2 Лекция 3.04

Циклические группы Чуть позже докажем, что все циклические группы изоморфны $(\mathbb{Z}, +), (\mathbb{Z}_n, +)$.

Определение 11. *Пусть G – группа, $H \subseteq G$ – подгруппа, g ($g \in G$) – какой-то элемент. Тогда левый смежный класс элемента g по подгруппе H это $gH = \{gh \mid h \in H\}$.*

Лемма 3. *Для любых $g_1, g_2 \in G$ верно $g_1H = g_2H$ или $g_1H \cap g_2H = \varnothing$.*

Доказательство. В случае пустого пересечения все очевидно. Пусть $g_1h_1 = g_2h_2$, где $h_1, h_2 \in H$. Тогда $g_1 = g_2h_2h_1^{-1}$, следовательно $g_1H = g_2h_2h_1^{-1}H_1 \subseteq g_2H$. Аналогично $g_2H \subseteq g_1H$, поэтому $g_1H = g_2H$. □

Лемма 4. $|gH| = |H|$.

Доказательство. Установим биекцию между gH и H. Пусть $\phi : gH \to H$, где $\phi(gh) = h$. Поймем, что ϕ – биекция. Пусть не так, $gh_1 = gh_2 \Rightarrow^{g^{-1}\cdot} h_1 = h_2$, противоречие. □

Определение 12. *Индекс подгруппы $H \subseteq G$ – это число различных левых смежных классов G по H. Обозначается как $[G : H]$.*

Теорема 1 (Лагранж)**.** *Пусть G – конечная группа. Тогда для любой подгруппы $H \subseteq G$:*

$$|G| = |H| \cdot [G : H]$$

Доказательство. Если $H = G$, то теорема верна. Возьмем в качестве первого класса H. Потом возьмем $g_1 \in G : g_1H \neq H$ и создадим второй класс g_1H. Затем возьмем еще один элемент $g_2 \in G : g_2H \neq H \wedge g_2H \neq g_1H$ и создадим еще один класс. И так далее. Размер каждого класса будет $|H|$. Всего классов, понятно, $[G : H]$. □

Следствие 1. Порядок подгруппы делит порядок группы. Иными словами, $|H|$ делит $|G|$, где $H \subseteq G$ – подгруппа.

Следствие 2. Порядок любого элемента делит порядок группы. То есть $\forall g \in G : \text{ord}(g) \mid |G|$. Это следует из того, что $\text{ord}(g) = |\langle g \rangle|$, а $\langle g \rangle$ – подгруппа.

Следствие 3. $\forall g \in G : g^{|G|} = e$.

Следствие 4 (Малая теорема Ферма)**.** Если p – простое, $(a, p) = 1$, то $a^{p-1} \equiv 1 \pmod{p}$. Это следствие можно доказать с помощью теории групп, ели взять $G = (\mathbb{Z}_p \setminus \{0\}, \times)$. Тогда $|G| = p - 1$, $a^{|G|} = a^{p-1} = e$.

Следствие 5. Пусть $|G| = p$, где p – простое. Тогда G – циклическая группа (в частности, коммутативная), и она порождается любым своим элементом (кроме нейтрального элемента e).

Доказательство. Возьмем $g \in G, g \neq e$. Рассмотрим $\langle g \rangle$. Так как $\langle g \rangle$ – подгруппа, $e \in \langle g \rangle$. Тогда $|\langle g \rangle| \geq 2$, и это число делит $|G| = p$, а так как p – простое, $|\langle g \rangle| = |G|$, следовательно $\langle g \rangle = G$. □

Определение 13. *Правый смежный класс элемента g по подгруппе $H \subseteq G$ – это множество $Hg = \{hg \mid h \in H\}$.*

Факт 1. Правых смежных классов столько же, сколько левых, то есть $\frac{|G|}{|H|} = [G : H]$.

Определение 14. *Подгруппа $H \subseteq G$ называется нормальной, если $\forall g \in G : gH = Hg$.*

Пример. Если G коммутативна, то любая подгруппа $H \subseteq G$ нормальная.

Утверждение 3. *Для подгруппы $H \subseteq G$ эквивалентны следующие условия:*

1. H – *нормальная*
2. $\forall g \in G : gHg^{-1} \subseteq H$
3. $\forall g \in G : gHg^{-1} = H$

Доказательство. Докажем $1 \Rightarrow 2$. Если $gH = Hg$, то $\forall h \in H\ \exists h' \in H : gh = h'g$. Тогда $ghg^{-1} = h'gg^{-1} = h'$ поэтому $gHg^{-1} \subseteq H$.

Теперь докажем $2 \Rightarrow 3$. Покажем, что $H \subseteq gHg^{-1}$. Возьмем $h \in H$. Заметим, что $h = gg^{-1}hgg^{-1} = g(g^{-1}hg)g^{-1}$. Тогда по (2) найдется $h' \in H : h = gh'g^{-1}$, поэтому $h \in gHg^{-1}$.

И наконец $3 \Rightarrow 1$. Заметим, что $gH = Hg \Rightarrow^{\cdot g^{-1}} gHg^{-1} = H$. □

Пример. $SL_n \subseteq GL_n$. Так как $\forall A \in GL_n, B \in SL_n : \det(ABA^{-1}) = \det B = 1$.

Определение 15. *Пусть G – некоторая группа, $H \subseteq G$ – подгруппа. Обозначим за G/H множество смежных классов. По определению положим $(g_1H)(g_2H) = g_1g_2H$. Ассоциативность выполняется, так как:*

$$((g_1H)(g_2H))(g_3H) = (g_1H)((g_2H)(g_3H)) = g_1g_2g_3H$$

В качестве нейтрального элемента возьмем eH. Для каждого элемента gH есть обратный $g^{-1}H$.

Докажем корректность этого определения. Тогда нужно проверить, что:

$$(g_1h_1H)(g_2h_2H) = g_1h_1g_2h_2H = g_1g_2H$$

Перепишем $g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2$. Тогда мы хотим, чтобы $g_2^{-1}h_1g_2 \in H$, из этого следует, что H — нормальная подгруппа. То есть определение выше верно только для нормальной H.

Корректность обратного доказывается аналогично.

Упражнение. Показать, что определение 15 верно только для нормальных групп.

Пример. Возьмем $G = (\mathbb{Z}, +), H = n\mathbb{Z}$. Тогда $G/H = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$. Каждый элемент Z_n является классом.

Как представлять фактор-группу?

Определение 16. *Пусть $(G, \circ), (F, \cdot)$ — группы. Тогда отображение $\varphi : G \to F$ называется гомоморфизмом, если:*

1. $\forall a, b \in G : \varphi(a \circ b) = \varphi(a) \cdot \varphi(b)$

Лемма 5. *Если $\varphi : G \to F$ — гомоморфизм, то:*

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

Доказательство. Докажем 1. $\varphi(e_Ge_G) = \varphi(e_G) = \varphi(e_G)\varphi(e_G)$. Умножим на $\varphi(e_G)^{-1}$, тогда $e_F = \varphi(e_G)$. Теперь 2. Заметим, что $\varphi(aa^{-1}) = \varphi(e) = \varphi(a)\varphi(a^{-1}) \Leftrightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$. □

Определение 17. *Гомоморфизм групп $\varphi : G \to F$ называется изоморфизмом, если φ — биекция.*

Упражнение. $\varphi^{-1} : F \to G$ тоже будет гомоморфизмом.

Определение 18. *Группы G и F изоморфны и пишем $G \cong F$, если $\exists \varphi : G \to F$ — изоморфизм.*

Теорема 2. *a) Любая бесконечная циклическая группа $G \cong (\mathbb{Z}, +)$.*
b) Любая конечная циклическая группа порядка $n \cong (\mathbb{Z}_n, +)$.

Доказательство. Сначала (a). $G = \langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$. Тогда определим $\varphi : G \to F$, где $\varphi(g^m) = m$.
Теперь (b). Мы знаем, что $G = \langle g \rangle = \{g^0, g^1, \dots, g^{n-1}\}$. Положим $\varphi(g^m) = m \pmod{n}$. □

Пример. Возьмем $(\mathbb{R}, +)$ и $(\mathbb{R}_{>0}, \times)$. Построим изоморфизм φ, такой что $\varphi(x) = e^x$. Тогда $\varphi(x+y) = e^{x+y} = e^x e^y$.