G$, является нормальной подгруппой группы автоморфизмов $\text{Aut}(G)$ (группа $\text{Inn}(G)$ называется группой внутренних автоморфизмов группы G);
- 3) $\text{Ker}(\tau) = Z(G)$, т. е. ядро $\text{Ker}(\tau)$ гомоморфизма τ совпадает с центром $Z(G)$ группы G ;
- 4) а) $\text{Inn}(G) \cong G/Z(G)$, группа $\text{Inn}(G)$ внутренних автоморфизмов изоморфна фактор-группе группы G по её центру $Z(G)$;

б) если G — некоммутативная группа, то группа $\text{Aut}(G)$ не является циклической (если $\text{Aut}(G)$ — циклическая группа, то её подгруппа $\text{Inn}(G)$ также циклическая, но тогда $G/Z(G) \cong \text{Inn}(G)$ — циклическая группа, и поэтому $G = Z(G)$ — абелева группа, что противоречит предположению);
- 5) имеет место точная последовательность

$$1 \rightarrow Z(G) \xrightarrow{i} G \xrightarrow{\tau} \text{Aut}(G) \xrightarrow{\pi} \text{Aut}(G)/\text{Inn}(G) \rightarrow 1,$$

где i — вложение, τ — гомоморфизм сопряжения, π — канонический гомоморфизм на фактор-группу (фактор-группа $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$ часто называется группой внешних автоморфизмов, хотя её элементы — смежные классы $\varphi \text{Inn}(G)$, где $\varphi \in \text{Aut}(G)$).

Доказательство.

1) Если $g, h \in G$, то

$$\tau(gh)(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = \tau(g)(\tau(h)(x))$$

для всех $x \in G$. Итак, $\tau(gh) = \tau(g)\tau(h)$ для всех $g, h \in G$, т. е. $\tau: G \rightarrow \text{Aut}(G)$ — гомоморфизм группы.

2) Совокупность $\text{Inn}(G) = \{\tau(g) \in \text{Aut}(G) \mid g \in G\}$ всех внутренних автоморфизмов $\tau(g)$, $g \in G$, в группе $\text{Aut}(G)$ как образ гомоморфизма τ является подгруппой группы $\text{Aut}(G)$.

Если $\alpha \in \text{Aut}(G)$ и $g \in G$, $x \in G$, то

$$\begin{aligned} \tau(\alpha(g))(x) &= \alpha(g)x\alpha(g)^{-1} = \alpha(g)x\alpha(g^{-1}) = \\ &= \alpha(g\alpha^{-1}(x)g^{-1}) = \alpha(\tau(g)(\alpha^{-1}(x))) = (\alpha\tau(g)\alpha^{-1})(x), \end{aligned}$$

поэтому

$$\alpha\tau(g)\alpha^{-1} = \tau(\alpha(g)) \in \text{Inn}(G),$$

следовательно,

$$\text{Inn}(G) \triangleleft \text{Aut}(G).$$

3) Элемент $g \in G$ принадлежит ядру $\text{Ker } \tau$ гомоморфизма τ тогда и только тогда, когда $\tau(g)(x) = x$ для всех $x \in G$, т. е. $g x g^{-1} = x$, или $gx = xg$, но это означает, что $g \in Z(G)$. Итак, $\text{Ker } \tau = Z(G)$.

4) В силу теоремы о гомоморфизме для сюръективного гомоморфизма $\tau: G \rightarrow \text{Inn}(G)$ имеем

$$\text{Inn}(G) = \text{Im } \tau \cong G / \text{Ker } \tau = G / Z(G).$$

5) Для указанной последовательности на каждом месте имеем равенство образа предыдущего гомоморфизма с ядром последующего гомоморфизма. Итак, последовательность

$$1 \rightarrow Z(G) \xrightarrow{i} G \xrightarrow{\pi} \text{Aut}(G) \xrightarrow{\text{Out}} \text{Out}(G) \rightarrow 1$$

является точной. □

Замечание 1.23.4. Если G — абелева группа, то $\text{Inn } G = 1_G$, и поэтому $\text{Aut}(G) = \text{Out}(G)$ (все автоморфизмы абелевой группы внешние).

Теорема 1.23.5. Если $Z(G) = \{e_G\}$, то $Z(\text{Aut}(G)) = \{1_G\}$.

Доказательство. Допустим противное. Пусть $f \in Z(\text{Aut}(G))$ и $f \neq 1_G$, $f(a) = b \neq a$ для $a, b \in G$. Тогда для любого $g \in G$

$$a^{-1}(f(g))a = f(a^{-1}ga) = f(a)^{-1}f(g)f(a) = b^{-1}f(g)b,$$

поэтому, поскольку $f(G) = G$, два внутренних автоморфизма сопряжения с помощью элементов a и b , $b \neq a$, совпадают: $a^{-1}za = b^{-1}zb$ для всех $z \in G$. Это противоречит тому, что

$$1 \rightarrow Z(G) \xrightarrow{i} G \xrightarrow{\pi} \text{Inn}(G) \rightarrow 1$$

и $Z(G) = \{1_G\}$, т. е. π — изоморфизм,

$$1 \rightarrow G \xrightarrow{\pi} \text{Inn}(G) \rightarrow 1. \quad \square$$

Замечание 1.23.6. Обратное утверждение к теореме 1.23.5 не имеет места. Например, если $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, то $Z(G) = G \neq \{e\}$, однако $\text{Aut}(G) \cong S_3$, $Z(S_3) = \{e\}$.

Упражнение 1.23.7. Автоморфизм $\alpha \in \text{Aut}(G)$ группы G называется центральным, если

$$\alpha(x) \in xZ(G),$$

где $Z(G)$ — центр группы G . Покажите, что группа центральных внутренних автоморфизмов изоморфна центру $Z(G/Z(G))$ фактор-группы $G/Z(G)$.

Замечание 1.23.8.

- 1) Если K — поле и $G = \text{GL}_n(K)$ — группа $(n \times n)$ -обратимых матриц над полем K , то $Z(G) = \{\lambda E \mid 0 \neq \lambda \in K\}$ — группа ненулевых скалярных матриц, и поэтому

$$\text{Inn}(\text{GL}_n(K)) \cong \text{GL}_n(K)/\{\lambda E \mid 0 \neq \lambda \in K\} = \text{PGL}_n(K) =$$

проективная линейная группа.

- 2) Если G — конечная нециклическая абелева группа, то группа $\text{Aut}(G)$ неабелева.
 3) Не существует такой группы G , что $[G, G] = S_4$.

Указание. Допустим, что $[G, G] \cong S_4$. Тогда для любого $g \in G$ отображение $h \mapsto g^{-1}hg$, $h \in [G, G]$, является автоморфизмом группы $[G, G]$. Так как $[G, G] \cong S_4$ и все автоморфизмы группы S_4 внутренние, то существует такой элемент $v \in [G, G]$, что $g^{-1}hg = v^{-1}hv$ для всех $h \in [G, G]$. Покажите, что в этой ситуации $G' = [G, G] = [G', G']$. Но это приводит к противоречию с тем, что $S_4' = A_4 \neq S_4$. \square

Упражнение 1.23.9.

- 1) $\text{Aut}(\mathbb{Q}) \cong \mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \cdot)$.
 2) $\text{Aut}(S_3) = \text{Inn}(S_3) \cong S_3$. Действительно: так как $Z(S_3) = \{e\}$, то $\text{Inn}(S_3) \cong S_3$, поэтому $|\text{Aut}(S_3)| \geq 6$; $S_3 = \{e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$, где $\alpha^3 = e = \beta^2$, $\alpha\beta = \alpha^2\beta$, $O(\alpha) = O(\alpha^2) = 3$, $O(\beta) = O(\alpha\beta) = O(\alpha^2\beta) = 2$, и поэтому $\varphi(\alpha) \in \{\alpha, \alpha^2\}$, $\varphi(\beta) \in \{\beta, \alpha\beta, \alpha^2\beta\}$ для любого $\varphi \in \text{Aut}(S_3)$, откуда $|\text{Aut}(S_3)| \leq 6$. Следовательно, $\text{Aut}(S_3) = \text{Inn}(S_3) \cong S_3$.
 3) Если p — простое число, $G = \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_n$, то

$$\begin{aligned} \text{Aut}(G) &\cong \text{GL}_r(\mathbb{Z}_p), \\ |\text{Aut}(G)| &= (p^r - 1)(p^r - p) \dots (p^r - p^{r-1}). \end{aligned}$$

4) $\text{Aut}\left(\underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_n\right) \cong \text{GL}_n(\mathbb{Z})$.

5) $\text{Aut}\left(\underbrace{\mathbb{Z}_m \oplus \dots \oplus \mathbb{Z}_m}_n\right) \cong \text{GL}_n(\mathbb{Z}_m)$.

6) $\text{Aut}(\mathbb{Z}_2 \oplus \mathbb{Z}_4) \cong D_8$.

- 7) $\text{Aut}(D_8) \cong D_8$, $Z(D_8) \neq \{e\}$, и поэтому группа D_8 обладает внешними автоморфизмами.
- 8) $\text{Aut}(Q_8) \cong S_4$.
- 9) $\text{Aut}((1\ 2)(3\ 4)(5\ 6), (3\ 4)) \cong S_3$.
- 10) $\text{Aut}(A_4) \cong S_4$.

Задача 1.23.10. Пусть $G = \langle(1\ 2), (1\ 3\ 5)(2\ 4\ 6)\rangle \subseteq S_6$, $H = \langle(1\ 2), (3\ 4), (5\ 6)\rangle$. Покажите, что $G \triangleright H$, $|\text{Aut}(G)| \leq 56$, $|\text{Aut}(H)| = 168$. Таким образом, $H \triangleleft G$, $|H| < |G|$, но $|\text{Aut}(H)| \nmid |\text{Aut}(G)|$.

Замечание 1.23.11. Конечные циклические группы нечётных порядков не могут быть группами автоморфизмов групп. Действительно, группа автоморфизмов абелевой группы, отличной от \mathbb{Z}_2 , содержит элемент порядка 2. Группа автоморфизмов $\text{Aut}(G)$ некоммутативной группы G содержит нормальную подгруппу внутренних автоморфизмов $\text{Inn}(G) \cong G/Z(G)$ (фактор-группа некоммутативной группы по центру не может быть циклической).

Теорема 1.23.12. Группа автоморфизмов $\text{Aut}(D_p)$ группы диэдра $G = D_p$ (т. е. группы симметрий правильного p -угольника), где p — нечётное простое число, содержит $p(p-1)$ элементов.

Доказательство.

1) Пусть $\{1, 2, \dots, p\}$ — множество вершин регулярного p -угольника. Тогда группа $G = D_p$ содержит следующие элементы: p -цикл $\sigma = (1\ 2\ \dots\ p)$ (вращение против часовой стрелки на угол $\frac{2\pi}{p}$), подстановку $\tau = (1)(2\ p)(3\ (p-1)) \dots \left(\frac{p+1}{2}\ \frac{p+3}{2}\right)$ (отражение относительно прямой, проходящей через вершину 1 и середину противоположной стороны). Ясно, что мы имеем $2p$ различных элементов группы G : σ^r и $\sigma^r\tau$, где $r = 0, 1, \dots, p-1$.

Так как $|G| = 2p$, то

$$G = \{\sigma^r, \sigma^r\tau \mid r = 0, 1, \dots, p-1\},$$

при этом $\sigma^r\tau$ — отражения, $O(\sigma^r\tau) = 2$, σ^r — вращения, $O(\sigma^r)$ — или 1, или p .

Если $f \in \text{Aut}(G)$, то по ??:

$$O(f(\sigma)) = p,$$

и поэтому $f(\sigma) = \sigma^r$, где $1 \leq r < p$;

$$O(f(\tau)) = 2,$$

и следовательно, $f(\tau) = \sigma^s\tau$, где $0 \leq s < p$. Ясно, что автоморфизм $f \in \text{Aut}(G)$ полностью определяется своими значениями $f(\sigma)$ и $f(\tau)$ на образующих σ и τ группы G , поскольку $f(\sigma^i) = f(\sigma)^i$, $f(\sigma^i\tau) = f(\sigma)^i f(\tau)$. Таким образом, возможностей для выбора f не более чем $p(p-1)$. Итак, мы показали, что $|\text{Aut}(G)| \leq p(p-1)$.

2) Наша цель теперь — построить $p(p-1)$ различных автоморфизмов в группе $\text{Aut}(G)$.

Ясно, что $Z(G) = 1$ (см. ??), поэтому (см. ??)

$$\text{Inn}(G) \cong G/Z(G) \cong G.$$

Следовательно,

$$|\text{Inn}(G)| = 2p,$$

и поскольку $\text{Inn}(G) \leqslant \text{Aut}(G)$, то по теореме Лагранжа порядок $|\text{Aut}(G)|$ группы $\text{Aut}(G)$ делится на p .

Далее, если $0 < r < p$, то построим гомоморфизм $f_r: G \rightarrow G$, для которого $f_r(\sigma) = \sigma^r$, $f_r(\tau) = \tau$. Проверим, что $f_r: G \rightarrow G$ — гомоморфизм групп, т. е. что $f_r(xy) = f_r(x)f_r(y)$ для всех $x, y \in G$. Действительно,

Далее, ясно, что f_r — сюръекция, поскольку элемент σ^r порождает циклическую группу $\langle \sigma \rangle$, и поэтому f_r — автоморфизм.

Так как $f_rf_s = f_{rs}$ для $0 < r, s < p$, то отображение

$$(\text{U}(\mathbb{Z}_p), \cdot) \rightarrow H = \{f_r \mid 1 \leqslant r < p\} \subseteq \text{Aut}(G), \quad r, (r, p) = 1 \mapsto f_r,$$

является гомоморфизмом групп. Этот гомоморфизм сюръективен.

Если же $f_r = 1_G$, то $r \equiv 1 \pmod{p}$, т. е. наше отображение инъективно.

Итак, мы установили изоморфизм групп $\text{U}(\mathbb{Z}_p) \cong H$. Так как $|\text{U}(\mathbb{Z}_p)| = p - 1$ и H — подгруппа группы $\text{Aut}(G)$, то порядок $|\text{Aut}(G)|$ делится на $p - 1$. Поскольку $(p, p - 1) = 1$, порядок группы $|\text{Aut}(G)|$ делится на $p(p - 1)$. Итак, $|\text{Aut}(G)| = p(p - 1)$. \square

Следствие 1.23.13. Если $G = \text{Dih}(2p)$, то

$$\begin{aligned} |\text{Inn}(G)| &= |G| = 2p, \\ |\text{Out}(G)| &= \frac{p(p-1)}{2p} = \frac{p-1}{2}, \end{aligned}$$

и поэтому $|\text{Out}(G)| = 1$ тогда и только тогда, когда $p = 3$ (в этом случае $G = \text{Dih}(G) \cong S_3$).
 $Z(G) = \{e\}$, $\text{Aut}(G) = \text{Inn}(G) \cong G$.

1.24. Теорема Гёльдера об автоморфизмах группы подстановок

Лемма 1.24.1. Пусть $n \geqslant 2$, $\varphi \in \text{Aut}(S_n)$ и существует такая транспозиция $\tau \in S_n$, что $\varphi(\tau)$ тоже транспозиция. Тогда $\varphi \in \text{Inn}(S_n)$.

Доказательство. Любой автоморфизм группы S_n переводит класс сопряжённых элементов в класс сопряжённых элементов. По условию леммы для любой транспозиции σ подстановка $\varphi(\sigma)$ также транспозиция.

Пусть $\tau_j = (j, j+1)$, $j = 1, \dots, n-1$. Тогда $\sigma_j = \varphi(\tau_j)$ — транспозиции. Так как $\tau_1\tau_2 \neq \tau_2\tau_1$, то $\sigma_1 = (i_1, i_2)$, $\sigma_2 = (i_2, i_3)$, $1 \leqslant i_1, i_2, i_3 \leqslant n$, $i_1 \neq i_3$. Более того, $\sigma_1\sigma_3 = \sigma_3\sigma_1$, $\sigma_2\sigma_3 \neq \sigma_3\sigma_2$. Продолжая этот процесс, получаем, что $\sigma_1 = (i_1, i_2)$, $\sigma_2 = (i_2, i_3), \dots, \sigma_{n-1} = (i_{n-1}, i_n)$, $\{i_1, \dots, i_n\} = \{1, 2, \dots, n\}$.

Пусть $\sigma \in S_n$, $\sigma(k) = i_k$ ($1 \leqslant k \leqslant n$). Тогда $f(\tau_j) = \sigma\tau_j\sigma^{-1}$, $j = 1, \dots, n-1$. Так как транспозиции $\tau_1, \dots, \tau_{n-1}$ порождают группу S_n , то $f(\tau) = \sigma\tau\sigma^{-1}$ для любой подстановки $\tau \in S_n$. \square

Лемма 1.24.2. Пусть $n \in \mathbb{N}$, $n \geqslant 2$, $n \neq 6$, τ — транспозиция, $\tau \in S_n$, $\varphi \in \text{Aut}(S_n)$. Тогда $\varphi(\tau)$ — транспозиция.

Доказательство. Так как $O(\tau) = 2$, то $O(\varphi(\tau)) = 2$. Следовательно, $\varphi(\tau)$ является произведением k независимых транспозиций, при этом $1 \leq k \leq \frac{n}{2}$. Если τ пробегает всё множество транспозиций, являющееся классом сопряжённых элементов, порождающих группу S_n , то $\varphi(\tau)$ пробегает класс сопряжённых элементов, порождающий группу S_n . Поэтому k — нечётное число.

Пусть $C(\tau)$ и $C(\varphi(\tau))$ — централизаторы подстановок τ и $\varphi(\tau)$ в группе S_n . Тогда

$$|C(\tau)| = |C(\varphi(\tau))|. \quad (*)$$

Но непосредственное вычисление показывает, что

$$|C(\tau)| = 2(n-2)!, \quad |C(\varphi(\tau))| = 2^k k!(n-2k)!.$$

Если $k > 1$, то из $(*)$ получаем, что

$$(n-2)(n-3)\dots(n-2k+1) = 2^{k-1}k!.$$

Если $k = 3$, то последнее равенство выполняется только при $n = 6$. Если $k > 3$, то левая часть рассматриваемого равенства не менее чем $(2k-2)!$ ($n \geq 2k$), $(2k-2)! > 2^{k-1}k!$. Следовательно, при $n \neq 6$ имеем $k = 1$, и $\varphi(\tau)$ — транспозиция. \square

Теорема 1.24.3 (Гёльдер). Пусть $n \neq 6$. Тогда $\text{Aut}(S_n) = \text{Inn}(S_n)$.

Доказательство. $S_1 = \{e\}$, S_2 — циклическая группа порядка 2. Для групп S_n , $n \geq 3$, $n \neq 6$, утверждение теоремы следует из лемм 1.24.2 и 1.24.1. \square

Замечание 1.24.4. Если $n \geq 3$, $n \neq 6$, то $Z(S_n) = e$ и $\text{Aut}(S_n) = \text{Inn}(S_n) = S_n$. Действительно, $Z(S_n) = e$ (см. ??), $\text{Inn}(S_n) \cong S_n/Z(S_n) \cong S_n$, и по теореме Гёльдера $\text{Aut}(S_n) \cong \text{Inn}(S_n) \cong S_n$.

Задача 1.24.5. Группа S_6 обладает внешними автоморфизмами.

Указание. В группе S_5 имеется шесть сопряжённых подгрупп H_i порядка 20. Одна из них:

$$H = \langle c = (1\ 2\ 3\ 4\ 5), d = (2\ 3\ 5\ 4) \rangle \triangleright \langle c \rangle,$$

$$dcd^{-1} = c^2, |H| = 20, |\langle c \rangle| = 5,$$

$$H = \{c^k d^l, 0 \leq k < 5, 0 \leq l < 4\} = \langle c \rangle \langle d \rangle.$$

На множестве $\{H_i, 1 \leq i \leq 6\}$ действует группа S_5 сопряжением. Это действие транзитивно (одна орбита). Ядро соответствующего гомоморфизма $S_5 \rightarrow S_6$ состоит из единичной подстановки в S_5 . Таким образом, группа S_6 содержит транзитивную подгруппу G , изоморфную группе S_5 .

Пусть $S_6/G = \{g_1G, \dots, g_6G\}$ — левые смежные классы группы S_6 по подгруппе G ($g_1 = e$). В группе G нет неединичных нормальных подгрупп группы S_6 , отображение $\varphi: S_6 \rightarrow S(S_6/G)$ из группы S_6 в группу подстановок на множестве S_6/G , заданное правилом

$$\varphi(\tau) = \begin{pmatrix} g_1G & \dots & g_6G \\ \tau(g_1)G & \dots & \tau(g_6)G \end{pmatrix} \text{ для } \tau \in S_6,$$

является изоморфизмом групп. Для $k = 1, \dots, 6$ положим $\tau(g_k)G = g_{i_k}G$. Тогда отображение

$$\begin{aligned}\psi: S(S_6/G) &\rightarrow S_6, \\ \psi\left(\begin{matrix} g_1G & \dots & g_6G \\ \tau(g_1)G & \dots & \tau(g_6)G \end{matrix}\right) &\mapsto \begin{pmatrix} 1 & \dots & 6 \\ i_1 & \dots & i_6 \end{pmatrix},\end{aligned}$$

также изоморфизм групп. Поэтому $\psi\varphi$ — автоморфизм группы S_6 . Покажите, что этот автоморфизм не является внутренним.

Упражнения 1.24.6 (трудные).

- 1) $(\text{Aut}(S_6) : \text{Inn}(S_6)) = 2$, $|\text{Aut}(S_6)| = 1440$.
- 2) $\text{Aut}(A_6) \cong \text{Aut}(S_6)$, $\text{Inn}(S_6) \cong S_6$.
- 3) Существует автоморфизм группы A_6 , непродолжаемый до автоморфизма группы S_6 .
- 4) Любой автоморфизм группы A_n при $n \neq 6$ индуцируется внутренним автоморфизмом группы S_n .

Упражнение 1.24.7. Пусть $G = \langle(1\ 2), (1\ 3\ 5)(2\ 4\ 6)\rangle \subset S_6$, $H = \langle(1\ 2), (3\ 4), (5\ 6)\rangle \subset G$. Покажите, что H — нормальная подгруппа группы G и в то же время $|\text{Aut}(H)| > |\text{Aut}(G)|$.

Замечание 1.24.8 (Бэр, Алперин).

- 1) Если G — группа с конечным числом эндоморфизмов, $|\text{End}(G)| < \infty$, то G — конечная группа.
- 2) Если G — периодическая группа с конечным числом автоморфизмов, $|\text{Aut}(G)| < \infty$, то G — конечная группа.
- 3) Если G — конечно порождённая группа, то $|\text{Aut}(G)| < \infty$ тогда и только тогда, когда группа G обладает циклической подгруппой конечного индекса, лежащей в центре.

1.25. Полупрямые произведения

Весьма полезной оказывается также конструкция, несколько более общая, чем рассмотренная конструкция прямого произведения.

Группа G называется *внутренним полупрямым произведением* нормальной подгруппы $N \triangleleft G$ и подгруппы $H \subset G$ (не предполагается, что $H \triangleleft G$), если $G = NH$ и $N \cap H = e$ (обозначение: $G = N \times H$).

Примеры 1.25.1 (полупрямых произведений).

- 1) $G = A_4 = V \times \langle(1\ 2\ 3)\rangle$, здесь: $|A_4| = 12$, $N = V \triangleleft A_4$ — нормальная подгруппа Клейна, $|V| = 4$; $H = \langle(1\ 2\ 3)\rangle$ — циклическая подгруппа, порождённая 3-циклом $(1\ 2\ 3)$, $|H| = 3$, H не является нормальной подгруппой в A_4 . Действительно: $V \cap \langle(1\ 2\ 3)\rangle = e$; $|V \cdot H| = |V| \cdot |H| = 12$, и поэтому $A_4 = V \cdot H$. \square
- 2) $S_4 = V \times S_3$.

3) Пусть K — поле. Тогда $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes H$, где $\mathrm{SL}_n(K) \triangleleft \mathrm{GL}_n(K)$,

$$H = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \mid 0 \neq \lambda \in K \right\} -$$

подгруппа в $\mathrm{GL}_n(K)$, при этом H не является нормальной подгруппой. Действительно:

a) если $A \in \mathrm{GL}_n(K)$, $|A| \neq 0$, то

$$A = \left(A \cdot \begin{pmatrix} |A|^{-1} & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \right) \cdot \begin{pmatrix} |A| & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} |A|^{-1} & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} = |A| |A|^{-1} = 1,$$

$$A \cdot \begin{pmatrix} |A|^{-1} & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_n(K), \quad \begin{pmatrix} |A| & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \in H,$$

и поэтому $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \cdot H$.

б) Если $B \in \mathrm{SL}_n(K) \cap H$, то $|B| = 1$,

$$B = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad \lambda = |B| = 1,$$

и следовательно, $B = E$. Поэтому $\mathrm{SL}_n(K) \cap H = E$. □

Теорема 1.25.2 (о строении внутреннего полупрямого произведения). Пусть G — группа, $N \triangleleft G$, H — подгруппа группы G , $G = N \rtimes H$ ($G = NH$, $N \cap H = e$). Тогда:

- 1) если $g = nh = n'h' \in G$, $n, n' \in N$, $h, h' \in H$, то $n = n'$, $h = h'$;
- 2) $G/N \cong H$ (другими словами, группа G является расширением группы N с помощью группы H , $e \rightarrow N \rightarrow G \rightarrow G/N = H \rightarrow e$);
- 3) для любого элемента $h \in H$ отображение

$$\theta(h): N \rightarrow N, \quad \theta(h)(n) = hn h^{-1} \text{ для } n \in N,$$

является автоморфизмом группы N ,

$$\theta(h) \in \mathrm{Aut}(N);$$

4) отображение

$$\theta: H \rightarrow \text{Aut}(N), \quad h \mapsto \theta(h),$$

является гомоморфизмом групп;

5) в группе $G = N \times H = NH$ имеем:

$$(n_1 h_1)(n_2 h_2) = (n_1 \theta(h_1)(n_2))(h_1 h_2)$$

для всех $n_1, n_2 \in N, h_1, h_2 \in H$.

Доказательство.

1) Если $g = nh = n'h' \in G = NH, n, n' \in N, h, h' \in H$, то $(n')^{-1}n = h'h^{-1} \in N \cap H = e$, и поэтому $(n')^{-1}n = e = h'h^{-1}$, и следовательно, $n = n', h = h'$.

2) $G/N = NH/N \cong H/(N \cap H) = H/\{e\} = H$.

3) Нормальная подгруппа N остается инвариантной, $\varphi(N) = N$, при внутреннем автоморфизме $\varphi: G \rightarrow G, \varphi(x) = h x h^{-1}$; отображение $\theta(h)$ является его ограничением на N , $\theta(h) = \varphi|_N$, и поэтому $\theta(h) \in \text{Aut}(N)$.

4) Если $n \in N, h_1, h_2 \in H$, то

$$\theta(h_1 h_2)(n) = (h_1 h_2)n(h_1 h_2)^{-1} = h_1(h_2 n h_2^{-1})h_1^{-1} = \theta(h_1)(\theta(h_2)(n)) = (\theta(h_1)\theta(h_2))(n),$$

и поэтому $\theta(h_1 h_2) = \theta(h_1)\theta(h_2)$.

5) Если $n_1, n_2 \in N, h_1, h_2 \in H$, то

$$(n_1 h_1)(n_2 h_2) = (n_1(h_1 n_2 h_2^{-1}))(h_1 h_2) = (n_1 \theta(h_1)(n_2))(h_1 h_2). \quad \square$$

Внешнее полупрямое произведение групп

Доказанная теорема подсказывает конструкцию *внешнего полупрямого произведения групп*.

Теорема 1.25.3. Пусть N и H — две группы, $\theta: H \rightarrow \text{Aut}(N)$ — фиксированный гомоморфизм. Рассмотрим множество

$$G = \{(n, h) \mid n \in N, h \in H\} = N \times H.$$

Определим на G операцию произведения, полагая

$$(n_1, h_1)(n_2, h_2) = (n_1 \theta(h_1)(n_2), h_1 h_2).$$

Тогда:

1) множество G с данной операцией является группой (с нейтральным элементом (e_N, e_H) и обратным элементом $(n, h)^{-1} = (\theta(h^{-1})(n^{-1}), h^{-1})$);

2) если

$$\begin{aligned} \bar{N} &= \{(n, e_H) \mid n \in N\}, \\ \bar{H} &= \{(e_N, h) \mid h \in H\}, \end{aligned}$$

то:

- a) $\bar{N} \triangleleft G$, $N \cong \bar{N}$ (при $n \mapsto (n, e_H)$); \bar{H} — подгруппа в G , $H \cong \bar{H}$ (при $h \mapsto (e_N, h)$);
 б) $G = \bar{N}\bar{H}$, $\bar{N} \cap \bar{H} = (e_N, e_H)$ (таким образом, $G = \bar{N} \times \bar{H}$ — внутренне полупрямое произведение своих нормальной подгруппы \bar{N} и подгруппы \bar{H});
 в) если гомоморфизм $\bar{\theta}: \bar{H} \rightarrow \text{Aut}(\bar{N})$ определён внутренним полупрямым произведением $G = \bar{N} \times \bar{H}$, $G = \bar{N}\bar{H}$, $\bar{N} \cap \bar{H} = (e_N, e_H)$ (в силу теоремы о строении внутреннего полупрямого произведения), то $\bar{\theta}$ согласован с исходным гомоморфизмом $\theta: H \rightarrow \text{Aut}(N)$:

$$\bar{\theta}((e_N, h))((n, e_H)) = (\theta(h)(n), e_H)$$

для всех $n \in N$, $h \in H$.

Доказательство.

1) Проверим, что выполнены групповые аксиомы для G

a) *Ассоциативность операции.* Если $n_1, n_2, n_3 \in N$, $h_1, h_2, h_3 \in H$, то

$$\begin{aligned} ((n_1, h_1)(n_2, h_2)(n_3, h_3)) &= (n_1\theta(h_1)(n_2), h_1h_2)(n_3, h_3) = \\ &= (n_1\theta(h_1)(n_2)\theta(h_1h_2)(n_3), (h_1h_2)h_3) = \\ &= (n_1\theta(h_1)(n_2)\theta(h_1)(\theta(h_2)(n_3)), h_1(h_2h_3)) = \\ &= (n_1\theta(h_1)(n_2\theta(h_2)(n_3)), h_1(h_2h_3)) = \\ &= (n_1, h_1)(n_2\theta(h_2)(n_3), h_2h_3) = (n_1, h_1)((n_2, h_2)(n_3, h_3)). \end{aligned}$$

б) *Наличие нейтрального элемента.* Для всех $n \in N$, $h \in H$ имеем

$$\begin{aligned} (n, h)(e_N, e_H) &= (n\theta(h)(e_N), h \cdot e_H) = (n \cdot e_N, h) = (n, h) = \\ &= (1_N(n), h) = (e_N\theta(e_H)(n), e_Hh) = (e_N, e_H)(n, h), \end{aligned}$$

поэтому (e_N, e_H) — нейтральный элемент в G .

в) *Наличие обратного элемента.* Для $n \in N$, $h \in H$ имеем

$$\begin{aligned} (n, h)(\theta(h^{-1})(n^{-1}), h^{-1}) &= (n\theta(h)(\theta(h^{-1})(n^{-1})), hh^{-1}) = \\ &= (n\theta(e_N)(n^{-1}), e_H) = (n1_N(n^{-1}), e_H) = (nn^{-1}, e_H) = (e_N, e_H) = \\ &= (\theta(h^{-1})(e_N), e_H) = (\theta(h^{-1})(n^{-1}n), e_H) = \\ &= (\theta(h^{-1})(n^{-1})\theta(h^{-1})(n), h^{-1}h) = (\theta(h^{-1})(n^{-1}), h^{-1})(n, h). \end{aligned}$$

Итак,

$$(n, h)^{-1} = (\theta(h^{-1})(n^{-1}), h^{-1}).$$

2) а) Для $n, n_1, n_2 \in N$, $h, h_1, h_2 \in H$ имеем

$$\begin{aligned} (n_1, e_H)(n_2, e_H) &= (n_1\theta(e_H)(n_2), e_H) = (n_11_N(n_2), e_H) = (n_1n_2, e_H); \\ (n, e_H)^{-1} &= (\theta(e_H)(n^{-1}), e_H) = (1_N(n^{-1}), e_H) = (n^{-1}, e_H); \\ (e_N, h_1)(e_N, h_2) &= (e_N\theta(h_1)(e_N), h_1h_2) = (e_N, h_1h_2); \\ (e_N, h)^{-1} &= (\theta(h^{-1})(e_N), h^{-1}) = (e_N, h^{-1}). \end{aligned}$$

Итак, \bar{N} и \bar{H} — подгруппы группы G , $N \cong \bar{N}$ (при отображении $n \mapsto (n, e_H)$), $H \cong \bar{H}$ (при отображении $h \mapsto (e_N, h)$). Кроме того,

$$(n, h)(n_1, e_H)(n, h)^{-1} = (n\theta(h)(n_1), h)(\theta(h^{-1})(n^{-1}), h^{-1}) =$$

$$\begin{aligned}
 &= (n\theta(h)(n_1)\theta(h)(\theta(h^{-1})(n^{-1})), e_H) = (n\theta(h)(n_1)\theta(e_H)(n^{-1}), e) = \\
 &= (n\theta(h)(n_1)1_N(n^{-1}), e_H) = (n\theta(h)(n_1)n^{-1}, e_H) \in \bar{N}.
 \end{aligned}$$

Таким образом, $\bar{N} \triangleleft G$.

б) Так как

$$(n, h) = (ne_N, h) = (n1_N(e_N), h) = (n\theta(e_H)(e_N), h) = (n, e_H)(e_N, h),$$

то $G = \bar{N}\bar{H}$.

Если $(n, e_H) = (e_N, h) \in \bar{N} \cap \bar{H}$, то $n = e_N$, $h = e_H$, и поэтому $\bar{N} \cap \bar{H} = (e_N, e_H)$. Таким образом, $G = \bar{N} \times \bar{H}$ для нормальной подгруппы \bar{N} и подгруппы \bar{H} .

в) В силу определения,

$$\bar{\theta}: \bar{H} \rightarrow \text{Aut}(\bar{N})$$

(по теореме 1.25.2, п. 4), имеем

$$\bar{\theta}((e_N, h))(n, e_H) = (e_N, h)(n, e_H)(e_N, h)^{-1} = (e_N\theta(h)(n)e_N^{-1}, e_H) = (\theta(h)(n), e_H). \quad \square$$

Замечание 1.25.4. Если $G = N \times H$, $G = NH$, $N \cap H = e$ и

$$\theta: H \rightarrow \text{Aut}(N)$$

ассоциированный гомоморфизм (теорема 1.25.2, $\theta(h)(n) = hnh^{-1}$ для $n \in N$, $h \in H$), то условие $nh = hn$ для всех $n \in N$, $h \in H$ равносильно тому, что $\theta(h)(n) = hnh^{-1} = n$, т. е. $\theta(h) = 1_N$ для всех $h \in H$. В этом случае мы получаем рассмотренную ранее конструкцию прямого произведения $G = N \times H$.

Пример 1.25.5. Пусть $N = \langle n \rangle$, $O(n) = 3$, $H = \langle h \rangle$, $O(h) = 4$,

$$\theta: H = \langle h \rangle \rightarrow \text{Aut}(\langle n \rangle) \cong \mathbb{Z}_2, \quad \theta(h)(n) = n^{-1}.$$

Тогда группа $G = \underset{\theta}{N} \times H$ называется *дициклической группой* порядка $|N \times H| = |N| \cdot |H| = 3 \cdot 4 = 12$. Отметим, что $G \not\cong A_4$, $G \not\cong \text{Dih}(12)$, поскольку $h \in G$, $O(h) = 4$.

1.26. Характеристические и A -инвариантные подгруппы для $A \subseteq \text{Aut } G$

Пусть H — подгруппа группы G и A — непустое подмножество группы автоморфизмов $\text{Aut}(G)$, $\emptyset \neq A \subseteq \text{Aut}(G)$. Будем говорить, что подгруппа H является *A -инвариантной подгруппой группы G* , если

$$\alpha(H) \subseteq H \quad \forall \alpha \in A \subseteq \text{Aut}(G), \quad h \in H.$$

Примеры 1.26.1.

- 1) Если $A = \{1_G\} \subseteq \text{Aut}(G)$, то каждая подгруппа H группы G является A -инвариантной.
- 2) Если $A = \text{Aut}(G)$, то $\text{Aut}(G)$ -инвариантная подгруппа H группы G называется *характеристической подгруппой* группы G .

- 3) Если $A = \text{Inn}(G) \subseteq \text{Aut}(G)$ — подгруппа всех внутренних автоморфизмов группы $\text{Aut}(G)$, то $\text{Inn}(G)$ -инвариантные подгруппы группы G — это в точности нормальные подгруппы группы G .
- 4) Если $\emptyset \subset A \subseteq \text{Aut}(G)$ и $\{H_i \mid i \in I\}$ — любое семейство A -инвариантных подгрупп группы G , то $\bigcap_{i \in I} H_i$ — A -инвариантная подгруппа.
- 5) Если G — конечная группа, $|G| = n = mq$, при этом в группе G содержится и только одна подгруппа H из m элементов, то H — характеристическая подгруппа.
- 6) Если $G = H \times K$, то $H' = H \times e_H \triangleleft G$, $K' = e_H \times K \triangleleft G$, но H' и K' не обязаны быть характеристическими подгруппами. Например, для любой нетривиальной группы $H \neq \{e_H\}$ при $K = H$ для группы $G = H \times H$ отображение

$$\alpha: G \rightarrow G, \quad \alpha((h_1, h_2)) = (h_2, h_1), \quad h_1, h_2 \in H,$$

является автоморфизмом группы G . Но:

$$\alpha(H \times e_H) = e_H \times H \neq H \times e_H; \quad \alpha(e_H \times H) = H \times e_H \neq e_H \times H.$$

Итак, $H' = H \times e_H$ и $H'' = e_H \times H$ — нормальные подгруппы, но не являются характеристическими.

Лемма 1.26.2. Если $H \triangleleft G$ и K — характеристическая подгруппа в H , то $K \triangleleft G$.

Доказательство. Если $g \in G$, то $g^{-1}Hg = H$. Таким образом, внутренний автоморфизм $\tau_g: x \mapsto g^{-1}xg$ группы G отображает группу H на себя. Следовательно, отображение

$$\tau_g|_H: H \rightarrow H, \quad h \mapsto g^{-1}hg,$$

является автоморфизмом группы H . В силу характеристичности подгруппы K в H

$$g^{-1}Hg = \tau_g|_H(K) \subseteq H$$

для всех $g \in G$. Итак, $K \triangleleft G$. □

Некоторым усилением предыдущей леммы 1.26.2 является следующее утверждение.

Лемма 1.26.3. Пусть G — группа, K, H — её подгруппы, $K \subseteq H \subseteq G$, $\emptyset \subset A \subseteq \text{Aut}(G)$. Если H — A -инвариантная подгруппа группы G , K — характеристическая подгруппа в H , то K — A -инвариантная подгруппа в G . В частности, если K — характеристическая подгруппа в H и H — характеристическая подгруппа в G , то K — характеристическая подгруппа в G (следует сравнить это с тем, что свойство отношения нормальности подгруппы не является транзитивным, см. ??).

Доказательство.

1) Если $\alpha \in A \subseteq \text{Aut}(G)$, то $\alpha(H) \subseteq H$ (H — A -инвариантная подгруппа). □

1.27. Прямые пределы групп

Пусть Λ — *направленное* частично упорядоченное множество (это означает, что для любых $\lambda, \mu \in \Lambda$ существует $\nu \in \Lambda$, для которого $\lambda \leq \nu, \mu \leq \nu$). Допустим, что имеем семейство групп $\{G_\lambda \mid \lambda \in \Lambda\}$ и совокупность гомоморфизмов $\alpha_\lambda^\mu: G_\lambda \rightarrow G_\mu$ для всех $\lambda \leq \mu$, при этом выполнены следующие условия:

- 1) $\alpha_\lambda^\lambda = 1_{G_\lambda}$ — тождественное отображение на G_λ ;
- 2) $\alpha_\mu^\lambda \alpha_\lambda^\mu = \alpha_\mu^\mu$ для всех $\lambda \leq \mu \leq \nu$.

Система

$$D = \{G_\lambda; \alpha_\lambda^\mu \mid \lambda \leq \mu \in \Lambda\}$$

называется *прямой системой* групп. Мы предполагаем, что $G_\lambda \cap G_\mu = \emptyset$ для всех $\lambda \neq \mu$ (это ограничение легко достигается).

Постройм группу

$$D = \lim_{\lambda \in \Lambda} G_\lambda$$

и гомоморфизмы $\theta_\lambda: G_\lambda \rightarrow D$ (*прямой предел* $\{D_\lambda, \theta_\lambda \mid \lambda \in \Lambda\}$ прямой системы D).

Основное соображение — отождествить элемент $g_\lambda \in G_\lambda$ со всеми его образами $\alpha_\lambda^\mu(g_\lambda)$, $\lambda \leq \mu$.

Рассмотрим на теоретико-множественном объединении групп

$$U = \bigcup_{\lambda \in \Lambda} G_\lambda$$

следующее отношение эквивалентности:

$$g_\lambda \sim \bar{g}_\mu, \quad \lambda, \mu \in \Lambda \iff \alpha_\lambda^\nu(g_\lambda) = \alpha_\mu^\nu(\bar{g}_\mu) \text{ для некоторого } \nu \geq \lambda, \mu.$$

Замечание 1.27.1. Если $\rho \geq \nu$, то

$$\alpha_\lambda^\rho(g_\lambda) = \alpha_\nu^\rho \alpha_\lambda^\nu(g_\lambda) = \alpha_\nu^\rho \alpha_\mu^\nu(\bar{g}_\mu) = \alpha_\mu^\rho(\bar{g}_\mu).$$

Действительно, это отношение — отношение эквивалентности:

- i) $g_\lambda = 1_{G_\lambda}(g_\lambda) = \alpha_\lambda^\lambda(g_\lambda)$, поэтому $g_\lambda \sim g_\lambda$;
- ii) если $g_\lambda \sim \bar{g}_\mu$, то $\alpha_\lambda^\nu(g_\lambda) = \alpha_\mu^\nu(\bar{g}_\mu)$, и поэтому $\alpha_\mu^\sigma(\bar{g}_\mu) = \alpha_\lambda^\sigma(g_\lambda)$ для $\nu \geq \lambda, \mu$, таким образом, $\bar{g}_\mu \sim g_\lambda$;
- iii) если $g_\lambda \sim \bar{g}_\mu, \bar{g}_\mu \sim \bar{g}_\gamma$, то $\alpha_\lambda^\nu = \alpha_\mu^\nu(\bar{g}_\mu)$ для $\nu \geq \lambda, \mu, \alpha_\mu^\sigma(\bar{g}_\mu) = \alpha_\gamma^\sigma(\bar{g}_\gamma)$ для $\sigma \geq \mu, \gamma$, в силу замечания для $\rho \geq \nu, \sigma$ (и поэтому $\rho \geq \mu, \gamma$) $\alpha_\lambda^\rho(g_\lambda) = \alpha_\mu^\rho(\bar{g}_\mu) = \alpha_\gamma^\rho(\bar{g}_\gamma)$, таким образом, $g_\lambda \sim \bar{g}_\gamma$.

Через $[g_\lambda]$ обозначим класс эквивалентных элементов, содержащий элемент g_λ , пусть

$$D = U/\sim = \left\{ [g_\lambda] \mid g_\lambda \in U = \bigcup_{\lambda \in \Lambda} G_\lambda \right\}.$$

Определим на D групповую операцию на классах, корректно используя их представители.

Пусть

$$g_\lambda \sim \bar{g}_\lambda \text{ и } g_\mu \sim \bar{g}_\mu.$$

Найдём индекс $\nu \in \Lambda$, для которого $\nu \geqslant \lambda, \bar{\lambda}, \mu, \bar{\mu}$, а также

$$\alpha_\lambda^\nu(g_\lambda) = \alpha_{\bar{\lambda}}^\nu(\bar{g}_{\bar{\lambda}}), \quad \alpha_\mu^\nu(g_\mu) = \alpha_{\bar{\mu}}^\nu(\bar{g}_{\bar{\mu}}),$$

поэтому

$$\alpha_\lambda^\nu(g_\lambda)\alpha_\mu^\nu(g_\mu) = \alpha_{\bar{\lambda}}^\nu(\bar{g}_{\bar{\lambda}})\alpha_{\bar{\mu}}^\nu(\bar{g}_{\bar{\mu}}).$$

Это позволяет корректно определить

$$[g_\lambda][g_\mu] = [\alpha_\lambda^\nu(g_\lambda)\alpha_\mu^\nu(g_\mu)],$$

где $\nu \geqslant \lambda, \mu$ (как мы уже видели, это определение не зависит от ν).

Проверка аксиом группы:

- i) $([g_\lambda][g_\mu])[g_\gamma] = [(\alpha_\lambda^\nu(g_\lambda)\alpha_\mu^\nu(g_\mu))\alpha_\gamma^\nu(g_\gamma)] = [\alpha_\lambda^\nu(g_\lambda)(\alpha_\mu^\nu(g_\mu)\alpha_\gamma^\nu(g_\gamma))] = [g_\lambda]([g_\mu][g_\gamma])$ (ассоциативность произведения);
- ii) $e_D = [e_{G_\lambda}]$ — нейтральный элемент;
- iii) $[g_\lambda]^{-1} = [g_\lambda^{\pm 1}]$ — обратный элемент.

Отображение

$$\theta_\lambda: G_\lambda \rightarrow D, \quad g_\lambda \mapsto [g_\lambda],$$

является гомоморфизмом групп, поскольку

$$\theta_\lambda(g_\lambda \bar{g}_\lambda) = [\bar{g}_\lambda \bar{g}_\lambda] = [\alpha_\lambda^\lambda(\bar{g}_\lambda)\alpha_\lambda^\lambda(\bar{g}_\lambda)] = [g_\lambda][\bar{g}_\lambda] = \theta_\lambda(g_\lambda)\theta_\lambda(\bar{g}_\lambda)$$

для всех $g_\lambda, \bar{g}_\lambda \in G_\lambda$.

Отметим основные свойства прямого предела.

Предложение 1.27.2. Пусть $\tilde{G}_\lambda = \text{Im}(\theta_\lambda)$, где $\theta_\lambda: G_\lambda \rightarrow D$, $\lambda \in \Lambda$, — построенный гомоморфизм групп.

- 1) $D = \bigcup_{\lambda \in \Lambda} \tilde{G}_\lambda$;
- 2) \tilde{G}_λ — подгруппа в \tilde{G}_μ при $\lambda \leqslant \mu$;
- 3) если все гомоморфизмы α_λ^μ инъективны, то все гомоморфизмы $\theta_\lambda: G_\lambda \rightarrow D$, $\lambda \in \Lambda$, также инъективны, $G_\lambda \cong \tilde{G}_\lambda$.

Доказательство.

- 1) Если $d \in D$, то $d = [g_\lambda] = \theta_\lambda(g_\lambda)$, $g_\lambda \in G_\lambda$.
- 2) Так как $[g_\lambda] = [\alpha_\lambda^\mu(g_\lambda)] \in \tilde{G}_\mu$, то $\tilde{G}_\lambda \subseteq \tilde{G}_\mu$ для $\lambda \leqslant \mu$.
- 3) Если $[g_\lambda] = \theta(g_\lambda) = e_D = [e_\lambda]$, то $\alpha_\lambda^\mu(g_\lambda) = \alpha_\lambda^\mu(e_\lambda) = e_\mu$ для некоторого $\mu \geqslant \lambda$.

Следовательно, $g_\lambda = e_\lambda$. \square

Таким образом, в предложении, п. 3, прямая система групп реализуется системой подгрупп. Важный частный случай: направленное частично упорядоченное множество Λ — цепь (т. е. для любых $i, j \in \Lambda$ либо $i \leqslant j$, либо $j \leqslant i$).

Пусть дана цепь групп G_1, G_2, \dots и инъективных гомоморфизмов $\sigma_i: G_i \rightarrow G_{i+1}$. Рассмотрим

$$\alpha_i^j = \sigma_i \sigma_{i+1} \dots \sigma_{j-1}$$

14-59

для $i < j$. Таким образом получаем направленную систему $\{G_i, \alpha_i^j \mid i \in \mathbb{N}\}$. Группа прямого предела

$$D = \varinjlim_{i \in \mathbb{N}} G_i$$

является объединением цепи подгрупп $\tilde{G}_1 \subseteq \tilde{G}_2 \subseteq \dots$, $\tilde{G}_i \cong G_i$, $D = \bigcup_{i \in \mathbb{N}} \tilde{G}_i$. Это позволяет строго говорить об объединении возрастающей цепи вложенных групп.

Примеры 1.27.3.

- 1) Пусть $G_i = \langle a_i \rangle$, $i \in \mathbb{N}$, — совокупность циклических групп, $|G_i| = O(a_i) = p^i$, где p — простое число,

$$\sigma_i: G_i = \langle a_i \rangle \rightarrow G_{i+1} = \langle a_{i+1} \rangle, \quad \sigma_i(a_i) = a_{i+1}^p.$$

Предел этой прямой системы циклических p -групп порядков p, p^2, \dots является их объединением. Эта бесконечная абелева p -группа называется *профлеровой группой типа p^∞* (одна из её прозрачных реализаций: группа всех комплексных корней степени p^i , $i \in \mathbb{N}$, как объединение вложенных друг в друга циклических групп корней степени p^i из 1). Эта абелева группа занимает достойное место в структурной теории абелевых групп.

- 2) Абелева группа рациональных чисел $\mathbb{Q} = (\mathbb{Q}, +)$ является прямым пределом бесконечных циклических групп.

Конец лекции № 14

15-1

Лекция №15

(28 октября 2011 г.)

Глава 1

Кольца

1.1. Кольца

Множество R с двумя бинарными операциями (сложением $+$ и умножением \cdot) называется ассоциативным кольцом с единицей, если:

- (1) относительно сложения $(R, +)$ — абелёва (т. е. коммутативная) группа;
- (2) умножение — ассоциативная операция, и существует нейтральный элемент 1 (т. е. $1 \cdot r = r = r \cdot 1$ для всех $r \in R$), называемый единицей;
- (3) сложение и умножение связаны законами дистрибутивности

$$(a + b)c = ac + bc, \quad c(a + b) = ca + cb$$

для всех $a, b, c \in R$.

Если операция умножения коммутативна, то кольцо $(R, +, \cdot)$ называется коммутативным кольцом. Коммутативные кольца являются одним из главных объектов изучения в коммутативной алгебре и алгебраической геометрии.

Замечания 1.1.1.

- ✓ 1) Исследуются и неассоциативные кольца. Например, если вместо ассоциативности 2) умножение удовлетворяет *тождеству Якоби*

$$a(bc) + b(ca) + c(ab) = 0$$

для всех $a, b, c \in R$ и

$$ab = -ba$$

для всех $a, b \in R$, то такое кольцо называется кольцом Ли.

- ✓ 2) Рассматриваются также и ассоциативные кольца без единицы. Например, чётные числа $R = 2\mathbb{Z}$ являются ассоциативным коммутативным кольцом без единицы.

Примеры ассоциативных колец

- 1) Кольцо $(\mathbb{Z}, +, \cdot)$ целых чисел; поля \mathbb{Q} , \mathbb{R} , \mathbb{C} , \mathbb{Z}_p
- 2) Кольцо непрерывных вещественных функций $C[0, 1]$ на отрезке $[0, 1]$ (для $f, g \in C[0, 1]$, $x \in [0, 1]$: $(f + g)(x) = f(x) + g(x)$, $(fg)(x) = f(x)g(x)$).
- 3) Кольцо многочленов $\mathbb{R}[x]$ с действительными коэффициентами.
- 4) Кольцо вычетов $(\mathbb{Z}_n, +, \cdot)$ по модулю n .

Мы уже убедились, что группа вычетов

$$(\mathbb{Z}_n, +) = \{C_0, C_1, \dots, C_{n-1}\}, \quad C_k = k + n\mathbb{Z},$$

по модулю n с операцией сложения

$$C_k + C_l = C_{k+l} = C_r, \quad \text{где } k+l = nq+r, \quad 0 \leq r \leq n-1,$$

является коммутативной группой (при этом, читайтесь!)

Определим операцию умножения, полагая

$$C_k \cdot C_l = C_{kl} = C_s, \quad \text{где } kl = n\tilde{q} + s, \quad 0 \leq s \leq n-1.$$

Проверим корректность этой операции. Если $C_k = C_{k'}$, $C_l = C_{l'}$, то $k' = k + nv$, $l' = l + nv$, $k' \cdot l' = kl + n(kv + ul + nuv)$, и поэтому $C_{k'l'} = C_{kl}$.

Так как

$$\begin{aligned} (C_k C_l) C_m &= C_{(kl)m} = C_{k(lm)} = C_k (C_l C_m), \\ C_k C_l &= C_{kl} = C_{lk} = C_l C_k, \\ C_1 C_k &= C_k = C_k C_1, \\ (C_k + C_l) C_m &= C_{(k+l)m} = C_{km+lm} = C_k C_m = C_l C_m, \end{aligned}$$

то $(\mathbb{Z}_n, +, \cdot)$ является ассоциативным коммутативным кольцом с единицей C_1 (называемым кольцом вычетов по модулю n).

Свойства колец $(R, +, \cdot)$

1. Так как $(R, +)$ — абелева группа, то: существует, и единственный, нейтральный элемент относительно сложения 0; для любого $a \in R$ существует, и единственный, противоположный элемент $-a$ (т. е. $a + (-a) = 0$); уравнение $x + b = a$ имеет, и единственное, решение $x = a - b = a + (-b)$.
2. Справедлив обобщённый закон ассоциативности для умножения, т. е. результат произведения для n сомножителей не зависит от расстановки скобок; единичный элемент 1 — единственный нейтральный элемент.
3. Проводя индукцию по n , убеждаемся в том, что

$$\begin{aligned} (a_1 + \dots + a_n)b &= a_1b + \dots + a_nb; \\ b(a_1 + \dots + a_n) &= ba_1 + \dots + ba_n. \end{aligned}$$

4. Так как $a0 = a(0 + 0) = a0 + a0$, то $a0 = 0$. Аналогично, $0a = 0$.
5. Так как $ab + (-a)b = (a + (-a))b = 0b = 0$, то $(-a)b = -ab$. Аналогично, $a(-b) = -ab$. Поэтому $(-a)(-b) = -(-a(-b)) = -(-ab) = ab$.
6. $(a-b)c = (a + (-b))c = ac + (-b)c = ac - bc$, $c(a-b) = c(a + (-b)) = ca + c(-b) = ca - cb$, т. е. дистрибутивность для разности.

Задача 11 Лемма 1.1.2. Пусть R — кольцо с 1, $n \in \mathbb{N}$, $a, b, a_1, a_2, \dots, a_s \in R$. Тогда:

- 1) если $ab = ba$, то

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

- 2) если $a_i a_j = a_j a_i$ для всех i, j , то

$$(a_1 + a_2 + \dots + a_s)^n = \sum \frac{n!}{(i_1!) \dots (i_s!)} a_1^{i_1} \dots a_s^{i_s},$$

где суммирование происходит по всем s -строчкам (i_1, i_2, \dots, i_s) таким, что $i_1 + i_2 + \dots + i_s = n$.

Доказательство.

- 1) Индукция по n с учётом равенства $C_n^k + C_n^{k-1} = C_{n+1}^{k+1}$ для $k < n$ и применением перестановочности элементов a и b и закона дистрибутивности.
- 2) Индукция по s ; $s = 2$ — пункт 1); если утверждение верно для s , то по 1):

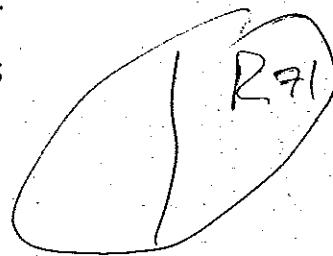
$$\begin{aligned} (a_1 + \dots + a_s + a_{s+1})^n &= ((a_1 + \dots + a_s) + a_{s+1})^n = \\ &= \sum_{k=0}^n C_n^k (a_1 + \dots + a_s)^k a_{s+1}^{n-k} = \sum_{k+j=n} \frac{n!}{k! j!} (a_1 + \dots + a_s)^k a_{s+1}^j = \\ &= \sum_{k+j=n} \frac{n!}{k! j!} \sum_{\substack{(i_1, \dots, i_s) \\ i_1 + \dots + i_s = k}} \frac{k!}{(i_1!) \dots (i_s!)} a_1^{i_1} a_2^{i_2} \dots a_s^{i_s} a_{s+1}^j = \\ &= \sum_{\substack{(i_1, \dots, i_{s+1}) \\ i_1 + \dots + i_{s+1} = n}} \frac{n!}{(i_1!) \dots (i_{s+1}!)} a_1^{i_1} a_2^{i_2} \dots a_{s+1}^{i_{s+1}} \quad (j = i_{s+1}). \end{aligned}$$

□

1.2. Подкольца

Подмножество S кольца R называется подкольцом, если:

- (a) S — подгруппа относительно сложения в группе $(R, +)$;
- (б) для $a, b \in S$ имеем $ab \in S$;
- (в) для кольца R с 1 предполагается, что $1 \in S$.



Задача 12 $R \oplus \mathbb{Z} \xrightarrow{r \mapsto (r, 0)}$
 $(r, n) \quad 0, 1$

Примеры подкольца

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{Z}_n, M_n(\mathbb{K})$$

Задача 1.2.1. Описать все подкольца в кольце вычетов \mathbb{Z}_n по модулю n .

Замечание 1.2.2. В кольце \mathbb{Z}_{10} элементы, кратные 5, образуют кольцо с 1, не являющееся подкольцом в \mathbb{Z}_{10} (у этих колец различные единичные элементы).

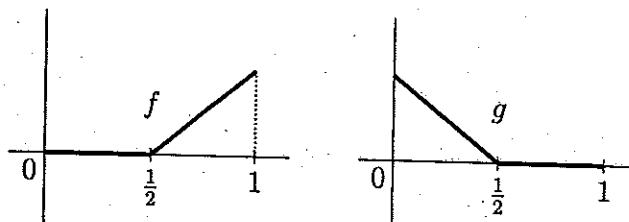
1.3. Делители нуля в кольцах

Определение 1.3.1. Если R — кольцо, $a, b \in R$ и $a \neq 0, b \neq 0, ab = 0$, то элемент a называется *левым делителем нуля* в R , элемент b называется *правым делителем нуля* в R .

Замечание 1.3.2. В коммутативных кольцах, естественно, нет различий между левыми и правыми делителями нуля.

Пример 1.3.3. В $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ нет делителей нуля.

Пример 1.3.4. Кольцо непрерывных функций $C[0, 1]$ имеет делители нуля. Действительно, если



то $f \neq 0, g \neq 0, fg = 0$.

Пример 1.3.5. Если $n = kl$, $1 < k, l < n$, то $C_k \neq C_0, C_l \neq C_0$, но $C_k C_l = C_0$, т. е. кольцо вычетов \mathbb{Z}_n по составному числу n имеет делители нуля.

Упражнение 1.3.6. Квадратная ненулевая матрица $0 \neq A \in M_n(\mathbb{R})$ является левым (правым) делителем нуля тогда и только тогда, когда $|A| = 0$.

Доказательство. 1) Пусть $0 \neq A$ — левый делитель нуля, т. е. $AX = 0$, где $X \neq 0$. Допустим, что $|A| \neq 0$. Тогда существует обратная матрица A^{-1} . Но $X = A^{-1}AX = A^{-1}0 = 0$. Противоречие.

2) Пусть $0 \neq A$ и $|A| = 0$. Найдём матрицу $0 \neq X = (x_{ij})$ такую, что $AX = 0$, т. е.

$$X = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} x_{11} \\ \vdots \\ x_{ni} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

для любого i -го столбца матрицы X . Поскольку определитель $|A|$ этой квадратной системы равен нулю, то имеется ненулевое решение, т. е. существует ненулевая матрица $X = (x_{ij})$ такая, что $AX = 0$. \square



Задача 1.3.7. Докажите, что однородная система из n линейных уравнений от n неизвестных $AX = (0)$, где

$$A \in M_n(R), \quad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad (0) \in \hat{R}_n,$$

над коммутативным кольцом R имеет ненулевое решение тогда и только тогда, когда определитель $|A|$ матрицы A — делитель нуля в кольце R .

Лемма 1.3.8. Если в кольце R нет (левых) делителей нуля, то из $ab = ac$, где $0 \neq a \in R$, $b, c \in R$, следует, что $b = c$ (т. е. возможность сокращать на ненулевой элемент слева, если нет левых делителей нуля; и справа, если нет правых делителей нуля).

Доказательство. Если $ab = ac$, то $a(b - c) = 0$. Так как a не является левым делителем нуля, то $b - c = 0$, т. е. $b = c$. \square

1.4. Нильпотентные элементы кольца

Элемент $x \in R$ называется *нильпотентным*, если $x^n = 0$ для некоторого $0 < n \in \mathbb{N}$. Наименьшее такое натуральное число n называется *степенью нильпотентности элемента*.

Ясно, что нильпотентный элемент является делителем нуля (если $n > 1$, то $x \cdot x^{n-1} = 0$, $x^{n-1} \neq 0$). Обратное утверждение неверно (в \mathbb{Z}_6 нет нильпотентных элементов, однако 2, 3, 4 — ненулевые делители нуля).

Упражнение 1.4.1. Кольцо \mathbb{Z}_n содержит нильпотентные элементы тогда и только тогда, когда n делится на m^2 , где $m \in \mathbb{N}$, $m \neq 1$.

Замечание 1.4.2. $x^n = 0 \implies 1 - x, 1 + x \in U(R)$, $(1 - x)(1 + x + \dots + x^{n-1}) = 1$.

1.5. Идемпотентные элементы кольца

Элемент x кольца R называется *идемпотентом*, если $x^2 = x$. Ясно, что $0^2 = 0$, $1^2 = 1$. Если $x^2 = x$ и $x \neq 0$, $x \neq 1$, то $x(x-1) = x^2 - x = 0$, и поэтому нетривиальные идемпотенты являются делителями нуля.

Лемма 1.5.1. Если $x^2 = x \in R$, то $Rx = Rx \oplus R(1-x)$.

Доказательство. 1) Так как

$$1 = x + (1-x),$$

то (левый) идеал $Rx + R(1-x)$ совпадает с R .

2) Если

$$z \in Rx \cap R(1-x),$$

то

$$z = rx = rx^2 = (rx)x = zx.$$

Так как $z = s(1-x)$, $s \in R$, то

$$z = (s(1-x))x = s(1-x)x = s(x - x^2) = x0 = 0.$$

1.6. Обратимые элементы кольца

Через $U(R)$ обозначим множество обратимых элементов ассоциативного кольца R , т. е. тех $r \in R$, для которых существует обратный элемент $s = r^{-1}$ (т. е. $rr^{-1} = 1 = r^{-1}r$).

Лемма 1.6.1. $U(R)$ является группой относительно операции умножения.

Доказательство. 1) Если $r, s \in U(R)$, то $rs \in U(R)$, поскольку $(rs)^{-1} = s^{-1}r^{-1}$.
 2) $1 \in U(R)$.

3) Если $r \in U(R)$, то $(r^{-1})^{-1} = r$, т. е. $r^{-1} \in U(R)$. \square

Пример 1.6.2. $U(\mathbb{Z}) = \{1, -1\}$, $U(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $U(\mathbb{R}) = \mathbb{R}^*$, $U(\mathbb{C}) = \mathbb{C}^*$.

Пример 1.6.3. $U(C[0, 1]) = \{f \in C[0, 1] \mid f(x) \neq 0 \forall x \in [0, 1]\}$.

Пример 1.6.4. $U(M_n(R)) = GL_n(R)$.

Пример 1.6.5. $U(\{\bar{0}, \bar{1}\}) = \{\bar{1}\}$.

Пример 1.6.6. Пусть $\mathbb{Z}_m = \{C_0, C_1, \dots, C_{m-1}\}$, $C_k = k + m\mathbb{Z}$, — кольцо вычетов по модулю m . Отметим, что $a + m\mathbb{Z} \in U(\mathbb{Z}_m)$, $a \in \mathbb{Z}$, тогда и только тогда, когда $(k + m\mathbb{Z})(l + m\mathbb{Z}) = 1 + m\mathbb{Z}$ для некоторого $l \in \mathbb{Z}$, т. е. $kl + m\mathbb{Z} = 1 + m\mathbb{Z}$, что означает $kl = 1 + mq$, $q \in \mathbb{Z}$, т. е. $(k, m) = 1$.

Итак, $|U(\mathbb{Z}_m)| = \varphi(m)$, где $\varphi(m)$ — число натуральных чисел $1 \leq k < m$, $(k, m) = 1$ (функция Эйлера). В частности, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(p) = p - 1$ для простого числа p . Более того, если $p \in \mathbb{N}$, то $\varphi(p) = p - 1$ тогда и только тогда, когда p — простое число.

Следствие теоремы Лагранжа для группы $U(\mathbb{Z}_m)$ порядка $\varphi(m)$ даёт следующее утверждение.

Теорема Эйлера. Если $k \in \mathbb{Z}$, $(k, m) = 1$, то

$$k^{\varphi(m)} \equiv 1 \pmod{m}.$$

Следствие 1.6.7 (малая теорема Ферма). Если k не делится на простое число p , то

$$k^{p-1} \equiv 1 \pmod{p}$$

(или, в другой форме, $k^p \equiv k \pmod{p}$).

Замечание 1.6.8. Если $p \in \mathbb{N}$, $0 < k < p$, $k^{p-1} \not\equiv 1 \pmod{p}$, то p не может быть простым числом. Отметим, что $3^{90} \equiv 1 \pmod{91}$, однако $91 = 7 \cdot 13$ — составное число. Таким образом, существуют составные числа n , для которых $a^n \equiv a \pmod{n}$ для любого $a \in \mathbb{N}$, $\text{НОД}(a, n) = 1$. Такие числа называются числами Кармайкла. Покажите, что $561 = 3 \cdot 11 \cdot 17$ — число Кармайкла.

Указание. Покажите, что $a^{560} \equiv 1 \pmod{p}$, $p = 3, 11, 17$.

Теорема 1.6.9 (теорема Вилсона). Если $p \in \mathbb{N}$, то p — простое число тогда и только тогда, когда

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказательство. Пусть $G = (\mathbb{Z}_p \setminus \{0\}, \cdot) = \mathbb{Z}_p^*$ — мультиликативная группа поля \mathbb{Z}_p . Если $a \in \mathbb{Z}_p^*$ и $O(a) = 2$, то $a^2 \equiv 1 \pmod{p}$, следовательно, $a^2 - 1 = (a - 1)(a + 1)$ делится на p , поэтому или $a \equiv 1 \pmod{p}$, или $a \equiv -1 \pmod{p}$. В силу леммы ?? в \mathbb{Z}_p

$$1 \cdot 2 \cdots (p-1) \equiv 1 \cdot (-1) \equiv -1 \pmod{p}.$$

Если $p = m \cdot n$, $m, n \in \mathbb{N}$, $1 < m, n < p$, то $(p-1)! \equiv 0 \pmod{m}$. Если при этом $(p-1)! \equiv -1 \pmod{p}$, то $(p-1)! + 1 = m \cdot n \cdot k$, где $k \in \mathbb{N}$, что приводит к противоречию. \square

Задача 1.6.10 (критерий Лукаса). Если $a, n \in \mathbb{N}$, $a^{n-1} \equiv 1 \pmod{n}$ и $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$ для всех простых делителей p числа $n-1$, то n — простое число. Например, 199 — простое число.

Задача 1.6.11. Если p — нечётное простое число, то $U(\mathbb{Z}/p^r\mathbb{Z})$ — циклическая группа порядка $p^{r-1}(p-1)$. В частности, 2 — образующий элемент группы $U(\mathbb{Z}_{3^r})$.

Задача 1.6.12. $|U(\mathbb{Z}/2^r\mathbb{Z})| = 2^{r-1}$, но при $r > 2$ группа $U(\mathbb{Z}/2^r\mathbb{Z})$ не является циклической (в частности, в группе $U(\mathbb{Z}/8\mathbb{Z})$ все неединичные элементы имеют порядок 2).

Задача 1.6.13. Докажите, что группа $U(\mathbb{Z}_n)$ циклическая тогда и только тогда, когда $n \in \{2, 4, p^\alpha, 2p^\alpha\}$, где p — нечётное простое число.

Упражнение 1.6.14 (квадратичные вычеты). Элемент $a \in \mathbb{Z}$ называется квадратичным вычетом по модулю $n \in \mathbb{N}$, если существует такое число $b \in \mathbb{Z}$, что $b^2 \equiv a \pmod{n}$. Например, -1 является квадратом по модулю 10 или 13, но не является квадратом по модулю 7.

Докажите, что

- 1) если p — простое число, $p \neq 2$, то множество квадратов в группе обратимых элементов $U(\mathbb{Z}_p)$ кольца \mathbb{Z}_p является подгруппой порядка $\frac{p-1}{2}$; более того, если K — конечное поле, $\text{char } K = p > 2$, то множество квадратов в $U(K) = K \setminus \{0\}$ — подгруппа порядка $\frac{|K|-1}{2}$;
- 2) пусть p — простое число, $p \neq 2, 3$. Тогда -3 является квадратичным вычетом по модулю p в том и только в том случае, когда $p \equiv 1 \pmod{3}$;
- 3) пусть p — простое число, $p \neq 2$, $f(x, y) = ax^2 + 2bxy + cy^2$, где $a, b, c \in \mathbb{Z}$, $d = ac - b^2$. Покажите, что сравнение $f(x, y) \equiv 0 \pmod{p}$ тогда и только тогда имеет ненулевое решение, когда число $-d$ либо делится на p , либо является квадратичным вычетом по модулю p . Если $d \not\equiv 0 \pmod{p}$, то число ненулевых решений сравнения $f(x, y) \equiv 0 \pmod{p}$ равно $(p-1) \left(1 + \left(\frac{-d}{p}\right)\right)$, здесь $\left(\frac{-d}{p}\right)$ — символ Лежандра, см. 4);
- 4) пусть p — нечётное простое число, C — множество (подгруппа) квадратов в $U(\mathbb{Z}_p)$, $x \rightarrow x^2$ — гомоморфизм $U(\mathbb{Z}_p) \rightarrow U(\mathbb{Z}_p)$. Ядро этого гомоморфизма совпадает с $\{1, -1\}$, а образ — с C . Поэтому $C \cong U(\mathbb{Z}_p)/\{1, -1\}$. Ясно, что $U(\mathbb{Z}_p)/C \cong \{1, -1\}$.

Для $x \in \mathbb{Z}_p$ определим символ Лежандра: $\left(\frac{x}{p}\right) = 1$, если x — квадрат по модулю p , и $\left(\frac{x}{p}\right) = -1$ в противном случае. Покажите, что

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) \left(\frac{y}{p}\right),$$

отображение $x \rightarrow \left(\frac{x}{p}\right)$ является гомоморфизмом групп $U(\mathbb{Z}_p) \rightarrow \{1, -1\}$.

- 5) если p — нечётное простое число, $x \in U(\mathbb{Z}_p)$, то $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ (критерий Эйлера), в частности, -1 является квадратичным вычетом тогда и только тогда, когда $p \equiv 1 \pmod{4}$;

- 6) если p и q — два различных простых числа, то

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

(квадратичный закон взаимности);

- 7) если p — нечётное простое число, то 2 является квадратом по модулю p тогда и только тогда, когда $p \equiv \pm 1 \pmod{8}$, другими словами, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

- 8) покажите, что 323 является квадратом по модулю 479 . Чему равен квадратный корень из 323 в \mathbb{Z}_{479} ?

Задача 1.6.15. Конечное коммутативное кольцо с n обратимыми элементами состоит из не более чём $(n+1)^2$ элементов.

Глава 2

Поля

2.1. Поля

Определение 2.1.1. Ассоциативное коммутативное кольцо K с 1, в котором для любого ненулевого элемента $a \in K$ существует обратный элемент a^{-1} , называется полем.

Лемма 2.1.2. Если K — поле, то уравнение $ax = b$, где $a \neq 0$, имеет одно и только одно решение (именно, $a^{-1}b$).

Доказательство. Если $ax = b$, то $x = a^{-1}ax = a^{-1}b$. Если $x = a^{-1}b$, то $ax = a(a^{-1}b) = b$. \square

Теорема 2.1.3. В поле K нет делителей нуля.

Доказательство. Допустим, что $a, b \in K$, $a \neq 0$, $b \neq 0$ и $ab = 0$. Тогда $b = a^{-1}(ab) = a^{-1}0 = 0$, противоречие. \square

Замечание 2.1.4. Обратное утверждение неверно. В кольце \mathbb{Z} целых чисел нет делителей нуля, но оно не является полем.

Примеры полей

$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_2$

Теорема 2.1.5. Кольцо вычетов \mathbb{Z}_n является полем тогда и только тогда, когда $n = p$ является простым числом.

Доказательство. 1) Если $n = kl$, $1 < k, l < n$, то в \mathbb{Z}_n есть делители нуля ($C_k C_l = C_0$, $C_k \neq C_0$, $C_l \neq C_0$), и поэтому \mathbb{Z}_n не является полем.

2) Пусть $n = p$ — простое число. Если $C_0 \neq C_k \in \mathbb{Z}_n$, то k не делится на p , поэтому $\text{НОД}(k, p) = 1$ и, следовательно, найдутся целые числа $u, v \in \mathbb{Z}$ такие, что $1 = ku + pv$. Тогда $ku = 1 - pv$, и поэтому $C_k C_u = C_1$, т. е. $C_u = C_k^{-1}$. Таким образом, \mathbb{Z}_p — поле. \square

Второе доказательство.

2') Если $n = p$ — простое число, то \mathbb{Z}_p — кольцо без делителей нуля (действительно, если $C_k C_l = C_0$, $C_k \neq C_0$, $C_l \neq C_0$, то $kl = pq$, но k и l не делятся на p , что приводит к противоречию). Доказательство завершает следующая лемма.

поэтому **Лемма 2.1.6.** Конечное коммутативное кольцо без делителей нуля является полем.

Доказательство. Пусть $R = \{r_0 = 0, r_1 = 1, \dots, r_{n-1}\}$ — кольцо из n элементов без делителей нуля. Для $r_k \neq 0$, $1 \leq k \leq n-1$, все произведения $r_k r_1, \dots, r_k r_{n-1}$ различны, поскольку r_k не является делителем нуля. Следовательно, найдётся i , для которого $r_k r_i = 1$, т. е. $r_i = r_k^{-1}$. \square

Задача 2.1.7. Пусть p — простое число. Тогда $1^2 + 2^2 + \dots + (p-1)^2 = 0$ в \mathbb{Z}_p .

Лемма 2.1.8. Пересечение $\bigcap_{i \in I} K_i$ любого семейства подполей K_i , $i \in I$, поля K является подполем. \square

Упражнение 2.1.9. Через $\mathbb{Q}[\sqrt{2}]$ обозначим наименьшее подполе в \mathbb{R} , содержащее поле \mathbb{Q} и элемент $\sqrt{2}$ (существующее по лемме 2.1.8). Покажите, что поля $\mathbb{Q}[\sqrt{2}]$ и $\mathbb{Q}[\sqrt{3}]$ не являются изоморфными.

Замечание 2.1.10. Для всякого элемента $x \in \mathbb{Z}_p$ имеем $x^p = x$.

Доказательство. Пусть $0 \neq a \in \mathbb{Z}_p$. Тогда $\{ay \mid 0 \neq y \in \mathbb{Z}_p\} = \{1, 2, \dots, p-1\}$, при этом все элементы вида ay различны (a обратим в \mathbb{Z}_p). Тогда совпадают их подполя:

$$\prod_{y \in \mathbb{Z}_p} = a^{p-1} \prod_{y \in \mathbb{Z}_p} y = \prod_{y \in \mathbb{Z}_p} y,$$

и поэтому $a^{p-1} = 1$. \square

Следствие 2.1.11. Если $0 < m < p$, то существует $0 < n < p$ такое, что $mn = 1 + kp$, $k \geq 0$. Действительно, $0 < n \leq p-1$, $n = m^{-1} \in \mathbb{Z}_p$.

Задача 2.1.12. В поле \mathbb{Z}_p любой элемент является суммой двух квадратов.

Задача 2.1.13.

1) Любое кольцо с 1, состоящее из двух элементов, изоморфно полю \mathbb{Z}_2 .

2) Любое кольцо с 1, состоящее из пяти элементов, изоморфно полю \mathbb{Z}_5 .

3) Любое кольцо с 1, состоящее из семи элементов, изоморфно полю \mathbb{Z}_7 .

Задача 2.1.14. Матрицы

$$\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$$

где $a, b \in \mathbb{Z}_5$, образуют поле из 25 элементов.

2.2. Характеристика поля

Рассмотрим поле P как абелеву группу $(P, +)$ относительно сложения, пусть $O(1)$ — порядок элемента 1 в этой группе. Если $O(1) = \infty$, то говорят, что характеристика $\text{char } P$ поля P равна 0 (т. е. для любых целых чисел $k, l \in \mathbb{Z}$ из $k \neq l$ следует, что $k \cdot 1 \neq l \cdot 1$ в P). Если $O(1) = p < \infty$, то полагают $\text{char } P = p$ и говорят, что P — поле конечной характеристики p (т. е. p — наименьшее натуральное число, для которого $p \cdot 1 = \underbrace{1 + \dots + 1}_{p} = 0$).

✓ Примеры 2.2.1.

- 1) $\text{char } \mathbb{Q} = 0$, $\text{char } \mathbb{R} = 0$, $\text{char } \mathbb{C} = 0$.
- 2) $\text{char } \mathbb{Z}_p = p$ (для простого числа p).

неко Теорема 2.2.2. Если P — поле и $\text{char } P = p > 0$, то p — простое число.

Доказательство. Допустим противное, т. е. что $p = st$, где $1 < s, t < p$. Тогда

$$(s \cdot 1)(t \cdot 1) = (\underbrace{1 + \dots + 1}_s)(\underbrace{1 + \dots + 1}_t) = st \cdot 1 = p \cdot 1 = 0,$$

но $s \cdot 1 \neq 0$, $t \cdot 1 \neq 0$ в поле P , что противоречит отсутствию делителей нуля в поле. \square

|| 2.3. Идеалы кольца

Определение 2.3.1. Пусть R — кольцо. Подмножество $\emptyset \neq I \subset R$ называется левым идеалом кольца R , если

- 1) I — подгруппа аддитивной группы $(R, +)$ кольца R ;
- 2) $rI \subseteq I$ для любого элемента $r \in R$ (т. е. $ri \in I$ для всех $i \in I$).

Аналогично определяется правый идеал: вместо 2) условие

- 2') $Ir \subseteq I$ для любого элемента $r \in R$ (т. е. $ir \in I$ для всех $i \in I$).

Если подмножество I в кольце R является и левым и правым идеалом, то I называется двусторонним идеалом кольца R (т. е. I — подгруппа в $(R, +)$, $rI \subseteq I$, $Ir \subseteq I$ для всех $r \in R$). Для двустороннего идеала I кольца R будем использовать обозначение $I \triangleleft R$.

✓ Примеры 2.3.2.

- 1) $\{0\}$ и R — идеалы кольца R .
- 2) $n\mathbb{Z} \triangleleft \mathbb{Z}$ для любого $n \in \mathbb{Z}$.
- 3) $I_a = \{f \in C[0, 1] \mid f(a) = 0\} \triangleleft C[0, 1]$ для любого $a \in [0, 1]$.

Задача 2.3.3. Коммутативное кольцо R с 1 является полем тогда и только тогда, когда все идеалы кольца R — это $\{0\}$ и R .

Упражнение 2.3.4. Если K — поле, то кольцо квадратных $(n \times n)$ -матриц $R = M_n(K)$ с элементами из поля K является простым кольцом (т. е. любой идеал $I \triangleleft R = M_n(K)$ либо нулевой, либо равен всему кольцу R). Совокупность всех матриц вида

$$\begin{pmatrix} 0 & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \dots & * \end{pmatrix}$$

образует левый идеал (не являющийся правым) в кольце $M_n(K)$. Совокупность всех матриц вида

$$\begin{pmatrix} 0 & 0 & \dots & 0 \\ * & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \dots & * \end{pmatrix}$$

образует правый идеал (не являющийся левым идеалом).

Упражнение 2.3.5. В кольце целочисленных матриц $M_n(\mathbb{Z})$ подкольцо $M_n(2\mathbb{Z})$ матриц с чётными элементами является двусторонним идеалом.

Любой ненулевой идеал кольца $M_n(\mathbb{Z})$ совпадает с $M_n(k\mathbb{Z})$ для некоторого $k \in \mathbb{N}$.

2.4. Операции с идеалами

Пусть I_1, \dots, I_n — (левые) идеалы кольца R , $n \geq 2$. Тогда

$$I_1 + \dots + I_n = \{a_1 + \dots + a_n \mid a_i \in I_i\} =$$

(левый) идеал кольца R (наименьший (левый) идеал кольца R , среди (левых) идеалов, содержащих все I_i , $i = 1, \dots, n$, называемый *суммой идеалов* I_1, \dots, I_n).

Пересечение (левых) идеалов $\bigcap_{i=1}^n I_i$ является (левым) идеалом кольца R (наибольший (левый) идеал среди (левых) идеалов, лежащих во всех идеалах I_i , $i = 1, \dots, n$).

Частично упорядоченное множество всех (левых) идеалов кольца R (по включению) является дедекиндовской решёткой.

Множество $I_1 I_2 \dots I_n$ всех конечных сумм элементов вида $a_1 a_2 \dots a_n$, где $a_i \in I_i$ для $i = 1, \dots, n$, является (левым) идеалом кольца R , называемым *произведением* (левых) идеалов I_1, \dots, I_n кольца R . Ясно, что для идеалов I_1, \dots, I_n кольца R имеем

$$I_1 I_2 \dots I_n \subseteq \bigcap_{i=1}^n I_i.$$

Если $I_1 = \dots = I_n = I$, то $I_1 I_2 \dots I_n = I^n$ называется *n-й степенью (левого) идеала I*.

Упражнение 2.4.1. Пусть I_1, \dots, I_n, I, J, L — (левые) идеалы кольца R . Тогда:

- 1) $(I + J) + L = I + (J + L)$;
- 2) $(IJ)L = I(JL)$;
- 3) $J(I_1 + I_2 + \dots + I_n) = JI_1 + JI_2 + \dots + JI_n$; $(I_1 + I_2 + \dots + I_n)L = I_1 L + I_2 L + \dots + I_n L$. \square

Замечание 2.4.2. В кольце целых чисел \mathbb{Z} имеем $U(\mathbb{Z}) = \{1, -1\}$, таким образом, в \mathbb{Z} много элементов, которые не являются делителями нуля, но не являются обратимыми элементами. В то же время в кольце матриц $M_n(K)$ над полем K и в конечном кольце R с единицей каждый ненулевой элемент либо обратим, либо является делителем нуля (т. е. любой неделитель нуля обратим).

Упражнение 2.4.3. В кольце \mathbb{Z}_{16} множество всех делителей нуля является идеалом (в кольце \mathbb{Z}_{12} это уже не так).

Упражнение 2.4.4.

- 1) Мультипликативная группа $K^* = (K \setminus \{0\})$ конечного поля является циклической.
- 2) В мультипликативной группе K^* произвольного поля K любая конечная подгруппа является циклической.
- 3) Сумма всех элементов конечного поля, отличного от \mathbb{Z}_2 , равна нулю.

Упражнение 2.4.5. Пусть K — конечное поле, $p = \text{char } K$, $q = |K|$. Тогда:

- 1) отображение $x \mapsto x^p$ является автоморфизмом поля K ;
- 2) $x^q = x$ для всех $x \in K$;
- 3) произведение всех ненулевых элементов поля K равно -1 .

2.5. Фактор-кольцо

Пусть $I \triangleleft R$ — двусторонний идеал кольца R с 1. Тогда I — подгруппа коммутативной группы $(R, +)$. Рассмотрим коммутативную фактор-группу

$$(R/I, +) = \{r + I \mid r \in R\},$$

где

$$(r + I) + (s + I) = r + s + I$$

для $r, s \in R$. На множестве R/I определим операцию умножения, полагая

$$(r + I)(s + I) = rs + I.$$

Проверим корректность определений умножения смежных классов. Пусть $r + I = r' + I$, $s + I = s' + I$, $r, r', s, s' \in R$. Тогда $r' = r + i_1$, $s' = s + i_2$, $i_1, i_2 \in I$. Поэтому

$$r's' = (r + i_1)(s + i_2) = rs + (i_1s + ri_2 + i_1i_2).$$

Так как $i_1s + ri_2 + i_1i_2 \in I$, то $r's' + I = rs + I$.

Покажем, что $(R/I, +, \cdot)$ является ассоциативным кольцом с 1.

Ассоциативность умножения: для $r, s, t \in R$ имеем

$$\begin{aligned} (r + I)((s + I)(t + I)) &= (r + I)(st + I) = r(st) + I = \\ &= (rs)t + I = (rs + I)(t + I) = ((r + I)(s + I))(t + I). \end{aligned}$$

Нейтральный элемент $1 + I$ относительно умножения: для $r \in R$

$$(r + I)(1 + I) = r + I = (1 + I)(r + I).$$

Законы дистрибутивности: для $r, s, t \in R$

$$\begin{aligned} ((r+I)+(s+I))(t+I) &= (r+s)t+I = rt+st+I = \\ &= (rt+I)+(st+I) = (r+I)(t+I)+(s+I)(t+I); \end{aligned}$$

$$\begin{aligned} (t+I)((r+I)+(s+I)) &= t(r+s)+I = tr+ts+I = \\ &= (tr+I)+(ts+I) = (t+I)(r+I)+(t+I)(s+I). \end{aligned}$$

Итак, мы доказали:

Теорема 2.5.1. Для двустороннего идеала $I \triangleleft R$ кольца R множество смежных классов $R/I = \{r+I \mid r \in R\}$ с операциями сложения $(r+I)+(s+I) = (r+s)+I$ и умножения $(r+I)(s+I) = rs+I$, где $r, s \in R$, является ассоциативным кольцом с единицей $1+I$.

Примеры 2.5.2.

- ✓ 1) $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$.
- ✓ 2) $C[0, 1]/I_a \cong \mathbb{R}$.
- 3) $\mathbb{Z}[i]/(2)$ не является полем; $\mathbb{Z}[i]/(3)$ — поле из девяти элементов.

2.6. Гомоморфизмы колец

Пусть R и R' — кольца. Отображение $f: R \rightarrow R'$ называется гомоморфизмом колец, если $f(a+b) = f(a) + f(b)$ и $f(ab) = f(a)f(b)$ для всех $a, b \in R$.

Через $\text{Im } f$ обозначим образ гомоморфизма f , т. е.

$$\text{Im } f = \{f(r) \in R' \mid r \in R\};$$

через $\text{Ker } f$ — ядро гомоморфизма f , т. е.

$$\text{Ker } f = \{a \in R \mid f(a) = 0\}.$$

Если гомоморфизм f является биекцией, то f называется изоморфизмом колец.

Отметим ряд свойств гомоморфизмов колец $f: R \rightarrow R'$.

1. Так как f — гомоморфизм абелевых групп $(R, +)$, $(R', +)$, то $f(0) = 0'$, $f(-a) = -f(a)$.

2. Если $R \ni 1$, $R' \ni 1'$ и $\text{Im } f = R'$, то $f(1) = 1'$, $f(a^{-1}) = f(a)^{-1}$ для обратимого элемента a . Действительно, если $a' \in R'$, то $a' = f(a)$, $a \in R$. Тогда

$$\begin{aligned} f(1)a' &= f(1)f(a) = f(1 \cdot a) = f(a) = a', \\ a'f(1) &= f(a)f(1) = f(a \cdot 1) = f(a) = a', \end{aligned}$$

т. е. $f(1) = 1'$;

$$\begin{aligned} f(a^{-1})f(a) &= f(a^{-1}a) = f(1) = 1', \\ f(a)f(a^{-1}) &= f(aa^{-1}) = f(1) = 1', \end{aligned}$$

т. е. $f(a^{-1}) = f(a)^{-1}$.

15-15-

Замечание 2.6.1. Это утверждение может не быть верным, если $\text{Im } f \neq R'$. Действительно, для гомоморфизма колец $f: \mathbb{R} \rightarrow M_2(\mathbb{R})$, где

$$f(a) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix},$$

имеем

$$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

т. е. даже

$$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

не является обратимым элементом в кольце $M_2(\mathbb{R})$.

3а. Если $f: R \rightarrow R'$ — гомоморфизм колец, то $\text{Ker } f$ — двусторонний идеал кольца R .

Доказательство. Так как $f: (R, +) \rightarrow (R', +)$ — гомоморфизм групп, то $\text{Ker } f$ — подгруппа в $(R, +)$.

Если $a \in \text{Ker } f$, т. е. $f(a) = 0$, $r, s \in R$, то

$$f(ra) = f(r)f(a) = f(r) \cdot 0 = 0,$$

$$f(as) = f(a)f(s) = 0 \cdot f(s) = 0,$$

так, $ra \in \text{Ker } f$, $as \in \text{Ker } f$, т. е. $\text{Ker } f \triangleleft R$. □

3б. Если $I \triangleleft R$ — двусторонний идеал кольца R , то отображение

$$\pi = \pi_I: R \rightarrow R/I, \quad \pi(r) = r + I \text{ для } r \in R,$$

является гомоморфизмом колец (канонический гомоморфизм), при этом $\text{Ker } \pi_I = I$.

Таким образом, ядра гомоморфизмов колец и только они являются двусторонними идеалами.

4. Гомоморфизм колец $f: R \rightarrow R'$ является изоморфизмом тогда и только тогда, когда $\text{Ker } f = \{0\}$ и $\text{Im } f = R'$ (следует вспомнить критерий изоморфизма для гомоморфизмов групп).

Ясно, что изоморфные кольца обладают одинаковыми кольцевыми свойствами. Например, если $f: R \rightarrow R'$ — изоморфизм колец, R поле, то R' также поле.

Упражнение 2.6.2. Если поле P содержит поле \mathbb{R} действительных чисел, $P \ni j$, $j^2 = -1$, и при этом любое подполе $P' \subset P$, содержащее R и j , совпадает с P , то поле P изоморфно полю \mathbb{C} комплексных чисел.

Упражнение 2.6.3. Поле $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ комплексных чисел изоморфно полю

$$C' = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in M_2(\mathbb{R}) \mid a, b \in \mathbb{R} \right\}.$$

Упражнение 2.6.4. $R[x]/R[x](x^2 + 1) \cong \mathbb{C}$.

Упражнение 2.6.5. Если R — коммутативное кольцо и $I \triangleleft R$, то R/I — поле тогда и только тогда, когда I — максимальный идеал.

Упражнение 2.6.6. Если R — коммутативное кольцо, то R — поле тогда и только тогда, когда в R нет идеалов, отличных от $\{0\}$.

Упражнение 2.6.7. Отображение $\mathbb{Z} \rightarrow \mathbb{Z}$, при котором $k + 3\mathbb{Z} \mapsto 4k + 6\mathbb{Z}$, является инъективным гомоморфизмом кольц.

2.7. Теорема о гомоморфизме для колец

Теорема 2.7.1. Пусть $f: R \rightarrow R'$ — сюръективный гомоморфизм колец, $I = \text{Ker } f$. Тогда существует изоморфизм колец $\psi: R/\text{Ker } f \rightarrow R'$, для которого следующая диаграмма коммутативна

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \pi_{\text{Ker } f} \downarrow & \swarrow \psi & \\ R/\text{Ker } f & & \end{array}$$

т. е. $f = \psi \pi_{\text{Ker } f}$.

Доказательство. В силу теоремы о гомоморфизме для групп биекция $\psi: R/\text{Ker } f \rightarrow R'$, для которой $\psi(r + \text{Ker } f) = f(r)$, является изоморфизмом абелевых групп $(R/\text{Ker } f, +)$ и $(R', +)$. Так как

$$\psi((r + \text{Ker } f)(s + \text{Ker } f)) = \psi(rs + \text{Ker } f) = f(rs) = f(r)f(s) = \psi(r + \text{Ker } f)\psi(s + \text{Ker } f),$$

то ψ — изоморфизм колец. \square

Пример 2.7.2 (вычисление фактор-кольца (с помощью теоремы о гомоморфизме)). Пусть $R = C[0, 1]$ — кольцо непрерывных функций на отрезке $[0, 1]$, $a \in [0, 1]$, $I_a = \{\varphi \in C[0, 1] \mid \varphi(a) = 0\} \triangleleft R$. Тогда $C[0, 1]/I_a \cong \mathbb{R}$.

Доказательство. Пусть $f: R = C[0, 1] \rightarrow \mathbb{R}$ — сюръективный гомоморфизм колец, для которого $f(\varphi) = \varphi(a)$ для $\varphi \in C[0, 1]$. Тогда $\text{Ker } f = I_a$, поэтому

$$C[0, 1]/I_a \cong \mathbb{R}. \quad \square$$

Задача 2.7.3. Докажите, что:

- 1) $K[x]/\langle x \rangle \cong K[x]/\langle x+1 \rangle \cong K$; $\mathbb{Z}[x]/\langle 3 \rangle \cong \mathbb{Z}_3[x]$;
- 2) $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$;
- 3) кольцо $\mathbb{Z}[i]/\langle a+ib \rangle$ состоит из $a^2 + b^2$ элементов;
- 4) $\mathbb{Z}[i]/\langle 2 \rangle$ не является полем;
- 5) $\mathbb{Z}[i]/\langle 3 \rangle$ — поле из 9 элементов;
- 6) $\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ — поле из 8 элементов;
- 7) если K — поле, $K[x]/\langle x^2 \rangle \cong K[x]/\langle (x-1)^2 \rangle$ тогда и только тогда, когда $\text{char } K = 2$;
- 8) фактор-кольца $\mathbb{Z}_3[x]/\langle x^3 + 1 \rangle$ и $\mathbb{Z}_3[x]/\langle x^3 + 2x^2 + x + 1 \rangle$ не изоморфны.

Задача 2.7.4. Пусть K — поле. Какие из фактор-колец $K[x]/\langle x^2 - 1 \rangle$, $K[x]/\langle x^2 + 1 \rangle$, $K[x]/\langle x^2 - 4 \rangle$, $K[x]/\langle x^2 + 2x + 2 \rangle$ изоморфны?

Задача 2.7.5. Пусть F_q — конечное поле из q элементов. Докажите, что кольцо всех функций $F_q \rightarrow F_q$ изоморфно фактор-кольцу $F_q[x]/\langle x^q - x \rangle$.

Лемма 2.7.6. Пусть R — ненулевое коммутативное кольцо. Тогда следующие условия эквивалентны:

- 1) R — поле;
- 2) в кольце R нет идеалов, отличных от 0 и R ;
- 3) любой ненулевой гомоморфизм $f: R \rightarrow S$, $\text{Im } f \neq 0$, в любое ненулевое кольцо S инъективен.

Доказательство. 1) \Rightarrow 2) Если $0 \neq I \triangleleft R$, $0 \neq x \in I$, то $1 = x \cdot x^{-1} \in I$, и поэтому $I = R$.

2) \Rightarrow 3) Пусть $f: R \rightarrow S$ — гомоморфизм колец, $\text{Ker } f \triangleleft R$, $\text{Ker } f \neq R$, поэтому $\text{Ker } f = 0$, следовательно, f — инъекция.

3) \Rightarrow 1) Если $x \in R \setminus U(R)$, то $Rx \triangleleft R$, $Rx \neq R$. Пусть $S = R/Rx$, $\pi: R \rightarrow R/Rx$ — канонический гомоморфизм, $\pi \neq 0$, $\text{Ker } \pi = Rx$. По предположению π — инъекция, следовательно, $Rx = 0$, что означает $x = 0$. \square

Упражнение 2.7.7. Повторяя конструкцию построения поля \mathbb{Q} рациональных чисел исходя из кольца целых чисел \mathbb{Z} , докажите, что если R — коммутативное кольцо без делителей нуля, то R можно вложить в его поле частных

$$Q(R) = \left\{ \left[\begin{array}{c} a \\ b \end{array} \right] \mid (a, b) \in R^2, b \neq 0 \right\},$$

где $\left[\begin{array}{c} a \\ b \end{array} \right]$ — класс дробей, эквивалентных дроби $\frac{a}{b}$ (здесь $\frac{a}{b} \sim \frac{c}{d}$, если $ad = bc$; сложение и умножение дробей и их классов эквивалентности определено по аналогии с рациональными дробями и рациональными числами).

Замечание 2.7.8. Все основные результаты о системах линейных уравнений, о матрицах, об определителе, о линейной зависимости справедливы над любым полем P (следует, конечно, помнить, что поле P может иметь характеристику $\text{char } P > 0$, а также то, что поле P может быть конечным).

Теорема 2.7.9 (китайская теорема об остатках над целыми числами, Китай, Греция, 2000 лет назад). Пусть $m_0, m_1, \dots, m_n \in \mathbb{Z}$, $(m_i, m_j) = 1$ для $i \neq j$, $u_i \in \mathbb{Z}_{m_i}$, $i = 0, 1, \dots, n$. Тогда для любого $a \in \mathbb{Z}$ существует, и при этом единственное, число $u \in \mathbb{Z}$ такое, что

$$1) a \leq u < a + m, \text{ где } m = \prod_{i=0}^n m_i;$$

$$2) u \equiv u_i \pmod{m_i}, 0 \leq i \leq n.$$

Доказательство. Единственность. Если $u, v \in \mathbb{Z}$ удовлетворяют условиям теоремы, то $u - v \in \mathbb{Z}_{m_i}$, $i = 0, 1, \dots, n$, и поэтому $u - v \in \mathbb{Z}_m$, $m = \prod_{i=0}^n m_i$, поскольку m_0, m_1, \dots, m_n взаимно просты. Кроме того, $|u - v| < m$. Поэтому $u - v = 0$, т. е. $u = v$.

Существование. Пусть $a \leq u < a + m$ (таких различных элементов m). Рассмотрим строчку длины $(n+1)$

$$(\varphi_{m_0}(u), \varphi_{m_1}(u), \dots, \varphi_{m_n}(u)) \in \mathbb{Z}_{m_0} \times \dots \times \mathbb{Z}_{m_n},$$

где

$$\varphi_n : \mathbb{Z} \rightarrow \mathbb{Z}_n, \quad \varphi(k) = k + n\mathbb{Z}.$$

По доказанному утверждению о единственности, мы получаем $m = \prod_{i=0}^n m_i$ различных строчек в множестве $\mathbb{Z}_{m_0} \times \dots \times \mathbb{Z}_{m_n}$, $|\mathbb{Z}_{m_0} \times \dots \times \mathbb{Z}_{m_n}| = \prod_{i=0}^n m_i = m$, т. е. наши строчки исчерпывают все строчки этого произведения. Следовательно,

$$(u_0, u_1, \dots, u_n) = (\varphi_{m_0}(u), \dots, \varphi_{m_n}(u))$$

для некоторого u , $a \leq u < a + m$, при этом однозначно определённого. \square

Замечание 2.7.10. Если $a_1, \dots, a_n \in \mathbb{Z}$ — попарно взаимно простые целые числа, $b_1, \dots, b_n \in \mathbb{Z}$ и мы ищем такое число c , что $c \equiv b_i \pmod{a_i}$, то можно найти число c с помощью следующего алгоритма. Обозначим

$$A = a_1 \cdot a_2 \cdots a_n.$$

Ясно, что

$$\text{НОД}\left(\frac{A}{a_i}, a_i\right) = 1, \quad 1 \leq i \leq n.$$

С помощью алгоритма Евклида находим такие числа $s_i, t_i \in \mathbb{Z}$, $1 \leq i \leq n$, что

$$s_i \cdot \frac{A}{a_i} + t_i \cdot a_i = 1.$$

Положим

$$c_i \equiv b_i \cdot s_i \pmod{a_i}, \quad i = 1, \dots, n,$$

$$c = \sum_{i=1}^n c_i \cdot \frac{A}{a_i} \pmod{A}.$$

Можно также искать элемент с следующим образом:

$$d_1 \equiv b_1 \pmod{a_1};$$

$$d_2 \equiv A_2(C_2(b_2 - d_1) \pmod{a_2}) + d_1;$$

$$d_3 \equiv A_3(C_3(b_3 - d_2) \pmod{a_3}) + d_2;$$

$$d_n \equiv A_n(C_n(b_n - d_{n-1}) \pmod{a_n}) + d_{n-1},$$

где $A_i = \prod_{j < i} a_j$, коэффициенты C_i удовлетворяют условиям $C_i A_i \equiv 1 \pmod{a_i}$ и получены при помощи алгоритма Евклида для A_i и a_i , $1 \leq i \leq n$. Тогда искомое число равно $c \equiv d_n$.

Указанный алгоритм может быть применён в любой евклидовой области, например в кольце многочленов от одной переменной над полем $K[x]$. Если, например, $a_i = x - u_i$, $1 \leq i \leq n$, где u_1, \dots, u_n — различные элементы поля K , $b_i \in K$, $1 \leq i \leq n$, то описанный алгоритм строит такой многочлен $f(x)$ степени меньше n , что

$$f \equiv b_i \pmod{\langle x - u_i \rangle}, \quad 1 \leq i \leq n.$$

Полученный многочлен является интерполяционным многочленом Лагранжа (см. ??). Таким образом, алгоритм реализации китайской теоремы об остатках для многочленов может рассматриваться как обобщение построения интерполяционного многочлена Лагранжа.

Пример 2.7.11. Пусть

$$a_1 = 40, \quad a_2 = 41, \quad a_3 = 43, \quad b_1 = 15, \quad b_2 = 32, \quad b_3 = 29.$$

Тогда, применяя алгоритм замечания 2.7.10, имеем

$$A = 70520, \quad \frac{A}{a_1} = 1763, \quad \frac{A}{a_2} = 1720, \quad \frac{A}{a_3} = 1640.$$

С помощью алгоритма Евклида получаем:

$$\begin{aligned} (-13) \cdot 1763 + 573 \cdot 40 &= 1; \\ 20 \cdot 1720 - 839 \cdot 41 &= 1; \\ (-7) \cdot 1640 + 267 \cdot 43 &= 1. \end{aligned}$$

Таким образом,

$$s_1 = -13; \quad s_2 = 20; \quad s_3 = -7;$$

$$C_1 = 15 \cdot (-13) = 5 \pmod{a_1};$$

$$C_2 = 32 \cdot 20 = 25 \pmod{a_2};$$

$$C_3 = 29 \cdot (-7) = 12 \pmod{a_3}$$

$$c = 5 \cdot 1763 + 25 \cdot 1720 + 12 \cdot 1640 = 71495 \equiv 975 \pmod{A}.$$

Пример 2.7.12. Если даны попарно взаимно простые числа 4, 5, 7, 9, $x \equiv 3 \pmod{4}$, $x \equiv 4 \pmod{5}$, $x \equiv 2 \pmod{7}$, $x \equiv 6 \pmod{9}$, то наименьшее натуральное число $x = 1059$ (в полуинтервале $[0, 1260)$).

Однако изменение даже одного из остатков на 1 может существенно изменить решение задачи: взаимно простые числа 40, 41, 43; $m = 40 \cdot 41 \cdot 43 = 70520$;

$$975 \equiv 15 \pmod{40}, \quad 975 \equiv 32 \pmod{41}, \quad 975 \equiv 29 \pmod{43};$$

$$60015 \equiv 15 \pmod{40}, \quad 60015 \equiv 32 \pmod{41}, \quad 60015 \equiv 30 \pmod{43}.$$

Если верить легендам, то название «китайская теорема об остатках» восходит к правилу китайских военачальников быстро подсчитывать число оставшихся в живых после сражения, перестраивая их в колонны шириной по близким взаимно простым числам, определяя остатки по неполным последним шеренгам, а затем восстанавливая исходное число по таблицам. Последний пример ещё раз подчёркивает роль дисциплины в военном деле.

Замечание 2.7.13. Описание эффективного алгоритма Гарнета (1959) нахождения решения в китайской теореме об остатках можно найти в [1].

Теорема 2.7.14 (китайская теорема об остатках для идеалов колец). Пусть I_1, \dots, I_n — идеалы кольца R (с 1) и $I_i + I_j = R$ для $i \neq j$. Если $b_1, \dots, b_n \in R$, то существует элемент $b \in R$ такой, что

$$b \equiv b_i \pmod{I_i}, \quad i = 1, \dots, n$$

(этот элемент b однозначно определён по модулю идеала $\bigcap_{i=1}^n I_i = I_1 \cap I_2 \cap \dots \cap I_n$).

Доказательство. Проведём индукцию по n . Для $n = 2$ из $R = I_1 + I_2$ имеем

$$1 = a_1 + a_2, \quad a_1 \in I_1, \quad a_2 \in I_2.$$

Рассмотрим $b = b_2 a_1 + b_1 a_2$. Тогда

$$b \equiv b_1 a_2 \pmod{I_1} \equiv b_1 \pmod{I_1};$$

$$b \equiv b_2 a_1 \pmod{I_2} \equiv b_2 \pmod{I_2}.$$

Пусть утверждение верно для семейств из $n - 1$ идеалов. Так как $I_1 + I_i = R$ для каждого $i \geq 2$, то найдём элементы $a_i \in I_1$, $b_i \in I_i$ такие, что $a_i + b_i = 1$, $i \geq 2$. Так как

$$1 = \prod_{i=2}^n (a_i + b_i) \in I_1 + \prod_{i=2}^n I_i,$$

то

$$I_1 + \prod_{i=2}^n I_i = R.$$

Для $n = 2$ мы проверили наше утверждение, поэтому существует такой элемент $y_1 \in R$, что

$$y_1 \equiv 1 \pmod{I_1};$$

$$y_1 \equiv 0 \pmod{\prod_{i=2}^n I_i}.$$

Аналогично, найдутся такие элементы $y_2, \dots, y_n \in R$, что

$$y_j \equiv 1 \pmod{I_j};$$

$$y_j \equiv 0 \pmod{I_i} \text{ при } i \neq j.$$

Элемент

$$b = b_1 y_1 + \dots + b_n y_n$$

удовлетворяет нашим требованиям.

В условиях теоремы каноническое отображение колец

$$f: R \rightarrow \prod_{i=1}^n (R/I_i)$$

сюръективно, имеет ядро

$$\text{Ker } f = \bigcap_{i=1}^n I_i,$$

что приводит к изоморфизму

$$R / \bigcap_{i=1}^n I_i \cong \prod_{i=1}^n R/I_i.$$

Это объясняет единственность построенного элемента $b \in R$ по модулю идеала $\bigcap_{i=1}^n I_i$. \square

Конец лекции № 15

Лекция №16 и 17 18, 19-20 (29 сентября 2011 г.)

Глава 3

Кольцо многочленов от одной переменной

3.1. Кольцо многочленов от одной переменной

Пусть P — произвольное поле (наиболее важные для нас случаи: $P = \mathbb{R}$, $P = \mathbb{C}$).

Под многочленом (ненулевым) от одной переменной x с коэффициентами из поля P будем понимать формальное выражение вида

$$f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + a_nx^n$$

(иногда удобнее записывать эту сумму одночленов $a_i x^i$ в другом порядке: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_i \in P$, $a_n \neq 0$ — старший коэффициент ($a_n x^n$ — старший член многочлена $f(x)$), a_0 — свободный член, $n = \deg f(x)$ — степень ненулевого многочлена $f(x)$ (нулевой многочлен — это $f(x) = a_0 = 0$).

Можно было вместо формальных выражений рассматривать счётные последовательности

$$(a_0, a_1, \dots, a_n, 0, 0, \dots), \quad a_i \in P,$$

в которых почти все a_i (т. е. все, кроме конечного числа) равны нулю (нулевой многочлен — это последовательность, в которой все компоненты равны нулю).

Два многочлена $f(x)$ и $g(x)$ называются равными, если равны соответствующие коэффициенты при каждой степени x^k переменной x .

Через $P[x]$ обозначим множество всех многочленов $f(x)$ с коэффициентами из поля P .

На множестве $P[x]$ введём операции сложения и умножения, для

$$f(x) = \sum_{i=0}^n a_i x^i, \quad g(x) = \sum_{i=0}^s b_i x^i$$

полагая

$$f(x) + g(x) = \sum_{i \geq 0} d_i x^i, \quad f(x)g(x) = \sum_{i \geq 0} t_i x^i,$$

где

$$d_i = a_i + b_i, \quad t_i = \sum_{\substack{k+l=i \\ 0 \leq k, l \leq i}} a_k b_l.$$

$$\begin{aligned} (a_k x^k)(b_l x^l) &= \\ &= a_k b_l x^{k+l} \end{aligned}$$

Теорема 3.1.1. $P[x]$ с операцией сложения и умножения — коммутативное ассоциативное кольцо.

Доказательство.

1) Так как при сложении складываются коэффициенты при одной степени x^i , т. е. $d_i = a_i + b_i$, то ясно, что $P[x]$ с операцией сложения — коммутативная группа.

2) Ясно, что операция умножения по определению коэффициента $t_i = \sum_{\substack{k+l=i \\ 0 \leq k, l \leq i}} a_k b_l$ коммутативна.

Пусть теперь $h(x) = \sum_{i \geq 0} c_i x^i$. Тогда, подсчитывая коэффициенты при степени x^i в $(f(x)g(x))h(x)$ и в $f(x)(g(x)h(x))$, видим, что

$$\sum_{u+m=i} \left(\sum_{k+l=u} a_k b_l \right) c_m = \sum_{k+l+m=i} a_k b_l c_m = \sum_{k+v=i} a_k \left(\sum_{l+m=v} b_l c_m \right).$$

Итак, мы проверили ассоциативность умножения многочленов.

Ясно, что $f(x) = 1$ (т. е. $a_0 = 1$) является нейтральным элементом для операции умножения.

3) Подсчитывая коэффициенты при степени x^i в $(f(x)+g(x))h(x)$ и $f(x)h(x)+g(x)h(x)$, видим, что

$$\sum_{k+l=i} (a_k + b_k) c_l = \sum_{k+l=i} a_k c_l + \sum_{k+l=i} b_k c_l,$$

т. е. установлен закон дистрибутивности в $P[x]$. \square

Замечание 3.1.2. Отображение $P \rightarrow P[x]$, для которого $a \mapsto f(x) = a_0 = a$, является инъективным гомоморфизмом колец (т. е. получили вложение поля P в кольцо многочленов $P[x]$).

Лемма 3.1.3.

a) $\deg(f(x) + g(x)) \leq \max(\deg f(x), \deg g(x))$.

б) $\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$.

Доказательство.

а) Если $i > \max(\deg f(x), \deg g(x))$, то $c_i = a_i + b_i = 0$.

б) Если $\deg f(x) = n$, $\deg g(x) = s$ и $i > n + s$, то $d_i = \sum_{\substack{k+l=i \\ 0 \leq k, l \leq i}} a_k b_l = 0$. При

этом $d_{n+s} = a_n b_s \neq 0$ (поскольку $a_n \neq 0$, $b_s \neq 0$ и в поле P нет делителей нуля). Итак, $d_{n+s} = a_n b_s \neq 0$ — старший коэффициент многочлена $f(x)g(x)$ — является произведением старших коэффициентов многочленов $f(x)$ и $g(x)$. Таким образом, $\deg(f(x)g(x)) = n + s = \deg f(x) + \deg g(x)$. \square

Следствие 3.1.4. В кольце многочленов $P[x]$ нет делителей нуля.

Доказательство. Как мы видели, если $f(x) \neq 0$, $\deg f(x) = n$, $a_n \neq 0$ — старший коэффициент многочлена $f(x)$, $g(x) \neq 0$, $\deg g(x) = s$, $b_s \neq 0$ — старший коэффициент многочлена $g(x)$, то $a_n b_s \neq 0$ — старший коэффициент многочлена $f(x)g(x)$, т. е. $f(x)g(x) \neq 0$. \square

Следствие 3.1.5. В кольце $P[x]$ (как в любом кольце без делителей нуля) можно сокращать на ненулевой многочлен, т. е. из $f(x)g(x) = f(x)h(x)$, $f(x) \neq 0$, следует, что $g(x) = h(x)$.

Следствие 3.1.6. $U(P[x]) = P \setminus \{0\}$ (здесь $U(R)$ — группа обратимых элементов кольца R).

Доказательство. Если $0 \neq a \in P$, то $a^{-1} \in P \subseteq P[x]$, т. е. $a \in U(P[x])$.

Если $f(x)g(x) = 1$, то $f(x) \neq 0$, $g(x) \neq 0$, $\deg f(x) + \deg g(x) = 0$, и поэтому $\deg f(x) = 0 = \deg g(x)$, т. е. $f(x) = a_0 \neq 0$, $a_0 \in P$. \square

Упражнение 3.1.7. Произведение двух линейных многочленов

$$(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd,$$

требующее четырёх умножений (ac , ad , bc , bd) и одного сложения ($ad + bc$), может быть вычислено с помощью трёх умножений и четырёх сложений и вычитаний:

$$ac, \quad bd, \quad u = (a+b)(c+d), \quad ad + bc = u - ac - bd.$$

А. А. Карацуба использовал это соображение для построения быстрых алгоритмов умножения чисел и многочленов.

Теорема 3.1.8 (алгоритм деления с остатком в кольце многочленов). Для любых многочленов $f(x), g(x) \in P[x]$, $g(x) \neq 0$, существуют (и притом единственны) многочлены $q(x), r(x) \in P[x]$ такие, что:

- 1) $f(x) = g(x)q(x) + r(x);$
- 2) либо $r(x) = 0$, либо $\deg r(x) < \deg g(x)$.

Доказательство-алгоритм (деление многочленов столбиком). Пусть

$$\begin{aligned} f(x) &= a_n x^n + \dots + a_1 x + a_0, \\ g(x) &= b_s x^s + \dots + b_1 x + b_0, \quad b_s \neq 0. \end{aligned}$$

Если $n < s$, то утверждение 1) очевидно:

$$f(x) = g(x) \cdot 0 + f(x).$$

Пусть $n \geq s$. Тогда:

$$f(x) - \frac{a_n}{b_s} x^{n-s} g(x) = f_1(x) = a_{1,n_1} x^{n_1} + \dots, \quad s \leq n_1 < n,$$

$$f_1(x) - \frac{a_{1,n_1}}{b_s} x^{n_1-s} g(x) = f_2(x) = a_{2,n_2} x^{n_2} + \dots, \quad s \leq n_2 < n_1,$$

$$\dots$$

$$f_{k-2}(x) - \frac{a_{k-2,n_{k-2}}}{b_s} x^{n_{k-2}-s} g(x) = f_{k-1}(x) = a_{k-1,n_{k-1}} x^{n_{k-1}} + \dots, \quad s \leq n_{k-1} < n_{k-2},$$

$$f_{k-1}(x) - \frac{a_{k-1,n_{k-1}}}{b_s} x^{n_{k-1}-s} g(x) = f_k(x) = a_{k,n_k} x^{n_k} + \dots, \quad \begin{cases} f_k(x) = 0 \text{ или} \\ n_k < s, \quad n_k < n_{k-1}. \end{cases}$$

Складывая все эти равенства и сокращая, получаем

$$f(x) - \left(\frac{a_n}{b_s} x^{n-s} + \dots + \frac{a_{k-1,n_{k-1}}}{b_s} x^{n_{k-1}-s} \right) g(x) = f_k(x),$$

т. е.

$$f(x) = q(x)g(x) + r(x),$$

где

$$q(x) = \frac{a_n}{b_s} x^{n-s} + \dots + \frac{a_{k-1,n_{k-1}}}{b_s} x^{n_{k-1}-s},$$

$$\underline{r(x) = f_k(x)}, \quad r(x) = 0 \text{ или } \deg(r(x)) < s = \deg g(x).$$

Если $f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x)$, при этом $r(x), r'(x)$ или равны нулю, или имеют степень, меньшую чём $\deg g(x) = s$, то

$$g(x)(q(x) - q'(x)) = r'(x) - r(x).$$

Если $q(x) - q'(x) \neq 0$, то получаем противоречие, поскольку степень левой части $\geq \deg g(x)$, а многочлен в правой части или ненулевой, или его степень $< \deg g(x)$. Итак, $q(x) = q'(x)$, и поэтому $r'(x) = r(x)$. \square

Замечание 3.1.9. Если P — подполе поля P' (например, $P = \mathbb{R} \subset \mathbb{C} = P'$), $f(x), g(x) \in P[x] \subseteq P'[x]$, $f(x) = g(x)q(x) + r(x)$ — деление с остатком в кольце многочленов $P'[x]$, то $q(x), r(x) \in P[x]$.

Задача 3.1.10. Найти все автоморфизмы кольца многочленов $\mathbb{R}[x]$.

Упражнение 3.1.11. Если F — поле, то группа всех автоморфизмов кольца $F[x]$, оставляющих на месте элементы из F , состоит из подстановок

$$x \rightarrow ax + b, \quad a, b \in F, \quad a \neq 0$$

(т. е. $f(x) \mapsto f(ax + b)$).

Трудная задача 3.1.12 (Абъянкар—Мох). Если многочлены $f(x), g(x) \in \mathbb{C}[x]$ порождают всё кольцо многочленов $\mathbb{C}[x]$, то либо степень многочлена f делит степень многочлена g , либо наоборот. Хотелось бы иметь простое комбинаторное доказательство этого утверждения.

3.2. Делимость в кольце многочленов $P[x]$

Пусть $f(x), \varphi(x) \in P[x]$, $\varphi(x) \neq 0$. Будем говорить, что многочлен $f(x)$ делится на $\varphi(x)$, если $f(x) = \varphi(x)q(x)$ (т. е. остаток $r(x)$ при делении на $\varphi(x)$ равен нулю).

Замечание 3.2.1. Совокупность $\varphi(x)P[x] = \{\varphi(x)f(x) \mid f(x) \in P[x]\}$ всех многочленов, делящихся на $\varphi(x)$, является идеалом в кольце $P[x]$ (называемым главным идеалом, порождённым $\varphi(x)$).

Отметим ряд свойств делимости многочленов.

Лемма 3.2.2. Если $f(x)$ делится на $g(x)$, $g(x)$ делится на $h(x)$, то $f(x)$ делится на $h(x)$.

Доказательство. Действительно, если $f(x) = g(x)q(x)$, $g(x) = h(x)\tilde{q}(x)$, то $f(x) = h(x)\tilde{q}(x)q(x)$. \square

Лемма 3.2.3. Если $f(x)$ и $g(x)$ делятся на $h(x)$, то $f(x) + g(x)$, $f(x) - g(x)$ делятся на $h(x)$.

Доказательство. Действительно, если $f(x) = h(x)q(x)$, $g(x) = h(x)\tilde{q}(x)$, то $f(x) \pm g(x) = h(x)(q(x) \pm \tilde{q}(x))$. \square

Лемма 3.2.4. Если многочлен $f(x)$ делится на $h(x)$, $g(x) \in P[x]$, то $f(x)g(x)$ делится на $h(x)$.

Доказательство. Действительно, если $f(x) = h(x)q(x)$, то $f(x)g(x) = h(x)(q(x)g(x))$. \square

Лемма 3.2.5. Если $f_1(x), \dots, f_k(x)$ делятся на $h(x)$, $g_1(x), \dots, g_k(x) \in P[x]$, то $f_1(x)g_1(x) + \dots + f_k(x)g_k(x)$ делится на $h(x)$.

Доказательство. Действительно, это вытекает из лемм 3.2.4 и 3.2.3. \square

Лемма 3.2.6. Если $0 \neq c \in P$, то любой многочлен $f(x) \in P[x]$ делится на c .

Доказательство. Действительно, $f(x) = c(c^{-1}f(x))$. \square

Лемма 3.2.7. Если $f(x)$ делится на $\varphi(x)$ и $0 \neq c \in P$, то $f(x)$ делится на $c\varphi(x)$.

Доказательство. Действительно, если $f(x) = \varphi(x)q(x)$, то $f(x) = (c\varphi(x))(c^{-1}q(x))$. \square

Лемма 3.2.8. Многочлены вида $cf(x)$, $0 \neq c \in P$, и только они являются делителями многочлена $f(x)$, имеющими степень $\deg f(x)$.

Лемма 3.2.9. Многочлен $f(x)$ делится на $g(x)$ и $g(x)$ делится на $f(x)$ тогда и только тогда, когда $g(x) = cf(x)$, $0 \neq c \in P$.

Лемма 3.2.10. Многочлены $f(x)$ и $cf(x)$, $0 \neq c \in P$, обладают одинаковым запасом делителей в кольце $P[x]$.

3.3. Наибольший общий делитель двух многочленов

Пусть $f(x), g(x) \in P[x]$. Многочлен $d(x) \in P[x]$ называется наибольшим общим делителем (Н.О.Д.) многочленов $f(x)$ и $g(x)$, если:

- ✓ 1) $d(x)$ — общий делитель многочленов $f(x)$ и $g(x)$ (т. е. $f(x) = d(x)q(x)$, $g(x) = d(x)\tilde{q}(x)$);
- ✓ 2) для любого общего делителя $d'(x)$ многочленов $f(x)$ и $g(x)$ многочлен $d(x)$ делится на $d'(x)$.

Обозначение: $d(x) = \text{НОД}(f(x), g(x))$.

Замечание 3.3.1. Из 2) следует, что $\deg d(x) \geq \deg d'(x)$, т. е. что $d(x)$ — общий делитель наибольшей степени. Правда, нам ещё надо установить существование НОД в нашем смысле.

Теорема 3.3.2 (алгоритм Евклида). Для любых $f(x), g(x) \in P[x]$:

- 1) существует наибольший общий делитель $d(x)$ многочленов $f(x)$ и $g(x)$;
- 2) $d(x) = \text{НОД}(f(x), g(x))$ находится по процедуре последовательного деления, восходящей к Евклиду;
- 3) наибольший делитель $d(x)$ определён однозначно с точностью до ненулевой константы $0 \neq c \in P$.

Доказательство. 1), 2) Рассмотрим процедуру Евклида:

$$f(x) = g(x)q_1(x) + r_1(x), \quad \deg r_1(x) < \deg g(x);$$

$$g(x) = r_1(x)q_2(x) + r_2(x), \quad \deg r_2(x) < \deg r_1(x);$$

$$r_1(x) = r_2(x)q_3(x) + r_3(x), \quad \deg r_3(x) < \deg r_2(x);$$

...

$$r_{k-3}(x) = r_{k-2}(x)q_{k-1}(x) + r_{k-1}(x), \quad \deg r_{k-1}(x) < \deg r_{k-2}(x);$$

$$r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x), \quad \deg r_k(x) < \deg r_{k-1}(x);$$

$$r_{k-1}(x) = r_k(x)q_{k+1}(x).$$

а) Поднимаясь последовательно вверх, мы видим, что $r_k(x)$ — общий делитель многочленов $g(x)$ и $f(x)$.

б) Если $d'(x)$ — общий делитель многочленов $f(x)$ и $g(x)$, то, опускаясь последовательно вниз, мы видим, что $d'(x)$ — делитель многочлена $d(x)$.

3) Если $d(x)$ и $d'(x)$ — два наибольших общих делителя, то они делятся друг на друга, и поэтому $d'(x) = cd(x)$, $0 \neq c \in P$. Ясно, что если $d(x)$ — наибольший общий делитель и $0 \neq c \in P$, то $cd(x)$ — также наибольший общий делитель. \square

Теорема 3.3.3 (о выражении наибольшего общего делителя через исходные многочлены). Если $f(x), g(x) \in P[x]$ и $d(x) = \text{НОД}(f(x), g(x))$, то существуют многочлены $u(x), v(x) \in P[x]$ такие, что

$$d(x) = f(x)u(x) + g(x)v(x)$$

(если при этом $\deg f(x) > 0$, $\deg g(x) > 0$, то можно считать, что

$$\deg u(x) < \deg g(x),$$

$$\deg v(x) < \deg f(x);$$

это позволяет искать многочлены $u(x), v(x)$ с неопределёнными коэффициентами).

Доказательство. Существование таких многочленов $u(x), v(x)$ следует из алгоритма Евклида нахождения $d(x) = r_k(x)$. Мы выражаем последовательно $r_k(x)$ сначала через $r_{k-2}(x)$ и $r_{k-1}(x)$, потом, подставляя выражение $r_{k-1}(x)$ через $r_{k-3}(x)$ и $r_{k-2}(x)$, через $r_{k-3}(x)$ и $r_{k-2}(x)$ и, завершая подъём, через $g(x)$ и $f(x)$.

Если найдены «плохие» $u(x)$ и $v(x)$, пусть, например, $\deg u(x) \geq \deg g(x)$, то $u(x) = g(x)q(x) + r(x)$, и поэтому $d(x) = f(x)r(x) + g(x)[v(x) + f(x)q(x)]$. Из сравнения степеней следует, что $\deg(v(x) + f(x)q(x)) < \deg f(x)$, поскольку $\deg(f(x)r(x)) < \deg f(x) + \deg g(x)$, $\deg d(x) \leq \deg f(x)$, $\deg d(x) \leq \deg g(x)$. \square

3.4. Взаимно простые многочлены

Многочлены $f(x), g(x) \in K[x]$ из кольца многочленов $K[x]$ над полем K называютсѧ *взаимно простыми*, если их наибольший делитель $d(x)$ равен 1 (то есть их общие делители — это лишь ненулевые многочлены нулевой степени $0 \neq c \in K$).

Теорема 3.4.1. Многочлены $f(x), g(x) \in K[x]$ взаимно просты тогда и только тогда, когда существуют такие многочлены $u(x), v(x) \in K[x]$, что

$$f(x)u(x) + g(x)v(x) = 1.$$

Доказательство. 1) Если многочлены $f(x)$ и $g(x)$ взаимно просты, то для их наибольшего делителя $d(x)$ имеем равенство $d(x) = 1$. Принимая во внимание выражение многочлены $d(x)$ через $f(x)$ и $g(x)$, получаем, что для некоторых $u(x), v(x) \in K[x]$

$$f(x)u(x) + g(x)v(x) = 1.$$

2) Если для $u(x), v(x) \in K[x]$ имеем

$$f(x)u(x) + g(x)v(x) = 1,$$

то любой общий делитель многочленов $f(x)$ и $g(x)$ является делителем многочлена 1. Таким образом,

$$\text{НОД}(f(x), g(x)) = 1,$$

другими словами, многочлены $f(x)$ и $g(x)$ взаимно просты. \square

Замечание 3.4.2. Многочлены $f(x)$ и $g(x)$ взаимно просты тогда и только тогда, когда

$$K[x]f(x) + K[x]g(x) = K[x]$$

(идеал кольца $K[x]$, порождённый многочленами $f(x)$ и $g(x)$, совпадает со всем кольцом многочленов $K[x]$).

Теорема 3.4.3 (основные свойства взаимно простых многочленов). Пусть $f(x), g(x), \varphi(x), \psi(x) \in K[x]$.

- 1) Если $(f, \varphi) = 1$, $(f, \psi) = 1$, то $(f, \varphi\psi) = 1$.
- 2) Если fg делится на φ и $(f, \varphi) = 1$, то g делится на φ .
- 3) Если f делится на φ и делится на ψ , $(\varphi, \psi) = 1$, то f делится на $\varphi\psi$.

Доказательство. 1) Пусть $fu + \varphi v = 1$ для $u(x), v(x) \in K[x]$. Умножая это равенство на ψ , получаем:

$$f(u\psi) + (\varphi\psi)v = \psi.$$

Отсюда следует, что любой общий делитель многочленов f и $\varphi\psi$ является делителем многочлена ψ . Но многочлены f и ψ взаимно просты, таким образом, $(f, \varphi\psi) = 1$.

2) Пусть для $u(x), v(x) \in K[x]$ имеем

$$fu + \varphi v = 1.$$

Умножив это равенство на $g(x)$, получим

$$(fg)u + \varphi(gv) = g,$$

и поэтому многочлен g делится на φ , поскольку оба слагаемых в левой части делятся на φ .

(3) Пусть $f = \varphi q$, где $q(x) \in K[x]$. Так как $f = \varphi q$ делится на ψ и $(\varphi, \psi) = 1$; то в силу 2) $q = \psi \chi$, где $\chi(x) \in K[x]$. Итак: $f = \varphi q = (\varphi \psi) \chi$. \square

Замечание 3.4.4. Определив наибольший общий делитель

$$d(x) = \text{НОД}(f_1(x), \dots, f_s(x))$$

многочленов $f_1(x), \dots, f_s(x) \in K[x]$, $s \geq 1$, как такой делитель этих многочленов $f_1(x), \dots, f_s(x)$, который делится на любой их общий делитель, получаем, проводя индукцию по s , что

$$d(x) = \text{НОД}(f_s(x), \text{НОД}(f_1(x), \dots, f_{s-1}(x)))$$

Упражнение 3.4.5. Если

$$f(x) = x(x-1), g(x) = x(x-2), h(x) = (x-1)(x-2) \in \mathbb{R}[x],$$

то

$$(f, g) = x, \quad (f, h) = (x-1), \quad (g, h) = (x-2), \quad (f, g, h) = 1. \quad \square$$

Замечание 3.4.6. Полностью аналогично в кольце \mathbb{Z} целых чисел устанавливается алгоритм деления с остатком ($n = mq + r$, $r = 0$ или $0 < r < |m|$) и алгоритм Евклида для нахождения наибольшего общего делителя $d = \text{НОД}(m, n)$ (с возможностью выражения в виде $d = mu + nv$, $u, v \in \mathbb{Z}$).

Аналогия объясняется тем, что кольцо \mathbb{Z} целых чисел (с функцией $N(n) = |n|$ для $n \in \mathbb{Z}$) и кольцо $P[x]$ многочленов (с функцией $N(f(x)) = \deg f(x)$ для $f(x) \in P[x]$) являются евклидовыми кольцами, т. е. коммутативными кольцами R с 1 без делителей нуля с функцией $N: R \setminus \{0\} \rightarrow \mathbb{N}$ такой, что $N(ab) \geq N(a)$ и для всех $a, b \in R$, $b \neq 0$, существуют $q, r \in R$ такие, что $a = bq + r$, где $r = 0$ или $N(r) < N(b)$. Поэтому в евклидовых кольцах имеет место алгоритм Евклида нахождения $d = \text{НОД}(a, b)$ и его представления в виде $d = au + bv$, $u, v \in R$. Последнее означает, что евклидово кольцо R является кольцом главных идеалов, т. е. каждый идеал $I \triangleleft R$ кольца R является главным, т. е. имеет вид $I = Ra$, $a \in R$. Действительно, если $0 \neq I \triangleleft R$ и a — ненулевой элемент в I с наименьшим значением $N(a)$, то, конечно, $Ra \subseteq I$, и для любого элемента $t \in I$ из его представления в виде $t = aq + r$, где $r = 0$ или $N(r) < N(a)$, следует, что $r = t - aq \in I$, но это противоречит выбору элемента a в I ; итак, $r = 0$; т. е. $t = aq \in Ra$; таким образом, $I = Ra$ — главный идеал.

Для любых двух элементов $a, b \in R$ кольца главных идеалов R наименьший идеал I , содержащий элементы a и b , $I = Ra + Rb = \{ra + sb \mid r, s \in R\}$, имеет вид $I = Rd$, $d \in R$, т. е. $Ra + Rb = Rd$. Но тогда $a = rd$, $b = sd$, $au + bv = d$, $r, s, u, v \in R$. Таким образом, d — общий делитель элементов a и b . Если d' — другой общий делитель элементов a и b , $a = d'q_1$, $b = d'q_2$, то $d = au + bv = d'(q_1u + q_2v)$. Итак, $d = \text{НОД}(a, b)$.

Упражнение 3.4.7.

- 1) Если $a, b, s, t \in \mathbb{Z}$ и $1 = sa + tb$, то $\text{НОД}(a, b) = 1$.
- 2) Если $m, n \in \mathbb{N}$, $\text{НОД}(m, n) = 1$ и mn — квадрат, то m также квадрат.

Задача 3.4.8. Пусть R — коммутативное кольцо без делителей нуля. Кольцо многочленов $R[x]$ является кольцом главных идеалов тогда и только тогда, когда R — поле.

Задача 3.4.9. Докажите, что над евклидовой областью любая квадратная матрица с определителем 1 является произведением элементарных матриц.

Замечание 3.4.10. В алгоритме Евклида можно для удобства делимое и делитель на каждом шаге умножать на любые ненулевые числа (при этом мы не заботимся о точном вычислении коэффициентов в частных $q_i(x)$).

Пример 3.4.11. Найти $\text{НОД}(f(x), g(x))$, где

$$\begin{aligned} f(x) &= 2x^4 + 2x^3 + x^2 - x - 1, \\ g(x) &= 3x^4 + 2x^2 - x + 2. \end{aligned}$$

Решение. $3f(x) = g(x)q_1(x) + r_1(x)$, где $q_1(x) = 2$, $r_1(x) = 6x^3 - x^2 - x - 7$. Делим $2g(x)$ на $r_1(x)$:

$$\begin{array}{r|l} 6x^4 + 0x^3 + 4x^2 - 2x + 4 & 6x^3 - x^2 - x - 7 \\ \hline 6x^4 - x^3 - x^2 - 7x & x : 1 \\ \hline x^3 + 5x^2 + 5x + 4 & \\ \hline 6x^3 + 30x^2 + 30x + 24 & \\ \hline 6x^3 - x^2 - x - 7 & \\ \hline 31x^2 + 31x + 31 & \end{array}$$

Многоточием ... отмечено место, в котором мы произвели домножение на 6 (соответственно многоточие : показывает, что мы не находим точные коэффициенты для $q_2(x)$). Таким образом,

$$g(x) = r_1(x)q_2(x) + r_2(x),$$

где с точностью до ненулевого множителя $r_2(x) = x^2 + x + 1$. Далее,

$$\begin{array}{r|l} 6x^3 - x^2 - x - 7 & x^2 + x + 1 \\ \hline 6x^3 + 6x^2 + 6x & 6x - 7 \\ \hline -7x^2 - 7x - 7 & \\ \hline -7x^2 - 7x - 7 & \\ \hline 0 & \end{array}$$

То есть $r_1(x)$ делится нацело на $r_2(x)$. Итак,

$$\text{НОД}(f(x), g(x)) = x^2 + x + 1.$$

Упражнение 3.4.12. Наибольший общий делитель $d(x)$ многочленов

$$f(x) = 3x^5 - 4x^4 + x^3 - 3x^2 + 4x - 1$$

и

$$g(x) = 3x^5 + 5x^4 + x^3 - x^2 - 3x + 1$$

представить в виде

$$d(x) = f(x)u(x) + g(x)v(x),$$

где $u(x)$, $v(x)$ — многочлены степеней, меньших чем степени многочленов $g(x)$ и $f(x)$ соответственно.

Решение. Сначала с помощью алгоритма Евклида находим

$$d(x) = 3x^3 + 2x^2 + 2x - 1,$$

при этом

$$f_1(x) = \frac{f(x)}{d(x)} = x^2 - 2x + 1,$$

$$g_1(x) = \frac{g(x)}{d(x)} = x^2 + x - 1.$$

Ищем многочлены $u(x)$ и $v(x)$ такие, что

$$1 = f_1(x)u(x) + g_1(x)v(x). \quad (*)$$

(*)

Так как степени многочленов $u(x)$ и $v(x)$ должны быть меньше двух, то $u(x) = ax + b$, $v(x) = cx + d$, где $a, b, c, d \in \mathbb{R}$. Приравнивая в (*) коэффициенты при одинаковых степенях переменной x , получаем систему линейных уравнений для a, b, c, d . Решая эту систему, получаем, что $a = 3$, $b = 5$, $c = -3$, $d = 4$. Итак,

$$d(x) = 3x^3 + 2x^2 + 2x - 1 = f(x)(3x + 5) + g(x)(-3x + 4).$$

Задача 3.4.13. Пусть $a, b \in \mathbb{N}$, $a > b$. Покажите, что если для того, чтобы вычислить $\text{НОД}(a, b)$, алгоритм Евклида требует n шагов, то $a \geq f_{n+2}$ и $b \geq f_{n+1}$. Если же $a = f_{n+2}$ и $b = f_{n+1}$, то алгоритм Евклида требует ровно n шагов (и $\text{НОД}(a, b) = 1$). Здесь f_{n+2}, f_{n+1} — числа Фибоначчи (см. ??).

Задача 3.4.14. Пусть R — коммутативное кольцо с 1 без делителей нуля. Кольцо многочленов $R[x]$ является кольцом главных идеалов тогда и только тогда, когда R — поле.

Задача 3.4.15. Подкольцо $\{x + iy\sqrt{3} \mid x, y \in \mathbb{Z}\}$ в поле \mathbb{C} комплексных чисел не имеет делителей нуля, но не является евклидовым кольцом.

348

~~KB *~~ 3.5. Алгоритм Евклида и цепные дроби

Определение 3.5.1. Коммутативное кольцо R без делителей нуля с функцией $d: R \rightarrow \mathbb{N} \cup \{-\infty\}$ называется евклидовым кольцом, если для любых $a, b \in R$, где $b \neq 0$, существуют такие $q, r \in R$, что

$$a = qb + r, \quad d(r) < d(b).$$

Пример 3.5.2:

- 1) $R = \mathbb{Z}$, $d(a) = |a|$. Если потребовать $r \geq 0$, то остаток r определён однозначно.
- 2) $R = K[x]$, где K — поле, и $d(f) = \deg(f)$ для $f \in K[x]$, $d(0) = -\infty$.
- 3) $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, $d(a + bi) = a^2 + b^2 = |a + bi|^2$.
- 4) R — поле, $d(a) = 1$ при $a \neq 0$ и $d(0) = 0$.

Рассмотрим схему алгоритма Евклида для $r_0, r_1 \in R$:

$$r_0 = r_1 q_1 + r_2$$

$$r_{i-1} = r_i q_i + r_{i+1}$$

...

$$r_{l-2} = r_{l-1} q_{l-1} + r_l$$

$$r_{l-1} = r_l q_l.$$

Тогда в поле частных $Q(R)$ кольца R :

$$\begin{aligned} r_0 r_1^{-1} &= \frac{r_0}{r_1} = \frac{q_1 r_1 + r_2}{r_1} = q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{\frac{r_2}{r_1}} = \dots = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_l}}} \end{aligned}$$

(обозначение: $\left[q_1; \frac{1}{q_2}, \dots, \frac{1}{q_l} \right]$). Полученное выражение называется выражением элемента $\frac{r_0}{r_1} \in Q(R)$ в виде обыкновенной конечной непрерывной (или цепной) дроби в поле частных $Q(R)$ кольца R .

Например, в $\mathbb{Q} = Q(\mathbb{Z})$:

$$\frac{62}{19} = \left[3; \frac{1}{3}, \frac{1}{1}, \frac{1}{4} \right], \quad \frac{126}{35} = \left[3; \frac{1}{1}, \frac{1}{1}, \frac{1}{2} \right].$$

~~3.6.~~ Цепные дроби и аппроксимация

Выражение вида

$$\alpha = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \dots}}} = \left[a_0; \frac{b_1}{a_1}, \frac{b_2}{a_2}, \dots \right]$$

называется *непрерывной* (или *цепной*) дробью (мы предполагаем, что $a_k \neq 0$). Если все $b_i = 1$, то непрерывная дробь называется *обыкновенной*.

Замечание 3.6.1. Для обыкновенной цепной дроби

$$\left[a_0; \frac{1}{a_1}, \frac{1}{a_2}, \dots \right]$$

её *подходящие дроби*

$$\frac{p_k}{q_k} = \left[a_0; \frac{1}{a_1}, \dots, \frac{1}{a_k} \right]$$

могут быть найдены из соотношений

$$p_0 = a_0, \quad p_{-1} = 1, \quad q_0 = 1, \quad q_{-1} = 0,$$

$$p_k = a_k p_{k-1} + p_{k-2}, \quad q_k = a_k q_{k-1} + q_{k-2}.$$

Действительная цепная дробь

$$\alpha = \left[a_0; \frac{b_1}{a_1}, \dots \right]$$

называется *сходящейся*, если существует предел

$$\alpha = \lim_{n \rightarrow \infty} \frac{P_n}{Q_n},$$

где

$$\frac{P_n}{Q_n} = \left[a_0; \frac{b_1}{a_1}, \dots, \frac{a_n}{b_n} \right]$$

Замечание 3.6.2. Нетрудно показать, что каждое положительное число $\alpha \in R$ можно разложить единственным образом на обыкновенную сходящуюся цепную дробь с натуральными элементами (более того, любая обыкновенная цепная дробь с натуральными элементами сходится). Например, целая часть числа $\sqrt{41}$ равна

$$[\sqrt{41}] = 6, \quad \sqrt{41} = 6 + \frac{1}{a_1},$$

$$a_1 = \frac{1}{\sqrt{41} - 6} = \frac{6 + \sqrt{41}}{5}, \quad [a_1] = 2, \quad a_1 = 2 + \frac{1}{a_2},$$

$$a_2 = \frac{1}{a_1 - 2} = \frac{4 + \sqrt{41}}{5} = 2 + \frac{1}{a_3},$$

$$a_3 = \frac{1}{a_2 - 2} = 12 + \frac{1}{a_4},$$

$$a_4 = \frac{1}{a_3 - 12} = \frac{6 + \sqrt{41}}{5} = a_1,$$

и далее коэффициенты a_i периодически повторяются. Поэтому

$$\sqrt{41} = [6; \frac{1}{2}, \frac{1}{2}, \frac{1}{12}, \frac{1}{2}, \frac{1}{2}, \frac{1}{12}, \frac{1}{2}, \frac{1}{2}, \frac{1}{12}, \dots].$$

Справедливо более общее утверждение: обыкновенная цепная дробь числа α периодична тогда и только тогда, когда α — квадратичная иррациональность.

Если элементы обыкновенной цепной дроби α — положительные действительные числа, $\frac{p_k}{q_k}$ — её подходящая дробь, то

$$\left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k q_{k+1}}.$$

Например, для

$$\frac{163}{59} = [2; \frac{1}{1}, \frac{1}{3}, \frac{1}{4}, \frac{1}{1}, \frac{1}{2}]$$

последняя подходящая дробь — это $\frac{163}{59}$, а предпоследняя — это $\frac{58}{21}$, поэтому

$$\left| \frac{163}{59} - \frac{58}{21} \right| < \frac{1}{59 \cdot 2} < 10^{-3}.$$

Эти соображения лежат в основе диофантовых приближений, а их аналоги для кольца многочленов от одной переменной — в основе аппроксимации Паде.

Упражнение 3.6.3.

1) $e = [1; \frac{1}{1}, \frac{1}{2}, \frac{1}{1}, \frac{1}{1}, \frac{1}{4}, \frac{1}{1}, \frac{1}{1}, \frac{1}{6}, \frac{1}{1}, \frac{1}{1}, \frac{1}{8}, \dots]$.

2) $\frac{1 + \sqrt{5}}{2} = [1; 1, 1, 1, \dots].$

3) Пусть $a, b \in \mathbb{R}$, $a \neq 0$, $b \neq 0$, $a^2 - 4b > 0$ и непрерывные дроби $\alpha = [a; \frac{-b}{a}, \frac{-b}{a}, \dots]$ и $\beta = [0; \frac{b}{a}, \frac{-b}{a}, \dots]$ сходятся. Тогда α и β — корни многочлена $x^2 - ax + b$.

4) Покажите, что

$$\frac{1-x}{1-5x+6x^2} = [0; \frac{1}{1}, \frac{-4x}{1}, \frac{-2x}{-4}, \frac{-12x}{-2}],$$

5) Для e^x Эйлер получил разложение

$$e^x = [0; \frac{1}{1}, \frac{-2x}{2+x}, \frac{x^2}{6}, \frac{x^2}{10}, \dots, \frac{x^2}{4n+2}, \dots],$$

сходящееся для любого $x \in \mathbb{C}$.

Трудная задача 3.6.4. Привести пример кольца главных идеалов, не являющегося евклидовым кольцом.

Замечание 3.6.5. В кольце без делителей нуля $\mathbb{Z}[x]$ для многочленов $7x^3 + 1$ и $2x$ имеем

$$\text{НОД}(7x^3 + 1, 2x) = 1,$$

но нет многочленов $u(x), v(x) \in \mathbb{Z}[x]$ таких, что

$$(7x^3 + 1)u(x) + 2xv(x) = 1.$$

Задача 3.6.6. Доказать, что $x^n - 1$ делится на $x^m - 1$ тогда и только тогда, когда n делится на m .

Задача 3.6.7. Доказать, что $(x^m - 1, x^n - 1) = x^{(m,n)} - 1$ для $m, n \in \mathbb{N}$.

Указание. Применить алгоритм Евклида (или доказать, что для $z \in \mathbb{C}$ $z^m = 1, z^n = 1$ тогда и только тогда, когда $z^{(m,n)} = 1$).

Теорема 3.6.8 (китайская теорема об остатках для многочленов). Пусть K — поле, $f_1(x), \dots, f_k(x) \in K[x]$, $\text{НОД}(f_1(x), \dots, f_k(x)) = 1$, $g_1(x), \dots, g_k(x) \in K[x]$. Тогда существует многочлен $h(x) \in K[x]$ такой, что

$$h(x) \equiv g_i(x) \pmod{f_i(x)}, \quad i = 1, \dots, k,$$

причём этот многочлен определён однозначно по модулю многочлена $f(x) = f_1(x) \dots f_k(x)$.

Доказательство. Так как $(f_i, F_i = f/f_i) = 1$, то

$$f_i(x)u_i(x) + F_i(x)v_i(x) = 1$$

для некоторых $u_i(x), v_i(x) \in K[x]$. Ясно, что

$$F_i(x)v_i(x) \equiv 1 \pmod{f_i}$$

и

$$F_j(x)v_i(x) \equiv 0 \pmod{f_j} \text{ для } j \neq i.$$

Существование $h(x)$. Пусть

$$h(x) = \sum g_i(x)v_i(x)F_i(x).$$

Тогда

$$h(x) \equiv g_i(x)v_i(x)F_i(x) \pmod{f_i(x)} \equiv g_i(x) \pmod{f_i(x)}.$$

Единственность $h(x)$. Если два многочлена $h_1(x)$ и $h_2(x)$ удовлетворяют условиям теоремы, то $h_1 - g_i$ и $h_2 - g_i$ делятся на f_i , поэтому $h_1 - h_2 = (h_1 - g_i) - (h_2 - g_i)$ делится на f_i , $i = 1, \dots, k$. Так как $\text{НОД}(f_1(x), \dots, f_k(x)) = 1$, то многочлен $h_1(x) - h_2(x)$ делится на $f(x) = f_1(x) \dots f_k(x)$. \square

Замечание 3.6.9. Китайская теорема об остатках для кольца многочленов над конечным полем $F_p[x]$ и малая теорема Ферма составляют основу алгоритма Берлекампа разложения целочисленного многочлена, свободного от квадратов по модулю p , в произведение неприводимых многочленов над полем F_p .

3.7. Основная теорема

*алгебры комплексных чисел
(теорема Гаусса, 1799 г.)*

Теорема 3.7.1. Если $f(x) \in \mathbb{C}[x]$, $\deg f(x) \geq 1$, то существует корень $c \in \mathbb{C}$ многочлена $f(x)$, т. е. $f(c) = 0$.

Доказательство.

Шаг 1 (существование абсолютного минимума вещественнонозначной функции $|f(x)|$ на комплексных числах \mathbb{C}). Напомним, что

$$|z_1 z_2| = |z_1| |z_2|$$

и

$$|z_1| - |z_2| \leq |z_1 + z_2| \leq |z_1| + |z_2|$$

для $z_1, z_2 \in \mathbb{C}$.

Лемма 3.7.2. Если $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$, $a_i \in \mathbb{C}$, $n \geq 1$, то найдётся радиус $0 < A \in \mathbb{R}$ такой, что

$$|f(z)| > |f(0)| \quad (\text{для всех } z \in \mathbb{C}, |z| > A)$$

(это означает, что вне круга радиуса A с центром в 0 значение функции $|f(x)|$ превосходит $|f(0)| = |a_0|$).

Доказательство. Пусть $0 \neq z \in \mathbb{C}$. Тогда

$$f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0 = z^n \left(1 + \frac{a_{n-1}}{z} + \dots + \frac{a_0}{z^n}\right),$$

и поэтому

$$\begin{aligned} |f(z)| &= |z|^n \left|1 + \left(\frac{a_{n-1}}{z} + \dots + \frac{a_0}{z^n}\right)\right| \geq \\ &\geq |z|^n \left(1 - \left|\frac{a_{n-1}}{z} + \dots + \frac{a_0}{z^n}\right|\right) \geq \\ &\geq |z|^n \left(1 - \frac{|a_{n-1}|}{|z|} - \dots - \frac{|a_0|}{|z|^n}\right) = \varphi(|z|), \end{aligned}$$

где

$$\varphi(t) = t^n \left(1 - \frac{|a_{n-1}|}{t} - \dots - \frac{|a_0|}{t^n}\right) \quad \text{для } t \in \mathbb{R}.$$

Ясно, что $\lim_{t \rightarrow +\infty} \varphi(t) = +\infty$, и поэтому для любого C (например, для $C = |f(0)| = |a_0|$) найдётся $\mathbb{R} \ni A > 0$ такое, что для $t > A$ имеем $\varphi(t) > C$. Итак, если $|z| = t > A$, то

$$|f(z)| \geq \varphi(|z|) = \varphi(t) > C = |f(0)| = |a_0|. \quad \square$$

Так как функция $|f(z)|: \mathbb{C} \rightarrow \mathbb{R}$ непрерывна как композиция двух непрерывных функций $\mathbb{C} \rightarrow \mathbb{C}$, $z \mapsto f(z)$, $\mathbb{C} \rightarrow \mathbb{R}$, $w \mapsto |w|$ (или если $z = u + vi$, $(u, v) \in \mathbb{R}^2$, то $f(z) = \psi_1(u, v) + \psi_2(u, v)i$, где $\psi_1(u, v)$ и $\psi_2(u, v)$ — многочлены с действительными коэффициентами от u, v , и поэтому $|f(z)| = \sqrt{\psi_1(u, v)^2 + \psi_2(u, v)^2}$ — непрерывная функция от (u, v)), то на замкнутом ограниченном множестве (компакте)

$$K = \{z \in \mathbb{C} \mid |z| \leq A\}$$

непрерывная функция $|f(z)|$ достигает своего минимума в точке $z_0 \in K$. В частности, $|f(z_0)| \leq |f(0)| = |a_0|$. Если $z \in \mathbb{C} \setminus K$, т. е. $|z| > A$, то, как мы видели,

$$|f(z_0)| \leq |f(0)| \leq |f(z)|.$$

Таким образом, в точке z_0 достигается абсолютный минимум функции $|f(z)|$ на \mathbb{C} .

Шаг 2. Мы покажем, что $f(z_0) = 0$, т. е. z_0 является корнем многочлена $f(x)$. Действительно, если $f(z_0) \neq 0$, то $|f(z_0)| > 0$ и, как показывает следующая лемма Даламбера, это допущение противоречит тому, что z_0 — абсолютный минимум функции $|f(x)|$.

Лемма 3.7.3 (лемма Даламбера). Пусть $f(x) \in \mathbb{C}[x]$, $\deg f(x) \geq 1$, $f(z_0) \neq 0$ для $z_0 \in \mathbb{C}$. Тогда для любого $\varepsilon > 0$ найдётся такой элемент $y \in \mathbb{C}$, что $|y| < \varepsilon$ и $|f(z_0 + y)| < |f(z_0)|$.

Доказательство. Если $z = z_0 + y$, т. е. $y = z - z_0$, то

$$f(z) = a_0 + a_1z + \dots + a_{n-1}z^{n-1} + z^n = c_0 + c_1y + \dots + c_{n-1}y^{n-1} + c_ny^n,$$

где $c_0 = f(z_0) \neq 0$ (при $y = 0$ имеем $z = z_0$), $c_n = 1$ (как коэффициент при y^n в $(z_0 + y)^n$).

Пусть $k > 0$ — наименьший номер слагаемого, для которого $c_k \neq 0$. Итак,

$$f(z) = c_0 + c_ky^k + c_{k+1}y^{k+1} + \dots + c_ny^n.$$

Основное соображение заключается в том, что в окрестности точки z_0 (т. е. $y = 0$) поведение многочлена определяется первыми двумя членами $c_0 + c_ky^k$.

Сначала пусть y_0 — одно из решений уравнения $c_0 + c_ky^k = 0$ (т. е. $y_0^k = -\frac{c_0}{c_k}$, y_0 — один из k корней из комплексного числа $-\frac{c_0}{c_k}$). Если, далее, $t \in (0, 1) \subseteq \mathbb{R}$, то $c_ky_0^k = -c_0$, и поэтому

$$\begin{aligned} f(z_0 + ty_0) &= c_0 + c_kt^ky_0^k + c_{k+1}t^{k+1}y_0^{k+1} + \dots + c_nt^n y_0^n = \\ &= c_0(1 - t^k) + (c_{k+1}y_0^{k+1} + \dots + c_nt^{n-(k+1)})t^{k+1}. \end{aligned}$$

Если $|c_{k+1}| |y_0|^{k+1} + \dots + |c_n| = M$, то

$$|f(z_0 + ty_0)| \leq |c_0|(1 - t^k) + Mt^{k+1} = |c_0| \left(1 - t^k \left(1 - \frac{Mt}{|c_0|}\right)\right).$$

Выберем $t \in (0, 1)$ достаточно малым, так что $Mt < |c_0|$, $t|y_0| = |ty_0| < \varepsilon$. Тогда $0 < 1 - \frac{Mt}{|c_0|} < 1$, и поэтому

$$|f(z_0 + ty_0)| < |c_0| = |f(z_0)|, \quad |ty_0| < \varepsilon.$$

Таким образом, $y = ty_0$ удовлетворяет утверждению леммы. \square

3.8. Значения и корни многочлена

Пусть K — поле,

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

Если $c \in K$, то элемент

$$f(c) = a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0 \in K$$

назовём значением многочлена $f(x)$ при $x = c$. Таким образом, получаем отображения:

$$f: K \rightarrow K, \quad c \mapsto f(c)$$

(полиномиальная функция, определяемая многочленом $f(x)$);

$$K[x] \rightarrow K, \quad f(x) \mapsto f(c)$$

(ясно, что если $f(x) = g(x)$ в $K[x]$, то $f(c) = g(c)$ для всех $c \in K$).

Лемма 3.8.1. Если в $K[x]$

$$\varphi(x) = f(x) + g(x), \quad \psi(x) = f(x)g(x)$$

и $c \in K$, то

$$\varphi(c) = f(c) + g(c), \quad \psi(c) = f(c)g(c).$$

Таким образом, отображение

$$\Delta_c: K[x] \rightarrow K, \quad f(x) \mapsto f(c),$$

является гомоморфизмом колец (при этом $\text{Кер } \Delta_c = \{f(x) \in K[x] \mid f(c) = 0\} \triangleleft K[x]$; $K[x]/\text{Кер } \Delta_c \cong K$).

Доказательство следует из определения сложения и умножения многочленов в кольце $K[x]$. \square

Элемент $c \in K$ называется корнем многочлена $f(x) \in K[x]$, если $f(c) = 0$.

Теорема 3.8.2 (Безу). Пусть $c \in K$. Остаток от деления многочлена $f(x)$ в кольце $K[x]$ на множитель $x - c$ равен значению $f(c)$ многочлена $f(x)$ при $x = c$.

Доказательство. В силу алгоритма деления

$$f(x) = (x - c)q(x) + r(x),$$

где или $r(x) = 0$, или $\deg r(x) = 0$, и поэтому $r(x) = r \in K$. Итак, $f(x) = (x - c)q(x) + r$, следовательно, $f(c) = (c - c)q(c) + r = r$, и поэтому

$$f(x) = (x - c)q(x) + f(c). \quad \square$$

Следствие 3.8.3. Элемент $c \in K$ является корнем многочлена $f(x) \in K[x]$ тогда и только тогда, когда многочлен $f(x)$ делится на $x - c$. \square

Замечание 3.8.4.

- 1) Если $a, b \in K$, $a \neq 0$, то делимость многочлена $f(x) \in K[x]$ на многочлен $ax + b = a\left(x - \left(-\frac{b}{a}\right)\right)$ равносильна делимости на многочлен $x - c$, $c = -\frac{b}{a}$, и поэтому нахождение корней многочлена $f(x) \in K[x]$ в поле K равносильно нахождению его линейных делителей в кольце $K[x]$.
- 2) Если $c \in K$, $\Delta_c: K[x] \rightarrow K$, $\Delta_c(f) = f(c)$, то

$$\text{Ker } \Delta_c = \{f(x) \in K[x] \mid f(c) = 0\} = (x - c)K[x] = I_c$$

(главный идеал в кольце $K[x]$, порождённый многочленом $x - c$), и поэтому $K[x]/I_c \cong K$.

**Схема (алгоритм) Горнера
(деления многочлена $f(x) \in K[x]$ на линейный многочлен $x - c$, $c \in K$)**

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

$$\begin{aligned} f(x) &= (x - c)q(x) + r, \quad r \in K, \\ q(x) &= b_{n-1} x^{n-1} + \dots + b_1 x + b_0 \in K[x]. \end{aligned}$$

Тогда, приравнивая коэффициенты при $x^n, x^{n-1}, \dots, x, 1$, соответственно получаем

$$\begin{aligned} a_n &= b_{n-1}; \\ a_{n-1} &= b_{n-2} - cb_{n-1}; \\ a_{n-2} &= b_{n-3} - cb_{n-2}; \\ &\dots \\ a_k &= b_{k-1} - cb_k; \\ &\dots \\ a_1 &= b_0 - cb_1; \\ a_0 &= r - cb_0. \end{aligned}$$

Пересчитывая, получаем

$$\begin{aligned} b_{n-1} &= a_n; \\ b_{n-2} &= cb_{n-1} + a_{n-1}; \\ b_{n-3} &= cb_{n-2} + a_{n-2}; \\ &\dots \\ b_{k-1} &= cb_k + a_k; \\ &\dots \\ b_0 &= cb_1 + a_1; \\ r &= cb_0 + a_0. \end{aligned}$$

Таким образом, коэффициенты частного b_{n-1}, \dots, b_1, b_0 и остаток $r = f(c)$ последовательно вычисляются по коэффициентам a_n, \dots, a_1, a_0 и элементу c , если использовать однотипную процедуру

	a_n	a_{n-1}	...	a_{k+1}	a_k	...	a_1	a_0
						↓		
c	b_{n-1}	$b_{n-2} =$ $=cb_{n-1} + a_{n-1}$...	$b_k =$ $=cb_{k+1} + a_{k+1}$	$b_{k-1} =$ $=cb_k + a_k$...	$b_0 =$ $=cb_1 + a_1$	$r =$ $=cb_0 + a_0$
						↑		

Пример 3.8.5. Пусть $f(x) = 2x^4 - x^2 + 3x - 2$, $c = -2$. Тогда

	2	0	-1	3	-2	
-2	2	-4	7	-11	20	

поэтому $f(x) = (x + 2)q(x) + 20$, где $q(x) = (x + 2)(2x^3 - 4x^2 + 7x - 11)$.

Замечание 3.8.6.

- Схема Горнера даёт быстрый алгоритм вычисления значения $r = f(c)$ многочлена $f(x) \in K[x]$ в точке c (минимизируя число умножений).
- Последовательное применение схемы Горнера позволяет построить эффективный алгоритм записи многочлена $f(x)$ в виде формулы Тейлора по степеням $(x - c)$. А именно, при первом применении схемы Горнера крайний правый коэффициент равен $f(c)$, при втором применении крайний справа коэффициент равен $f'(c)$, при третьем — $\frac{f''(c)}{2!}$, и так далее. Таким образом, если $\deg f(x) = n$, то

$$f(x) = f(c) + f'(c)(x - c) + \frac{f''(c)}{2!}(x - c)^2 + \dots + \frac{f^{(n)}(c)}{n!}(x - c)^n$$

(формула Тейлора).

Например, для

$$f(x) = x^4 - 6x^3 - 2x^2 + 5x - 4$$

и $c = 5$ имеем

	1	-6	-2	5	-4	
5	1	-1	-7	-30	-154	$= f(5)$
5	1	4	13	35		$= f'(5)$
5	1	9	58		$= \frac{f''(5)}{2!}$	
5	1	14		$= \frac{f^{(3)}(5)}{3!}$		
	1			$= \frac{f^{(4)}(5)}{4!}$		

Таким образом,

$$f(x) = (x - 5)^4 + 14(x - 5)^3 + 58(x - 5)^2 + 35(x - 5) - 154.$$

3.9. Кратные корни

Пусть $f(x) \in K[x]$, $c \in K$, и c — корень многочлена $f(x)$, т. е. $f(c) = 0$. По теореме Безу многочлен $f(x)$ делится на $x - c$. Возможно, многочлен $f(x)$ делится на более высокие степени многочлена $x - c$. Пусть $k \in \mathbb{N}$ — такое натуральное число, что $f(x)$ делится на $(x - c)^k$, но не делится на $(x - c)^{k+1}$, поэтому

$$f(x) = (x - c)^k \varphi(x),$$

многочлен $\varphi(x) \in K[x]$ уже не делится на $x - c$ (это равносильно тому, что $\varphi(c) \neq 0$). В этом случае число k назовём *кратностью* корня c многочлена $f(x)$, а сам корень c — *k -кратным корнем* многочлена $f(x)$. Если $k = 1$, то корень c называется *простым корнем* многочлена $f(x)$.

3.10. Производные многочленов

В началах вещественного анализа мы видели, что в кратных нулях многочлена его производная обращается в ноль. В случае произвольного поля K производные многочленов также весьма полезны, как мы убедимся, для исследования кратных корней. В случае произвольных полей K (например, конечных полей) использование пределов для введения производной не представляется возможным. Для многочлена

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

определим его *производную* $f'(x)$ *формально*:

$$f'(x) = n a_n x^{n-1} + \dots + 2 a_2 x + a_1 \in K[x].$$

Иногда удобно оператор дифференцирования на кольце многочленов $K[x]$ обозначать через

$$\mathcal{D}: K[x] \rightarrow K[x], \quad \mathcal{D}(f) = f'.$$

Теорема 3.10.1. Оператор дифференцирования

$$\mathcal{D}: K[x] \rightarrow K[x], \quad \mathcal{D}(f) = f',$$

на кольце многочленов обладает следующими свойствами:

1) \mathcal{D} — линейный оператор ($\mathcal{D}(f+g) = \mathcal{D}(f) + \mathcal{D}(g)$, $\mathcal{D}(af) = a\mathcal{D}(f)$ для всех $f, g \in K[x]$, $a \in K$);

2) выполнено правило Лейбница

$$\mathcal{D}(fg) = f \cdot \mathcal{D}(g) + \mathcal{D}(f) \cdot g$$

для всех $f, g \in K[x]$;

3) $\mathcal{D}(x) = 1$.

Доказательство. Ясно, что

$$\mathcal{D}: K[x] \rightarrow K[x], \quad \mathcal{D}(f) = \sum_{k=1}^n k a_k x^{k-1}$$

для

$$f = \sum_{k=0}^n a_k x^k \in K[x], \quad \text{—}$$

линейный оператор на линейном пространстве $K[x]$ над полем K . Также ясно, что $\mathcal{D}(x) = 1$.

Проверим выполнение правила Лейбница. Зафиксируем

$$f = \sum_{k=0}^n a_k x^k \in K[x]$$

и положим

$$U_f = \{g \in K[x] \mid \mathcal{D}(fg) = f\mathcal{D}(g) + \mathcal{D}(f)g\}.$$

Для $h \in K[x]$ рассмотрим линейный оператор

$$L_h: K[x] \rightarrow K[x], \quad L_h(f) = hf$$

(левое умножение на h). Тогда

$$U_f = \text{Ker}(\mathcal{D} \cdot L_f - L_f \cdot \mathcal{D} - L_{\mathcal{D}(f)})$$

является линейным K -подпространством в $K[x]$ (как ядро указанного линейного оператора).

Если $a \in K$, то $\mathcal{D}(a) = 0$ и $\mathcal{D}(fa) = \mathcal{D}(f)a$, поэтому $K \subseteq U_f$.

Если $m \in \mathbb{N}$, то $x^m \in U_f$, поскольку

$$\begin{aligned} \mathcal{D}(fx^m) &= \mathcal{D}\left(\sum_{k=0}^n a_k x^{k+m}\right) = \sum_{k=0}^n a_k \mathcal{D}(x^{k+m}) = \\ &= \sum_{k=0}^n (k+m)a_k x^{k+m-1} = \sum_{k=0}^n m a_k x^{k+m-1} + \sum_{k=1}^n k a_k x^{k-1+m} = f\mathcal{D}(x^m) + \mathcal{D}(f)x^m. \end{aligned}$$

Итак, $U_f = K[x]$, и следовательно, правило Лейбница выполнено для всех $f, g \in K[x]$. \square

Следствие 3.10.2.

1) Оператор дифференцирования

$$\mathcal{D}: K[x] \rightarrow K[x], \quad \mathcal{D}(f) = f'$$

однозначно определён правилами 1)–3).

2) Если $f(x) \in K[x]$ и $m \in \mathbb{N}$, то $(f^m(x))' = m \cdot f^{m-1}(x) \cdot f'(x)$.

- 3) Если $f^{(i)}(x) = (f^{(i-1)}(x))' - i$ -я производная (i раз применяется оператор дифференцирования \mathcal{D} , т. е. оператор \mathcal{D}^i), то $f^{(n)}(x) = n! a_n$ и $f^{(n+1)}(x) = 0$ для

$$f(x) = \sum_{i=0}^n a_i x^i \in K[x]$$

(следовательно, если $\text{char } K = 0$ и $n = \deg f(x)$, то $f^{(n)}(x) \neq 0$).

- 4) Если $f, g \in K[x]$, $i \geq 1$, то

$$(fg)^{(i)} = \sum_{j=0}^i C_i^j f^{(i-j)} g^{(j)},$$

- 5) Пусть $f, g \in K[x]$. Тогда

$$\mathcal{D}[f(g)] = (\mathcal{D}(f))(g) \cdot \mathcal{D}(g)$$

(правило замены).

Лемма 3.10.3. Пусть K — поле, $f = f(x) \in K[x]$ и $f' = 0$. Тогда:

- 1) если $\text{char } K = 0$, то f — константа ($f = a_0 \in K$);
- 2) если $\text{char } K = p \neq 0$, то $f = g(x^p)$ для некоторого многочлена $g \in K[x]$.

Доказательство. Если

$$f(x) = a_n x^n + \dots + a_0 \in K[x]$$

и $f' = 0$, то $ia_i = 0$ для всех $i = 0, 1, \dots, n$.

1) Если $\text{char } K = 0$, то $a_i = 0$ для $i > 0$, и поэтому $f(x) = a_0 \in K$.

2) Если $\text{char } K = p \neq 0$, то $a_i = 0$ для всех i , не делящихся на p , и поэтому

$$f(x) = a_{rp} x^{rp} + \dots + a_p x^p + a_0 = g(x_p),$$

где $g(x) = a_{rp} x^r + \dots + a_p x + a_0$.

Теорема 3.10.4 (формула Тейлора). Пусть K — поле, $\text{char } K = 0$, $f(x) \in K[x]$, $\deg f(x) = n$, $c \in K$. Тогда:

$$f(x) = \frac{f^{(n)}(c)}{n!} (x - c)^n + \dots + \frac{f^{(2)}(c)}{2!} (x - c)^2 + \frac{f'(c)}{1!} (x - c) + f(c).$$

Доказательство. Представим наш многочлен в виде

$$f(x) = \sum_k b_k (x - c)^k$$

(пусть $x = y + c$; записываем многочлен $f(x) = f(y + c)$ как многочлен от y). Далее,

$$f^{(i)} = \sum_k k(k-1)\cdots(k-i+1)b_k (x - c)^{k-i}.$$

При $x = c$ получаем

$$f^{(i)}(c) = i! b_i.$$

Замечание 3.10.5.

- 1) Вычисление коэффициентов в формуле Тейлора можно производить по схеме Горнера (см. с. 43).
- 2) Если K — поле, $\text{char } K \neq 0$, $f(x)$, $\deg(f(x)) = n$,

$$f(x) = a_n x^n + \dots + a_1 x + a_0,$$

то

$$f(x) = b_n(x - c)^n + \dots + b_1(x - c) + b_0, \quad i \in K,$$

однако коэффициенты b_i не могут быть вычислены по формуле Тейлора. Но коэффициенты b_i , $0 \leq i \leq b_{n-1}$ ($b_n = a_n$) можно вычислить, последовательно применяя схему Горнера (см., например, ??).

3.11. Кратные корни многочленов и производные

Пусть K — поле, $f(x) \in K[x]$ и в некотором расширении F поля K , $K \subset F$,

$$f = a(x - c_1)^{k_1} \cdots (x - c_r)^{k_r},$$

где c_1, \dots, c_r — различные корни в поле F , k_1, \dots, k_r — их кратность. Следующая лемма позволяет нам выяснить, когда многочлен $f(x) \in K[x]$ имеет кратный корень в некотором расширении F , не выходя за пределы поля K и не вычисляя корни многочлена f .

Лемма 3.11.1. Пусть K — поле, $f(x) \in K[x]$, $c \in K$, $f(c) = 0$. Тогда c — кратный корень многочлена $f(x)$ (т. е. $f(x)$ делится на $(x - c)^2$) тогда и только тогда, когда $f'(c) = 0$.

Доказательство. Так как $f(c) = 0$, то $f(x) = (x - c)g(x)$, при этом c — кратный корень многочлена $f(x)$ тогда и только тогда, когда $g(c) = 0$. Дифференцируя, получаем

$$f'(x) = (x - c)g'(x) + g(x).$$

При $x = c$ видим, что $f'(c) = 0$ тогда и только тогда, когда $g(c) = 0$. □

Теорема 3.11.2. Пусть K — поле, $f(x) \in K[x]$. Расширение F поля K , $K \subset F$, в котором многочлен $f(x)$ имеет кратный корень, существует тогда и только тогда, когда многочлены $f(x)$ и $f'(x)$ не являются взаимно простыми.

Доказательство. 1) Если многочлен $f(x)$ имеет кратный корень c в расширении F поля K , $K \subset F$, то по лемме 3.11.1 многочлены $f(x)$ и $f'(x)$ имеют общий корень $c \in F$, $f(c) = f'(c) = 0$. Следовательно, $f(x)$ и $f'(x)$ не взаимно просты в $F[x]$ (оба многочлена делятся на $x - c$), а поэтому не являются взаимно простыми и в $K[x]$.

2) Если $f(x)$ и $f'(x)$ не являются взаимно простыми, то они имеют общий корень (корень многочлена $d(x) = \text{НОД}(f(x), f'(x))$, см. ??) в некотором расширении F поля K . Следовательно, в расширении F многочлен $f(x)$ имеет кратный корень. □

Теорема 3.11.3. Пусть $f(x)$ — неприводимый многочлен в $K[x]$. Тогда $f(x)$ не имеет кратных корней ни в каком расширении поля K , кроме случая, когда $f'(x) = 0$. В частности, если $\text{char } K = 0$, то $f(x)$ не имеет кратных корней ни в каком расширении поля K .

Доказательство. 1) В силу теоремы 3.11.2 нам надо показать, что $f(x)$ и $f'(x)$ взаимно просты, кроме того случая, когда $f'(x) = 0$. Так как $f(x)$ — неприводимый многочлен, то $f(x)$ имеет общий множитель, отличный от константы, с другим многочленом $g(x)$, если только $f(x)$ делит $g(x)$. Но $\deg f'(x) < \deg f(x)$ (при условии $f'(x) \neq 0$). Поэтому $f(x)$ и $f'(x)$ не имеют отличных от константы общих множителей (при условии $f'(x) \neq 0$).

2) Если $\text{char } K = 0$, то производная многочлена, отличного от константы, отлична от нуля. \square

Следующее утверждение над полями нулевой характеристики является ключевым в процедуре отделения кратных корней (следствие 3.11.5).

Теорема 3.11.4 (о понижении кратности корня при переходе к производной). Пусть K — поле, $\text{char } K = 0$, $f(x) \in K[x]$, $c \in K$ — корень многочлена $f(x)$ кратности k . Тогда:

- 1) если $k > 1$, то c является $(k-1)$ -кратным корнем производной $f'(x)$;
- 2) если $k = 1$, то c не является корнем производной $f'(x)$.

Доказательство. Пусть $f(x) = (x - c)^k \varphi(x)$, $k \geq 1$, $\varphi(x) \in K[x]$, $\varphi(x)$ не делится на многочлен $x - c$. Дифференцируя, получаем

$$f'(x) = (x - c)^k \varphi'(x) + k(x - c)^{k-1} \varphi(x) = (x - c)^{k-1} [(x - c)\varphi'(x) + k\varphi(x)].$$

Так как $\text{char } K = 0$, то $0 \neq k \cdot 1 \in K$ и слагаемое $k\varphi(x)$ не делится на $x - c$, и поэтому многочлен $(x - c)\varphi'(x) + k\varphi(x)$ также не делится на $x - c$. Итак, $(x - c)^{k-1}$ — наибольшая степень многочлена $x - c$, на которую делится многочлен $f'(x)$. \square

Следствия 3.11.5.

- 1) k -кратный корень многочлена $f(x)$ является $(k-s)$ -кратным корнем s -й производной $f^{(s)}(x)$ этого многочлена при $k \geq s$ (впервые не является корнем для k -й производной $f^{(k)}(x)$).
- 2) Многочлен $g(x) = f(x)/\text{НОД}(f(x), f'(x))$ имеет те же корни, что и многочлен $f(x)$, но все они имеют кратность, равную 1 (это преимущество многочлена $g(x)$ позволяет применять многие алгоритмы локализации и численного нахождения корней).

Замечание 3.11.6. Из формулы Тейлора (см. теорему 3.10.4) для многочлена $f(x) \in K[x]$ над полем K нулевой характеристики также имеет, что c является корнем в точности кратности k тогда и только тогда, когда

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

Если $\text{char } K = p$ и $k < p$, то это утверждение остается верным.

Замечание 3.11.7 (о кратности корня). Пусть K — поле нулевой характеристики,

$$J_l(c) = \begin{pmatrix} c & 1 & & 0 \\ & \ddots & \ddots & \\ 0 & & \ddots & 1 \\ & & & c \end{pmatrix} \in M_l(K), \quad l \in \mathbb{N}, \quad J_0(c) = c \in K$$

(жордановы клетки размера l). Тогда для многочлена $h(x) = (x - c)^l$ имеем $h(J_l(c)) = 0 \in M_l(K)$, но $h'(J_l(c)) \neq 0$ для $h'(x) = (x - c)^{l-1}$ (более того, $h(x)$ — минимальный анулирующий многочлен матрицы $J_l(c)$).

Пусть $f(x) \in K[x]$, $\deg(f(x)) = n \geq 1$, c — корень многочлена $f(x)$, $f(c) = 0$. Тогда корень c имеет кратность k в том и только в том случае, когда $f(J_k(c)) = 0 \in M_k(K)$, но $f(J_{k+1}(c)) \neq 0 \in M_{k+1}(K)$.

Действительно, пусть

$$f(x) = (x - c)^k g(x), \quad g(x) \in K[x], \quad g(c) \neq 0.$$

Тогда

$$f(J_k(c)) = (J_k(0))^k g(J_k(c)) = 0 \in M_k(K).$$

Если

$$g(x) = b_s(x - c)^s + \dots + b_1(x - c) + b_0, \quad k + s = n, \quad b_i \in K,$$

то так как $g(c) \neq 0$, то $b_0 \neq 0$ и

$$f(J_{k+1}(c)) = b_0(J_{k+1}(0))^k \neq 0 \in M_{k+1}(K).$$

Если теперь $f(J_k(c)) = 0 \in M_k(K)$, $f(J_{k+1}(c)) \neq 0 \in M_{k+1}(K)$, поскольку минимальный анулирующий многочлен матрицы $J_k(c)$ делится на $(x - c)^k$. Так как $f(J_{k+1}(c)) \neq 0$, то многочлен $f(x)$ не делится на $(x - c)^{k+1}$. \square

Замечание 3.11.8.

- 1) Если $K = \mathbb{Z}_2$, $\mathbb{Z}_2 = 2$, $f(x) = x^2 + 1 = (x - 1)^2$, то $f'(x) = 2x = 0$ (это показывает существенность в теореме 3.11.4 предположения о том, что $\text{char } K = 0$).
- 2) Пусть K — поле, $\text{char } K = p > 0$, $r \geq 1$, $x \mapsto x^p$ — эндоморфизм Фробениуса поля K . Для любого $a \in K$ имеем $(x - a)^{p^r} = x^{p^r} - a^{p^r}$. Если $b \in K$ и многочлен $x^{p^r} - b$ имеет корень c в K , то $c^{p^r} = b$ и $x^{p^r} - b = (x - a)^{p^r}$. Следовательно, многочлен имеет ровно один корень кратности p^r . В частности, $(x - 1)^{p^r} = x^{p^r} - 1$.

Замечание 3.11.9. Несколько другой подход к решению задачи о существовании кратных корней связан с понятием дискриминанта многочлена (см. ??) и его выражения через результант.

Упражнение 3.11.10. Для определения кратности корня многочлена над полем положительной характеристики полезно рассматривать гиперпроизводные этого многочлена. Пусть K — поле, $f(x) \in K[x]$.

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

Для $k \in \mathbb{N} \cup \{0\}$ определим k -ю гиперпроизводную $E^{(k)}(f)$ многочлена $f(x)$ следующим образом:

$$E^{(k)}(f) = \sum_{i=0}^n C_k^i a_i x^{i-d},$$

где полагаем $C_k^d = 0$ при $d > i$. Если $\text{char } K = 0$, то

$$E^{(k)}(f) = \frac{1}{k!} f^{(k)}(x).$$

Покажите, что:

- 1) гиперпроизводные — K -линейные отображения из $K[x]$ в $K[x]$;
 2) если $c \in K$, то

$$E^{(k)}((x - c)^l) = C_l^k (x - t)^{l-k};$$

- 3) если $\text{char } K = p > 0$, $h(x) = v(x, x^{p^s})$, где $v(x, y) \in K[x]$, $s \in \mathbb{N}$, то для $0 \leq k < p^s$ гиперпроизводная $E^{(k)}(h)$ равна k -й частной производной многочлена $v(x, y)$ по x с последующей подстановкой $y = x^{p^s}$;
- 4) если K — произвольное поле, $f \in K[x]$ и элемент $c \in K$ является общим корнем гиперпроизводных $E^{(k)}(f)$ для $k = 0, 1, \dots, m-1$, то c — корень многочлена $f(x)$ кратности не менее чем m .

Замечание 3.11.11. Отделение кратных корней многочлена над полем K конечной характеристики $\text{char } K = p > 0$ является более трудоёмкой процедурой.

Например, если K — совершенное поле (это означает, что либо $\text{char } K = 0$, либо $K^p = K$, если $\text{char } K = p$; в частности, поле K совершенное, если K — алгебраически замкнутое поле или если K — конечное поле), то можно действовать следующим образом.

Будем предполагать, что извлечение корня $\sqrt[p]{a}$ степени p из элемента a поля K производится конструктивно.

Алгоритм отделения кратных корней многочлена $f(x) \in K[x]$, $\deg(f(x)) \geq 1$, состоит в следующем.

Если $f'(x) = 0 \in K[x]$, то $f(x) = q(x^p)$, где $q(t) \in K[t]$ (см. лемму 3.10.3),

$$q(t) = b_lt^l + \dots + b_1t + b_0, \quad b_i \in K.$$

Но для многочлена

$$r(x) = \sqrt[p]{b_l}x^l + \dots + \sqrt[p]{b_1}x + \sqrt[p]{b_0} \in K[x]$$

имеем

$$(r(x))^p = q(x^p) = f(x),$$

и достаточно отделить кратные корни многочлена $r(x)$, $\deg(r(x)) < \deg(f(x))$. К многочлену $r(x)$ применим описываемый алгоритм.

Пусть теперь $f'(x) \neq 0 \in K[x]$. Тогда, используя факториальность кольца $K[x]$, мы можем предполагать, что $f(x) = g(x) \cdot h(x)$ — произведение неприводимых сомножителей над K , кратности неприводимых сомножителей в $g(x)$ строго меньше p , а в $h(x)$ — кратны p или $h(x) = 1$. Тогда $h'(x) = 0$, $f'(x) = g'(x) \cdot h(x)$. С помощью алгоритма Евклида находим

$$\text{НОД}(f(x), f'(x)) = \text{НОД}(g(x), g'(x))h(x).$$

Положим

$$G(x) = \frac{f(x)}{\text{НОД}(f(x), f'(x))} = \frac{g(x)}{\text{НОД}(g(x), g'(x))}.$$

Таким образом, многочлен $G(x)$ имеет те же корни (неприводимые сомножители), что и многочлен $g(x)$, но с единичными кратностями.

Находим $d(x) = \text{НОД}(f, G(x))$, $f_1(x) = \frac{f(x)}{d(x)}$, затем находим $d_1(x) = \text{НОД}(f_1(x), G(x))$.

Если $d_1(x) \neq 1$ ($\deg(d_1(x)) > 1$), то положим $f_2(x) = \frac{f_1(x)}{d_1(x)}$, находим $d_3(x) = \text{НОД}(f_2(x), G(x))$ и т. д. Продолжая этот процесс, находим многочлен $h(x)$, имеющий

всё те же корни (неприводимые сомножители) с теми же кратностями, что и многочлен $h(x)$, за исключением корней многочлена $G(x)$ (ни один корень многочлена $G(x)$ не является корнем многочлена $\tilde{h}(x)$), или $\tilde{h}(x) = 1$. Если $\tilde{h}(x) = 1$, то $G(x)$ — искомый многочлен.

Если $\tilde{h}(x) \neq 1$, то ясно, что $(\tilde{h}(x))' = 0$. Учитывая, что $\deg(\tilde{h}(x)) < \deg f(x)$, применяя алгоритм отделения корней к $\tilde{h}(x)$, получаем многочлен $H(x)$, имеющий те же корни (неприводимые сомножители), что и многочлен $\tilde{h}(x)$, но с единичными кратностями.

Окончательно, для искомого многочлена $F(x)$ полагаем $F(x) = G(x) \cdot H(x)$.

Рассмотрим пример (мы не вычисляем разложение многочлена на неприводимые сомножители, а используем это разложение лишь для сокращения выкладок):

$$f(x) = 2(x-1)^2(x+1)^3(x+2)((x-1)^{p+1}(x+1)^2(x+3))^p,$$

где $p > 3$. Тогда

$$\begin{aligned} G(x) &= 2(x-1)(x+1)(x+2), & \tilde{h}(x) &= (x+3)^{p^2}, \\ H(x) &= x+3, & F(x) &= 2(x-1)(x+1)(x+2)(x+3). \end{aligned}$$

Все вычисления для построения многочлена $F(x)$ производятся с помощью алгоритмов деления, алгоритма Евклида и алгоритма извлечения корней степени p из коэффициентов.

Для конечных полей существуют другие, более эффективные, методы для отделения кратных неприводимых сомножителей, а также для разложения многочлена на неприводимые сомножители.

Если K — конечное поле, $|K| = q$, то так как все элементы поля K удовлетворяют уравнению $x^q - x = 0$, то для отыскания всех корней многочлена $f(x) \in K[x]$, лежащих в поле K , достаточно рассмотреть многочлен $f_1(x) = \text{НОД}(f(x), x^q - x)$.

3.12. Разложение многочленов с комплексными коэффициентами на линейные множители

Чтобы

Теорема 3.12.1 (о разложении многочлена с комплексными коэффициентами в произведение линейных множителей). Пусть $f(x) \in \mathbb{C}[x]$, $\deg f(x) = n \geq 1$. Тогда

$$f(x) = a(x - \alpha_1) \dots (x - \alpha_n), \quad a, \alpha_1, \dots, \alpha_n \in \mathbb{C},$$

при этом это разложение единственное (с точностью до порядка сомножителей).

Доказательство. В силу теоремы Гаусса

$$f(x) = (x - c)q(x), \quad q(x) \in \mathbb{C}[x], \quad \deg q(x) = n - 1.$$

Применим далее теорему Гаусса к $q(x)$, если $n - 1 \geq 1$. Продолжая этот процесс, убеждаемся в существовании разложения на линейные множители.

Пусть теперь

$$f(x) = a(x - \alpha_1) \dots (x - \alpha_n) = b(x - \beta_1) \dots (x - \beta_n), \quad a, b, \alpha_i, \beta_j \in \mathbb{C}, \quad a \neq 0, \quad b \neq 0.$$

Ясно, что $a = b$. Если $\alpha_i \neq \beta_j$ для всех $j = 1, \dots, n$, то

$$f(\alpha_i) = 0 = b(\alpha_i - \beta_1) \dots (\alpha_i - \beta_n) \neq 0.$$

Поэтому в оба разложения входит одинаковое множество различных корней. Убедимся в совпадении кратностей вхождения каждого корня в оба разложения. Действительно, если

$$f(x) = (x - \alpha)^r q_1(x) = (x - \alpha)^s q_2(x), \quad q_1(\alpha) \neq 0, \quad q_2(\alpha) \neq 0, \quad r < s,$$

то, сокращая в $\mathbb{C}[x]$ на $(x - \alpha)^r$, получаем $q_1(x) = (x - \alpha)^{s-r} q_2(x)$, и поэтому $q_1(\alpha) = 0$, что противоречит $q_1(\alpha) \neq 0$. \square

Следствие 3.12.2. Если $\alpha_1, \dots, \alpha_r$ — различные корни многочлена $f(x) \in \mathbb{C}[x]$, k_1, \dots, k_r — их кратности, $n = \deg f(x)$, то $n = k_1 + \dots + k_r$ (т. е. многочлен степени $n = \deg f$ имеет ровно n корней с учётом их кратности).

Замечание 3.12.3 (о неприводимых многочленах над полем комплексных чисел). По аналогии с определением простых чисел в кольце целых чисел \mathbb{Z} многочлен $f(x) \in P[x]$, $\deg f(x) \geq 1$, называется **неприводимым**, если $f(x)$ нельзя представить в виде $f(x) = \varphi(x)\psi(x)$, $\deg \varphi(x) \geq 1$, $\deg \psi(x) \geq 1$. (иными словами, если $\varphi(x)$ — делитель многочлена $f(x)$, $\deg \varphi(x) \geq 1$, то $\deg \varphi(x) = n = \deg f(x)$).

Таким образом, мы установили, что **неприводимые многочлены над полем \mathbb{C} комплексных чисел — это в точности многочлены первой степени**. Из единственности разложения на линейные множители над \mathbb{C} получаем существование и единственность разложения на неприводимые многочлены над \mathbb{C} .

Лемма 3.12.4. Если $f(x), g(x) \in P[x]$, $\deg f(x) \leq n$, $\deg g(x) \leq n$, $f(x)$ и $g(x)$ совпадают в $(n+1)$ -й различных точках $\alpha_1, \dots, \alpha_{n+1} \in P$, то $f(x) = g(x)$.

Доказательство. Пусть $h(x) = f(x) - g(x)$. Тогда если $h(x) \neq 0$, то $\deg h(x) \leq n$ и $h(\alpha_i) = f(\alpha_i) - g(\alpha_i) = 0$ для $i = 1, \dots, n+1$. Но это противоречит тому, что число различных корней не превосходит степени многочлена. \square

Следствие 3.12.5. Если $|P| = \infty$ (в частности, для $P = \mathbb{Q}, \mathbb{R}$ или \mathbb{C}), то формальное и функциональное определение равенства многочленов совпадают.

Замечание 3.12.6. Для конечного поля \mathbb{Z}_2 разные многочлены x и x^2 в точках 0 и 1 принимают одинаковые значения, т. е. равны как функции.

Следствие 3.12.7. Данная лемма также может быть использована и для доказательства единственности в интерполяционной формуле Лагранжа.

Проверь | **Теорема Виета.** Если

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - \alpha_1)\dots(x - \alpha_n),$$

то

$$a_{n-1} = -(\alpha_1 + \alpha_2 + \dots + \alpha_n),$$

$$a_{n-2} = \alpha_1\alpha_2 + \dots + \alpha_{n-1}\alpha_n,$$

$$\dots$$

$$a_1 = (-1)^{n-1}(\alpha_1\alpha_2\dots\alpha_{n-1} + \dots + \alpha_2\alpha_3\dots\alpha_n),$$

$$a_0 = (-1)^n\alpha_1\alpha_2\dots\alpha_n.$$

Доказательство. В силу закона дистрибутивности умножение на $(x - \alpha)$ сводится к умножениям на x и на $-\alpha$. Формулы Виета получаются подсчетом коэффициента при x^k (т. е. надо при указанных раскрытиях скобок k раз выбрать x и, следовательно, $(n-k)$ раз корни). \square

Упражнение 3.12.8. Пусть сумма корней многочлена с комплексными коэффициентами (считая кратность) равна нулю. Докажите, что сумма корней производной этого многочлена также равна нулю.

Упражнение 3.12.9. Пусть x_1, \dots, x_n — корни многочлена $1 + x + x^2 + \dots + x^n \in \mathbb{C}[x]$. Тогда:

$$1) \text{ многочлен } (1+x)^{n+1} - x^{n+1} \text{ имеет корни } \frac{1}{x_1 - 1}, \dots, \frac{1}{x_n - 1};$$

$$2) \frac{1}{x_1 - 1} + \frac{1}{x_2 - 1} + \dots + \frac{1}{x_n - 1} = -\frac{n}{2}.$$

3.13. Многочлены

с действительными коэффициентами

В этом разделе мы рассмотрим свойства многочленов из $\mathbb{R}[x]$ (т. е. над полем $P = \mathbb{R}$ действительных чисел).

Лемма 3.13.1. Если $f(x) \in \mathbb{R}[x]$, $\alpha \in \mathbb{C}$, $f(\alpha) = 0$, то $f(\bar{\alpha}) = 0$.

Доказательство. Пусть

$$f(x) = a_n x^n + \dots + a_1 x + a_0, \quad a_i \in \mathbb{R}.$$

Тогда $f(\alpha) = a_n \alpha^n + \dots + a_1 \alpha + a_0 = 0$. Так как

$$\overline{(z_1 + z_2)} = \bar{z}_1 + \bar{z}_2, \quad \overline{(z_1 z_2)} = \bar{z}_1 \bar{z}_2,$$

то

$$\begin{aligned} 0 &= \bar{0} = \overline{a_n \alpha^n + \dots + a_1 \alpha + a_0} = \\ &= \bar{a}_n \bar{\alpha}^n + \dots + \bar{a}_1 \bar{\alpha} + \bar{a}_0 = \\ &= a_n \bar{\alpha}^n + \dots + a_1 \bar{\alpha} + a_0 = f(\bar{\alpha}). \end{aligned}$$

Лемма 3.13.2. Если $\alpha \in \mathbb{C} \setminus \mathbb{R}$ (т. е. $\bar{\alpha} \neq \alpha$), то $\text{НОД}(x - \alpha, x - \bar{\alpha}) = 1$.

Доказательство. Если $d(x) = \text{НОД}(x - \alpha, x - \bar{\alpha})$, то или $\deg d(x) = 0$ (т. е. $d(x) = 1$), или $\deg d(x) = 1$. Если $\deg d(x) = 1$, то $(x - \alpha) = d(x) \cdot c$, $(x - \bar{\alpha}) = d(x) \cdot d$, $c, d \in \mathbb{C}$, т. е. $d(x) = c^{-1}(x - \alpha) = d^{-1}(x - \bar{\alpha})$. Поэтому $c^{-1} = d^{-1}$, $c^{-1}\alpha = d^{-1}\bar{\alpha}$, т. е. $\alpha = \bar{\alpha}$, что противоречит предположению. \square

Следствие 3.13.3. Если $f(x) \in \mathbb{R}[x]$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$, $f(\alpha) = 0$, то $f(x) = \varphi(x)q(x)$, где $\varphi(x) = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} \in \mathbb{R}[x]$, $q(x) \in \mathbb{R}[x]$.

Доказательство. Так как $f(\alpha) = 0$, то $f(\bar{\alpha}) = 0$. Тогда $f(x) = (x - \alpha)q_1(x)$ делится на $x - \bar{\alpha}$, но $x - \alpha$ и $x - \bar{\alpha}$ взаимно просты (поскольку $\bar{\alpha} \neq \alpha$), и поэтому $f(x) = (x - \alpha)(x - \bar{\alpha})q(x)$. Так как $f(x), (x - \alpha)(x - \bar{\alpha}) \in \mathbb{R}[x]$, то $q(x) \in \mathbb{R}[x]$. \square

Лемма 3.13.4. Если $f(x) \in \mathbb{R}[x]$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$, $f(\alpha) = 0$, то кратности корней α и $\bar{\alpha}$ в многочлене $f(x)$ совпадают.

Доказательство. Пусть кратность корней $\bar{\alpha}$ и α равны соответственно k и l . Допустим противное, что $k < l$ (симметрично, $k > l$, и тогда учтём, что $\alpha = \bar{\alpha}$). Тогда для $\varphi(x) = (x - \alpha)(x - \bar{\alpha})$ имеем

$$f(x) = (x - \bar{\alpha})^k(x - \alpha)^l q(x) = \varphi(x)^k(x - \alpha)^{l-k}q(x), \quad q(\alpha) \neq 0, \quad q(\bar{\alpha}) \neq 0.$$

Тогда $\tilde{f}(x) = (x - \alpha)^{l-k}q(x) \in \mathbb{R}[x]$ (как частное от деления двух многочленов из $\mathbb{R}[x]$: $f(x)$ на $\varphi(x)^k$), однако $\tilde{f}(\alpha) = 0$, но $\tilde{f}(\bar{\alpha}) = (\bar{\alpha} - \alpha)^{l-k}q(\bar{\alpha}) \neq 0$, что противоречит нашей теореме для $f(x) \in \mathbb{R}[x]$. \square

Следствие 3.13.5. Комплексные корни многочлена с действительными коэффициентами, не являющиеся действительными, попарно сопряжены.

Следствие 3.13.6 (о разложении на неприводимые многочлены над полем \mathbb{R} действительных чисел). Неприводимые многочлены над \mathbb{R} — это в точности многочлены первой степени и многочлены второй степени без действительных корней. Каждый многочлен $f(x) \in \mathbb{R}[x]$, $\deg f(x) \geq 1$, представляется (и при этом однозначно, с точностью до порядка сомножителей, в виде произведения константы $a \in \mathbb{R}$, многочленов вида $(x - \alpha)$, $\alpha \in \mathbb{R}$, и многочленов вида $(x - \alpha)(x - \bar{\alpha})$, где $\alpha \in \mathbb{C} \setminus \mathbb{R}$, соответствующих паре сопряжённых корней α и $\bar{\alpha}$). Доказательство единственности следует из единственности разложения на линейные множители над полем \mathbb{C} комплексных чисел.

Задача 3.13.7. Пусть $f(x) = x^m(x - 1)^n \in \mathbb{R}[x]$, $F(x) = f^{(m)}(x)$ (m -я производная многочлена $f(x)$). Доказать, что все корни многочлена $F(x)$ являются положительными правильными рациональными дробями в \mathbb{Q} .

Задача 3.13.8. Разложить на неприводимые множители над полем \mathbb{R} многочлены $x^4 + 4$ и $x^5 - 1$; разложить многочлен $f(x) = x^4 + x^3 - 2x^2 + 12x - 16 \in \mathbb{R}[x]$ на неприводимые множители над полем \mathbb{R} (методом неопределённых коэффициентов или применяя формулу корней Феррари).

Упражнение 3.13.9. Проверить, что многочлен

$$f(x) = (\cos \varphi + x \sin \varphi)^n - \cos(n\varphi) - x \sin(n\varphi) \in \mathbb{R}[x]$$

делится на $x^2 + 1$.

Указание. $f(i) = 0 = f(-i)$.

Задача 3.13.10. Найдите многочлен наименьшей степени с целыми коэффициентами, имеющий корень $\sqrt{2} + \sqrt{3}i$.

3.14. Неприводимые многочлены над произвольным полем K

Напомним, что многочлен $f(x) \in K[x]$ над полем K называется неприводимым, если $\deg f(x) \geq 1$ и многочлен $f(x)$ нельзя представить в виде $f(x) = \varphi(x)\psi(x)$, где $1 \leq \deg \varphi(x) < \deg f(x)$, $1 \leq \deg \psi(x) < \deg f(x)$.

Пример 3.14.1. Над любым полем K все многочлены первой степени неприводимы, многочлен второй или третьей степени неприводим тогда и только тогда, когда он не имеет корней в поле K .

Пример 3.14.2. Итог нашего изучения неприводимых многочленов над \mathbb{C} и над \mathbb{R} :

- над полем комплексных чисел \mathbb{C} неприводимы многочлены первой степени и только они;
- над полем действительных чисел \mathbb{R} неприводимы многочлены первой степени и многочлены второй степени без действительных корней, и только они.

Пример 3.14.3. Многочлен $x^4 + 1$ неприводим над полем \mathbb{Q} рациональных чисел.

Задача 3.14.4. Пусть K — подполе в \mathbb{C} , $f \in K[x]$ — неприводимый многочлен. Тогда f не имеет кратных корней в \mathbb{C} .

3.15. Свойства неприводимых многочленов

1) Если $p(x) \in K[x]$ — неприводимый многочлен и $0 \neq c \in K$, то $cp(x)$ также неприводимый многочлен.

2) Если $f(x), p(x) \in K[x]$ и $p(x)$ — неприводимый многочлен, то либо $f(x)$ делится на $p(x)$, либо $d(x) = \text{НОД}(f(x), p(x)) = 1$ (т. е. $f(x)$ и $p(x)$ взаимно просты). Действительно, либо $d(x) = p(x)$, либо $d(x) = 1$.

3) Если $f(x)g(x) = p(x)q(x)$, где $p(x)$ — неприводимый многочлен, то либо $f(x) = p(x)\tilde{q}(x)$, либо $g(x) = p(x)\tilde{\tilde{q}}(x)$. Если $f(x)$ не делится на $p(x)$, то $(f(x), p(x)) = 1$, и поэтому $g(x)$ делится на $p(x)$.

В кольце \mathbb{Z} целых чисел каждое целое число $n \in \mathbb{Z}$, отличное от 1 и -1, представимо, и притом единственным образом, в виде произведения простых чисел (доказательство индукцией по $|n| \in \mathbb{N}$). Множество простых чисел бесконечно (если p_1, \dots, p_n — все простые числа, то простой делитель p числа $p_1p_2 \dots p_n + 1$ отличен от всех p_1, \dots, p_n , что приводит к противоречию). Аналогичные утверждения верны для кольца многочленов $K[x]$ над полем K .

Теорема 3.15.1. Для любого поля K в кольце многочленов $K[x]$ любой многочлен $f(x) \in K[x]$, $\deg f(x) \geq 1$, разложим (и единственным образом) в произведение неприводимых многочленов.

Доказательство. 1) Проведём индукцию по $\deg f(x)$. Если $\deg f(x) = 1$, то многочлен $f(x)$ неприводим. Пусть утверждение о разложении в произведение неприводимых многочленов верно для всех многочленов степени $< n$, и пусть $\deg f(x) = n$. Если $f(x)$ — неприводимый многочлен, то всё доказано. В противном случае $f(x) = \varphi(x)\psi(x)$,

$1 \leq \deg \varphi(x) < \deg f(x) = n$, $1 \leq \deg \psi(x) < \deg f(x) = n$, и поэтому $\varphi(x)$ и $\psi(x)$ являются произведениями неприводимых многочленов, следовательно, $f(x) = \varphi(x)\psi(x)$ также является произведением неприводимых многочленов.

2) Индукцией по $n = \deg f(x)$ докажем единственность разложения. Для $n = 1$ утверждение очевидно. Пусть

$$f(x) = p_1(x) \dots p_s(x) = q_1(x) \dots q_t(x),$$

где $s \leq t$. Так как $q_1(x) \dots q_t(x)$ делится на $p_1(x)$, то $q_i(x) = cp_1(x)$, где $1 \leq i \leq t$. Так как в кольце $K[x]$ нет делителей нуля, то, сокращая на $p_1(x)$, получаем

$$p_2(x) \dots p_s(x) = cq_1(x) \dots \widehat{q_i(x)} \dots q_t(x).$$

Применение индуктивного предположения завершает доказательство теоремы. \square

Следствие 3.15.2. Кратность вхождения k_i неприводимого многочлена $p_i(x)$ определена однозначно, т. е. имеем каноническое разложение

$$f(x) = a_n p_1^{k_1}(x) \dots p_r^{k_r}(x),$$

где $\{p_i(x), i = 1, \dots, r\}$ — различные неприводимые многочлены со старшим коэффициентом, равным 1, k_i — их кратности, $a_n \in K$.

Упражнение 3.15.3. В терминах канонических разложений найти наибольший общий делитель, наименьшее общее кратное и поведение кратности при дифференцировании.

Упражнение 3.15.4. Если R — область главных идеалов, то R — кольцо с однозначной факторизацией (факториальное кольцо).

Упражнение 3.15.5.

1) Кольцо $\mathbb{Z}[x]$ не является кольцом главных идеалов (и поэтому не является евклидовым кольцом), но является факториальным кольцом.

2) В $\mathbb{Z}[x]$ НОД($7x^3 + 1, 2x$) = 1, но не существует таких многочленов $u(x), v(x) \in \mathbb{Z}[x]$, что $u(x)(7x^3 + 1) + v(x) \cdot 2x = 1$.

Упражнение 3.15.6. Кольцо $\mathbb{Z}[\sqrt{2}]$ — евклидова область ($N(x + y\sqrt{2}) = |x^2 - 2y^2|$ для $x, y \in \mathbb{Z}$). Аналогично, $\mathbb{Z}[\sqrt{3}]$ — евклидова область с нормой $N(x + y\sqrt{3}) = |x^2 - 3y^2|$.

Упражнение 3.15.7. Кольцо $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ гауссовых чисел является евклидовой областью (то есть евклидовым кольцом без делителей нуля), кольца $\mathbb{Z}[\sqrt{3}i] = \{a + b\sqrt{3}i \mid a, b \in \mathbb{Z}\}$ и $\mathbb{Z}[10]$ не являются факториальными кольцами.

Упражнение 3.15.8. В кольце $\mathbb{Q}[\sqrt{5}i]$ имеем различные разложения на простые множители:

$$21 = 3 \cdot 7 = (1 + 2\sqrt{5}i)(1 - 2\sqrt{5}i);$$

у элементов 147 и $21 - 42\sqrt{5}i$ нет НОД: рассмотрите общие делители 21 и $7 - 14\sqrt{5}i$.

Упражнение 3.15.9. Кольцо $D[x]$ является факториальной областью для любой факториальной области D .

Упражнение 3.15.10. Если многочлен

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

имеет рациональный корень $\frac{k}{l}$, где $k, l \in \mathbb{Z}$, $(k, l) = 1$, то a_0 делится на k , a_n делится на l .

Указание.

$$0 = l^n f\left(\frac{k}{l}\right) = a_n k^n + a_{n-1} k^{n-1} l + \dots + a_1 k l^{n-1} + a_0 l^n.$$

В частности, если $a_n = 1$, то рациональный корень многочлена $f(x)$ является целым числом, которое делит число a_0 .

Упражнение 3.15.11 (лемма Гаусса). Если $f(x) \in \mathbb{Z}[x]$ и $f(x) = g(x)h(x)$, где $g(x), h(x) \in \mathbb{Q}[x]$, то $\lambda g(x), \lambda^{-1}h(x) \in \mathbb{Z}[x]$ для некоторого $0 \neq \lambda \in \mathbb{Q}$.

Упражнение 3.15.12 (критерий неприводимости Эйзенштейна над полем \mathbb{Q}). Пусть $f(x) = \sum_{i=0}^n a_i x^i$, $a_i \in \mathbb{Z}$. Если простое число p делит все коэффициенты, кроме a_n , и p^2 не делит a_0 , то $f(x)$ неприводим над полем \mathbb{Q} рациональных чисел. Например, $f(x) = x^4 + 3x^2 - 9x + 6$ ($p = 3$).

Упражнение 3.15.13. Если p — простое число, то многочлен деления круга на p частей

$$f(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}$$

неприводим над полем \mathbb{Q} рациональных чисел.

Указание. Произвести замену $x = y + 1$ и применить критерий Эйзенштейна.

Но если $n = ab$, где $a, b \in \mathbb{N}$, $a, b > 1$, то

$$x^{n-1} + \dots + x + 1 = \frac{(x^a)^b - 1}{x^a - 1} \cdot \frac{x^a - 1}{x - 1}.$$

Упражнение 3.15.14 (критерий Полиа). Пусть для многочлена

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

$A = \max\{|a_{n-1}|, \dots, |a_0|\}$, $k \in \mathbb{Z}$, $k \geq \frac{A}{|a_n|} + \frac{3}{2}$. Если $f(k-1) \neq 0$ и $f(k)$ — простое число, то многочлен $f(x)$ неприводим над полем \mathbb{Q} .

Упражнение 3.15.15. Многочлен

$$f(x) = x^3 - x^2 + x + 1 \in \mathbb{Q}[x]$$

неприводим.

Указание. Применить критерий Полиа: $A = 1$, $k = 3$, $f(3) = 22$, $f(4) = 53$ — простое число.

Упражнение 3.15.16 (критерий Кона). Пусть для многочлена

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

имеем: $0 \leq a_i \leq 9$, $i = 0, 1, \dots, n$; $N = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0$ — простое число. Тогда многочлен $f(x)$ неприводим над полем \mathbb{Q} .

Упражнение 3.15.17. Многочлен

$$f(x) = 2x^4 + x^3 + 5x^2 + 6x + 3 \in \mathbb{Q}[x]$$

неприводим.

Указание. Применить критерий Кона: $N = 21563$ — простое число.

Упражнение 3.15.18. Если

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x],$$

$n = 2l$ или $2l + 1$, $f(x)$ принимает значения ± 1 более чем при $2l$ целых значениях x , то $f(x)$ неприводим над полем \mathbb{Q} .

Упражнение 3.15.19. Многочлен

$$f(x) = x^3 - 3x^2 + 3 \in \mathbb{Q}[x]$$

неприводим.

Указание. Здесь по предыдущему критерию $3 = 2 \cdot 1 + 1$, $l = 1$, $3 > 2l = 2$, $f(-1) = -1$, $f(1) = 1$, $f(2) = -1$.

Упражнение 3.15.20. Многочлены второй или третьей степени над полем \mathbb{Q} (как и над любым полем K) неприводимы тогда и только тогда, когда они не имеют корня в \mathbb{Q} (в поле K). Многочлен

$$f(x) = x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0 \in \mathbb{Q}[x]$$

приводим над полем \mathbb{Q} тогда и только тогда, когда: либо он имеет рациональный корень; либо связанный с ним многочлен третьей степени

$$k(t) = 8t^3 - 4b_2 t^2 + (2b_1 b_3 - 8b_0)t - (b_0 b_3^2 - 4b_0 b_2 + b_1^2)$$

имеет такой рациональный корень t_0 , что

$$\lambda = \sqrt{2t_0 + \frac{b_3^2}{4} - b_2}, \mu = \sqrt{t_0^2 - b_0} \in \mathbb{Q},$$

и тогда

$$f(x) = \left[x^2 + \left(\frac{b_3}{2} + \lambda \right) x + (t_0 + \mu) \right] \left[x^2 + \left(\frac{b_3}{2} - \lambda \right) x + (t_0 - \mu) \right].$$

Упражнение 3.15.21. Покажите, что многочлены $x^n - 2$ и $x^{2^k} + 1$ неприводимы в $\mathbb{Z}[x]$.

Упражнение 3.15.22 (алгоритм Кронекера разложения на неприводимые множители многочлена над полем \mathbb{Q} , 1882 г.). Пусть $f(x) \in \mathbb{Z}[x]$, $n = \deg f(x) > 0$, k — наибольшее натуральное число, для которого $k \leq \frac{n}{2}$. Если $f(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{Z}[x]$, $\deg g(x) \leq \deg h(x)$, то $\deg g(x) \leq k$. Придавая переменной x любые $k+1$ различных целых значений $c_i \in \mathbb{Z}$, $i = 1, \dots, k+1$, получаем

$$f(c_i) = g(c_i)h(c_i), \quad i = 1, \dots, k+1,$$

где $g(c_i), h(c_i) \in \mathbb{Z}$, при этом $g(c_i)$ является делителем числа $f(c_i)$.

Если d_i — делитель числа $f(c_i)$, то по интерполяционной теореме Лагранжа многочлен $g(x)$, для которого $g(c_i) = d_i$, $i = 1, \dots, k+1$ и $\deg g(x) \leq k$, определяется однозначно. Среди всех найденных таких многочленов $g(x)$ надо выбрать те, которые делят многочлен $f(x)$.

Упражнение 3.15.23. Многочлен

$$f(x) = x^5 - x^4 - 2x^3 - 8x^2 + 6x - 1 \in \mathbb{Z}[x]$$

разложить на неприводимые множители над полем \mathbb{Q} (применить алгоритм Кронекера: $f(x) = (x^2 - 3x + 1) \times (x^3 + 2x^2 + 3x - 1)$), сомножители неприводимы над \mathbb{Q} как многочлены второй и третьей степени без рациональных корней.

Упражнение 3.15.24. Пусть

$$f(x) = x^8 + 4x^7 - 2x^6 - 20x^5 + 3x^4 + 44x^3 + 22x^2 - 4x + 34 \in \mathbb{Q}[x].$$

Разложите $f(x)$ на неприводимые многочлены.

Ответ. $f(x) = (x^4 + 4x^3 + 6x^2 + 4x + 2)(x^4 - 8x^3 + 24x^2 - 32x + 17)$.

Упражнение 3.15.25. Разложите многочлен

$$f(x) = 12x^3 + 10x^2 - 36x + 35 \in \mathbb{Z}[x]$$

на неприводимые многочлены.

Ответ. $f(x) = (2x + 5)(6x^2 - 10x + 7)$.

Теорема 3.15.26. Над любым полем K (конечным или бесконечным) число неприводимых многочленов бесконечно.

Доказательство повторяет рассуждение Евклида для целых чисел. Если $\{p_1(x), \dots, p_n(x)\}$ — все неприводимые многочлены, то неприводимый делитель $p(x)$ многочлена $p_1(x) \dots p_n(x) + 1$ не совпадает с $p_1(x), \dots, p_n(x)$, что приводит к противоречию. \square

Следствие 3.15.27. Если поле K конечно, то неприводимые многочлены могут иметь степень больше любого натурального числа n (в отличие от полей \mathbb{C} и \mathbb{R}).

Задача 3.15.28. Доказать, что многочлены $x^3 + x + 1$ и $x^4 + x + 1$ неприводимы над полем \mathbb{Z}_2 .

Задача 3.15.29. Найти все неприводимые многочлены степени ≤ 4 над полем \mathbb{Z}_2 . В частности, x^2+x+1 — единственный многочлен степени 2 над \mathbb{Z}_2 , x^3+x+1 и x^3+x^2+1 — все неприводимые многочлены степени 3 над \mathbb{Z}_2 .

Упражнение 3.15.30. Покажите, что многочлен x^3+x+1 неприводим в $\mathbb{Z}_5[x]$.

Задача 3.15.31. Разложить многочлен $x^5+x^3+x^2+1$ на неприводимые множители над полем \mathbb{Z}_2 .

Задача 3.15.32. Разложить многочлен x^4+x^3+x+2 на неприводимые множители над полем \mathbb{Z}_3 .

Задача 3.15.33. Разложить многочлен $x^4+3x^3+2x^2+x+4$ на неприводимые множители над полем \mathbb{Z}_5 .

Задача 3.15.34. Доказать, что многочлен x^4-10x^2+1 неприводим над полем \mathbb{Q} , но приводим над любым полем \mathbb{Z}_p .

Задача 3.15.35. Многочлен с целыми коэффициентами

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) + 1,$$

где a_1, \dots, a_n — различные целые числа, неприводим в $\mathbb{Q}[x]$.

Указание. Пусть $\varphi(x), \psi(x) \in \mathbb{Z}[x]$ и $f(x) = \varphi(x) \cdot \psi(x)$. Тогда для всех $i = 1, \dots, n$ имеем $\varphi(a_i) \cdot \psi(a_i) = -1$, поэтому $\varphi(a_i) = -\psi(a_i)$. Если $\deg \varphi, \deg \psi \leq n-1$, то, так как многочлен $\varphi(x) + \psi(x)$ обращается в 0 в n различных точках, то имеем $\varphi(x) = -\psi(x)$. Следовательно, $f(x) = -(\psi(x))^2$, что противоречит различным знакам при x^n в левой и правой частях.

Задача 3.15.36. Многочлен $x^{4n}+x^n+1$ неприводим над \mathbb{Z}_2 тогда и только тогда, когда $n = 3^k \cdot 5^m$ для некоторых неотрицательных целых чисел k и m .

Упражнение 3.15.37. Если $f \in \mathbb{Z}[x]$, старший коэффициент многочлена f равен 1 и f неприводим по модулю p , где p — простое число, то f неприводим над \mathbb{Q} .

Задача 3.15.38. Многочлен x^4+1 неприводим над \mathbb{Z} , но разлагается на множители по модулю любого простого числа p .

Задача 3.15.39. Пусть p — простое число, $f \in \mathbb{Z}_p[x]$, $\deg f = n$. Тогда многочлен $f(x)$ неприводим в том и только в том случае, когда для любого простого делителя q числа n : $f(x)$ делит $x^{p^n} - x$; $\text{НОД}(x^{p^{n/q}} - x, f(x)) = 1$. Покажите, что многочлен $x^{10} + x^3 + 1$ неприводим в $\mathbb{Z}_2[x]$.

Задача 3.15.40. Пусть I_p^n — число неприводимых многочленов степени n в $\mathbb{Z}_p[x]$ со старшим коэффициентом 1. Докажите, что:

$$p^n = \sum_{d|n} d \cdot I_p^d; \quad I_p^n = \frac{1}{n} \sum_{d|n} \mu(d) p^{n/d};$$

$I_p^n \geq 1$ для любого простого числа p и $n \in \mathbb{N}$; для простого числа n

$$I_p^n = \frac{p(p^{n-1}-1)}{n}.$$

Упражнение 3.15.41. Разложите на неприводимые множители многочлен

$$f(x) = x^6 - 3x^5 + x^4 - 3x^3 - x^2 - 3x + 1 \in \mathbb{Z}_{11}[x].$$

Ответ. $f(x) = (x+1)(x^2+5x+3)(x^3+2x^2+3x+4)$.

Задача 3.15.42. Разложите $f(x) = x^{15} - 1 \in \mathbb{Z}_{11}[x]$ на неприводимые множители.

Ответ. $f(x) = (x-1)(x-3)(x-4)(x-5)(x+2)(x^2+3x-2)(x^2+5x+3)(x^2+4x+5) \times (x^2-2x+4)(x^2+x+1)$.

3.16. Функция Мёбиуса (1832 г.)

Отображение

$$\mu: \mathbb{N} \rightarrow \{0, 1, -1\} \subseteq \mathbb{Z},$$

заданное правилом

$$\mu(1) = 1;$$

$$\mu(p_1 \dots p_t) = (-1)^t, \text{ если } p_1, \dots, p_t \text{ — различные простые числа;}$$

$$\mu(n) = 0, \text{ если } n \text{ делится на квадрат некоторого простого числа;}$$

называется *функцией Мёбиуса*.

Замечание 3.16.1. $\mu(n)$ — это сумма всех комплексных первообразных корней степени n из 1.

Полезное свойство функции Мёбиуса:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1. \end{cases} \quad (3.1)$$

Действительно, если $n > 1$, то пусть p_1, \dots, p_k — все различные простые делители числа n . Рассматривая только ненулевые слагаемые в $\sum_{d|n} \mu(d)$, имеем

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^k \mu(p_i) + \sum_{1 \leq i_1 < i_2 \leq k} \mu(p_{i_1} p_{i_2}) + \dots + \mu(p_1 p_2 \dots p_k) = \\ &= 1 + C_k^1(-1) + C_k^2(-1)^2 + \dots + C_k^k(-1)^k = (1 + (-1))^k = 0. \end{aligned}$$

3.17. Формула обращения Мёбиуса (правило Дедекинда—Лиувилля, 1857 г.)

Пусть $f, g: \mathbb{N} \rightarrow A$, где $(A, +)$ — абелева группа по сложению. Тогда

$$g(n) = \sum_{d|n} f(d)$$

тогда и только тогда, когда

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Мультипликативная форма этого утверждения:

$$g(n) = \prod_{d|n} f(d) \iff f(n) = \prod_{d|n} g(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)}.$$

Действительно, с учётом (3.1) имеем

$$\begin{aligned} \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) &= \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{m|\frac{n}{d}} f(m) = \\ &= \sum_{c|n} \sum_{d|\frac{n}{m}} \mu(d) f(m) = \sum_{m|n} f(m) \sum_{d|\frac{n}{m}} \mu(d) = f(n). \end{aligned}$$

Обратный переход доказывается аналогично.

Задача 3.17.1. Доказать, что если $I_q(k)$ — число неприводимых многочленов степени k со старшим коэффициентом, равным единице, над конечным полем из q элементов, то

$$I_q(k) = \frac{1}{k} \sum_{d|k} \mu\left(\frac{k}{d}\right) q^d.$$

Указание. Ясно, что

$$\sum_{d|k} I_q(d) d = q^k,$$

далее надо применить формулу обращения Мёбиуса.

3.18. Функция Эйлера

Функция Эйлера $\varphi(n)$: $\varphi: \mathbb{N} \rightarrow \mathbb{N}$, $\varphi(1) = 1$, для $n > 1$ $\varphi(n)$ — число таких чисел $1 \leq k < n$, что $(k, n) = 1$.

Замечание 3.18.1. $\varphi(n)$ — число первообразных комплексных корней n -й степени из 1.

Замечание 3.18.2. $\varphi(n)$ — число обратимых элементов кольца вычетов \mathbb{Z}_n (т. е. $|U(\mathbb{Z}_n)| = \varphi(n)$).

Задача 3.18.3 (лемма Гаусса).

$$n = \sum_{d|n} \varphi(d).$$

Задача 3.18.4.

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = \sum_{d|n} d \mu\left(\frac{n}{d}\right)$$

(применение обращения Мёбиуса к предыдущему разложению).

Задача 3.18.5 (следствие из задачи 3.18.4). Если p_1, \dots, p_r — различные простые делители числа n , то

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

В частности, если p — простое число, то

$$\varphi(p^n) = p^n - p^{n-1}, \quad \varphi(p) = p - 1$$

(например, $\varphi(2^n) = 2^{n-1}$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$).

Задача 3.18.6. Число $p \in \mathbb{N}$ является простым тогда и только тогда, когда $\varphi(p) = p - 1$.

Задача 3.18.7. Если $(m, n) = 1$, то $\varphi(mn) = \varphi(m)\varphi(n)$.

Задача 3.18.8. Если $n > 2$, то $\varphi(n)$ — чётное число.

Задача 3.18.9. Если $a, m \in \mathbb{N}$ и $(a, m) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$ (см. теорему Эйлера как следствие теоремы Лагранжа). В частности, если p — простое число, то для любого $a \in \mathbb{N}$, $1 \leq a < p$, $a^{p-1} \equiv 1 \pmod{p}$, то есть если $a \not\equiv 0 \pmod{p}$, то $a^{p-1} \equiv 1 \pmod{p}$, малая теорема Ферма).

Задача 3.18.10. Пусть $n > 1$ и k — число простых чисел, делящих n . Тогда $\varphi(n) \geq 2^{k-1}$.

Задача 3.18.11. $\lim_{n \rightarrow \infty} \varphi(n) = +\infty$.

Задача 3.18.12. Пусть $A \in M_n(\mathbb{Z})$, $A = (a_{ij})$, $a_{ij} = \text{НОД}(i, j)$. Покажите, что $|A| = \varphi(1)\varphi(2) \cdots \varphi(n)$, где φ — функция Эйлера.

Задача 3.18.13. Пусть имеются бусинки n различных цветов, $N(m, n)$ — число различных ожерелий длины m , состоящих из имеющихся бусинок. Покажите, что

$$N(m, n) = \frac{1}{m} \sum_{d|m} n^d \varphi\left(\frac{m}{d}\right) = \frac{1}{m} \sum_{d|m} \varphi(d) n^{m/d}.$$

3.19. Многочлены деления круга

Пусть $n \in \mathbb{N}$, $\varphi(n)$ — функция Эйлера, $\varepsilon_1, \dots, \varepsilon_{\varphi(n)}$ — все примитивные корни степени n из 1. Многочлен

$$\Phi_n(x) = \prod_{i=1}^{\varphi(n)} (x - \varepsilon_i)$$

называется n -м многочленом деления круга ($\deg \Phi_n(x) = \varphi(n)$).

Задача 3.19.1.

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Задача 3.19.2. Применяя мультиплективную формулу обращения Мёбиуса, показать, что

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu\left(\frac{n}{d}\right)}.$$

Задача 3.19.3. Для простого числа p

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 = \frac{x^p - 1}{x - 1}.$$

Задача 3.19.4.

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d < n}} \Phi_d(x)},$$

что даёт возможность вычислить $\Phi_n(x)$ индуктивно.

Задача 3.19.5. $\Phi_n(x) \in \mathbb{Z}[x]$; свободный член многочлена $\Phi_n(x)$ равен -1 при $n = 1$ и равен 1 при $n > 1$; старший коэффициент многочлена $\Phi_n(x)$ равен 1 .

Задача 3.19.6. При небольших n :

$$\begin{aligned} \Phi_1(x) &= x - 1; & \Phi_2(x) &= x + 1; & \Phi_3(x) &= x^2 + x + 1; \\ \Phi_4(x) &= x^2 + 1; & \Phi_5(x) &= x^4 + x^3 + x^2 + x + 1; \\ \Phi_6(x) &= x^2 - x + 1; \\ \Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1; \\ \Phi_8(x) &= x^4 + 1; & \Phi_9(x) &= x^6 + x^3 + 1; \\ \Phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1; \\ \Phi_{11}(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1; \\ \Phi_{12}(x) &= x^4 - x^2 + 1; \\ \Phi_{13}(x) &= x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1; \\ \Phi_{14}(x) &= x^6 - x^5 + x^4 - x^3 + x^2 - x + 1; \\ \Phi_{15}(x) &= x^8 - x^7 + x^6 - x^4 + x^3 - x + 1. \end{aligned}$$

Замечание 3.19.7. Первые 104 многочлена деления круга имеют коэффициенты, равные $0, \pm 1$, однако многочлен $\Phi_{105}(x)$ имеет -2 одним из своих коэффициентов,

$$\begin{aligned} \Phi_{105}(x) = 1 + x + x^2 - x^5 - x^6 - 2x^7 - x^8 - x^9 + x^{12} + x^{13} + x^{14} + x^{15} + \\ + x^{16} + x^{17} - x^{20} - x^{22} - x^{24} - x^{26} - x^{28} + x^{31} + x^{32} + x^{33} + x^{34} + \\ + x^{35} + x^{36} - x^{39} - x^{40} - 2x^{41} - x^{42} - x^{43} + x^{46} + x^{47} + x^{48}. \end{aligned}$$

Более того, модули коэффициентов многочлена $\Phi_n(x)$ не ограничены при стремлении n к бесконечности (И. Шур). Если же n является произведением двух различных простых чисел или степенью простого числа, то все коэффициенты многочлена Φ_n равны $\pm 1, 0$.

Задача 3.19.8. Если p — простое число и $p \mid n$, то $\Phi_{pn}(x) = \Phi_n(x^p)$; если же $p \nmid n$, то $\Phi_{pn}(x) = \frac{\Phi_n(x^p)}{\Phi_p(x)}$. В частности, для $k \geq 1$ имеем $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$.

Задача 3.19.9. Если k делится на любой простой делитель числа n , то $\Phi_n(x) = \Phi_k(x^{\frac{n}{k}})$.

Задача 3.19.10. Если n делится на простое число p и не делится на p^2 , то $\Phi_n(x) = \Phi_{\frac{n}{p}}(x^p)(\Phi_{\frac{n}{p}}(x))^{-1}$.

Задача 3.19.11. Если m — нечётное число, $m > 1$, то $\Phi_{2m}(x) = \Phi_m(-x)$.

Задача 3.19.12. $\Phi_n(x) = x^{\varphi(n)}\Phi_n(x^{-1})$.

Задача 3.19.13. Для любого числа $n \in \mathbb{N}$ многочлен $\Phi_n(x)$ неприводим над полем рациональных чисел \mathbb{Q} . Однако многочлены $\Phi_n(x)$ могут быть приводимы над конечными полями. Например, в кольце $\mathbb{Z}_2[x]$ над полем \mathbb{Z}_2

$$\Phi_4(x) = (x+1)^2; \quad \Phi_{15}(x) = (x^4+x^3+1)(x^4+x+1).$$

В кольце $\mathbb{Z}_3[x]$ над полем \mathbb{Z}_3

$$\Phi_8(x) = (x^2+x-1)(x^2-x-1).$$

Упражнение 3.19.14. Покажите, что $x^{15} - 1 = \Phi_{15}(x)\Phi_5(x)\Phi_3(x)\Phi_1(x)$ в $\mathbb{Z}_2[x]$.

3.20. Рациональные дроби и функции

Пусть K — поле, $K[x]$ — кольцо многочленов над полем K . Рациональной дробью называется пара многочленов

$$\frac{f(x)}{g(x)}, \quad f(x), g(x) \in K[x], \quad g(x) \neq 0.$$

На рациональных дробях рассматривается следующее отношение эквивалентности: две рациональные дроби $\frac{f(x)}{g(x)}$ и $\frac{f_1(x)}{g_1(x)}$ равны, если $f(x)g_1(x) = g(x)f_1(x)$.

Упражнение 3.20.1. Показать, что классы равных между собой рациональных дробей (называемые рациональными функциями) с естественно определёнными операциями сложения и умножения образуют поле $K(x)$ рациональных функций (поле частных кольца $K[x]$). Так как $K \subset K[x] \subset K(x)$, то $\text{char } K = \text{char } K(x)$.

Рациональная дробь $\frac{f(x)}{g(x)}$ называется несократимой, если многочлены $f(x)$ и $g(x)$ взаимно просты, и правильной, если $\deg f(x) < \deg g(x)$ (или если $f(x) = 0$).

Лемма 3.20.2. Всякая рациональная дробь $\frac{f(x)}{g(x)}$ равна некоторой несократимой дроби $\frac{f_1(x)}{g_1(x)}$, определяемой однозначно, с точностью до множителя $0 \neq c \in K$ (т. е. $\frac{cf_1(x)}{cg_1(x)}$).

Доказательство. 1) Если $d(x) = \text{НОД}(f(x), g(x))$, $f(x) = d(x)f_1(x)$, $g(x) = d(x)g_1(x)$, $(f_1(x), g_1(x)) = 1$, то $\frac{f(x)}{g(x)} = \frac{f_1(x)}{g_1(x)}$.

2) Если $\frac{f(x)}{g(x)} = \frac{\varphi(x)}{\psi(x)}$ — две равные несократимые дроби, то $f(x)\psi(x) = g(x)\varphi(x)$. Так как правая часть делится на $g(x)$ и $(f(x), g(x)) = 1$, то $\psi(x)$ делится на $g(x)$. Аналогично, левая часть делится на $\psi(x)$, $(\varphi(x), \psi(x)) = 1$, и поэтому $g(x)$ делится на $\psi(x)$. Таким образом, $cg(x) = \psi(x)$, $0 \neq c \in K$. Поэтому $cf(x)g(x) = g(x)\varphi(x)$. Сокращая на $g(x)$, получаем $\varphi(x) = cf(x)$. \square

Лемма 3.20.3. Всякая рациональная дробь $\frac{f(x)}{g(x)}$ представима (и единственным образом) в виде суммы многочлена и правильной дроби.

Доказательство. (1) Пусть $f(x) = g(x)q(x) + r(x)$, где или $r(x) = 0$, или $\deg r(x) < \deg g(x)$. Тогда $\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$.

(2) Если $\frac{f(x)}{g(x)} = \bar{q}(x) + \frac{\varphi(x)}{\psi(x)}$, где $\bar{q}(x) \in K[x]$, или $\varphi(x) = 0$, или $\deg \varphi(x) < \deg \psi(x)$, то

$$q(x) - \bar{q}(x) = \frac{\varphi(x)g(x) - \psi(x)r(x)}{\psi(x)g(x)}.$$

Из сравнения степеней видим, что $q(x) = \bar{q}(x)$, $\varphi(x)g(x) - \psi(x)r(x) = 0$, т. е. $\frac{\varphi(x)}{\psi(x)} = \frac{r(x)}{g(x)}$. \square

Правильная рациональная дробь $\frac{f(x)}{g(x)}$ называется простейшей, если $g(x) = p^k(x)$, где $p(x)$ — неприводимый многочлен, $k \geq 1$ и $\deg f(x) < \deg p(x)$.

Теорема 3.20.4. Всякая правильная рациональная дробь разлагается (и единственным образом) в сумму простейших.

Доказательство существования разложения

Сначала докажем следующее утверждение.

Лемма 3.20.5. Если $\frac{f(x)}{g(x)h(x)}$ — правильная дробь и $(g(x), h(x)) = 1$, то

$$\frac{f(x)}{g(x)h(x)} = \frac{u(x)}{h(x)} + \frac{v(x)}{g(x)},$$

где $\frac{u(x)}{h(x)}$, $\frac{v(x)}{g(x)}$ — правильные дроби.

Доказательство. Пусть

$$g(x)\bar{u}(x) + h(x)\bar{v}(x) = 1.$$

Умножая на $f(x)$, получаем

$$g(x)\bar{u}(x)f(x) + h(x)\bar{v}(x)f(x) = f(x).$$

Пусть $\bar{u}(x)f(x) = h(x)q(x) + u(x)$, где или $u(x) = 0$, или $\deg u(x) < \deg h(x)$. Тогда

$$g(x)u(x) + h(x)v(x) = f(x),$$

где $v(x) = \bar{v}(x)f(x) + g(x)q(x)$. Из сравнения степеней получаем, что $\deg v(x) < \deg g(x)$. Тогда

$$\frac{f(x)}{g(x)h(x)} = \frac{u(x)}{h(x)} + \frac{v(x)}{g(x)},$$

$\frac{u(x)}{h(x)}$ и $\frac{v(x)}{g(x)}$ — правильные дроби. \square

Если $g(x) = p_1^{k_1}(x) \dots p_r^{k_r}(x)$ — разложение в произведение неприводимых многочленов, то

$$\frac{f(x)}{g(x)} = \frac{u_1(x)}{p_1^{k_1}(x)} + \dots + \frac{u_r(x)}{p_r^{k_r}(x)},$$

где слагаемые в правой части — правильные дроби.

Далее, если $\frac{u(x)}{p^k(x)}$ — правильная дробь и $p(x)$ — неприводимый многочлен, то, проводя последовательно деления с остатком

$$\begin{aligned} u &= p^{k-1}s_1 + u_1, \\ u_1 &= p^{k-2}s_2 + u_2, \\ &\dots \\ u_{k-2} &= ps_{k-1} + u_{k-1}, \end{aligned}$$

получаем

$$u = p^{k-1}s_1 + p^{k-2}s_2 + \dots + ps_{k-1} + u_{k-1},$$

и поэтому

$$\frac{u}{p^k} = \frac{u_{k-1}}{p^k} + \frac{s_{k-1}}{p^{k-1}} + \dots + \frac{s_1}{p} -$$

разложение в сумму простейших дробей. \square

Доказательство единственности представления правильной рациональной дроби в виде суммы простейших дробей

Допустим противное, т. е. что некоторая правильная рациональная дробь допускает два различных представления в виде суммы простейших дробей. Вычитая из одного представления другое и приводя подобные члены, приходим к нетривиальной сумме простейших дробей, равной нулю. Пусть $p_1(x), \dots, p_s(x)$ — все различные неприводимые многочлены, входящие своими степенями в знаменатели. Пусть k_i — наивысшая среди них степень многочлена $p_i(x)$, $i = 1, \dots, s$. Умножим наши равенства на $p_1^{k_1-1}(x)p_2^{k_2}(x)\dots p_s^{k_s}(x)$, тогда все слагаемые в нашей сумме окажутся многочленами, кроме одного, который из $\frac{u(x)}{p_1^{k_1}(x)}$ превратится в дробь $\frac{u(x)p_2^{k_2}(x)\dots p_s^{k_s}(x)}{p_1(x)}$. Так как многочлен $p_1(x)$ неприводим, а все множители числителя взаимно просты с $p_1(x)$, то числитель не делится нацело на знаменатель. Разделив числитель на $p_1(x)$ с остатком, мы получим, что сумма многочлена и отличной от нуля правильной дроби равна нулю, что приводит нас к противоречию. \square

Пример 3.20.6. $\frac{f(x)}{g(x)} \in \mathbb{R}(x)$,

$$\begin{aligned} f(x) &= 2x^4 - 10x^3 + 7x^2 + 4x + 3, \\ g(x) &= x^5 - 2x^3 + 2x^2 - 3x + 2. \end{aligned}$$

Так как $g(x) = (x+2)(x-1)^2(x^2+1)$, то разложение в сумму простейших дробей ищем в виде

$$\frac{f(x)}{g(x)} = \frac{A}{x+2} + \frac{B}{(x-1)^2} + \frac{C}{x-1} + \frac{Dx+E}{x^2+1}.$$

Приводя дроби к общему знаменателю и сравнивая коэффициенты при степенях, вычисляем, что

$$A = 3, \quad B = 1, \quad C = -2, \quad D = 1, \quad E = -3,$$

т. е.

$$\frac{f(x)}{g(x)} = \frac{3}{x+2} + \frac{1}{(x-1)^2} - \frac{2}{x-1} + \frac{x-3}{x^2+1}.$$

Замечание 3.20.7. В частном случае, когда знаменатель $g(x)$ рациональной дроби $\frac{f(x)}{g(x)}$, $\deg f < \deg g$, имеет различные корни x_1, x_2, \dots, x_n ,

$$g(x) = (x - x_1)(x - x_2) \cdots (x - x_n),$$

рациональная дробь имеет разложение в простейшие:

$$\frac{f(x)}{g(x)} = \sum_{i=1}^n \frac{A_i}{x - x_i}.$$

Умножая обе части равенства на $x - x_i$ и подставляя $x = x_i$, получаем

$$A_i = \frac{f(x_i)}{\prod_{\substack{j=1 \\ i \neq j}}^n (x_i - x_j)} = \frac{f(x_i)}{g'(x_i)},$$

следовательно,

$$\frac{f(x)}{g(x)} = \sum_{i=1}^n \frac{f(x_i)}{(x - x_i)g'(x_i)}.$$

Отсюда (умножая на $g(x)$ это равенство) получаем другой вывод интерполяционной формулы Лагранжа:

$$f(x) = \sum_{i=1}^n \frac{g(x)f(x_i)}{(x - x_i)g'(x_i)}.$$

Упражнение 3.20.8. Покажите, что

$$\frac{n!}{(x+1)(x+2) \cdots (x+n)} = \frac{C_n^1}{x+1} - \frac{2C_n^2}{x+2} + \frac{3C_n^3}{x+3} + \cdots + (-1)^{n+1} \frac{n \cdot C_n^n}{x+n}.$$

3.21. Границы корней многочлена с действительными коэффициентами

Лемма 3.21.1. Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{R}[x],$$

$a_n \neq 0$, $A = \max\{|a_0|, |a_1|, \dots, |a_{n-1}|\}$, $K = 1 + \frac{A}{|a_n|}$. Тогда если $x_0 \in \mathbb{R}$ и $|x_0| \geq K$, то x_0 не является корнем многочлена $f(x)$. Таким образом, если многочлен $f(x)$ имеет действительные корни, то все они принадлежат интервалу $(-K, K)$.

Доказательство. Ясно, что $K \geq 1$. Если $K = 1$, то $A = 0$ и $a_0 = a_1 = \dots = a_{n-1} = 0$, то есть $f(x) = a_n x^n$, все его корни равны нулю. Ясно, что число x_0 такое, что $|x_0| \geq 1$, не является его корнем.

Если же $K > 1$, то $|x_0| \geq K > 1$. Тогда

$$\begin{aligned} D &= |a_{n-1}x_0^{n-1} + \dots + a_1x_0 + a_0| \leqslant \\ &\leqslant |a_{n-1}| |x_0|^{n-1} + \dots + |a_1| |x_0| + |a_0| \leqslant \\ &\leqslant A(|x_0|^{n-1} + \dots + |x_0| + 1) = A \frac{|x_0|^n - 1}{|x_0| - 1} < A \frac{|x_0|^n}{|x_0| - 1}. \end{aligned}$$

Так как $|x_0| \geq 1 + \frac{A}{|a_n|}$, то $|x_0| - 1 \geq \frac{A}{|a_0|}$, следовательно, $|a_0| \geq \frac{A}{|x_0| - 1}$, и поэтому $D < |a_0 x_0^n|$. Ясно, что $|f(x_0)| \geq |a_0 x_0^n| - D > 0$, поэтому $f(x) \neq 0$. \square

Замечание 3.21.2. Аналог утверждения леммы 3.21.1 справедлив для комплексных многочленов (неравенство Коши): если $f(z) = a_n z^n + \dots + a_0 \in \mathbb{C}[x]$, $a_n \neq 0$, $f(x) = 0$ ($x \in \mathbb{C}$), то

$$|x| < 1 + \frac{\max\{|a_0|, |a_1|, \dots, |a_n|\}}{|a_n|}.$$

См. также следствие 3.29.4.

Для положительных корней более точная (верхняя) граница даётся следующей оценкой Маклорена.

Теорема 3.21.3. Пусть

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{R}[x],$$

$a_n > 0$, $K_1 = 1 + \sqrt[m]{\frac{M}{a_n}}$, где M — максимум модуля отрицательных коэффициентов многочлена $f(x)$, $(n-m)$ — номер первого отрицательного коэффициента, считая с левой стороны. Если $x_0 \in \mathbb{R}$ и $x_0 \geq K_1$, то $f(x_0) \neq 0$.

Доказательство. Если многочлен $f(x)$ не имеет отрицательных коэффициентов, то он не имеет положительных корней.

Если же $M > 0$ и $x_0 \geq K_1$, то $x_0 > 1$ и

$$\begin{aligned} f(x_0) &= a_n x_0^n + \dots + a_{n-m+1} x_0^{n-m+1} + a_{n-m} x_0^{n-m} + \dots + a_1 x_0 + a_0 \geq \\ &\geq a_n x_0^n - M(x_0^{n-m} + \dots + x_0 + 1) = a_n x_0^n - M \frac{x_0^{n-m+1} - 1}{x_0 - 1} = \\ &= \frac{x_0^{n-m+1}(a_n x_0^{m-1}(x_0 - 1) - M)}{x_0 - 1} + \frac{M}{x_0 - 1} > \\ &> \frac{x_0^{n-m+1}(a_n x_0^{m-1}(x_0 - 1) - M)}{x_0 - 1} > \frac{x_0^{n-m+1}(a_n(x_0 - 1)^m - M)}{x_0 - 1} \geq \\ &\geq \frac{x_0^{n-m+1} \left(a_n \left(\sqrt[m]{\frac{M}{a_n}} \right)^m - M \right)}{x_0 - 1} = \frac{x_0^{n-m+1}(M - M)}{x_0 - 1} = 0. \end{aligned}$$

Итак, мы показали, что $f(x_0) > 0$. \square

Пусть $f(x) \in \mathbb{R}[x]$, $\deg f(x) = n > 0$, N_0 — верхняя граница его положительных корней, $\varphi_1(x) = x^n f\left(\frac{1}{x}\right)$, $\varphi_2(x) = f(-x)$, $\varphi_3(x) = x^n f\left(-\frac{1}{x}\right)$, N_1, N_2, N_3 — соответственно верхние границы положительных корней многочленов $\varphi_1(x), \varphi_2(x), \varphi_3(x)$. Ясно, что $\frac{1}{N_1}$ — нижняя граница положительных корней многочлена $f(x)$, $-N_2$ и $-\frac{1}{N_3}$ — соответственно нижняя и верхняя границы отрицательных корней многочлена $f(x)$.

Замечание 3.21.4 (Ньютона). Из представления многочлена $f(x)$ в виде многочлена Тейлора в точке $c \in \mathbb{R}$,

$$f(x) = f(c) + f'(c)(x - c) + \dots + \frac{f^{(n)}(c)}{n!}(x - c)^n,$$

следует, что если

$$f(c) > 0, f'(c) > 0, \dots, f^{(n)}(c) > 0,$$

то c — верхняя граница положительных корней многочлена $f(x)$. Как и выше, нижняя граница отрицательных корней находится с помощью верхней границы положительных корней многочлена $f(-x)$.

Пример 3.21.5. $f(x) = x^4 - 3x^3 + 8x^2 - 5 = 0$.

а) Тогда $K = 1 + \sqrt[8]{\frac{5}{1}} = 9$, то есть все действительные корни многочлена $f(x)$ (если они есть) принадлежат интервалу $(-9, 9)$.

б) Оценка Маклорена даёт $N_0 = K_1 = 1 + \frac{5}{1} = 6$ (верхняя граница положительных корней). Для получения нижней оценки отрицательных корней рассматриваем

$$\varphi_2(x) = f(-x) = x^4 + 3x^3 + 8x^2 - 5,$$

$N_2 = K'_1 = 1 + \sqrt[4]{\frac{5}{1}}, N_2 < 2,5, -N_2 > -2,5$. Таким образом, для корней получаем интервал $(-2,5, 6) (\subset (-9, 9))$.

в) Рассмотрим теперь производные многочлена $f(x)$:

$$\begin{aligned} f(x) &= x^4 - 3x^3 + 8x^2 - 5, \\ f'(x) &= 4x^3 - 9x^2 + 16x, \\ f''(x) &= 12x^2 - 18x + 16, \\ f^{(3)}(x) &= 24x - 18, \\ f^{(4)}(x) &= 24. \end{aligned}$$

Нетрудно видеть, что

$$f(1) > 0, f'(1) > 0, f''(1) > 0, f^{(3)}(1) > 0, f^{(4)}(1) > 0.$$

Таким образом, 1 — верхняя граница положительных корней многочлена $f(x)$. Рассматривая многочлен $\varphi_2(x) = f(-x)$, с помощью метода Ньютона убеждаемся в том, что -1 — нижняя граница отрицательных корней многочлена $f(x)$. Итак, все действительные корни многочлена $f(x)$ (если они есть) принадлежат интервалу $(-1, 1)$.

Теорема 3.21.6 (Коши). Пусть

$$f(x) = x^n - b_{n-1}x^{n-1} - \dots - b_1x - b_0 \in \mathbb{R}[x],$$

$b_i \in \mathbb{R}$, $b_i \geq 0$, при этом хотя бы один из этих коэффициентов b_i отличен от нуля. Тогда:

- 1) многочлен $f(x)$ имеет единственный положительный корень с кратностью 1,
- 2) модули $|\alpha|$ остальных корней α не превосходят числа c , т. е. $|\alpha| \leq c$.

Доказательство. 1) Функция

$$F(x) = -\frac{f(x)}{x^n} = -1 + \frac{b_{n-1}}{x} + \dots + \frac{b_0}{x^n}$$

при возрастании x от 0 к $+\infty$ строго убывает от $+\infty$ до -1 , следовательно, она обращается в нуль ровно в одной точке $c > 0$. Для $x \neq 0$ условия $f(x) = 0$ и $F(x) = 0$ равносильны, поэтому $f(c) = 0$.

Так как

$$F'(c) = -\frac{f'(c)}{c^n} + \frac{nf(c)}{c^{n+1}} = -\frac{f'(c)}{c^n} = -\frac{b_{n-1}}{c^2} - \dots - \frac{nb_0}{c^{n+1}} < 0,$$

то $f'(c) \neq 0$, поэтому кратность корня многочлена $f(x)$ равна 1.

2) Пусть $f(\alpha) = 0$, $\alpha \in \mathbb{C}$. Допустим противное, т. е. что $c < |\alpha|$. Тогда

$$0 = F(c) > F(|\alpha|) = -\frac{f(|\alpha|)}{|\alpha|^n}.$$

Следовательно, $f(|\alpha|) > 0$. С другой стороны,

$$\alpha^n = b_{n-1}\alpha^{n-1} + \dots + b_1\alpha + b_0,$$

поэтому

$$|\alpha|^n \leq b_{n-1}|\alpha|^{n-1} + \dots + b_1|\alpha| + b_0,$$

т. е. $f(|\alpha|) \leq 0$, что приводит к противоречию.

Итак, мы показали, что $|\alpha| \leq c$.

Замечание 3.21.7. В условиях теоремы Коши возможно, что $|\alpha| = c$ для $\alpha \neq 0$: так как

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

то многочлен $x^{2n} - x^n - 1$ имеет ровно n корней, модули которых равны единственному положительному корню этого многочлена.

Замечание 3.21.8. Если в теореме Коши дополнительно предположить, что наибольший общий делитель номеров положительных коэффициентов a_i равен 1, то многочлен $f(x)$ имеет единственный положительный корень $c > 0$, а модули остальных корней α строго меньше, чем c (т. е. $|\alpha| < c$).

Упражнение 3.21.9. Пусть $z_1, \dots, z_n \in \mathbb{C}$ — точки, в которых расположены единичные массы,

$$m = \frac{z_1 + \dots + z_n}{n}$$

центр масс точек z_1, \dots, z_n . Если $z_0 \in \mathbb{C}$, то

$$m(z_0) = z_0 + n \left(\frac{1}{z - z_0} + \dots + \frac{1}{z_n - z_0} \right)^{-1} -$$

центр масс точек z_1, \dots, z_n относительно точки z_0 . Пусть

$$f(z) = (z - z_1) \dots (z - z_n) \in \mathbb{C}[z],$$

тогда центр масс корней многочлена $f(z)$ относительно произвольной точки $z_0 \in \mathbb{C}$ вычисляется по формуле

$$m(z_0) = z_0 - n \frac{f(z_0)}{f'(z_0)}.$$

Действительно, следует учесть, что

$$\frac{f'(z)}{f(z)} = (z - z_1)^{-1} + \dots + (z - z_n)^{-1}.$$

Упражнение 3.21.10 (теорема Лагерра). Пусть $f(z) \in \mathbb{C}[z]$, $\deg f(z) = n$, c — его корень кратности 1, тогда центр масс всех $n - 1$ остальных корней относительно точки $c \in \mathbb{C}$ равен $c - 2(n - 1) \frac{f'(c)}{f''(c)}$.

3.22. Число действительных корней многочлена с действительными коэффициентами на отрезке

Пусть $f(x) \in \mathbb{R}[x]$ — многочлен с действительными коэффициентами. Одно из достижений алгоритмической (компьютерной) алгебры — *теорема Штурма* (1829 г.), дающая алгоритм для вычисления числа действительных корней многочлена $f(x) \in \mathbb{R}[x]$ на отрезке $[a, b]$, $a, b \in \mathbb{R}$, $a < b$ (случай $a = -\infty$, $b = +\infty$ для расширенной прямой $\bar{\mathbb{R}}$ даёт число всех вещественных корней многочлена $f(x)$).

Ясно, что достаточно эту задачу решить для многочлена без кратных корней (общий случай сводится к этому переходом от многочлена $f(x)$ к многочлену $f(x)/(f(x), f'(x))$, имеющему в точности те же корни, что и многочлен $f(x)$, но кратности, равной 1). В этом случае $\text{НОД}(f(x), f'(x)) = c \neq 0$, $c \in \mathbb{R}$.

3.23. Алгоритм Евклида и система многочленов Штурма

На основе алгоритма Евклида нахождения наибольшего общего делителя построим следующую каноническую систему многочленов Штурма для многочлена $f(x) \in \mathbb{R}[x]$.

Пусть $f_0(x) = f(x)$, $f_1(x) = f'(x)$. Далее используем следующую модификацию в алгоритме Евклида (остатки от последующих делений будем брать с противоположным знаком):

$$f_0(x) = f_1(x)q_1(x) - f_2(x),$$

$$\vdots$$

$$f_{k-1}(x) = f_k(x)q_k(x) - f_{k+1}(x),$$

$$\vdots$$

$$f_{s-2}(x) = f_{s-1}(x)q_{s-1}(x) - f_s(x),$$

$$f_{s-1}(x) = f_s(x)q_s(x) - 0,$$

здесь $f_s(x) = \text{НОД}(f(x), f'(x)) = c \neq 0$, $c \in \mathbb{R}$ (т. е. ненулевая константа).

Под канонической системой Штурма для многочлена $f(x) \in \mathbb{R}[x]$ без кратных корней понимаем следующую систему многочленов:

$$f_0(x) = f(x), \quad f_1(x) = f'(x), \quad f_2(x), \dots, \quad f_s(x) = c \neq 0.$$

Свойства системы многочленов Штурма $f_0(x), f_1(x), \dots, f_s(x)$

1) Соседние многочлены $f_k(x)$ и $f_{k+1}(x)$ не имеют общих корней.

Доказательство. Пусть

$$f_k(\alpha) = 0 = f_{k+1}(\alpha), \quad \text{где } \alpha \in \mathbb{R}.$$

Тогда

$$f_{k-1}(\alpha) = f_k(\alpha)q_k(\alpha) - f_{k+1}(\alpha) = 0,$$

и поэтому, поднимаясь вверх по схеме алгоритма Евклида, имеем $f'(\alpha) = 0$, $f(\alpha) = 0$, что противоречит отсутствию кратных корней для $f(x)$. \square

2) Ясно, что последний многочлен $f_s(x) = c \neq 0$, $c \in \mathbb{R}$, не имеет действительных корней.

3) Если $1 \leq k \leq s-1$ и $f_k(\alpha) = 0$, $\alpha \in \mathbb{R}$, то

$$f_{k-1}(\alpha)f_{k+1}(\alpha) < 0$$

(т. е. действительные ненулевые числа $f_{k-1}(\alpha)$ и $f_{k+1}(\alpha)$ имеют противоположные знаки).

Доказательство. Так как

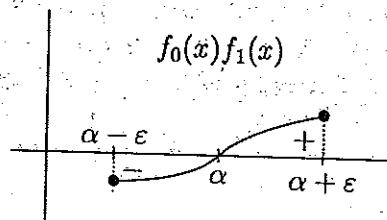
$$f_{k-1}(x) = f_k(x)q_k(x) - f_{k+1}(x),$$

то

$$f_{k-1}(\alpha) = -f_{k+1}(\alpha),$$

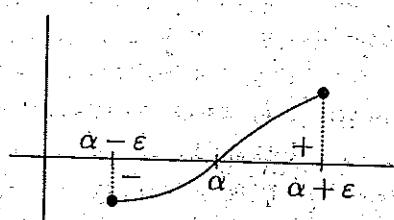
при этом в силу 1) $f_{k-1}(\alpha) \neq 0$. \square

4) Если $f(\alpha) = 0$ для $\alpha \in \mathbb{R}$, то многочлен $f_0(x)f_1(x)$ при переходе через $x = \alpha$ меняет знак — на +, т. е. график многочлена $f_0(x)f_1(x)$ в достаточно малой окрестности $O(\alpha) = (\alpha - \varepsilon, \alpha + \varepsilon)$ точки α имеет следующий вид:

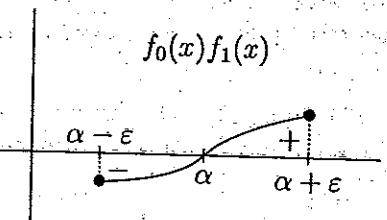


Доказательство. Так как $f_0(\alpha) = f(\alpha) = 0$, то в силу 1) $f_1(\alpha) = f'(\alpha) \neq 0$.

Случай а). Пусть $f_1(\alpha) = f'(\alpha) > 0$. Тогда $f_1(x) = f'(x) > 0$ во всех точках x достаточно малой окрестности $O(\alpha) = (\alpha - \varepsilon, \alpha + \varepsilon)$ точки α . Таким образом, в этой окрестности $O(\alpha)$ функция $f(x)$ строго возрастающая, т. е.

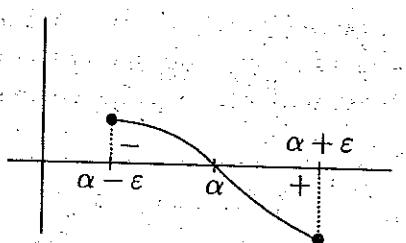


Умножая в этой окрестности на непрерывную функцию $f_1(x)$, где $f_1(x) > 0$, получаем, что функция $f_0(x)f_1(x)$

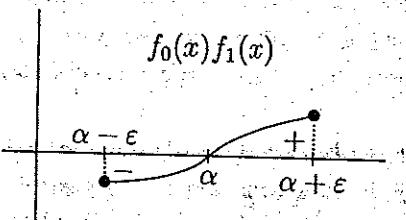


переходит со знака — на + в достаточно малой окрестности $O(\alpha)$ точки α .

Случай б). Пусть $f_1(\alpha) = f'(\alpha) < 0$. Тогда $f_1(x) = f'(x) < 0$ во всех точках x достаточно малой окрестности $O(\alpha) = (\alpha - \varepsilon, \alpha + \varepsilon)$ точки α . Таким образом, в этой окрестности $O(\alpha)$ функция $f(x)$ строго убывающая, т. е.



Умножая в этой окрестности на непрерывную функцию $f_1(x)$, где $f_1(x) < 0$, получаем, что функция $f_0(x)f_1(x)$



переходит со знака $-$ на $+$ в достаточно малой окрестности $O(\alpha)$ точки α . \square

3.24. Число перемен знаков в системе значений многочленов системы Штурма

Если $f(x) \in \mathbb{R}[x]$, $(f(x), f'(x)) = 1$,

$$f_0(x) = f(x), f_1(x) = f'(x), \dots, f_s(x) =$$

система многочленов Штурма для многочлена $f(x)$, $c \in \mathbb{R}$, то в ряду действительных чисел

$$f_0(c), f_1(c), \dots, f_s(c)$$

выбросим нулевые значения и подсчитаем число перемен знаков $W(c)$ в оставшемся ряду ненулевых действительных чисел.

Теорема Штурма. Пусть $f(x) \in \mathbb{R}[x]$ — многочлен с действительными коэффициентами без кратных корней (т. е. $\text{НОД}(f(x), f'(x)) = 1$),

$$f_0(x) = f(x), f_1(x) = f'(x), \dots, f_s(x) =$$

его система Штурма, $a, b \in \mathbb{R}$, $a < b$ (возможно, $a = -\infty$, $b = +\infty$ для расширенной действительной оси), $f(a) \neq 0$, $f(b) \neq 0$. Тогда:

- 1) $W(a) \geq W(b)$;
- 2) разность $W(a) - W(b)$ равна числу действительных корней между a и b (т. е. в интервале (a, b)).

Доказательство. Проанализируем поведение знаков значений многочленов системы Штурма

$$f_0(\alpha), f_1(\alpha), \dots, f_s(\alpha)$$

при движении $\alpha \in \mathbb{R}$ от $-\infty$ к $+\infty$.

Случай 1 (переход через корень α многочлена $f_k(\alpha)$, $1 \leq k \leq s-1$). Пусть $f_k(\alpha) = 0$ для $1 \leq k \leq s-1$. Тогда в силу свойства 1) $f_{k-1}(\alpha) \neq 0$, $f_{k+1}(\alpha) \neq 0$. Тогда в достаточно малой окрестности $O(\alpha) = (\alpha - \varepsilon, \alpha + \varepsilon)$ многочлены $f_{k-1}(x)$ и $f_{k+1}(x)$ не имеют корней, и поэтому сохраняют знаки своих значений, которые, в силу 3), противоположны.

Рассмотрим таблицу значений многочленов $f_{k-1}(x)$, $f_k(x)$, $f_{k+1}(x)$ в точках $\alpha - \varepsilon$, α , $\alpha + \varepsilon$:

$\alpha - \varepsilon$	$f_{k-1}(\alpha - \varepsilon)$	$f_k(\alpha - \varepsilon)$	$f_{k+1}(\alpha - \varepsilon)$
α	$f_{k-1}(\alpha)$	$f_k(\alpha) = 0$	$f_{k+1}(\alpha)$
$\alpha + \varepsilon$	$f_{k-1}(\alpha + \varepsilon)$	$f_k(\alpha + \varepsilon)$	$f_{k+1}(\alpha + \varepsilon)$

в которой для среднего столбца возможны столбцы

$$\begin{pmatrix} - \\ 0 \\ + \end{pmatrix} \quad \text{или} \quad \begin{pmatrix} + \\ 0 \\ - \end{pmatrix}$$

крайние столбцы (первый и третий) имеют постоянные противоположные знаки, т. е.

$$\begin{pmatrix} - \\ - \\ - \end{pmatrix} \text{ и } \begin{pmatrix} + \\ + \\ + \end{pmatrix}, \quad \text{или} \quad \begin{pmatrix} + \\ + \\ + \end{pmatrix} \text{ и } \begin{pmatrix} - \\ - \\ - \end{pmatrix}.$$

Таким образом, во всех возможных четырёх случаях при переходе через α от $\alpha - \varepsilon$ к $\alpha + \varepsilon$ число перемен знаков $W(x)$ не меняется (оно равно 1 для нашей таблицы):

$$\underbrace{\begin{array}{c} \begin{pmatrix} - & - & + \\ - & 0 & + \\ - & + & + \end{pmatrix}, \quad \begin{pmatrix} + & - & - \\ + & 0 & - \\ + & + & - \end{pmatrix}; \\ \begin{pmatrix} - & + & + \\ - & 0 & + \\ - & - & + \end{pmatrix}, \quad \begin{pmatrix} + & + & - \\ + & 0 & - \\ + & - & - \end{pmatrix}. \end{array}}$$

Случай 2 (переход через корень α многочлена $f_0(x) = f(x)$). Пусть $f_0(\alpha) = f(\alpha) = 0$ для $\alpha \in \mathbb{R}$. Тогда в силу 1) $f_1(\alpha) \neq 0$. Поэтому в достаточно малой окрестности $O(\alpha) = (\alpha - \varepsilon, \alpha + \varepsilon)$ точки α многочлен $f_1(x)$ сохраняет знак (не обращаясь в нуль).

Вариант а: $f_1(x) > 0$ для всех $x \in O(\alpha)$. Так как в силу 4) при переходе через α произведение $f(x)f_1(x)$ меняет знак $-$ на знак $+$, то многочлен $f(x)$ при переходе через α также меняет знак $-$ на знак $+$. Таким образом, возможна следующая таблица для

$$\begin{array}{c|cc} \alpha - \varepsilon & f_0(\alpha - \varepsilon) & f_1(\alpha - \varepsilon) \\ \hline \alpha & f_0(\alpha) & f_1(\alpha) \\ \alpha + \varepsilon & f_0(\alpha + \varepsilon) & f_1(\alpha + \varepsilon) \end{array} ;$$

$$\begin{pmatrix} - & + \\ 0 & + \\ + & + \end{pmatrix},$$

т. е. наш счётчик $W(x)$ в этой таблице при переходе через α уменьшил своё значение на 1 (от 1 к 0).

Вариант б: $f_1(x) < 0$ для всех $x \in O(\alpha)$. Так как в силу 4) при переходе через α произведение $f(x)f_1(x)$ меняет знак $-$ на знак $+$, то многочлен $f(x)$ при переходе через α меняет знак $+$ на знак $-$. Таким образом, возможна лишь следующая таблица:

$$\begin{pmatrix} + & - \\ 0 & - \\ - & - \end{pmatrix},$$

т. е. наш счётчик $W(x)$ в этой таблице при переходе через α уменьшил своё значение на 1 (от 1 к 0). \square

Пример 3.24.1. $f(x) = x^3 + 3x^2 - 1 \in \mathbb{R}[x]$. Тогда $f_1(x) = f'(x) = 3x^2 + 6x$. Ясно, что $\text{НОД}(f(x), f'(x)) = 1$. Далее по алгоритму Евклида $f_2(x) = 2x + 1$, $f_3(x) = 1$. Следовательно,

	f_0	f_1	f_2	f_3	$W(x)$
$x = -\infty$	-	+	-	+	3
$x = +\infty$	+	+	+	+	0

т. е. $f(x)$ имеет три действительных корня.

Более того, теорема Штурма является эффективным средством (в комбинации с определением границ корней) для решения *проблемы локализации* (указания интервалов, содержащих ровно один действительный корень; это позволяет к этому интервалу применять алгоритмы нахождения корня). Например, в нашем случае, так как $x^3 + 3x^2 = x^2(x+3) > 1$ при $x \geq 1$ и для $x = -z$ многочлен $-f(z) = z^3 - 3z^2 - 1$ при $z \geq 4$ не имеет корней ($z^2(z-3) > 1$ при $z \geq 4$), то все действительные корни многочлена $f(x)$ принадлежат интервалу $(-4, 1)$. Более точно,

	f_0	f_1	f_2	f_3	$W(x)$
-3	-	+	-	+	3
-1	+	-	-	+	2
0	-	0	+	+	1
1	+	+	+	+	0

т. е. интервалы $(-3, -1)$, $(-1, 0)$, $(0, 1)$ содержат в точности по одному действительному корню.

Замечание 3.24.2. Теорема Штурма справедлива для любой *системы многочленов Штурма*

$$\varphi_0(x), \varphi_1(x), \dots, \varphi_s(x), \text{ где } \varphi_0(x) = f(x),$$

удовлетворяющих рассмотренным свойствам 1)–4) последовательности многочленов в теореме Штурма.

Пример 3.24.3. Система

$$\lambda_0 f_0(x), \lambda_1 f_1(x), \dots, \lambda_s f_s(x),$$

где $\lambda_0, \dots, \lambda_s > 0$, f_0, \dots, f_s — каноническая система Штурма, является системой Штурма.

Замечание 3.24.4 (система Штурма для отрезка $[a, b]$). Последовательность ненулевых многочленов

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

называется системой Штурма для многочлена $f(x)$ на отрезке $[a, b]$, если выполнены следующие условия:

- 1) если $f_k(c) = 0$ для $c \in [a, b]$ и $1 \leq k \leq s-1$, то $f_{k-1}(c)f_{k+1}(c) < 0$;
- 2) последний многочлен $f_s(x)$ не имеет корней на $[a, b]$;
- 3) $f_0(a)f_0(b) \neq 0$;
- 4) если $f(c) = 0$ для $c \in [a, b]$, то функция $f_0(x)f_1(x)$ меняет знак с – на +, если x , возрастая, проходит через точку c .

Теорема Штурма для интервала. Число действительных корней многочлена $f(x)$ степени $n \geq 1$ на интервале (a, b) равно $W(a) - W(b)$ (для любой фиксированной системы Штурма для многочлена $f(x)$ на отрезке $[a, b]$).

Доказательство аналогично приведённому доказательству теоремы Штурма. \square

Замечание 3.24.5 (теорема Декарта). Так как для $0 < c \in \mathbb{R}$ число перемен знаков в системе коэффициентов многочлена $f(x) \in \mathbb{R}[x]$ меньше числа перемен знаков в системе коэффициентов произведения $(x-c)f(x)$ на нечётное число, то из этого выводится теорема Декарта (более слабая оценка, чем в теореме Штурма): число положительных корней многочлена $f(x) \in \mathbb{R}[x]$, засчитываемых каждый столько раз, какова его кратность, равно числу перемен знаков в системе коэффициентов этого многочлена или меньше этого числа на чётное число (если все корни многочлена $f(x)$ действительны, то число положительных корней равно числу перемен знаков в системе коэффициентов многочлена $f(x)$).

Замечание 3.24.6 (теорема Бюдана—Фурье). Оценку для числа корней на интервале (a, b) (а не только на интервале $(0, +\infty)$, как в теореме Декарта) даёт следующая теорема Бюдана—Фурье (Бюдан, 1822 г.; Фурье, 1820 г.).

Пусть $f(x) \in \mathbb{R}[x]$, $\deg f(x) = n$, $c \in \mathbb{R}$, $f(c) \neq 0$, $S_+(c)$ — число перемен знаков в системе чисел

$$f(c), f'(c), \dots, f^{(n)}(c). \quad (3.2)$$

Если $f^{(k)}(c) = f^{(k+1)}(c) = \dots = f^{(k+l-1)}(c) = 0$, но $f^{(k-1)}(c) \neq 0$, $f^{(k+l)}(c) \neq 0$, то считаем, что $f^{(k+i)}(c)$, $0 \leq i \leq l-1$, имеет такой же знак, как $f^{(k+l)}(c)$, если разность $l-i$ чётная, и противоположный знак, если это число нечётно, а через $S_-(c)$ обозначим число перемен знаков в системе (3.2) с учётом знаков, приписанных этим способом числам $f^{(k)}(c), \dots, f^{(k+l-1)}(c)$.

Теорема 3.24.7 (Бюдан—Фурье). Пусть $f(x) \in \mathbb{R}[x]$, $a, b \in \mathbb{R}$, $a < b$, $f(a) \neq 0$, $f(b) \neq 0$. Тогда число корней многочлена $f(x)$ в интервале (a, b) , подсчитываемых каждый столько раз, какова его кратность, равно $S_+(a) - S_-(b)$ или меньше этого числа на чётное число.

Следствие 3.24.8. Пусть все корни многочлена $f(x) \in \mathbb{R}[x]$ вещественны, $a, b \in \mathbb{R}$, $f(a) \neq 0$, $f(b) \neq 0$. Тогда число корней многочлена $f(x)$, лежащих в интервале (a, b) , равно $W(f_a(x)) - W(f_b(x))$, где

$$f_a(x) = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} x^k = f(x+a),$$

$$f_b(x) = \sum_{k=0}^n \frac{f^{(k)}(b)}{k!} x^k = f(x+b),$$

$W(f_a(x))$ и $W(f_b(x))$ — число перемен знаков в системе коэффициентов многочленов $f_a(x)$ и $f_b(x)$ соответственно.

Упражнение 3.24.9. Число перемен знаков в системе коэффициентов многочлена $f(x) = x^3 - 3x + 1$ равно 2. Поэтому число положительных корней многочлена $f(x)$ равно либо 2, либо 0. Число перемен знаков в системе коэффициентов многочлена $f(-x) = -x^3 + 3x + 1$ равно 1, следовательно, число отрицательных корней многочлена $f(x)$ равно 1. Дополнительно, вычисляя дискриминант кубического многочлена $f(x)$, получаем, что все корни многочлена $f(x)$ действительны.

Упражнение 3.24.10. Для характеристического многочлена $f(x) = -x^3 + 14x + 20$ симметрической матрицы

$$\begin{pmatrix} -2 & 1 & 1 \\ 1 & 1 & 3 \\ 1 & 3 & 1 \end{pmatrix}$$

известно, что все корни действительны. Поэтому, применяя теорему Декарта, получаем, что число положительных корней многочлена $f(x)$ равно 1. Так как число перемен знаков в системе коэффициентов многочлена $f(-x) = x^3 - 14x + 20$ равно 2, то число отрицательных корней многочлена $f(x)$ равно 2.

Упражнение 3.24.11. Пусть

$$f(x) = 1 + x + \frac{x^2}{2!} + \dots + \frac{x^n}{n!}$$

(урезанная экспонента), $a, b \in \mathbb{R}$, $a < b < 0$. Положим $\varphi_0(x) = f(x)$, $\varphi_1(x) = f'(x)$, $\varphi_2(x) = -f(x) + f'(x) = -\frac{x^n}{n!}$.

Нетрудно видеть, что система $\varphi_0(x)$, $\varphi_1(x)$, $\varphi_2(x)$ является системой Штурма для многочлена $f(x)$ на отрезке $[a, b]$. Полагая, что число a достаточно большое по модулю, а число b достаточно мало, применяя теорему Штурма для отрезка, получаем, что при чётном n многочлен $f(x)$ не имеет вещественных корней, а при нечётном n имеет один отрицательный корень. При $n = 3$ каноническая система Штурма содержит четыре многочлена

$$f_0(x) = f(x) = 1 + x + \frac{x^2}{2} + \frac{x^3}{6},$$

$$f_1(x) = f'(x) = 1 + x + \frac{x^2}{2},$$

$$f_2(x) = -\left(\frac{1}{3}x + \frac{2}{3}\right),$$

$$f_3(x) = -1,$$

а построенная выше система Штурма для отрезка $[a, b]$ содержит три многочлена $\varphi_0(x)$, $\varphi_1(x)$, $\varphi_2(x)$.

Задача 3.24.12. Пусть $f \in \mathbb{Z}[x]$, $\deg f = n$, старший коэффициент многочлена f равен 1. Докажите, что невозможна ситуация, когда многочлен f имеет n корней (считая кратность) на интервале $(m, m+1)$, где $n \in \mathbb{Z}$.

Упражнение 3.24.13. Многочлены Лежандра (сферические функции) определяются рекуррентной формулой

$$(n+1)P_{n+1}(x) - (2n+1)xP_n(x) + nP_{n-1}(x) = 0,$$

где $P_0(x) = 1$, $P_1(x) = x$, или формулами

$$P_n(x) = \frac{1}{2^n n!} \frac{d^n((x^2 - 1)^n)}{dx^n}.$$

Нетрудно показать, что при всех n $P_n(x)$ — многочлен степени n , а также что $P_n(x)$ — интеграл дифференциального уравнения

$$(x^2 - 1)y'' + 2xy' - n(n+1)y = 0;$$

$$\frac{1}{\sqrt{1-2xz+z^2}} = \sum_{n=0}^{\infty} P_n(x)z^n.$$

Покажите, что система многочленов

$$P_m(x), P_{m-1}(x), \dots, P_1(x), P_0(x) -$$

система Штурма для многочлена $f(x) = P_m(x)$.

Упражнение 3.24.14. Покажите с использованием теоремы Бюдана—Фурье, что многочлен

$$f(x) = 3x^8 - 2x^5 + x^4 + 4x^2 - x - 1$$

имеет ровно один корень на интервале $(-2, 0)$.

Задача 3.24.15. Каждый действительный многочлен $f(x)$ можно представить в виде рациональной дроби, числитель и знаменатель которой — действительные многочлены, в знаменателе нет переменны знаков, а в числителе число перемен знаков равно числу положительных корней многочлена $f(x)$.

Указание. $f(x) = \frac{f(x)(1+x)^k}{(1+x)^k}$ для достаточного большого k .

Задача 3.24.16 (теорема Шура). Пусть f — многочлен степени n , имеющий лишь действительные корни, λ_n — наибольший корень многочлена f , λ_{n-k} — наибольший корень производной $f^{(k)}$, $k = 1, 2, \dots, n-1$. Тогда

$$\lambda_n - \lambda_{n-1} \leq \lambda_{n-1} - \lambda_{n-2} \leq \dots \leq \lambda_2 - \lambda_1.$$

Задача 3.24.17 (А. Г. Хованский). Пусть $f \in \mathbb{R}[x]$, $\deg f \geq 1$, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, $a_n \neq 0$,

$$j(f) = \begin{cases} 0, & \text{если } n \text{ — чётное число,} \\ 1, & \text{если } n \text{ нечётное и } a_n > 0, \\ -1, & \text{если } n \text{ нечётное и } a_n < 0. \end{cases}$$

Рациональная дробь $\frac{f'}{f}$ однозначно может быть представлена в виде непрерывной дроби

$$\frac{f'}{f} = \left[0; \frac{1}{f_1}, \frac{1}{f_2}, \dots, \frac{1}{f_k} \right].$$

Покажите, что число вещественных корней многочлена $f(x)$ (без учёта кратностей) равно

$$j(f_1) - j(f_2) + \dots + (-1)^{k-1} j(f_k).$$

Например, пусть $f(x) = -x^3 + 1$. Тогда

$$\begin{aligned} f'(x) &= -3x^2, \\ \frac{f'(x)}{f(x)} &= \frac{-3x^2}{-x^3 + 1} = \frac{1}{(\frac{x^3-1}{3x^2})} = \frac{1}{\frac{1}{3}x + \frac{1}{-3x^2}}, \end{aligned}$$

$$f_1(x) = \frac{1}{3}x, \quad f_2(x) = -3x^2.$$

$$j(f_1) = 1, \quad j(f_2) = 0, \quad j(f_1) - j(f_2) = 1,$$

и многочлен $f(x)$ имеет один действительный корень.

3.25. Приближённое вычисление корней многочленов с действительными коэффициентами

Метод деления отрезка (метод дихотомии, или метод вилки)

Пусть многочлен $f(x) \in \mathbb{R}[x]$ имеет единственныи корень на отрезке $[a, b]$ (пусть $f(x)$ имеет разные знаки в точках a и b ; этого можно достичь, отделяя кратные корни многочлена $f(x)$). Деля на части отрезок $[a, b]$ и определяя знак многочлена $f(x)$ в точках деления, мы можем сужать отрезок, содержащий корень, и осуществлять приближённое вычисление корня. Однако скорость сходимости этого метода мала (по сравнению с другими методами).

Метод непрерывных дробей

Пусть действительный многочлен $f(x) \in \mathbb{R}[x]$ степени n имеет простой (то есть кратности 1) корень c в интервале $(a, a+1)$. Тогда $c - a \in (0, 1)$. Положим $y = \frac{1}{x-a}$, то есть $x = \frac{1}{y} + a$. Многочлен $g(y) = y^n f\left(\frac{1}{y} + a\right)$ имеет корень $b = \frac{1}{c-a}$ в интервале $(1, +\infty)$. Пусть $a_1 < b < a_1 + 1$, $z = \frac{1}{y - a_1}$, $d = \frac{1}{b - a_1}$, $a_2 < d < a_2 + 1$, $w = \frac{1}{z - a_2}$, $e = \frac{1}{d - a_2}$, $a_3 < e < a_3 + 1$ и так далее. Тогда:

$$a + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}} < c < a + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}.$$

Продолжая этот процесс, получаем всё более точные приближения корня с непрерывными дробями.

Метод хорд и метод Ньютона

Пусть функция $f(x)$ и её производные $f'(x)$, $f''(x)$ непрерывны на отрезке $[a, b]$, $f(a)f(b) < 0$, производные $f'(x)$ и $f''(x)$ сохраняют знак на $[a, b]$. В частности, из этого следует, что существует такая точка c , $a < c < b$, что $f(c) = 0$; функция $f(x)$ возрастает (или убывает) на $[a, b]$, поэтому корень c единственен; график функции $f(x)$ выпуклый вниз (вверх) на $[a, b]$.

Эти предположения относительно функции $f(x)$ легко могут быть реализованы для многочленов: достаточно отделить кратные корни многочлена $f(x)$, затем локализовать корни многочлена $f(x)$. Так как $f'(x)$ и $f''(x)$ — многочлены, то, отделяя корни многочлена $f(x)$ и применяя теорему Штурма к многочленам $f(x)$ и $f'(x)$, мы рассматриваем такой отрезок $[a, b]$, что он содержит лишь один корень с многочленом $f(x)$ (кратности один), $f(a)f(b) < 0$ и многочлен $f'(x)$ не имеет корней на отрезке $[a, b]$. Если при этом $f''(c) = 0$, то задача о приближённом вычислении корня с многочленом $f(x)$ сводится к вычислению корня с многочленом $f''(x)$, имеющего меньшую степень, чем многочлен $f(x)$. Если же $f''(c) \neq 0$, то, вновь применяя теорему Штурма и сужая отрезок $[a, b]$, мы приходим к ситуации, когда $f(a)f(b) < 0$, многочлен $f(x)$ имеет лишь один корень внутри отрезка $[a, b]$, многочлены $f'(x)$ и $f''(x)$ сохраняют знак на $[a, b]$.

Метод хорд. За приближённое значение корня принимается число

$$x_1 = a - \frac{(b-a)f(a)}{f(b)-f(a)} = b - \frac{(b-a)f(b)}{f(b)-f(a)}.$$

Геометрически это означает, что вместо корня c , где точка $(c, 0)$ является точкой пересечения графика функции $f(x)$ с осью абсцисс, берётся пересечение с осью абсцисс хорды, соединяющей точки $(a, f(a))$ и $(b, f(b))$. Продолжая этот процесс, можно построить приближение корня с любой степенью точности.

Так, например, если $f' > 0$, $f'' > 0$ на $[a, b]$, $f(a) < 0$, $f(b) > 0$, то $f(x_1) < 0$, и последовательные приближения вычисляем по формуле

$$x_{n+1} = x_n - \frac{(b-x_n)f(x_n)}{f(b)-f(x_n)}.$$

При этом для любого n : $a < x_n < x_{n+1} < c$, где $f(c) = 0$, $\lim_{n \rightarrow \infty} x_n = c$, $|x_n - c| \leq \frac{|f(x_n)|}{m}$, где m — наименьшее значение функции $|f'(x)|$ на отрезке $[a, b]$.

Метод хорд часто называют методом пропорциональных частей, методом линейной интерполяции или методом ложного положения.

Более эффективным методом является метод Ньютона.

Метод Ньютона (метод касательных, или метод линеаризации). Для первого приближения к корню с положим

$$x_1 = b - \frac{f(b)}{f'(b)}$$

Геометрически x_1 — это абсцисса точки пересечения с осью x касательной к графику функции $f(x)$ в точке $(b, f(b))$. Если $f(b)$ одного знака с $f''(x)$ на $[a, b]$, то x_1 лежит между c и b ($f(c) = 0$). Если $f(a)$ одного знака с $f''(x)$, то полагаем

$$x'_1 = a - \frac{f(a)}{f'(a)}$$

(и тогда x'_1 — абсцисса точки пересечения с осью x касательной к графику функции $f(x)$ в точке $(a, f(a))$, x'_1 лежит между a и c).

Повторяя этот процесс, мы получаем последовательность убывающих чисел x_n , $b > x_n > x_{n+1} > c$ (или последовательность возрастающих чисел x'_n , $a < x'_n < x'_{n+1} < c$), где

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)},$$

$$x'_{n+1} = x'_n - \frac{f(x'_n)}{f'(x'_n)},$$

при этом $\lim_{n \rightarrow \infty} x_n = c$ ($\lim_{n \rightarrow \infty} x'_n = c$). Если, как и раньше, m — наименьшее значением функции $|f'(x)|$ на $[a, b]$, M — наибольшее значение функции $|f''(x)|$ на $[a, b]$, то

$$|x_{n+1} - c| \leq \frac{M}{2m} |x_n - c|^2$$

(аналогичная формула справедлива для x'_n). Этим обеспечивается достаточно близкое приближение x_n к c (x'_n к c).

При определённых условиях метод Ньютона можно использовать для приближённого вычисления комплексных корней комплексных многочленов.

Задача о глобальной сходимости метода Ньютона для рациональных энтоморфизмов Римановой сферы является открытой проблемой.

Упражнение 3.25.1. Покажите, что метод Ньютона для нахождения корней многочлена $x^2 - x - 1$ с начальным условием $x_0 = 1$ сходится к корню $\frac{1 + \sqrt{5}}{2}$, а с начальным условием $x_0 = 0$ — к корню $\frac{1 - \sqrt{5}}{2}$.

Иногда целесообразно применять **модифицированный метод Ньютона**, в котором последовательные приближения определяются формулами

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)},$$

то есть $(x_{n+1}, 0)$ — точка пересечения прямой, проходящей через точку $(x_n, f(x_n))$ и имеющей угловой коэффициент $f'(x_n)$, с осью x . Эта прямая лишь на первом шаге совпадает с касательной к графику функции $f(x)$. В случае применения модифицированного метода Ньютона вычислительная схема упрощается, однако скорость сходимости модифицированного метода Ньютона меньше, чем обычного метода Ньютона.

Часто при практических вычислениях удобно одновременно использовать метод Ньютона и метод хорд.

Метод секущих использует итерационный процесс

$$x_{n+1} = x_n - \frac{f(x_n)(x_{n-1} - x_n)}{f(x_{n-1}) - f(x_n)},$$

при этом приближения x_0 и x_1 задаются заранее. Приближение x_0 можно выбирать, как и в методе Ньютона, а приближение x_1 брать вблизи точки x_0 , между x_0 и предполагаемым корнем. Достоинством метода секущих является очень простая вычислительная схема, однако в плане численной устойчивости он проигрывает методу Ньютона.

Пример 3.25.2. Многочлен $f(x) = x^3 - 2x^2 - 4x - 7$ имеет единственный корень внутри отрезка $[3, 4]$, на этом отрезке его производные $f'(x)$ и $f''(x)$ сохраняют знак, наименьшее значение $f'(x)$ на этом отрезке $m = 11$. Для первого приближения по методу хорд полагаем

$$x_1 = 3 - \frac{f(3)}{f(4) - f(3)} = 3 + \frac{10}{19}.$$

Для вычисления корня с точностью до 0,01, используя оценку

$$|x_n - c| \leq \frac{|f(x_n)|}{m},$$

где $f(c) = 0$, необходимо совершить три шага метода:

$$x_3 \approx 3,63.$$

При использовании метода Ньютона полагаем

$$x_1 = 4 - \frac{f(4)}{f'(4)} = 4 - \frac{9}{28}.$$

Уже $x_2 \approx 3,63$ даёт приближение корня с точностью до 0,01.

Метод итерации

Пусть $f(x) \in \mathbb{C}[x]$. Преобразуем уравнение $f(x) = 0$ к виду $x = \varphi(x)$ (либо перенося a_1x в правую часть и деля на $-a_1$ при $a_1 \neq 0$; либо полагая $x = x + df(x)$, $d \neq 0$).

Пусть x_0 — начальное приближение к корню уравнения. Определим последовательность x_n , полагая $x_{n+1} = \varphi(x_n)$, $n = 0, 1, 2, \dots$. Можно показать, что если для любых x', x'' из круга $\{x \in \mathbb{C} \mid |x - x_0| \leq \delta\}$ функция $\varphi(x)$ удовлетворяет неравенству

$$|\varphi(x') - \varphi(x'')| \leq q|x' - x''|,$$

где $0 < q < 1$, и выполнено неравенство

$$\frac{m}{1-q} \leq \delta,$$

где $m = |x_0 - \varphi(x_0)|$, то уравнение $x = \varphi(x)$ имеет в круге $\{x \in \mathbb{C} \mid |x - x_0| \leq \delta\}$ единственный корень c , к которому сходится последовательность $\{x_n\}$, при этом скорость сходимости определяется неравенством

$$|x_n - c| \leq \frac{m}{1-q} q^n.$$

Замечание 3.25.3. Существуют и другие методы приближённого вычисления корней многочленов. Например, метод Лобачевского (1834), иногда называемый методом Лобачевского—Греффе—Данделена, имеющий довольно сложную вычислительную схему, не требует знания начального приближения к корню многочлена и применим к нахождению начального приближения. Метод Лобачевского позволяет одновременно приближённо вычислять все корни многочлена.

3.26. Проблема Рауса—Гурвица, устойчивые многочлены

Многочлен $f(z) \in \mathbb{C}[z]$ называется *устойчивым*, если все его комплексные корни лежат в левой полуплоскости (т. е. вещественные части a всех корней $c = a + bi$ многочлена $f(z)$ отрицательны, $a < 0$). Этот класс многочленов возник в теории устойчивости движения (в частности, для применения теоремы А. А. Ляпунова). Ясно, что делитель устойчивого многочлена устойчив, произведение устойчивых многочленов также является устойчивым.

Замечание 3.26.1. Пусть дана линейная однородная система дифференциальных уравнений

$$\frac{d\hat{X}}{dt} = A \cdot \hat{X}$$

с постоянной матрицей $A \in M_n(\mathbb{R})$,

$$\hat{X} = \begin{pmatrix} x_1(t) \\ \vdots \\ x_n(t) \end{pmatrix}$$

Решение этой системы даётся формулой

$$X_{\hat{C}}(t) = e^A \cdot \hat{C} \quad (t \geq 0),$$

см. ?? (начальное условие $\hat{X}(0) = \hat{C} \in \hat{\mathbb{R}}_n$).

Система $\frac{d\hat{X}}{dt} = A \cdot \hat{X}$ асимптотически устойчива, если все решения $\hat{X} = \hat{X}(t)$ обладают свойством $\lim_{t \rightarrow \infty} \hat{X}(t) = (0)$.

Критерий А. М. Ляпунова асимптотической устойчивости системы: система $\frac{d\hat{X}}{dt} = A \cdot \hat{X}$ асимптотически устойчива тогда и только тогда, когда все собственные числа матрицы A имеют отрицательные вещественные части (иными словами, когда характеристический многочлен матрицы A устойчив).

Теорема А. М. Ляпунова (1892). Пусть $A \in M_n(\mathbb{R})$. Тогда все собственные числа матрицы A имеют отрицательные действительные части в том и только в том случае, когда существует (и единственна) такая положительно определённая симметрическая матрица $B \in M_n(\mathbb{R})$ ($B^t = B$, $X \cdot V \cdot X^t > 0$ для любой строки $X \in \mathbb{R}^n$), что

$$A^t \cdot B + B \cdot A = -E.$$

Эта теорема позволяет свести задачу об определении устойчивости системы к решению системы линейных уравнений.

Проблема Раяса—Гурвица заключается в следующем: по коэффициентам a_0, a_1, \dots, a_n многочлена $f(z) = \sum_{i=0}^n a_i z^i \in \mathbb{C}[z]$ определить, устойчив ли он.

Большая часть известных критериев устойчивости относится к многочленам с действительными коэффициентами. Это объясняется возможностью редукции общей проблемы к случаю действительных коэффициентов.

Лемма 3.26.2 (о редукции проблемы устойчивости для многочленов с комплексными коэффициентами к случаю многочленов с вещественными коэффициентами). Пусть

$$\begin{aligned} f(z) &= a_n z^n + \dots + a_1 z + a_0 \in \mathbb{C}[z], \\ \bar{f}(z) &= \bar{a}_n z^n + \dots + \bar{a}_1 z + \bar{a}_0 \in \mathbb{C}[z], \\ g(z) &= f(z)\bar{f}(z). \end{aligned}$$

Тогда:

- 1) многочлен $f(z)$ устойчив тогда и только тогда, когда устойчив многочлен $g(z) = f(z)\bar{f}(z)$;
- 2) $g(z) = f(z)\bar{f}(z) \in \mathbb{R}[z]$, т. е. $g(z)$ — многочлен с действительными коэффициентами.

Доказательство. Так как отображение $c = a + bi \mapsto \bar{c} = a - bi$ является автоморфизмом поля комплексных чисел \mathbb{C} , то отображение $f \mapsto \bar{f}$ является автоморфизмом кольца многочленов $\mathbb{C}[z]$.

Если

$$f(z) = a_n z^n + \dots + a_0 = a_n(z - c_1) \dots (z - c_n),$$

где $c_1, \dots, c_n \in \mathbb{C}$ — корни многочлена $f(z)$, то

$$\bar{f}(z) = \bar{a}_n z^n + \dots + \bar{a}_0 = \bar{a}_n(z - \bar{c}_1) \dots (z - \bar{c}_n),$$

где корень $c = a + bi$ многочлена $f(z)$ соответствует корню $\bar{c} = a - bi$ многочлена $\bar{f}(z)$, при этом вещественная часть a у них одна и та же. Таким образом, многочлен $f(z)$ устойчив тогда и только тогда, когда устойчив многочлен $g(z) = f(z)\bar{f}(z)$.

Так как

$$g(z) = f(z)\bar{f}(z) = a_n \bar{a}_n \prod_{i=1}^n (z - c_i)(z - \bar{c}_i), \quad a_n \bar{a}_n \in \mathbb{R},$$

$$(z - c)(z - \bar{c}) = (z - (a + bi))(z - (a - bi)) = z^2 - 2a + (a^2 + b^2) \in \mathbb{R}[z],$$

то $g(z) \in \mathbb{R}[z]$, т. е. $g(z)$ — многочлен с действительными коэффициентами. \square

Лемма 3.26.3. Если многочлен

$$f(z) = a_n z^n + \dots + a_1 z + a_0 = a_n(z - c_1) \dots (z - c_n) \in \mathbb{C}[z]$$

с комплексными коэффициентами ($a_n \neq 0$, c_1, \dots, c_n — его корни, $c_j = a_j + b_j i$) является устойчивым (т. е. $a_j < 0$, $j = 1, \dots, n$), то:

1) $a_0 \neq 0$;

2) $\operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$.

Доказательство. 1) Так как $f(0) = a_0$, то $a_0 = 0$ тогда и только тогда, когда 0 является корнем многочлена $f(z)$. Так как многочлен $f(z)$ устойчивый, то $a_0 \neq 0$.

2) Так как $c_j \neq 0$, $j = 1, \dots, n$, и

$$\frac{1}{c_j} = \frac{a_j}{a_j^2 + b_j^2} - \frac{b_j}{a_j^2 + b_j^2} i,$$

то

$$\operatorname{Re}\left(\frac{1}{c_j}\right) = \frac{a_j}{a_j^2 + b_j^2} < 0.$$

Поэтому

$$\operatorname{Re}\left(\sum_{j=1}^n \frac{1}{c_j}\right) < 0.$$

В силу следствия к теореме Виета:

$$-\frac{a_1}{a_0} = \sum_{j=1}^n \frac{1}{c_j},$$

следовательно,

$$\operatorname{Re}\left(-\frac{a_1}{a_0}\right) = \operatorname{Re}\left(\sum_{j=1}^n \frac{1}{c_j}\right) < 0. \quad \square$$

Лемма 3.26.4 (свойство левой полуплоскости в \mathbb{C}). Если $z = a + bi, w = u + vi \in \mathbb{C}$, $a = \operatorname{Re}(z) < 0$, $u = \operatorname{Re}(w) < 0$, то

$$|z + \bar{w}| > |z - w|.$$

Доказательство.

$$\begin{aligned}|z + \bar{w}|^2 - |z - w|^2 &= |(\bar{a} + u) + (b - v)i|^2 - |(\bar{a} - u) + (b - v)i|^2 = \\&= (\bar{a} + u)^2 + (b - v)^2 - (\bar{a} - u)^2 - (b - v)^2 = 4au > 0,\end{aligned}$$

следовательно,

$$|z + \bar{w}| > |z - w|. \quad \square$$

Замечание 3.26.5. Если

$$f(z) = a_n z^n + \dots + a_1 z + a_0 \in \mathbb{C}[z],$$

то определим

$$\tilde{f}(z) = z^n f\left(\frac{1}{z}\right) = a_0 z^n + \dots + a_{n-1} z + a_n$$

(«обращённый» многочлен). Так как знаки $\operatorname{Re}(c)$ и $\operatorname{Re}\left(\frac{1}{c}\right)$ для $0 \neq c \in \mathbb{C}$ совпадают, то многочлен $f(z)$ устойчив тогда и только тогда, когда устойчив многочлен $\tilde{f}(z)$.

Теорема 3.26.6 (теорема А. Стодолы, 1894 г.). Если многочлен

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{R}[x]$$

с действительными коэффициентами степени n , $a_n > 0$, является устойчивым, то все его коэффициенты $a_n, a_{n-1}, \dots, a_1, a_0$ положительны.

Доказательство. Пусть

$$f(x) = a_n x^n + \dots + a_1 x + a_0 = a_n (x - c_1) \dots (x - c_n),$$

где $c_j = a_j + b_j i \in \mathbb{C}$, $j = 1, \dots, n$, — корни многочлена $f(x)$. Так как многочлен $f(x)$ устойчивый, то $a_j < 0$ для всех $j = 1, \dots, n$.

Отрицательному действительному корню $c \in \mathbb{R}$, $c < 0$, соответствует множитель $x - c$ с положительными коэффициентами.

Паре ненулевых сопряжённых корней $a + bi$, $a - bi$, где $a < 0$, в каноническом разложении соответствует множитель

$$(x - (a + bi))(x - (a - bi)) = x^2 - 2ax + a^2 + b^2$$

с положительными коэффициентами.

Так как $a_n > 0$ и произведение многочленов с положительными коэффициентами является многочленом с положительными коэффициентами, то $a_n > 0$, $a_{n-1} > 0, \dots, a_1 > 0$, $a_0 > 0$. \square

Замечание 3.26.7. Многочлен $f(x) \in \mathbb{R}[x]$ степени 1 или 2 с вещественными коэффициентами и с положительным старшим членом устойчив тогда и только тогда, когда все его коэффициенты положительны.

Действительно, для многочлена первой степени $a_1 x + a_0$, $a_1 > 0$, его единственный корень $-\frac{a_0}{a_1}$ отрицателен тогда и только тогда, когда $a > 0$.

Многочлен второй степени $a_2x^2 + a_1x + a_0$, $a_2 > 0$, имеет корни

$$\frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_2}.$$

Если дискриминант $D = a_1^2 - 4a_0a_2 < 0$, то $a_0 > 0$ и вещественная часть обоих корней равна $\frac{a_1}{2a_2}$, т. е. устойчивость многочлена в этом случае равносильна тому, что $a_1 > 0$.

Если же $D = a_1^2 - 4a_0a_2 > 0$, то оба корня вещественны. Если $a_1 > 0$ и $a_0 > 0$, то оба корня отрицательны.

Пример 3.26.8 (показывающий, что при степени ≥ 3 положительность коэффициентов недостаточна для его устойчивости). Многочлен

$$x^3 + x^2 + 4x + 30 \in \mathbb{R}[x]$$

имеет все положительные коэффициенты, но не является устойчивым (его корни -3 , $1 \pm 3i$; среди них два корня имеют положительную вещественную часть).

Упражнение 3.26.9 (критерий Вышнеградского устойчивости многочлена третьей степени). Многочлен с вещественными коэффициентами

$$f = a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{R}[x],$$

$a_3 > 0$, устойчив тогда и только тогда, когда все его коэффициенты положительны (т. е. $a_3 > 0$, $a_2 > 0$, $a_1 > 0$, $a_0 > 0$) и имеет место неравенство $a_1a_2 > a_0a_3$.

Упражнение 3.26.10. Многочлен

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{R}[x]$$

устойчив тогда и только тогда, когда

$$a_3 > 0, \quad a_0 > 0, \quad a_3a_2 > a_1, \quad a_1(a_3a_2 - a_1) > a_3^2a_0.$$

Следующая теорема даёт прозрачный критерий устойчивости многочленов с действительными коэффициентами (продолжая линию: что надо добавить к условию положительности всех коэффициентов).

Теорема 3.26.11. Пусть

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{R}[x] —$$

многочлен с действительными коэффициентами,

$$g(x) = x^m + b_{m-1}x^{m-1} + \dots + b_1x + b_0 —$$

многочлен степени $m = \frac{n(n-1)}{2}$, корнями которого служат все суммы пар корней многочлена $f(x)$. Тогда:

- 1) $g(x) \in \mathbb{R}[x]$;

2) многочлен $f(x)$ устойчив тогда и только тогда, когда все коэффициенты многочленов $f(x)$ и $g(x)$ положительны.

Доказательство. 1) Многочлен $g(x)$ имеет действительные коэффициенты, поскольку его комплексные, не являющиеся действительными, корни разбиваются на пары сопряжённых корней. Действительно, если $r \in \mathbb{R}$, $c, d \in \mathbb{C} \setminus \mathbb{R}$, $f(r) = f(c) = f(d) = 0$, то $f(\bar{c}) = f(\bar{d}) = 0$, при этом $\frac{3(3-1)}{2} = 3$ суммы пар из $\{r, c, \bar{c}\}$, $c \neq \bar{c}$, имеют вид $c + \bar{c} \in \mathbb{R}$, $r + c, r + \bar{c} \in \mathbb{C} \setminus \mathbb{R}$, где $\overline{r+c} = r + \bar{c}$; $\frac{4(4-1)}{2} = 6$ сумм пар из $\{c, \bar{c}, d, \bar{d}\}$, $c \neq \bar{c}$, $d \neq \bar{d}$, имеют вид $c + \bar{c}, d + \bar{d} \in \mathbb{R}$, $c + d, \bar{c} + \bar{d} = \overline{c + d}, c + \bar{d}, \bar{c} + d = \overline{c + \bar{d}}$ (в случае кратных корней $c = d$: $c + \bar{d} = c + \bar{c}, \bar{c} + d = \bar{c} + c \in \mathbb{R}$).

2а) Если многочлен $f(x)$ устойчив, то по определению вещественные части всех его корней отрицательны, следовательно, вещественные части всех сумм пар его корней также отрицательны, т. е. многочлен $g(x)$ также устойчив.

Применяя к устойчивым многочленам $f(x), g(x) \in \mathbb{R}[x]$ теорему Стодолы, убеждаемся в том, что все коэффициенты многочленов $f(x)$ и $g(x)$ положительны.

2б) Допустим, что все коэффициенты многочленов $f(x)$ и $g(x) \in \mathbb{R}[x]$ положительны. Тогда все действительные корни многочленов $f(x), g(x) \in \mathbb{R}[x]$ отрицательны.

Таким образом, если $c \in \mathbb{R}$ и $f(c) = 0$, то $c < 0$, если $c = a + bi, \bar{c} = a - bi \in \mathbb{C} \setminus \mathbb{R}$, $f(c) = f(\bar{c}) = 0$, — пара сопряжённых корней многочлена $f(x)$, то действительное число $2a = (a + bi) + (a - bi) \in \mathbb{R}$ является действительным корнем многочлена $g(x)$, и поэтому $2a < 0$, следовательно, $a < 0$.

Итак, мы показали, что действительные части всех корней многочлена $f(x)$ отрицательны, т. е. что $f(x)$ — устойчивый многочлен. \square

3.27. Преобразования И. Шура

Пусть

$$\begin{aligned} f(z) &= a_n z^n + \dots + a_1 z + a_0 \in \mathbb{C}[z], \quad a_n \neq 0; \\ \bar{f}(z) &= \bar{a}_n z^n + \dots + \bar{a}_1 z + \bar{a}_0 \end{aligned}$$

(замена всех коэффициентов a_k на их сопряжённые \bar{a}_k);

$$f^*(z) = \bar{f}(-z);$$

т. е.

$$f^*(z) = (-1)^n \bar{a}_n z^n + (-1)^{n-1} \bar{a}_{n-1} z^{n-1} + \dots + \bar{a}_0$$

(перемена знаков в многочлене $\bar{f}(z)$ при нечётных степенях переменной z).

Лемма 3.27.1. Если $f, f_1, f_2 \in \mathbb{C}[z]$, то

$$(f_1 + f_2)^* = f_1^* + f_2^*;$$

$$(f_1 f_2)^* = f_1^* f_2^*;$$

$$(cf)^* = \bar{c} f^* \text{ для } c \in \mathbb{C};$$

$$f^{**} = f$$

(в частности, отображение $f(z) \mapsto f^*(z)$ является автоморфизмом кольца $\mathbb{C}[z]$).

Доказательство. Так как отображение $c \mapsto \bar{c}$ является автоморфизмом поля комплексных чисел \mathbb{C} , то (как мы видели) отображение $f \mapsto \bar{f}$ является автоморфизмом кольца многочленов $\mathbb{C}[z]$, при этом $(\bar{cf})(z) = \bar{c}\bar{f}(z)$ для $c \in \mathbb{C}$. Далее:

$$\begin{aligned} (f_1 + f_2)^*(z) &= \overline{(f_1 + f_2)}(-z) = (\bar{f}_1 + \bar{f}_2)(-z) = \bar{f}_1(-z) + \bar{f}_2(-z) = f_1^*(z) + f_2^*(z); \\ (f_1 f_2)^*(z) &= \overline{(f_1 f_2)}(-z) = (\bar{f}_1 \bar{f}_2)(-z) = \bar{f}_1(-z) \bar{f}_2(-z) = f_1^*(z) f_2^*(z); \\ (cf)^* &= (\bar{c}\bar{f})(-z) = \bar{c}(\bar{f}(-z)) = \bar{c}f^*(z); \\ f^{**}(z) &= (\bar{f}(-z))^* = f(z). \end{aligned}$$

□

Следствие 3.27.2. Если $c \in \mathbb{C}$, то $f(c) = 0$ тогда и только тогда, когда $f^*(-\bar{c}) = 0$, при этом кратности корней c и $-\bar{c}$ одинаковы.

Доказательство. Пусть $c_1, \dots, c_n \in \mathbb{C}$ — корни многочлена $f(z)$, т. е.

$$f(z) = a_n(z - c_1) \dots (z - c_n).$$

Тогда (в силу леммы 3.27.1)

$$f^*(z) = \bar{a}_n(-z - \bar{c}_1) \dots (-z - \bar{c}_n) = (-1)^n \bar{a}_n(z - (-\bar{c}_1)) \dots (z - (-\bar{c}_n)),$$

т. е. $-\bar{c}_1, \dots, -\bar{c}_n$ — корни многочлена $f^*(z)$.

□

Лемма 3.27.3. Если $f(z) \in \mathbb{C}[z]$ — устойчивый многочлен, то для $c = a + bi \in \mathbb{C}$:

- 1) $0 \leq |f(c)| < |f^*(c)|$, если $\operatorname{Re}(c) = a < 0$;
- 2) $0 \leq |f^*(c)| < |f(c)|$, если $\operatorname{Re}(c) = a > 0$;
- 3) $0 < |f(c)| = |f^*(c)|$, если $\operatorname{Re}(c) = a = 0$.

Доказательство. Пусть $c_1 = a_1 + b_1 i, \dots, c_n = a_n + b_n i$ — все корни устойчивого многочлена $f(z)$, тогда $a_j < 0$ для всех $j = 1, \dots, n$. Для $c \in \mathbb{C}$

$$\begin{aligned} |c + \bar{c}_j|^2 - |c - c_j|^2 &= \\ &= |(a + a_j) + (b - b_j)i|^2 - |(a - a_j) + (b - b_j)i|^2 = \\ &= (a + a_j)^2 + (b - b_j)^2 - (a - a_j)^2 - (b - b_j)^2 = 4aa_j. \end{aligned}$$

Таким образом,

$$|c - c_j| < |c + \bar{c}_j|, \text{ если } a < 0;$$

$$|c + \bar{c}_j| < |c - c_j|, \text{ если } a > 0;$$

$$|c - c_j| < |c + \bar{c}_j|, \text{ если } a = 0.$$

Так как

$$f(c) = a_n(c - c_1) \dots (c - c_n),$$

$$f^*(c) = (-1)^n \bar{a}_n(c - (-\bar{c}_1)) \dots (c - (-\bar{c}_n)),$$

то из полученных неравенств следуют утверждения 1)–3) леммы.

□

Определение 3.27.4. Если $\alpha, \beta \in \mathbb{C}$, $|\alpha| > |\beta|$, то многочлен $g(z) = \alpha f(z) - \beta f^*(z)$ называется преобразованием Шура многочлена $f(z)$.

Замечание 3.27.5. Если многочлен $g(z)$ является преобразованием Шура многочлена $f(z)$, то многочлен $f(z)$ также будет преобразованием Шура многочлена $g(z)$.

Действительно, так как $g = \alpha f - \beta f^*$, то по лемме 3.27.1 $g^* = \bar{\alpha}f^* - \bar{\beta}f$. Поэтому если

$$\alpha_1 = \frac{\bar{\alpha}}{|\alpha|^2 - |\beta|^2}, \quad \beta_1 = \frac{-\bar{\beta}}{|\alpha|^2 - |\beta|^2},$$

то

$$\begin{aligned}\alpha\alpha_1 + \bar{\beta}\beta_1 &= \frac{\alpha\bar{\alpha} - \beta\bar{\beta}}{|\alpha|^2 - |\beta|^2} = \frac{|\alpha|^2 - |\beta|^2}{|\alpha|^2 - |\beta|^2} = 1; \\ \alpha_1\beta + \bar{\alpha}\beta_1 &= \frac{\bar{\alpha}\beta - \bar{\beta}\alpha}{|\alpha|^2 - |\beta|^2} = 0.\end{aligned}$$

Следовательно,

$$\alpha_1 g - \beta_1 g^* = \alpha_1(\alpha f - \beta f^*) - \beta_1(\bar{\alpha}f^* - \bar{\beta}f) = (\alpha\alpha_1 + \bar{\beta}\beta_1)f - (\alpha_1\beta + \bar{\alpha}\beta_1)f^* = f.$$

Ясно, что

$$|\alpha_1| = \frac{|\alpha|}{|\alpha|^2 - |\beta|^2} > \frac{|\beta|}{|\alpha|^2 - |\beta|^2} = |\beta_1|. \quad \square$$

Предложение 3.27.6. Многочлен $f(z) \in \mathbb{C}[z]$ устойчив тогда и только тогда, когда устойчивым является любое (некоторое) его преобразование Шура $g(z) = \alpha f(z) - \beta f^*(z)$, где $\alpha, \beta \in \mathbb{C}$, $|\alpha| > |\beta|$.

Доказательство. 1) Пусть многочлен $f(z)$ устойчив. Если $c = a+bi \in \mathbb{C}$, $\operatorname{Re}(c) = a \geq 0$, то в силу леммы 3.27.3 (п. 2) и 3))

$$|f(c)| > |f^*(c)| \text{ или } |f(c)| = |f^*(c)| > 0.$$

Так как $|\alpha| > |\beta|$, то

$$|\alpha f(c)| = |\alpha| |f(c)| > |\beta| |f^*(c)| = |\beta| |f^*(c)|.$$

Таким образом, если $g(c) = 0$, т. е. $g(c) = \alpha f(c) - \beta f^*(c) = 0$, следовательно $\alpha f(c) = \beta f^*(c)$, и поэтому $a < 0$. Итак, мы показали, что многочлен $f(z)$ устойчивый.

2) Если многочлен $g(z)$ устойчивый, то в силу замечания 3.27.5 многочлен $f(z)$ является преобразованием Шура многочлена $g(z)$, поэтому в силу 1) $f(z)$ — устойчивый многочлен. \square

Теорема 3.27.7 (редукция проблемы к многочлену меньшей степени). Пусть $c = a+bi \in \mathbb{C}$, $\operatorname{Re}(c) = a < 0$, $f(z) \in \mathbb{C}[z]$, $\deg f(z) = n$. Многочлен $f(z)$ устойчив тогда и только тогда, когда

1) $|f(c)| < |f^*(c)|$;

2) многочлен

$$F(z, c) = \frac{f^*(c)f(z) - f(c)f^*(z)}{z - c} \in \mathbb{C}[z]$$

степени $n - 1$ является устойчивым.

Доказательство. а) Пусть многочлен $f(z)$ устойчив. Так как $\operatorname{Re}(c) = a < 0$, то в силу п. 1 леммы 3.27.3

$$|f(c)| < |f^*(c)|.$$

Поэтому многочлен

$$g(z) = f^*(c)f(z) - f(c)f^*(z)$$

является преобразованием Шура устойчивого многочлена $f(z)$; по предложению 3.27.6 $g(z)$ — устойчивый многочлен.

Многочлен $g(z)$ имеет степень n (ясно, что $\deg g(z) \leq n$; его коэффициент при z^n равен $f^*(c)a_n - f(c)(-1)^n\bar{a}_n$; так как $|a_n| > 0$ и $|f(c)| < |f^*(c)|$, то

$$|f^*(c)a_n| = |f^*(c)||a_n| < |f(c)||a_n| = |f(c)||\bar{a}_n| = |f(c)(-1)^n\bar{a}_n|,$$

и поэтому коэффициент при z^n многочлена $g(z)$ ненулевой).

Так как

$$g(c) = f^*(c)f(c) - f(c)f^*(c) = 0,$$

то c — корень многочлена $g(z)$, и поэтому многочлен $g(z)$ делится на $z - c$, $g(z) = (z - c)F(z, c)$,

$$F(z, c) = \frac{g(z)}{z - c} \in \mathbb{C}[z]$$

является многочленом степени $n - 1$. Так как $g(z)$ — устойчивый многочлен, то его делитель $F(z, c)$ также является устойчивым многочленом.

б) Пусть выполнены условия 1) и 2).

Так как

$$g(z) = f^*(c)f(z) - f(c)f^*(z) = (z - c)F(z, c)$$

и многочлен $F(z, c)$ устойчив (условие 2)), то устойчив и многочлен $g(z)$.

Так как $|f(c)| < |f^*(c)|$ (условие 1)), то многочлен

$$g(z) = f^*(c)f(z) - f(c)f^*(z)$$

является преобразованием Шура многочлена $f(z)$, при этом $g(z)$ — устойчивый многочлен. Согласно предложению 3.27.6 многочлен $f(z)$ также устойчив. \square

Рассмотрим многочлен от двух переменных (z и c):

$$F_f(z, c) = F(z, c) = \frac{f^*(c)f(z) - f(c)f^*(z)}{z - c} \in \mathbb{C}[z, c].$$

Так как $F(z, c) = F(c, z)$, то многочлен $F(z, c)$ симметричен, и поэтому степень многочлена $F(z, c)$ по c равна его степеней по z , т. е. равна $n - 1$, где $n = \deg f(z)$.

Разлагая многочлен $F(z, c)$ по степеням c^k переменной c , получаем

$$F(z, c) = F_{n-1}(z)c^{n-1} + \dots + F_1(z)c + F_0(z),$$

где $F_k(z) \in \mathbb{C}[z]$, $\deg F_k(z) \leq n - 1$, $0 \leq k \leq n - 1$.

Многочлен

$$T_f(z, c) = T(z, c) = F_1(z)c + F_0(z)$$

назовём *c-хвостом* многочлена $F_f(z, c)$.

Лемма 3.27.8. Если $T(z, c) = F_1(z)c + F_0(z)$ — c -хвост многочлена $F(z, c) \in \mathbb{C}[z, c]$,

$$\varphi(z, c) = \bar{a}_0(z + c) - \bar{a}_1zc \in \mathbb{C}[z, c],$$

$$\psi(z, c) = a_0(z + c) + a_1zc \in \mathbb{C}[z, c],$$

то

$$z^2T(z, c) = f(z)\varphi(z, c) - f^*(z)\psi(z, c).$$

Доказательство. Так как

$$(z - c)F(z, c) = f^*(c)f(z) - f(c)f^*(z),$$

то

$$(z - c) \sum_{k=0}^{n-1} F_k(z)c^k = f^*(c)f(z) - f(c)f^*(z),$$

поэтому

$$-F_{n-1}(z)c^n + \sum_{k=1}^{n-1} [zF_k(z) - F_{k-1}(z)]c^k + zF_0(z) = \left(\sum_{k=0}^n (-1)^k \bar{a}_k c^k \right) f(z) - \left(\sum_{k=0}^n a_k c^k \right) f^*(z).$$

Приравнивая соответственно коэффициенты при нулевой (свободный член) и первой степенях по c , получаем

$$\begin{aligned} zF_0(z) &= \bar{a}_0 f(z) - a_0 f^*(z); \\ zF_1(z) - F_0(z) &= -\bar{a}_1 f(z) - a_1 f^*(z). \end{aligned} \tag{*}$$

Отсюда

$$\begin{aligned} z^2T(z, c) &= z^2(F_1(z)c + F_0(z)) = \\ &= zc[zF_1(z) - F_0(z)] + (z + c)zF_0(z) = \\ &= zc[-\bar{a}_1 f(z) - a_1 f^*(z)] + (z + c)[\bar{a}_0 f(z) - a_0 f^*(z)] = \\ &= f(z)[\bar{a}_0(z + c) - \bar{a}_1zc] - f^*(z)[a_0(z + c) + a_1zc], \end{aligned}$$

то есть

$$z^2T(z, c) = f(z)\varphi(z, c) - f^*(z)\psi(z, c)$$

(утверждение леммы). □

Следствие 3.27.9.

$$z^2[T(z, c)\varphi^*(z, c) + T^*(z, c)\psi(z, c)] = f(z)[\varphi(z, c)\varphi^*(z, c) - \psi(z, c)\psi^*(z, c)].$$

Доказательство. При фиксированном $c \in \mathbb{C}$ применим к установленному в лемме 3.27.8 равенству автоморфизм $f \mapsto f^*$ кольца $\mathbb{C}[z]$ (см. лемму 3.27.1):

$$z^2T^*(z, c) = [z^2T(z, c)]^* = [f(z)\varphi(z, c) - f^*(z)\psi(z, c)] = f^*(z)\varphi^*(z, c) - f(z)\psi^*(z, c).$$

Следовательно,

$$\begin{aligned} z^2[T(z, c)\varphi^*(z, c) + T^*(z, c)\psi(z, c)] &= [f(z)\varphi(z, c) - f^*(z)\psi(z, c)]\varphi^*(z, c) + \\ &+ [f^*(z)\varphi^*(z, c) - f(z)\psi^*(z, c)]\psi(z, c) = f(z)[\varphi(z, c)\varphi^*(z, c) - \psi(z, c)\psi^*(z, c)]. \end{aligned} \tag{□}$$

Теорема 3.27.10 (критерий устойчивости Шура). Пусть

$$f(z) = a_n z^n + \dots + a_1 z + a_0 \in \mathbb{C}[z] -$$

многочлен с комплексными коэффициентами степени n , $a_n \neq 0$. Тогда:

- 1) если многочлен $f(z)$ устойчив, то $a_0 \neq 0$, $\operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$ и для всех $c \in \mathbb{C}$ таких, что $\operatorname{Re}(c) < 0$, c -хвост $T(z, c) = F_1(z)c + F_0(z)$ многочлена

$$F(z, c) = \frac{f^*(c)f(z) - f(c)f^*(z)}{z - c}$$

устойчив (как многочлен степени $n-1$ из $\mathbb{C}[z]$);

- 2) если $a_0 \neq 0$, $\operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$ и многочлен $T(z, c) \in \mathbb{C}[z]$ устойчив хотя бы для одного $c \in \mathbb{C}$ такого, что $\operatorname{Re}(c) < 0$, то многочлен $f(z) \in \mathbb{C}[z]$ также устойчив.

Доказательство. 1а) Если $f(z)$ — устойчивый многочлен, то в силу леммы 3.26.3 $a_0 \neq 0$; $\operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$.

Для доказательства устойчивости многочлена $T(z, c)$ (как многочлена из $\mathbb{C}[z]$) для всех $0 \neq c \in \mathbb{C}$ таких, что $\operatorname{Re}(c) < 0$, надо показать, что $T(d, c) \neq 0$ для любого $d \in \mathbb{C}$ такого, что $\operatorname{Re}(d) \geqslant 0$.

Случай а). Пусть $F_0(d) \neq 0$. Рассмотрим многочлен

$$\begin{aligned} \Phi(t) &= t^{n-1}F\left(d, \frac{1}{t}\right) = \\ &= t^{n-1}\left(F_{n-1}(d)\frac{1}{t^{n-1}} + \dots + F_0(d)\right) = \\ &= F_{n-1}(d) + F_{n-2}(d)t + \dots + F_1(d)t^{n-2} + F_0(d)t^{n-1} \in \mathbb{C}[t] \end{aligned}$$

(так как $F_0(d) \neq 0$, то $\deg \Phi(t) = n-1$).

Заметим, что действительные части всех корней t_0 многочлена $\Phi(t)$ неотрицательны. В самом деле, если $0 \neq t_0 \in \mathbb{C}$, $\operatorname{Re}(t_0) < 0$, то $\operatorname{Re}\left(\frac{1}{t_0}\right) < 0$. В силу теоремы 3.27.7 (см. п. 2)) многочлен

$$F\left(z, \frac{1}{t_0}\right) = f_{\frac{1}{t_0}}(z) \in \mathbb{C}[z]$$

устойчив. Так как $\operatorname{Re}(d) \geqslant 0$, то $F\left(d, \frac{1}{t_0}\right) \neq 0$, следовательно, $\Phi(t_0) = t^{n-1}F\left(d, \frac{1}{t_0}\right) \neq 0$.

По теореме Виета сумма всех корней многочлена $\Phi(t) \in \mathbb{C}[t]$, $\Phi(t) = F_0(d)t^{n-1} + F_1(d)t^{n-2} + \dots + F_{n-1}(d)$, $F_0(d) \neq 0$, равна $-\frac{F_1(d)}{F_0(d)}$, и поэтому

$$\operatorname{Re}\left(-\frac{F_1(d)}{F_0(d)}\right) \geqslant 0.$$

Допустим противное: $T(d, c) = 0$, то есть $F_1(d)c + F_0(d) = 0$, где $0 \neq c \in \mathbb{C}$, $\operatorname{Re}(c) < 0$. Тогда $\frac{F_1(d)}{F_0(d)} = \frac{1}{c}$, и поэтому $\operatorname{Re}\left(\frac{1}{c}\right) \geq 0$, следовательно, $\operatorname{Re}(c) \geq 0$, что противоречит нашему выбору числа $c \in \mathbb{C}$.

Таким образом, мы показали, что $T(d, c) \neq 0$ для любого $d \in \mathbb{C}$ такого, что $\operatorname{Re}(d) \geq 0$ и $F_0(d) \neq 0$.

Случай б). Пусть $F_0(d) = 0$.

Допустим противное: $T(d, c) = 0$, то есть $F_1(d)c + F_0(d) = 0$, где $0 \neq c \in \mathbb{C}$, $\operatorname{Re}(c) < 0$. В силу равенств (*) из доказательства леммы 3.27.8 имеем

$$0 = \bar{a}_0 f(d) - a_0 f^*(d);$$

$$0 = \bar{a}_1 f(d) + a_1 f^*(d).$$

Поэтому

$$(\bar{a}_0 a_1 + a_0 \bar{a}_1) f(d) = 0.$$

Так как многочлен $f(z) \in \mathbb{C}[z]$ устойчив и $\operatorname{Re}(d) \geq 0$, то $f(d) \neq 0$. Поэтому $\bar{a}_0 a_1 + a_0 \bar{a}_1 = 0$, при этом $0 \neq a_0 \in \mathbb{C}$. Следовательно, $\frac{a_1}{a_0} = -\left(\frac{\bar{a}_1}{\bar{a}_0}\right)$, то есть $\operatorname{Re}\left(\frac{a_1}{a_0}\right) = 0$, что противоречит уже установленному неравенству $\operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$. Итак, мы пришли к противоречию, тем самым доказано, что и в случае б) имеем $T(d, c) \neq 0$ для всех $0 \neq c \in \mathbb{C}$, $d \in \mathbb{C}$, $\operatorname{Re}(c) < 0$, $\operatorname{Re}(d) \geq 0$.

1б) Покажем, что степень нашего многочлена

$$F(z, c) = \frac{f^*(c)f(z) - f(c)f^*(z)}{z - c} \in \mathbb{C}[z]$$

равна в точности $n - 1$, если $a_0 \neq 0$ и $\operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$.

Ясно, что $\deg F(z, c) \leq n - 1$. Допустим, что $\deg F(z, c) < n - 1$. Тогда коэффициент при z^{n+1} в многочлене из леммы 3.27.8

$$z^2 T(z, c) = f(z)\varphi(z, c) - f^*(z)\psi(z, c)$$

равен нулю, то есть

$$a_n(\bar{a}_0 - \bar{a}_1 c) - (-1)^n \bar{a}_n(a_0 + a_1 c) = 0.$$

Поэтому ($|a_n| = |\bar{a}_n| \neq 0$)

$$|\bar{a}_0 - \bar{a}_1 c| = |a_0 + a_1 c|.$$

Однако если $z = \frac{1}{c}$, $w = -\frac{a_1}{a_0}$, поскольку $\operatorname{Re}(z) < 0$, $\operatorname{Re}(w) < 0$, то $|z + \bar{w}| > |z - w|$ (см. лемму 3.26.4), т. е.

$$\left| \frac{1}{c} - \frac{\bar{a}_1}{\bar{a}_0} \right| > \left| \frac{1}{c} + \frac{a_1}{a_0} \right|.$$

Умножая это неравенство на $|\bar{a}_0 c| = |a_0 c|$, получаем

$$|\bar{a}_0 - \bar{a}_1 c| > |a_0 + a_1 c|,$$

что противоречит установленному ранее равенству.

2) Допустим теперь, что $a_0 \neq 0$, $\operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$ и для некоторого $c \in \mathbb{C}$ такого, что $\operatorname{Re}(c) < 0$, многочлен

$$T(z, c) = F_1(z)c + F_0(z) \in \mathbb{C}[z]$$

устойчив. Покажем, что многочлен $f(z) \in \mathbb{C}[z]$ устойчив. Допустим противное, то есть предположим, что $f(d) = 0$ для некоторого $0 \neq d \in \mathbb{C}$ такого, что $\operatorname{Re}(d) \geq 0$. В силу следствия 3.27.9

$$d^2[T(d, c)\varphi^*(d, c) + T^*(d, c)\psi(d, c)] = 0.$$

Следовательно,

$$T(d, c)\varphi^*(d, c) + T^*(d, c)\psi(d, c) = 0.$$

Поэтому

$$|T(d, c)| \cdot |\varphi^*(d, c)| = |T^*(d, c)| \cdot |\psi(d, c)|.$$

Так как многочлен $T(z, c) \in \mathbb{C}[z]$ устойчив и $\operatorname{Re}(d) \geq 0$, то по лемме 3.27.3 (п. 2) и 3))

$$0 \leq |T^*(d, c)| < |T(d, c)|$$

или

$$0 < |T(d, c)| = |T^*(d, c)|.$$

Поэтому

$$|\varphi^*(d, c)| \leq |\psi(d, c)|. \quad (3.3)$$

Однако если $z, w \in \mathbb{C}$ и $\operatorname{Re}(z) < 0$, $\operatorname{Re}(w) < 0$, то

$$|z + \bar{w}| > |z - w|$$

(см. лемму 3.26.4).

Если $z = -\frac{a_1}{a_0} - \frac{1}{d}$, $w = \frac{1}{c}$, то так как $\operatorname{Re}(c) < 0$, то $\operatorname{Re}(w) < 0$; так как $\operatorname{Re}(d) \geq 0$ и $\operatorname{Re}\left(\frac{a_1}{a_0}\right) > 0$, то $\operatorname{Re}(z) < 0$. Поэтому

$$\left| \frac{a_1}{a_0} + \frac{1}{d} - \frac{1}{\bar{c}} \right| = \left| -\frac{a_1}{a_0} - \frac{1}{d} + \frac{1}{\bar{c}} \right| > \left| -\frac{a_1}{a_0} - \frac{1}{d} - \frac{1}{c} \right| = \left| \frac{a_1}{a_0} + \frac{1}{d} + \frac{1}{c} \right|.$$

Умножая это неравенство на $|a_0 d \bar{c}| = |a_0 d c|$, получаем

$$|a_1 d \bar{c} + a_0 \bar{c} - a_0 d| > |a_1 d c + a_0 c + a_0 d|.$$

Так как (см. лемму 3.27.8)

$$\varphi(z, c) = \bar{a}_0(z + c) - \bar{a}_1 z c, \quad \psi(z, c) = a_0(z + c) + a_1 z c,$$

то

$$\varphi^*(z, c) = a_0(-z + \bar{c}) + a_1 z \bar{c},$$

и поэтому

$$\begin{aligned} |\varphi^*(d, c)| &= |a_0(-d + \bar{c}) + a_1 d \bar{c}| = \\ &= |a_1 d \bar{c} + a_0 \bar{c} - a_0 d| > |a_1 d c + a_0 c + a_0 d| = \\ &= |a_0(d + c) + a_1 d c| = |\psi(d, c)|. \end{aligned}$$

Это приводит нас к противоречию с $|\varphi^*(d, c)| \leq |\psi(d, c)|$ (см. (3.3)), что завершает доказательство теоремы. \square

Следствие 3.27.11. Пусть

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{R}[x], \quad a_n > 0,$$

$$\tilde{f}(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n,$$

$c = -1$, $f_{(x)}^{(1)} = \frac{1}{2} \widetilde{T}_{\tilde{f}}(x, -1)$. Тогда многочлен $f(x)$ устойчив тогда и только тогда, когда $a_{n-1} > 0$ и многочлен $f_{(x)}^{(1)}$ устойчив.

Доказательство. В силу замечания 3.26.5 многочлен $f(x)$ устойчив тогда и только тогда, когда устойчив многочлен $\tilde{f}(x)$.

Применяя теорему Шура к $\tilde{f}(x)$ (при $c = -1$), убеждаемся в том, что устойчивость многочлена $\tilde{f}(x)$ равносильна условиям

$$a_n \neq 0, \quad \operatorname{Re} \frac{a_{n-1}}{a_n} > 0, \quad T_{\tilde{f}}(x, -1) \text{ — устойчивый многочлен},$$

то есть, поскольку $a_n > 0$, равносильна условиям

$$a_{n-1} > 0, \quad f^{(1)}(x) = \frac{1}{2} \widetilde{T}_{\tilde{f}}(x, -1) \text{ — устойчивый многочлен.} \quad \square$$

3.28. Теорема Гурвица об устойчивых многочленах (с действительными коэффициентами)

Из критерия устойчивости Шура мы выведем сейчас один из наиболее ярких результатов теории устойчивых многочленов — теорему Гурвица. Мы ограничимся рассмотрением случая многочлена с действительными коэффициентами.

Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{R}[x],$$

$a_n > 0$, $\deg f(x) = n$.

Матрицей Гурвица многочлена $f(x)$ называется квадратная $(n \times n)$ -матрица

$$H(f) = \begin{pmatrix} a_{n-1} & a_{n-3} & a_{n-5} & \dots & a_{-n+1} \\ a_n & a_{n-2} & a_{n-4} & \dots & a_{-n+2} \\ 0 & a_{n-1} & a_{n-3} & \dots & a_{-n+3} \\ 0 & a_n & a_{n-2} & \dots & a_{-n+4} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_0 \end{pmatrix} \in M_n(\mathbb{R}),$$

при чётном $n = 2k$ последняя строка имеет вид

$$(0 \dots 0 \ a_n \ a_{n-2} \ \dots \ a_0),$$

при нечётном $n = 2k + 1$ последняя строка имеет вид

$$(0 \dots 0 \ a_{n-1} \ a_{n-3} \ \dots \ a_0),$$

при этом предполагается, что $a_k = 0$ при $k < 0$ и при $k > n$, таким образом: $H(f) = (h_{ij}) \in M_n(\mathbb{R})$, где $h_{ij} = a_{n+i-2j}$, а i -я строка матрицы $H(f)$ имеет вид

$$H_i = (a_{n+i-2}, a_{n+i-4}, a_{n+i-6}, \dots, a_{n+i-2j}, \dots, a_{-n+i}).$$

Определителями Гурвица многочлена $f(x) \in \mathbb{R}[x]$ называются главные миноры матрицы Гурвица $H(f)$ многочлена $f(x)$:

$$D_1 = a_{n-1}, \quad D_2 = \begin{vmatrix} a_{n-1} & a_{n-3} \\ a_n & a_{n-2} \end{vmatrix}, \quad D_3 = \begin{vmatrix} a_{n-1} & a_{n-3} & a_{n-5} \\ a_n & a_{n-2} & a_{n-4} \\ 0 & a_{n-1} & a_{n-3} \end{vmatrix}, \dots, \quad D_n = |H(f)|.$$

Предложение 3.28.1 (связь определителей Гурвица многочленов $f(x), f^{(1)}(x) \in \mathbb{R}[x]$). Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{R}[x], \quad a_n > 0, \quad \deg f(x) = n;$$

$$\tilde{f}(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \in \mathbb{R}[x];$$

$$f^{(1)}(x) = \frac{1}{2} T_{\tilde{f}}(x, -1) = b_{n-1} x^{n-1} + \dots + b_1 x + b_0 \in \mathbb{R}[x]$$

$$(T_{\tilde{f}}(x, -1) = 2b_{n-1} + 2b_{n-2} x + \dots + 2b_1 x^{n-2} + 2b_0 x^n);$$

D_1, D_2, \dots, D_n — главные миноры матрицы Гурвица $H(f) \in M_n(\mathbb{R})$; $D_1^{(1)}, D_2^{(1)}, \dots, D_{n-1}^{(1)}$ — главные миноры матрицы Гурвица $H(f^{(1)}) \in M_{n-1}(\mathbb{R})$. Тогда для любого индекса $j = 1, \dots, n-1$ имеем

$$D_j^{(1)} = \begin{cases} (a_n a_{n-1})^{\frac{j-1}{2}} D_{j+1}, & \text{если } j \text{ нечётно,} \\ a_n (a_n a_{n-1})^{\frac{j-2}{2}} D_{j+1}, & \text{если } j \text{ чётно.} \end{cases}$$

Доказательство. Пусть

$$\tilde{g}(x) = a_n + a_{n-2} x^2 + \dots;$$

$$\tilde{h}(x) = a_{n-1} x + a_{n-3} x^3 + \dots$$

Тогда

$$\tilde{f}(x) = \tilde{g}(x) + \tilde{h}(x), \quad \tilde{f}^*(x) = \tilde{g}(x) - \tilde{h}(x).$$

В силу леммы 3.27.8 (применённой к $\tilde{f}(x)$, $c = -1$)

$$\begin{aligned} x^2 T_{\tilde{f}}(x, -1) &= \tilde{f}(x) \varphi(x, -1) - \tilde{f}^* \psi(x, -1) = \\ &= (\tilde{g}(x) + \tilde{h}(x))(a_n(x-1) + a_{n-1}x) - \\ &\quad - (\tilde{g}(x) - \tilde{h}(x))(a_n(x-1) - a_{n-1}x) = \\ &= 2a_{n-1}x\tilde{g}(x) + 2a_n(x-1)\tilde{h}(x). \end{aligned}$$

Так как

$$T_{\tilde{f}}(x, -1) = 2b_{n-1} + \dots + 2b_1 x^{n-2} + 2b_0 x^{n-1},$$

то, сокращая на 2, получим

$$x^2(b_{n-1} + \dots + b_0 x^n) = a_{n-1}x(a_n + a_{n-2}x^2 + \dots) + a_n(x-1)(a_{n-1}x + a_{n-3}x^3 + \dots).$$

Приравнивая коэффициенты при степенях x^k получаем

$$b_{n-1} = a_n a_{n-1} \quad (\text{при } x^2),$$

$$b_{n-2} = a_{n-1} a_{n-2} - a_n a_{n-3} \quad (\text{при } x^3),$$

...

$$b_{n-(2k-1)} = a_n a_{n-(2k-1)} \quad (\text{при } x^{2k}),$$

$$\left. b_{n-2k} = a_{n-1} a_{n-2k} - a_n a_{n-(2k+1)} \quad (\text{при } x^{2k+1}) \right\} k = 1, 2, \dots,$$

...

Это означает, что матрица Гурвица многочлена $f^{(1)}(x)$ имеет вид

$$H(f^{(1)}) = \begin{pmatrix} b_{n-2} & b_{n-4} & b_{n-6} & \dots \\ b_{n-1} & b_{n-3} & b_{n-5} & \dots \\ 0 & b_{n-2} & b_{n-4} & \dots \\ \dots & b_{n-1} & b_{n-3} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} =$$

$$= \begin{pmatrix} a_{n-1} a_{n-2} - a_n a_{n-3} & a_{n-1} a_{n-4} - a_n a_{n-5} & a_{n-1} a_{n-6} - a_n a_{n-7} & \dots \\ a_n a_{n-1} & a_n a_{n-3} & a_n a_{n-5} & \dots \\ 0 & a_{n-1} a_{n-2} - a_n a_{n-3} & a_{n-1} a_{n-4} - a_n a_{n-5} & \dots \\ 0 & a_n a_{n-1} & \dots & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \in M_{n-1}(\mathbb{R}),$$

при этом, в наших обозначениях, её главные миноры имеют вид

$$D_1^{(1)} = b_{n-2} = a_{n-1} a_{n-2} - a_n a_{n-3};$$

$$D_2^{(1)} = \begin{vmatrix} b_{n-2} & b_{n-4} \\ b_{n-1} & b_{n-3} \end{vmatrix} = \begin{vmatrix} a_{n-1} a_{n-2} - a_n a_{n-3} & a_{n-1} a_{n-4} - a_n a_{n-5} \\ a_n a_{n-1} & a_n a_{n-3} \end{vmatrix};$$

...

$$D_{n-1}^{(1)} = |H(f^{(1)})|.$$

Рассмотрим следующее окаймление матрицы $H(f^{(1)})$ до $(n \times n)$ -матрицы:

$$C = \begin{pmatrix} a_n a_{n-1} & a_n a_{n-3} & a_n a_{n-5} & \dots \\ 0 & a_{n-1} a_{n-2} - a_n a_{n-3} & a_{n-1} a_{n-4} - a_n a_{n-5} & \dots \\ 0 & a_n a_{n-1} & a_n a_{n-3} & \dots \\ 0 & 0 & a_{n-1} a_{n-2} - a_n a_{n-3} & \dots \\ 0 & 0 & a_n a_{n-1} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix} \in M_n(\mathbb{R}),$$

при этом главные миноры матрицы C равны

$$a_n a_{n-1}, \quad a_n a_{n-1} D_1^{(1)}, \quad a_n a_{n-1} D_2^{(1)}, \dots, \quad a_n a_{n-1} D_{n-1}^{(1)}.$$

Прибавляя в матрице C первую строку ко второй ($C'_2 = C_2 + C_1$), третью строку к четвёртой ($C'_4 = C_4 + C_3$) и т. д., мы приходим к матрице

$$C' = \begin{pmatrix} a_n a_{n-1} & a_n a_{n-3} & a_n a_{n-5} & \dots \\ a_n a_{n-1} & a_{n-1} a_{n-2} & a_{n-1} a_{n-4} & \dots \\ 0 & a_n a_{n-1} & a_n a_{n-3} & \dots \\ 0 & a_n a_{n-1} & a_{n-1} a_{n-2} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

с теми же главными минорами, что и для матрицы C .

Вынося из нечётных строк матрицы C' общий множитель a_n , а из чётных строк общий множитель a_{n-1} , получаем матрицу Гурвица $H(f)$ многочлена $f(x)$. Поэтому главные миноры матрицы C' (а следовательно, и матрицы C) имеют вид

$$a_n a_{n-1}, \quad a_n a_{n-1} D_2, \dots, \quad a_n^k a_{n-1}^k D_{2k}, \quad a_n^{k+1} a_{n-1}^k D_{2k+1}, \dots$$

Сравнивая выражения главных миноров матрицы через $D_k^{(1)}$ и через D_k , получаем утверждение предложения. \square

Теорема 3.28.2 (теорема Гурвица (1895 г.) для многочленов с действительными коэффициентами). Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{R}[x],$$

$a_n > 0$, D_1, \dots, D_n — главные миноры матрицы Гурвица $H(f)$ многочлена $f(x)$. Многочлен $f(x)$ устойчив тогда и только тогда, когда

$$D_1 > 0, \quad D_2 > 0, \dots, \quad D_n > 0.$$

Доказательство. Проведём индукцию по степени $n = \deg f(x)$. Для $n = 1$ утверждение очевидно. Пусть утверждение теоремы Гурвица верно для всех многочленов, степень которых $\leq n - 1$.

Пусть теперь $f(x) = a_n x^n + \dots + a_0 \in \mathbb{R}[x]$, $\deg f(x) = n$, $a_n > 0$. В силу следствия к теореме Шура, $f(x)$ — устойчивый многочлен тогда и только тогда, когда $a_{n-1} > 0$ и устойчив многочлен $f^{(1)}(x)$ степени $\leq n - 1$. Используя индуктивное предположение, получаем, что многочлен $f(x)$ устойчив тогда и только тогда, когда $a_{n-1} > 0$ и все определители Гурвица $D_1^{(1)}, \dots, D_{n-1}^{(1)}$ матрицы Гурвица $H(f^{(1)})$ положительны (старший коэффициент b_{n-1} многочлена $f^{(1)}(x)$ равен $a_n a_{n-1}$ (см. доказательство замечания), и, поскольку $a_n > 0$, условие $a_{n-1} > 0$ равносильно тому, что $b_{n-1} > 0$). Согласно предложению 3.28.1 неравенства

$$a_{n-1} > 0, \quad D_1^{(1)} > 0, \dots, \quad D_{n-1}^{(1)} > 0$$

(с учётом $a_n > 0$) равносильны неравенствам

$$D_1 = a_{n-1} > 0, \quad D_2 > 0, \dots, \quad D_n > 0.$$

Таким образом, многочлен $f(x)$ устойчив тогда и только тогда, когда

$$D_1 > 0, \quad D_2 > 0, \dots, \quad D_n > 0. \quad \square$$

Упражнение 3.28.3. Сформулируйте критерий Гурвица для многочленов $f(z) \in \mathbb{C}[z]$ с комплексными коэффициентами.

Упражнение 3.28.4 (теорема Льенара—Шипара, 1914 г.). Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{R}[x],$$

$a_n > 0$, тогда

- 1) если $n = 2m + 1$ — нечётное число, то многочлен $f(x)$ устойчив тогда и только тогда, когда

$$D_2 > 0, D_4 > 0, \dots, D_{n-1} > 0;$$

- 2) если $n = 2m$ — чётное число, то многочлен $f(x)$ устойчив тогда и только тогда, когда

$$D_1 > 0, D_3 > 0, \dots, D_{n-1} > 0.$$

Следствие 3.28.5. Положительность всех определителей Гурвица чётного порядка равносильна положительности всех определителей Гурвица нечётного порядка.

Пример 3.28.6. $f(x) = x^3 + 2x^2 + 3x + 1 \in \mathbb{R}[x]$, $a_3 = 1 > 0$,

$$H(f) = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 3 & 0 \\ 0 & 2 & 1 \end{pmatrix},$$

$$D_1 = 2 > 0, D_2 = \begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix} = 5 > 0, D_3 = \begin{vmatrix} 2 & 1 & 0 \\ 1 & 3 & 0 \\ 0 & 2 & 1 \end{vmatrix} = 5 > 0,$$

следовательно, $f(x)$ — устойчивый многочлен.

Пример 3.28.7. $f(x) = x^3 + 2x^2 + x + 3 \in \mathbb{R}[x]$, $a_3 = 1 > 0$,

$$H(f) = \begin{pmatrix} 2 & 3 & 0 \\ 1 & 1 & 0 \\ 0 & 2 & 3 \end{pmatrix},$$

$$D_2 = \begin{vmatrix} 2 & 3 \\ 1 & 1 \end{vmatrix} = -1 < 0,$$

следовательно, многочлен $f(x)$ не является устойчивым (хотя все его коэффициенты положительны), т. е. хотя бы один его корень лежит в правой полуплоскости (поскольку у него нет чисто мнимых корней).

Пример 3.28.8 (схема Рауса, 1875 г.). На основе теории Штурма и теории индексов английский механик Раус предложил алгоритм для определения числа k корней многочлена $f(x) \in \mathbb{R}[x]$ с действительными коэффициентами, расположенных в правой полу平面 { $z \in \mathbb{C} \mid \operatorname{Re} z > 0$ }; при $k = 0$ этот алгоритм даёт критерий устойчивости.

Пусть

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{R}[x],$$

$a_n > 0$. Составим таблицу Рауса

$$R(f) = \begin{pmatrix} r_0^{(1)} & r_1^{(1)} & r_2^{(1)} & \dots \\ r_0^{(2)} & r_1^{(2)} & r_2^{(2)} & \dots \\ \dots & \dots & \dots & \dots \\ r_0^{(p)} & r_1^{(p)} & r_2^{(p)} & \dots \end{pmatrix},$$

где первая строка R_1 равна $H_2 = (a_n a_{n-2}, a_{n-4}, \dots)$ (второй строке матрицы Гурвица $H(f)$); вторая строка R_2 равна $H_1 = (a_{n-1}, a_{n-3}, a_{n-5}, \dots)$ (первой строке матрицы Гурвица $H(f)$); при $i \geq 3$ строка R_i определяется по формуле

$$r_j^{(i)} = r_{j+1}^{(i-2)} - \frac{r_0^{(i-2)}}{r_0^{(i-1)}} r_{j+1}^{(i-1)}$$

(т. е. $R_{i-2} - \frac{r_0^{(i-2)}}{r_0^{(i-1)}} R_{i-1} = (0, R_i)$, другими словами: из $(i-2)$ -й строки вычитается $(i-1)$ -я строка, умноженная на такое число, чтобы начальный элемент строки обратился в нуль; этот нулевой член отбрасывается, получившаяся строка сдвигается на одну позицию влево); построение останавливается на p -й строке, если $r_0^{(p+1)} = 0$.

Критерий Рауса. Многочлен

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{R}[x]$$

с действительными коэффициентами, $a_n > 0$, устойчив тогда и только тогда, когда процесс построения таблицы Рауса $R(f)$ не останавливается до $(n+1)$ -й строки (регулярный случай), при этом все элементы начального столбца этой таблицы Рауса положительны.

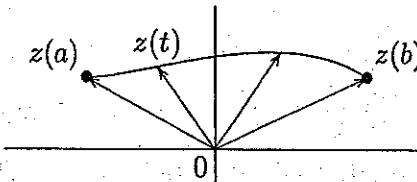
Замечание. В регулярном случае число k корней многочлена $f(x)$, лежащих в правой полуплоскости, равно числу перемен знаков в первом столбце таблицы Рауса $R(f)$.

Замечание 3.28.9. Используя начальные топологические понятия и результаты, связанные с индексами особых точек векторных полей, покажите, что многочлен $f(z)$ степени n устойчив тогда и только тогда, когда точка $f(it)$ при изменении t от $-\infty$ до $+\infty$ обходит начало координат $\frac{n}{2}$ раз (в сторону от 1 к i).

3.29. Комментарий к вопросу о распределении корней многочлена с комплексными коэффициентами на комплексной плоскости

1. Согласованный выбор аргумента точки комплексной плоскости, движущейся по непрерывной линии:

Пусть $z: [a, b] \rightarrow \mathbb{C}$ — непрерывная функция (т. е. $z(t) = x(t) + y(t)i$ — непрерывная функция от t , где $a \leq t \leq b$, $a, b \in \mathbb{R}$, принимающая комплексные значения), при этом $z(t) \neq 0$ для всех $t \in [a, b]$ (т. е. линия $z(t)$, $t \in [a, b]$, не проходит через точку 0 в комплексной плоскости \mathbb{C})



и поэтому определена многозначная функция аргумент $\text{Arg } z(t) = \arg z(t) + 2\pi k$.

Из непрерывности функции $z(t)$ следует непрерывность функций $x(t)$, $y(t)$ и $|z(t)| = \sqrt{x(t)^2 + y(t)^2}$ на компакте $[a, b]$, а поэтому и их равномерная непрерывность. Поэтому:

а) функция $|z(t)|$ на отрезке $[a, b]$ достигает своего минимума и, следовательно,

$$r = \inf\{|z(t)| \mid t \in [a, b]\} > 0;$$

- б) можно накрыть отрезок $[a, b]$ конечным числом интервалов прямой \mathbb{R} , на пересечении каждого из которых с $[a, b]$ колебание функции не превосходит $\frac{r}{2}$, и следовательно, на каждом таком интервале можно считать, что $\arg z(t)$ меняется непрерывно (при фиксации значения в начале интервала);
- в) таким образом, выбрав значение аргумента $\arg z(a)$ в начале пути $z(a)$, можно выбрать значение аргумента $\arg z(t)$ при всех t так, что функция $\arg z(t)$ является непрерывной функцией от t .

Замечание 3.29.1. Условие $z(t) \neq 0$ для $t \in [a, b]$ существенно. Действительно, если $z(t) = t$ для $t \in [-1, 1]$, то:

при $t < 0$ имеем $\operatorname{Arg} z(t) = (2k + 1)\pi$;

при $t > 0$ имеем $\operatorname{Arg} z(t) = 2k\pi$.

Итак, нельзя согласовать выбор $\arg z(t)$ для $t \in [-1, 1]$ (доопределив значение при $t = 0$) так, чтобы получить непрерывность при $t = 0$.

2. Согласование выбора аргумента для произведения непрерывных комплексных функций $z(t) = z_1(t) \dots z_k(t)$, $t \in [a, b]$ ($z_i(t) \neq 0$ для всех $i = 1, \dots, k$, $t \in [a, b]$).

Выберем при $t = a$ значения аргументов $\operatorname{Arg} z_1(t), \dots, \operatorname{Arg} z_k(t)$ и $\operatorname{Arg} z(t)$ так, что

$$\operatorname{arg} z(a) = \sum_{j=1}^k \operatorname{arg} z_j(a).$$

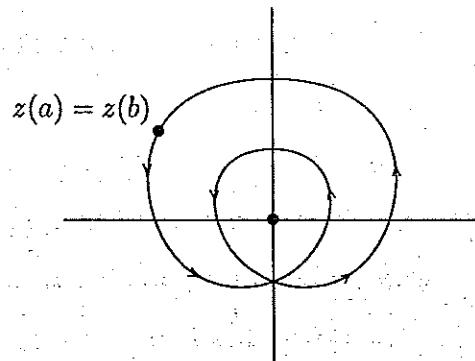
Тогда при непрерывном изменении аргументов (возможном в силу 1) равенство

$$\operatorname{arg} z(t) = \sum_{j=1}^k \operatorname{arg} z_j(t)$$

сохранится при всех $t \in [a, b]$ (как непрерывная функция разность $\operatorname{arg} z(t) - \sum_{j=1}^k \operatorname{arg} z_k(t)$, принимающая значения $2k\pi$ и равная 0 при $t = a$, равна 0 при всех $t \in [a, b]$).

3. Замкнутая непрерывная линия: $z(t)$ — непрерывная комплекснозначная функция действительного переменного $t \in [a, b] \subset \mathbb{R}$, $z(a) = z(b)$ ($z(t) \neq 0$ для всех $t \in [a, b]$). В этом случае при непрерывном изменении аргумента $\operatorname{arg} z(t)$ разность значений при $t = a$ и $t = b$ может отличаться на $k \cdot 2\pi$, $k \in \mathbb{Z}$. Геометрический смысл целого числа k : число полных оборотов вокруг начала координат $z = 0$ точки $z(t)$ при обходе этой точки в направлении возрастания параметра t от a к b (с учётом знака в соответствии с направлением обхода, т. е. + для обхода против часовой стрелки, - для обхода по часовой стрелке). Например,

для указанного направления обхода $k = 2$ (при противоположном обходе $k = -2$).



4. Принцип аргумента. Под *простым замкнутым контуром* Γ будем понимать непрерывную замкнутую линию в комплексной плоскости \mathbb{C} без самопересечений (т. е. $z(t)$ — непрерывная функция, $t \in [a, b]$, $z(a) = z(b)$, $z(t_1) \neq z(t_2)$ при $a < t_1 < t_2 < b$). *Теорема Жордана* утверждает, что простой замкнутый контур разбивает $\mathbb{C} \setminus \Gamma$ на две связные части: внутренность контура и внешняя часть контура. Пример простого замкнутого контура:

$$\Gamma = \Gamma(z_0, r) = \{z \in \mathbb{C} \mid |z - z_0| = r\} —$$

окружность радиуса r с центром в $z_0 \in \mathbb{C}$.

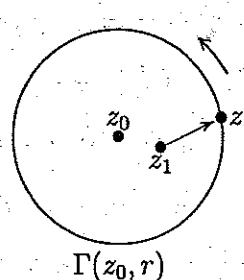
Лемма 3.29.2. Пусть $z = z(t)$ обходит простой замкнутый контур в положительном направлении, $z_1 \in \mathbb{C} \setminus \Gamma$. Тогда

$$\Delta_{\Gamma} \arg(z - z_1) = \begin{cases} 2\pi, & \text{если } z_1 \text{ внутри } \Gamma; \\ 0, & \text{если } z_1 \text{ вне } \Gamma \end{cases}$$

(здесь $\Delta_{\Gamma} \arg(z - z_1)$ — приращение $\arg(z - z_1)$ при обходе по Γ вокруг z_1 в \mathbb{C}).

Доказательство для произвольного простого замкнутого контура достаточно сложно и требует техники, выходящей за рамки данного курса. Мы проведём его для частного случая окружности $\Gamma(z_0, r)$.

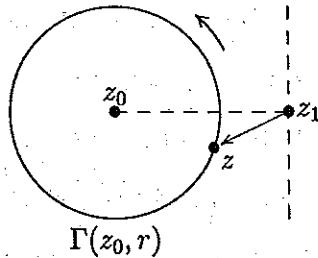
Случай а): z_1 находится внутри контура $\Gamma(z_0, r)$.



Ясно, что при обходе один раз в положительном направлении вектор $z - z_1$ обернётся вокруг своего начала z_1 тоже один раз в положительном направлении, то есть

$$\Delta_{\Gamma} \arg(z - z_1) = 2\pi.$$

Случай б): z_1 находится вне контура $\Gamma(z_0, r)$



Так как при обходе точкой z контура $\Gamma(z_0, r)$ в этом случае колебания аргумента $\arg(z - z_1)$ не превосходят π ,

$$\Delta_{\Gamma} \arg(z - z_1) = 0.$$

Теорема 3.29.3 (принцип аргумента). Пусть многочлен $f(z) \in \mathbb{C}[z]$ не имеет корней на простом замкнутом контуре $\Gamma \subset \mathbb{C}$. Тогда число комплексных корней многочлена $f(z)$ (с учётом их кратностей) внутри контура Γ равно

$$\frac{\Delta_{\Gamma} \arg f(z)}{2\pi}$$

(здесь $\Delta_{\Gamma} \arg f(z)$ — приращение аргумента $\arg f(z)$ при обходе точкой $z = z(t)$ контура Γ один раз в положительном направлении).

Доказательство. Пусть $\deg f(z) = n > 0$,

$$f(z) = a_n(z - z_1) \dots (z - z_n),$$

где z_1, \dots, z_n — корни многочлена (с учётом кратностей). При обходе точкой $z = z(t)$ простого контура сомножители и их произведение $f(z(t))$ меняются непрерывно. В силу п. 2 можно считать, что

$$\arg f(z) = \arg a_n + \arg(z - z_1) + \dots + \arg(z - z_n).$$

Следовательно,

$$\Delta_{\Gamma} \arg f(z) = \sum_{j=1}^n \Delta_{\Gamma} \arg(z - z_j)$$

(при однократном обходе $z = z(t)$ по контуру Γ).

В силу леммы 3.29.2

$$\Delta_{\Gamma} \arg(z - z_j) = \begin{cases} 2\pi, & \text{если } z_j \text{ внутри } \Gamma, \\ 0, & \text{если } z_j \text{ вне } \Gamma. \end{cases}$$

Поэтому

$$\Delta_{\Gamma} \arg f(z) = m \cdot 2\pi,$$

где m — число корней z_j , расположенных внутри контура Γ . Следовательно,

$$m = \frac{\Delta_{\Gamma} \arg f(z)}{2\pi}.$$

5. Теорема Руше. Пусть $f(z), g(z) \in \mathbb{C}[z]$, Γ — простой замкнутый контур в комплексной плоскости \mathbb{C} . Если

$$|f(z) - g(z)| < |g(z)|$$

для всех $z \in \Gamma$, то внутри контура Γ располагается одинаковое число корней многочленов $f(z)$ и $g(z)$ (с учётом кратностей).

Доказательство. 1) Проверим, что к многочленам $g(z)$ и $f(z)$ можно применить принцип аргумента. Так как

$$|g(z)| > |f(z) - g(z)| \geq 0,$$

то

$$|g(z)| > 0$$

для всех $z \in \Gamma$; кроме того,

$$|f(z)| = |g(z) + (f(z) - g(z))| \geq |g(z)| - |f(z) - g(z)| > 0$$

для всех $z \in \Gamma$. Таким образом, $g(z)$ и $f(z)$ не обращаются в 0 на контуре Γ .

Так как

$$f(z) = g(z) \left(1 + \frac{f(z) - g(z)}{g(z)} \right),$$

то

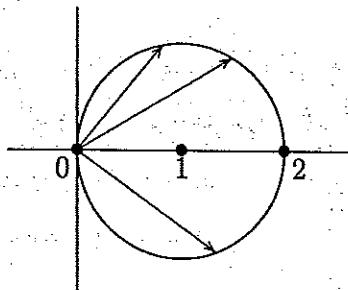
$$\Delta_{\Gamma} \arg f(z) = \Delta_{\Gamma} \arg g(z) + \Delta_{\Gamma} \arg \left(1 + \frac{f(z) - g(z)}{g(z)} \right)$$

(точка $z = z(t)$ пробегает контур Γ).

Поскольку

$$\left| \frac{f(z) - g(z)}{g(z)} \right| < 1,$$

комплексное число $1 + \frac{f(z) - g(z)}{g(z)}$ лежит в правой полуплоскости,



поэтому

$$\Delta_{\Gamma} \arg \left(1 + \frac{f(z) - g(z)}{g(z)} \right) = 0.$$

Итак,

$$\Delta_{\Gamma} \arg f(z) = \Delta_{\Gamma} \arg g(z).$$

В силу принципа аргумента число корней многочлена $f(z)$ и число корней многочлена $g(z)$ внутри контура Γ совпадают:

$$\frac{\Delta_{\Gamma} \arg f(z)}{2\pi} = \frac{\Delta_{\Gamma} \arg g(z)}{2\pi}.$$

□

Следствие 3.29.4 (другое доказательство теоремы Гаусса с оценкой для модуля корней). Пусть

$$f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0 \in \mathbb{C}[z]$$

и $R = 1 + a$, где $a = \max\{|a_i|, 0 \leq i \leq n-1\}$. Тогда внутри круга

$$\{z \in \mathbb{C} \mid |z| \leq R\}$$

расположены все n корней многочлена $f(z)$ (с учётом их кратностей).

Доказательство. Внутри рассматриваемого круга

$$\{z \in \mathbb{C} \mid |z| \leq R\}$$

многочлен $g(z) = z^n$ имеет корень 0 кратности n . Проверим условия теоремы Руше в этом случае, то есть что для всех $\{z \in \mathbb{C} \mid |z| = R = 1 + a\}$ имеем

$$\begin{aligned} |f(z) - g(z)| &= |a_{n-1}z^{n-1} + \dots + a_1z + a_0| \leq \\ &\leq a(|z|^{n-1} + |z|^{n-2} + \dots + 1) = a \frac{|z|^n - 1}{|z| - 1} = \\ &= \frac{a(|z|^n - 1)}{a} = |z|^n - 1 < |z|^n = |g(z)|. \end{aligned}$$

□

Пример 3.29.5. Определим число корней многочлена

$$f(z) = z^8 - 4z^5 + z^2 - 1,$$

модуль которых меньше единицы. Положим $g(z) = -4z^5$ и $\Gamma = \{z \in \mathbb{C} \mid |z| = 1\}$. Тогда $h(z) = f(z) - g(z) = z^8 + z^2 - 1$. Для $z \in \Gamma$ (т. е. $|z| = 1$) имеем:

$$\begin{aligned} |g(z)| &= |-4z^5| = 4; \\ |h(z)| &= |z^8 + z^2 - 1| \leq |z^8| + |z^2| + 1 = 3 < 4 = |g(z)|. \end{aligned}$$

Следовательно, по теореме Руше многочлен $f(z)$ имеет внутри окружности $\Gamma = \{z \in \mathbb{C} \mid |z| = 1\}$ столько же корней, сколько и многочлен $g(z) = -4z^5$, то есть пять корней. Итак, многочлен $f(z)$ имеет пять корней, по модулю меньших единицы.

6. Непрерывная зависимость комплексных корней многочлена от его коэффициентов.

Теорема 3.29.6. Пусть $g(z) \in \mathbb{C}[z]$, $\deg g(z) = n \geq 1$. Тогда корни многочлена $g(z)$ при достаточно малом изменении его коэффициентов меняются сколь угодно мало (при этом кратные корни могут распадаться в совокупность корней, количество которых совпадает с кратностью исходного корня).

Доказательство. Пусть $c \in \mathbb{C}$ — корень кратности k многочлена $g(z)$.

Выберем окружность $\Gamma = \Gamma(c, r)$ достаточно малого радиуса r такого, что внутри контура Γ нет корней многочлена $g(z)$, отличных от c . Пусть

$$M = \inf\{|g(z)|, z \in \Gamma\}.$$

Так как функция $|g(z)|: \Gamma \rightarrow \mathbb{R}$ непрерывна на компакте Γ и $|g(z)| \neq 0$ для всех $z \in \Gamma$, то $M > 0$.

На линейном пространстве $\mathbb{C}_n[z]$ многочленов $f(z) \in \mathbb{C}[z]$, $\deg f(z) \leq n$,

$$\mathbb{C}_n[z] = \{f(z) = a_n z^n + \dots + a_1 z + a_0 \mid a_i \in \mathbb{C}\} \cong \mathbb{C}^n,$$

рассматриваем топологию, в которой базис окрестностей для $f(z)$ состоит из совокупностей многочленов вида

$$V(a_n)z^n + \dots + V(a_1)z + V(a_0),$$

где $V(a_i)$ — окрестность для $a_i \in \mathbb{C}$, $i = 0, 1, \dots, n$.

Выберем коэффициенты многочлена $h(z) \in \mathbb{C}_n[z]$ настолько малыми, что

$$|h(z)| < M$$

для всех $z \in \Gamma$.

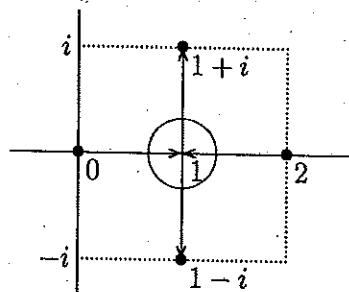
Применим к многочленам $f(z) = g(z) + h(z)$, $g(z) \in \mathbb{C}[z]$ теорему Руше на контуре Γ , поскольку

$$|f(z) - g(z)| = |h(z)| < |g(z)|$$

для всех $z \in \Gamma$. Следовательно, внутри контура $\Gamma = \Gamma(c, r)$ «деформированный» многочлен $f(z) = g(z) + h(z)$ имеет столько же корней (с учётом кратностей), сколько имел многочлен $g(z)$, то есть k корней. \square

 **Замечание 3.29.7.** Простой корень (то есть $k = 1$) при малом изменении коэффициентов многочлена $g(z)$ остаётся простым корнем многочлена $f(z) = g(z) + h(z)$.

 **Замечание 3.29.8.** Если $f(z) = z^2 - 2z + t \in \mathbb{C}[z]$, $t \in \mathbb{R}$, $0 \leq t \leq 2$, то корни имеют вид $z_{1,2} = 1 \pm \sqrt{1-t}$. При изменении t от 0 до 1 корни $z_1 = 0$ и $z_2 = 2$ (при $t = 0$) сближаются по вещественной оси $\mathbb{R} \subset \mathbb{C}$, превращаясь в корень $z_{1,2} = 1$ кратности 2 (при $t = 1$). При изменении t от 1 до 2 корень $z_{1,2}$ кратности 2 (при $t = 1$) расходится по прямой $\operatorname{Re} z = 1$ до корней $1+i$ и $1-i$ (при $t = 2$):



Таким образом, для многочлена

$$g(z) = z^2 - 2z + 1 = (z - 1)^2$$

и его корня $c = 1$ кратности 2 в любой его малой окрестности $\{z \in \mathbb{C} \mid |z - 1| < \varepsilon\}$, $0 < \varepsilon \in \mathbb{R}$, малое шевеление $f(z) = g(z) + \delta$, $0 < \delta = \delta(\varepsilon) \in \mathbb{R}$, многочлена гарантирует, что в окрестности $\{z \in \mathbb{C} \mid |z - 1| < \varepsilon\}$ многочлен $f(z)$ будет иметь также два корня (но уже различные).

3.30.

Если A , B и C — положительно определённые матрицы, то корни многочлена $|\lambda^2 A + \lambda B + C|$ имеют отрицательные вещественные части.

Задача 3.30.1.

- 1) Пусть $A = (a_{ij}) \in M_n(\mathbb{R})$, $a_{ij} \geq 0$ для всех i, j , $i \neq j$, и существуют такие положительные числа $\alpha_1, \dots, \alpha_n$, что

$$\sum_{j=1}^n \alpha_j a_{ij} < 0, \quad i = 1, \dots, n.$$

Тогда A — устойчивая матрица.

- 2) Пусть $A = (a_{ij}) \in M_n(\mathbb{C})$ и

$$\operatorname{Re}(a_{ii}) < -\sum_{\substack{j=1 \\ j \neq i}}^n |a_{ij}|, \quad i = 1, \dots, n.$$

Тогда A — устойчивая матрица.

Задача 3.30.2. Пусть $A \in M_n(\mathbb{C})$,

$$A = \begin{pmatrix} a_1 + b_1 & a_2 & 0 & 0 & \dots & \dots & \dots \\ -1 & b_2 & a_3 & 0 & \dots & \dots & \dots \\ 0 & -1 & b_3 & a_4 & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & -1 & b_{n-1} & a_n \\ \dots & \dots & \dots & \dots & 0 & -1 & b_n \end{pmatrix}$$

(все элементы вне главной диагонали и двух соседних с ней равны нулю), $a_j \in \mathbb{R}$, $b_k = 0$ или $b_k \in i \cdot \mathbb{R}$. Докажите, что число положительных членов в последовательности $a_1, a_1 a_2, \dots, a_1 a_2 \cdots a_n$ равно числу собственных значений матрицы A , имеющих положительные действительные части.

Замечание 3.30.3 (критерий устойчивости в терминах цепных дробей, теорема Уолла—Франка). Пусть

$$f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0 \in \mathbb{C}[z], \quad a_k = d_k + ib_k, \quad k = 0, 1, \dots, n-1,$$

$$g(z) = \alpha_{n-1}z^{n-1} + i\beta_{n-2}z^{n-2} + \alpha_{n-3}z^{n-3} + i\beta_{n-4}z^{n-4} + \dots$$

Тогда $f(z)$ является устойчивым многочленом в том и только в том случае, когда

$$\frac{g(z)}{f(z)} = \left[0; \frac{1}{1+c_1+d_1z}, \frac{1}{c_2+d_2z}, \dots, \frac{1}{c_n+d_nz} \right]$$

(обыкновенная конечная цепная дробь), где $\operatorname{Re}(c_j) = 0$ и $d_j > 0$, $j = 1, 2, \dots, n$.

Следствие 3.30.4. Пусть

$$\begin{aligned} f(x) &= x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{R}[x], \\ g(x) &= a_{n-1}x^{n-1} + a_{n-3}x^{n-3} + \dots \end{aligned}$$

Тогда $f(x)$ является устойчивым многочленом в том и только в том случае, когда

$$\frac{g(x)}{f(x)} = \left[0; \frac{1}{1+b_1x}, \frac{1}{b_2x}, \frac{1}{b_3x}, \dots, \frac{1}{b_nx} \right],$$

где $b_i > 0$, $i = 1, 2, \dots, n$.

Отметим, что обыкновенная цепная дробь, описанная в теореме и следствии, может быть получена с помощью алгоритма деления.

Упражнение 3.30.5. Используя следствие 3.30.4 и алгоритм деления, покажите, что многочлен

$$f(x) = x^4 + 5x^3 + 10x^2 + 10x + 4$$

является устойчивым.

Указание. $g(x) = 5x^3 + 10x$,

$$\frac{g(x)}{f(x)} = \frac{1}{\left(\frac{f(x)}{g(x)} \right)} = \frac{1}{1+h_1(x)},$$

где

$$h_1(x) = \frac{1}{5}x + \frac{8x^2 + 4}{5x^3 + 10x} = \left(\frac{1}{5}x \right) + \frac{1}{h_2(x)},$$

где

$$h_2(x) = \frac{5}{8}x + \frac{\frac{15}{2}x}{8x^2 + 4} = \left(\frac{5}{8}x \right) + \frac{1}{h_3(x)}, \quad h_3(x) = \frac{16}{15}x + \frac{1}{\frac{15}{8}x}.$$

$$\frac{g(x)}{f(x)} = \left[0; \frac{1}{1+\frac{1}{5}x}, \frac{1}{\frac{5}{8}x}, \frac{1}{\frac{16}{15}x}, \frac{1}{\frac{15}{8}x} \right].$$

Задача 3.30.6. При каких вещественных значениях параметра c многочлен

$$f(x) = x^4 + 5x^3 + 10x^2 + 10x + c$$

устойчив.

Ответ. $0 < c < 16$.

Замечание 3.30.7. Теорема Гаусса—Люка утверждает, что если выпуклое подмножество комплексной плоскости содержит все корни многочлена $f(z) \in \mathbb{Z}[z]$, то это подмножество содержит также все корни производной $f'(z)$.

Действительно, пусть

$$f(z) = c(z - z_1) \cdots (z - z_n),$$

где $c, z_i \in \mathbb{C}$, $1 \leq i \leq n$. Тогда

$$\frac{f'(z)}{f(z)} = \frac{1}{z - z_1} + \dots + \frac{1}{z - z_n}.$$

Если $w \in \mathbb{C}$, $f'(w) = 0$, $f(w)$ и w не принадлежат выпуклой оболочке точек z_1, \dots, z_n на комплексной плоскости, то через точку w можно провести прямую, не пересекающую выпуклую оболочку точек z_1, \dots, z_n . При этом векторы $w - z_1, \dots, w - z_n$ лежат в одной полуплоскости, определяемой указанной прямой. Поэтому векторы $\frac{1}{w - z_1}, \dots, \frac{1}{w - z_n}$ также лежат в одной полуплоскости, и следовательно,

$$\frac{f'(w)}{f(w)} = \frac{1}{w - z_1} + \dots + \frac{1}{w - z_n} \neq 0.$$

Полученное противоречие доказывает теорему Гаусса—Люка. \square

Задача 3.30.8. Пусть $n \geq 3$,

$$q_n(z) = \frac{(1+z)^n - 1 - z^n}{z} \in \mathbb{C}[z].$$

Для каких n все корни многочлена $q_n(z)$ лежат на единичной окружности.

Указание. Все корни многочленов

$$\begin{aligned} q_3(z) &= 3(1+z), & q_4(z) &= 4(2+3z+2z^2), \\ q_5(z) &= 5(1+z)(1+z+z^2), & q_7(z) &= 7(1+z)(1+z+z^2)^2 \end{aligned}$$

расположены на единичной окружности. Многочлен $q_6(z)$ может быть записан в виде $(a+bz+az^2)(c+dz+cz^2)$, где ad и bc — корни многочлена $t^2 - 15t + 48$. Отсюда вытекает, что все корни многочлена $q_6(z)$ лежат на единичной окружности.

Для $n \geq 8$ многочлен $q'_n(z)$ имеет корень, по модулю превосходящий 1. По теореме Гаусса—Люка это справедливо и для $q_n(z)$.

Задача 3.30.9. Пусть

$$f(z) = a_n z^n + \dots + a_1 z + a_0 \in \mathbb{R}[z], \quad a_0 > a_1 > \dots > a_n > 0.$$

Докажите, что единичный круг на комплексной плоскости $|z| \leq 1$ не содержит ни одного корня многочлена $f(z)$.

Указание. При $z = 1$

$$f(z) = a_n + \dots + a_0 > 0;$$

при $z \in \mathbb{R}$, $0 \leq z < 1$ имеем

$$|(a_0 - a_1)z + (a_1 - a_2)z^2 + \dots + (a_{n-1} - a_n)z^n + a_n z^{n+1}| < a_0 - a_1 + a_1 - a_2 + \dots + a_{n-1} - a_n + a_n = a_0,$$

и поэтому

$$|(1-z)f(z)| \geq a_0 - |(a_0 - a_1)z + \dots + a_n z^{n+1}| > 0;$$

при $|z| \geq 1$, $z \notin \{x \in \mathbb{R} \text{ mod } 0 \leq x \leq 1\}$ получаем

$$|(1-z)f(z)| \geq a_0 - |(a_0 - a_1)z + (a_1 - a_2)z^2 + \dots + (a_{n-1} - a_n)z^n + a_n z^{n+1}| > a_0 - (a_0 - a_1 + \dots + a_n) = 0$$

(числа $(a_0 - a_1)z, (a_1 - a_2)z^2, \dots, a_n z^{n+1}$ не могут одновременно иметь один аргумент: если φ — аргумент числа z и $\varphi = 2\varphi$ (аргумент числа z^2), то $\varphi = 2\pi k$, $k \in \mathbb{Z}$, и в нашем случае $z \in \mathbb{R}$, $0 \leq z \leq 1$).

Задача 3.30.10 (критерий Шура—Кона).

- 1) Оба корня $w = t_1, t_2$ действительного многочлена $t^2 + bt + c$ удовлетворяют условию $|w| < 1$ тогда и только тогда, когда $|b| < 1 + c < 2$.
- 2) Все три корня w действительного многочлена $t^3 + bt^2 + ct + d$ удовлетворяют условию $|w| < 1$ тогда и только тогда, когда $|bd - c| < 1 - d^2$, $|b + d| < |1 + c|$.

Упражнение 3.30.11 (обобщение теоремы Ролля). Пусть $f \in \mathbb{C}[x]$, $\deg f = n \geq 2$. Если $z_1, z_2 \in \mathbb{C}$, $z_1 \neq z_2$ и $f(z_1) = f(z_2)$, то диск

$$\left\{ z \in \mathbb{C} \mid \left| z - \frac{z_1 + z_2}{2} \right| \leq \left| \frac{z_1 - z_2}{2} \right| \cdot \operatorname{ctg} \frac{\pi}{n} \right\}$$

содержит по крайней мере один корень многочлена $f'(x)$.

Задача 3.30.12 (неравенство Ландау). Пусть

$$f(z) = a_n z^n + \dots + a_1 z + a_0 \in \mathbb{C}[z], \quad a_n \neq 0, \quad f(z) = a_n \prod_{i=1}^n (z - z_i),$$

$$\|f\|_2 = \sqrt{\sum_{i=0}^n |a_i|^2}, \quad M(f) = |a_n| \cdot \prod_{i=1}^n \max\{1, |z_i|\}.$$

Докажите, что $M(f) \leq \|f\|_2$.

Указание. Пусть z_1, \dots, z_k — корни многочлена $f(z)$, находящиеся вне единичного круга. Тогда

$$M(f) = |a_n| \cdot |z_1| \cdots |z_k|.$$

Положим

$$h(x) = a_n \cdot \prod_{j=1}^k (\bar{z}_j x - 1) \prod_{j=k+1}^n (x - z_j) = b_n x^n + \dots + b_0 \in \mathbb{C}[x].$$

Если $g \in \mathbb{C}[x]$ и $z \in \mathbb{C}$, то

$$\|(x+z)g(x)\|_2 = \|(\bar{z}x+1)g(x)\|_2.$$

Применяя k раз это соображение, получаем $\|f\|_2 = \|h\|_2$. Но $\|h\|_2 \geq |b_n| = M(f)$.

Задача 3.30.13. Пусть $f(z) \in \mathbb{C}[z]$, $\deg f = n$, f имеет не менее двух различных корней. Тогда многочлен $F = f \cdot f' \cdots f^{(n-1)}$ степени $\frac{n(n+1)}{2}$ имеет не менее $n+1$ различных корней.

Задача 3.30.14 (Коши, Кнут). Пусть $n \geq 1$,

$$f(z) = a_n z^n + \dots + a_0 \in \mathbb{C}[z], \quad a_n \neq 0, \quad f(x) = 0 \quad (x \in \mathbb{C}).$$

Тогда:

$$|x| \leq \max \left\{ \left| \frac{n \cdot a_{n-1}}{a_n} \right|, \left| \frac{n \cdot a_{n-2}}{a_n} \right|^{1/2}, \dots, \left| \frac{n \cdot a_0}{a_n} \right|^{1/n} \right\};$$

$$|x| \leq 2 \max \left\{ \left| \frac{a_{n-1}}{a_n} \right|, \left| \frac{a_{n-2}}{a_n} \right|^{1/2}, \dots, \left| \frac{a_0}{a_n} \right|^{1/n} \right\}.$$

Если $a_0 \neq 0$, то с помощью этих оценок легко получить границы минимального модуля корня многочлена $f(z)$ (заменив в исходном многочлене z на $\frac{1}{z}$ и находя границу R максимального модуля корня многочлена $a_0z^n + \dots + a_n$; $\frac{1}{R}$ будет искомой границей минимального модуля корня).

Задача 3.30.15 (Энестрём, Какея). Всё корни многочлена

$$f(z) = \sum_{j=0}^n a_j z^j \in \mathbb{R}[z]$$

с положительными коэффициентами принадлежат множеству

$$\left\{ z \in \mathbb{C} \mid \min_{1 \leq i \leq n} \left(\frac{a_{i-1}}{a_i} \right) \leq |z| \leq \max_{1 \leq i \leq n} \left(\frac{a_{i-1}}{a_i} \right) \right\}.$$

Замечание 3.30.16. Пусть $f \in \mathbb{C}[t]$. Через $n_0(f)$ обозначим количество различных корней многочлена f .

Теорема Мейсона—Стоттерса. Пусть $f, g, h \in \mathbb{C}[t]$ — не равные константе взаимно простые многочлены, $f + g = h$. Тогда

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq n_0(fgh) - 1.$$

С использованием теоремы Мейсона—Стоттерса покажите, что если $n \in \mathbb{N}$, $n \geq 3$, то не существует решений уравнения

$$(x(t))^n + (y(t))^n = (z(t))^n$$

с не равными константе взаимно простыми многочленами $x(t), y(t), z(t) \in \mathbb{C}[t]$.

Гипотеза Смейла (1981 г.). Пусть $f(z) \in \mathbb{C}[z]$ — такой многочлен степени n , что $f(0) = 0$, $f'(0) \neq 0$. Тогда

$$\min \left\{ \left| \frac{f(z)}{zf'(0)} \right| \mid f'(z) = 0 \right\} \leq M,$$

где $M = 1$ или, возможно, $M = \frac{n-1}{n}$.

Смайл доказал гипотезу для $n = 4$. Рассматривая $f(z) = a_1 z + a_n z^n$, легко убедиться, что M не может быть меньше, чем $\frac{n-1}{n}$.

Задача 3.30.17. Пусть

$$f(z) = z^n + b_{n-1} z^{n-1} + \dots + b_1 z + b_0 \in \mathbb{C}[z].$$

Покажите, что

$$\max_{|z|=1} \{|f(z)|\} \geq 1$$

(равенство достигается лишь для $f(z) = z^n$).

Задача 3.30.18.

- ✓ 1) *Неравенство Маркова.* Пусть $\deg f \leq n$, $|f(x)| \leq M$ при $-1 \leq x \leq 1$. Тогда $|f'(x)| \leq M \cdot n^2$ при $-1 \leq x \leq 1$.
- ✓ 2) *Неравенство Бернштейна.* Пусть $f(z) \in \mathbb{C}[z]$, $\deg f \leq n$ и $|f(z)| \leq M$ при $|z| = 1$. Тогда $|f'(z)| \leq M \cdot n$ при $|z| = 1$.

Гипотеза Сендана. Пусть

$$f(z) = \prod_{i=1}^n (z - z_i), \quad n \geq 2,$$

все корни лежат в замкнутом единичном диске. Тогда каждый из замкнутых дисков $\bar{D}(z_1, 1), \dots, \bar{D}(z_n, 1)$ содержит корень производной $f'(z)$.