

3 Лекция 4.04

Как представлять себе фактор-группу G/H ?

Определение 19. С каждым гомоморфизмом $\varphi : G \rightarrow F$ связаны ядро $\ker \varphi$ и образ $\operatorname{Im} \varphi$. Формально $\ker \varphi = \{g \in G \mid \varphi(g) = e_F\}$, $\operatorname{Im} \varphi = \{f \in F \mid \exists g \in G : \varphi(g) = f\}$.

Упражнение. $\ker \varphi$ и $\operatorname{Im} \varphi$ являются подгруппами в G и F соответственно.

Лемма 6. Гомоморфизм $\varphi : G \rightarrow F$ инъективен $\Leftrightarrow \ker \varphi = \{e_G\}$.

Доказательство. \Rightarrow очевидно.

Теперь \Leftarrow . Пусть $\varphi(a) = \varphi(c)$. Тогда $\varphi(a) \cdot \varphi(c)^{-1} = \varphi(a) \cdot \varphi(c^{-1}) = \varphi(ac^{-1}) = e_F$. Следовательно $ac^{-1} \in \ker \varphi$, поэтому $ac^{-1} = e_G \Leftrightarrow a = c$. \square

Следствие 6. Гомоморфизм φ является изоморфизмом тогда и только тогда, когда $\ker \varphi = \{e_G\}$ и $\operatorname{Im} \varphi = F$.

Предложение 1. $\ker \varphi$ — нормальная подгруппа в G .

Доказательство. Надо проверить, что $\forall g \in G, a \in \ker \varphi : gag^{-1} \in \ker \varphi$.

$$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) = \varphi(g)e_F\varphi(g)^{-1} = e_F$$

\square

Еще раз про фактор-группы Пусть $H \subseteq G$ — подгруппа. Тогда определим $G/H = \{gH \mid g \in G\}$. На нем операция \circ действует как:

$$(g_1H) \circ (g_2H) = g_1g_2H$$

Теорема 3 (О гомоморфизме). Пусть $\varphi : G \rightarrow F$ — гомоморфизм. Тогда $G/\ker \varphi \cong \operatorname{Im} \varphi$.

Формальное доказательство. Построим отображение $\psi : G/\ker \varphi \rightarrow \operatorname{Im} \varphi$. Положим $\psi(g \ker \varphi) = \varphi(g)$. Проверим корректность. Возьмем $gh, h \in \ker \varphi$.

$$\varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)e_F = \varphi(g)$$

Сюръективность верна по определению. Теперь проверим инъективность. Пусть $\psi(g_1 \ker \varphi) = \psi(g_2 \ker \varphi)$. Тогда $\varphi(g_1) = \varphi(g_2) \Leftrightarrow \varphi(g_1g_2^{-1}) = e_F \Leftrightarrow g_1g_2^{-1} \in \ker \varphi$.

Осталось проверить, что $\psi((g_1 \ker \varphi)(g_2 \ker \varphi)) = \psi(g_1 \ker \varphi)\psi(g_2 \ker \varphi)$.

$$\psi((g_1 \ker \varphi)(g_2 \ker \varphi)) = \psi(g_1g_2 \ker \varphi) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1 \ker \varphi)\psi(g_2 \ker \varphi)$$

\square

Пример. Обобщим пример $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. Пусть $G = (\mathbb{R}, +)$, $H = (\mathbb{Z}, +)$. Рассмотрим гомоморфизм $\varphi : \mathbb{R} \rightarrow (\mathbb{C} \setminus \{0\}, \times)$, причем $\varphi(a) = e^{2\pi ia}$. Тогда образом будет окружность $\{z \in \mathbb{C} \mid |z| = 1\}$, а ядром — все целые числа, так как $\forall a \in \mathbb{Z} : e^{2\pi ia} = 1$.

Определение 20. Центр группы G — это подмножество $Z(G) = \{a \in G \mid \forall b \in G : ab = ba\}$.

Предложение 2. $Z(G) \subseteq G$ — нормальная подгруппа.

Для доказательства вспомним, что $(ab)^{-1} = b^{-1}a^{-1}$.

Доказательство. Понятно, что $e \in G$. Возьмем $a, c \in Z(G)$ и проверим, что $ac^{-1} \in Z(G)$. Возьмем произвольный $b \in G$ и проверим:

$$(ac^{-1})b = ac^{-1}(b^{-1})^{-1} = a(b^{-1}c)^{-1} = a(b^{-1}c)^{-1} = a(cb^{-1})^{-1} = abc^{-1} = b(ac^{-1})$$

Теперь проверим нормальность: $\forall a \in Z(G), b \in G : bab^{-1} = abb^{-1} = a \in Z(G)$. □

Замечание 1. $Z(G) = G \Leftrightarrow$ группа G коммутативна.

Пример. $Z(S_n) = e, Z(GL_n) = \{\lambda E \mid \lambda \in \mathbb{R}\}$.

Определение 21. Прямым произведением групп G_1, \dots, G_m называется множество $G_1 \times \dots \times G_m = \{(g_1, \dots, g_m) \mid \forall i : g_i \in G_i\}$. Определим операцию \circ :

$$(g_1, \dots, g_m) \circ (g'_1, \dots, g'_m) = (g_1g'_1, \dots, g_mg'_m)$$

Нейтральным элементом будет $(1, \dots, 1)$. Определим обратное $(g_1, \dots, g_m)^{-1} = (g_1^{-1}, \dots, g_m^{-1})$.

Замечание 2. $G_1 \times \dots \times G_m$ — коммутативна $\Leftrightarrow \forall i : G_i$ — коммутативна.

Замечание 3. $G_1 \times \dots \times G_m$ — конечна $\Leftrightarrow \forall i : G_i$ — конечна.

Теорема 4 (О факторизации по сомножителям). Пусть H_1, \dots, H_m — нормальные подгруппы в группах G_1, \dots, G_m соответственно. Тогда подгруппа $H_1 \times \dots \times H_m \subseteq G_1 \times \dots \times G_m$ — нормальная. Кроме того,

$$(G_1 \times \dots \times G_m) / (H_1 \times \dots \times H_m) \cong (G_1/H_1) \times \dots \times (G_m/H_m)$$

Доказательство. Докажем нормальность.

$$(g_1, \dots, g_m)(h_1, \dots, h_m)(g_1, \dots, g_m)^{-1} = (g_1h_1g^{-1}, \dots, g_mh_mg_m^{-1}) \in H_1 \times \dots \times H_m$$

Сопоставим $(g_1, \dots, g_m)(H_1 \times \dots \times H_m) \rightarrow (g_1H_1, \dots, g_mH_m)$. Можно доказать по определению, что такое отображение является изоморфизмом. □

Абелевы группы Наша цель — классифицировать конечные абелевы группы.

Теорема 5. Если $n = tk$ — произведение натуральных чисел, и $(t, k) = 1$, то $\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_k$.

Доказательство. Это вариация КТО. Построим отображение $\varphi(x) = (x \bmod t, x \bmod k)$. Корректность очевидна. Сохранение операции выполняется по определению. Для инъективности нужно проверить, что ядро тривиально. По определению, $\ker \varphi = \{x \mid \varphi(x) = (0, 0)\}$. Тогда $k \mid x \wedge t \mid x \Rightarrow k \mid n$, поэтому в ядре лежит только 0.

Наконец поскольку $|\mathbb{Z}_n| = |\mathbb{Z}_m| \cdot |\mathbb{Z}_k|$, инъективность влечет сюръективность. □

Упражнение. $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$, потому что в \mathbb{Z}_4 есть элементы порядка 4, а именно 1 и 3.

Следствие 7. Пусть $n = p_1^{\alpha_1} \cdot \dots \cdot p_s^{\alpha_s}$. Тогда $\mathbb{Z}_n = \mathbb{Z}_{p_1^{\alpha_1}} \times \dots \times \mathbb{Z}_{p_s^{\alpha_s}}$.

Всюду далее рассматриваем $(A, +)$ — абелеву группу. Также будем обозначать прямое произведение $G_1 \times G_2$ как $A \oplus B$. Определим умножение на целое число:

$$\forall a \in A : s \cdot a = \begin{cases} a + a + \dots + a, s \text{ раз, если } s > 0 \\ 0, \text{ если } s = 0 \\ (-a) + (-a) + \dots + (-a), -s \text{ раз, если } s < 0 \end{cases}$$

Определение 22. *Линейной комбинацией назовем $s_1 a_1 + \dots + s_k a_k$.*

Определение 23. *Абелева группа A называется конечно порожденной, если $\exists a_1, \dots, a_n \in A$, такие что:*

$$\forall a \in A : a = s_1 a_1 + \dots + s_n a_n$$

для некоторых $s_i \in \mathbb{Z}$.

Определение 24. *Группа A называется свободной, если в ней есть базис, то есть такие a_1, \dots, a_n , что*

$$\forall a \in A : a = a_1 s_1 + \dots + a_n s_n$$

при единственном наборе s_1, \dots, s_n ($s_i \in \mathbb{Z}$).