Лекции курса «Алгебра», лекторы И. В. Аржанцев и Р. С. Авдеев
ФКН НИУ ВШЭ, 1-й курс ОП ПМИ, 4-й модуль, 2014/2015 учебный год

Лекция 2

Нормальные подгруппы. Факторгруппы и теорема о гомоморфизме. Центр группы. Прямое произведение групп. Факторизация по сомножителям. Разложение конечной циклической группы.

Определение 1. Подгруппа H группы G называется *нормальной*, если $gH = Hg$ для любого $g \in G$.

Предложение 1. *Для подгруппы $H \subseteq G$ следующие условия эквивалентны:*
(1) *H нормальна;*
(2) *$gHg^{-1} \subseteq H$ для любого $g \in G$;*
(3) *$gHg^{-1} = H$ для любого $g \in G$.*

Доказательство. (1)⇒(2) Пусть $h \in H$ и $g \in G$. Поскольку $gH = Hg$, имеем $gh = h'g$ для некоторого $h' \in H$. Тогда $ghg^{-1} = h'gg^{-1} = h' \in H$.
(2)⇒(3) Так как $gHg^{-1} \subseteq H$, остаётся проверить обратное включение. Для $h \in H$ имеем $h = gg^{-1}hgg^{-1} = g(g^{-1}hg)g^{-1} \subseteq gHg^{-1}$, поскольку $g^{-1}hg \in H$ в силу пункта (2), где вместо g взято g^{-1}.

(3)⇒(1) Для произвольного $g \in G$ в силу (3) имеем $gH = gHg^{-1}g \subseteq Hg$, так что $gH \subseteq Hg$. Аналогично проверяется обратное включение. □

Условие (2) в этом предложении кажется излишним, но именно его удобно проверять при доказательстве нормальности подгруппы H.

Обозначим через G/H множество (левых) смежных классов группы G по нормальной подгруппе H. На G/H можно определить бинарную операцию следующим образом:
$$(g_1H)(g_2H) := g_1g_2H.$$

Зачем здесь нужна нормальность подгруппы H? Для проверки корректности: заменим g_1 и g_2 другими представителями g_1h_1 и g_2h_2 тех же смежных классов. Нужно проверить, что $g_1g_2H = g_1h_1g_2h_2H$. Это следует из того, что $g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2$ и $g_2^{-1}h_1g_2$ лежит в H.

Ясно, что указанная операция на множестве G/H ассоциативна, обладает нейтральным элементом eH и для каждого элемента gH есть обратный элемент $g^{-1}H$.

Определение 2. Множество G/H с указанной операцией называется *факторгруппой* группы G по нормальной подгруппе H.

Пример 1. Если $G = (\mathbb{Z}, +)$ и $H = n\mathbb{Z}$, то G/H — это в точности группа вычетов $(\mathbb{Z}_n, +)$.

Как представлять себе факторгруппу? В этом помогает теорема о гомоморфизме. Но прежде чем её сформулировать, обсудим ещё несколько понятий.

Определение 3. Пусть G и F — группы. Отображение $\varphi\colon G \to F$ называется *гомоморфизмом*, если $\varphi(ab) = \varphi(a)\varphi(b)$ для любых $a, b \in G$.

Замечание 1. Подчеркнём, что в этом определении произведение ab берётся в группе G, в то время как произведение $\varphi(a)\varphi(b)$ — в группе F.

Лемма 1. *Пусть $\varphi\colon G \to F$ — гомоморфизм групп, и пусть e_G и e_F — нейтральные элементы групп G и F соответственно. Тогда:*
(а) *$\varphi(e_G) = e_F$;*
(б) *$\varphi(a^{-1}) = \varphi(a)^{-1}$ для любого $a \in G$.*

Доказательство. (а) Имеем $\varphi(e_G) = \varphi(e_Ge_G) = \varphi(e_G)\varphi(e_G)$. Теперь умножая крайние части этого равенства на $\varphi(e_G)^{-1}$ (например, слева), получим $e_F = \varphi(e_G)$.

(б) Имеем $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e_G) = e_F$, откуда $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

Определение 4. Гомоморфизм групп $\varphi\colon G \to F$ называется *изоморфизмом*, если отображение φ биективно.

Упражнение 1. Пусть $\varphi\colon G \to F$ — изоморфизм групп. Проверьте, что обратное отображение $\varphi^{-1}\colon F \to G$ также является изоморфизмом.

Определение 5. Группы G и F называют *изоморфными*, если между ними существует изоморфизм.

Обозначение: $G \cong F$ (или $G \simeq F$).

В алгебре группы рассматривают с точностью до изоморфизма: изоморфные группы считаются «одинаковыми».

Теорема 1. (а) *Всякая бесконечная циклическая группа G изоморфна группе* $(\mathbb{Z}, +)$.
(б) *Всякая циклическая группа порядка n изоморфна группе* $(\mathbb{Z}_n, +)$.

Доказательство. Пусть $G = \langle g \rangle$. Тогда в первом случае изоморфизм устанавливает отображение $\langle g \rangle \to \mathbb{Z}$, $g^k \mapsto k$, а во втором — отображение $\langle g \rangle \to \mathbb{Z}_n$, $g^k \mapsto k \pmod n$. □

Пример 2. Отображение $\varphi\colon \mathbb{R} \to \mathbb{R}_{>0}$, $a \mapsto e^a$, устанавливает изоморфизм между группами $(\mathbb{R}, +)$ и $(\mathbb{R}_{>0}, \times)$.

Определение 6. С каждым гомоморфизмом групп $\varphi\colon G \to F$ связаны его *ядро*

$$\mathrm{Ker}(\varphi) = \{g \in G \mid \varphi(g) = e_F\}$$

и *образ*

$$\mathrm{Im}(\varphi) = \{a \in F \mid \exists g \in G : \varphi(g) = a\}.$$

Ясно, что $\mathrm{Ker}(\varphi) \subseteq G$ и $\mathrm{Im}(\varphi) \subseteq F$ — подгруппы.

Лемма 2. *Гомоморфизм групп $\varphi\colon G \to F$ инъективен тогда и только тогда, когда* $\mathrm{Ker}(\varphi) = \{e_G\}$.

Доказательство. Ясно, что если φ инъективен, то $\mathrm{Ker}(\varphi) = \{e_G\}$. Обратно, пусть $g_1, g_2 \in G$ и $\varphi(g_1) = \varphi(g_2)$. Тогда $g_1^{-1}g_2 \in \mathrm{Ker}(\varphi)$, поскольку $\varphi(g_1^{-1}g_2) = \varphi(g_1^{-1})\varphi(g_2) = \varphi(g_1)^{-1}\varphi(g_2) = e_F$. Отсюда $g_1^{-1}g_2 = e_G$ и $g_1 = g_2$. □

Следствие 1. *Гомоморфизм групп $\varphi\colon G \to F$ является изоморфизмом тогда и только тогда, когда $\mathrm{Ker}(\varphi) = \{e_G\}$ и $\mathrm{Im}(\varphi) = F$.*

Предложение 2. *Пусть $\varphi\colon G \to F$ — гомоморфизм групп. Тогда подгруппа $\mathrm{Ker}(\varphi)$ нормальна в G.*

Доказательство. Достаточно проверить, что $g^{-1}hg \in \mathrm{Ker}(\varphi)$ для любых $g \in G$ и $h \in \mathrm{Ker}(\varphi)$. Это следует из цепочки равенств

$$\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})e_F\varphi(g) = \varphi(g^{-1})\varphi(g) = \varphi(g)^{-1}\varphi(g) = e_F.$$

□

Теорема о гомоморфизме. Пусть $\varphi\colon G \to F$ — гомоморфизм групп. Тогда группа $\mathrm{Im}(\varphi)$ изоморфна факторгруппе $G/\mathrm{Ker}(\varphi)$.

Доказательство. Рассмотрим отображение $\psi\colon G/\mathrm{Ker}(\varphi) \to F$, заданное формулой $\psi(g\mathrm{Ker}(\varphi)) = \varphi(g)$. Проверка корректности: равенство $\varphi(gh_1) = \varphi(gh_2)$ для любых $h_1, h_2 \in \mathrm{Ker}(\varphi)$ следует из цепочки

$$\varphi(gh_1) = \varphi(g)\varphi(h_1) = \varphi(g) = \varphi(g)\varphi(h_2) = \varphi(gh_2).$$

Отображение ψ сюръективно по построению и инъективно в силу того, что $\varphi(g) = e_F$ тогда и только тогда, когда $g \in \mathrm{Ker}(\varphi)$ (т. е. $g\mathrm{Ker}(\varphi) = \mathrm{Ker}(\varphi)$). Остаётся проверить, что ψ — гомоморфизм:

$$\psi((g\mathrm{Ker}(\varphi))(g'\mathrm{Ker}(\varphi))) = \psi(gg'\mathrm{Ker}(\varphi)) = \varphi(gg') = \varphi(g)\varphi(g') = \psi(g\mathrm{Ker}(\varphi))\psi(g'\mathrm{Ker}(\varphi)).$$

□

Тем самым, чтобы удобно реализовать факторгруппу G/H, можно найти такой гомоморфизм $\varphi\colon G \to F$ в некоторую группу F, что $H = \mathrm{Ker}(\varphi)$, и тогда $G/H \cong \mathrm{Im}(\varphi)$.

Пример 3. Пусть $G = (\mathbb{R}, +)$ и $H = (\mathbb{Z}, +)$. Рассмотрим группу $F = (\mathbb{C} \setminus \{0\}, \times)$ и гомоморфизм

$$\varphi\colon G \to F, \quad a \mapsto e^{2\pi\imath a} = \cos(2\pi a) + i\sin(2\pi a).$$

Тогда $\mathrm{Ker}(\varphi) = H$ и факторгруппа G/H изоморфна окружности S^1, рассматриваемой как подгруппа в F, состоящая из комплексных чисел с модулем 1.

Определение 7. *Центр* группы G — это подмножество

$$Z(G) = \{a \in G \mid ab = ba \text{ для всех } b \in G\}.$$

Ясно, что группа G абелева тогда и только тогда, когда $Z(G) = G$.

Предложение 3. *Центр $Z(G)$ является нормальной подгруппой группы G.*

Доказательство. Сначала докажем, что $Z(G)$ — подгруппа в G. Для этого надо показать, что $ab^{-1} \in Z(G)$ для любых $a, b \in Z(G)$. В самом деле, для произвольного элемента $g \in G$ имеем

$$ab^{-1}g = ab^{-1}(g^{-1})^{-1} = a(g^{-1}b)^{-1} = a(bg^{-1})^{-1} = a(g^{-1})^{-1}b^{-1} = agb^{-1} = gab^{-1}.$$

Далее, если $a \in Z(G)$ и $g \in G$, то

$$g^{-1}agb = g^{-1}gab = ab = ba = bag^{-1}g = bg^{-1}ag$$

для всех $b \in G$. Значит, $g^{-1}ag \in Z(G)$ и подгруппа $Z(G)$ нормальна. □

Определим ещё одну важную конструкцию, позволяющую строить новые группы из имеющихся.

Определение 8. *Прямым произведением* групп $G_1, \ldots, G_m$ называется множество

$$G_1 \times \ldots \times G_m = \{(g_1, \ldots, g_m) \mid g_1 \in G_1, \ldots, g_m \in G_m\}$$

с операцией $(g_1, \ldots, g_m)(g'_1, \ldots, g'_m) = (g_1g'_1, \ldots, g_mg'_m)$.

Ясно, что эта операция ассоциативна, обладает нейтральным элементом $(e_{G_1}, \ldots, e_{G_m})$ и для каждого элемента $(g_1, \ldots, g_m)$ есть обратный элемент $(g_1^{-1}, \ldots, g_m^{-1})$.

Замечание 2. Группа $G_1 \times \ldots \times G_m$ коммутативна в точности тогда, когда коммутативна каждая из групп $G_1, \ldots, G_m$.

Замечание 3. Если все группы $G_1, \ldots, G_m$ конечны, то $|G_1 \times \ldots \times G_m| = |G_1| \cdot \ldots \cdot |G_m|$.

Следующий результат связывает конструкции факторгруппы и прямого произведения.

Теорема о факторизации по сомножителям. Пусть $H_1, \ldots, H_m$ — нормальные подгруппы в группах $G_1, \ldots, G_m$ соответственно. Тогда $H_1 \times \ldots \times H_m$ — нормальная подгруппа в $G_1 \times \ldots \times G_m$ и имеет место изоморфизм групп

$$(G_1 \times \ldots \times G_m)/(H_1 \times \ldots \times H_m) \cong G_1/H_1 \times \ldots \times G_m/H_m.$$

Доказательство. Прямая проверка показывает, что $H_1 \times \ldots \times H_m$ — нормальная подгруппа в $G_1 \times \ldots \times G_m$. Требуемый изоморфизм устанавливается отображением

$$(g_1, \ldots, g_m)(H_1 \times \ldots \times H_m) \mapsto (g_1H_1, \ldots, g_mH_m).$$

□

Теорема 2. *Пусть $n = ml$ — разложение натурального числа n на два взаимно простых множителя. Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \cong \mathbb{Z}_m \times \mathbb{Z}_l.$$

Доказательство. Рассмотрим отображение

$$\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_l, \quad k \pmod{n} \mapsto (k \pmod{m}, k \pmod{l}).$$

Поскольку m и l делят n, отображение φ определено корректно. Ясно, что φ — гомоморфизм. Далее, если k переходит в нейтральный элемент $(0, 0)$, то k делится и на m, и на l, а значит, делится на n в силу взаимной простоты m и l. Отсюда следует, что гомоморфизм φ инъективен. Поскольку множества $\mathbb{Z}_n$ и $\mathbb{Z}_m \times \mathbb{Z}_l$ содержат одинаковое число элементов, отображение φ биективно. □

Следствие 2. *Пусть $n \geqslant 2$ — натуральное число и $n = p_1^{k_1} \ldots p_s^{k_s}$ — его разложение в произведение простых множителей (где $p_i \neq p_j$ при $i \neq j$). Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}.$$

Список литературы

[1] Э. Б. Винберг. Курс алгебры. М.: Факториал Пресс, 2002 (глава 4, § 6 и глава 10, § 1)
[2] А. И. Кострикин. Введение в алгебру. Основы алгебры. М.: Наука. Физматлит, 1994 (глава 4, § 2)
[3] А. И. Кострикин. Введение в алгебру. Основные структуры алгебры. М.: Наука. Физматлит, 2000 (глава 1, § 4)
[4] Сборник задач по алгебре под редакцией А. И. Кострикина. Новое издание. М.: МЦНМО, 2009 (глава 13, § 58, 60)