

6. Шестая лекция, 31 января 2019 г.

От абелевых групп вернемся к произвольным группам.

6.1. Автоморфизмы групп.

ОПРЕДЕЛЕНИЕ 6.1. *Автоморфизм* группы — это её изоморфизм на себя.

ПРИМЕР 6.2. Отображение $A \mapsto (A^T)^{-1}$ является автоморфизмом группы матриц.

Все автоморфизмы группы G образуют группу, обозначаемую через $\text{Aut } G$.

Любой элемент $g \in G$ задаёт автоморфизм $a(g) \in \text{Aut } G$ при помощи *сопряжения*: $a(g)x = gxg^{-1}$. Такие автоморфизмы называются *внутренними*, их множество обозначается $\text{Int } G$.

Ясно, что $\text{Int } G$ — подгруппа в $\text{Aut } G$. Эта подгруппа нормальна: для любого автоморфизма $\varphi \in \text{Aut } G$ верно, что $\varphi a(g) \varphi^{-1} = a(\varphi(g))$.

Итак, у нас имеется отображение $G \rightarrow \text{Aut } G$ (каждому элементу группы $g \in G$ сопоставляется внутренний автоморфизм $a(g) \in \text{Aut } G$). Несложно проверить, что это отображение является гомоморфизмом:

$$a(gh)x = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = a(g)a(h)x.$$

Его ядро — это центр $Z(G)$ группы G . По теореме о гомоморфизме $\text{Int } G \cong G/Z(G)$.

ПРИМЕР 6.3. При $n \geq 3$ центр симметрической группы S_n тривиален. Поэтому $\text{Int } S_n \cong S_n$. Можно доказать, что при $n \neq 6$ никаких других автоморфизмов у S_n нет, а при $n = 6$ подгруппа $\text{Int } G \subset \text{Aut } G$ имеет индекс 2.

ПРИМЕР 6.4. Найдём группу $\text{Aut } \mathbb{Z}/n\mathbb{Z}$. Пусть $\varphi \in \text{Aut } \mathbb{Z}/n\mathbb{Z}$, $\varphi(\bar{1}) = \bar{k}$. Тогда

$$\varphi(\bar{\ell}) = \bar{k}\bar{\ell} = \bar{k} \cdot \bar{\ell},$$

где умножение понимается в смысле кольца $\mathbb{Z}/n\mathbb{Z}$. Таким образом, всякий автоморфизм группы $\mathbb{Z}/n\mathbb{Z}$ имеет вид $\varphi_k: \ell \rightarrow k\ell$. Обратно, для любого k отображение $\ell \mapsto k\ell$ является гомоморфизмом группы $\mathbb{Z}/n\mathbb{Z}$ в себя. Значит, гомоморфизм φ_k является автоморфизмом тогда и только тогда, когда k обратимо в кольце $\mathbb{Z}_n$. Поэтому $\text{Aut } \mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})^*$.

6.2. Полупрямое произведение. Понятие внутреннего автоморфизма позволяет переформулировать определение нормальной подгруппы: подгруппа нормальна тогда и только тогда, когда она инвариантна относительно всех внутренних автоморфизмов.

Пусть N — нормальная подгруппа в G , H — произвольная подгруппа. Тогда произведение $NH = \{nh : n \in N, h \in H\}$ является подгруппой. Действительно,

$$\begin{aligned}(n_1h_1)(n_2h_2) &= n_1(h_1n_2h_1^{-1})h_1h_2, \\ (nh)^{-1} &= h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1}.\end{aligned}$$

Кроме того, $NH = HN$.

ОПРЕДЕЛЕНИЕ 6.5. Говорят, что группа G разлагается в *полупрямое произведение* своих подгрупп N и H , если

- (1) N — нормальная подгруппа;
- (2) $N \cap H = \{e\}$;
- (3) $NH = G$.

Обозначение: $G = N \rtimes H$ (иногда используется другой значок: $G = N \ltimes H$).

ЗАМЕЧАНИЕ 6.6. Мнемоническое правило: острие треугольника в значке $\rtimes$ показывает на нормальную подгруппу, и это похоже на запись $N \triangleleft G$.

Как и в случае прямого произведения, свойства 2) и 3) эквивалентны тому, что каждый элемент из G единственным образом представляется в виде произведения элементов из N и H .

ПРИМЕР 6.7. $S_n = A_n \rtimes \langle (12) \rangle$.

УПРАЖНЕНИЕ 6.8. (вариация на тему предыдущего примера). Пусть известно, что $S_n = A_n \rtimes \langle \sigma \rangle$. Что можно сказать о перестановке σ ?

ПРИМЕР 6.9. $S_4 = V_4 \rtimes S_3$, где V_4 — четверная группа Клейна, а S_3 вложена в S_4 как группа перестановок, оставляющих на месте символ 4.

ПРИМЕР 6.10. $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes \{\mathrm{diag}(\lambda, 1, \dots, 1) \mid \lambda \in K^*\}$.

6.3. «Внешнее» полупрямое произведение групп. Мы только что определили разложение группы в полупрямое произведение двух своих подгрупп (одна из которых должна быть нормальной). Можно действовать иначе: для двух групп N и H рассмотреть их *внешнее* полупрямое произведение, т.е. построить группу $G = N \ltimes H$ аналогично тому, как это делалось для прямого произведения. Отличие от прямого произведения состоит в том, что для описания полупрямого произведения необходима дополнительная информация — а именно, нужно задать для каждого элемента из H нужно задать автоморфизм $\alpha(h)$ группы N , которым h будет действовать на N . Это соответствие должно быть гомоморфизмом групп $H \rightarrow \mathrm{Aut} N$.

Итак, пусть $N \times H$ — прямое произведение N и H как множеств, т.е. множество пар (n, h) . Пусть также задан гомоморфизм $\alpha: H \rightarrow \mathrm{Aut} N$. Определим на множестве $N \times H$ умножение следующим образом:

$$(n_1, h_1)(n_2, h_2) = (n_1 \alpha(h_1)n_2, h_1 h_2).$$

Обратный элемент к (n, h) будет определяться так:

$$(n, h)^{-1} = (\alpha(h^{-1})n^{-1}, h^{-1}).$$

Тем самым на $N \times H$ будет задана структура группы, которая называется *внешним полупрямым произведением* N и H и обозначается через $N \ltimes_{\alpha} H$. При этой конструкции разным гомоморфизмам α будут соответствовать, вообще говоря, неизоморфные группы! Так, например, если α переводит каждый элемент H в тождественный автоморфизм группы N , то полученная группа будет прямым произведением групп N и H .

Обратно, если группа G раскладывается в полупрямое произведение своих подгрупп: $G = N \ltimes H$, то имеется изоморфизм групп $N \ltimes_{\alpha} H \rightarrow G$. (Как при этом будет действовать на N автоморфизм $\alpha(h)$?)

ПРИМЕР 6.11. Рассмотрим две циклические группы: $\langle a \rangle_n \cong \mathbb{Z}/n\mathbb{Z}$ и $\langle b \rangle_m \cong \mathbb{Z}/m\mathbb{Z}$. Гомоморфизм $\langle b \rangle_m \rightarrow \mathrm{Aut} \mathbb{Z}/n\mathbb{Z}$ полностью определяется тем, как действует образующая b . Как обсуждалось на прошлой лекции, $\mathrm{Aut} \mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}/n\mathbb{Z})^*$, поэтому всякий автоморфизм $\mathbb{Z}/n\mathbb{Z}$ есть возведение элемента a в некоторую степень k . Таким образом, задать гомоморфизм $\langle b \rangle_m \rightarrow \mathbb{Z}/n\mathbb{Z}$ значит задать такое k , что $k^m \equiv 1 \pmod n$. Такое полупрямое произведение обозначается через $\langle a \rangle_n \ltimes_k \langle b \rangle_m$. Вообще говоря, при различных k эти группы могут оказаться изоморфными.

В частности, если $(\varphi(n), m) = 1$, то $k = 1$, и всякий такой гомоморфизм α тривиален, т.е. в этом случае не бывает полупрямых произведений $\mathbb{Z}/n\mathbb{Z}$ и $\mathbb{Z}/m\mathbb{Z}$, отличных от прямого произведения.

ПРИМЕР 6.12. Рассмотрим группу $\langle a \rangle_n \ltimes_{-1} \langle b \rangle_2$. Она задаётся соотношениями соотношениями $a^n = b^2 = 1$ и $bab^{-1} = a^{-1}$. Поэтому это группа самосовмещений n -угольника.

E-mail address: esmirnov@hse.ru