ОСНОВЫ ТЕОРИИ ГРУПП

1.1 Основные понятия

Определение 1.1. *Группа* — это непустое множество G с бинарной операцией $\cdot$, обладающей следующими свойствами:

- Ассоциативность: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Существование нейтрального элемента: $\exists e \in G$: $\forall a \in G$ $ae = ea = a$
- Существование обратного элемента: $\forall a \in g$ $\exists a^{-1} \in G$: $aa^{-1} = a^{-1}a = e$

Обозначение — $(G, \cdot)$, если операция очевидна — просто G. Группа называется *абелевой*, если операция $\cdot$ коммутативна ($a \cdot b = b \cdot a$).

Замечание. Нейтральный и обратные элементы единственны.

Определение 1.2. *Подгруппа* $H < G$ — это непустое подмножество $H \subseteq G$, замкнутое относительно операций: $\forall a, b \in H$ $a \cdot b \in H$, $\forall a \in H$ $a^{-1} \in H$.

Замечание. H — также группа, с той же операцией (ограниченной на H).

Определение 1.3. *Порядок группы* — число её элементов $|G|$. *Порядок элемента* группы $g \in G$ — это наименьшее $n \in \mathbb{N}$ такое, что $g^n = e$ (и ∞, если такого n нет). Обозначение: $|g|$ или $\operatorname{ord} g$.

Определение 1.4. Если $M \subset G$, то *подгруппа, порождённая* M — это пересечение всех подгрупп, содержащих M. Также $\langle M \rangle = \{a_1 \dots a_n \mid a_i \in M \vee a_i^{-1} \in M\}$. Обозначение: $\langle M \rangle$. Если существует $g \in G$ такой, что $\langle g \rangle = G$, то группа G — *циклическая.*

Пример. $\langle G \rangle = G$, $\langle \varnothing \rangle = \{e\}$.

Замечание. $\operatorname{ord} g = |\langle g \rangle|$.

Определение 1.5. Биекция $\varphi : G \to H$, сохраняющая операцию ($\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$), называется *изоморфизмом групп* G и H. Если он существует, то G и H *изоморфны* ($G \cong H$).

1.2 Примеры групп

1. $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$ — единственные (с точностью до изоморфизма) циклические группы. Подгруппа циклической группы — также циклическая.
2. $(F, +)$, $(F^*, \cdot)$, где F — поле.
3. $(V, +)$, где V — линейное пространство.

4. S_n — группа перестановок n элементов (т. е. биекций $\{1, \dots, n\} \to \{1, \dots, n\}$) относительно композиции. Перестановку можно записать в виде таблицы, или же в виде произведение независимых циклов (цикл $\pi = (a_1 \dots a_k)$ — это перестановка такая, что $\pi(a_i) = a_{i+1}$ для $i = 1, \dots, k-1$ и $\pi(a_k) = a_1$, остальные элементы неподвижны). Кроме того, S_n порождается множеством всех транспозиций. Знак перестановки $\sigma \in S_n$ есть $(-1)^\sigma = \operatorname{sgn} \sigma = (-1)^{N(\sigma)}$, где $N(\sigma)$ — число инверсий в σ (совпадает по чётности с количеством транспозиций в любом разложении σ).

5. $GL_n(F)$ — группа невырожденных матриц над F относительно умножения.

6. $GL(V)$, где V — линейное пространство над F, — обратимые преобразования V относительно композиции. $GL(V) \cong GL_{\dim V}(F)$.

7. Подгруппы этих групп, в частности:
   - $A_n < S_n$ — подгруппа всех чётных перестановок.
   - $SL_n(F) < GL_n(F)$ — подгруппа всех матриц с единичным определителем.
   - $O_n < GL_n(\mathbb{R})$ — подгруппа всех ортогональных матриц.
   - $\mathbb{C}_n < \mathbb{C}^*$: $\mathbb{C}_n = \{z \in \mathbb{C} \mid z^n = 1\}$, $\mathbb{C}_n \cong \mathbb{Z}_n$.

1.3 Смежные классы

Определение 1.6. Пусть $H < G$, $g \in G$. *Левый смежный класс* элемента g по H — это gH, *правый* — Hg, где $AB = \{ab \mid a \in A, b \in B\}$ для $A, B \subset G$ (вместо одного элемента подразумевается множество из этого элемента). G/H — множество всех левых смежных классов по H, $H \backslash G$ — правых.

Замечание. Для любых $a, b \in G$ $aH \cap bH \neq \varnothing \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH = bH \Leftrightarrow b \in aH$. Значит, левые (правые) смежные классы — разбиение G.

Утверждение 1.1. *Пусть $H < G$. Тогда G/H равномощно $H \backslash G$.*

Доказательство. Построим биекцию $\varphi : G/H \to H \backslash G$: $\varphi(gH) = Hg^{-1}$. Заметим, что $\varphi(gH) = Hg^{-1} = H^{-1}g^{-1} = (gH)^{-1}$, а тогда φ корректно определено и является отображением из G/H в $H \backslash G$. Биективность следует из существования $\varphi^{-1} : Hg \mapsto g^{-1}H$. ∎

Замечание. Отображение $gH \mapsto Hg$ не всегда корректно определено.

Определение 1.7. Если $H < G$, то *индексом* H в G называется $|G : H| = |G/H| = |H \backslash G|$.

Теорема 1.1 (Лагранжа)**.** *Для конечной группы $|G| = |H| \cdot |G : H|$.*

Следствие. *$|H|$ делит $|G|$, и для любого $g \in G$ $|g|$ делит $|G|$.*

1.4 Нормальные подгруппы

Определение 1.8. Пусть $H < G$. H называется *нормальной подгруппой* в G ($H \triangleleft G$), если $\forall g \in G\ gH = Hg$.

Замечание. Эквивалентно: $H = g^{-1}Hg$.

Примеры.

1. $G \triangleleft G$.

2. $\{e\} \triangleleft G$.

3. Если G — абелева, то все подгруппы нормальны.

4. $A_n \triangleleft S_n$. Действительно, если $\sigma \in A_n$, то $\sigma A_n = A_n = A_n\sigma$. Иначе, $\sigma A_n = S_n \setminus A_n = A_n\sigma$.

5. $\langle(1\,2)\rangle \ntriangleleft S_3$. $\langle(1\,2)\rangle = \{\mathrm{id}, (1\,2)\}$. $(1\,3)\langle(1\,2)\rangle = \{(1\,3), (1\,2\,3)\}$, но $\langle(1\,2)\rangle(1\,3) = \{(1\,3), (1\,3\,2)\}$.

Утверждение 1.2. *Пусть $H < G$, $|G : H| = 2$. Тогда $H \triangleleft G$.*

Доказательство. G разбивается на левые смежные классы по H, один из них — $H = eH$, а значит другой — $G \setminus H$. Аналогично, правые смежные классы — H и $G \setminus H$. Значит, если $g \in H$, то $gH = Hg = H$. Если же $g \in G \setminus H$, то $gH = G \setminus H = Hg$. ∎

Утверждение 1.3. *Пусть $H_1, H_2 \triangleleft G$. Тогда $H_1 \cap H_2 \triangleleft G$.*

Доказательство. $H_1 \cap H_2 < G$ — тривиально. Проверим, что для произвольного $g \in G$ верно $g^{-1}(H_1 \cap H_2)g = H_1 \cap H_2$. $\forall h \in H_1 \cap H_2\ g^{-1}hg \in H_1 \wedge g^{-1}hg \in H_2 \Rightarrow g^{-1}hg \in H_1 \cap H_2$. Мы показали, что $\forall g \in G\ g^{-1}(H_1 \cap H_2)g \subseteq H_1 \cap H_2$. Этого достаточно: $g(H_1 \cap H_2)g^{-1} \subseteq H_1 \cap H_2 \Rightarrow H_1 \cap H_2 = g^{-1}g(H_1 \cap H_2)g^{-1}g \subseteq g^{-1}(H_1 \cap H_2)g$. ∎

Замечание. Если $H < G$ и $\forall g \in G\ g^{-1}Hg \subseteq H$, то $\forall g \in G\ g^{-1}Hg = H$.

Утверждение 1.4. *Пусть $H \triangleleft G$, $K < G$. Тогда $HK = \{hk : h \in H, k \in K\} < G$. Если $K \triangleleft G$, то и $HK \triangleleft G$.*

Доказательство. Покажем, что $HK = KH$. Действительно, $HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH$. Теперь покажем, что $HK < G$: $(HK)(HK) = H(KH)K = HHKK = HK$; $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$.

Если же $K \triangleleft G$, то $\forall g \in G\ gHK = HgK = HKg \Rightarrow HK \triangleleft G$. ∎

Циклическая группа — группа, которая может быть порождена одним элементом a, то есть все её элементы являются степенями a (или, если использовать аддитивную терминологию, представимы в виде na, где n — целое число).

Гомоморфизмы групп

Пусть $(G, *)$ и $(H, \circ)$ - группы. Отображение $f : G \to H$ называется **гомоморфизмом групп,** если для любых $a, b \in G$

$$f(a * b) = f(a) \circ f(b).$$

Ядром гомоморфизма групп $f : G \to H$ называется множество

$$Kerf = \{g \in G \mid f(a) = e\},$$

где e - единица в H.

Образом гомоморфизма f называется множество всех элементов вида $f(g)$:

$$Imf = \{b \in H \mid \exists\, a \in G, f(a) = b\}.$$

Инъективный гомоморфизм называется **мономорфизмом**, сюръективный - **эпиморфизмом**, биективный - **изоморфизмом.**

Примеры.

1. Пусть $G = (\mathbb{R}^n, +)$, $H = (\mathbb{R}^m, +)$, $f : \mathbb{R}^n \to \mathbb{R}^m -$ линейное отображение. Тогда $f -$ гомоморфизм групп.

2. Пусть $(G, *)$ и $(H, \circ)$ - произвольные группы. Отображение $f : G \to H$ определим следующим образом: $f(g) = e$ для любого элемента $g \in G$. Здесь $e-$ единица в H. Покажем, что $f-$ гомоморфизм групп. Действительно,

$$f(a * b) = e = e \circ e = f(a) \circ f(b).$$

Ядро гомоморфизма $Kerf = G$, а образ $Imf = \{e\}$.

3. Пусть $G = (\mathbb{R}, +)$, $H = (\mathbb{R}^*, \cdot)$, $f : G \to H$, $f(x) = 2^x$. Покажем, что $f-$ гомоморфизм. Действительно,

$$f(x + y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y).$$

Так как $2^x = 1$ только при $x = 0$, то $Kerf = \{0\}$ и, следовательно, $f-$ мономорфизм.

Как известно, $2^x \in \mathbb{R}^+$ для любого $x \in \mathbb{R}$. Поэтому $Imf \subseteq \mathbb{R}^+$. Кроме того, любое положительное число y можно записать в виде $y = 2^x = f(x)$, где $x = \log_2 y \in \mathbb{R}$. Следовательно, $Imf = \mathbb{R}^+$.

Свойства гомоморфизмов групп

Пусть $(G, *)$ и $(H, \circ)$ – группы, $f : G \to H$ – гомоморфизм групп.

(1) Единица группы G переходит в единицу группы H, то есть $f(e) = e$.

(2) Для любого элемента $a \in G$ справедливо: $f(a^{-1}) = (f(a))^{-1}$.

(3) Для любого элемента $a \in G$ выполняется: $f(a^n) = (f(a))^n$.

(4) Гомоморфизм f инъективен тогда и только тогда, когда ядро $Kerf$ тривиально, то есть состоит только из нейтрального элемента.

(5) Ядро гомоморфизма является нормальной подгруппой в G, образ гомоморфизма является подгруппой в H.

(6) Композиция гомоморфизмов групп является гомоморфизмом групп.

(7) Если $f : G \to H$ – изоморфизм групп, то $f^{-1} : H \to G$ – тоже изоморфизм групп (существует в силу биективности).

Теорема Кэли:

Любая конечная группа $(G, \circ)$ изоморфна некоторой подгруппе группы перестановок множества элементов этой группы. При этом каждый элемент $a \in G$ сопоставляется с перестановкой π_a, задаваемой тождеством $\pi_a(g) = a \circ g,$ где *g* — произвольный элемент группы *G*.

Конечные поля

Поле – множество с двумя операциями * и +, являющееся абелевой группой по операции + и взятое без 0 (нейтрального элемента по операции +) абелевой группой по операции *, причем a*(b+c)=a*b+a*c,то есть выполняется закон *дистрибутивности*.

Лемма 1. *Если поле $\mathbb{F}$ состоит из q элементов, то каждый элемент поля $\mathbb{F}$ является корнем многочлена $x^q - x$.*

Лемма 2. *Для любого поля F и любого его автоморфизма φ неподвижные точки этого автоморфизма образуют подполе в F.*

Теорема 1. *Для любого простого p и натурального n существует поле из p^n элементов, и все такие поля изоморфны (обозначение: $\mathbb{F}_{p^n}$).*

Теорема 2. *Поле $\mathbb{F}_{p^n}$ содержит $\mathbb{F}_{p^m}$ в качестве подполя тогда и только тогда, когда $m|n$.*

Теорема 3. *Мультипликативная группа конечного поля является циклической.*

Полезные факты из теории чисел:

1. Множество вычетов по простому модулю – поле.
2. (*Малая теорема Ферма*) Если p – простое число, и a – целое число, не делящееся на a, то a^{p-1}-1 делится на p.
3. Если целые числа n и m взаимно просты, то существуют такие целые числа x и y, что nx+my=1.