Lomonosov Moscow
State University

Механико-математический факультет

Алгебра, 3 семестр, 2 поток

Преподаватель:	Куликова Ольга Викторовна
Авторы:	Соколов Егор
Группа:	208
Контакт:	Мой телеграм для связи

Москва
Последняя компиляция: 16 октября 2025 г.

Содержание

1 Группы

1.1 Основные понятия

Определение. Пусть G - множество. Бинарной операцией на G называется отображение $* : G \times G \to G$.

Определение. Множество G с бинарной операцией $*$ называется группой, если выполнены следующие аксиомы:

1. $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$;
2. $\exists e \in G : \forall a \in G \quad a * e = e * a = a$;
3. $\forall a \in G \ \exists b \in G : a * b = b * a = e$

Различные формы записи группы:

1. Мультипликативная форма (терминология):
Операция - " $\cdot$ " (умножение);
Нейтральный элемент - единичный (1);
Элемент из аксиомы 3 - обратный (a^{-1} для $a \in G$);
2. Аддитивная форма (терминология):
Операция - " $+$ " (сложение);
Нейтральный элемент - нулевой (0);
Элемент из аксиомы 3 - противоположный ($-a$ для $a \in G$);

Определение. Если G - группа и $\forall a, b \in G \ a \cdot b = b \cdot a$, то G - абелева (коммутативная) группа.

Замечание. Обычно для обозначения абелевых групп будем использовать аддитивную форму записи, для иных - мультипликативную.

Утверждение (Простейшие свойства групп)**.**

1. *Единичный элемент единственный;*
2. $\forall a \in G$ *обратный к* a *элемент единственный;*
3. $(ab)^{-1} = b^{-1}a^{-1}$*;*
4. *Если* $a, b \in G$*, то решение уравнения* $ax = b$ $(xa = b)$ *единственно.*

Доказательство.

1. (От противного) Допустим, что $\exists\ e_1, e_2 \in A$ - единичные. Тогда $e_1 = e_1 * e_2 = e_2$ по определению единичного элемента.

2. Допустим $\exists\ b_1, b_2$ - обратные к a элементы: $b_1 \neq b_2$
   В силу ассоциативности:
$$b_1 * (a * b_2) = (b_1 * a) * b_2$$
$$b_1 * e = e * b_2$$
$$b_1 = b_2$$

3. $abb^{-1}a^{-1} = aea^{-1} = e$;
   $b^{-1}a^{-1}ab = b^{-1}eb = e \Longrightarrow (ab)^{-1} = b^{-1}a^{-1}$

4. $ax = b \Longleftrightarrow a^{-1}ax = a^{-1}b \Longleftrightarrow x = a^{-1}b$;
   $xa = b \Longleftrightarrow xaa^{-1} = ba^{-1} \Longleftrightarrow x = ba^{-1}$;

□

Определение. Мощность множества G называется порядком группы G.
Обозначается $|G|$.
Если $|G| < \infty$, то группа называется конечной, иначе бесконечной.

Примеры.

1. $(\mathbb{Z}, +), (\mathbb{Z}_n, +)$;

2. $GL_n(F)$ - группа невырожденных матриц порядка n с коэффициентами из поля F;

3. Пусть Ω - множество. Преобразованиями Ω назовём биекции $f : \Omega \to \Omega$.
   $S(\Omega)$ - множество всех преобразований Ω - образует группу относительно композиции.
   Если $\Omega = \{1, ..., n\}$, то $S(n) = S_n$ - группа подстановок.

4. Если $G = \{a_1, ..., a_n\}$ - конечная группа, то её можно задать с помощью таблицы умножения (таблицы Кэли).
   Например, для $Z_2 = \{0, 1\}$:

	0	1
0	0	1
1	1	0

5. Группа кватернионов: $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$
   Таблица Кэли для кватернионов:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	i	-1

Определение. Подмножество $H \subseteq G$ называется подгруппой группы G, если:

1. $\forall a, b \in H \ ab \in H$;
2. $\forall a \in H \ a^{-1} \in H$;
3. $1 \in H$ (можно заменить на $H \neq \varnothing$)

Обозначается $H \leq G$.

Утверждение. *Подгруппа H группы G является группой относительно бинарной операции группы G.*

Примеры.

1. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ ($\mathbb{N} \nleq \mathbb{Z}$, т.к. не группа);
2. $GL_n(F) \geq SL_n(F) = \{A \in GL_n(F) | \det A = 1\}$ - унимодулярная группа.
3. $GL_n(F) \geq O_n(F) \geq SO_n(F)$ ($O_n(F)$ - ортогональная группа, $SO_n(F)$ - специальная ортогональная группа);
4. $GL_n(F) \geq$ группа строго треугольных матриц.

Определение. Любая подгруппа группы $S(\Omega)$ называется группой преобразований множества Ω.

Примеры.

1. $GL(V)$ ($\leq S(V)$) - группа всех невырожденных линейных операторов векторного пространства V;
2. $Aff(\mathbb{A})$ - группа всех невырожденных аффинных преобразований аффинного пространства $\mathbb{A}$;

3. $\mathcal{E}^2$ - аффинно-евклидово двумерное пространство.
   $\mathrm{Isom}\ \mathcal{E}^2$ - группа изометрий (движений) на $\mathcal{E}^2$.
   $\mathrm{Isom}\ \mathcal{E}^2 \geq O_2 \geq SO_2$, где O_2 - группа движений, сохраняющих точку O, SO_2 - группа поворотов вокруг точки O.

4. $T \subseteq \mathcal{E}^2$ - некоторая фигура.
   $\mathrm{Sym}\ T = \{f \in \mathrm{Isom}\ \mathcal{E}^2 \mid f(T) = T\}$ - группа симметрий фигуры T.

   - Если T - окружность с центром в точке O, то $\mathrm{Sym}\ T = O_2$;
   - Если T - правильный n-угольник с центром в точке O, то $\mathrm{Sym}\ T = D_n$ - группа Диэдра.
     $|D_n| = 2n$, т.к. n поворотов и n симметрий.

Определение. Пусть $(G_1, *, e_1), (G_2, \circ, e_2)$ - группы. Отображение $\varphi : G_1 \to G_2$ - изоморфизм, если

1. φ - биекция;

2. $\forall a, b \in G_1\ \varphi(a * b) = \varphi(a) * \varphi(b)$

Если между G_1 и G_2 существует изоморфизм, то G_1 и G_2 называются изоморфными. Обозначается $G_1 \simeq G_2$.

Пример. $D_3 \simeq S_3$.

Доказательство. D_3 - группа движений, переводящая равносторонний треугольник в себя. Если пронумеровать вершины изначального треугольника, то каждый элемент группы D_3 будет соответствовать подстановке, переводящей старый порядок вершин в новый. Определение изоморфизма проверяется очевидно. □

Утверждение. *Изоморфность групп - отношение эквивалентности на множестве групп.*

Утверждение (Свойства изоморфизмов).

1. $\varphi(e_1) = e_2$*;*

2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$*;*

3. $G_1 \simeq G_2 \Longrightarrow |G_1| = |G_2|$.

   Замечание. Обратное утверждение неверно (например, $S_3 \not\simeq \mathbb{Z}_6$).

Пример. $SO_2 \simeq (U, \cdot)$, где $U = \{z \in \mathbb{C} : |z| = 1\}$.

Определение. Пусть $(G, \cdot, e)$ - группа, $k \in \mathbb{Z}, g \in G$.
Мультипликативный термин - элемент g в степени k:

$$g^k = \begin{cases} \underbrace{g \cdot g \cdot ... \cdot g}_{k}, k > 0 \\ \underbrace{g^{-1} \cdot g^{-1} \cdot ... \cdot g^{-1}}_{-k}, k < 0 \\ e, k = 0 \end{cases}$$

Определение. Пусть $(G, +, e)$ - группа, $k \in \mathbb{Z}, g \in G$.
Аддитивный термин - кратное элемента g:

$$kg = \begin{cases} \underbrace{g + g + ... + g}_{k}, k > 0 \\ \underbrace{(-g) + (-g) + ... + (-g)}_{-k}, k < 0 \\ e, k = 0 \end{cases}$$

Утверждение (Свойства $(k, m \in \mathbb{Z}, g \in G)$)**.**

1. $g^k \cdot g^m = g^{k+m}$;

2. $(g^k)^m = g^{km}$;

3. $(g^k)^{-1} = g^{-k}$.

Утверждение. *Множество всех элементов g^k, где $k \in \mathbb{Z}$, $g \in G$, образует подгруппу в G. Обозначается $\langle g \rangle = \{e, g, g^{-1}, g^2, g^{-2}, ...\}$.*

Определение. $\langle g \rangle$ - циклическая подгруппа. порождённая элементом g.

Примеры.

1. $G = \mathbb{Z} : \langle 2 \rangle = 2\mathbb{Z}$ - чётные целые числа;
2. $G = \mathbb{Z}_6 : \langle 2 \rangle = \{0, 2, 4\}$;
3. $G = \mathbb{C} : \langle i \rangle = \{\pm 1, \pm i\}$

Пусть $(G, \cdot, e)$ - группа, $g \in G$. Если $\forall k, m \in \mathbb{Z} : k \neq m \Longrightarrow g^k \neq g^m$, то $\langle g \rangle$ - бесконечная (элемент g имеет бесконечный порядок).
Если $\exists k, m \in \mathbb{Z} : k \neq m, g^k = g^m \Longrightarrow g^{k-m} = e \Longrightarrow$ существует наименьшее $n \in \mathbb{N}$ такое, что $g^n = e$ (элемент g имеет порядок n)

Определение. Порядком элемента $g \in G$ называется наименьшее натуральное число n такое, что $g^n = e$, если такое существует. Иначе говорят, что элемент g имеет бесконечный порядок. Обозначается ord g.

Примеры.

1. $G = \mathbb{Z} : \text{ord } 2 = \infty$;

2. $G = \mathbb{Z}_{12} : \text{ord } 2 = 6$;

3. $G = \mathbb{C}^* : \text{ord } 2 = \infty$
   ($\mathbb{C}^*$ - мультипликативная группа поля, $\mathbb{C} \setminus \{0\}$ относительно умножения).

Утверждение 1 (Свойства элементов конечного порядка)**.**

1. $g^m = e \Longleftrightarrow \text{ord } g \mid m$;

2. $g^m = g^l \Longleftrightarrow m \equiv l (\text{mod ord } g)$

Доказательство.

1. Разделим m на $n = \text{ord } g$ с остатком: $m = nq + r$, где $0 \leqslant r < n$. Тогда:

$$e = g^m = (g^n)^q \cdot g^r = g^r \Longrightarrow r = 0$$

   так как $r < n$, где n - минимальное натуральное число такое, что $g^n = 0$.

2. Следует из 1.

□

Следствие. ord $g = |\langle g \rangle|$

Доказательство. Если ord $g = \infty$: $\forall k \neq l \ g^k \neq g^l \Longrightarrow$ подгруппа $\langle g \rangle = \{e, g^{\pm 1}, g^{\pm 2}, ...\}$ бесконечна.
Если ord $g = n : \langle g \rangle = \{e, g^1, ...g^{n-1}\}$ - все эти элементы различны из пункта 2 утверждения, а других нет по определению порядка. □

Примеры.

1. $i \in \mathbb{C}^*$ - ord $i = 4$;

2. $\sigma \in S_n$:
   Если $\sigma = (i_1, ..., i_k)$ - цикл длины k, то ord $\sigma = k$.
   Так как любая подстановка раскладывается в произведение независимых циклов и независимые циклы коммутируют, если $\sigma = \tau_1 ... \tau_n$, где τ_i - независимые циклы, то верно: ord $\sigma =$ НОК $\{|\tau_1|, ..., |\tau_n|\}$.
   Например, $\sigma = (23)(145) \Longrightarrow$ ord $\sigma = 6$.

Утверждение 2. *Пусть* $n =$ ord g. *Тогда* ord $g^k = \frac{n}{\text{НОД}(n,k)}$.

Доказательство. Пусть ord $g^k = m$. Из утверждения 1: $g^{mk} = e \Longleftrightarrow n|mk$, откуда $\frac{n}{\text{НОД}(n,k)}|m$, т.е. $m \geqslant \frac{n}{\text{НОД}(n,k)}$. Очевидно, что при $m = \frac{n}{\text{НОД}(n,k)}$ $n|mk$. □

Определение. Множество $S \subseteq G$ называется порождающим множеством для группы G, если $\forall g \in G\ \exists s_1, ..., s_k \in S: \ g = s_1^{\varepsilon_1} ... s_k^{\varepsilon_k}$, где $\varepsilon_i = \pm 1$ (s_i не обязательно различны).
При этом говорят, что G порождается множеством S.
Если $\exists$ конечное множество S такое, что S порождает G, то G называется конечно порождённой, и бесконечно порождённой иначе.
Обозначается $\langle S \rangle = \{s_1^{\varepsilon_1} ... s_k^{\varepsilon_k} | \varepsilon_i = \pm 1\}$ - группа, порождённая S.

Примеры.

1. $S_n = \langle$все транспозиции$\rangle$;

2. $GL_n(F) = \langle$все элементарные матрицы$\rangle$

3. $Q_8 = \langle i, j \rangle$;

4. $D_n = \langle \alpha, s \rangle$, где α - поворот на $\frac{2\pi}{n}$, а s - любая из симметрий.

5. Группа Клейна: $H = \{\text{id}, a = (12)(34), b = (13)(24), c = (14)(23)\} \leq S_4$
   Это группа симметрий прямоугольника, не являющегося квадратом: a, c - симметрии относительно средних линий, b - поворот на π вокруг центра.
   Таблица Кэли для группы Клейна:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

   Отсюда $\{e, a, b, c\} = \langle a, b \rangle$.

6. $\mathbb{Q}$ - бесконечно порождённая.

1.2 Циклические группы

Определение. Группа G называется циклической, если G порождается одним элементом, т.е. $\exists g \in G : \forall h \in G\ \exists k \in \mathbb{Z} : h = g^k$. Элемент g также называется образующим элементом группы G.

Примеры.

1. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$, $\mathbb{Z}_n = \langle 1 \rangle$;

2. U_n - множество всех комплексных корней степени n из 1.
   U_n - группа относительно умножения, причём $U_n = \langle \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \rangle$.

Утверждение 3. *Если* $G = \langle g \rangle$, *то* $|G| = \operatorname{ord} g$.

Доказательство. Очевидно из определения порождающего множества. □

Замечание. Для групп конечного порядка, очевидно, выполняется и обратное утверждение: если $\operatorname{ord} g = |G| < \infty$, то $G = \langle g \rangle$.

Далее циклическую группу порядка n будем обозначать $\langle g \rangle_n$.

Утверждение 4. *Пусть* $G = \langle g \rangle_n$. *Тогда* $G = \langle g^k \rangle \Longleftrightarrow \text{НОД}(k, n) = 1$.

Доказательство. Из утверждения 3 $|G| = \operatorname{ord} g$. Тогда:

$$G = \langle g^k \rangle \Longleftrightarrow \operatorname{ord} g^k = \frac{n}{\text{НОД}(n,k)} = n \Longleftrightarrow \text{НОД}(n,k) = 1$$

□

Теорема 1 (Классификация циклических групп)**.**

1. *Если циклическая группа* G *бесконечна, то* $G \simeq \mathbb{Z}$;

2. *Если циклическая группа* G *конечна и имеет порядок* n, *то* $G \simeq \mathbb{Z}_n$.

Доказательство.

1. Пусть $\operatorname{ord} g = \infty, \forall h \in G\ \exists k \in \mathbb{Z} : h = g^k$
   Рассмотрим отображение $\varphi : G \to \mathbb{Z}$ такого вида: $\varphi : g^k \mapsto k$. Очевидно, что φ - сюръекция (в $k \in \mathbb{Z}$ перешёл $g^k \in G$).

$\varphi(g^k) = \varphi(g^m) \Longrightarrow k = m \Longrightarrow g^k = g^m$ - отсюда φ - инъекция.
Проверим сохранение операции:

$$\varphi(g^k \cdot g^m) = \varphi(g^{k+m}) = k + m = \varphi(g^k) + \varphi(g^m)$$

Отсюда φ - изоморфизм.

2. Пусть $\operatorname{ord} g = n$. Рассмотрим отображение $\varphi : \mathbb{Z}_n \to G$ такого вида: $\varphi : k \mapsto g^k$. Очевидно, что φ - сюръекция (в $g^k \in G$ перешёл $k \in \mathbb{Z}_n$).
$k \equiv m (\bmod n) \Longleftrightarrow g^k = g^m$ - отсюда φ - инъекция.
Сохранение операции - аналогично пункту 1.
Отсюда φ - изоморфизм.

$\square$

Следствие. *Если G_1, G_2 - циклические группы, то $G_1 \simeq G_2 \Longleftrightarrow |G_1| = |G_2|$.*

Доказательство.
$\Longrightarrow$: верно всегда;
$\Longleftarrow$: из теоремы: если G_1 бесконечна, то $G_1 \simeq \mathbb{Z} \simeq G_2$, иначе $G_1 \simeq \mathbb{Z}_n \simeq G_2$, где $n = |G_1| = |G_2|$. $\square$

Теорема 2.

1. *Любая подгруппа циклической группы является циклической.*
2. *Подгруппы циклической группы G порядка n находятся во взаимно однозначном соответствии с делителями n, т.е.*

$$\forall H \leq G \ |H| \mid n \text{ и } \forall d | n \ \exists! \ H \leq G : |H| = d$$

3. *Подгруппы группы $\mathbb{Z}$ исчерпываются группами $k\mathbb{Z} = \langle k \rangle$, где $k \in \mathbb{N} \cup \{0\}$.*

Доказательство.

1. Пусть $G = \langle g \rangle, H \leq G$. Если $H = \{e\}$, то $H = \langle e \rangle$.
При $H \neq \{e\} : \forall h \in H \ \exists k \in \mathbb{Z} : h = g^k$. Так как $g^k \in H \Longrightarrow g^{-k} \in H$ и в H есть элемент, отличный от e, $\exists$ наименьшее $k \in \mathbb{N} : g^k \in H$.
Докажем, что $H = \langle g^k \rangle$. Рассмотрим произвольный $g^m \in H$. Разделим m на k с остатком: $m = kq + r, 0 \leqslant r < k$. Тогда:

$$g^m = (g^k)^q \cdot g^r \Longrightarrow g^r = (g^k)^{-q} \cdot g^m$$

то есть $g^r \in H$, а в силу того, что k - наименьшее натуральное число такое, что $g^k \in H$, имеем $r = 0$. Значит, $g^m = (g^k)^q$, а отсюда $H = \langle g^k \rangle$.

2. $G = \langle g \rangle_n, H \leq G \overset{1}{\Longrightarrow} H = \langle g^k \rangle$.
   Так как $g^n = e \in H$, то в силу рассуждений пункта 1 при $m = n$ получаем $k|n \Longrightarrow n = kq$.
   Отсюда $H = \{e, g^k, g^{2k}, ..., g^{(q-1)k}\} \Longrightarrow |H| = q$, где $q|n$.
   Обратно, $\forall d|n \ \exists! H = \langle g^{\frac{n}{d}} \rangle$ (в силу описания выше других подгрупп такого порядка нет).

3. Из пункта 1 в аддитивной форме получаем, что $H \leq \mathbb{Z} = \langle 1 \rangle \Longrightarrow H = \langle k \cdot 1 \rangle$

$\square$

Следствие. *В циклической группе простого порядка существуют ровно две подгруппы - тривиальная и сама группа.*

Примеры.

1. $H \leq \mathbb{Z}_5 \Longrightarrow H = \{0\}, H = \mathbb{Z}_5$;

2. $H \leq \mathbb{Z}_6 \Longrightarrow H = \{0\}, H = \langle 2 \rangle, H = \langle 3 \rangle, H = \mathbb{Z}_6$.

1.3 Смежные классы

Определение. Пусть $(G, \cdot, e)$ - произвольная группа, $H \leq G, g \in G$.
Рассмотрим множества:

$$gH = \{gh | h \in H\} \text{ - левый смежный класс G по H с представителем g}$$

$$Hg = \{hg | h \in H\} \text{ - правый смежный класс G по H с представителем g}$$

Утверждение (Свойства смежных классов)**.**

1. *$\forall a \in G \ a \in aH$;*

2. *если $a \in bH$, то $bH = aH$; в частности, любые два смежных класса либо не пересекаются, либо совпадают.*

3. *$aH = bH \Longleftrightarrow b^{-1}a \in H$;*
   (Верны аналогичные утверждения для правых смежных классов)

Доказательство.

1. Очевидно;

2. $a \in bH \Longrightarrow \exists h \in H : a = bh \Longrightarrow \forall \tilde{h} \in H \ a\tilde{h} = bh\tilde{h} \in bH \Longrightarrow aH \subseteq bH$.
   Аналогично $bH \subseteq aH \Longrightarrow aH = bH$.

3. $\Longrightarrow$: $aH = bH \Longrightarrow a \in bH (a \in aH) \Longrightarrow \exists h \in H : a = bh \Longrightarrow b^{-1}a = h \in H$
   $\Longleftarrow$: $b^{-1}a = h \in H \Longrightarrow a = bh \Longrightarrow aH = bH$ по пункту 2.

□

Утверждение. *Отношение $a \equiv b \pmod H \Leftrightarrow b^{-1}a \in H$ является отношением эквивалентности, причём классы эквивалентности совпадают с левыми смежными классами (аналогично $ab^{-1} \in H$ для правых).*

Доказательство.

- Рефлексивность: $a^{-1}a = e \in H \Longrightarrow a \equiv a \pmod H$;
- Симметричность: $a \equiv b \pmod H \Rightarrow b^{-1}a \in H \Rightarrow a^{-1}b = (b^{-1}a)^{-1} \in H \Rightarrow b \equiv a \pmod H$;
- Транзитивность: $a \equiv b, b \equiv c \pmod H \Longrightarrow c^{-1}b, b^{-1}a \in H \Longrightarrow c^{-1}b \cdot b^{-1}a = c^{-1}a \in H \Longrightarrow a \equiv c \pmod H$.

Совпадение классов эквивалентности с левыми смежными классами следует из пункта 3 предыдущего утверждения. □

Утверждение. *Если G - абелева, то $\forall a \in G : aH = Ha$.*
(В общем случае данное утверждение неверно).

Доказательство. $\forall a \in G :\ \{ah : h \in H\} = \{ha : h \in H\} \Longrightarrow aH = Ha.$ □

Примеры.

1. $H = \langle (12) \rangle \leq S_3 \ \ (H = \{id, (12)\}),\ g = (13).$
   $(13)(12) = (123);\ (12)(13) = (132).$
   Тогда $\{(13), (123)\} = gH \neq Hg = \{(13), (132)\}.$
2. $H = 3\mathbb{Z} \leq \mathbb{Z}$. Смежные классы - $3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$.
3. $H = \mathbb{R} \leq \mathbb{C}$. Смежные классы - $a + bi + \mathbb{R} = bi + \mathbb{R}$.

Утверждение. *Множество $\{aH : a \in G\}$ находится во взаимно однозначном соответствии с множеством $\{Ha : a \in G\}$.*

Доказательство. $gH \leftrightarrow Hg^{-1} : x = gh \in gH \leftrightarrow x^{-1} = h^{-1}g^{-1} \in Hg^{-1}.$ □

Следствие. $|\{aH : a \in G\}| = |\{Ha : a \in G\}|$

Определение. Мощность множества левых смежных классов группы G по подгруппе H называется индексом H в G. Обозначение: $|G:H|$

Пример. $|\mathbb{Z}:3\mathbb{Z}|=3$, т.к. смежные классы - $\{3\mathbb{Z},\ 1+3\mathbb{Z},\ 2+3\mathbb{Z}\}$.

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

Доказательство. Так как $|G| < \infty$, то $|H| < \infty$, т.е. $H = \{h_1, \dots, h_k\}$.
$\forall g \in G,\ gH = \{gh_1, \dots, gh_k\}$, причем $gh_i = gh_j \Rightarrow h_i = h_j \Rightarrow |gH| = |H|$. Отсюда, если $|G:H| = n$:

$$G = \bigsqcup_{i=1}^{n} a_i H \Longrightarrow |G| = \sum_{i=1}^{n} |a_i H| = |G:H| \cdot |H|$$

□

Следствие 1. *Если G - конечная группа, $H \leq G$, то $|H| \mid |G|$.*
(Обратное утверждение неверно).

Упражнение. Пусть $G = A_4$ (группа чётных перестановок).
$|A_4| = \frac{4!}{2} = 12$. Докажем, что в A_4 нет подгруппы порядка 6.
Предположим, что $H \leq A_4$ и $|H| = 6$. A_4 состоит из элемента id, 3 элементов вида $(ab)(cd)$ и восьми элементов вида (abc). Значит, H содержит хотя бы один элемент вида (abc) (с точностью до перенумерования - (123)). Тогда H содержит и $(123)^{-1} = (132)$. Также знаем, что группа чётного порядка содержит элемент порядка 2 (иначе в группе все элементы, кроме e, разбиваются на пары обратных, и элементов нечётное число), поэтому H содержит $\sigma = (**)(**)$.
Рассмотрим $\omega = \sigma(123)\sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3))$ (это равенство легко проверить, подставив в него $\sigma(1), ..., \sigma(4)$). Очевидно, что это цикл длины 3, не оставляющий на месте 4 (т.к. σ не оставляет на месте 4). Значит, ω и ω^{-1} принадлежат H и не совпадают с предыдущими элементами (и друг с другом), т.е.

$$H = \{id, (123), (132), \sigma, \omega, \omega^{-1}\}$$

Осталось перебрать возможные значения σ:

- $\sigma = (12)(34) \Longrightarrow (123)(12)(34)(132) = (14)(23) \notin H$;
- $\sigma = (13)(24) \Longrightarrow (123)(13)(24)(132) = (12)(34) \notin H$;
- $\sigma = (14)(23) \Longrightarrow (123)(14)(23)(132) = (13)(24) \notin H$;

Отсюда таких H не существует.

Следствие 2. *Если G - конечная группа, то* $\forall g \in G : \operatorname{ord} g \mid |G|$

Доказательство. $\operatorname{ord} g = |\langle g \rangle| \mid |G|$. $\square$

Следствие 3. *Если G - конечная группа порядка n, то $\forall g \in G : g^n = e$ в G.*

Доказательство. По следствию 2: $n = \operatorname{ord} g \cdot k \Rightarrow g^n = g^{(\operatorname{ord} g)\cdot k} = e^k = e$. $\square$

Пример. Пусть $G = \mathbb{Z}_p^*$, p - простое, $|\mathbb{Z}_p^*| = p - 1$. По следствию 3:
$\forall a \in \mathbb{Z}_p^* : a^{p-1} = 1$ в $\mathbb{Z}_p^*$, отсюда $\forall a \in \mathbb{Z},\ p \nmid a : a^{p-1} \equiv 1 \pmod p$ - малая теорема Ферма.

Следствие 4. *Любая группа G простого порядка p является циклической.*

Доказательство. $\forall a \in G,\ a \neq e : \operatorname{ord} a \neq 1,\ \operatorname{ord} a \mid |G| = p \Rightarrow \operatorname{ord} a = |G| \Rightarrow G = \langle a \rangle$. $\square$

Упражнение. Доказать, что с точностью до изоморфизма существует ровно две группы порядка 4 - $\mathbb{Z}_4$ и V_4.

Доказательство. Пусть G - группа порядка 4. Заметим, что по следствию 2 порядок неединичного элемента в G может быть равен либо 2, либо 4. Если в G есть элемент порядка 4, то G циклическая, а тогда по теореме о классификации циклических групп $G \simeq \mathbb{Z}_4$.
Пусть $G = \{e, a, b, c\}, \operatorname{ord} a = \operatorname{ord} b = \operatorname{ord} c = 2$. Посмотрим, чему может быть равно ab:

- $ab = e \Longrightarrow aab = a \Longrightarrow b = a$ - противоречие;
- $ab = a \Longrightarrow aab = aa \Longrightarrow b = e$ - противоречие;
- $ab = b \Longrightarrow abb = bb \Longrightarrow a = e$ - противоречие.

Отсюда $ab = c$ - аналогично произведение любых двух различных неединичных элементов равно третьему. Отсюда таблица Кэли для G имеет вид

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

откуда видно, что $G \simeq V_4$. $\square$

Упражнение. Доказать, что если в группе G все неединичные элементы имеют порядок 2, то G - абелева.

Доказательство. $\operatorname{ord} a = 2 \Longrightarrow a = a^{-1} \Longrightarrow \forall a, b \in G : ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$ □

Пример. $H = \langle (12) \rangle \leq S_3,\ g = (13) \Rightarrow gH \neq Hg$

Определение. Подгруппа H группы G называется нормальной, если

$$\forall g \in G : gH = Hg \Longleftrightarrow \forall g \in G : gHg^{-1} = H \Longleftrightarrow$$
$$\Longleftrightarrow \forall g \in G : gHg^{-1} \subseteq H \Longleftrightarrow \forall g \in G,\ \forall h \in H : ghg^{-1} \in H$$

Обозначение: $H \trianglelefteq G$.

Эквивалентность определений:

- $1 \Longleftrightarrow 2$ - очевидно;
- $2 \Longleftrightarrow 3$:
  $\Longleftarrow$: $gHg^{-1} \subseteq H \Leftrightarrow H \subseteq g^{-1}Hg$ - из условия на всевозможные g получаем равенство;
  $\Longrightarrow$ - очевидно;
- $3 \Longleftrightarrow 4$ - из определения смежного класса.

□

Примеры.

1. $A_n \trianglelefteq S_n$, так как $\forall \sigma \in S_n,\ \forall \tau \in A_n : \sigma\tau\sigma^{-1} \in A_n$.
2. $SL_n(\mathbb{R}) \trianglelefteq GL_N(\mathbb{R})$, так как $\forall A \in GL_n(\mathbb{R}),\ \forall B \in SL_n(\mathbb{R}) : \det(ABA^{-1}) = \det B = 1 \Rightarrow ABA^{-1} \in SL_n(\mathbb{R})$.

Утверждение. *В абелевой группе любая подгруппа является нормальной.*

Упражнение. Докажите, что если $|G : H| = 2$, то $H \trianglelefteq G$ для произвольной группы G и произвольной подгруппы $H \leq G$.

Доказательство. Если $|G : H| = 2$, то G разбивается на два непересекающихся левых (правых) смежных класса по H. Очевидно, что один из этих классов в обоих случаях - сама подгруппа H. Тогда $\forall g \in G \setminus H$ группа G разбивается на левые смежные классы H и gH, а также на правые смежные классы H и Hg, откуда $gH = Hg$. Также очевидно, что $\forall h \in H : hH = H = Hh$. Значит, $\forall g \in G : gH = Hg \Longrightarrow H \trianglelefteq G$. □

1.4 Факторгруппа

Утверждение. *Пусть G - группа, $H \trianglelefteq G$. Тогда множество всех смежных классов G по $H : G/H = \{eH, aH, ...\}$ образует группу относительно операции $aH \cdot bH = abH$.*

Доказательство.

1. Проверим корректность операции, т.е. $\begin{cases} aH = \tilde{a}H \\ bH = \tilde{b}H \end{cases} \implies abH = \tilde{a}\tilde{b}H.$

   Действительно, если $\begin{cases} a = \tilde{a}h_a \\ b = \tilde{b}h_b \end{cases}$ из равенства смежных классов, то:

   $$\forall x \in abH \implies \exists h \in H : x = abh = \tilde{a}h_a\tilde{b}h_b h = \tilde{a}\tilde{b}h'h_b h \in \tilde{a}\tilde{b}H$$

   $(H \trianglelefteq G \implies Hb = bH \implies \exists h' \in H : h_a\tilde{b} = \tilde{b}h')$

2. Проверим, что это группа:

   - Ассоциативность:

     $aH(bH \cdot cH) = aH(bcH) = a(bc)H = (ab)cH = (abH)cH = (aH \cdot bH)cH$

   - Нейтральный элемент:

     $$eH = H : aH \cdot eH = aeH = aH = eaH = eH \cdot aH$$

   - Обратный элемент:

     $$\forall\ aH\ \exists\ a^{-1}H : aH \cdot a^{-1}H = eH = a^{-1}H \cdot aH$$

□

Определение. Группа G/H называется факторгруппой G по H.

Замечание. Если $H \ntrianglelefteq G$, то операция $aH \cdot bH = abH$ некорректна:

$$\langle(12)\rangle \leq S_3 :\ (13)H = (132)H, (23)H = (123)H;$$

$$(13)(23)H = (132)H \neq H = (123)(123)H$$

Примеры.

1. $\mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}_3 = \{0, 1, 2\}$;
2. $A_n \trianglelefteq S_n, S_n/A_n \simeq \mathbb{Z}_2$ (по чётности);
3. $\mathbb{R} \trianglelefteq \mathbb{C}, \mathbb{C}/\mathbb{R} \simeq \mathbb{R}$ $(bi + \mathbb{R} \mapsto b)$.

1.5 Гомоморфизмы групп

Определение. Пусть $(G, \cdot, e), (\tilde{G}, \cdot, \tilde{e})$ - группы. Отображение $\varphi : G \to \tilde{G}$ называется гомоморфизмом групп G и $\tilde{G}$, если $\forall a, b, \in G$ $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Замечание. В частности, изоморфизм - биективный гомоморфизм.

Утверждение (Свойства гомоморфизмов)**.**

1. $\varphi(e) = \tilde{e}$*;*

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

Определение. Множество $\operatorname{Im} \varphi = \{b \in \tilde{G} \mid \exists a \in G : \varphi(a) = b\}$ - образ гомоморфизма. Множество $\operatorname{Ker} \varphi = \{a \in G \mid \varphi(a) = \tilde{e}\}$ - ядро гомоморфизма.

Утверждение 1.

1. $\operatorname{Im} \varphi \leq \tilde{G}$*;*

2. $\operatorname{Ker} \varphi \trianglelefteq G$*.*

Доказательство.

1. $\operatorname{Im} \varphi \subseteq \tilde{G}$

   - $x, y \in \operatorname{Im} \varphi \Rightarrow \exists a, b \in G : x = \varphi(a), y = \varphi(b) \Longrightarrow xy = \varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{Im} \varphi$;
   - $\tilde{e} = \varphi(e) \in \operatorname{Im} \varphi$;
   - $\forall x \in \operatorname{Im} \varphi \ \exists a \in G : \varphi(a) = x \Longrightarrow x^{-1} = (\varphi(a))^{-1} = \varphi(a^{-1}) \in \operatorname{Im} \varphi$

   Отсюда $\operatorname{Im} \varphi \leq \tilde{G}$.

2. $\operatorname{Ker} \varphi \subseteq G$

   - $\forall a, b \in \operatorname{Ker} \varphi : \varphi(a) = \varphi(b) = \tilde{e} \Longrightarrow \varphi(ab) = \varphi(a)\varphi(b) = \tilde{e} \Longrightarrow$
     $ab \in \operatorname{Ker} \varphi$;
   - $\tilde{e} = \varphi(e) \Longrightarrow e \in \operatorname{Ker} \varphi$;
   - $\forall a \in \operatorname{Ker} \varphi \Rightarrow \varphi(a^{-1}) = (\varphi(a))^{-1} = \tilde{e}^{-1} = \tilde{e} \Longrightarrow a^{-1} \in \operatorname{Ker} \varphi$

   Отсюда $\operatorname{Ker} \varphi \leq G$.
   $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = \tilde{e} \Rightarrow ghg^{-1} \in \operatorname{Ker} \varphi \Longrightarrow$ $\operatorname{Ker} \varphi \trianglelefteq G$.

$\square$

Утверждение 2. *$\varphi(a) = \varphi(b) \iff a\text{Ker }\varphi = b\text{Ker }\varphi$.*
В частности, φ инъективно $\iff \text{Ker }\varphi = \{e\}$.

Доказательство.

$$\varphi(a) = \varphi(b) \iff \varphi(a)\varphi(b)^{-1} = \tilde{e} \iff \varphi(ab^{-1}) = \tilde{e} \iff$$

$$ab^{-1} \in \text{Ker }\varphi \iff a\text{Ker }\varphi = b\text{Ker }\varphi$$

$\square$

Пример. $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^* : \varphi(A) = \det A$.
$\text{Ker }\varphi = SL_n(\mathbb{R}), \text{Im }\varphi = \mathbb{R}^* \Longrightarrow R^* \simeq GL_n(\mathbb{R})/SL_n(\mathbb{R})$.

Теорема (О гомоморфизме)**.** *Пусть $G, \tilde{G}$ - группы, $\varphi : G \to \tilde{G}$ - гомоморфизм. Тогда $G/\text{Ker }\varphi \simeq \text{Im }\varphi$.*

Доказательство. Для начала заметим, что $\text{Ker }\varphi \trianglelefteq G$, поэтому факторгруппа $G/\text{Ker }\varphi$ определена.
Рассмотрим $\psi :\ g\text{Ker }\varphi \mapsto \varphi(g)$:

- Корректность:
  По утверждению 2: $g_1\text{Ker }\varphi = g_2\text{Ker }\varphi \Longrightarrow \varphi(g_1) = \varphi(g_2)$;

- Биективность:
  Сюръективность: $\forall b \in \text{Im }\varphi\ \exists a \in G : \varphi(a) = b \Longrightarrow \psi(a\text{Ker }\varphi) = b$;
  Инъективность: по утверждению 2: $\psi(a\text{Ker }\varphi) = \psi(b\text{Ker }\varphi) \Longrightarrow \varphi(a) = \varphi(b) \Longrightarrow a\text{Ker }\varphi = b\text{Ker }\varphi$;

- Сохранение операции:

$$\psi((g_1\text{Ker }\varphi)(g_2\text{Ker }\varphi)) = \psi(g_1g_2\text{Ker }\varphi) = \varphi(g_1g_2) =$$

$$= \varphi(g_1)\varphi(g_2) = \psi(g_1\text{Ker }\varphi)\psi(g_2\text{Ker }\varphi)$$

Отсюда $\psi : G/\text{Ker }\varphi \to \text{Im }\varphi$ - изоморфизм. $\square$

Пример. Пусть $G = S_n, \tilde{G} = \mathbb{R}^*, \varphi(\sigma) = \operatorname{sgn}\sigma$.
Тогда из теоремы о гомоморфизме:

$$\text{Im }\varphi = \{\pm 1\}, \text{Ker }\varphi = A_n \Longrightarrow S_n/A_n \simeq \{\pm 1\} \simeq \mathbb{Z}_2$$

Следствие 1. *Гомоморфизм* $\varphi : G \to \tilde{G}$ *- изоморфизм* $\iff \begin{cases} \text{Ker } \varphi = \{e\} \\ \text{Im } \varphi = \tilde{G} \end{cases}$

Доказательство.
$\Longrightarrow$ - очевидно из биективности;
$\Longleftarrow$ - изоморфизм из теоремы совпадёт с φ. □

Следствие 2. *Если* $|G| < \infty$*, то* $|G| = |\text{Ker } \varphi| \cdot |\text{Im } \varphi|$.

Доказательство. $|G| = |G/\text{Ker } \varphi| \cdot |\text{Ker } \varphi| = |\text{Im } \varphi| \cdot |\text{Ker } \varphi|$. □

Утверждение. *Пусть* G *- группа,* $H \trianglelefteq G$*. Тогда* $\exists$ *такая группа* $\tilde{G}$*, что* $\exists$ *сюръективный гомоморфизм* $\pi : G \to \tilde{G}$*, причём* $\text{Ker } \pi = H$*.*

Доказательство. Подходят $\tilde{G} = G/H, \pi : g \mapsto gH$. □

Определение. Приведённый выше гомоморфизм $\pi : G \mapsto G/H$ называется естественным (натуральным) гомоморфизмом из G в G/H.

Определение. Эпиморфизм - сюръективный гомоморфизм.

Утверждение. *Пусть* $\varphi : G \to \tilde{\tilde{G}}$ *- произвольный эпиморфизм с ядром* H*. Тогда* $\exists$ *изоморфизм* $\psi : G/H \to \tilde{\tilde{G}}$ *такой, что* $\varphi = \psi \circ \pi$*, где* π *- натуральный гомоморфизм из* G *в* G/H*.*

Доказательство. По теореме о гомоморфизме $G/\text{Ker } \varphi \simeq \text{Im } \varphi$.
Так как φ - сюръекция, $\text{Im } \varphi = \tilde{\tilde{G}}$, также по условию $\text{Ker } \varphi = H$. Тогда $\psi : G/H \to \tilde{\tilde{G}}$ - изоморфизм, заданный в доказательстве теоремы о гомоморфизме: $\psi : gH \mapsto \varphi(g)$.
Взяв этот изоморфизм, получим $\varphi = \psi \circ \pi$ (так как $g \overset{\pi}{\mapsto} gH \overset{\psi}{\mapsto} \varphi(g)$). □

2 Свободные группы

Определение. Тривиальные (групповые) соотношения - соотношения, которые выводятся из аксиом группы (и, соответственно, есть в любой группе).

Построим группу, в которой нет других соотношений.

Определение. Пусть A - множество символов (букв), A^{-1} - множество символов (букв) a^{-1}, где $a \in A$.
Условия на эти множества:

1. $\forall a^{-1} \in A^{-1} \Longrightarrow a^{-1} \notin A$;
   $\forall a \in A \Longrightarrow a \notin A^{-1}$;

2. $(a^{-1})^{-1} = a$;
   Буквы a, a^{-1} назовём взаимно обратными.

Множество $A^{\pm 1} = A \sqcup A^{-1}$ называется алфавитом.
Слово в алфавите $A^{\pm 1}$ - конечная последовательность букв $X = x_1...x_k$, где $x_i \in A^{\pm 1}$.
Длина слова X (обозначается $|X|$) - количество букв в X.

Пример. $A = \{a, b\} : X = abaab^{-1} \Rightarrow |X| = 5$.

Определение. Слово $X = x_1...x_k$ - сократимое, если $\exists i \in \overline{1, .., k-1} : x_i = x_{i+1}^{-1}$.
Сокращением взаимно обратных букв назовём вычёркивание пары x_i, x_{i+1} из X (получим слово длины $|X| - 2$).
За конечное число сокращений получим слово $\tilde{X}$, не являющееся сократимым - такое $\tilde{X}$ называется результатом полного сокращения слова X.

Определение. Рассмотрим множество $F(A)$ всех несократимых слов в $A^{\pm 1}$.
Введём бинарную операцию на $F(A)$: пусть $X = x_1...x_k, Y = y_1...y_m$.
Если $x_k \neq y_1^{-1}$, то XY - конкатенация (приписывание) X и Y:
$XY = x_1...x_k y_1...y_m, |XY| = k + m$.
Если $x_k = y_1^{-1}$, то XY - результат полного сокращения слова $x_1...x_k y_1...y_m$.

Пример. $(abcda^{-1}b)(b^{-1}ad^{-1}aab) = abcaab$.

Определение. Если $|X| = 0$, то X называется пустым словом (обозначим λ).
Пустое слово по определению несократимо и лежит в $F(A)$.

Теорема. $F(A)$ *с приведённой выше бинарной операцией - группа.*

Доказательство.

1. Ассоциативность:
   Пусть $X = x_1 ... x_k, Z = z_1 ... z_m$.
   Случай $|Y| = 0 \Longrightarrow Y = \lambda$ очевиден ($XZ = XZ$);
   Индукция по длине слова Y:
   База индукции: $|Y| = 1 \Longrightarrow Y = a \in A^{\pm 1}$. Индукция по $|X| + |Z|$:
   База внутренней индукции:
   $|X| + |Z| = 0$ - очевидно ($a = a$);
   $|X| + |Z| = 1$ - очевидно (одно из слов X, Z пустое);
   Шаг внутренней индукции ($k + m - 2 \to k + m$) - рассмотрим случаи:

   - $a^{-1} \neq x_k, a^{-1} \neq z_1 : X(YZ) = x_1 ... x_k a z_1 ... z_m = (XY)Z$;
   - $a^{-1} = x_k, a^{-1} \neq z_1 : X(aZ) = X(a z_1 ... z_m) =$
     $=$ результат полного сокращения $x_1 ... x_{k-1} a^{-1} a z_1 ... z_m =$
     $=$ результат полного сокращения $x_1 ... x_{k-1} z_1 ... z_m = (Xa)Z$;
   - $a^{-1} \neq x_k, a^{-1} = z_1$ - аналогично предыдущему;
   - $a^{-1} = x_k, a^{-1} = z_1$: пусть $X = X' a^{-1}, Z = a^{-1} Z'$. Тогда:
     $X(aZ) = X(a(a^{-1}Z')) = XZ' = (X'a^{-1})Z'$
     $(Xa)Z = (X'a^{-1}a)Z = X'Z = X'(a^{-1}Z')$
     При этом $|X'| + |Y'| = k + m - 2$, то есть $X'(a^{-1}Z') = (X'a^{-1})Z'$ по предположению внутренней индукции.

   Во всех случаях $X(aZ) = (Xa)Z \Longrightarrow$ база доказана.
   Шаг индукции: Пусть $Y = y_1 ... y_l$. Тогда:

   $$X(YZ) = X(y_1 ... y_l \cdot Z) = X((y_1 ... y_{l-1} \cdot y_l)Z) \overset{1}{=} X((y_1 ... y_{l-1}) \cdot (y_l Z)) \overset{2}{=}$$

   $$\overset{2}{=} (X \cdot y_1 ... y_{l-1})(y_l Z) \overset{3}{=} (X \cdot y_1 ... y_l)Z = (XY)Z$$

   1, 3 - из утверждения базы индукции; 2 - по предположению индукции.

2. λ - нейтральный элемент;

3. обратный элемент к $x_1 ... x_k$ - элемент $x_k^{-1} ... x_1^{-1}$.

□

Определение. Построенная группа $F(A)$ называется свободной группой с базисом A. (A также называется свободной порождающей системой группы). Любая группа, изоморфная $F(A)$, также называется свободной.

Утверждение. *Пусть* $H \leq SL_2(\mathbb{Z}) : H = \langle \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} \rangle$.
Тогда $H \simeq F(A)$ *с базисом* $A = \{a, b\}$.

Доказательство. Без доказательства. $\square$

Утверждение. *Все базисы свободной группы равномощны.*

Доказательство. Без доказательства. $\square$

Определение. Ранг свободной группы - мощность её базиса.

Замечание. Заметим, что в $F(A)$ результат умножения определён однозначно $\Longrightarrow$ однозначно определён элемент $x_1 \cdot ... \cdot x_k$, где $x_i \in A^{\pm 1}$.
Тогда если считать слово $x_1...x_k$ результатом умножения $x_1 \cdot ... \cdot x_k$, то можно опускать знак умножения, и в этом смысле работать и с сократимыми словами.

Пример. $abb^{-1}ba^{-1}a = a \cdot b \cdot b^{-1} \cdot b \cdot a^{-1} \cdot a = ab \in F(A)$.

Теорема 1 (Универсальное свойство свободной группы)**.**
Пусть G *- группа,* $\{g_i \mid i \in I\} \subset G$ *- произвольное множество её элементов. Рассмотрим свободную группу* $F(A)$ *с базисом* $A = \{a_i \mid i \in I\}$.
Тогда отображение $\varphi : a_i \mapsto g_i$ *продолжается до гомоморфизма* $\varphi : F(A) \to G$, *причём единственным образом.*

Доказательство. Пусть $W = a_{i_1}^{\varepsilon_1}...a_{i_k}^{\varepsilon_k}$ - несократимое слово из $F(A)$, где $\varepsilon_i = \pm 1, a_{i_j} \in A$. Зададим $\varphi : F(A) \to G$ по правилу $\varphi(W) = g_{i_1}^{\varepsilon_1}...g_{i_k}^{\varepsilon_k}$.
Проверим, что φ - гомоморфизм ($W, \tilde{W} \in F(A), W = a_{i_1}^{\varepsilon_1}...a_{i_k}^{\varepsilon_k}, \tilde{W} = a_{j_1}^{\tau_1}...a_{j_m}^{\tau_m}$):

$$\varphi(W\tilde{W}) = \varphi(a_{i_1}^{\varepsilon_1}...a_{i_k}^{\varepsilon_k} \cdot a_{j_1}^{\tau_1}...a_{j_m}^{\tau_m}) = g_{i_1}^{\varepsilon_1}...g_{i_k}^{\varepsilon_k} \cdot g_{j_1}^{\tau_1}...g_{j_m}^{\tau_m} =$$
$$= (g_{i_1}^{\varepsilon_1}...g_{i_k}^{\varepsilon_k}) \cdot (g_{j_1}^{\tau_1}...g_{j_m}^{\tau_m}) = \varphi(W)\varphi(\tilde{W})$$

Единственность такого гомоморфизма очевидна:
$\varphi(a_{i_1}^{\varepsilon_1}...a_{i_k}^{\varepsilon_k}) = \varphi(a_{i_1})^{\varepsilon_1}...\varphi(a_{i_k})^{\varepsilon_k} = g_{i_1}^{\varepsilon_1}...g_{i_k}^{\varepsilon_k}$ - определено однозначно. $\square$

Пример. (несвободной группы)
$S_3 = \langle (12), (123) \rangle : \forall g \in S_3\ g^6 = id$. Попытаемся продолжить до гомоморфизма $S_3 \to Q_8$ отображение $\varphi : (12) \mapsto i, (123) \mapsto j$:
$-1 = i^2 = \varphi((12))^2 = \varphi((12)^2) = \varphi(id) = 1$ - противоречие.

Следствие 1. *Пусть* G *- группа,* $M = \{g_i \mid i \in I\}$ *- порождающее множество* G, $F(A)$ *- свободная группа с базисом* $A = \{a_i \mid i \in I\}$.
Тогда $\exists!$ *сюръективный гомоморфизм* $\varphi : F(A) \to G$ *такой, что* $\forall i \in I$: $\varphi(a_i) = g_i$.

Доказательство. Достаточно показать, что в этом случае гомоморфизм из доказательства теоремы сюръективен - это следует из того, что множество $\{g_i \mid i \in I\}$ порождает группу G (каждый элемент представим как $g_{i_1}^{\varepsilon_1}...g_{i_k}^{\varepsilon_k} = \varphi(a_{i_1}^{\varepsilon_1}...a_{i_k}^{\varepsilon_k})$). □

Следствие 2. *Любая группа G изоморфна факторгруппе некоторой свободной группы по некоторой её нормальной подгруппе.*

Доказательство. Пусть $\varphi : F(A) \to G$ - гомоморфизм из следствия 1.
Так как $\mathrm{Ker}\ \varphi \trianglelefteq F(A)$, из теоремы о гомоморфизме $G = \mathrm{Im}\ \varphi \simeq F(A)/\mathrm{Ker}\ \varphi$. □

Определение. Сюръективный гомоморфизм $\varphi : F(A) \to G$ - из следствия 1 называется копредставлением группы G.

Замечание. Копредставление зависит от выбора порождающего множества M.

2.1 Задание группы порождающими и определяющими соотношениями

По следствию 2: $G \simeq F(A)/N$, где $N \trianglelefteq F(A)$. Отсюда задание группы G сводится к заданию A и N.
N - нормальная $\Longrightarrow \forall f \in F(A), \forall h \in N : fhf^{-1} \in N$.

Определение. Пусть $\mathcal{R} \subseteq F(A)$. Нормальным замыканием множества $\mathcal{R}$ в группе $F(A)$ называется наименьшая (по включению) нормальная подгруппа, содержащая $\mathcal{R}$. Обозначается $\langle\langle\mathcal{R}\rangle\rangle^{F(A)}$

Утверждение.
$\langle\langle\mathcal{R}\rangle\rangle^{F(A)} = \{(f_1 r_1^{\varepsilon_1} f_1^{-1})...(f_k r_k^{\varepsilon_k} f_k^{-1}) \mid r_i \in \mathcal{R}, f_i \in F(A), \varepsilon_i = \pm 1\}$

Доказательство.
Пусть $\{(f_1 r_1^{\varepsilon_1} f_1^{-1})...(f_k r_k^{\varepsilon_k} f_k^{-1}) \mid r_i \in \mathcal{R}, f_i \in F(A), \varepsilon_i = \pm 1\} = H$. Тогда:
$\langle\langle\mathcal{R}\rangle\rangle^{F(A)} \trianglelefteq F(A) \Longrightarrow \forall r_i \in \mathcal{R}, f_i \in F(A), \varepsilon_i \in \{\pm 1\} : f_i r_i^{\varepsilon_i} f_i^{-1} \in \langle\langle\mathcal{R}\rangle\rangle^{F(A)} \Longrightarrow H \subseteq \langle\langle\mathcal{R}\rangle\rangle^{F(A)}$. Осталось показать, что $H \trianglelefteq F(A)$:

$$\forall h \in H, g \in F(A) : ghg^{-1} = g(f_1 r_1^{\varepsilon_1} f_1^{-1})...(f_k r_k^{\varepsilon_k} f_k^{-1})g^{-1} =$$

$$= ((gf_1) r_1^{\varepsilon_1} (f_1^{-1} g^{-1}))...((gf_k) r_k^{\varepsilon_k} (f_k^{-1} g^{-1})) =$$
$$= ((gf_1) r_1^{\varepsilon_1} (gf_1)^{-1})...((gf_k) r_k^{\varepsilon_k} (gf_k)^{-1}) \in H$$

Отсюда минимальная группа, содержащая $\mathcal{R}$, в точности равна H. □

Утверждение. *Любую нормальную подгруппу* $N \trianglelefteq F(A)$ *можно задать как* $N = \langle\langle \mathcal{R} \rangle\rangle^{F(A)}$ *для подходящего* $\mathcal{R} \subset F(A)$.

Доказательство. Очевидно, подойдёт $\mathcal{R} = N$. □

Элементарные преобразования над словами в $F(A)$:
(под словами в $F(A)$ подразумеваются любые произведения букв, а не только элементы $F(A)$)

- ЭП1: $W = W_1 a^\varepsilon a^{-\varepsilon} W_2 \mapsto \tilde{W} = W_1 W_2$, где $a \in A, \varepsilon = \pm 1$;
- ЭП2: $W = W_1 r^\varepsilon W_2 \mapsto \tilde{W} = W_1 W_2$, где $r \in \mathcal{R}, \varepsilon = \pm 1$;
- ЭП1$'$ - обратное к ЭП1;
- ЭП2$'$ - обратное к ЭП2;

Определение. Назовём слова W и $\tilde{W}$ $\mathcal{R}$-эквивалентными, если от W можно с помощью ЭП перейти к $\tilde{W}$.

Утверждение. *$\mathcal{R}$-эквивалентность - отношение эквивалентности.*

Доказательство.

- Рефлексивность - очевидно;
- Симметричность - следует из обратимости каждого ЭП;
- Транзитивность - очевидно;

□

Теорема 2. *Следующие условия эквивалентны:*

1. $W \in \langle\langle \mathcal{R} \rangle\rangle^{F(A)}$;
2. *W $\mathcal{R}$-эквивалентно пустому слову λ;*
3. *Если для произвольной группы G с порождающим множеством $M = \{g_i \mid i \in I\}$ (т.е. заданным копредставлением $\varphi : F(A) \to G$) верно, что $\forall r \in \mathcal{R} : \varphi(r) = 1$ в G, то $\varphi(W) = 1$ в G.*

Доказательство.

- $1 \Longrightarrow 2 :$ $\quad W \in \langle\langle \mathcal{R} \rangle\rangle^{F(A)} \Longrightarrow W = (f_1 r_1^{\varepsilon_1} f_1^{-1}) ... (f_k r_k^{\varepsilon_k} f_k^{-1}) \underset{\text{ЭП2}}{\Longrightarrow} W \sim \tilde{W} = (f_1 f_1^{-1}) ... (f_k f_k^{-1}) \underset{\text{ЭП1}}{\Longrightarrow} \lambda$;

- $2 \Longrightarrow 3$ Пусть $\varphi : F(A) \to G$ взят из условия теоремы. Покажем, что при ЭП образ слова не меняется:

    1. $\varphi(W_1 a^\varepsilon a^{-\varepsilon} W_2) = \varphi(W_1)\varphi(a)^\varepsilon \varphi(a)^{-\varepsilon}\varphi(W_2) = \varphi(W_1)\varphi(W_2) = \varphi(W_1 W_2)$;
    2. $\varphi(W_1 r^\varepsilon W_2) = \varphi(W_1)\varphi(r)^\varepsilon \varphi(W_2) = \varphi(W_1)\cdot 1^\varepsilon \cdot \varphi(W_2) = \varphi(W_1 W_2)$;

  При ЭП, обратных этим, образ слова аналогично не изменяется.
  Тогда если $W \underset{\text{ЭП}}{\sim} \lambda$, то $\varphi(W) = \varphi(\lambda) = 1$.

- $3 \Longrightarrow 1:\quad \forall r \in \mathcal{R} : \varphi(r) = 1 \Longrightarrow r \in \operatorname{Ker} \varphi;\ \varphi(W) = 1 \Longrightarrow W \in \operatorname{Ker} \varphi$.
  Рассмотрим в качестве G группу $F(A)/N$, где $N = \langle\langle \mathcal{R} \rangle\rangle^{F(A)}$, а в качестве φ - π (естественный гомоморфизм $F(A) \to F(A)/N$).
  $r \in N \Longrightarrow \pi(r) = 1$. Тогда по условию 3: $\pi(W) = 1 \Longrightarrow W \in \operatorname{Ker} \varphi = N$.

□

Определение. Если $W \in F(A)$ удовлетворяет любому из условий теоремы 2, то говорят, что соотношение $W = 1$ следует из соотношений $\{r = 1 \mid r \in \mathcal{R}\}$ или является следствием соотношений $\mathcal{R}$.

Определение. Рассмотрим копредставление произвольной группы G, т.е. $\varphi : F(A) \to G$, где $A = \{a_i \mid i \in I\}$. Пусть слово $W \in F(A)(W = a_{i_1}^{\varepsilon_1}...a_{i_k}^{\varepsilon_k})$ такое, что $\varphi(W) = g_{i_1}^{\varepsilon_1}...g_{i_k}^{\varepsilon_k} = 1$ в G.
Тогда говорят о соотношении $W = 1$.
(Для упрощения записи вместо g_i пишут a_i).

Определение. Множество $\mathcal{R} \subset F(A)$ называется определяющим множеством соотношений группы G, если любое соотношение группы G следует из $\mathcal{R}$.
При этом элементы $\mathcal{R}$ называются определяющими соотношениями G. Обозначается $G = \langle A \mid \mathcal{R} \rangle$ (данная запись также называется копредставлением G).

Примеры.

1. $\mathbb{Z}_3 = \langle a | a^3 = 1\rangle; a^{12} = 1$ - следствие;
2. $V_4 = \langle a, b | a^2 = b^2 = 1, ab = ba\rangle; (ab)^2 = 1$ - следствие.

Теорема (Теорема Дика).
*Пусть G - группа, заданная копредставлением $\langle A \mid R\rangle$, где $A = \{a_i \mid i \in I\}$.
Пусть H - произвольная группа, $\{h_i \mid i \in I\} \subset H$ - произвольное множество её элементов.
Тогда отображение φ на порождающих $\varphi : a_i \mapsto h_i\ \forall i \in I$ продолжается до*

гомоморфизма $\varphi : G \to H$ *тогда и только тогда, когда* $\forall r \in \mathcal{R}: \ \varphi(r) = 1$ *в* H.

Доказательство. Если $\varphi : a_i \mapsto h_i$ и φ - гомоморфизм, то должно выполняться $\varphi(a_{i_1}^{\varepsilon_1} ... a_{i_k}^{\varepsilon_k}) = h_{i_1}^{\varepsilon_1} ... h_{i_k}^{\varepsilon_k}$. Если это отображение корректно, то очевидно, что оно является искомым гомоморфизмом. Покажем корректность:
Пусть $W = \tilde{W}$ в G. Тогда $\tilde{W}W^{-1} = 1$ в $G \Longrightarrow \tilde{W}W^{-1} \in \langle\langle \mathcal{R} \rangle\rangle^{F(A)}$ (так как по определению копредставления соотношение $\tilde{W}^{-1}W = 1$ следует из R).
Отсюда $\tilde{W}W^{-1} \sim \lambda \Longrightarrow W \sim \tilde{W}W^{-1}W = \tilde{W}$. Из размышлений доказательства перехода $2 \Longrightarrow 3$ теоремы 2 видно, что из условия $\forall r \in \mathcal{R}: \ \varphi(r) = 1$ в H следует, что образ не изменяется при ЭП, то есть $\varphi(W) = \varphi(\tilde{W})$, т.е. отображение корректно. $\square$

3 Прямое произведение групп

3.1 Внешнее прямое произведение

Пусть $G_1, ..., G_k$ - группы.
$G = G_1 \times ... \times G_k = \{(g_1, ..., g_k) | g_i \in G_i\}$.
$(g_1, ..., g_k) \cdot (\tilde{g}_1, ..., \tilde{g}_k) = (g_1\tilde{g}_1, ..., g_k\tilde{g}_k)$
($g_i\tilde{g}_i$ перемножаются по правилу бинарной операции на G_i).

Утверждение. $(G, \cdot)$ - *группа.*

Доказательство.

1. $(a_1, ..., a_k)((b_1, ..., b_k)(c_1, ..., c_k)) = (a_1(b_1c_1), ..., a_k(b_kc_k)) =$
   $= ((a_1b_1)c_1, ..., (a_kb_k)c_k) = ((a_1, ..., a_k)(b_1, ..., b_k))(c_1, ..., c_k)$
2. Нейтральный элемент - $(e_1, ..., e_k)$ (e_i - нейтральный в G_i)
3. $(g_1, ..., g_k)^{-1} = (g_1^{-1}, ..., g_k^{-1})$

$\square$

Определение. Данная группа $(G, \cdot)$ называется прямым произведением групп $G_1, ..., G_k$. Обозначается $G = G_1 \times ... \times G_k$; G_i называются множителями.
В аддитивной терминологии те же рассуждения определяют прямую сумму $G = G_1 \oplus ... \oplus G_k$, где G_i - слагаемые.

Примеры.

1. $G_1 = \mathbb{Z}_3, G_2 = S_3, G = G_1 \times G_2$.
   $(1, (12)) \cdot (2, (13)) = (1 + 2, (12)(13)) = (0, (132))$.
2. $D_n(\mathbb{F}) \simeq \underbrace{\mathbb{F}^* \times ... \times \mathbb{F}^*}_{n}$ ($D_n(\mathbb{F})$ - группа диагональных матриц порядка n).

Утверждение.

1. *Если* $(m, n) = 1$, *то* $\mathbb{Z}_m \times \mathbb{Z}_n \simeq Z_{nm}$ - *циклическая группа;*
2. *Если* $(m, n) \neq 1$, *то* $\mathbb{Z}_m \times \mathbb{Z}_n$ - *не циклическая.*

Доказательство.

1. Обозначим за $[a]_s \in \mathbb{Z}_s$ класс вычетов по модулю s, содержащий a.
   Рассмотрим отображение $\varphi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ такое, что $\varphi : [a]_{mn} \mapsto ([a]_m, [a]_n)$. Очевидно, что это гомоморфизм:
   $$\varphi([a]_{mn} \cdot [b]_{mn}) = ([ab]_m, [ab]_n) = ([a]_m, [a]_n)([b]_m, [b]_n) = \varphi([a]_{mn})\varphi([b]_{mn})$$
   Найдём Ker φ :
   $$\varphi([a]_{mn}) = ([0]_m, [0]_n) \iff \begin{cases} m \mid a \\ n \mid a \end{cases} \underset{(m,n)=1}{\Longrightarrow} mn \mid a \Longrightarrow \mathrm{Ker}\ \varphi = \{[0]_{mn}\}$$
   По теореме о гомоморфизме $\mathrm{Im}\ \varphi = \mathbb{Z}_{mn}/\mathrm{Ker}\ \varphi = \mathbb{Z}_{mn} \Longrightarrow |\mathrm{Im}\ \varphi| = mn$.
   Так как $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$ и $\mathrm{Im}\ \varphi \leq \mathbb{Z}_m \times \mathbb{Z}_n,\ \mathrm{Im}\ \varphi = \mathbb{Z}_m \times \mathbb{Z}_n$.
   Отсюда φ - биекция (инъекция из Ker $\varphi = \{e\}$), т.е. φ -изоморфизм.

2. Пусть $(m, n) = d \neq 1$ $(m = dk_1, n = dk_2)$. Тогда $\forall g = (g_1, g_2) \in \mathbb{Z}_m \times \mathbb{Z}_n$:
   $$(g_1, g_2)^{dk_1k_2} = (g_1^{dk_1k_2}, g_2^{dk_1k_2}) = (0^{k_2}, 0^{k_1}) = (0, 0)$$
   Отсюда ord $(g_1, g_2) = dk_1k_2 = \frac{mn}{d} < mn = |\mathbb{Z}_m \times \mathbb{Z}_n|$. Значит, $\mathbb{Z}_m \times \mathbb{Z}_n$ не является циклической.

□

Следствие. *Пусть* $n = p_1^{s_1}...p_k^{s_k}$ *- разложение на простые множители. Тогда* $\mathbb{Z}_n = \mathbb{Z}_{p_1^{s_1}} \times ... \times \mathbb{Z}_{p_k^{s_k}}$.

Доказательство. Очевидно следует из теоремы. □

Следствие. *(Китайская теорема об остатках) Если числа* $a_1, ..., a_n$ *попарно взаимно просты, то для любых целых* $r_1, ..., r_n$ $(0 \leq r_i < n)$ $\exists! N$ $(0 \leq N < a_1 \cdot ... \cdot a_n)$ *такой, что* $N \equiv r_i (\mathrm{mod}\ a_i)$

Доказательство. Из теоремы следует, что $\mathbb{Z}_{a_1} \times ... \times \mathbb{Z}_{a_n} \simeq \mathbb{Z}_a$ $(a = a_1 \cdot ... \cdot a_n)$. Это означает, что набор остатков $(r_1, ..., r_n) \in \mathbb{Z}_{a_1} \times ... \times \mathbb{Z}_{a_n}$ изоморфизм из теоремы однозначно переводит в элемент $N \in \mathbb{Z}_a$ такой, что $r_i = [N]_{a_i}$, что и требовалось. □

3.2 Внутреннее прямое произведение

Определение. Пусть G - группа, $H_1, ..., H_k \leq G$.
G раскладывается в прямое произведение подгрупп $H_1, ..., H_k$, если:

1. $\forall g \in G \ \exists! \ h_i \in H_i : g = h_1 ... h_k$;

2. $\forall i \neq j : \forall h_i \in H_i, h_j \in H_j \ h_i h_j = h_j h_i$.

Обозначается $G = H_1 \times ... \times H_k$ ($G = H_1 \oplus ... \oplus H_k$ в аддитивной терминологии).

Замечание. Из определения следует, что $(h_1...h_k)(\tilde{h}_1...\tilde{h}_k) = (h_1\tilde{h}_1)...(h_k\tilde{h}_k)$.

Определение. Пусть $H, N \leq G$. Обозначим $NH = \{nh | n \in N, h \in H\}$

Утверждение. *Пусть $N \trianglelefteq G, H \leq G$. Тогда NH - подгруппа в G, причём $NH = HN$.*

Доказательство. Рассмотрим $(n_1h_1)(n_2h_2) = \underbrace{n_1(h_1n_2h_1^{-1})}_{=\tilde{n}}\underbrace{h_1h_2}_{=\tilde{h}} = \tilde{n}\tilde{h} \in NH$.
$e \in N \cap H \Longrightarrow e \cdot e = e \in NH$.
$(nh)^{-1} = h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1} \in NH$.
Отсюда NH - подгруппа. Покажем, что $NH = HN$:

$$\forall nh \in NH : \ nh = (hh^{-1})nh = h(h^{-1}nh) \in HN \Longrightarrow NH \subseteq HN$$

$$\forall hn \in HN : \ hn = hn(h^{-1}h) = (hnh^{-1})h \in NH \Longrightarrow HN \subseteq NH$$

Отсюда $NH = HN$. □

Лемма 1. *Пусть $H, N \trianglelefteq G, H \cap N = \{e\}$. Тогда $\forall h \in H, n \in N \ nh = hn$.*

Доказательство. Рассмотрим выражение $(hn)(nh)^{-1} = hnh^{-1}n^{-1}$:

$$hnh^{-1}n^{-1} = h(nh^{-1}n^{-1}) \in H; \quad hnh^{-1}n^{-1} = (hnh^{-1})n^{-1} \in N$$

Значит, $hnh^{-1}n^{-1} \in H \cap N = \{e\} \Longrightarrow (hn)(nh)^{-1} = e \Longrightarrow hn = nh$ □

Теорема 1. *Пусть $H_1, H_2 \leq G$. Тогда* $G = H_1 \times H_2 \Longleftrightarrow \begin{cases} (1) \ H_1, H_2 \trianglelefteq G \\ (2) \ H_1 \cap H_2 = \{e\} \\ (3) \ G = H_1H_2 \end{cases}$

Доказательство.
$\Longrightarrow$: Пусть $G = H_1 \times H_2$.
(3) - очевидно из пункта 1 определения.
(1): $\forall h_1 \in H_1, g \in G : \ g = \tilde{h}_1\tilde{h}_2$ $(\tilde{h}_1 \in H_1, \tilde{h}_2 \in H_2) \Longrightarrow$

$$gh_1g^{-1} = \tilde{h}_1(\tilde{h}_2h_1\tilde{h}_2^{-1})\tilde{h}_1^{-1} \underset{\text{(2 из опр)}}{=} \tilde{h}_1h_1\tilde{h}_1^{-1} \in H_1$$

Отсюда $H_1 \trianglelefteq G$ (аналогично $H_2 \trianglelefteq G$).
(2): Пусть $\exists h \in H_1 \cap H_2$. Тогда $h = he = eh$ - два разложения на произведение

элементов подгрупп. Они совпадают только в случае $h = e$, т.е. $H_1 \cap H_2 = \{e\}$.
$\Longleftarrow$: Пусть даны условия (1) - (3).
По лемме 1 из (1), (2) очевидно следует пункт 2 определения.
Из (3): $\forall g \in G\ \exists h_i \in H_i : g = h_1 h_2$.
Допустим, что это разложение не единственно, т.е. $h_1 h_2 = \tilde{h}_1 \tilde{h}_2$.
Тогда $\tilde{h}_1^{-1} h_1 = \tilde{h}_2 h_2^{-1}$, а так как $H_1 \cap H_2 = \{e\}$, имеем $h_1 = \tilde{h}_1, h_2 = \tilde{h}_2$. □

Теорема 2. *Пусть* $H_1, ..., H_k \leq G$.

$$\text{Тогда } G = H_1 \times ... \times H_k \Longleftrightarrow \begin{cases} (1)\ H_1, ..., H_k \trianglelefteq G \\ (2)\ \forall i\ H_i \cap \langle H_j \mid j \neq i \rangle = \{e\} \\ (3)\ G = H_1 ... H_k \end{cases}$$

Доказательство.
$\Longrightarrow$: Пусть $G = H_1 \times ... \times H_k$.
(3) - очевидно из пункта 1 определения.
(1): $\forall h_i \in H_i, g \in G :\ g = \tilde{h}_1 ... \tilde{h}_k\ (\tilde{h}_i \in H_i) \Longrightarrow$

$$g h_1 g^{-1} = (\tilde{h}_1 ... \tilde{h}_k) h_i (\tilde{h}_k^{-1} ... \tilde{h}_1^{-1}) \underset{\text{(2 из опр)}}{=} \tilde{h}_i h_i \tilde{h}_i^{-1} \in H_i$$

Отсюда $H_i \trianglelefteq G$.
(2): Пусть $\exists h \in H_i \cap \langle H_j \mid j \neq i \rangle$. Тогда $h = he = eh$ - два разложения на произведение элементов подгрупп. Они совпадают только в случае $h = e$, т.е. $H_i \cap \langle H_j \mid j \neq i \rangle = \{e\}$.
$\Longleftarrow$: Пусть даны условия (1) - (3).
По лемме 1 из (1), (2) очевидно следует пункт 2 определения.
Из (3): $\forall g \in G\ \exists h_i \in H_i : g = h_1 ... h_k$.
Допустим, что это разложение не единственно, т.е. $h_1 ... h_k = \tilde{h}_1 ... \tilde{h}_k$.
Тогда $\forall i : \tilde{h}_i^{-1} h_i = \prod\limits_{j \neq i} \tilde{h}_j h_j^{-1}$, а так как $H_i \cap \langle H_j \mid j \neq i \rangle = \{e\}$, имеем $h_i = \tilde{h}_i$. □

Примеры.

1. $V_4 = \{e, a, b, c\} = \{e, a\} \times \{e, b\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$;
2. $\mathbb{C}^* = \mathbb{R}_+ \times U\ (z = r \cdot e^{iy})$.
3. $\mathbb{Z}$ не раскладывается в произведение нетривиальных подгрупп.
   Предположим противное, т.е. $\mathbb{Z} = H_1 \times ... \times H_m$. Подгруппы $\mathbb{Z}$ имеют вид $k\mathbb{Z}$, т.е. $\mathbb{Z} = k_1\mathbb{Z} \times ... \times k_m\mathbb{Z}, k_i \neq 0$. Но тогда $k_1 k_2 \in H_1 \cap H_2$ и $k_1 k_2 \neq 0$, что противоречит теореме 2.

3.3 Связь между внутренним и внешним прямым произведением

Теорема 3.

1. *Если группа G раскладывается в прямое произведение подгрупп $H_1, ..., H_k$, то G изоморфна прямому произведению групп $G_1, ..., G_k$, где $\forall i$ $G_i \simeq H_i$;*
2. *Если группа G изоморфна прямому произведению групп $G_1, ..., G_k$, то $\exists H_i \leq G$ такие, что $G_i \simeq H_i$ и G раскладывается в прямое произведение $H_1, ..., H_k$.*

Доказательство.

1. Имеем: $H_i \leq G, G = H_1 \times ... \times H_k$.
   Рассмотрим отображение $\varphi : G \to G_1 \times ... \times G_k$, где $G_i = H_i$, такое, что $\forall g = h_1...h_k \in G \;\; \varphi(h_1...h_k) \mapsto (h_1, ..., h_k)$. Это изоморфизм:
   - Биекция - очевидна;
   - Гомоморфизм:
   $$\varphi((h_1...h_k) \cdot (h'_1...h'_k)) = \varphi(h_1h'_1...h_kh'_k) = (h_1h'_1, ..., h_kh'_k) =$$
   $$= (h_1, ..., h_k) \cdot (h'_1, ..., h'_k) = \varphi(h_1...h_k) \cdot \varphi(h'_1...h'_k)$$
2. Имеем: $G_1, ..., G_k$ - группы, $G = \{(g_1, ..., g_k) \mid g_i \in G_i\}$.
   Тогда $H_i = \{(e, ..., e, g_i, e, ..., e) \mid g_i \in G_i\}$ очевидно является подгруппой G, изоморфной G_i.
   Покажем, что $G = H_1 \times ... \times H_k$:
   - $\forall g = (g_1, ..., g_k) \in G \; \exists! \; h_i = (e, ..., e, g_i, e, ..., e) : g = h_1...h_k$;
   - $\forall i \neq j, h_i = ((e, ..., e, a_i, e, ..., e)) \in H_i, h_j = (e, ..., e, b_j, e, ..., e) \in H_j :$
   $$h_ih_j = (e, ..., e, a_i, e, ..., e, b_j, e, ..., e) = h_jh_i$$

□

Теорема 4. *Пусть $H_i \leq G, G = H_1 \times ... \times H_k, N_i \trianglelefteq H_i$. Тогда:*

1. *$N_1 \times ... \times N_k \trianglelefteq G$;*
2. *$G/(N_1 \times ... \times N_k) \simeq (H_1/N_1) \times ... \times (H_k/N_k)$.*

Доказательство.

1. Очевидно, что $N_1 \times ... \times N_k = N \leq G$.
   Покажем нормальность: $\forall g = h_1...h_k \in G, n = n_1...n_k \in N$

$$gng^{-1} = (h_1...h_k)(n_1...n_k)(h_k^{-1}...h_1^{-1}) \underset{(n_i \in H_i)}{=} (\overset{\in N_1}{h_1 n_1 h_1^{-1}})...(\overset{\in N_k}{h_k n_k h_k^{-1}}) \in N$$

2. Рассмотрим гомоморфизм $\varphi : G \to (H_1/N_1) \times ... \times (H_k/N_k)$ такой, что $\varphi : h_1...h_k \mapsto (h_1 N_1, ..., h_k N_k)$. Это сюръективный гомоморфизм, причём $\operatorname{Ker} \varphi = N_1 \times ... \times N_k$. Отсюда по теореме о гомоморфизме получаем необходимое утверждение.

$\square$

Следствие. *Если $G = H_1 \times H_2$, то $G/H_1 \simeq H_2, G/H_2 \simeq H_1$.*

4 Конечнопорождённые абелевы группы

Замечание. В данном разделе используется аддитивная терминология:
$(A, +)$ - абелева группа, $\forall a \in A, n \in \mathbb{Z}$:

$$na = \begin{cases} \underbrace{a + ... + a}_{n}, \ n > 0; \\ 0, \ a = 0; \\ \underbrace{(-a) + ... + (-a)}_{|n|}, \ n < 0 \end{cases}$$

Свойства. *($\forall a, b, \in A, \ n, m, \in \mathbb{Z}$)*

1. *$(n + m)a = na + ma$;*

2. *$n(a + b) = na + nb$;*

3. *$(nm)a = n(ma)$*

Доказательство. Непосредственный разбор случаев - знаков m, n. □

Определение. (Целочисленнной) линейной комбинацией элементов $a_1, ..., a_k \in A$ называется выражение $n_1a_1 + ... + n_ka_k$ $(n_i \in \mathbb{Z})$.
Если элемент $b \in A$ равен некоторой линейной комбинации $a_1, ..., a_k \in A$, то говорят, что b выражается через $a_1, ..., a_k$.

Определение. Система элементов $a_1, ..., a_k$ называется линейно зависимой, если $\exists n_1, ..., n_k \in \mathbb{Z}$, не все равные 0, такие, что $n_1a_1 + ... + n_ka_k = 0$.
В противном случае система $a_1, ..., a_k$ называется линейно независимой.

Пример. $A = \mathbb{Z}_3 \oplus \mathbb{Z}_4$. Система из одного элемента $(1, 1)$ - линейно зависима: $12 \cdot (1, 1) = (0, 0)$

Определение. Пусть A - абелева группа, $a_1, ..., a_k \in A$.
Будем обозначать $\langle a_1, ..., a_k \rangle = \{n_1a_1 + ... + n_ka_k \mid n_i \in \mathbb{Z}\}$
(для бесконечного числа a_k - всевозможные конечные линейные комбинации)

Утверждение. *$\langle a_1, ..., a_k \rangle$ - наименьшая подгруппа A, содержащая $a_1, ..., a_k$.*

Доказательство. Пусть H - наименьшая подгруппа, содержащая $a_1, ..., a_k$. Тогда с одной стороны $\langle a_1, ..., a_k \rangle \subseteq H$ по определению подгруппы, а с другой стороны $\langle a_1, ..., a_k \rangle$, очевидно, подгруппа в A. Значит, $H = \langle a_1, ..., a_k \rangle$ □

Определение. Если $A = \langle a_1, ..., a_k \rangle$, то говорят, что A порождается $a_1, ..., a_k$. Элементы $a_1, ..., a_k$ называются порождающими (образующими).

Определение. Если $\exists$ конечное множество элементов $a_1, ..., a_k \in A$, что $A = \langle a_1, ..., a_k \rangle$, то A называется конечнопорождённой.

Примеры.

1. $\mathbb{Q}$ - не конечнопорождённая;

2. U (комплексные корни из 1) - не конечнопорождённая;

3. $\mathbb{Z}, \mathbb{Z}_n$ - конечнопорождённые (циклические);

4. $\mathbb{Z} \oplus \mathbb{Z}$ - конечнопорождённая, не циклическая (примеры систем порождающих - $(1,0), (0,1)$ или $(3,0), (4,5), (0,1)$)

Определение. Линейно независимая система порождающих группы A называется базисом (или свободной системой порождающих).

Утверждение. *(не было в лекции)*
$a_1, ..., a_k$ - базис $\Longleftrightarrow$ любой элемент A выражается через $a_1, ..., a_k$ единственным образом.

Доказательство.
$\Longrightarrow$: Из определения базиса любой элемент имеет разложение по базису.

$$\alpha_1 e_1 + ... + \alpha_n e_n = a = \alpha_1' e_1 + ... + \alpha_n' e_n \Longrightarrow (\alpha_1 - \alpha_1')e_1 + ... + (\alpha_n - \alpha_n')e_n = 0$$

Отсюда из линейной независимости $\alpha_i = \alpha_i' \ \forall i$, т.е. разложение единственно.
$\Longleftarrow$: Любой элемент $a \in A$ имеет разложение по $a_1, ..., a_n$ - система $a_1, ..., a_n$ порождает A. Разложение любого элемента единственно $\Longrightarrow$ 0 имеет только тривиальное разложение $\Longrightarrow a_1, ..., a_n$ линейно независимы. $\square$

Пример. $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ - не имеет базиса: любая система элементов в ней линейно зависима $(12 \cdot a = 0 \ \forall a \in A)$.

Определение. Конечнопорождённая абелева группа, имеющая базис, называется свободной абелевой группой. По определению $A = \{0\}$ - свободная абелева группа.

Пример. $\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{n}$ - свободная абелева группа;

Базис - $(1, 0, ...0), (0, 1, ..., 0), ..., (0, 0, ..., 1)$. Проверим это:

1. Линейная независимость:

$$\alpha_1 e_1 + ... + \alpha_n e_n = 0 \Longrightarrow (\alpha_1, ..., \alpha_n) = (0, ..., 0) \Longrightarrow \alpha_i = 0 \ \forall i$$

2. Порождаемость группы:

$$\forall a \in \mathbb{Z}^n : a = (a_1, ..., a_n) = a_1 e_1 + ... + a_n e_n$$

Лемма. *(Основная лемма о линейной зависимости для абелевых групп)*
Если абелева группа A обладает базисом из n элементов, то любая система из $m > n$ элементов линейно зависима.

Доказательство. Пусть $e_1, ..., e_n$ - базис группы A, $a_1, ..., a_m \in A$ - произвольные элементы. Тогда из определения базиса:

$$\begin{cases} a_1 = \alpha_{11} e_1 + ... + \alpha_{1n} e_n \longrightarrow (\alpha_{11}, ..., \alpha_{1n}) \\ \vdots \\ a_m = \alpha_{m1} e_1 + ... + \alpha_{mn} e_n \longrightarrow (\alpha_{m1}, ..., \alpha_{mn}) \end{cases}$$

Строки $\overline{\alpha}_i = (\alpha_{i1}, ..., \alpha_{in})$ можно рассматривать как векторы из пр-ва $\mathbb{Q}^n$ над $\mathbb{Q}$. Так как $m > n$, по ОЛЛЗ для векторных пространств система $\overline{\alpha}_1, ..., \overline{\alpha}_m$ линейно зависима, т.е. $\exists \lambda_1, ..., \lambda_m \in \mathbb{Q}$, не все равные нулю, что $\lambda_1 \overline{\alpha}_1 + ... + \lambda_m \overline{\alpha}_m = 0$. Тогда если d - НОК знаменателей ненулевых λ_i, то $(d\lambda_1)\overline{\alpha}_1 + ... + (d\lambda_m)\overline{\alpha}_m = 0$ - нетривиальная целочисленная линейная комбинация, равная нулю.
Тогда $(d\lambda_1)a_1 + ... + (d\lambda_m)a_m = 0$, т.е. $a_1, ..., a_m$ линейно зависимы. □

Теорема 1. *Все базисы свободной абелевой группы A равномощны.*

Доказательство. Очевидно следует из ОЛЛЗ для абелевых групп. □

Определение. Число элементов в базисе свободной абелевой группы A называется рангом группы A. Обозначается $\mathrm{rk}\ A$. По определению $A = \{0\} \Longrightarrow \mathrm{rk}\ A = 0$.

Теорема 2. *Все свободные абелевы группы ранга n изоморфны между собой (в частности, изоморфны $\mathbb{Z}^n$).*

Доказательство.
Пусть A - свободная абелева группа, $\mathrm{rk}\ A = n$, $e_1, ..., e_n$ - базис. Рассмотрим отображение $\varphi : A \to \mathbb{Z}^n$ такое, что $\forall a = \alpha_1 e_1 + ... + \alpha_n e_n \in A \ \varphi(a) = (\alpha_1, ..., \alpha_n)$. Покажем, что φ - изоморфизм:

1. Биекция - следует из единственности разложения по базису;

2. Гомоморфизм: пусть $a = \alpha_1 e_1 + ... + \alpha_n e_n, b = \beta_1 e_1 + ... + \beta_n e_n$. Тогда:

$$\varphi(a+b) = \varphi((\alpha_1+\beta_1)e_1 + ... + (\alpha_n+\beta_n)e_n) = ((\alpha_1+\beta_1), ..., (\alpha_n+\beta_n)) =$$

$$= (\alpha_1, ..., \alpha_n) + (\beta_1, ..., \beta_n) = \varphi(a) + \varphi(b)$$

Отсюда $A \simeq \mathbb{Z}^n$.
Если $\mathrm{rk}\ A = \mathrm{rk}\ B = n$, то $A \simeq \mathbb{Z}^n \simeq B \Longrightarrow A \simeq B$. □

Теорема 3. *Любая подгруппа B свободной абелевой группы A ранга n является свободной абелевой, причём* $\mathrm{rk}\ B \leqslant n$.

Доказательство. Случай $n = 0$ очевиден. Индукция по n:
База: $n = 1 \Longrightarrow A \simeq \mathbb{Z} \Longrightarrow A = \langle e \rangle$.
Знаем, что любая подгруппа циклической группы - циклическая.
Пусть $B = \langle ke \rangle, k \in \mathbb{N} \cup \{0\}$. Тогда:

$$k = 0 \Longrightarrow B = \{0\} \Longrightarrow \mathrm{rk}\ B = 0 < 1 = \mathrm{rk}\ A$$

$$k \neq 0 \Longrightarrow B = \langle ke \rangle \simeq \mathbb{Z} \Longrightarrow \mathrm{rk}\ B = 1 = \mathrm{rk}\ A$$

Шаг: пусть $e_1, ..., e_n$ - базис свободной группы A.
Рассмотрим $\tilde{A} = \langle e_1, ..., e_{n-1} \rangle \leq A$ - свободная абелева ранга $n-1$.
Рассмотрим $\tilde{B} = B \cap \tilde{A}$ - подгруппу B в $\tilde{A}$. По предположению индукции $\tilde{B}$ - свободная абелева, причём $\mathrm{rk}\ \tilde{B} \leqslant \mathrm{rk}\ \tilde{A} = n-1$.
Если $B = \tilde{B}$, то теорема доказана.
Иначе рассмотрим гомоморфизм (проекцию на $\langle e_n \rangle$)
$\pi : A \to \mathbb{Z} : \forall a = \alpha_1 e_1 + ... + \alpha_n e_n \in A\ \pi(a) = \alpha_n$ ($\mathrm{Ker}\ \pi = \tilde{A}, \mathrm{Im}\ \pi = \mathbb{Z}$).
Знаем, что $\pi(B)$ - подгруппа в $\mathbb{Z} \Longrightarrow \pi(B) = \langle k \rangle$ ($k \neq 0$ из $B \neq \tilde{B}$).
Рассмотрим $b_0 \in B$ такой, что $\pi(b_0) = k$, т.е. $b_0 = \beta_1 e_1 + ... + \beta_{n-1} e_{n-1} + k e_n$. Докажем, что если $b_1, ..., b_s$ - базис $\tilde{B}$, то $b_0, b_1, ..., b_s$ - базис B (тогда B - свободная абелева, $\mathrm{rk}\ B \leqslant n$)

1. Проверим линейную независимость:

$$\lambda_0 b_0 + ... + \lambda_s b_s = 0 \Rightarrow \pi(\lambda_0 b_0 + ... + \lambda_s b_s) = 0 \Rightarrow \lambda_0 \pi(b_0) + ... + \lambda_s \pi(b_s) = 0 \Longrightarrow$$

$$\lambda_0 k = 0 \Rightarrow \lambda_0 = 0$$

Линейная комбинация $\lambda_1 b_1 + ... + \lambda_s b_s = 0$ тривиальна, так как $b_1, ..., b_s$ - базис $\tilde{B}$. Отсюда $b_0, b_1, ..., b_s$ линейно независимы.

2. $\langle b_0, b_1 ..., b_s \rangle \stackrel{?}{=} B$:
   Рассмотрим произвольный $b \in B$. $\pi(b) \in \langle k \rangle \Longrightarrow \pi(b) = tk,\ t \in \mathbb{Z}$.
   Пусть $\tilde{b} = b - tb_0$. Тогда $\pi(\tilde{b}) = \pi(b) - t\pi(b_0) = tk - tk = 0 \Longrightarrow \tilde{b} \in \operatorname{Ker} \pi = \tilde{A} \Longrightarrow \tilde{b} \in \tilde{A} \cap B = \tilde{B} \Longrightarrow \tilde{b} = t_1 b_1 + ... + t_s b_s \Longrightarrow b = tb_0 + t_1 b_1 + ... + t_s b_s$.

□

4.1 Связь между базисами свободной абелевой группы

Определение. Пусть A - свободная абелева группа, $\mathcal{E} = \{e_1, ..., e_n\}$, $\tilde{\mathcal{E}} = \{\tilde{e}_1, ..., \tilde{e}_n\}$ - базисы A.

$$\begin{cases} \tilde{e}_1 = c_{11} e_1 + ... + c_{n1} e_n \\ \vdots \\ \tilde{e}_n = c_{1n} e_1 + ... + c_{nn} e_n \end{cases} \Longrightarrow (\tilde{e}_1, ..., \tilde{e}_n) = (e_1, ..., e_n) C,\ C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & & \vdots \\ c_{n1} & \dots & c_{nn} \end{pmatrix}$$

Такая $C \in M_n(\mathbb{Z})$ называется матрицей перехода от $\mathcal{E}$ к $\tilde{\mathcal{E}}$.

Утверждение.
Пусть $C \in M_n(\mathbb{Z})$. Тогда C - матрица перехода $\Longleftrightarrow \det C = \pm 1$.

Доказательство.
$\Longrightarrow$: Пусть C - матрица перехода от $\mathcal{E}$ к $\tilde{\mathcal{E}}$, D - от $\tilde{\mathcal{E}}$ к $\mathcal{E}$. Тогда:

$$\begin{cases} (\tilde{e}_1, ..., \tilde{e}_n) = (e_1, ..., e_n) C \\ (e_1, ..., e_n) = (\tilde{e}_1, ..., \tilde{e}_n) D \end{cases} \Longrightarrow CD = DC = E \Longrightarrow D = C^{-1}$$

$$\det C \cdot \det D = \det CD = \det E = 1$$

Так как $C, D \in M_n(\mathbb{Z})$, $\det C, \det D \in \mathbb{Z} \Longrightarrow \det C = \pm 1$.
$\Longleftarrow$: $C \in M_n(\mathbb{Z}), \det C = \pm 1$. Рассмотрим некоторый базис $\mathcal{E} = \{e_1, ..., e_n\}$ и докажем, что $(\tilde{e}_1, ..., \tilde{e}_n) = (e_1, ..., e_n) C$ - базис.

1. Проверим линейную независимость:
   Если $\lambda_1 \tilde{e}_1 + ... + \lambda_n \tilde{e}_n = 0$, то линейная комбинация столбцов C с теми же λ_i также равна 0. Из $\det C \neq 0$ столбцы линейно независимы, т.е. $\lambda_i = 0\ \forall i$.

2. $\langle \tilde{e}_1 ..., \tilde{e}_n \rangle \stackrel{?}{=} A$:
   Так как $\det C = \pm 1$, $\exists D = C^{-1} \in M_n(\mathbb{Z})$ (из формулы явного выражения элементов обратной матрицы элементы D целые) $\Longrightarrow (e_1, ..., e_n) = (\tilde{e}_1, ..., \tilde{e}_n) D$.

$\forall a \in A$ целочисленно выражается через $e_1, ..., e_n$, каждый e_i целочисленно выражается через $\tilde{e}_1, ..., \tilde{e}_n \Longrightarrow a$ целочисленно выражается через $\tilde{e}_1, ..., \tilde{e}_n$

$\square$

4.2 Элементарные преобразования свободных абелевых групп

Определение. (ЭП свободных абелевых групп)
Пусть A - свободная абелева группа, $e_1, ..., e_n$ - базис A.

- **ЭП1**: $\tilde{e}_i = e_i + ke_j,\ i \neq j, k \in \mathbb{Z};\quad \tilde{e}_s = e_s,\ s \neq i;$
- **ЭП2**: $\tilde{e}_i = e_j;\quad \tilde{e}_j = e_i;\quad \tilde{e}_s = e_s,\ s \neq i, j\ (i \neq j);$
- **ЭП3**: $\tilde{e}_i = -e_i;\quad \tilde{e}_s = e_s,\ s \neq i;$

Матрицы перехода при этих ЭП:
ЭП1:

$$\begin{array}{c} \\ \\ i \\ \\ j \\ \\ \\ \end{array} \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 1 & & \lambda & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix}$$

ЭП2: :

$$\begin{array}{c} \\ \\ i \\ \\ j \\ \\ \\ \end{array} \begin{pmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & 1 & \\ & & & & & & 1 \end{pmatrix}$$

ЭП3:

$$\begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & -1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

называются (целочисленными) элементарными матрицами.

Определение. (ЭП строк целочисленных матриц)

- **ЭП1**: $\overline{a_i} \to \overline{a_i} + \lambda\overline{a_j}, \quad i \neq j, k \in \mathbb{Z}$;
- **ЭП2**: $\overline{a_i} \leftrightarrow \overline{a_j}, \quad i \neq j$;
- **ЭП3**: $\overline{a_i} \to (-1)\overline{a_i}$;

(Аналогично определены ЭП над столбцами матрицы)

Приведение целочисленной матрицы с помощью целочисленных ЭП к "диагональному" виду

Пусть $A = (a_{ij}) \in M_{n\times m}(\mathbb{Z})$. Будем говорить, что матрица A имеет "диагональный" вид, если либо $A = 0$, либо $a_{ii} = \alpha_i \in \mathbb{N}, i = \overline{1,l}$ и $a_{ij} = 0$ иначе.

$$A = \left(\begin{array}{ccc|c} \alpha_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & \alpha_l & \\ \hline & 0 & & 0 \end{array}\right)$$

Лемма. *Любую матрицу $M \in M_{n\times m}(\mathbb{Z})$ за конечное число целочисленных ЭП над строками и столбцами можно привести к "диагональному"виду.*

Доказательство. Индукция по n - числу строк матрицы. При фиксированном n индукция по $\nu(M)$ - наименьшему по модулю ненулевому элементу M.
Если $M = 0$, то утверждение доказано, поэтому далее $M \neq 0$.
База индукции: $n = 1 \Longrightarrow M = (a_{11}, ..., a_{1m})$.

База внутренней индукции: $\nu(M) = 1$ - очевидна (если в строке есть 1, то с помощью неё можно занулить все оставшиеся элементы).

Шаг внутренней индукции: Пусть $\nu(M) = |a_{1j}|$. Если $a_{1j} < 0$, то применим ЭП3 к стоблцу j; если $j > 1$, то применением ЭП2 поменяем 1-й и j-й столбцы местами. После этих операций $\nu(M) = a_{11}$.
$\forall j > 1 : a_{1j} = a_{11}q_j + r_j$, где $0 \leqslant r_j < a_{11}$. Вычитая с помощью ЭП1 из j-го столбца 1-й, умноженный на q_j, получим строку $\tilde{M} = (a_{11}, r_2, ..., r_m)$.
Если все $r_j = 0$, то диагональный вид получен, иначе можно воспользоваться предположением индукции $(\nu(\tilde{M}) < \nu(M))$.
Шаг индукции: Пусть $\nu(M) = |a_{ij}|$. Сначала сделаем a_{ij} положительным (ЭП3), затем переставим его в верхний левый угол (ЭП2).

Случай 1: $M = \left(\begin{array}{c|ccc} a_{11} & 0 & \dots & 0 \\ \hline 0 & & & \\ \vdots & & C & \\ 0 & & & \end{array}\right)$ - по предположению индукции приводим

C к диагональному виду;

Случай 2: $\exists j > 1 : a_{1j} \neq 0$. Тогда, аналогично базе индукции, с помощью ЭП1 приводим верхнюю строчку к виду: $\forall j > 1 : a_{1j} = 0$.

Случай 3: $\exists j > 1 : a_{j1} \neq 0$ - аналогично случаю 2 (ЭП строк вместо столбцов). $\square$

Упражнение. Доказать, что с помощью конечного числа целочисленных ЭП над строками и столбцами

$$M \sim \left(\begin{array}{ccc|c} \alpha_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & \alpha_l & \\ \hline & 0 & & 0 \end{array}\right)$$

где $\alpha_l \mid \alpha_{l-1}, \alpha_{l-1} \mid \alpha_{l-2}, ..., \alpha_2 \mid \alpha_1$.

Доказательство. По лемме можем с помощью ЭП привести M к диагональному виду. Индукция по l - числу ненулевых α в диагональном виде:

База: $l = 0, 1$ - очевидно;

Шаг: Из теории чисел знаем, что для чисел α_1, α_i существуют $a, b \in \mathbb{Z}$, что $a\alpha_1 + b\alpha_i = d_i = \text{НОД}(\alpha_1, \alpha_i)$. Значит, с помощью ЭП1 можно сделать $a_{1i} = d_i$. Тогда следующими операциями:

$$\begin{pmatrix} \alpha_1 & \cdots & 0 & \cdots & 0 \\ & \ddots & & & \\ 0 & & \alpha_i & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix} \sim \begin{pmatrix} \alpha_1 & \cdots & d_i & \cdots & 0 \\ & \ddots & & & \\ 0 & & \alpha_i & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix} \sim \begin{pmatrix} \alpha_1 & \cdots & d_i & \cdots & 0 \\ & \ddots & & & \\ k\alpha_1 & & 0 & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 0 & \cdots & d_i & \cdots & 0 \\ & \ddots & & & \\ k\alpha_1 & & 0 & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix} \sim \begin{pmatrix} k\alpha_1 & \cdots & 0 & \cdots & 0 \\ & \ddots & & & \\ 0 & & d_i & & 0 \\ & & & \ddots & \\ 0 & & & & \alpha_l \end{pmatrix}$$

можем сделать так, чтобы $\alpha_i \mid \alpha_1$. Причём α_1 при этих операциях домножается на $k \in \mathbb{Z}$, а значит, делимость на все предыдущие α_j сохраняется. Тогда за $l - 1$ таких наборов операций можно сделать α_1 общим кратным всех α, а матрица без первой строки и первого столбца приводится к нужному виду по предположению индукции. $\square$

Пример. $(12, 10, 6) \sim (6, 10, 12) \sim (6, 4, 0) \sim (4, 6, 0) \sim (4, 2, 0) \sim (2, 4, 0) \sim (2, 0, 0)$.

(По сути - обобщённый алгоритм Евклида, остаётся НОД чисел 12, 10 и 6).

4.3 Согласованные базисы свободной абелевой группы и её подгруппы

Теорема 1.
Пусть A - свободная абелева группа ранга $n, B \leq A$ - подгруппа ранга m. Тогда $\exists$ базисы $\tilde{e}_1, ..., \tilde{e}_n$ группы A и $\tilde{f}_1, ..., \tilde{f}_m$ подгруппы B такие, что $\tilde{f}_i = \alpha_i \tilde{e}_i,\ \alpha_i \in \mathbb{N}$.

Доказательство. Пусть $e_1, ..., e_n$ и $f_1, ..., f_m$ - некоторые базисы A и B соответственно. Так как $f_i \in A$, $(f_1, ..., f_m) = (e_1, ..., e_n)C$, где $C \in M_{n\times m}(\mathbb{Z})$.
Если $\tilde{f}_1, ..., \tilde{f}_m$ - другой базис B, то $(f_1, ..., f_m) = (\tilde{f}_1, ..., \tilde{f}_m)T$, где $T \in M_{m\times m}(\mathbb{Z})$
Если $\tilde{e}_1, ..., \tilde{e}_n$ - другой базис A, то $(e_1, ..., e_n) = (\tilde{e}_1, ..., \tilde{e}_n)S$, где $S \in M_{n\times n}(\mathbb{Z})$ $(\det T, S = \pm 1)$. Отсюда

$$(\tilde{f}_1, ..., \tilde{f}_m)T = (\tilde{e}_1, ..., \tilde{e}_n)SC \Longrightarrow (\tilde{f}_1, ..., \tilde{f}_m) = (\tilde{e}_1, ..., \tilde{e}_n)\tilde{C}, \quad \tilde{C} = SCT^{-1}$$

Тогда если S, T^{-1} - элементарные матрицы, то SC - ЭП над строками C, а CT^{-1} - ЭП над столбцами C. По лемме 1 C с помощью ЭП можно привести к виду $\tilde{C} = \begin{pmatrix} \begin{matrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_m \end{matrix} \\ \hline 0 \end{pmatrix}$ (нулей среди α_i не будет, т.к. векторы базиса f ЛНЗ). Отсюда и получаем требуемое равенство $\tilde{f}_i = \alpha_i \tilde{e}_i,\ \alpha_i \in \mathbb{N}$. □

Теорема. *(не было в лекции)*
Пусть $G = G_1 \times ... \times G_s$, $H = H_1 \times ... \times H_s$, причём $H \subseteq G$ и $H_i \trianglelefteq G_i$. Тогда $H \trianglelefteq G$ и $G/H = G_1/H_1 \times ... \times G_s/H_s$.

Доказательство.
Будем работать с внешним прямым произведением. Рассмотрим отображение

$$\varphi : G \to G_1/H_1 \times ... \times G_s/H_s$$

$$\varphi(g_1, ..., g_s) = (g_1H_1, ..., g_sH_s)$$

φ - гомоморфизм, так как по i-й компоненте φ реализует естественный гомоморфизм $G \to G/H_i$.
Ядро φ - наборы $(g_1, ..., g_s)$, которые отображаются в нейтральный элемент, т.е. в $(H_1, ..., H_s)$. Получаем

$$\varphi(g_1, ..., g_s) = (H_1, ..., H_s) \Longleftrightarrow g_i \in H_i,\ \forall i = 1, ..., s$$

Таким образом, $\operatorname{Ker} \varphi = H_1 \times ... \times H_s$.
Из определения φ очевидна сюръективность, т.е. $\operatorname{Im} \varphi = G_1/H_1 \times ... \times G_s/H_s$, а значит, из теоремы о гомоморфизме получаем необходимое утверждение. □

Замечание. Для абелевых групп из теоремы получим следующее утверждение:
Пусть $A = A_1 \oplus ... \oplus A_n$, $B \leq A$, $B = B_1 \oplus ... \oplus B_n$.
Тогда $A/B = (A_1 \oplus ... \oplus A_n)/(B_1 \oplus ... \oplus B_n) \simeq A_1/B_1 \oplus ... \oplus A_n/B_n$

Следствие 1. *В условиях теоремы 1:*

$$A/B \simeq \mathbb{Z}_{\alpha_1} \oplus ... \oplus \mathbb{Z}_{\alpha_m} \oplus \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{n-m}$$

Доказательство. По теореме 1: $\tilde{f}_1 = \alpha_1 \tilde{e}_1, ..., \tilde{f}_m = \alpha_m \tilde{e}_m$.

$A = \langle \tilde{e}_1 \rangle \oplus ... \oplus \langle \tilde{e}_m \rangle \oplus \langle \tilde{e}_{m+1} \rangle \oplus ... \oplus \langle \tilde{e}_n \rangle$; $B = \langle \alpha_1 \tilde{e}_1 \rangle \oplus ... \oplus \langle \alpha_m \tilde{e}_m \rangle \oplus \langle 0 \rangle \oplus ... \oplus \langle 0 \rangle$

Тогда из замечания выше:

$$A/B \simeq \langle \tilde{e}_1 \rangle / \langle \alpha_1 \tilde{e}_1 \rangle \oplus ... \oplus \langle \tilde{e}_m \rangle / \langle \alpha_m \tilde{e}_m \rangle \oplus \langle \tilde{e}_{m+1} \rangle / \langle 0 \rangle \oplus ... \oplus \langle \tilde{e}_n \rangle / \langle 0 \rangle \simeq$$

$$\simeq \mathbb{Z}_{\alpha_1} \oplus ... \oplus \mathbb{Z}_{\alpha_m} \oplus \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{n-m}$$

□

Следствие 2. *В условиях теоремы 1:* $\mathrm{rk}\ A = \mathrm{rk}\ B \Longleftrightarrow |A : B| < \infty$.

Доказательство. По определению $|A : B| = |A/B|$.
Из следствия 1 видно, что если $\mathrm{rk}\ A = \mathrm{rk}\ B$, то $A/B \simeq \mathbb{Z}_{\alpha_1} \oplus ... \oplus \mathbb{Z}_{\alpha_n}$, и $|A/B| < \infty$, а иначе в прямой сумме встретится слагаемое $\mathbb{Z}$, то есть найдётся элемент бесконечного порядка. □

Утверждение 1. *(Универсальное свойство абелевой группы)*
Пусть $S = \{a_1, ..., a_n\}$ - система порождающих абелевой группы A.
Тогда следующие утверждения эквивалентны:

1. *A - свободная с базисом S;*
2. *$\forall$ абелевой группы D, $\forall\ d_1, ..., d_n \in D\ \exists!$ гомоморфизм $\varphi : A \to D$ т.ч. $\varphi : a_i \mapsto d_i\ \forall i$.*

Доказательство.
$1 \Longrightarrow 2$: S - базис $A \Longrightarrow \forall a \in A\ \exists! \alpha_i \in \mathbb{Z} : a = \alpha_1 a_1 + ... + \alpha_n a_n$.
Рассмотрим отображение $\varphi : A \to D$, заданное как $a = \alpha_1 a_1 + ... + \alpha_n a_n \mapsto \alpha_1 d_1 + ... + \alpha_n d_n$. Оно корректно вследствие единственности разложения по базису, а также очевидно является гомоморфизмом с нужным свойством.
$2 \Longrightarrow 1$. Рассмотрим свободную группу D ранга n, в ней рассмотрим базис

$d_1, ..., d_n$. По условию $\exists!$ гомоморфизм $\varphi : A \to D$, причём $a_i \mapsto d_i$.
Предположим, что $a_1, ..., a_n$ линейно зависимы. Тогда

$$\lambda_1 a_1 + ... + \lambda_n a_n = 0 \Longrightarrow \varphi(\lambda_1 a_1 + ... + \lambda_n a_n) = \lambda_1 d_1 + ... + \lambda_n d_n = 0$$

Противоречие с линейной независимостью $d_1, ..., d_n$. Значит, $a_1, ..., a_n$ - базис. □

Следствие 3. *Любая конечнопорождённая абелева группа изоморфна свободной абелевой группе по некоторой её подгруппе B.*

Доказательство. Пусть $D = \langle d_1, ..., d_n \rangle$. Рассмотрим свободную абелеву группу A ранга n с базисом $a_1, ..., a_n$.
По утверждению 1 $\exists$ гомоморфизм $\varphi : A \to D$ такой, что $\varphi(a_i) = d_i$.
Из порождаемости гомоморфизм сюръективен, а значит, по теореме о гомоморфизме $D = \mathrm{Im}\ \varphi \simeq A/\mathrm{Ker}\ \varphi$, где $\mathrm{Ker}\ \varphi \leq A$. □

Следствие 4. *Любая конечнопорождённая абелева группа раскладывается в сумму циклических подгрупп.*

Доказательство. $D \simeq A/B \simeq \mathbb{Z}_{\alpha_1} \oplus ... \oplus \mathbb{Z}_{\alpha_m} \oplus \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{n-m}$ □

Следствие 5. *Любая конечнопорождённая абелева группа D раскладывается в прямую сумму конечной абелевой группы и свободной абелевой группы.*

Доказательство. $D \simeq (\mathbb{Z}_{\alpha_1} \oplus ... \oplus \mathbb{Z}_{\alpha_m}) \oplus \mathbb{Z}^{n-m}$ □

Определение. Группа, в которой каждый неединичный элемент имеет бесконечный порядок, называется группой без кручения.

Упражнение. Если A - свободная абелева, то A - без кручения.

Доказательство. Предположим, что $b \in A$ - элемент конечного порядка m. По определению свободной группы $b = \alpha_1 a_1 + ... + \alpha_n a_n$, причём не все α_i равны 0. Тогда $m\alpha_1 a_1 + ... + m\alpha_n a_n = mb = 0$ - противоречие с линейной независимостью базиса. □

Следствие 6. *Если A - конечнопорождённая абелева группа без кручения, то A - свободная абелева группа.*

Доказательство. В обозначениях следствия 5 $m = 0$. □

4.4 Основная теорема о конечнопорождённых абелевых группах

Определение. Группа G называется периодической, если $\forall g \in G$ g имеет конечный порядок.

Определение. Периодическая группа G называется p-группой, где p - простое, если $\forall g \in G$ $\exists s \in \mathbb{N} : \operatorname{ord} g = p^s$.

Упражнение.
Доказать, что конечная группа G является p-группой $\Longleftrightarrow |G| = p^m$ $(m \in \mathbb{N})$.

Доказательство.
$\Longleftarrow$ - очевидно, т.к. $\forall g \in G : \ \operatorname{ord} g \mid p^m = |G|$;
$\Longrightarrow$: на будущих лекциях будет доказательство в терминах силовских подгрупп.
□

Определение. Группа G называется примарной, если G является p-группой для некоторого простого p.

Утверждение. *Существуют конечнопорождённые (не абелевы) бесконечные p-группы.*

Доказательство. Без доказательства. □

Пример. Не конечнопорождённая примарная абелева группа:
$\mathbb{C}_{p^\infty}$ - группа комплексных корней степеней p^m из 1.

Лемма 1. *Пусть A - конечнопорождённая абелева группа, $B \leq A$ такая, что A/B - свободная абелева группа. Тогда $\exists$ $C \leq A$ - свободная абелева группа такая, что $A \simeq B \oplus C$.*

Доказательство. Пусть $\overline{e}_1, ...\overline{e}_n$ - базис $\mathbb{Z}^n \simeq A/B$, и пусть $\varphi : A/B \to \mathbb{Z}^n$ - изоморфизм. Тогда $\varphi^{-1}(\overline{e}_i) = e_i + B$, где $e_i \in A$.
Рассмотрим $C = \langle e_1, ..., e_n \rangle$.
Покажем, что $e_1, ..., e_n$ - базис C, т.е. докажем линейную независимость $e_1, ..., e_n$:

$$\lambda_1 e_1 + ... + \lambda_n e_n = 0 \Longrightarrow \lambda_1 e_1 + ... + \lambda_n e_n + B = B \Longrightarrow \varphi(\lambda_1 e_1 + ... + \lambda_n e_n + B) =$$

$$= \lambda_1 \overline{e}_1 + ... + \lambda_n \overline{e}_n = 0 \Longrightarrow \forall i \ \lambda_i = 0 \ \text{ т.к. } \overline{e}_1, ...\overline{e}_n \text{ - базис } \mathbb{Z}^n$$

Покажем, что $A = B \oplus C$, или, что равносильно, что $A = B + C$ и $B \cap C = \{0\}$:

- $B \cap C = \{0\}$: Рассмотрим $b \in B \cap C$. Тогда:

$$b = \mu_1 e_1 + ... + \mu_n e_n \Longrightarrow \mu_1 e_1 + ... + \mu_n e_n + B = b + B = B \Longrightarrow$$

$$\Longrightarrow \varphi(\lambda_1 e_1 + ... + \lambda_n e_n + B) = \lambda_1 \overline{e}_1 + ... + \lambda_n \overline{e}_n = 0 \Longrightarrow \forall i \ \lambda_i = 0$$

- $A = B + C$: Рассмотрим произвольный $a \in A$.
$\varphi(a + B) = \overline{a} \in \mathbb{Z}^n$, где $\overline{a} = \mu_1 \overline{e}_1 + ... + \mu_n \overline{e}_n$. Тогда

$$\varphi(a - \sum_i \mu_i e_i + B) = 0 \Longrightarrow a - \sum_i \mu_i e_i + B = B \Longrightarrow \exists\, b \in B : a = b + \sum_i \mu_i e_i$$

□

Лемма 2. *Все элементы конечного порядка абелевой группы A образуют подгруппу в A.*

Доказательство. Обозначим за Tor A множество всех элементов конечного порядка группы A.

1. $a, b \in \text{Tor } A \Longrightarrow \exists\, n, m \in \mathbb{N} : na = mb = 0 \Longrightarrow$
$\Longrightarrow (n \cdot m)(a + b) = (n \cdot m)a + (n \cdot m)b = 0 \Longrightarrow (a + b)$ имеет конечный порядок.

2. $0 \in \text{Tor } A$ - очевидно.

3. $\forall a \in \text{Tor } A \Longrightarrow -a \in \text{Tor } A$, т.к. $n(-a) = -na = 0$.

□

Определение. Подгруппа Tor A ("torsion subgroup") называется подгруппой кручения группы A.

Упражнение. Доказать, что в группе $D_\infty = \langle a, b \mid a^2 = 1, aba^{-1} = b^{-1} \rangle$ все элементы конечного порядка не образуют подгруппу.

Замечание. Группа Диэдра D_n отлична от D_∞ наличием соотношения $b^n = 1$, (a - любая симметрия правильного n-угольника, b - поворот на $\frac{2\pi}{n}$).

Доказательство. Заметим, что ord $ba = 2$:

$$a = a^{-1} \Longrightarrow baba = b(aba^{-1}) = bb^{-1} = 1$$

Также ord $a = 2 : a^2 = 1$. При этом ord $(ba)a =$ ord $b = \infty$. Значит, произведение элементов конечного порядка может быть элементом бесконечного порядка, т.е. все элементы конечного порядка не образуют подгруппу в D_∞. □

Лемма 3. *Пусть A - абелева группа. Тогда $A/\mathrm{Tor}\ A$ - группа без кручения.*

Доказательство. От противного: пусть $\overline{a} \in A/\mathrm{Tor}\ A, \overline{a} \neq 0, \mathrm{ord}\ \overline{a} = n$.
Тогда $\overline{a} = a + \mathrm{Tor}\ A,\ a \in A$.

$$n\overline{a} = 0 \Longrightarrow n(a + \mathrm{Tor}\ A) = \mathrm{Tor}\ A \Longrightarrow na \in \mathrm{Tor}\ A \Longrightarrow$$

$$\Longrightarrow \exists\ m \in \mathbb{N} : m(na) = 0 \Longrightarrow (mn)a = 0 \Longrightarrow a \in \mathrm{Tor}\ A \Longrightarrow \overline{a} = 0$$

- противоречие с $\overline{a} \neq 0$. Значит, $A/\mathrm{Tor}\ A$ - группа без кручения. □

Лемма 4. *Пусть A - конечнопорождённая абелева группа. Тогда $A = \mathrm{Tor}\ A \oplus C$, где $C \leq A$ - свободная абелева группа,* $\mathrm{Tor}\ A$ *- конечная.*

Доказательство. Пусть $A = \langle a_1, ..., a_n \rangle$.
Тогда $A/\mathrm{Tor}\ A = \langle a_1 + \mathrm{Tor}\ A, ..., a_n + \mathrm{Tor}\ A \rangle$. Кроме того, по лемме 3 $A/\mathrm{Tor}\ A$ - группа без кручения, а отсюда по следствию 6 из универсального свойства абелевой группы - свободная. Отсюда по лемме 1 $\exists\ C \leq A$ - свободная абелева группа такая, что $A \simeq \mathrm{Tor}\ A \oplus C$.
Осталось показать, что $\mathrm{Tor}\ A$ - конечная: $\mathrm{Tor}\ A \simeq A/C = \langle a_1 + C, ..., a_n + C \rangle \Longrightarrow \mathrm{Tor}\ A = \langle b_1, ..., b_n \rangle$ - конечнопорождённая. Тогда если $k_i = \mathrm{ord}\ b_i$, то $\forall b \in \mathrm{Tor}\ A$

$$b = \lambda_1 b_1 + ... + \lambda_n b_n,\ \lambda_i \in \mathbb{Z}, 0 \leqslant \lambda_i < k_i \Longrightarrow |\mathrm{Tor}\ A| \leqslant k_1 ... k_n$$

□

Лемма 5. *Пусть A - конечная абелева группа. Тогда A раскладывается в прямую сумму своих p-подгрупп A_p, причём набор этих подгрупп определён однозначно.*

Доказательство.

- Существование разложения:
  Рассмотрим произвольное простое p и обозначим за A_p множество всех элементов A порядков p^m. Проверим, что A_p - подгруппа A:

  1. $a, b \in A_p, p^{m_1}a = p^{m_2}b = 0 \Longrightarrow p^{m_1+m_2}(a+b) = p^{m_2} \cdot p^{m_1}a + p^{m_1} \cdot p^{m_2}b = 0$
     Отсюда $a, b \in A_p \Longrightarrow a + b \in A_p$;
  2. $0 \in A_p$ - очевидно;
  3. $p^m a = 0 \Longrightarrow p^m(-a) = -p^m a = 0$. Отсюда $a \in A_p \Longrightarrow -a \in A_p$.

  Докажем, что $A = A_{p_1} \oplus ... \oplus A_{p_s}$:

1. $A_{p_1} \oplus ... \oplus A_{p_s}$ - прямая сумма.
   По критерию прямой суммы достаточно показать, что $A_{p_i} \cap \langle \bigcup\limits_{j \neq i} A_{p_j} \rangle = \{0\}$. Рассмотрим $a \in A_{p_i} \cap \langle \bigcup\limits_{j \neq i} A_{p_j} \rangle$. Так как $a \in A_{p_i}$, то $p_i^{m_i} a = 0$. С другой стороны, $a = \sum\limits_{j \neq i} a_j$, то есть $(\prod\limits_{j \neq i} p_j^{m_j}) a = 0$.
   Так как $\prod\limits_{j \neq i} p_j^{m_j}$ и $p_i^{m_i}$ взаимно просты, имеем $1 \cdot a = a = 0$.
2. $A = A_{p_1} \oplus ... \oplus A_{p_s}$. Рассмотрим произвольный $a \in A$. Пусть $\text{ord } a = n = p_1^{\alpha_1} ... p_s^{\alpha_s}$. Обозначим $n_i = \frac{n}{p_i^{\alpha_i}}$.
   Так как НОД$(n_1, ..., n_s) = 1, \exists\ l_i \in \mathbb{Z} : l_1 n_1 + ... + l_s n_s = 1$. Отсюда $a = l_1 n_1 a + ... + l_s n_s a$. Так как $p_i^{\alpha_i}(l_i n_i a) = l_i n a = 0$, имеем $l_i n_i a \in A_{p_i}$.
   Значит, a раскладывается в линейную комбинацию элементов A_{p_i}.

- Единственность разложения - от противного: пусть

$$A = \tilde{A}_{\tilde{p}_1} \oplus ... \oplus \tilde{A}_{\tilde{p}_s} = A_{p_1} \oplus ... \oplus A_{p_s}$$

Очевидно, что (возможно, после переупорядочивания) $p_i = \tilde{p}_i$, так как порядок подгруппы конечной группы делит порядок группы. Так как A_{p_i} - максимальная p_i-подгруппа в A (содержит все элементы A порядка p_i^m), $\tilde{A}_{p_i} \subseteq A_{p_i}$.
Предположим, что $\exists a \in A_{p_i} : a \notin \tilde{A}_{p_i}$. Так как $a \in A = \tilde{A}_{p_1} \oplus ... \oplus \tilde{A}_{p_s}$, $a = \tilde{a}_{p_i} + b$, где $\tilde{a}_{p_i} \in \tilde{A}_{p_i}, b \in \langle \bigcup\limits_{j \neq i} A_{p_j} \rangle$. Тогда $\text{ord } a = p_i^{m_1}, \text{ord } \tilde{a}_{p_i} = p_i^{m_2} \Longrightarrow$

$$p_i^{m_1+m_2} a = p_i^{m_1+m_2} \tilde{a}_{p_i} + p_i^{m_1+m_2} b \Longrightarrow p_i^{m_1+m_2} b = 0, \text{а также } \prod_{j \neq i} p_j^{\alpha_j} b = 0$$

$\prod\limits_{j \neq i} p_j^{\alpha_j}$ и $p_i^{m_1+m_2}$ взаимно просты $\Longrightarrow b = 0$, т.е. $a = \tilde{a}_{p_i} \in \tilde{A}_{p_i}$ - противоречие.
Значит, такого a не существует, то есть $A_{p_i} \subseteq \tilde{A}_{p_i}$. Отсюда $A_{p_i} = \tilde{A}_{p_i}$.

□

Лемма 6. *Пусть A - конечная абелева p-группа. Тогда если $A = A_1 \oplus ... \oplus A_s = B_1 \oplus ... \oplus B_t$, где A_i, B_i - примарные циклические подгруппы, то $s = t$ и набор порядков $|A_1|, ..., |A_s|$ совпадает с набором порядков $|B_1|, ..., |B_t|$ (т.е. разложение единственно с точностью до порядка слагаемых).*

Доказательство. Индукция по $|A|$:
База: $|A| = p \Longrightarrow A \simeq \mathbb{Z}_p$ - такое разложение единственно;
Шаг: Пусть $|A_i| = p^{n_i}, |B_i| = p^{m_i}$. Упорядочим их: пусть

$$n_1 \geqslant n_2 \geqslant ... \geqslant n_{\tilde{s}} \geqslant n_{\tilde{s}+1} = ... = n_s = 1$$

$$m_1 \geqslant m_2 \geqslant ... \geqslant m_{\tilde{t}} \geqslant m_{\tilde{t}+1} = ... = m_t = 1$$

Пусть $A_i = \langle a_i \rangle_{p^{n_i}}, B_i = \langle b_i \rangle_{p^{m_i}}$. Рассмотрим множество $pA = \{pa \mid a \in A\}$. Очевидно, что $pA \leq A$. Тогда:

$$A = \langle a_1 \rangle \oplus ... \oplus \langle a_{\tilde{s}} \rangle \oplus \langle a_{\tilde{s}+1} \rangle \oplus ... \oplus \langle a_s \rangle$$

$$\forall a \in A: \ a = \alpha_1 a_1 + ... + \alpha_{\tilde{s}} a_{\tilde{s}} + \alpha_{\tilde{s}+1} a_{\tilde{s}+1} + ... + \alpha_s a_s \Longrightarrow pa = \alpha_1 pa_1 + ... + \alpha_{\tilde{s}} pa_{\tilde{s}}$$

($A_{\tilde{s}+1}, ..., A_s$ - циклические порядка p, поэтому $\alpha_{\tilde{s}+1} pa_{\tilde{s}+1} + ... + \alpha_s pa_s = 0$)
Тогда $pA = \langle pa_1 \rangle \oplus ... \oplus \langle pa_{\tilde{s}} \rangle$. При этом $\mathrm{ord}\ (pa_1) = p^{n_1-1}, ..., \mathrm{ord}\ (pa_{\tilde{s}}) = p^{n_{\tilde{s}}-1}$.
Значит, $|pA| = p^{n_1+...+n_{\tilde{s}}-\tilde{s}} < |A|$.
Аналогично $pA = \langle pb_1 \rangle \oplus ... \oplus \langle pb_{\tilde{t}} \rangle, |pA| = p^{m_1+...+m_{\tilde{t}}-\tilde{t}} < |A|$.
Тогда по предположению индукции разложения pA совпадают (порядок слагаемых одинаковый в силу упорядоченности), то есть

$$\tilde{s} = \tilde{t}; \quad \forall i = \overline{1...\tilde{s}}: \ n_i - 1 = m_i - 1 \Longrightarrow n_i = m_i$$

При этом $|A| = |A_1| \cdot ... \cdot |A_{\tilde{s}}| \cdot |A_{\tilde{s}+1}| \cdot ... \cdot |A_s| = p^{n_1+...+n_{\tilde{s}}+s-\tilde{s}}$, а с другой стороны $|A| = |B_1| \cdot ... \cdot |B_{\tilde{t}}| \cdot |B_{\tilde{t}+1}| \cdot ... \cdot |B_t| = p^{m_1+...+m_{\tilde{t}}+t-\tilde{t}}$. Отсюда

$$n_1 + ... + n_{\tilde{s}} + s - \tilde{s} = m_1 + ... + m_{\tilde{t}} + t - \tilde{t}; \ \tilde{s} = \tilde{t}; \ n_i = m_i \Longrightarrow s = t$$

□

Теорема. ***(Основная т. о конечнопорождённых абелевых группах)***
Пусть A - конечнопорождённая абелева группа. Тогда A изоморфна прямой сумме (конечных) примарных циклических подгрупп и бесконечных циклических подгрупп:

$$A \simeq \mathbb{Z}_{p_1^{s_1}} \oplus ... \oplus \mathbb{Z}_{p_k^{s_k}} \oplus \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{m}$$

причём число m и набор $p_1^{s_1}, ..., p_k^{s_k}$ определены однозначно для группы A.

Доказательство.

- **Существование разложения**
  Из следствия 4 универсального свойства абелевой группы для A имеем:

  $$A \simeq A_0/B_0 \simeq \mathbb{Z}_{\alpha_1} \oplus ... \oplus \mathbb{Z}_{\alpha_m} \oplus \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{n-m}$$

  Также из аналога китайской теоремы об остатках знаем, что если $\alpha = q_1^{\nu_1} ... q_\mu^{\nu_\mu}$, где q_i - различные простые, то $\mathbb{Z}_\alpha = \mathbb{Z}_{q_1^{\nu_1}} \oplus ... \oplus \mathbb{Z}_{q_\mu^{\nu_\mu}}$. Отсюда из разложения выше получаем искомое разложение.

- **Единственность разложения**

  По лемме 4 для A имеет место разложение $A = \text{Tor } A \oplus C$, где $\text{Tor } A$ - конечная, C - свободная. Заметим, что $\text{rk } C = \text{rk } A/\text{Tor } A$. Так как $\text{Tor } A$ - инвариант A, то $A/\text{Tor } A$, а тогда и $\text{rk } C$ - инварианты A.

  Так как $C \simeq \mathbb{Z} \oplus ... \oplus \mathbb{Z}$, а $\mathbb{Z}_{p_1^{s_1}} \oplus ... \oplus \mathbb{Z}_{p_k^{s_k}}$ - конечная, имеем $C = \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{m}$, то есть $m = \text{rk } C$, а отсюда m однозначно определено для A.

  Пусть $B = \text{Tor } A$. По лемме 5 $B \simeq A_{\tilde{p}_1} \oplus ... \oplus A_{\tilde{p}_l}$, причём это разложение на примарные подгруппы единственно с точностью до порядка слагаемых. А из леммы 6 каждая $A_{\tilde{p}_i}$ раскладывается на циклические примарные однозначно с точностью до порядка слагаемых. Значит, набор порядков $p_1^{s_1}, ..., p_k^{s_k}$ определён однозначно для A.

$\square$

Пример. Все абелевы группы порядка 8 с точностью до изоморфизма:
$8 = 2^3 = 2^2 \cdot 2 = 2 \cdot 2 \cdot 2 \Longrightarrow A_1 \simeq \mathbb{Z}_8;\ A_2 \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2;\ A_3 = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Пример. $V_4 = \{e, a, b, c\}$
$V_4 = \langle a \rangle_2 \oplus \langle b \rangle_2 = \langle b \rangle_2 \oplus \langle c \rangle_2$, но разложение из теоремы единственно: $V = \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Замечание. Для не конечнопорождённых абелевых групп утверждение теоремы неверно, контрпримером служит следующее упражнение:

Упражнение. Доказать, что $\mathbb{Q}$ не раскладывается в прямую сумму циклических (вообще говоря, произвольных) подгрупп.

Доказательство. Пусть $H_1, H_2 \trianglelefteq \mathbb{Q}$ - нетривиальные нормальные подгруппы $\mathbb{Q}$. Тогда $\exists\ h_1 = \in H_1, h_2 \in H_2 : h_1, h_2 \neq 0$. Тогда:

$$h_1 = \frac{m_1}{n_1}, h_2 = \frac{m_2}{n_2} \Longrightarrow m_2 n_1 h_1 = m_1 n_2 h_2 \in H_1 \cap H_2$$

то есть $H_1 \cap H_2 \neq \{0\}$. Отсюда $\mathbb{Q}$ не раскладывается в прямую сумму подгрупп.

$\square$

Определение. Экспонентой (периодом, показателем) конечной группы G называется наименьшее общее кратное порядков элементов группы G.
Обозначается $\exp G$.

Утверждение. *Если G конечна, то $\exp G \mid |G|$*

Доказательство. Для конечных групп знаем, что порядок группы является общим кратным всех порядков элементов группы. Так как наименьшее общее кратное набора чисел делит любое общее кратное этого набора, получаем необходимое утверждение. $\square$

Утверждение. *Конечная абелева группа A циклическая* $\iff \exp A = |A|$.

Доказательство.
$\Longrightarrow$: $A = \langle a \rangle \Longrightarrow \operatorname{ord} a = |A| \Longrightarrow \exp A \geqslant |A| \Longrightarrow \exp A = |A|$ (т.к. $\exp A \mid |A|$).
$\Longleftarrow$: От противного: пусть $\exp A = |A|$, но A - не циклическая. По основной теореме о конечнопорождённых абелевых группах $A \simeq \mathbb{Z}_{p_1^{s_1}} \oplus ... \oplus \mathbb{Z}_{p_m^{s_m}}$. Если все $p_1, ..., p_m$ различны, то A циклическая по аналогу китайской теоремы об остатках - противоречие. Если среди них есть совпадающие, то можем без ограничения общности считать, что $p_1 = p_2, s_1 \leqslant s_2$. Обозначим $\mathbb{Z}_{p_i^{s_i}} = \langle a_i \rangle \Longrightarrow \forall a \in A:$ $a = \sum\limits_{i=1}^{m} \alpha_i a_i$. Тогда если в равенстве $|A| = p_1^{s_1} p_2^{s_2} ... p_m^{s_m}$ обозначить $t = p_2^{s_2} ... p_m^{s_m}$, то $\forall a \in A:\ ta = \sum\limits_{i=1}^{m} \alpha_i t a_i = 0$.
(очевидно, что $ta_i = 0$ для $a \neq 1$, а $ta_1 = 0$ в силу $p_1 = p_2, s_1 \leqslant s_2$)
Тогда t - общее кратное всех порядков элементов A, то есть $\exp A \mid t$, но $t < A = \exp A$ - противоречие. Значит, A - циклическая. $\square$

Теорема. *Пусть $\mathbb{F}$ - произвольное поле, A - конечная подгруппа в $\mathbb{F}^*$.*
Тогда A - циклическая.

Доказательство. (мультипликативная терминология)
Из определения поля F^* - абелева группа, а значит A также абелева.
От противного: пусть A не циклическая, т.е. $\exp A < |A|$. Тогда если $\exp A = n$, то $\forall a \in A\ a^n = 1$. Рассмотрим многочлен $x^n - 1$ над полем $\mathbb{F}$. Его степень равна n, а число его корней в $\mathbb{F}$ хотя бы $|A|$, что больше n по предположению - противоречие. $\square$

Пример. $\mathbb{F} = \mathbb{Z}_p:\ A = F^*$ - циклическая. Например, $\mathbb{Z}_5^* = \langle 3 \rangle_4$.

Следствие. *Мультипликативная группа любого конечного поля - циклическая.*

5 Действия группы на множестве

Определение. Пусть X - произвольное множество. Биективное отображение $f : X \to X$ называется преобразованием множества X.
Множество всех преобразований X обозначается $S(X)$.

Утверждение. $S(X)$ - *группа относительно композиции.*

Доказательство.

1. Ассоциативность - очевидно;

2. Нейтральный элемент - тождественное преобразование;

3. Обратный элемент - обратное преобразование (существует, т.к. биекция)

$\square$

Определение. Группа $S(X)$ называется группой всех преобразований X.
Произвольная $H \leq S(X)$ называется группой преобразований множества X.

Пример. $GL(V)$ - группа невырожденных линейных операторов векторного пространства $V : GL(V) \leq S(V)$.

Определение. Пусть G - произвольная группа, X - произвольное множество. Действием группы G на множестве X называется гомоморфизм $\alpha : G \to S(X)$.
Обозначается $G \curvearrowright X$ (или $G : H$)
Элементы множества X при этом называются точками.
$\forall g \in G : g \mapsto \alpha(g)$ - преобразование множества X, т.е. биекция $X \to X$.
Равенство $\alpha(g)(x) = y (\in X)$ записывают как $\alpha(g)x = y$ или $gx = y$.

Так как α - гомоморфизм, имеем:

$\forall g_1, g_2 \in G : \alpha(g_1 g_2) = \alpha(g_1)\alpha(g_2) \Longrightarrow \alpha(g_1 g_2)x = (\alpha(g_1)\alpha(g_2))x = \alpha(g_1)(\alpha(g_2)x)$

Отсюда $(g_1 g_2)x = g_1(g_2 x)$. Аналогично:

$$\forall g \in G : \alpha(g^{-1}) = (\alpha(g))^{-1} \Longrightarrow \alpha(g^{-1})x = (\alpha(g)x)^{-1}$$

Отсюда $g^{-1}x = y \Longleftrightarrow gy = x$.
Если $H \leq S(X)$, то определено "тавтологическое" действие H на $X : \alpha(h) = h$ - вложение $H \to S(X)$.

Пример. $GL(V) \curvearrowright V$: $\alpha(g)x = x \ \forall g \in G, x \in X$

В общем случае: $\alpha G \to S(X)$ - гомоморфизм, то есть $\mathrm{Im}\ \alpha \leq S(X), \mathrm{Ker}\ \alpha \trianglelefteq G$.

Определение. Ker α называется ядром неэффективности действия группы G на X.
Если $\mathrm{Ker}\ \alpha = \{e\}$, то действие называется эффективным.

Замечание. Всякое действие группы G на множестве X индуцирует и другие действия. Например:

1. $G \curvearrowright 2^X$;

2. Если $Y \subset X$ - инвариантное подмножество относительно G, то $G \curvearrowright Y$.

Пример. Пусть K - равносторонний треугольник, $G = \mathrm{Sym}\ K \leq S(X)$, где X - множество точек треугольника.
Тогда если $Y = \{v_1, v_2, v_3\}$ - вершины треугольника, а $Z = \{e_1, e_2, e_3\}$ - стороны треугольника, то действие $G \curvearrowright X$ индуцирует также и действия $G \curvearrowright Y, G \curvearrowright Z$

Пример. Пусть задано $G \curvearrowright X$, $\mathbb{F}$ - поле, $Y = \{f : X \to \mathbb{F}\}$ - алгебра всех функций $X \to \mathbb{F}$. Рассмотрим $\alpha : G \to S(Y) : \forall g \in G\ \alpha(g)f = \tilde{f}$ такое, что $\tilde{f}(x) = f(g^{-1}x)\ \forall x \in X$. Покажем, что α - гомоморфизм:

$$\forall g_1, g_2 \in G: \ (\alpha(g_1g_2)f)(x) = f((g_1g_2)^{-1}(x)) = f(g_2^{-1}(g_1^{-1}x)) = (\alpha(g_2)f)(g_1^{-1}x) =$$

$$= \alpha(g_1)(\alpha(g_2)f)(x) = (\alpha(g_1)\alpha(g_2)f)(x)$$

Замечание. Если $G \curvearrowright X, H \leq G$, то определено также действие $H \curvearrowright X$ - ограничение действия на подгруппу.

Пример. $G = S_3 \curvearrowright X$, где $X = \{1, 2, 3\}$ - действуют как подстановки.
$H = \langle(1, 2, 3)\rangle \leq G$ - определено действие $H \curvearrowright X$ как ограничение $G \curvearrowright X$.