## Часть 1. Группы и подгруппы

**Определение 1.1.** Пусть $G$ — произвольная группа. Непустое подмножество $H \subset G$ называется подгруппой, если $HH \subset H$ и $H^{-1} \subset H$, то есть для любых $h, h' \in H$ имеем $hh' \in H$, $h^{-1} \in H$.

**Замечание 1.2.** Из определения следует, что $e \in H$.

**Примеры 1.3.**
1. Если $G$ — группа и $x \in G$, то множество $\langle x \rangle := \{ x^n \mid n \in \mathbb{Z} \}$ называется циклической подгруппой, порожденной элементом $x$. Вообще, группа $G$ называется циклической, если $G = \langle x \rangle$ для некоторого $x \in G$ (покажите, что всякая циклическая группа изоморфна либо $\mathbb{Z}$, либо $\mathbb{Z}/n\mathbb{Z}$). В этом случае $x$ называется образующей группы $G$.

   В частности, имеем следующие подгруппы $n\mathbb{Z} := \langle n \rangle \subset \mathbb{Z}$, $\frac{1}{n}\mathbb{Z} := \langle 1/n \rangle \subset \mathbb{Q}/\mathbb{Z}$.
2. Пусть $X$ — любая алгебраическая структура, а $S \subset X$ — произвольное подмножество. Тогда $N_S = \{ f \in \mathrm{Aut}(X) \mid f(S) = S \}$ и $Z_S = \{ f \in \mathrm{Aut}(X) \mid \forall s \in S \ f(s) = s \}$ — подгруппы в $\mathrm{Aut}(X)$.
3. Пусть $G$ — группа, а $S \subset G$ — подмножество. Тогда $N_S = \{ g \in G \mid gSg^{-1} = S \}$ (нормализатор множества $S$) и $Z_S = \{ g \in G \mid \forall s \in S \ gs = sg \}$ (централизатор множества $S$) — подгруппы в $G$.
4. Пусть $G$ — группа, а $H_1, H_2 \subset G$ — подгруппы. Тогда $H_1 \cap H_2 \subset G$ — подгруппа. Более того, если $\{ H_i \}_{i \in I}$ — произвольное семейство подгрупп в $G$, то $\bigcap_{i \in I} H_i$ — подгруппа в $G$.
5. Пусть $H \subset G$ — подгруппа и $x \in G$. Тогда $xHx^{-1} = \{ xhx^{-1} \mid h \in H \}$ — подгруппа в $G$.

**Упражнение 1.4.** 1) Докажите, что если $G$ — циклическая группа, то либо $G \cong \mathbb{Z}$, либо $G \cong \mathbb{Z}/n\mathbb{Z}$. 2) Покажите, что всякая подгруппа циклической группы — циклическая.

Пусть $H \subset G$ — подгруппа, $x \in G$ — произвольный элемент. Множество $xH = \{ xh \mid h \in H \} \subset G$ называется левым смежным классом группы $G$ по подгруппе $H$. Аналогично, $Hx = \{ hx \mid h \in H \} \subset G$ называется правым смежным классом $G$ по $H$. Заметим, что смежные классы $xH$ и $Hx$ не являются подгруппами (за исключением случая $x \in H$). При аддитивной записи класс смежности обозначается $x + H$.

**Лемма 1.5.** *Смежные классы $xH$ и $yH$ либо не пересекаются, либо совпадают. Умножение слева на $yx^{-1}$ задает биекцию $xH \to yH$.*

Доказательство: пусть $xH \cap yH \neq \emptyset$. Тогда $xh_1 = yh_2$ для некоторых $h_1, h_2 \in H$. Следовательно $x = yh_2h_1^{-1}$ и $xH = yh_2h_1^{-1}H \subset yH$. Аналогично $y = xh_1h_2^{-1}$ и $yH = xh_1h_2^{-1}H \subset xH$. Значит $xH = yH$. Второе утверждение — очевидно. □

Множество всех левых смежных классов $G$ по $H$ обозначается через $G/H$, а множество всех правых смежных классов $G$ по $H$ обозначается через $H\backslash G$. Иногда также рассматривают двойные смежные классы $G$ по $H$ — множества вида $HxH = \{ h_1xh_2 \mid h_1, h_2 \in H \}$. Легко проверить, что для двойных смежных классов выполненно первое (но не второе!) утверждение леммы 1.5. Множество всех двойных смежных классов $G$ по $H$ обозначается через $H\backslash G/H$.

Количество различных левых смежных классов группы $G$ по $H$ обозначается $(G : H)$ и называется индексом подгруппы $H$ в $G$. Индекс тривиальной подгруппы $(G : 1)$ равен количеству элементов в группе $G$ и называется также порядком группы $G$.

Следующая теорема вытекает из леммы 1.5.

**Теорема 1.6.** *Если $H \subset G$ — подгруппа, то $(G : 1) = (G : H)(H : 1)$ в том смысле, что если два из индексов конечны, то конечен и третий и выполняется равенство.*

**Следствие 1.7.** *Если $p$ — простое и $G$ — группа порядка $p$, то $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Доказательство: возьмем произвольный $1 \neq x \in \mathbb{Z}$. По теореме 1.6 порядок подгруппы $\langle x \rangle \subset G$ — делитель числа $p$, следовательно $\langle x \rangle = G$, то есть $G$ — циклическая. □

**Определение 1.8.** Порядком элемента $x \in G$ называется порядок подгруппы $\langle x\rangle \subset G$. Показателем элемента $x \in G$ называется любое положительное число $n$, такое что $x^n = e$. Аналогично, показателем группы $G$ называется любое положительное число $n$, такое что $\forall x \in G \quad x^n = e$.

**Лемма 1.9.** *Пусть $x \in G$. Тогда $(i)$ порядок $x$ делит любой из его показателей; $(ii)$ порядок $x$ делит порядок группы $G$; $(iii)$ наименьший показатель группы $G$ равен НОК порядков всех ее элементов.*

Доказательство: рассмотрим последовательность $\{1, x, x^2, \dots\}$ степеней $x$. Если $x^n = x^m$ и $n > m$, то $x^{n-m} = 1$. Следовательно, либо все эелементы в последовательности различны, либо она периодична. Пусть $d$ — минимальный период последовательности. Тогда $x^d = 1$ и все элементы в множестве $\{1, x, \dots, x^{d-1}\}$ различны. Следовательно $d$ равен порядку группы $\langle x\rangle$, то есть порядку $x$. Пусть теперь $n$ — показатель элемента $x$. Разделим $n$ на $d$ с остатком: $n = qd + r$, $0 \leqslant r < d$. Тогда $x^r = x^{n-qd} = x^n(x^d)^{-q} = x^n = 1$, следовательно $r = 0$, то есть $d|n$, что доказывает утверждение $(i)$. Утверждение $(ii)$ немедленно следует из теоремы 1.6. Чтобы доказать утверждение $(iii)$ заметим, что показатель группы является показателем любого из ее элементов, и, следовательно, общим кратным всех ее элементов. □

## Часть 2. Гомоморфизмы групп

**Определение 2.1.** Ядром гомоморфизма групп $f : G \to G'$ называется $\operatorname{Ker} f = \{x \in G \mid f(x) = e'\}$. Образом гомоморфизма групп $f : G \to G'$ называется $\operatorname{Im} f = \{y \in G' \mid y = f(x), x \in G\}$.

Легко видеть, что ядро и образ гомоморфизма групп $f : G \to G'$ являются подгруппами.

**Лемма 2.2.** *Пусть $f : G \to G'$ — гомоморфизм групп. Тогда $f$ является мономорфизмом $\iff \operatorname{Ker} f = \{e\}$; $f$ является эпиморфизмом $\iff \operatorname{Im} f = G'$.*

Доказательство: пусть $f : G \to G'$ — гомоморфизм групп и $f(x) = f(y)$. Тогда $f(x^{-1} \circ y) = f(x^{-1}) \circ f(y) = f(x)^{-1} \circ f(y) = (f(y))^{-1} \circ f(y) = e'$, следовательно $x^{-1} \circ y \in \operatorname{Ker} f$. Далее очевидно. □

Ясно, что всякая подгруппа является образом некоторого гомоморфизма. Действительно, если $H \subset G$ — подгруппа, то вложение $H \to G$ является мономорфизмом, образ которого равен $H$. Однако ядром гомоморфизма может быть уже далеко не любая подгруппа.

**Определение 2.3.** Подгруппа $H \subset G$ называется нормальной, если $\forall x \in G \quad xHx^{-1} = H$.

**Замечание 2.4.** Достаточно проверять, что $\forall x \in G \quad xHx^{-1} \subset H$.

Если $H$ — нормальная подгруппа в $G$, то пишут $H \triangleleft G$.

**Лемма 2.5.** *Ядро гомоморфизма групп является нормальной подгруппой.*

Доказательство: пусть $f : G \to G'$ — гомоморфизм групп. Покажем, что $x(\operatorname{Ker} f)x^{-1} \subset \operatorname{Ker} f$. Действительно, $g \in \operatorname{Ker} f \implies f(g) = e' \implies f(xgx^{-1}) = f(x)f(g)f(x)^{-1} = f(x)f(x)^{-1} = e' \implies xgx^{-1} \in \operatorname{Ker} f$. □

**Примеры 2.6.**
1. $\{e\}$ и $G$ — нормальны в $G$.
2. Любая подгруппа в коммутативной группе нормальна.
3. Подгруппы $\{e\}$, $\left\langle\binom{123}{231}\right\rangle$ и $\mathfrak{S}_3$ в группе $\mathfrak{S}_3$ нормальны, а подгруппы $\left\langle\binom{123}{213}\right\rangle$, $\left\langle\binom{123}{321}\right\rangle$ и $\left\langle\binom{123}{132}\right\rangle$ — нет.
4. Подгруппа $Z_S$ нормальна в $N_S$ (см. пример 1.3.2).
5. Центр группы $Z_G = \{g \in G \mid \forall x \in G \quad gx = xg\}$ — нормален.
6. Если $H \subset G$ — любая подгруппа, то $\cap_{x\in G} xHx^{-1}$ — нормальна в $G$.
7. Если $H_1, H_2 \triangleleft G$, то $H_1 \cap H_2 \triangleleft G$.
8. Если $K \subset H \subset G$ и $K \triangleleft G$, то $K \triangleleft H$.
9. Если $H \subset G$ — любая подгруппа, то $H \triangleleft N_H$. Более того, если $H \subset K \subset G$ и $H \triangleleft K$, то $K \subset N_H$.
10. Если $H \subset G$ — подгруппа и $K$ — подгруппа в $N_H$, то $KH$ — подгруппа в $G$ и $H$ — нормальна в $KH$.

**Лемма 2.7.** *Если $H \subset G$ — нормальная подгруппа, то $\forall x \in G \quad xH = Hx$.*

Доказательство: $xH = (xH)e = (xH)(x^{-1}x) = (xHx^{-1})x = Hx$. $\square$

Пусть $H \subset G$ — нормальная подгруппа. Тогда ясно, что $(xH)(yH) = x(Hy)H = x(yH)H = (xy)(HH) = xyH$. Определим на множестве левых классов смежности $G/H$ бинарную операцию:

$$(xH) \circ (yH) := xyH. \tag{2.8}$$

Из приведенных выше рассуждений следует, что она корректно определена (результат зависит только от классов смежности $xH$ и $yH$, но не от элементов $x$ и $y$).

**Теорема 2.9.** *Если $H \subset G$ — нормальная подгруппа, то множество $G/H$ с операцией $\circ$ является группой. Более того, проекция $f : G \to G/H$, $x \mapsto xH$ является эпиморфизмом групп, причем $\operatorname{Ker} f = H$.*

Доказательство: ассоциативность очевидна:

$$((xH) \circ (yH)) \circ (zH) = ((xy)H) \circ (zH) = ((xy)z)H = (x(yz))H = (xH) \circ ((yz)H) = (xH) \circ ((yH) \circ (zH)).$$

Далее, покажем, что класс смежности $eH = H$ является единицей:

$$(xH) \circ (eH) = (xe)H = xH, \quad (eH) \circ (xH) = (ex)H = xH.$$

Наконец, проверим, что класс $x^{-1}H$ является обратным к классу $xH$:

$$(xH) \circ (x^{-1}H) = (xx^{-1})H = eH, \quad (x^{-1}H) \circ (xH) = (x^{-1}x)H = eH.$$

Таким образом, $G/H$ — действительно группа. Вторая же часть теоремы очевидна. $\square$

Группа $G/H$ называется факторгруппой группы $G$ по нормальной подгруппе $H$. Группы $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}/\mathbb{Z}$, $\mathbb{R}/\mathbb{Z}$ и $\mathbb{C}/\mathbb{Z}$ из прошлой лекции являются примерами факторгрупп.

**Теорема 2.10.** *Пусть $f : G \to G'$ — гомоморфизм групп. Тогда $G/\operatorname{Ker} f \cong \operatorname{Im} f$* (канонический изоморфизм).

Доказательство: пусть $H = \operatorname{Ker} f$. Определим отображение $\bar{f} : G/H \to \operatorname{Im} f$ формулой $\bar{f}(xH) = f(x)$. Проверим корректность определения: если $xH = yH$, то $y = xh$, $h \in H$ и $f(y) = f(xh) = f(x)f(h) = f(x)e' = f(x)$, так как $h \in H = \operatorname{Ker} f$. Заметим далее, что

$$\bar{f}(xH \circ yH) = \bar{f}(xyH) = f(xy) = f(x)f(y) = \bar{f}(xH)\bar{f}(yH) \quad \text{и} \quad \bar{f}(eH) = f(e) = e',$$

следовательно $\bar{f}$ — гомоморфизм групп. Наконец, если $\bar{f}(xH) = f(x) = e'$, то $x \in \operatorname{Ker} f = H$, следовательно $xH = eH$, то есть $\bar{f}$ — мономорфизм. Кроме того, очевидно, что $\bar{f}$ — эпиморфизм. Следовательно, $\bar{f}$ — изоморфизм. $\square$

**Следствие 2.11.** $(i)$ *Если $f : G \to G'$ — эпиморфизм групп, то $G' \cong G/\operatorname{Ker} f$.* $(ii)$ *Всякий гомоморфизм групп $f : G \to G'$ раскладывается в композицию канонических эпиморфизма, изоморфизма и мономорфизма $G \to G/\operatorname{Ker} f \to \operatorname{Im} f \to G'$.*