

Теория групп, 3 семестр

ИВАЩЕНКО ДМИТРИЙ

DISCLAIMER: THESE PAGES COME WITH ABSOLUTELY NO WARRANTY, USE AT YOUR OWN RISK ;) THIS WORK IS LICENSED BY WTFPL, YOU CAN REDISRIIBUTE IT AND/OR MODIFY IT UNDER THE TERM OF DO WHAT THE FUCK YOU WANT TO PUBLIC LICENSE, VERSION 2
Багрепорты, комментарии, предложения и прочее приветствуются посредством vk.com/skird, а также e-mail

Благодарность. Спасибо Павлу Ахтямову за лекции 8, 10, 11.

Последние изменения: 6 января 2015 г. 22:42

СОДЕРЖАНИЕ

Лекция 1. Понятие группы и подгруппы	4
1. Группы, примеры групп	4
2. Подгруппы	5
3. Изоморфизмы групп	5
4. Подгруппы, порожденные подмножествами	5
Лекция 2. Циклические группы, группа перестановок	6
5. Циклические группы. Порядок элемента группы	6
6. Группа перестановок	7
Лекция 3. Смежные классы	8
7. Левый и правый смежные классы	8
8. Индекс подгруппы и теорема Лагранжа	9
9. Нормальные подгруппы	10
10. Сопряженные элементы	10
Лекция 4. Гомоморфизмы групп	11
11. Основные свойства гомоморфизмов	11
12. Факторгруппа	12
Лекция 5. Действие группы на множестве	15
13. Определение действия группы	15
14. Ядро, орбита, стабилизатор	16
15. Примеры действий групп	17

Лекция 6. Автоморфизмы группы, p-группы и лемма Бернсайда	18
16. Действие группы на себя сопряжениями	18
17. Группа автоморфизмов	19
18. Действие группы на свои подгруппы сопряжениями	19
19. p -группы	20
20. Лемма Бернсайда	20
Лекция 7. Произведения групп	21
21. k -транзитивные действия и обобщения леммы Бернсайда	21
22. Прямое произведение групп	22
23. Полупрямое произведение групп	23
Лекция 8. Разрешимые группы	24
24. Коммутант группы	24
25. Характеризация коммутанта	25
26. Разрешимые группы	26
Лекция 9. Простые группы	26
27. Критерий разрешимости	26
28. Простые группы	27
Лекция 10. Свободные группы и образующие соотношения	29
29. Построение свободных групп	29
30. Образующие соотношения	30
31. Примеры задания групп образующими соотношениями	31
Лекция 11. Теоремы Силова	31
32. Теоремы Силова	31
33. Строение силовских p -подгрупп	33
Лекция 12. Конечнопорожденные абелевы группы	34
34. Конечнопорожденные абелевы группы и их базисы	34
35. Группы без кручения	35
36. Строение конечнопорожденных абелевых групп	36
Лекция 13. Классификация конечнопорожденных абелевых групп	38
37. Представление примарными циклическими группами	38
38. Представление непериодической части	38

Лекция 1. Понятие группы и подгруппы

1. ГРУППЫ, ПРИМЕРЫ ГРУПП

Определение. *Группа* - множество G с определенной на нем бинарной операцией. $\forall a, b$ определено $a \cdot b \in G$ или, опуская знак умножения $ab \in G$. Групповая операция задается следующими свойствами:

- 1) ассоциативность: $\forall a, b, c \in G \rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- 2) существование нейтрального элемента: $\exists e \in G : \forall a \in G \rightarrow a \cdot e = e \cdot a = a$
- 3) существование обратного элемента: $\forall a \in G \exists a^{-1} \in G : a \cdot a^{-1} = a^{-1} \cdot a = e$

Группа называется *абелевой*, если групповая операция коммутативна ($\forall a, b \in G \rightarrow a \cdot b = b \cdot a$)

Мы будем использовать записи (G, \cdot) , $(G, +)$ и подобные в случае, если неочевидно, какая операция используется в группе.

Замечание. Произведение $g_1 \cdot \dots \cdot g_n$ не зависит от расстановки скобок, поэтому такую запись мы считаем корректной

Утверждение. $\forall g \in G \exists! g^{-1} \in G : g \cdot g^{-1} = g^{-1} \cdot g = e$.

Доказательство. Пусть a — левый обратный к g элемент: $a \cdot g = e$, а b — правый обратный: $g \cdot b = e$.

Тогда рассмотрим $a \cdot g \cdot b = (a \cdot g) \cdot b = e \cdot b = b$, но $a \cdot g \cdot b = a \cdot (g \cdot b) = a \cdot e = a$. Значит $a = b$, тогда обратный элемент единственен. \square

Упражнение. Показать, что если вместо существования обратного требовать только существование правого обратного, то полученная структура тоже будет группой.

Пример.

- 1) $(\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$.
- 2) $(\mathbb{R}, +)$ и для $\forall F$ — поля $(F, +)$ (по определению).
- 3) $(\mathbb{R} \setminus \{0\}, \times)$ и для $\forall F$ — поля $(F \setminus \{0\}, \times)$ (по определению).

Более общо, если R — кольцо, то $(R, +)$ и (R^*, \times) — абелевы группы. R^* — множество элементов, обратимых в R .

Нужно заметить, что если $a, b \in R^*$, то $\exists a^{-1}, b^{-1} \in R^*$, а значит $a \cdot b \in R^*$, так как $b^{-1} \cdot a^{-1}$ — обратный к $a \cdot b$.

- 4) $M_{n \times n}(F)$ — кольцо, $(M_{n \times n}(F))^*$ — группа $GL_n(F)$, чаще всего не абелева.
- 5) \mathbb{Z}_n — кольцо, тогда по операции умножения $(\mathbb{Z}_n)^*$ — группа из элементов, взаимно простых с n . (Ясно, что если $\gcd(a, n) > 1$, то обратного нет, в противном случае $\exists u, v : a \cdot u + n \cdot v = 1 \Rightarrow a \cdot u \equiv 1 \pmod{n}$ и u будет обратным к a). Отсюда легко видеть, что $|\mathbb{Z}_n^*| = \varphi(n)$.
- 6) S_n — группа перестановок, то есть биекций множества $[n] = \{1, \dots, n\}$ на себя с операцией композиции. Если нужно рассмотреть Ω — произвольное множество, то введем $S(\Omega)$ — множество биекций $\Omega \mapsto \Omega$ с операцией композиции. Ясно, что это тоже группа.

2. ПОДГРУППЫ

Определение. Подмножество $H \subset G$ есть подгруппа группы G , если оно замкнуто относительно групповой операции и для него выполняются утверждения (1) — (3) из определения группы. При этом пишут, что $H < G$.

Пример.

0) $\{e\} < G$, $G < G$ — несобственные подгруппы.

1) $GL_n(F) > D_n(F^*)$ — группа диагональных матриц.

2) $GL_n(F) > SL_n(F) = \{A \in GL_n(F), \det A = 1\}$.

3) $GL_n(F) > T_n(F)$ — группа верхнетреугольных матриц без нулей на диагонали.

Упражнение. Проверить, что $T_n(F)$ — группа.

4) $GL_n(\mathbb{R}) > O_n$ — группа ортогональных матриц.

5) $O_2 > D_n = \{f \in O_n : f(P_n) = P_n\}$, где P_n — правильный многоугольник. Легко видеть, что в D_n входят n поворотов и n осевых симметрий.

Упражнение. Проверить, что $|D_n| = 2 \cdot n$

3. ИЗОМОРФИЗМЫ ГРУПП

Определение. Пусть G, H — группы и $\exists \varphi : G \mapsto H$ — изоморфизм, если

1) φ — биекция.

2) $\forall a, b \in G \rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

3) $\forall a \in G \rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$.

Если $\exists \varphi$ — изоморфизм между G и H , то G называется изоморфной H и пишут $G \cong H$.

Пример.

1) $D_3 \cong S_3$.

2) $\mathbb{C}^* > \mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\}$, $\mathbb{C}_n \cong \mathbb{Z}_n$.

4. ПОДГРУППЫ, ПОРОЖДЕННЫЕ ПОДМНОЖЕСТВАМИ

Определение. G — группа, $M \subset G$ — подмножество. Подгруппой, порожденной подмножеством M , называется пересечение всех подгрупп G , содержащих M

$$(M) = \bigcap_{\substack{H \leq G \\ M \subset H}} H$$

Утверждение.

1) Пересечение любого количества подгрупп — подгруппа.

2) $(M) = \{e\} \cup \{a_1 \cdot \dots \cdot a_k : \forall i = 1, \dots, k \rightarrow a_i \in M \vee a_i^{-1} \in M\}$

Доказательство. Пусть $K = \bigcap_{H_i \leq G} H_i$. Если $a, b \in K$, то

$$a, b \in H_i \Rightarrow a \cdot b \in H_i \Rightarrow a \cdot b \in H_i, \quad a^{-1} \in H_i \Rightarrow a \cdot b \in K, \quad a^{-1} \in K$$

Кроме того, в любой подгруппе есть e , значит он есть и в K , то есть K не пусто.

Обозначим теперь за N множество из пункта (2). Ясно, что $N \subset (M)$: если $a_1 \cdot \dots \cdot a_k \in N$, то $a_i \in (M) \Rightarrow a_1 \cdot \dots \cdot a_k \in (M)$.

Докажем, что $(M) \subset N$. Это так, потому что (M) является подгруппой, содержащей M . Нужно только проверить, что N — это подгруппа.

Если $m \in M$, то $m \in N$. Если $a_1, \dots, a_k, b_1, \dots, b_l \in N$, то $(a_1 \cdot \dots \cdot a_k)(b_1 \cdot \dots \cdot b_l) \in N$, то есть N — замкнута. $e \in N$ — нейтральный, ассоциативность очевидна, $(a_1 \cdot \dots \cdot a_k)^{-1} = a_k^{-1} \cdot \dots \cdot a_1^{-1}$. \square

Пример. $r \in D_n$ — поворот на $\frac{2\pi}{n}$. Тогда $\langle r \rangle \cong \mathbb{Z}_n$.

Определение. Если $M \subset G$ таково, что $\langle M \rangle = G$, то G порождена M , а M — порождающее множество.

Пример. $\mathbb{Z}_n = \langle 1 \rangle$, $\mathbb{Z} = \langle 1 \rangle$, $GL_n(F) = \langle \{\text{элементарные матрицы}\} \rangle$

Лекция 2. Циклические группы, группа перестановок

5. ЦИКЛИЧЕСКИЕ ГРУППЫ. ПОРЯДОК ЭЛЕМЕНТА ГРУППЫ

Определение. Циклической назовем группу, порожденную одним элементом.

Теорема. Если G — циклическая группа, то либо $G \cong \mathbb{Z}$, либо $G \cong \mathbb{Z}_n$ при $n \in \mathbb{N}$.

Доказательство. Пусть $G = \langle g \rangle$, $g \in G$. Рассмотрим все степени g : $\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots$. Есть два случая.

1) Все степени g различны. Тогда проведем изоморфизм $\varphi: \mathbb{Z} \rightarrow G$, $\varphi(k) = g^k$. Это биекция, так как все элементы различны. Кроме того, $\varphi(k+l) = g^{k+l} = g^k \cdot g^l = \varphi(k) \cdot \varphi(l)$, $\varphi(-k) = \varphi(k)^{-1}$, то есть $G \cong \mathbb{Z}$.

2) $\exists k \neq l: g^k = g^l \Rightarrow g^{k-l} = g^{k-l} = g^k \cdot (g^l)^{-1} = e = g^{l-k}$. И так $\exists n \in \mathbb{N}: g^n = e$. Будем считать, что n взято наименьшим из возможных. Тогда

а) g^0, \dots, g^{n-1} попарно различны, так как если $g^k = g^l$ для $0 \leq l, k < n$, то $g^{k-l} = g^{l-k} = e$, что невозможно по минимальности n

б) $G = \{g^0, \dots, g^{n-1}\}$. $\forall k \in \mathbb{Z}$, $k = q \cdot n + r$, где $q, r \in \mathbb{Z}$, $0 \leq r < n$. Тогда $g^k = g^{qn+r} = (g^n)^q \cdot g^r = g^r$.

Наконец, пусть $\varphi: \mathbb{Z}_n \rightarrow G$, $\varphi(k) = g^k$. Тогда φ — биекция, так как пункты а) и б) доказывают инъективность и сюръективность. Также $\varphi(k+l)$ это или g^{k+l} или $g^{k+l-n} = g^{k+l} = g^k \cdot g^l = \varphi(k) \cdot \varphi(l)$. Аналогично $\varphi(-k) = g^{-k} = g^{n-k} = (g^k)^{-1} = \varphi(k)^{-1}$. Значит $\mathbb{Z}_n \cong G$. \square

Определение. Пусть G — группа, $g \in G$. Порядок элемента $\text{ord } g = \min n \in \mathbb{N}: g^n = e$. Если такого n нет, то порядок будем считать бесконечным.

Утверждение. $\text{ord } g = |\langle g \rangle|$

Замечание. Если $\langle g \rangle \cong \mathbb{Z}$, то $\text{ord } g = \infty$. Иначе $\langle g \rangle \cong \mathbb{Z}_n$ и $\text{ord } g = n$ по предыдущему доказательству.

Теорема. Подгруппа циклической группы также циклическая.

Доказательство. Можно считать, что $G = \mathbb{Z}$ или $G = \mathbb{Z}_n$.

1) $G = \mathbb{Z}$. Пусть $H \leq G$. Если $H = (0)$, то все очевидно. Иначе $\exists h \in H$, $h \neq 0$. Выберем h с наименьшим $|h|$. Тогда $H \geq (h) = h \cdot \mathbb{Z}$. Пусть $H \neq (h)$, тогда $\exists g \in H \setminus (h)$. Тогда $g = q \cdot h + r$, $q, r \in \mathbb{Z}$, $0 \leq r < |h|$. Тогда $r = (g - q \cdot h) \in H$, а это противоречит выбору h , если $r \neq 0$. Тогда $r = 0$ и $g \in (h)$. Итак, $(h) = H$.

2) $G = \mathbb{Z}_n$. Проходит тоже самое рассуждение, если мы считаем g и h целыми числами. При этом $h \mid n$. Если $n = q \cdot h + r$, то $r = n - q \cdot h = -q \cdot h \in H$. Если $r \neq 0$, то противоречие с выбором h .

Итак, в обоих случаях $H = (h)$, при этом во втором случае если $h \neq 0$, то $h \mid n$. \square

Замечание. В двухпорожденной группе могут быть подгруппы, порожденные любым количеством элементов.

6. ГРУППА ПЕРЕСТАНОВОК

Замечание. Знак перестановки есть $(-1)^\sigma = \text{sgn } \sigma = (-1)^{N(\sigma)}$. И $(-1)^{\sigma_1} \cdot (-1)^{\sigma_2} = (-1)^{\sigma_1 \cdot \sigma_2}$. Значит $A_n = \{\sigma \in S_n : (-1)^\sigma = 1\} \leq S_n$ — подгруппа, которая носит название *знакопеременной группы*.

Теорема. (Кэли) Если G — произвольная конечная группа, $|G| = n$, то G изоморфна подгруппе в S_n .

Доказательство. $S_n \cong S(G)$ — группа биекций из G в G . Пусть $h \in G$, тогда определим биекцию $\varphi_h : G \rightarrow G$, $\varphi_h(g) = h \cdot g$.

Таким образом $\varphi_h \in S(G)$. Пусть $h_1, h_2 \in G$. $\varphi_{h_1 \cdot h_2}(g) = h_1 \cdot h_2 \cdot g = \varphi_{h_1}(\varphi_{h_2}(g)) = \varphi_{h_1} \circ \varphi_{h_2}(g)$. Кроме того, $\varphi_e(g) = g$.

$H = \{\varphi_h \mid h \in G\}$ — подгруппа в $S(G)$, так как

$$\varphi_{h_1} \circ \varphi_{h_2} = \varphi_{h_1 \cdot h_2} \in H, \quad \varphi_h \circ \varphi_{h^{-1}} = \varphi_e = \text{id} = \varphi_{h^{-1}} \circ \varphi_h \Rightarrow (\varphi_h)^{-1} = \varphi_{h^{-1}} \in H$$

Наконец, $G \cong H$. $\psi : G \rightarrow H$, $\psi(h) = \varphi_h$ — изоморфизм, так как сохраняет операцию $\psi(h_1 \cdot h_2) = \psi(h_1) \circ \psi(h_2)$. ψ — биекция: если $h_1 \neq h_2$, то $\varphi_{h_1}(e) = h_1 \neq h_2 = \varphi_{h_2}(e)$.

Итак, теорема доказана. \square

Замечание. Пусть $\sigma \in S_n$. Стандартная запись: $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$. Далее мы введем другую, более удобную форму записи.

Определение. Пусть $a_1, \dots, a_k \in [n]$ — различные элементы. Циклом (a_1, \dots, a_k) называется перестановка $\sigma \in S_n$, такая что

$$\sigma(a_1) = a_2, \dots, \sigma(a_{k-1}) = \sigma(a_k), \sigma(a_k) = \sigma(a_1), \quad \sigma(x) = x, \quad x \notin \{a_1, \dots, a_k\}$$

Число k называется *длиной цикла*. Цикл длины 2 называется *транспозицией*. Семейство циклов называется *независимым*, если $\forall a \in [n]$ является элементом не более одного цикла из семейства.

Утверждение.

1) Любая перестановка $\sigma \in S_n$ раскладывается в произведение некоторого неотрицательного количества независимых циклов

2) Если σ_1, σ_2 — независимые циклы, то $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$

Доказательство.

1) Нарисуем оргграф с $V = [n]$, $E = \{(k; \sigma(k)) \mid k \in [n]\}$. Исходящая степень вершины k всегда 1, так же как и входящая. Это значит, что граф разбивается в несвязное объединение ориентированных циклов. Эти циклы в графе соответствуют независимым циклам в группе S_n .

2) Если σ_1, σ_2 — независимые циклы, то для некоторого фиксированного k без потери общности $\sigma_1(k) = k$. Тогда $\sigma_2 \circ \sigma_1(k) = \sigma_2(k)$, $\sigma_1 \circ \sigma_2(k) = \sigma_2(k)$. То есть в каждом элементе $\sigma_1 \circ \sigma_2$ и $\sigma_2 \circ \sigma_1$ совпадают. \square

Замечание. Если $\sigma_1, \dots, \sigma_t$ — независимые циклы, то $(\sigma_1 \circ \dots \circ \sigma_t)^k = \sigma_1^k \circ \dots \circ \sigma_t^k$.

Утверждение. Если σ — произведение независимых циклов длин l_1, \dots, l_t , то $\text{ord } \sigma = \text{LCM}(l_1, \dots, l_t)$.

Доказательство. $\text{ord}(a_1, \dots, a_k) = k$ по очевидным соображениям.

Ясно, что если $\sigma = \tau_1 \circ \dots \circ \tau_t$, то $\sigma^N = \tau_1^N \circ \dots \circ \tau_t^N$. Если $N = \text{LCM}(l_1, \dots, l_t)$, то $\sigma_i^N = \text{id} \Rightarrow \sigma^N = \text{id}$.

Если теперь $N < \text{LCM}(l_1, \dots, l_n)$, то $\exists i : N$ не кратно l_i . Тогда $\sigma_i^N \neq \text{id}$. Тогда $\exists \sigma_i^N(x) \neq x$, для остальных $i \neq j \rightarrow \sigma_j(x) = x$, тогда $\sigma^N(x) \neq x \Rightarrow \sigma^N \neq \text{id}$.

Итак, $\text{ord } \sigma = \text{LCM}(l_1, \dots, l_t)$. \square

Утверждение. Группа S_n порождается всеми транспозициями.

Доказательство. Индукция по n . База $n = 1$ тривиальна. Положим, все перестановки размера $\leq n - 1$ можно разложить в произведение транспозиций.

Пусть $\sigma \in S_n$; и $i = \sigma(n)$. Положим $\sigma' = (i, n) \circ \sigma$. Тогда $\sigma'(n) = (i, n)(i) = n$, то есть σ' по сути есть перестановка размера $n - 1$. Тогда по предположению индукции σ' раскладывается в произведение нескольких транспозиций, а тогда $\sigma = (i, n) \circ \sigma'$. \square

Упражнение.

а) $S_n = ((1, 2), \dots, (n - 1, n))$

б) $S_n = ((1, 2), (1, 2, \dots, n))$

Упражнение. Придумать группу, не порождающуюся двумя элементами.

Лекция 3. Смежные классы

7. ЛЕВЫЙ И ПРАВЫЙ СМЕЖНЫЕ КЛАССЫ

Замечание. Пусть $A, B \subset G$. Тогда $AB = \{ab : a \in A, b \in B\}$. если при этом $A = \{a\}$, то будем писать просто aB , $|aB| = |B|$.

Определение. Пусть G — группа, $H \leq G$, $g \in G$, тогда *левым смежным классом* g по подгруппе H будем называть множество gH . *Правым смежным классом* будет называть Hg .

Замечание. Если $g \in H$, то $gH = H$

Пример. Пусть $G = \mathbb{Z}$, $H = n\mathbb{Z}$. Тогда для $g \in G$ имеем $g + n\mathbb{Z}$ — все числа, сравнимые с g по модулю n .

Теорема. Пусть $H \leq G$, $g_1, g_2 \in G$. Тогда следующие условия равносильны:

- (1) $g_1H = g_2H$
- (2) $g_1H \cap g_2H \neq \emptyset$
- (3) $g_1^{-1} \cdot g_2 \in H$

Доказательство.

(1) \Rightarrow (2). $H \neq \emptyset$, $g_1H = g_2H \Rightarrow g_1H \cap g_2H \neq \emptyset$

(2) \Rightarrow (3). $x = g_1h_1 = g_2h_2$, $h_1, h_2 \in H$. Но тогда $g_1^{-1} \cdot g_2 = h_1 \cdot h_2^{-1} \in H$

(3) \Rightarrow (1). Если $g_1^{-1} \cdot g_2 \in H \Rightarrow g_2^{-1} \cdot g_1 \in H$. Далее, $g_2H = g_1 \cdot (g_1^{-1} \cdot g_2) H = g_1 \cdot ((g_1^{-1} \cdot g_2) H)$. Так как $g_1^{-1} \cdot g_2 \in H$, то $(g_1^{-1} \cdot g_2) H = H$, а значит $g_2H = g_1H$. \square

Замечание. Если мы определим отношение $g_1 \sim g_2 \Leftrightarrow g_1^{-1} \cdot g_2 \in H$, то это будем отношением эквивалентности, так как это утверждение равносильно утверждению $g_1H = g_2H$.

Класс эквивалентности g — это $\{g' \mid g^{-1} \cdot g' \in H\} = \{g' \mid g' \in gH\} = gH$.

Замечание. То же верно и для правых смежных классов, то есть $Hg_1 = Hg_2 \Leftrightarrow Hg_1 \cap Hg_2 \neq \emptyset \Leftrightarrow g_1 \cdot g_2^{-1} \in H$.

Замечание. Множество левых смежных классов элементов группы G по подгруппе H обозначается G/H ; множество правых смежных классов — $H \backslash G$.

Утверждение. $|G/H| = |H \backslash G|$

Доказательство. Сопоставим классу $gH \in G/H$ сопоставим правый смежный класс Hg^{-1} . Этот класс определен однозначно, ибо $Hg^{-1} = (gH)^{-1} = \{x^{-1} \mid x \in gH\}$. Обратное отображение строится также, значит это биекция и $|G/H| = |H \backslash G|$. \square

Замечание. Если $g_1H = g_2H$, то необязательно $Hg_1 = Hg_2$.

8. ИНДЕКС ПОДГРУППЫ И ТЕОРЕМА ЛАГРАНЖА

Определение. Индекс подгруппы H в группе G — это $|G/H| = |H \backslash G|$. Индекс часто обозначается $|G : H|$.

Теорема. (Лагранжа). Пусть G — конечная группа, $H \leq G$. Тогда $|G| = |H| \cdot |G : H|$.

Доказательство. Группа G разбивается на левые смежные классы по H . Этих классов ровно $|G : H|$ и каждый имеет вид gH и мощность $|H|$. Отсюда получаем утверждение теоремы. \square

Замечание. $|H| \mid |G|$ в условиях теоремы Лагранжа.

Замечание. Если $g \in G$, $|G| < \infty$, то $\text{ord } g \mid |G|$.

Утверждение. (малая теорема Ферма). Если $a \in \mathbb{Z}_p^*$, p — простое, то $a^{p-1} \equiv 1 \pmod{p}$

Доказательство. $\text{ord } a \mid |\mathbb{Z}_p^*| \Rightarrow \text{ord } a \mid (p-1) \Rightarrow a^{p-1} = (a^{\text{ord } a})^{\frac{p-1}{\text{ord } a}} = 1$. \square

Утверждение. (теорема Эйлера). Если $(a, n) = 1$, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Доказательство. $\text{ord } a \mid |\mathbb{Z}_n^*|$, $|\mathbb{Z}_n^*| = \varphi(n) \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$. \square

9. НОРМАЛЬНЫЕ ПОДГРУППЫ

Определение. Пусть $H \leq G$. Эта подгруппа называется нормальной (обозначается $H \triangleleft G$), если $\forall g \in G \rightarrow gH = Hg$.

Замечание. Необязательно, чтобы $\forall h \in H \rightarrow gh = hg$.

Замечание. $gH = Hg \Leftrightarrow H = gHg^{-1}$.

Пример. Если G — абелева, то любая ее подгруппа нормальна.

Пример. $A_n \triangleleft S_n$. Если $\sigma \in A_n$ и $\tau \in S_n$, то $\text{sgn}(\tau \cdot \sigma \cdot \tau^{-1}) = \text{sgn}(\tau) \cdot \text{sgn}(\tau^{-1}) \cdot \text{sgn}(\sigma) = \text{sgn}(\sigma)$. Значит $\tau^{-1}A_n\tau \subset A_n$. Аналогично $\tau^{-1}A\tau \subset A_n \Rightarrow A_n \subset \tau A_n \tau^{-1}$. Итак, $\tau A_n \tau^{-1} = A_n$, и подгруппа A_n — нормальна.

Пример. Пусть $G = S_3$, $H = ((1, 2))$. Тогда $(1, 2) \in H$, $(1, 3)(1, 2)(1, 3)^{-1} = (1, 3)(1, 2)(1, 3) = (2, 3) \notin H$. Значит, $H \not\triangleleft G$. $(1, 3)H(1, 3)^{-1} \neq H \Leftrightarrow (1, 3)H \neq H(1, 3)$.

Утверждение. Пусть $H_i \triangleleft G$, $\forall i \in I$. Тогда $\bigcap_{i \in I} H_i \triangleleft G$.

Доказательство. Мы знаем, что $H = \bigcap_{i \in I} H_i \leq G$. Если $h \in H$, $g \in G$, то $\forall i \rightarrow h \in H_i$, $\forall i \rightarrow ghg^{-1} \in H_i \Rightarrow ghg^{-1} \in H$. Итак, $gHg^{-1} \leq H$, а значит $gHg^{-1} = H$. \square

Утверждение. Пусть $H \triangleleft G$, $K \leq G$. Тогда $HK \leq G$. При этом, если $K \triangleleft G$, то и $HK \triangleleft G$.

Доказательство. Заметим, что $HK = \bigcap_{k \in K} Hk = \bigcup_{k \in K} Hk = KH$.

Тогда $(HK) \cdot (HK) = H(KH)K = HH \cdot KK = HK$. Итак, HK замкнута относительно умножения.

Также, $(HK)^{-1} = (K^{-1}H^{-1}) = KH = HK$. Значит, она замкнута относительно взятия обратного.

Наконец, если $K \triangleleft G$, то $\forall g \in G \rightarrow gH = Hg$, $gK = Kg$. Тогда $gHK = HgK = HKg \Rightarrow HK \triangleleft G$. \square

Замечание. Если $H \leq G$, $K \leq G$, но не нормальны, то HK не обязательно подгруппа.

Пример. Если $G = S_3$, $H = ((1, 2))$, $K = ((1, 3))$, то $|HK| = 4$. Значит, $|HK|$ не может быть подгруппой G по теореме Лагранжа.

10. СОПРЯЖЕННЫЕ ЭЛЕМЕНТЫ

Определение. Пусть $g, h \in G$. Тогда элемент $g^{-1} \cdot h \cdot g$ называется сопряженным к h при помощи g и обозначается h^g .

Утверждение.

$$(1) (g_1 \cdot g_2)^h = g_1^h \cdot g_2^h$$

$$(2) g^{h_1 \cdot h_2} = (g^{h_1})^{h_2}$$

Доказательство.

$$(1) g_1^h \cdot g_2^h = h^{-1} \cdot g_1 \cdot h \cdot h^{-1} \cdot g_2 \cdot h = h^{-1} \cdot (g_1 \cdot g_2) \cdot h = (g_1 g_2)^h$$

$$(2) g^{h_1 h_2} = (h_1 h_2)^{-1} g (h_1 h_2) = h_2^{-1} (h_1^{-1} g h_1) h_2 = (g^{h_1})^{h_2} \quad \square$$

Определение. Элементы g_1, g_2 называются сопряженными, если $\exists h \in G : g_1^h = g_2$

Утверждение. Отношение сопряженности есть отношение эквивалентности.

Доказательство. $g^e = g$; $g_1^h = g_2 \Rightarrow g_2^{h^{-1}} = (g_1^h)^{h^{-1}} = g_1^e = g_1$; $g_1^{h_1} = g_2$, $g_2^{h_2} = g_3 \Rightarrow g_3 = (g_1^{h_1})^{h_2} = g_1^{h_1 h_2}$ \square

Определение. Класс элемента g относительно этого отношения называется *классом сопряженности* элемента g и обозначается g^G .

Утверждение. Пусть $H \leq G$. Тогда $H \triangleleft G \Leftrightarrow H$ — объединение нескольких классов сопряженности.

Доказательство.

$$H \triangleleft G \Leftrightarrow \forall h \in H, g \in G \rightarrow h^g \in H \Leftrightarrow \forall h \in H \rightarrow h^G \subset H \Rightarrow H = \bigcup_{h \in H} h^G$$

Наоборот, если $H = \bigcup_{i \in I} h_i^G$, то

$$\forall h \in H \exists i \in I : h \in h_i^G \Rightarrow h^G = h_i^G \subset H$$

\square

Лекция 4. Гомоморфизмы групп

11. ОСНОВНЫЕ СВОЙСТВА ГОМОМОРФИЗМОВ

Определение. Пусть $(G, \cdot), (H, \times)$ — группы. Отображение $\varphi : G \mapsto H$ называется *гомоморфизмом*, если

$$\forall g_1, g_2 \in G \rightarrow \varphi(g_1 \cdot g_2) = \varphi(g_1) \times \varphi(g_2)$$

Гомоморфизм называется *эпиморфизмом*, если он сюръективен.

Гомоморфизм называется *мономорфизмом* (вложением), если он инъективен.

Определение. Образ гомоморфизма $Im \varphi = \varphi(G) = \{\varphi(g) : g \in G\}$.

Определение. Ядро гомоморфизма $\ker \varphi = \varphi^{-1}(e_H) = \{g \in G : \varphi(g) = e\}$.

Пример.

(1) $\forall G, H \varphi : G \mapsto H, \varphi(g) = e$. Тогда $Im \varphi = \{e\}$, $\ker \varphi = G$.

(2) $\varphi : \mathbb{Z} \mapsto \mathbb{Z}_n, \varphi(k) = k \bmod n$. Тогда $Im \varphi = \mathbb{Z}_n$, $\ker \varphi = n\mathbb{Z}$.

(3) $\varphi : GL_n(F) \mapsto F^*, \varphi(A) = \det A$. Тогда $Im \varphi = F^*$, $\ker \varphi = SL_n(F)$.

(4) Пусть G — группа, $a \in G$.

$$\varphi : G \mapsto G, \varphi(g) = g^a = a^{-1} \cdot g \cdot a$$

Тогда $(g_1 \cdot g_2)^a = g_1^a \cdot g_2^a$, а также есть обратное отображение $\varphi^{-1}(h) = a \cdot h \cdot a^{-1} \Rightarrow \varphi$ — биекция на себя. Такие гомоморфизмы называются *автоморфизмами*.

Утверждение. Пусть $\varphi : G \mapsto H$ — гомоморфизм, тогда

(1) $\varphi(e) = e$

(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$

Доказательство.

- (1) $\varphi(e) = \varphi(e^2) = \varphi(e) \cdot \varphi(e) \Rightarrow e_H = \varphi(e_G)$
 (2) $\varphi(g) \cdot \varphi(g^{-1}) = \varphi(g \cdot g^{-1}) = \varphi(e) = e$. Аналогично, $\varphi(g^{-1}) \cdot \varphi(g) = e$. Итак, $\varphi(g^{-1})$ и есть $\varphi(g)^{-1}$ \square

Утверждение. Пусть $\varphi : G \mapsto H$ — гомоморфизм. Тогда

- (1) $\text{Im } \varphi < H$
 (2) $\ker \varphi \triangleleft G$

Доказательство.

- (1) Пусть $h_1, h_2 \in \text{Im } \varphi$, тогда

$$\begin{aligned} h_1 &= \varphi(g_1), \quad h_2 = \varphi(g_2), \quad g_i \in G \\ h_1 \cdot h_2 &= \varphi(h_1) \cdot \varphi(h_2) = \varphi(h_1 \cdot h_2) \in \text{Im } \varphi \\ h^{-1} &= \varphi(g^{-1}) \in \text{Im } \varphi \end{aligned}$$

Тогда $\text{Im } \varphi < H$.

- (2)

$$\begin{aligned} g_1, g_2 \in \ker \varphi &\Rightarrow \varphi(g_1) = \varphi(g_2) = e \\ \varphi(g_1 \cdot g_2) &= e \cdot e = e \Rightarrow g_1 \cdot g_2 \in \ker \varphi \\ \varphi(g_1^{-1}) &= e^{-1} = e \Rightarrow g_1^{-1} \in \ker \varphi \end{aligned}$$

Тогда $\ker \varphi < G$.

Покажем, что $\ker \varphi$ — нормальная подгруппа. Пусть $g \in \ker \varphi$, $a \in G$. Тогда

$$\varphi(g^a) = \varphi(a^{-1} \cdot g \cdot a) = \varphi(a)^{-1} \cdot \varphi(g) \cdot \varphi(a) = \varphi(a)^{-1} \cdot \varphi(a) = e$$

Итак, $g \in \ker \varphi \Rightarrow g^a \in \ker \varphi$, то есть $a^{-1} \cdot \ker \varphi \cdot a \subset \ker \varphi \Rightarrow \ker \varphi \triangleleft G$. \square

Замечание.

- (1) Пусть $K < H$. Тогда K — образ некоторого гомоморфизма. Можно предъявить хотя бы $\varphi : K \mapsto H$, $\varphi(k) = k$.
 (2) Пусть $\varphi : G \mapsto H$ — гомоморфизм, $K < G$. Тогда $\varphi|_K : K \mapsto H$ — также гомоморфизм. Значит, $\text{Im } \varphi|_K = \varphi(K)$ — подгруппа в H . $\ker \varphi|_K = K \cap \ker \varphi$.

12. ФАКТОРГРУППА

Утверждение. Пусть G — группа, $H \triangleleft G$. Определим на G/H умножение следующим образом:

$$(g_1 H) \cdot (g_2 H) = g_1 H g_2 H = g_1 \cdot g_2 H \cdot H = g_1 \cdot g_2 \cdot H$$

Тогда $(G/H, \cdot)$ — группа. Операция корректно определена, так как H — нормальная подгруппа.

Доказательство.

- (1) Ассоциативность очевидна $(g_1 H) \cdot ((g_2 H) \cdot (g_3 H)) = g_1 \cdot g_2 \cdot g_3 \cdot H = ((g_1 H) \cdot (g_2 H)) \cdot (g_3 H)$
 (2) Нейтральный элемент $eH = H$, так как $gH \cdot eH = geH = gH = egH = eH \cdot gH$
 (3) Обратный элемент: $gH \cdot g^{-1}H = g^{-1}H \cdot gH = eH \Rightarrow g^{-1}H = (gH)^{-1}$ \square

Определение. Полученная группа называется *факторгруппой* группы G по нормальной подгруппе H и обозначается она G/H .

Теорема. Пусть $H \triangleleft G$. Тогда отображение $\pi_H : G \mapsto G/H$, задаваемое как $\pi_H(g) = gH$ — это эпиморфизм, причем $\ker \pi_H = H$.

Доказательство.

$$\pi_H(g_1 \cdot g_2) = g_1 \cdot g_2 H = g_1 H \cdot g_2 H = \pi_H(g_1) \cdot \pi_H(g_2)$$

Значит π_H — эпиморфизм, так как любой элемент $gH \in G/H$ является образом $g \in G$.

$$g \in \ker \pi_H \Leftrightarrow \pi_H(g) = H \Leftrightarrow gH = H \Leftrightarrow g \in H$$

Значит $\ker \pi_H = H$, что и требовалось показать. \square

Определение. Гомоморфизм π_H называется *естественным гомоморфизмом* из G в G/H .

Теорема. (основная теорема о гомоморфизмах) Пусть $\varphi : G \mapsto K$ — гомоморфизм групп. Тогда

(1) $\forall k \in \text{Im } \varphi \rightarrow \varphi^{-1}(k)$ — это левый смежный класс по $\ker \varphi$

(2) $\text{Im } \varphi \cong G/\ker \varphi$

Доказательство.

(1)

$$\begin{aligned} k \in \text{Im } \varphi &\Rightarrow k = \varphi(g), \quad g \in G \\ \varphi(g') &= k \Leftrightarrow \varphi(g') \cdot \varphi(g^{-1}) = k \cdot k^{-1} = e \\ \varphi(g' \cdot g^{-1}) &= e \Leftrightarrow g' \cdot g^{-1} \in \ker \varphi \\ g' &\in \ker \varphi \cdot g = g \cdot \ker \varphi \end{aligned}$$

Так как ядро — нормальная подгруппа.

(2) Пусть $H = \ker \varphi$. Определим отображение $\psi : G/H \mapsto \text{Im } \varphi$ формулой

$$\psi(gH) = \varphi(g) = \varphi(gH)$$

Тогда ψ — изоморфизм.

- $\psi(g_1 H \cdot g_2 H) = \psi(g_1 g_2 H) = \varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) = \psi(g_1 H) \cdot \psi(g_2 H) \Rightarrow \psi$ — гомоморфизм.
- Если $\psi(g_1 H) = \psi(g_2 H) \Rightarrow \varphi(g_1) = \varphi(g_2) \Rightarrow g_1$ и g_2 лежат в одном смежном классе по подгруппе H . Значит $g_1 H = g_2 H$. Так, ψ — инъекция.
- Если $k \in \text{Im } \psi$, то $k = \varphi(g)$, $g \in G \Rightarrow k = \psi(gH) \Rightarrow \psi$ — сюръекция.

\square

Пример. $\varphi : \mathbb{Z} \mapsto \mathbb{Z}_n$. $\varphi(k) = k \bmod n$. $\text{Im } \varphi = \mathbb{Z}_n \cong \mathbb{Z}/\ker \varphi = \mathbb{Z}/n\mathbb{Z}$.

Упражнение. $\mathbb{Z}_{mn}/n\mathbb{Z}_{mn} \cong ?$

Теорема. (1-я теорема о гомоморфизмах) Пусть $H \triangleleft G$, $K < G$. Тогда

$$H \cap K \triangleleft K, \quad HK < G$$

и при этом

$$K/(H \cap K) \cong HK/H$$

Доказательство. То, что HK — подгруппа в G мы уже доказывали. Рассмотрим естественный гомоморфизм $\pi = \pi_H : G \mapsto G/H$. Пусть $L = \pi(K) < G/H$.

$$1) \pi|_K : K \mapsto G/H$$

$$\begin{aligned} \text{Im } \pi|_K &= L \\ \ker \pi|_K &= K \cap H \end{aligned}$$

Значит по основной теореме $L \cong K/(K \cap H)$

$$2) \pi|_{HK} : HK \mapsto G/H.$$

$$\begin{aligned} \text{Im } \pi|_{HK} &= \pi(HK) = \pi(H) \cdot \pi(K) = \pi(K) = L \\ \ker \pi|_{HK} &= HK \cap H = H \end{aligned}$$

По основной теореме, $L \cong (HK)/H$. □

Упражнение. Построить явно изоморфизм $\psi : K/(K \cap H) \mapsto (HK)/K$.

Теорема. (2-я теорема о гомоморфизмах) Пусть $H \triangleleft G$, $K \triangleleft G$, причем $H < K < G$. Тогда $G/K = (G/H)/(K/H)$.

Доказательство. Определим $\varphi : G/H \mapsto G/K$ формулой

$$\varphi(gH) = gH \cdot K = gK$$

Тогда

$$\varphi(g_1H \cdot g_2H) = g_1K \cdot g_2K = \varphi(g_1H) \cdot \varphi(g_2H)$$

То есть φ — гомоморфизм. $\text{Im } \varphi = G/K$, так как $\varphi^{-1}(gK) \ni gH$.

$$gH \in \ker \varphi \Leftrightarrow gHK = K \Rightarrow g \in K \Rightarrow gH \in (K/H)$$

То есть $\ker \varphi = (K/H) \triangleleft (G/H)$. Тогда по основной теореме

$$\text{Im } \varphi = G/K \cong (G/H)/(K/H)$$

□

Пример. $G = \mathbb{Z}$, $H = n\mathbb{Z}$, $K = mn\mathbb{Z}$, $G > H > K$.

$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, тогда $G/H = \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}_{mn}$.

$K/H = n\mathbb{Z}/mn\mathbb{Z}$.

$\varphi : G/H \mapsto \mathbb{Z}_{mn} - \varphi(K/H) = n\mathbb{Z}_{nm}$.

По второй теореме о гомоморфизмах $\mathbb{Z}_n \cong (G/H)/(K/H) \cong \mathbb{Z}_{mn}/n\mathbb{Z}_{mn}$.

Лекция 5. Действие группы на множестве

13. ОПРЕДЕЛЕНИЕ ДЕЙСТВИЯ ГРУППЫ

Замечание. Если Ω — множество, то через $S(\Omega)$ мы обозначаем группу всех биекций из Ω в Ω .

Определение. Группа G *действует на множестве* Ω , если зафиксирован гомоморфизм $I : G \mapsto S(\Omega)$.

Определение. Группа G *действует на множестве* Ω , если задано отображение $\cdot : G \times \Omega \mapsto \Omega$, такое, что

$$(1) \forall g_1, g_2 \in G, w \in \Omega \rightarrow g_1(g_2 w) = (g_1 g_2) w$$

$$(2) \forall w \in \Omega \rightarrow e \cdot w = w$$

Утверждение. Два определения равносильны.

Доказательство. Пусть G действует на Ω в первом смысле, то есть $\exists I : G \mapsto S(\Omega)$. Вместо $I(g)$ будем писать I_g .

Тогда определим $\forall g \in G, w \in \Omega \rightarrow g \cdot w = I_g(w)$. Тогда

$$\begin{aligned} g_1 \cdot (g_2 w) &= I_{g_1}(I_{g_2}(w)) = (I_{g_1} \circ I_{g_2})(w) = I_{g_1 g_2}(w) \\ e \cdot w &= I_e(w) = id(w) = w \end{aligned}$$

Если G действует на Ω во втором смысле, то определим $\forall g \in G$ отображение $I_g : \Omega \mapsto \Omega, I_g(w) = g \cdot w$. Тогда

$$I_{g_1 g_2}(w) = (g_1 g_2) \cdot w = g_1(g_2 \cdot w) = I_{g_1} \circ I_{g_2}(w) \Rightarrow I_{g_1 g_2} = I_{g_1} \circ I_{g_2}$$

Далее, $I_g \circ I_{g^{-1}} = I_e = id = I_{g^{-1}} \circ I_g$. Тогда I_g — сюръективно (так как $I_g \circ I_{g^{-1}} = id$ — сюръективно) и инъективно (так как $I_{g^{-1}} \circ I_g = id$ — инъективно).

Итого, два определения эквивалентны. \square

Пример.

(1) S_n действует на $\{1, \dots, n\} = [n]$ ($\sigma \cdot k = \sigma(k)$)

(2) Аналогично $GL_n(F)$ действует на F^n ($A \cdot x = Ax$)

(3) Группа диэдра $D_n < O_2(\mathbb{R}) < GL_2(\mathbb{R})$ действует не только на \mathbb{R}^2 , но и, например, на множестве вершин правильного многоугольника. ($f \in D_n, A$ — вершина $\Rightarrow f \cdot A = f(A)$)

Это не единственные множества, на которые действуют эти группы.

(4) S_n действует на $[n]^2: \sigma(i, j) = (\sigma(i), \sigma(j))$.

(5) $GL_n(F)$ действует на множестве всех подпространств в $V = F^n$. Действительно, $GL_n(F)$ можно интерпретировать как множество изоморфизмов $V \mapsto V$, а при таком изоморфизме $\forall U \subset V \rightarrow \varphi(U) \subset V$.

(6) Аналогично, D_n действует на множество всех прямых, проходящих через центр многоугольника и его вершину.

14. ЯДРО, ОРБИТА, СТАБИЛИЗАТОР

Определение. Ядро действия группы на множестве — это ядро гомоморфизма $I : G \mapsto S(G)$ (или, что тоже самое, $\{g \in G \mid \forall w \in \Omega \rightarrow gw = w\}$)

Если ядро действия тривиально, действие называется *точным* (эффективным)

Пример. Все действия выше точны, кроме случая D_2

Определение. Пусть $w \in \Omega$.

Орбитой w называется $Gw = \{gw : g \in G\}$.

Стабилизатором (стационарной подгруппой) w называется $St_G(w) = \{g \in G \mid gw = w\}$.

Замечание. Таким образом действие точно тогда и только тогда, когда $\bigcap_{w \in \Omega} St_G(w) = \{e\}$.

Пример.

(1) Если S_n действует на $[n]$, то $S_n(k) = [n]$

(2) Если GL_n действует на F^n , то орбита $\forall 0 \neq v \in F^n \rightarrow GL_n(F) \cdot v = F^n \setminus \{0\}$, $GL_n(F) \cdot 0 = \{0\}$

Определение. Элементы множества $x, y \in \Omega$ называются *эквивалентными* относительно действия группы G , если $x \in Gy$.

Обозначать будем $x \sim_G y$

Утверждение. \sim_G — отношение эквивалентности, причем классы эквивалентности есть орбиты действия G .

Доказательство.

(1) $x \sim_G x$, так как $x \cdot e = x$

(2) $x \sim_G y \Rightarrow \exists g \in G \Rightarrow x = g \cdot y \Rightarrow g^{-1}x = g^{-1}gy = ey = y$, а значит $y \sim_G x$

(3) Если $x \sim_G y$, $y \sim_G z$, то $x = g_1y$, $y = g_2z \Rightarrow x = (g_1g_2)z \Rightarrow x \sim_G z$.

Итак, \sim_G — эквивалентность. Класс эквивалентности x есть $\{y \mid x \in Gy\}$, то есть это орбита Gy . \square

Пример. Пусть $H < G$. Определим действие H на множестве G как $h \cdot g = hg$. Тогда орбиты этого действия — это правые смежные классы. Тогда утверждение о том, что правые смежные классы либо не пересекаются, либо совпадают, что следует из того, что \sim_H — отношение эквивалентности.

Упражнение. Определить действие H на G так, чтобы орбитами были левые смежные классы (легко видеть, что $h \cdot g = gh$ не проходит).

Утверждение. $\forall w \in \Omega, St(w) < G$.

Доказательство. Если $g_1, g_2 \in St(w)$, то $g_1w = g_2w = w$ и $g_1g_2w = g_1w = w \Rightarrow g_1g_2 \in St(w)$.

Также для любого g_1 верно $g_1w = w \Rightarrow g_1^{-1}g_1w = g_1^{-1}w \Rightarrow g_1^{-1} \in St(w)$.

Наконец $ew = w \Rightarrow e \in St(w) \Rightarrow St(w) \neq \emptyset$. \square

Утверждение. Пусть $x, y \in \Omega, g \in G : x = gy$. Тогда

$$\{h \in G : x = hy\} = St(x) \cdot g = g \cdot St(y)$$

Доказательство. Пусть $h \in G$

$$(1) \ x = hy \Leftrightarrow gy = hy \Leftrightarrow y = g^{-1}hy \Leftrightarrow (g^{-1}h) \in St(y) \Rightarrow h \in g \cdot St(y)$$

$$(2) \ x = hy \Leftrightarrow x = hg^{-1}x \Leftrightarrow (hg^{-1}) \in St(x) \Rightarrow h \in St(x) \cdot g \quad \square$$

Замечание. Некоторые следствия этого утверждения

(1) $St(y) = g^{-1} \cdot St(x) \cdot g$, то есть для любых двух эквивалентных элементов их стабилизаторы сопряжены.

(2) Если Gw — конечна, то количество элементов в ней есть $|Gw| = |G : St(w)|$

Доказательство. Биекцию между Gw и $G/St(w)$ построим следующим образом

$$Gw \ni x \mapsto \{g \in G \mid x = gw\}$$

Это биекция по утверждению. \square

(3) Если G — конечна, то $|Gw| \mid \text{ord } G$ просто по теореме Лагранжа.

Теорема. (формула орбит) Пусть G действует на конечном множестве Ω . Тогда Ω распадается на непересекающиеся орбиты:

$$\Omega = \Omega_1 \sqcup \dots \sqcup \Omega_k$$

Причем, если $w_i \in \Omega_i$, то

$$|\Omega| = \sum_{i=1}^k |\Omega_i| = \sum_{i=1}^k |G : St(w_i)|$$

Доказательство. В сущности, теорему мы уже доказали предыдущими утверждениями и следствиями из них. \square

15. ПРИМЕРЫ ДЕЙСТВИЙ ГРУПП

Пример.

(1) Группа G действует на G левыми сдвигами:

$$I : G \mapsto S(G), \ I_g(h) = gh$$

Тогда $\ker I = \{e\} \Rightarrow$ действие точно. Тогда G вкладывается в $S(G)$, что утверждает теорема Кэли.

(2) G действует левыми сдвигами на множество G/H , где $H < G$.

$g \cdot aH = gaH$. Тогда орбита класса aH — это G/H . Найдем теперь ядро действия

$$St(aH) = \{g \mid gaH = aH\} = \{g \mid a^{-1}ga \in H\} = \{g \in G \mid g \in aHa^{-1}\} = aHa^{-1}$$

Тогда $\ker I = \bigcap_{a \in G} aHa^{-1}$.

Утверждение. Это есть наибольшая нормальная подгруппа, содержащаяся в H

Доказательство. $\forall a \in G$ мы знаем, что aHa^{-1} — подгруппа. Тогда $\ker I = \bigcap_{a \in G} aHa^{-1}$ тоже подгруппа.

Кроме того, $\forall g \in G \rightarrow g^{-1} \cdot \ker I \cdot g = \bigcap_{a \in G} (g^{-1}a)H(g^{-1}a)^{-1}$. Так как $g^{-1} \cdot a$ вместе с a пробегает всю группу, то

$$g^{-1} \cdot \ker I \cdot g = \bigcap_{a \in G} aHa^{-1} = \ker I$$

То есть ядро нормально в G

Наконец, если $K \triangleleft G$, $K < H$, то $K = g^{-1}Kg < g^{-1}Hg \Rightarrow K \subset \ker I$. \square

Упражнение. Пусть $H < G$, $|G : H| = n$. Показать, что $|G : \ker I| \leq n!$

Лекция 6. Автоморфизмы группы, p -группы и лемма Бернсайда

16. ДЕЙСТВИЕ ГРУППЫ НА СЕБЯ СОПРЯЖЕНИЯМИ

Пример. Еще один пример действия группы: G действует на себя сопряжениями. $g, h \in G \Rightarrow h^g = g^{-1}hg$. Отображение

$$\begin{aligned} I_g : G &\mapsto G, \quad I_g(h) = h^{g^{-1}} = ghg^{-1} \\ I_{g_1g_2}(a) &= g_1 \cdot (g_2 \cdot a \cdot g_2^{-1}) \cdot g_1^{-1} = I_{g_1} \circ I_{g_2}(a) \end{aligned}$$

Итого, группа действует на себя сопряжениями, возникает гомоморфизм $I : G \mapsto S(G)$

Орбита элемента $a \in G$ — это a^G , класс сопряженности.

Стабилизатор элемента $a \in G$ — это его *централизатор* $C_G(a) = \{g : gag^{-1} = a\} = \{g \in G : ga = ag\}$.

Замечание. $C_G(a)$ — подгруппа.

Утверждение. Пусть G — конечная группа, $a \in G$. Тогда $|a^G|$ делит $|G|$, более того он делит $\frac{|G|}{\text{ord } a}$.

Доказательство. $|a^G|$ — это мощность орбиты a , то есть

$$|a^G| = |G : St_G(a)| = |G : C_G(a)| = \frac{|G|}{|C_G(a)|} \Rightarrow |a^G| \mid |G|$$

Более того, $a \in C_G(a) \Rightarrow a^{a^{-1}} = a \cdot a \cdot a^{-1} = a \in C_G(a)$. Значит $\langle a \rangle < C_G(a)$, то есть $|(a)| \mid |C_G(a)|$.

Значит, $|a^G| = \frac{|G|}{|C_G(a)|} \mid \frac{|G|}{\text{ord } a}$. \square

17. ГРУППА АВТОМОРФИЗМОВ

Замечание. Для любого $g \in G$, I_g — изоморфизм из G в G (автоморфизм). Действительно,

$$I_g(ab) = (ab)^{g^{-1}} = a^{g^{-1}} \cdot b^{g^{-1}} = I_g(a) \cdot I_g(b)$$

Значит I_g — автоморфизм, так как он обратим.

Определение. Через $\text{Aut } G$ обозначается группа всех автоморфизмов группы G .

Определение. Тогда на самом деле можно считать, что $I : G \mapsto \text{Aut } G$, а образ $\text{Im } I$ называется группой внутренних автоморфизмов группы G , и обозначается $\text{Inn } G$.

Любой элемент этого образа называется внутренним автоморфизмом.

Определение. Ядро действия $\ker I = \{g \in G \mid \forall a \in G \rightarrow gag^{-1} = a\} = \{g \in G \mid \forall a \in G \rightarrow ga = ag\}$ называется центром группы G и обозначается $Z(G)$.

Замечание.

$$(1) Z(G) \triangleleft G$$

$$(2) \text{Inn } G \cong G/Z(G)$$

Доказательство. $Z(G) = \ker I \Rightarrow Z(G) \triangleleft G$. $\text{Inn}(G) = \text{Im } I \cong G/\ker I = G/Z(G)$. \square

Замечание. Пусть G — абелева группа, тогда $Z(G) = G$, $\text{Inn } G = \{id\}$. В то же время $\text{Aut } G$ не обязательно тривиальна, например при $n > 2$ можно предъявить нетривиальный изоморфизм $\varphi : \mathbb{Z}_n \mapsto \mathbb{Z}_n$, $\varphi(a) = (-a) \pmod n$. То есть бывают не внутренние автоморфизмы.

Замечание. Теперь мы можем легко понять, почему сопряжение подгруппы есть подгруппа. В самом деле, если $H < G$, то $gHg^{-1} = I_g(H) < G$.

Упражнение. $\text{Inn } G < \text{Aut } G$. Показать, что $\text{Inn } G \triangleleft \text{Aut } G$

18. ДЕЙСТВИЕ ГРУППЫ НА СВОИ ПОДГРУППЫ СОПРЯЖЕНИЯМИ

Пример. G действует сопряжениями на множество всех своих подгрупп:

$$I_g(H) = gHg^{-1} < G$$

То, что это действие следует из тех же самых выкладок, что и в обычном действии сопряжениями.

Орбита H — множество всех подгрупп, сопряженных с ней.

Стабилизатор H — называется ее *нормализатором*: $N_G(H) = \{g \in G \mid gH = Hg\}$

Утверждение. Если $H < G$, то $N_G(H)$ — наибольшая по включению подгруппа такая, что $H \triangleleft N$.

Доказательство. Так как $N_G(H)$ — стационарная подгруппа элемента H , то $N_G(H) < G$. Так как $\forall g \in N_G(H) \rightarrow gH = Hg$, то $H \triangleleft N_G(H)$.

Наконец, если $K < G$, $H \triangleleft K$, то $\forall g \in K \rightarrow gH = Hg \Rightarrow \forall g \in K \rightarrow g \in N_G(H) \Rightarrow K < N_G(H)$ \square

Замечание. Если G — конечна, то $H \leq N_G(H) \Rightarrow |H^G| = |G : N_G(H)| = \frac{|G|}{|N_G(H)|} \mid \frac{|G|}{|H|} = |G : H|$

Упражнение. Если $H < G$, $|G : H| < \infty$, то $|H^G| \mid |G : H|$.

19. p -ГРУППЫ

Определение. Пусть G — группа, $1 < |G| < \infty$, а p — простое число. G называется p -группой, если $\exists n : |G| = p^n$.

Замечание. Если G — p -группа, то порядки ее элементов и подгрупп — это степени p .

Пример. Если $|G| = p$, то $\forall e \neq g \in G \rightarrow \text{ord } g = p$, то есть $\langle g \rangle = G$. Итак, G — циклическая.

Теорема. Если G — p -группа, то $Z(G) \neq \{e\}$.

Доказательство. Рассмотрим действие G на себя сопряжением. Пусть $g_1^G, \dots, g_k^G, \dots, g_l^G$ — все классы сопряженности, причем $g_i \in Z(G) \Leftrightarrow i \leq k$. Так, $k = |Z(G)|$.

Тогда при $i \leq k \rightarrow g_i^G = \{g_i\}$, так как $g_i^h = h^{-1} \cdot g_i \cdot h = g_i$.

При $i > k : |g_i^G| > 1$, так как найдется не коммутирующий элемент.

Тогда по формуле орбит

$$|G| = \sum_{i=1}^l |g_i^G| = \sum_{i=1}^k |g_i^G| + \sum_{i=k+1}^l |g_i^G| = |Z(G)| + \sum_{i=k+1}^l |G : C_G(g_i)|$$

Заметим, что при $k > i \rightarrow C_G(g_i) \neq G \Rightarrow |G : C_G(g_i)| \vdots p$. Тогда так как $|G| \vdots p$, то и $|Z(G)| \vdots p$, а значит и $|Z(G)| > 1$. \square

Теорема. Пусть G — неабелева группа. Тогда $G/Z(G)$ — не циклический.

Доказательство. Предположим противное $G/Z(G) = \langle aZ(G) \rangle$, $a \in G$. Это значит, что левые смежные классы по $Z(G)$ имеют вид $a^n Z(G)$ где $n \in \mathbb{Z}$.

Пусть $g_1, g_2 \in G$, тогда $g_i \in a^{n_i} Z(G)$, то есть $g_1 = a^{n_1} z_1$, $g_2 = a^{n_2} z_2$, $z_i \in Z(G)$.

Тогда $g_1 g_2 = \underbrace{a^{n_1} z_1 a^{n_2} z_2}_{\text{попарно коммутируют}} = a^{n_2} z_2 a^{n_1} z_1 = g_2 \cdot g_1$. Тогда G — абелева, противоречие. \square

Замечание. Как следствие, если $|G| = p^2$, то G — абелева.

Доказательство. G — p -группа, тогда $|Z(G)| > 1$. Если $|Z(G)| = p^2$, то $Z(G) = G$ — абелева.

Если же $|Z(G)| = p$, то $|G/Z(G)| = p$, а значит фактор нетривиальный и циклический, а этого не бывает в неабелевых группах. \square

Упражнение. Привести пример неабелевой группы порядка p^3 (Подсказка: пример есть среди матричных групп)

20. ЛЕММА БЕРНСАЙДА

Определение. Пусть группа G действует на Ω . Ее действие *транзитивно*, если у него ровно одна орбита. Иными словами,

$$\forall w_1, w_2 \in \Omega \rightarrow \exists g \in G : gw_1 = w_2$$

Пример. S_n действует на $[n]$ транзитивно.

Теорема. (лемма Бернсайда) Пусть конечная группа G действует на множество транзитивно. Для $g \in G$ обозначим количество неподвижных точек перестановки элемента g

$$Fix(g) = |\{w \in \Omega \mid gw = w\}|$$

Тогда $\sum_{g \in G} Fix(g) = |G|.$

Доказательство. Построим таблицу $|G| \times |\Omega|$:

В клетке (g, w) ставим \star , если $gw = w$. Тогда общее количество звездочек есть $\sum_{g \in G} Fix(G)$.

С другой стороны в столбце, соответствующем $w \in \Omega$ стоит ровно $|St_a(w)|$ звездочек. Однако, так как действие транзитивно, то $|St_a(w)| = \frac{|G|}{|Gw|} = \frac{|G|}{|\Omega|}$.

Значит $\sum_{g \in G} Fix(G) = \sum_{w \in \Omega} |\Omega| \cdot \frac{|G|}{|\Omega|} = |G|.$ □

Замечание. $|\Omega| = |Gw| \leq |G| \Rightarrow |\Omega| < \infty$.

Замечание. Пусть конечная группа G действует на конечно множество Ω . Тогда количество орбит есть

$$\frac{1}{|G|} \sum_{g \in G} Fix(g)$$

Доказательство. Разобьем Ω на орбиты:

$$\Omega = \Omega_1 \sqcup \dots \sqcup \Omega_k$$

Для $g \in G$ обозначим $Fix_i(g) = |\{w \in \Omega_i : gw = w\}|$. Тогда G действует на Ω_i транзитивно, то есть

$$\sum_{g \in G} Fix(g) = \sum_{g \in G} \sum_{i=1}^k Fix_i(g) = \sum_{i=1}^k \sum_{g \in G} Fix_i(g) = \sum_{i=1}^k |G| = k \cdot |G|$$

Таким образом, $k = \frac{1}{|G|} \cdot \sum_{g \in G} Fix(g)$ □

Лекция 7. Произведения групп

21. k -ТРАНЗИТИВНЫЕ ДЕЙСТВИЯ И ОБОБЩЕНИЯ ЛЕММЫ БЕРНСАЙДА

Замечание. Если G действует на Ω , то можно определить действие на Ω^2 :

$$g(w_1, w_2) = (gw_1, gw_2)$$

Это действие не транзитивно, если $|\Omega| > 1$, так как $g(w, w)$ состоит из одинаковых элементов.

Тогда можно определить действие на $\Omega^{[2]} = \{(w_1, w_2) \mid w_1, w_2 \in \Omega, w_1 \neq w_2\}$

Определение. G действует на Ω *2-транзитивно*, если действие G на $\Omega^{[2]}$ транзитивно.

Замечание. Аналогично определяется k -транзитивное действие

Пример. S_n действует на $[n]$ k -транзитивно для любого $k \leq n$

Упражнение. Пусть конечная группа G действует на Ω 2-транзитивно, тогда

$$\sum_{g \in G} \text{Fix}(g)^2 = 2 \cdot |G|$$

22. ПРЯМОЕ ПРОИЗВЕДЕНИЕ ГРУПП

Определение. Пусть G, H — две группы. Их *прямым произведением* называется группа

$$(G \times H, \cdot) = \{(g, h) \mid g \in G, h \in H\}$$

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

Замечание. Ассоциативность очевидно следует из ассоциативности в G и H . Нейтральный элемент (e_G, e_H) , обратным элементом будет $(g, h) = (g^{-1}, h^{-1})$.

Утверждение.

- (1) $G \cong G \times \{e_H\} \triangleleft G \times H$, $H \cong \{e_G\} \times H \triangleleft G \times H$
- (2) $G \times H \cong H \times G$
- (3) $(G \times H) \times K \cong G \times (H \times K)$

Доказательство.

- (1) $\varphi(g) = (g, e_H)$ — изоморфизм. Далее, $\psi : G \times H \mapsto H$, $\psi((g, h)) = h$ — гомоморфизм и $\ker \psi = G \times \{e_H\}$. Значит наша подгруппа нормальна. Аналогично для H .
- (2) $(g, h) \mapsto (h, g)$ — изоморфизм.
- (3) $((g, h), k) \mapsto (g, (h, k))$ — изоморфизм. □

Замечание. В связи с пунктом 3, скобки будем опускать.

Замечание. Если G и H абелевы, то вместо прямого произведения часто пишут $G \oplus H$, называя его *прямой суммой* групп.

Теорема. Пусть G — группа, $A, B \triangleleft G$ такие, что $A \cap B = \{e\}$, а $A \times B = G$. Тогда $G \cong A \times B$

Доказательство. Пусть $a \in A$, $b \in B$. Тогда рассмотрим $aba^{-1}b^{-1}$, $c = \underbrace{aba^{-1}}_{\in B} \cdot b^{-1} \in B$.

Аналогично $c = a \cdot bab^{-1} \in A$.

Значит, $c \in A \cap B = \{e\}$, то есть $c = e \Rightarrow ab = ba$. Теперь построим $\varphi : A \times B \rightarrow G$, $\varphi((a, b)) = ab$.

1) φ — гомоморфизм:

$$\varphi((a_1, b_1)) \cdot \varphi((a_2, b_2)) = a_1 b_1 a_2 b_2 = a_1 a_2 b_1 b_2 = \varphi((a_1 a_2, b_1 b_2))$$

2) φ — сюръекция, так как $A \times B = G$.

3) φ — инъекция. Если $\varphi((a_1, b_1)) = \varphi((a_2, b_2))$, то $a_1 b_1 = a_2 b_2$. Тогда $A \ni a_2^{-1} a_1 = b_2 b_1^{-1} \in B$, то есть

$$a_2^{-1} a_1 = b_2 b_1^{-1} = e \Rightarrow a_1 = a_2, b_1 = b_2$$

□

Замечание. В условиях теоремы G — внутреннее прямое произведение подгрупп A, B .

Упражнение. Найти критерий того, что G — прямое произведение своих подгрупп A_1, \dots, A_n

Пример. Пусть $\gcd(n, k) = 1$. Положим $G \cong \mathbb{Z}_{nk}$, $A = n\mathbb{Z}_{nk} \cong \mathbb{Z}_k$, $B = k\mathbb{Z}_{nk} \cong \mathbb{Z}_n$.

$A, B \triangleleft G$, $A \cap B = \{0\}$, $|A + B| = |A| \cdot |B| \Rightarrow A + B = G$. Таким образом, $\mathbb{Z}_{nk} \cong \mathbb{Z}_n \times \mathbb{Z}_k$ (китайская теорема об остатках)

Утверждение. Пусть G, H — группы, $G_1 < G$, $H_1 < H$. Тогда $G_1 \times H_1 < G \times H$; эта подгруппа нормальная, если $G_1 \triangleleft G$, $H_1 \triangleleft H$, в этом случае $(G \times H) / (G_1 \times H_1) = (G/G_1) \times (H/H_1)$.

Доказательство. $G_1 \times H_1 < G \times H$ — очевидно. Пусть $G_1 \triangleleft G$, $H_1 \triangleleft H$, тогда определим

$$\begin{aligned}\varphi : G \times H &\mapsto (G/G_1) \times (H/H_1) \\ \varphi((g, h)) &= (gG_1, hH_1)\end{aligned}$$

Тогда φ — сюръекция и гомоморфизм. $\ker \varphi = G_1 \times H_1$. По основной теореме о гомоморфизмах имеем

$$(G/G_1) \times (H/H_1) = (G \times H) / (G_1 \times H_1)$$

Также $G_1 \times H_1 \triangleleft G \times H$ как ядро гомоморфизма. □

Упражнение. Если $G_1 \times H_1 \triangleleft G \times H$, тогда $G_1 \triangleleft G$, $H_1 \triangleleft H$.

23. ПОЛУПРЯМОЕ ПРОИЗВЕДЕНИЕ ГРУПП

Определение. Пусть $A, B < G$, $A \cap B = \{e\}$, $AB = G$, $A \triangleleft G$. Тогда G называется *полупрямым произведением* A и B , $G = A \rtimes B$.

Замечание. Если G — полупрямое произведение A и B . Тогда $\forall g \in G \rightarrow g = ab$, $a \in A$, $b \in B$ и это представление единственно. Более того, $G/A = AB/A \cong B/(B \cap A) = B$.

Пример. 1) $S_n = A_n \rtimes ((1\ 2))$ так как $A_n \cap ((1\ 2)) = \{id\}$, $A_n \times ((1\ 2)) = S_n$ и $A_n \triangleleft S_n$.

Но $S_n \not\cong A_n \times ((1\ 2))$. В противном случае у S_n был бы нетривиальный центр, соответствующий $(id, (1\ 2))$. Но

Упражнение. центр S_n тривиален при $n \geq 3$.

2) Может быть, что $G/A = B$, но G не является полупроизведением A на подгруппу G , изоморфную B .

$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, но в \mathbb{Z} нет подгруппы, изоморфной \mathbb{Z}_n .

Замечание. Как описать все полупроизведения?

Пусть $G = A \rtimes B$. Тогда B действует на A сопряжениями. Более того, $\forall b \in B$ задает автоморфизм φ_b группы A .

Иными словами, появляется гомоморфизм

$$\varphi : B \mapsto \text{Aut}(A)$$

Этим гомоморфизмом полупроизведение задано уже однозначно. $\forall g \in G \rightarrow g = a_g b_g$, $a_g \in A$, $b_g \in B$.

Тогда $g, h \in G$, $gh = a_g b_g \cdot a_h b_h = a_g \cdot b_g \cdot a_h b_g^{-1} \cdot b_g \cdot b_h = (a_g \cdot \varphi_{b_g}(a_h)) \cdot (b_g \cdot b_h)$.

Итак, G — изоморфна группе, множество элементов которой есть $A \times B$, операция: $(a_1, b_1)(a_2, b_2) = (a_1 \varphi_{b_1}(a_2), b_1 b_2)$.

Упражнение. Пусть A, B — произвольные группы, а $\varphi : B \mapsto \text{Aut}(A)$ — гомоморфизм. Тогда определение сверху задает группу, являющуюся полупрямым произведением $A \times \{e\}$ и $\{e\} \times B$. Оно обозначается $A \rtimes_{\varphi} B$.

Лекция 8. Разрешимые группы

24. КОММУТАНТ ГРУППЫ

Определение. Пусть $x, y \in G$. Их коммутатором называется $[a, b] = xyx^{-1}y^{-1}$.

Утверждение.

- (1) $xy = [x, y]yx$, в частности $xy = yx \Leftrightarrow [x, y] = e$
- (2) $[x, y]^{-1} = [y, x]$
- (3) $[x, y]^g = [x^g, y^g]$

Доказательство.

- (1) $[x, y]yx = xyx^{-1}y^{-1}yx = xy$
- (2) $[x, y]^{-1} = yxy^{-1}x^{-1} = [y, x]$
- (3) Следует из того, что сопряжение — автоморфизм. □

Замечание. Если $\varphi : G \mapsto A$, A — абелева, то $\forall x, y \in G \rightarrow \varphi([x, y]) = e$.

Определение. Коммутантом группы G называется $G' = (\{[x, y] \mid x, y \in G\})$

Определение. Взаимным коммутантом $H, K \triangleleft G$ называется $[H, K] = (\{[h, k] \mid h \in H, k \in K\})$

Замечание. Легко видеть, что $G' = [G, G]$

Утверждение. Пусть $\varphi : G \mapsto H$ — гомоморфизм, тогда $\varphi(G') \subset H'$. Если φ — эпиморфизм ($\text{Im } \varphi = H$), то $\varphi(G') = H'$.

Доказательство. Если $x, y \in G$, то $\varphi([x, y]) = [\varphi(x), \varphi(y)] \in H'$. Так как G' порожден такими элементами, то $\varphi(G') \subset H'$.

Если φ — эпиморфизм, то $\forall a, b \in H \rightarrow \exists x, y \in G : \varphi(x) = a, \varphi(y) = b$. Так,

$$\varphi(G') = (\{[\varphi(x), \varphi(y)] \mid x, y \in G\}) = (\{[a, b] \mid a, b \in H\}) = H'$$

□

Утверждение. Если $K \triangleleft G$, то $K' \triangleleft G$.

Доказательство. Покажем, что $\forall g \in G \rightarrow gK'g^{-1} = K'$. Рассмотрим автоморфизм $\varphi_g : G \mapsto G$, $\varphi_g(x) = gxg^{-1}$. Поскольку $K \triangleleft G$, то $gKg^{-1} = K \Rightarrow \varphi_g(K) = K$. Тогда $\varphi_g|_K$ — сюръективный гомоморфизм из K в K . Тогда $\varphi_g(K') = K'$. □

Замечание. Отсюда получаем, что $G \triangleleft G' \triangleleft G'' \triangleleft \dots \triangleleft G^{(n)} \triangleleft \dots$

25. ХАРАКТЕРИЗАЦИЯ КОММУТАНТА

Лемма. Пусть $H \triangleleft G$, $H < K < G$. Если $K/H \triangleleft G/H$, то $K \triangleleft G$.

Доказательство. Рассмотрим канонические эпиморфизмы

$$\pi_1 : G \mapsto G/H, \quad \pi_2 : G/H \mapsto (G/H) / (K/H)$$

Из композиции — эпиморфизм, причем $\ker(\pi_1 \circ \pi_2) = \pi_1^{-1}(\pi_2^{-1}(e)) = \pi_1^{-1}(K/H) = K$. Так, $K \triangleleft G$. \square

Теорема. Пусть G — некоторая группа, тогда

(1) Если $G' < K < G$, то $K \triangleleft G$

(2) Для любой $K \triangleleft G \rightarrow G/K$ — абелева $\Leftrightarrow G' < K$

Доказательство. Рассмотрим канонический эпиморфизм $\pi : G \mapsto G/G'$. $(G/G')' = \pi(G') = \{e_{G/G'}\}$. Значит G/G' — абелева, раз ее коммутант тривиален. При этом $\pi(K) = K/G' < G/G'$. Так как G/G' — абелева, то $K/G' \triangleleft G/G'$, то есть $K \triangleleft G$.

Далее, если $G' < K$, то по второй теореме о гомоморфизмах $G/K \cong (G/G') / (K/G')$ абелева как факторгруппа абелевой группы.

В обратную сторону, рассмотрим канонический эпиморфизм $\pi_K : G \mapsto G/K$. Если G/K — абелева, то $(G/K)' = \{e\}$. Но $(G/K)' = \pi_K(G')$. Значит, $\pi_K(G') = \{e\}$, то есть $G' < K$. \square

Замечание. Из этой теоремы следует следующая характеристика коммутанта: G' — наименьшая по включению нормальная подгруппа в G , такая, что факторгруппа по ней абелева.

Определение. Пусть G — группа, $M \subset G$. Тогда нормальной подгруппой, порожденной M называется

$$(M)_n = \bigcap_{K \triangleleft G, M \subset K} K$$

Утверждение. $(M)_n = (M^G)$

Доказательство. Ясно, что $M^G \subset (M)_n$, так как $(M)_n^G = (M)_n$. Покажем, что $(M^G) \triangleleft G$. Пусть $\varphi_g \in \text{Inn } G$, тогда $\varphi_g(M^G) = M^G \Rightarrow \varphi_g((M^G)) = M^G$. Поэтому $M^G \triangleleft G \Rightarrow (M)_n \subset M^G$. \square

Теорема. Пусть $G = (\{g_i\} \mid i \in I)$. Тогда $G' = (\{[g_i, g_j] \mid i, j \in I\})_n$

Доказательство. Пусть $H = (\{[g_i, g_j] \mid i, j \in I\})_n$. Тогда $H < G'$, так как порождена частью порождающих элементов G' .

Рассмотрим $G/H = (\{g_i H \mid i \in I\})$. Далее, $[g_i H, g_j H] = [g_i, g_j] H = H$, так как $[g_i, g_j] \in H$. Так, $g_i H \cdot g_j H = g_j H \cdot g_i H$ и G/H — абелева, откуда $H > G'$, а значит $H = G'$. \square

Пример. Найдем S'_n . Во-первых, если $x, y \in S_n$, то $[x, y] = xyx^{-1}y^{-1} \in A_n$, а значит $S'_n < A_n$. С другой стороны $[(i \ j)(i \ k)] = (i \ j)(i \ k)(i \ j)(i \ k) = (i \ j \ k) \in S'_n$. Но все тройные циклы порождают A_n , поэтому $A_n = S'_n$.

Упражнение. Пусть $H \triangleleft G$. Положим $K = [H, G]$. Тогда K — наименьшая нормальная подгруппа, такая что $H/K \subset Z(G/K)$.

26. РАЗРЕШИМЫЕ ГРУППЫ

Определение. Пусть G — группа. Если $\exists n \in \mathbb{N} : G^{(n)} = \{e\}$, то G называется *разрешимой группой*. Наименьшее такое n называют *степенью разрешимости* G .

Утверждение. Пусть $H \triangleleft G$. Тогда G — разрешима тогда и только тогда, когда разрешимы H и G/H .

Доказательство. Пусть G имеет степень разрешимости n . Тогда $H < G \Rightarrow H' < G' \Rightarrow \dots \Rightarrow H^{(n)} < G^{(n)} = \{e\} \Rightarrow H^{(n)} = \{e\}$, то есть H тоже разрешима.

Теперь рассмотрим естественный эпиморфизм $\pi : G \mapsto G/H$. Тогда $(G/H)' = \pi(G')$, то есть $\pi|_{G'} : G' \mapsto (G/H)'$ — тоже естественный эпиморфизм. Продолжая далее, $\pi|_{G^{(n)}} : G^{(n)} \mapsto (G/H)^{(n)}$ — естественный эпиморфизм, то есть $(G/H)^{(n)} = \pi(G^{(n)}) = \{e_{G/H}\}$, то есть (G/H) — разрешима.

Теперь, если $H^{(k)} = \{e\}$ и $(G/H)^{(l)} = \{e\}$, то рассматривая естественный эпиморфизм π , получаем, что $\pi(G^{(l)}) = (G/H)^{(l)} = \{e_{G/H}\}$. Но тогда $G^{(l)} < H \Rightarrow G^{(l+k)} < H^{(k)} = \{e\} \Rightarrow G^{(l+k)} = \{e\}$, то есть G — разрешима. \square

Замечание. Если $K_1, K_2 \triangleleft G$ — разрешимые подгруппы, то $K_1 K_2$ — разрешимая подгруппа.

Доказательство. По первой теореме о гомоморфизмах $K_1 K_2 / K_2 \cong K_1 / (K_1 \cap K_2)$. K_1 — разрешима, значит и $K_1 / (K_1 \cap K_2)$ вместе с $K_1 K_2 / K_2$. Так как K_2 — разрешима, то $K_1 K_2$ тоже, что нам и нужно. \square

Лекция 9. Простые группы

27. КРИТЕРИЙ РАЗРЕШИМОСТИ

Теорема. Пусть G — конечная группа. Тогда в ней есть наибольшая (по включению) нормальная разрешимая подгруппа N . Более того, G/N не содержит разрешимых подгрупп, кроме тривиальной.

Доказательство. В G конечное количество нормальных разрешимых подгрупп K_1, \dots, K_n . Пусть $N = K_1 \cdot \dots \cdot K_n$, тогда N — тоже нормальная разрешимая и содержит K_1, \dots, K_n . Это и есть искомая подгруппа.

Предположим, что в G/N есть нормальная разрешимая подгруппа L . Пусть $\pi : G \mapsto G/N$ — канонический эпиморфизм и $K = \pi^{-1}(L)$. Тогда K — подгруппа, содержащая N , при этом $L = K/N$. Так как N и K/N — разрешимы, то и K — разрешима. Более того, так как $L \triangleleft G/N \Rightarrow K \triangleleft G$. Поскольку N — наибольшая нормальная разрешимая подгруппа, то $K \leq N$. Таким образом $K = N \Rightarrow L = N/N = \{e\}$. \square

Теорема. Пусть G — некоторая группа, тогда следующие условия равносильны:

- (1) G — разрешима
- (2) В G существует цепочка подгрупп $G = G_0 > G_1 > \dots > G_n = \{e\}$, такая что $G_i \triangleleft G$ и G_i/G_{i+1} — абелева. (нормальный ряд подгрупп)
- (3) В G существует цепочка подгрупп, такая, что $G = G_0 > \dots > G_n = \{e\}$, такая, что $G_{i+1} \triangleleft G_i$ и G_i/G_{i+1} — абелева. (субнормальный ряд подгрупп)

Доказательство.

(1) \Rightarrow (2). Положим $G_i = G^{(i)}$. Тогда $G^{(i)} \triangleleft G$ и $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$ — абелева.

(2) \Rightarrow (3). $G_i \triangleleft G \Rightarrow G_i \triangleleft G_{i-1}$.

(3) \Rightarrow (1). Докажем индукцией по i , что $G_i \geq G^{(i)}$. При $i = 0$ это верно.

Пусть $G_i \geq G^{(i)}$. При этом G_i/G_{i+1} — абелева, значит $G_{i+1} \geq (G_i)'$. Поскольку $G_i \geq G^{(i)}$, то $G_{i+1} \geq (G^{(i)})' = G^{(i+1)}$. Итого, $\{e\} = G_n > G^{(n)} \Rightarrow G^{(n)} = \{e\} \Rightarrow G$ — разрешима. \square

Замечание. Существуют разрешимые группы сколь угодно большой степени разрешимости.

Упражнение. Проверить, что S_4 — разрешима.

28. ПРОСТЫЕ ГРУППЫ

Определение. Группа G , $|G| > 1$, называется *простой*, если в ней нет нетривиальных нормальных подгрупп.

Утверждение. Абелева группа $|G|$ проста, тогда и только тогда, когда $G \cong \mathbb{Z}_p$, где p — простое.

Доказательство. Все подгруппы G нормальны, так как она абелева. Тогда $\forall g \neq e \rightarrow (g) \triangleleft G$. Так как G — проста, то $(g) = G$, так как $(g) \neq \{e\}$. Значит G — циклическая, то есть либо $G \cong \mathbb{Z}$, либо $G \cong \mathbb{Z}_n$. Но \mathbb{Z} не проста, так как в ней есть нормальная подгруппа $2\mathbb{Z}$.

Пусть $G \cong \mathbb{Z}_n$. Если n — простое, то порядок любой подгруппы либо 1, либо n , то есть G действительно проста. Если же $n = kl$, $k, l > 1$, то $G \cong \mathbb{Z}_n \supset k\mathbb{Z}_n \neq \mathbb{Z}_n$, то есть G — не проста. \square

Утверждение. Пусть G — не абелева простая группа. Тогда $G' = G$, и она неразрешима.

Доказательство. $G' \triangleleft G$, $G' \neq \{e\}$. Так как G — проста, то $G' = G \Rightarrow G^{(n)} = G$, то есть она неразрешима. \square

Лемма. Пусть $G > H, K$. Тогда $|G : H| \geq |K : K \cap H|$.

Доказательство. Пусть $G = g_1H \sqcup \dots \sqcup g_nH$, $|G : H| = n$. Пусть $K \cap g_iH \neq \emptyset$, то есть $k \in K \cap g_iH$. Тогда $g_iH = kH$, а значит $K \cap g_iH = K \cap kH \Rightarrow kK \cap kH = k(K \cap H)$. Мы получили левый смежный класс в K по подгруппе $K \cap H$.

Итак, $K = \bigsqcup_i K \cap g_iH = \bigsqcup_{i: K \cap g_iH \neq \emptyset} K_i(K \cap H)$, это и значит, что $|K : K \cap H| \leq |G : H|$. \square

Теорема. Группа A_5 — проста.

Доказательство. Напомним, что если $H < G$, то $H \triangleleft G \Leftrightarrow H$ — объединение нескольких классов сопряженности.

Выпишем классы сопряженности элементов из A_5 в S_5 :

$(e)^{S_5}, (1\ 2\ 3)^{S_5}, (1\ 2\ 3\ 4\ 5)^{S_5}, (1\ 2)(3\ 4)^{S_5}$ (в количестве 1, 20, 24, 15 элементов соответственно).

Для $\sigma \in A_5$, σ^{S_5} — либо 1 класс сопряженности в A_5 , либо распадается на несколько.

При этом $|\sigma^{S_5}| = |S_5 : C_{S_5}(\sigma)|$, а $|\sigma^{A_5}| = |A_5 : C_{A_5}(\sigma)|$. При этом $C_{A_5}(\sigma) = C_{S_5}(\sigma) \cap A_5$. Тогда по предыдущей лемме

$$|C_{S_5}(\sigma) : C_{A_5}(\sigma)| \leq |S_5 : A_5| = 2$$

Если $|C_{S_5}(\sigma) : C_{A_5}(\sigma)| = 2$, тогда индексы $|S_5 : C_{S_5}(\sigma)| = |A_5 : C_{A_5}(\sigma)|$, тогда $|\sigma^{S_5}| = |\sigma^{A_5}|$.

Если же $|C_{S_5}(\sigma) : C_{A_5}(\sigma)| = 1$, то $|\sigma^{S_5}| = 2|\sigma^{A_5}|$, то есть класс сопряженности распадается на 2 класса.

Исследуем, как ведут себя указанные выше классы:

$$C_{S_5}((1\ 2\ 3)) \ni (4\ 5) \Rightarrow C_{A_5}((1\ 2\ 3)) \neq C_{S_5}((1\ 2\ 3))$$

$$C_{S_5}((1\ 2)(3\ 4)) \ni (1\ 2) \Rightarrow C_{A_5}((1\ 2)(3\ 4)) \neq C_{S_5}((1\ 2)(3\ 4))$$

$C_{S_5}((1\ 2\ 3\ 4\ 5)) = \frac{|S_5|}{|(1\ 2\ 3\ 4\ 5)^{S_5}|} = 5 \Rightarrow |C_{S_5}((1\ 2\ 3\ 4\ 5)) : C_{A_5}((1\ 2\ 3\ 4\ 5))| \neq 2$, то есть $(1\ 2\ 3\ 4\ 5)^{S_5}$ распадается на два (можно сопрячь любой нечетной перестановкой и получить представителя). Таким образом:

Класс	Число элементов
id^{A_5}	1
$(1\ 2\ 3)^{A_5}$	20
$(1\ 2)(3\ 4)^{A_5}$	15
$(1\ 2\ 3\ 4\ 5)^{A_5}$	12
$(1\ 2\ 3\ 5\ 4)^{A_5}$	12

Пусть теперь $H \triangleleft A_5$, $H \neq \{id\}$. Если $(1\ 2\ 3)^{A_5} \subset H$, то $|H| \geq 20 + 1 = 21$, то есть $|H| = 30$ или $|H| = 60$. Но для $|H| = 30$ необходим еще один класс из 9 элементов.

Итак, $(1\ 2\ 3)^{A_5} \not\subset H$, значит $|H|$ не может делиться на 3. Тогда $|H| \leq 20$, что невозможно.

Остается только случай $|H| = 60$, а значит в G нет нормальных подгрупп кроме тривиальных. \square

Теорема. При $n \geq 5$ группа A_n — простая.

Доказательство. Доказываем индукцией по n . База при $n = 5$ уже доказана.

Пусть $n \geq 6$. Пусть $H \triangleleft A_n$, $H \neq \{id\}$. Пусть $id \neq \sigma \in H$. Возможны два случая:

1) Если у σ есть неподвижная точка. Без ограничения общности $\sigma(n) = n$. Тогда в A_n есть подгруппа A_{n-1} (из всех элементов, оставляющих n неподвижным). Более того $H \cap A_{n-1} \ni \sigma$, то есть $\{id\} \neq H \cap A_{n-1} \triangleleft A_{n-1}$. Тогда по предположению индукции $H \cap A_{n-1} = A_{n-1}$, в частности $(1\ 2\ 3) \in H$. Тогда $(1\ 2\ 3) \in H$, то есть все тройные циклы лежат в H и они порождают всю A_n , то есть $H = A_n$, что нам и нужно.

2) У σ нет неподвижных точек. Тогда рассмотрим разложение σ в произведение независимых циклов. Возможны 2 случая:

а) $\sigma = (1\ 2)(3\ 4\ \dots) \dots$ (без ограничения общности). Положим $\sigma' = \sigma^{(4\ 5\ 6)} = (1\ 2)(3\ 6\ \dots) \dots \neq \sigma$. Тогда $id \neq \sigma' \cdot \sigma^{-1}$ и $\sigma' \cdot \sigma^{-1}(1) = 1 \Rightarrow \sigma' \cdot \sigma^{-1}$ — не тождественный элемент из H , оставляющий на месте 1, то есть имеет место пункт 1.

б) $\sigma = (1\ 2\ 3\ \dots) \dots$, причем первый цикл не оканчивается на 4 (так как элементов 6). Тогда положим $\sigma' = \sigma^{(1\ 2)(3\ 4)} = (2\ 1\ 4) \dots$. Теперь $\sigma\sigma'(2) = 2$, $\sigma\sigma' \in H$, а также $\sigma\sigma'(1) = \sigma(4) \neq 1$. В этом случае снова получаем условие пункта 1.

Итого, A_n — простая. \square

Замечание. Существуют и другие простые группы, к примеру $SO_3(\mathbb{R})$ — группа преобразований пространства, сохраняющих ориентацию. Также при $n \geq 3$ или $|F| \geq 3$ проста группа $PSL_n(F) = SL_n(F)/Z(SL_n(F))$.

Замечание. Современная классификация простых конечных групп претендует на полноту, однако суммарный объем статей, в которых изложены все доказательства имеет порядок 10^4 страниц.

Лекция 10. Свободные группы и образующие соотношения

29. ПОСТРОЕНИЕ СВОБОДНЫХ ГРУПП

Определение. Группа $F_n = (f_1, \dots, f_n)$ называется свободной группой со свободными порождающими f_1, \dots, f_n , если для любой группы G и любых $g_1, \dots, g_n \in G$ существует гомоморфизм $\varphi: F_n \mapsto G$, такой, что $\varphi(f_i) = g_i$

Замечание. Гомоморфизм будет единственным, так как он задан образами порождающих однозначно.

Замечание. Построим свободную группу F_n . Зафиксируем f_1, \dots, f_n — буквы, F_n — все конечные последовательности над алфавитом $\Sigma = \{f_1, \dots, f_n, f_1^{-1}, \dots, f_n^{-1}\}$, в которых для любого $1 \leq i \leq n$ буквы f_i и f_i^{-1} не стоят рядом.

Произведение слов определим как их конкатенацию с последующим сокращением.

Пример. $f_1 f_2 f_1^{-1} \in F_2$. $f_1 f_2 f_2^{-1} f_3 \notin F_3$. $(f_1 f_2) \cdot (f_2^{-1} f_3) = f_1 f_3$.

Теорема. Построенное F_n является группой.

Доказательство.

- (1) Пустое слово \emptyset является нейтральным элементом.
- (2) Обратным элементом к слову $w = a_1 \cdot \dots \cdot a_k$ будет $w^{-1} = a_k^{-1} \cdot \dots \cdot a_1^{-1}$
- (3) Осталось проверить ассоциативность операции. Для этого покажем, что если $A \in \Sigma^*$, то сокращая подряд стоящие обратные в произвольной последовательности, мы получим один и тот же результат. Сделаем это индукцией по $|A|$.

База $|A| < 2$ очевидна. Покажем переход. Если в слове $|A|$ возможно единственное сокращение, то переход верен.

Пусть A имеет вид $A = \dots x x^{-1} \dots y y^{-1} \dots$, причем, сокращая первую пару, мы получаем A_1 , вторую — A_2 . По предположению индукции в них вычеркивание проводится однозначно. Заметим, что слова, которые получаются из слова A_3 (в котором мы провели одновременное сокращение), получаются из обоих слов A_1 и A_2 . При этом для A_3 также верно предположение. Значит из A_1 и A_2 получаются одинаковые слова.

Итак, какое бы вычеркивание ни было первым, результат определен однозначно, что доказывает шаг индукции.

Теперь ассоциативность операции можно показать, рассмотрев слово $w_1 w_2 w_3$. Так как любые последовательности сокращений приводят к одинаковому результату, то $(w_1 w_2) w_3 = w_1 (w_2 w_3)$. \square

Теорема. Построенная F_n является свободной группой со множеством свободных порождающих $\{f_1, \dots, f_n\}$

Доказательство. Рассмотрим произвольную группу G и элементы $g_1, \dots, g_n \in G$. Определим отображение $\varphi: F_n \mapsto G$ формулой

$$\varphi(f_{i_1}^{p_1} \cdot \dots \cdot f_{i_k}^{p_k}) = g_{i_1}^{p_1} \cdot \dots \cdot g_{i_k}^{p_k}$$

Тогда $\varphi(f_i) = g_i$, а также $\varphi(w_1)\varphi(w_2) = g_{i_1}^{p_1} \cdots g_{i_k}^{p_k} \cdot g_{j_1}^{q_1} \cdots g_{j_l}^{q_l} = \varphi(w_1 w_2)$ после сокращения, то есть φ — гомоморфизм.

Итого, F_n — свободная группа. \square

Замечание. Если F_n — свободная группа со свободными порождающими f_1, \dots, f_n , то у нее могут быть и другие наборы свободных порождающих.

Упражнение. Показать, что множество $\{f_1, \dots, f_{n-1}, f_{n-1}f_n\}$ является множеством свободных порождающих для F_n .

Теорема. Пусть G_n, F_n — свободные группы со свободными порождающими g_1, \dots, g_n и f_1, \dots, f_n соответственно. Тогда $G_n \cong F_n$, причем существует изоморфизм $\varphi : F_n \mapsto G_n$, такой что $\varphi(f_i) = g_i$.

Доказательство. По определению существует гомоморфизмы $\varphi : F_n \mapsto G_n$, $\varphi(f_i) = g_i$ и $\psi : G_n \mapsto F_n$, $\psi(g_i) = f_i$. Тогда $\varphi \circ \psi(g_i) = g_i$, то есть $\varphi \circ \psi = id_{G_n}$. Аналогично, $\psi \circ \varphi = id_{F_n}$, из чего следует, что φ и ψ — биекции, то есть φ — искомый изоморфизм. \square

Пример. $F_1 \cong (f_1) \cong \mathbb{Z}$. При $n \geq 2$ F_n не абелева, так как есть гомоморфизм в S_3 , где есть два некоммутирующих элемента.

Замечание. Если F_n есть какое-то свойство, то оно есть во всех группах.

Упражнение. Доказать, что F_n неразрешима при $n \geq 2$.

Упражнение. Рассмотрим группу $SL_2(\mathbb{Z}[x])$ и подгруппу $G = \left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \right)$. Доказать, что $G \cong F_2$.

30. ОБРАЗУЮЩИЕ СООТНОШЕНИЯ

Определение. Пусть $F_n = (f_1, \dots, f_n)$ — свободная группа со своими свободными образующими. Пусть $w_1(f_1, \dots, f_n), \dots, w_k(f_1, \dots, f_n)$ — некоторое множество слов. Пусть $F_n \triangleright K = (w_1, \dots, w_k)_n$.

Говорят, что группа $G = (a_1, \dots, a_n)$ задана соотношениями $w_1(a_1, \dots, a_n), \dots, w_k(a_1, \dots, a_n)$, если существует гомоморфизм $\varphi : F_n \mapsto G$, $\varphi(f_i) = a_i$, такой что $\ker \varphi = K$.

Замечание. Подразумевается, что все слова $w_i(a_1, \dots, a_n)$ равны нейтральному элементу, а $\ker \varphi = K$ указывает на то, что других соотношений нет.

Так как φ — сюръективно, то $G \cong F_n/K$.

Мы будем обозначать описанную группу через $G = (a_1, \dots, a_n \mid w_1 = \dots = w_k = e)$. В частности $F_n = (f_1, \dots, f_n)$ — свободная группа без соотношений.

Теорема. Если $G = (g_1, \dots, g_n \mid w_1 = \dots = w_k = e)$, H — группа, причем $\exists h_1, \dots, h_n \in H : w_1(h_1, \dots, h_n) = \dots = w_k(h_1, \dots, h_n) = e$, то существует гомоморфизм $\varphi : G \mapsto H$, $\varphi(g_i) = h_i$.

Доказательство. По определению свободной группы получаем $\Theta : F_n \mapsto H$, $\Theta(f_i) = h_i$. Теперь

$$\Theta(w_i(f_1, \dots, f_n)) = w_i(h_1, \dots, h_n) = e \Rightarrow w_i(f_1, \dots, f_n) \in \ker \Theta$$

Тогда и $K \subset \ker \Theta$. По второй теореме о гомоморфизмах получаем $Im \Theta \cong F_n / \ker \Theta \cong (F_n / K) / (\ker \Theta / K)$.

Поскольку $F_n / K \cong G$, то существует гомоморфизм $\psi : G \mapsto Im \Theta$, $\ker \psi = \ker \Theta / K$ (естественный эпиморфизм).

При этом $\psi(g_i) = \psi(f_i K) = f_i \cdot \ker \Theta = h_i$, что и требовалось доказать. \square

31. ПРИМЕРЫ ЗАДАНИЯ ГРУПП ОБРАЗУЮЩИМИ СООТНОШЕНИЯМИ

Пример. $G = (a, b \mid a^2 = b^2 = (ab)^2 = e)$

Произвольный элемент $g \in G$ имеет вид $g = a^{\alpha_1} b^{\beta_1} \dots a^{\alpha_k} b^{\beta_k}$, $\alpha_i, \beta_i \in \mathbb{Z}$. Раз $a^2 = b^2 = e$, то можно считать, что $\alpha_i, \beta_i \in \{0, 1\}$, то есть $g = abab\dots$ или $g = baba\dots$. Далее, $(ab)^2 = e \Rightarrow ab = b^{-1}a^{-1} = ba$, то есть $g = a^\alpha b^\beta$, $\alpha, \beta \in \{0, 1\}$. Значит, $|G| \leq 4$, так как она исчерпывается элементами $\{e, a, b, ab\}$.

Теперь рассмотрим $H = \mathbb{Z}_2 \times \mathbb{Z}_2$. Рассмотрим $a' = (1, 0)$, $b' = (0, 1)$. Тогда $(a')^2 = (b')^2 = (a'b')^2 = e$. Значит, существует гомоморфизм $\varphi : G \mapsto H$, $\varphi(a) = a'$, $\varphi(b) = b'$. Так как $H = (a', b')$, то $\varphi(G) = H$, то $|G| \geq 4 \Rightarrow |G| = 4$.

Значит φ является изоморфизмом и $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Пример. $Q_8 = (a, b \mid a^4 = e, b^2 = a^2, bab^{-1} = a^{-1})$

Рассуждая аналогично, используя то, что $ba = a^{-1}b$, а также что a и b имеют конечный порядок, получаем, что произвольный элемент g можно представить в виде $g = a^\alpha b^\beta$, $\alpha, \beta \in \{0, 1, 2, 3\}$. Далее, $b^2 = a^2$, поэтому можно считать, что $\beta \in \{0, 1\}$. Итак, $|G| \leq 8$.

Построим явно группу G . Для этого рассмотрим $H < GL_2(\mathbb{C})$, $H = \left(\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right)$.

Легко проверить, что

$$(a')^4 = E, (b')^2 = (a')^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, b'a'(b')^{-1} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = (a')^{-1}$$

Значит, существует гомоморфизм $\varphi : G \mapsto H$, $\varphi(a) = a'$, $\varphi(b) = b'$. Так как они порождают H , то $|Q_8| \geq |H| \geq 8 \Rightarrow |Q_8| = 8$, φ — изоморфизм, $Q_8 \cong H$.

Замечание. Не существует алгоритма, который по определяющим соотношениям определяет строение группы.

Лекция 11. Теоремы Силова

32. ТЕОРЕМЫ СИЛОВА

Замечание. Пусть G — конечная группа порядка n . При каких k в G есть подгруппа порядка k ?

Не для любого делителя n найдется группа такого порядка.

Пример. Пусть $G = A_4$. Тогда в G нет подгруппы порядка 6. Пусть $H < A_4$, $|H| = 6$. Тогда $|A_4 : H| = 2 \Rightarrow H \triangleleft A_4$. Пусть тогда φ — канонический гомоморфизм, $\varphi : A_4 \mapsto A_4/H$.

Теперь $\text{ord}(i j k) = 3 \Rightarrow \varphi((i j k)) = e$. Поскольку A_4 порождается тройными циклами, то $\varphi(A_4) = \{e\}$. Однако, это противоречит тому, что $\varphi(A_4) \cong A_4/H$.

Определение. Пусть G — конечная группа, $|G| = n = p^k \cdot t$, $t \not\equiv 0 \pmod{p}$. Тогда подгруппа порядка p^k называется *силовской p -подгруппой* G .

Теорема. (Силов) Пусть G — конечная группа, $|G| = n$, $p \mid n$. Тогда верны следующие три теоремы Силова:

- (1) В G существует силовская p -подгруппа.
- (1') Любая p -подгруппа G лежит в некоторой силовской p -подгруппе.
- (2) Все силовские p -подгруппы сопряжены между собой
- (3) Пусть N_p — количество силовских p -подгрупп G . Тогда $N_p \equiv 1 \pmod{p}$

Доказательство. Сперва докажем, что из (1) следует (1') и (2).

Пусть $P < G$ — некоторая p -подгруппа ($|P| = p^i$), а $Q < G$ — силовская p -подгруппа. Рассмотрим действие P на множестве смежных классов $\Omega = G/Q$ левыми сдвигами: если группа действует левыми сдвигами, то и подгруппа тоже.

Пусть $n = p^k \cdot t$, $t \not\equiv 0 \pmod{p}$. Тогда $|Q| = p^k$, $|\Omega| = t$. Рассмотрим разбиение Ω на орбиты: $\Omega = \Omega_1 \sqcup \dots \sqcup \Omega_s$ и пусть $a_i Q \in \Omega_i$. Тогда

$$|\Omega| = \sum_{i=1}^s |\Omega_i| = \sum_{i=1}^s |P : St_p(a_i Q)|$$

Раз $|P| = p^i$, то $|P : St_p(a_i Q)|$ — это степень p . С другой стороны $|\Omega| \not\equiv 0 \pmod{p}$. Значит $\exists j : |P : St_p(a_j Q)| = p^0 = 1 = |\Omega_j|$.

Итак, $\Omega_j = \{a_j Q\}$, значит $Pa_j Q = a_j Q \Rightarrow P \cdot a_j Q a_j^{-1} = a_j Q a_j^{-1}$. Однако $a_j Q a_j^{-1}$ сопряжена с силовской p -подгруппой, то есть тоже является силовской p -подгруппой. $P \cdot R = R \Rightarrow P \subset R$, откуда вытекает утверждение (1')

Если P — силовская p -подгруппа, то, рассуждая аналогично, получим, что $P \subset a_j Q a_j^{-1}$. Учитывая, что $|P| = |Q|$, получаем, что $P = a_j Q a_j^{-1}$, то есть утверждение (2).

Теперь докажем (1) и (3). Пусть опять $n = p^k \cdot t$, $t \not\equiv 0 \pmod{p}$. Положим $|\Omega| = \{A \subset G : |A| = p^k\}$. Тогда $|\Omega| = C_n^{p^k} = D$. Далее, группа G действует на Ω левыми сдвигами. Рассмотрим разбиение действия на орбиты $\Omega = \Omega_1 \sqcup \dots \sqcup \Omega_l$ и выберем $A_i \in \Omega_i$. Распишем формулу орбит

$$|\Omega| = \sum_{i=1}^l |\Omega_i| = \sum_{i=1}^l |G : St_G(A_i)|$$

Изучим $H_i = St_G(A_i) < G$. По определению, $H_i A_i = A_i$. Тогда $\forall a \in A_i \rightarrow H_i a \subset A_i$. Это значит, что A_i — объединение нескольких правых смежных классов по H_i . Так как $|A_i| = p^k$, то $|H_i| \mid |A_i|$, то есть $|H_i| = p^{\alpha_i}$. Тогда $|G : H_i| = t \cdot p^{k-\alpha_i}$ — делится на p , если $k > \alpha_i$. Итак, если H_i — не силовская, то $|G : H_i|$ кратен p , иначе A_i — правый смежный класс по H_i , то есть $A_i = H_i g$, $\Omega_i = \{b H_i g, b \in G\}$.

Пусть теперь H_1, \dots, H_m — силовские, а H_{m+1}, \dots, H_l — нет. Тогда $|\Omega| \equiv m \cdot t \pmod{p}$. Заметим, что если H_i — силовская, то в $\Omega_i \ni g^{-1} A_i = g^{-1} H_i g$ — силовская подгруппа, причем только одна. Если же Q — силовская, то ее орбита — это ее левые смежные классы, значит в орбите ровно t элементов и $St_G(Q)$ — силовская подгруппа.

Итак, орбит $\Omega_1, \dots, \Omega_m$ столько же, сколько силовских подгрупп, $m = N_p$. Тогда $D \equiv t \cdot N_p \pmod{p}$. Причем N_p зависит от группы, а все остальное только от n .

Тогда рассмотрим группу \mathbb{Z}_n . В ней ровно одна силовская подгруппа $t \cdot \mathbb{Z}_n$. Значит $D \equiv t \pmod{p}$. Тогда и для любой группы G верно $t \cdot N_p \equiv D \equiv t \pmod{p}$.

В итоге, $N_p \equiv 1 \pmod{p}$, что доказывает утверждения (1) и (3). \square

33. СТРОЕНИЕ СИЛОВСКИХ p -ПОДГРУПП

Утверждение. Пусть $p \neq q$ — простые числа, $|G| = pq$. Тогда G — не простая.

Доказательство. Пусть $p > q$. В G есть силовская p -подгруппа P , $|P| = p$. Более того, все силовские p -подгруппы сопряжены, то есть имеют вид $g^{-1}Pg$. G действует на силовские p -подгруппы сопряжением, причем это действие транзитивно. Значит $N_p = \frac{|G|}{|St_G(P)|}$, то есть $N_p \mid |G|$. С другой стороны $N_p \equiv 1 \pmod{p}$, а такой делитель у pq только один.

Итого $N_p = 1$, то есть $\forall g \in G \rightarrow g^{-1}Pg = P$, а значит $P \triangleleft G$. \square

Замечание. Поскольку $St_G(P) > P$, то $N_p \mid \frac{|G|}{|P|}$.

Замечание. Пусть $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, P_1, \dots, P_k — силовские подгруппы. Исследуем вопрос, когда $G \cong P_1 \times \dots \times P_k$?

Теорема. Пусть G — группа, $|G| = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$, P_1, \dots, P_k — силовские подгруппы соответствующих порядков. Тогда следующие утверждения равносильны

$$(1) G = P_1 \times \dots \times P_k$$

$$(2) \forall i \in [k] \rightarrow P_i \triangleleft G$$

$$(3) \forall i \in [k] \rightarrow N_{p_i} = 1$$

Доказательство. Покажем, что (2) эквивалентно (3).

Если $P_i \triangleleft G$, то $g^{-1}P_i g = P_i$, то есть $N_{p_i} = 1$, так как все силовские p -подгруппы сопряжены. Если же P_i — не нормальная, то $\exists g \in G : g^{-1}P_i g \neq P_i$, то есть существует хотя бы две силовских p -подгруппы.

Из (1) немедленно следует (2), так как $P_i \triangleleft P_1 \times \dots \times P_k$.

Обратное следствие покажем индукцией по k . При $k = 1$ утверждение тривиально.

Переход: поскольку $P_1, \dots, P_{k-1} \triangleleft G$, то $H = P_1 \cdot \dots \cdot P_{k-1} \triangleleft G$ (по следствию из первой теоремы о гомоморфизмах), причем $|H| = p_1^{\alpha_1} \cdot \dots \cdot p_{k-1}^{\alpha_{k-1}}$, так как порядок H делится на порядок сомножителей.

По предположению индукции, так как $P_1, \dots, P_{k-1} \triangleleft H$, то $H = P_1 \times \dots \times P_{k-1}$. Далее, $H \triangleleft G$, $P_k \triangleleft G$, $H \cdot P_k = P_1 \cdot \dots \cdot P_k = G$ и при этом $|H \cap P_k| \mid \gcd(|H|, |P_k|) = 1$. Тогда по критерию разложения в прямое произведение, получаем $G \cong P_1 \times \dots \times P_k$, что и требовалось показать. \square

Теорема. Пусть G — группа, $|G| = p^n \cdot t$, $t \not\equiv 0 \pmod{p}$, $0 \leq i \leq n$. Тогда в G есть группа порядка p^i .

Доказательство. Пусть K — силовская p -подгруппа в G , найдем ее подгруппу $H < K$, $|H| = p^i$. Проведем индукцию по n .

База при $n = 0, 1$ тривиальна.

Переход: положим $n \geq 2$, $i \geq 1$. Так как центр любой p -группы нетривиален, то $Z(K) \neq \{e\}$, то есть $\exists g \in Z(K)$, $g \neq e$. $\text{ord } g = p^j \Rightarrow \text{ord } g^{p^{j-1}} = p$.

Пусть $x = g^{p^{j-1}}$, а $L = \langle x \rangle$, $|L| = p$ и $L \triangleleft K$, так как $L < Z(K)$. Так как $L \triangleleft K$, то $|K/L| = p^{n-1}$ и в K/L существует подгруппа H_1 порядка p^{i-1} по предположению индукции. Пусть $\pi : K \rightarrow K/L$ — канонический эпиморфизм и положим $H = \pi^{-1}(H_1)$. Тогда $H < K$ и $|H_1| \cdot |L| = p^i$, что доказывает переход. \square

Упражнение. Пусть $|G| = p^n \cdot t$, $t \not\equiv 0 \pmod{p}$, $H < G$, $|H| = p^i$, $i < n$. Доказать, что H лежит в подгруппе порядка p^{i+1} .

Замечание. Подгруппы порядка p^i не обязаны быть изоморфными и тем более сопряженными. Пример можно найти в $\mathbb{Z}_p \times \mathbb{Z}_p$.

Лекция 12. Конечнопорожденные абелевы группы

34. КОНЕЧНОПОРОЖДЕННЫЕ АБЕЛЕВЫ ГРУППЫ И ИХ БАЗИСЫ

Определение. Группа называется k -*порожденной*, если она порождена k элементами. Группа называется конечнопорожденной, если $\exists k \in \mathbb{N}$, такое что она k -порождена.

Замечание. Работая с абелевыми группами, мы будем использовать аддитивную нотацию.

Утверждение. Пусть A_1, \dots, A_n — циклические абелевы группы. Тогда их прямая сумма абелева и конечнопорождена.

Доказательство. $G = A_1 \oplus \dots \oplus A_n$, очевидно, абелева.

Если $A_i = (a_i)$, то $G = ((a_1, 0, \dots, 0), \dots, (0, \dots, 0, a_n))$. □

Замечание. $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ при $\gcd(n, m) = 1$. Отметим, что такое разложение не единственно.

Оказывается, что обратное к этому утверждению верно. Далее, мы докажем это.

Определение. Пусть G — абелева группа, $g_1, \dots, g_k \in G$. Система элементов (g_1, \dots, g_k) называется *независимой*, если для любых целых n_1, \dots, n_k из равенства $\sum_{i=1}^k n_i g_i = 0$ следует, что $\forall i \in [k] \rightarrow n_i = 0$.

В противном случае система называется *зависимой*.

Определение. Независимая система (g_1, \dots, g_k) называется *базисом* абелевой группы G , если G порождена этой системой.

Лемма. Пусть G порождена некоторыми элементами $G = (a_1, \dots, a_k)$, пусть (b_1, \dots, b_n) — независимая в G система. Тогда $n \leq k$.

Доказательство. Любой $b_i \in G$ выражается через (a_1, \dots, a_k) , то есть $(b_1, \dots, b_n) = (a_1, \dots, a_k) \cdot B$, $B \in M_{k \times n}(\mathbb{Z})$.

Пусть $n > k$. Тогда столбцы матрицы ЛЗ над \mathbb{Q} , то есть $B \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$, $\alpha_i \in \mathbb{Q}$, $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \neq 0$.

Домножим на НОК знаменателей дробей, считаем, что $\alpha_i \in \mathbb{Z}$.

Тогда $(b_1, \dots, b_n) \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = (a_1, \dots, a_k) B \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$, то есть элементы (b_1, \dots, b_n) — зависимы, противоречие. □

Замечание. Если в абелевой группе G есть два базиса, то они равномощны.

Доказательство. Если (a_1, \dots, a_k) и (b_1, \dots, b_n) — базисы, то $n \leq k$ и $k \leq n$. □

Замечание. Но мы еще не доказали, почему хотя бы один базис существует.

35. ГРУППЫ БЕЗ КРУЧЕНИЯ

Определение. Абелева группа G называется абелевой группой *без кручения*, если в ней нет нетривиальных элементов конечного порядка.

Теорема. Любая конечно порожденная абелева группа без кручения обладает базисом.

Доказательство. Выберем наименьший набор порождающих (a_1, \dots, a_k) . Если существует такое независимое множество, то оно и является базисом. Положим, что любое k -элементное порождающее множество зависимо, то есть существует соотношение

$$\sum_{i=1}^k n_i a_i = 0$$

Из всех таких систем и всех соотношений выделим систему с соотношением $n_1 a_1 + \dots + n_k a_k = 0$, $|n_1| \neq 0$, $|n_1|$ — минимальным (всегда можно переставить порождающие)

1) $|n_1| = 1$. $a_1 + \sum_{i=2}^k n_i a_i = 0 \Rightarrow a_1 = -\sum_{i=2}^k n_i a_i$, то есть (a_2, \dots, a_k) порождает G , что противоречит минимальности k .

2) $|n_1| > 1$. Можно считать $n_1 > 0$, так как можно домножить на -1 .

Заметим, что все n_i делятся на n_1 . Если это не так, то скажем $n_2 = qn_1 + r$, $q \in \mathbb{Z}$, $0 < r < n_1$. Положим $a'_1 = a_1 + qa_2$.

Тогда (a'_1, a_2, \dots, a_k) порождают всю группу (так как $a_1 = a'_1 - qa_2$) и при этом

$$0 = n_1 a_1 + \dots + n_k a_k = n_1 a_1 + (qn_1 a_2 + r a_2) + \dots + n_k a_k = n_1 a'_1 + r a_2 + \dots + n_k a_k$$

Получили зависимость с коэффициентом $0 < r < n_1$. Противоречие с минимальностью n_1 .

Итак, $n_i = q_i n_1$, $q_i \in \mathbb{Z}$. Но тогда $0 = \sum_{i=1}^k n_i a_i = n_1 \sum_{i=1}^k q_i a_i$. Поскольку группа без кручения, то

$$0 = \sum_{i=1}^k q_i a_i = a_1 + \sum_{i=2}^k q_i a_i. \quad \text{Это противоречит минимальности } n_1. \quad \square$$

Замечание.

(1) По сути в доказательстве предъявлен алгоритм поиска базиса

(2) Можно заметить из доказательства, что любой набор из наименьшего количества порождающих элементов является базисом.

(3) Однако не любой набор из k независимых элементов — базис.

Пример. $G = \mathbb{Z}$, набор $\{2\}$.

Замечание. Как следствие, любая конечнопорожденная абелева группа без кручения изоморфна \mathbb{Z}^k при $k \in \mathbb{Z}_+$

Доказательство. Пусть (a_1, \dots, a_k) — базис в группе.

Тогда определим $\varphi : \mathbb{Z}^k \mapsto G$, $\varphi(n_1, \dots, n_k) = \sum_{i=1}^k n_i a_i$. Очевидно, φ — гомоморфизм. Тогда

Ит $\varphi = G$, так как она порождена базисом. С другой стороны если $(n_1, \dots, n_k) \in \ker \varphi$, то (a_1, \dots, a_k) зависимы с этими коэффициентами. Из того, что это базис, получаем $n_1 = \dots = n_k = 0 \Rightarrow \ker \varphi = 0$. Поэтому φ — гомоморфизм. \square

Замечание. Без условия конечнопорожденности теорема и следствие неверны, даже если разрешить бесконечные базисы.

Пример. $(\mathbb{Q}, +)$. В этой группе нет пары независимых элементов, но она не обладает базисом.

36. СТРОЕНИЕ КОНЕЧНОПОРОЖДЕННЫХ АБЕЛЕВЫХ ГРУПП

Теорема. Пусть $A = \mathbb{Z}^k$ с базисом $a_i = \left(0, \dots, 0, \underbrace{1}_i, 0, \dots, 0\right)$. Тогда для любой абелевой группы B и любых ее элементов b_1, \dots, b_k \exists гомоморфизм $\varphi: A \mapsto B$ такой, что $\varphi(a_i) = b_i$.

Замечание. В силу этой теоремы группа A называется *свободной абелевой группой*.

Доказательство. Положим $\varphi(n_1, \dots, n_k) = \sum_{i=1}^k n_i b_i$. Тогда очевидно, что φ — гомоморфизм и $\varphi(a_i) = b_i$. \square

Замечание. Если F_k — свободная группа ранга k , то $F_k/F'_k \cong \mathbb{Z}^k$

Доказательство. $F'_k = ([f_i, f_j] : 1 \leq i, j \leq k)_n$, где $F_k = (f_1, \dots, f_k)$.

Значит, $F_k/F'_k = (b_1, \dots, b_k \mid [b_i, b_j] = e, 1 \leq i, j \leq k)$. В группе \mathbb{Z}^k мы имеем $[a_i, a_j] = e$. Значит существует гомоморфизм $\varphi: F_k/F'_k \mapsto \mathbb{Z}^k$, причем $\varphi(b_i) = a_i$. С другой стороны F_k/F'_k — абелева группа, так что существует гомоморфизм $\psi: \mathbb{Z}^k \mapsto F_k/F'_k$, $\psi(a_i) = b_i$. Тогда $\varphi \circ \psi(a_i) = a_i$, $\psi \circ \varphi(b_i) = b_i \Rightarrow \varphi \circ \psi = id_{\mathbb{Z}^k}$, $\psi \circ \varphi = id_{F_k/F'_k}$. Значит φ и ψ — взаимно обратные изоморфизмы. \square

Утверждение. Пусть B — k -конечно порожденная абелева группа. Тогда $\exists N < \mathbb{Z}^k : B \cong \mathbb{Z}^k/N$.

Доказательство. Если B порождена b_1, \dots, b_k , то $\exists \varphi: \mathbb{Z}^k \mapsto B$, $\varphi(a_i) = b_i \Rightarrow Im \varphi = B \cong \mathbb{Z}^k / ker \varphi$. \square

Теорема. Пусть $A = \mathbb{Z}^k$ и $B < A$, тогда B — конечнопорождена, более того, в A и B существуют базисы (a_1, \dots, a_k) и (b_1, \dots, b_l) , $l \leq k$, такие, что $b_i = m_i a_i$, $m_i \in \mathbb{Z}$, причем $m_1 \mid m_2 \mid \dots \mid m_l$.

Замечание. Такие базисы обычно называются *согласованными*.

Доказательство. Индукция по k .

Если $k = 1$, то $A = \mathbb{Z}$, $B = m\mathbb{Z}$ и $a_1 = 1$, $b_1 = m$, если $m \neq 0$ или $l = 0$, если $m = 0$.

Пусть $k > 1$ и $B \neq 0$ (иначе все тривиально). Докажем переход:

Выберем базис a_1, \dots, a_k в A и $0 \neq b \in B$, так чтобы $b = \sum_{i=1}^k n_i a_i$, причем $n_1 \neq 0$ и $|n_1|$ — минимален.

(1) n_i делится на n_1 при всех $1 \leq i \leq k$. Пусть это не так, и $n_2 = qn_1 + r$, $q \in \mathbb{Z}$, $0 < r < |n_1|$. Тогда положим $a'_1 = a_1 + qa_2$ и тогда $b = na'_1 + ra_2 + \dots + n_k a_k$, причем $0 < r < |n_1|$, при этом (a'_1, a_2, \dots, a_k) — базис в A . Противоречие с минимальностью $|n_1|$.

Положим $a'_1 = a_1 + \frac{n_2}{n_1} a_2 + \dots + \frac{n_k}{n_1} a_k$, тогда (a'_1, a_2, \dots, a_k) — базис в A , поскольку $a_1 = a'_1 - \frac{n_2}{n_1} a_2 - \dots - \frac{n_k}{n_1} a_k$ и $b = n_1 a'_1$.

(2) Пусть теперь $b' \in B$, $b' = d_1 a'_1 + \sum_{i=2}^k d_i a_i$. Тогда d_1 делится на n_1 . Если это не так, то $d_1 = qn_1 + r$, $q \in \mathbb{Z}$, $0 < r < |n_1|$. Рассмотрим в B элемент $b'' = b' - qb$. Тогда

$$b'' = (d_1 - qn_1) a'_1 + \sum_{i=2}^n d_i a_i = r a'_1 + \sum_{i=2}^k d_i a_i = r a'_1 + \sum_{i=2}^k d_i a_i \neq 0$$

Снова получаем противоречие с выбором n_1 . Итак, d_1 кратно n_1 .

(3) d_i : n , $1 \leq i \leq k$. Рассмотрим в B элемент $c = b' - tb$, где $t = \frac{d_1}{n_1} - 1$. Тогда $c = n_1 a'_1 + \sum_{i=2}^k d_i a_i \neq$

0. Применяя рассуждения пункта (1), получаем, что d_i : n_1 .

Обозначим через A' группу, порожденную a_2, \dots, a_k , а через $B' = A' \cap B$. Тогда $A = (a'_1) \oplus A'$, ибо $(a'_1) \cap A' = 0$, $(a'_1) + A' = A$.

Далее $B = (b) \oplus B'$. Действительно $(b) \cap B' = 0$, так как $b \in (a'_1)$, $B' \subset A'$. С другой стороны если $b' \in B$, то $b' = d_1 a'_1 + \sum_{i=2}^k d_i a_i = \frac{d_1}{n_1} \cdot b + \underbrace{\sum_{i=2}^k d_i a_i}_{B \cap A'}$. Значит $b' \in (b) + B'$. Итак, $(b) + B' = B$,

что влечет $B = (b) \oplus B'$.

При это $A' \cong \mathbb{Z}^{k-1}$, значит в A' существуют согласованные базисы $(a'_2, a'_3, \dots, a'_k)$ и (b_2, \dots, b_l) , где $b_i = m_i a'_i$. Тогда $(a'_1, a'_2, \dots, a'_k)$ — базис в A , а (b, b'_2, \dots, b'_l) (положим $b'_1 = b$), и $b_i = m_i a'_i$, где $m_1 = n_1$. Кроме того, $m_2 \mid \dots \mid m_k$. Осталось доказать, что $m_1 \mid m_2$.

Рассмотрим $b'_2 \in B' \subset A' \Rightarrow b'_2 = \sum_{i=2}^k d_i a_i = n_1 \cdot \underbrace{\sum_{i=2}^k \frac{d_i}{n_1} a_i}_{\in A'} = n_1 \cdot \sum_{i=2}^k d'_i a'_i$. С другой стороны,

$$b'_2 = m_2 a'_2.$$

Так как (a'_1, \dots, a'_k) — базис, разложения совпадают, то есть $m_2 = n_1 \cdot d_2$, значит $n_1 = m_1 \mid m_2$. \square

Замечание. Пусть G — конечнопорожденная абелева группа. Тогда $\exists k \in \mathbb{Z}_+$, целые $m_1 \mid m_2 \mid \dots \mid m_l$: $G \cong \mathbb{Z}^k \oplus \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_l}$.

Доказательство. Пусть G t -порождена. Тогда $G \cong \mathbb{Z}^t / B$, $B < \mathbb{Z}^t$. Выберем в \mathbb{Z}^t и B согласованные базисы (a_1, \dots, a_t) и (b_1, \dots, b_l) , где $b_i = m_i a_i$, $m_1 \mid \dots \mid m_l$.

Тогда $\mathbb{Z}^t = (a_1) \oplus (a_2) \oplus \dots \oplus (a_t)$, $B = (b_1) \oplus (b_2) \oplus \dots \oplus (b_l)$, $(b_i) < (a_i)$.

Значит, $G \cong \mathbb{Z}^t / B \cong (a_1) / (b_1) \oplus \dots \oplus (a_l) / (b_l) \oplus (a_{l+1}) \oplus \dots \oplus (a_t) \cong \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_l} \oplus \mathbb{Z}^{t-l}$. \square

Замечание. В доказательстве теоремы про согласованные базисы мы проводили замены базиса вида $(a_1, \dots, a_k) \mapsto (a_1 + d \cdot a_2, a_2, \dots, a_k)$. Покажем, что это базис. Действительно, он порождает всю группу, так как через него выражаются все элементы исходного базиса. Независимость следует, например, из замечания к теореме о базисе группы без кручения о том, что любой набор порождающих из минимального возможного количества элементов — базис.

Другое объяснение состоит в том, что если $n_1 a'_1 + \sum_{i=2}^k n_i a_i = 0$, то $n_1 a_1 + (d \cdot n_1 + n_2) + \sum_{i=3}^k n_i a_i = 0$, причем это тоже нетривиальная линейная комбинация.

Лекция 13. Классификация конечнопорожденных абелевых групп**37. ПРЕДСТАВЛЕНИЕ ПРИМАРНЫМИ ЦИКЛИЧЕСКИМИ ГРУППАМИ**

Теорема. Конечнопорожденная абелева группа G представима в виде

$$G \cong \mathbb{Z}^k \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\alpha_s}}, \quad k \in \mathbb{Z}_+, \quad \alpha_i \in \mathbb{N}, \quad p_i - \text{простые}$$

Замечание. Группа $G \cong \mathbb{Z}_{p^\alpha}$, где p — простое, называется примарной циклической группой.

Доказательство. Если $(n, m) = 1$, то $\mathbb{Z}_{mn} \cong \mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$. Значит, если $m = p_1^{\alpha_1} \dots p_t^{\alpha_t}$, то

$$\mathbb{Z}_m = \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \dots \oplus \mathbb{Z}_{p_t^{\alpha_t}}$$

Применяя это рассуждение к каждому \mathbb{Z}_{m_i} в представлении G , получаем требуемое. \square

Замечание. Далее мы покажем, что числа k и $p_1^{\alpha_1}, \dots, p_s^{\alpha_s}$ определены однозначно с точностью до перестановки степеней простых.

38. ПРЕДСТАВЛЕНИЕ НЕПЕРИОДИЧЕСКОЙ ЧАСТИ

Определение. Пусть G — произвольная абелева группа. Ее *периодической частью* $P(G)$ называется множество всех ее элементов конечного порядка.

$$P(G) = \{a \in G : \text{ord } a < \infty\}$$

Утверждение. Если G — абелева группа, то $P(G) < G$.

Доказательство. В самом деле, $e \in P(G)$, так как $\text{ord } e = 1$.

Если $\text{ord } a = n$, $\text{ord } b = m$, то $(ab)^{nm} = a^{nm} \cdot b^{nm} = e \cdot e = e \Rightarrow \text{ord } ab < \infty$.

Далее, если $\text{ord } a = n$, то $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e \Rightarrow \text{ord } a^{-1} < \infty$. \square

Утверждение. Пусть G — абелева группа. Тогда $G/P(G)$ — группа без кручения.

Доказательство. Пусть некоторый элемент $gP(G)$ порядка $n < \infty$. Тогда $(gP(G))^n = P(G) \Rightarrow g^n P(G) = P(G) \Rightarrow g^n \in P(G)$. Значит, элемент g^n имеет конечный порядок k в G . Тогда $g^{nk} = 0 \Rightarrow g \in P(G) \Rightarrow g \cdot P(G) = P(G)$, то есть этот элемент есть нейтральный. \square

Замечание. В неабелевой группе множество элементов конечного порядка не обязана быть подгруппой. Например, в O_3 существуют две симметрии S_1, S_2 порядка 2 относительно плоскостей π_1 и π_2 , композиция которых будет поворотом вокруг прямой $l = \pi_1 \cap \pi_2$ на угол, равный удвоенному углу между плоскостями. Если этот угол выбрать, к примеру, равным 1 радиану, то этот поворот будет иметь бесконечный порядок.

Утверждение. Пусть $G = \mathbb{Z}^k \oplus \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_l}$, где $k \in \mathbb{Z}_+$, $m_i \in \mathbb{N}$. Тогда $P(G) = (0) \oplus \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_l}$, а $G/P(G) \cong \mathbb{Z}^k$.

Доказательство. Пусть $a \in G$, $a = (a_0, \dots, a_l)$, $a_0 \in \mathbb{Z}^k$, $a_i \in \mathbb{Z}_{m_i}$. Если $a_0 = 0$, то $m_1 m_2 \dots m_l \cdot a = 0 \Rightarrow a \in P(G)$.

Если $a_0 \neq 0$, то $\text{ord } a_0 = \infty \Rightarrow \text{ord } a = \infty \Rightarrow a \notin P(G)$. Тогда $G/P(G) \cong (\mathbb{Z}^k / (0)) \oplus (\mathbb{Z}_{m_1} / \mathbb{Z}_{m_1}) \oplus \dots \oplus (\mathbb{Z}_{m_l} / \mathbb{Z}_{m_l}) \cong \mathbb{Z}^k$. \square

Утверждение. Пусть $G \cong \mathbb{Z}^{k_1} \oplus \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_l} \cong \mathbb{Z}^{k_2} \oplus \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_s}$. Тогда $k_1 = k_2$ и $\mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_l} \cong \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_s}$.

Доказательство. $\mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_s} \cong P(G) \cong \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_l}$. $\mathbb{Z}^{k_1} \cong G/P(G) \cong \mathbb{Z}^{k_2}$. Так как $\mathbb{Z}^{k_1} \cong \mathbb{Z}^{k_2}$ и в этой группе есть базисы из k_1 и k_2 элементов, то $k_1 = k_2$. \square

39. РАЗЛОЖЕНИЕ ПЕРИОДИЧЕСКОЙ ЧАСТИ

Утверждение. Пусть G — конечные абелевы группа, $p \mid |G|$, $G = \mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_k}} \oplus \mathbb{Z}_{p_1^{\beta_1}} \oplus \dots \oplus \mathbb{Z}_{p_s^{\beta_s}}$, p и p_i — простые, $p_i \neq p$. Тогда силовская p -подгруппа в G — это $H = \mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_k}} \oplus (0) \oplus \dots \oplus (0)$.

Доказательство. $|G| = p^{\alpha_1 + \dots + \alpha_n} \cdot p_1^{\beta_1} \cdot \dots \cdot p_s^{\beta_s}$. $|H| = p^{\alpha_1 + \dots + \alpha_n}$. Значит это действительно силовская p -подгруппа. \square

Замечание. В абелевой группе силовская p -подгруппа единственна, так как по второй теореме Силова, все силовские подгруппы сопряжены.

Утверждение. Пусть p — простое число, G — абелева p -группа, $G \cong \mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_k}} \cong \mathbb{Z}_{p^{\beta_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\beta_l}}$. Тогда $k = l$ и наборы $(\alpha_1, \dots, \alpha_k)$ и $(\beta_1, \dots, \beta_l)$ совпадают с точностью до перестановки.

Доказательство. Индукция по $|G|$.

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

Пусть $|G| = p^n$, $n > 1$. Положим $H = \{a \in G \mid pa = 0\}$. Тогда $H < G$.

Посмотрим на образ H при изоморфизме в $\mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_k}}$ и $\mathbb{Z}_{p^{\beta_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\beta_l}}$. В первом случае H переходит в

$$p^{\alpha_1-1}\mathbb{Z}_{p^{\alpha_1}} \oplus \dots \oplus p^{\alpha_k-1}\mathbb{Z}_{p^{\alpha_k}}$$

Отсюда, $|H| = p^k$. Аналогично, $|H| = p^l$, откуда $k = l$.

$G/H \cong (\mathbb{Z}_{p^{\alpha_1}}/p^{\alpha_1-1}\mathbb{Z}_{p^{\alpha_1}}) \oplus \dots \oplus (\mathbb{Z}_{p^{\alpha_k}}/p^{\alpha_k-1}\mathbb{Z}_{p^{\alpha_k}}) \cong \mathbb{Z}_{p^{\alpha_1-1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_k-1}} \cong \mathbb{Z}_{p^{\beta_1-1}} \oplus \dots \oplus \mathbb{Z}_{p^{\beta_l-1}}$. Применим к G/H предположение индукции. Некоторые из α_i и β_i могут быть нулями, допустим это несколько последних индексов каждой суммы. Тогда

$$G/H = \mathbb{Z}_{p^{\alpha_1-1}} \oplus \dots \oplus \mathbb{Z}_{p^{\alpha_{k'}-1}} \cong \mathbb{Z}_{p^{\beta_1-1}} \oplus \dots \oplus \mathbb{Z}_{p^{\beta_{l'}-1}}$$

И значит $k' = l'$ и $(\alpha_1, \dots, \alpha_{k'})$ совпадает с $(\beta_1, \dots, \beta_{l'})$ с точностью до перестановки, $\alpha_{k'+1} = \dots = \alpha_k = 1 = \beta_{l'+1} = \dots = \beta_l$. Это доказывает утверждение для G . \square

Теорема. Пусть G — конечнопорожденная абелева группа. Тогда $\exists k \in \mathbb{Z}_+$, простые p_1, \dots, p_l и натуральные $\alpha_1, \dots, \alpha_l$:

$$G \cong \mathbb{Z}^k \oplus \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_l^{\alpha_l}}$$

При этом число k а также набор $(p_1^{\alpha_1}, \dots, p_l^{\alpha_l})$ определены однозначно с точностью до перестановки степеней простых.

Доказательство. Существование разложения уже доказано. Число k определяется из $G/P(G)$. Также $P(G) \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_l^{\alpha_l}}$.

Если $P(G)$ представима в таком виде двумя способами, то разобьем каждую прямую сумму на части, соответствующие одному простому. Части, соответствующие одному простому изоморфны, так как они изоморфны силовской p -подгруппе в G .

В этих частях степени p_i отличаются только перестановкой по последнему утверждению. \square

Упражнение. Единственен ли набор чисел k и $m_1 \mid m_2 \mid \dots \mid m_l$, такой что $G \cong \mathbb{Z}^k \oplus \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_l}$?

Замечание. Подгруппы в G , изоморфные \mathbb{Z}^k и $\mathbb{Z}_{p^{\alpha_i}}$, однозначно не определяются.

Пример. \mathbb{Z}_p^2 — 2-мерное линейное пространство над \mathbb{Z}_p . Произвольной базис (e_1, e_2) дает нам искомое разложение, но базис можно выбрать разными способами.

Упражнение. Найти другое прямое разложение $\mathbb{Z} \oplus \mathbb{Z}_2$.

Теорема. Пусть F — поле, а $G < F^*$, $|G| < \infty$. Тогда G — циклическая.

Доказательство. Как мы знаем, $G \cong \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_l}$, где $m_1 \mid m_2 \mid \dots \mid m_l$. Это значит, что $\forall g \in G < F^* \rightarrow \text{ord } g \mid m_l$. Это означает, что $\forall g \in G \rightarrow g^{m_l} = 1$.

Таким образом, все элементы группы G являются корнями многочлена $x^{m_l} - 1$. В поле таких корней не больше, чем m_l . То есть $|G| \leq m_l \Rightarrow G \cong \mathbb{Z}_{m_l}$. \square