19. Девятнадцатая лекция, 14 февраля 2022 г.

19.1. **Прямые произведения.** Для начала напомним понятие прямого произведения групп.

Определение 19.1. Группа G раскладывается в *прямое произведение* своих подгрупп $G_1, \dots, G_k$, если:

(1) каждый элемент $g \in G$ единственным образом представляется в виде произведения $g = g_1 \dots g_k$, где $g_i \in G_i$;
(2) $g_i g_j = g_j g_i$ при $g_i \in G_i$, $g_j \in G_j$, $i \neq j$.

Обозначение: $G = G_1 \times \dots \times G_k$.

Во-первых, из условия 1) (точнее, из единственности такого представления) следует, что $G_i \cap G_j = \{e\}$. Далее, если условие 1) выполнено, то условие 2) равносильно требованию нормальности групп G_i. Докажем это.

Лемма 19.2. *Пусть G_1 и G_2 — нормальные подгруппы в G, причем $G_1 \cap G_2 = \{e\}$. Тогда $g_1 g_2 = g_2 g_1$ для любых $g_1 \in G_1$, $g_2 \in G_2$.*

Доказательство. Докажем, что $g_1 g_2 g_1^{-1} g_2^{-1} = e$. Действительно,

$$g_1 g_2 g_1^{-1} g_2^{-1} = (g_1 g_2 g_1^{-1}) g_2^{-1} \in G_2,$$

т.к. в силу нормальности группы G_2 имеем $g_1 g_2 g_1^{-1} \in G_2$. По той же причине $g_1 g_2 g_1^{-1} g_2^{-1} = g_1 (g_2 g_1^{-1} g_2^{-1}) \in G_1$. Значит, $g_1 g_2 g_1^{-1} g_2^{-1} \in G_1 \cap G_2$, то есть равняется единице. □

Рассмотрим случай двух множителей отдельно.

Предложение 19.3. *Группа G разлагается в прямое произведение своих подгрупп G_1 и G_2 тогда и только тогда, когда*

(1) *G_1 и G_2 — нормальные подгруппы;*
(2) *$G_1 \cap G_2 = \{e\}$;*
(3) *$G_1 G_2 = G$, т.е. каждый элемент $g \in G$ представляется в виде $g = g_1 g_2$, где $g_1 \in G_1$, $g_2 \in G_2$.*

Доказательство. Часть «только тогда» доказана выше. Пусть теперь выполнены условия 1)–3). Тогда по предыдущей лемме $g_1 g_2 = g_2 g_1$ при $g_1 \in G_1$, $g_2 \in G_2$. Проверим единственность такого представления. Пусть $g_1 g_2 = \tilde{g}_1 \tilde{g}_2$. Тогда $\tilde{g}_1^{-1} g_1 = g_2 \tilde{g}_2^{-1} \in G_1 \cap G_2 = \{e\}$. Поэтому $g_1 = \tilde{g}_1$, $g_2 = \tilde{g}_2$. □

Выше мы предполагали, что группы G_i — подгруппы в одной и той же группе G. В этой ситуации иногда говорят о *внутреннем* прямом произведении. Можно, наоборот, для заданного набора групп G_i (вообще говоря, не вложенных в какую-то большую группу) построить такую группу G, которая будет раскладываться в прямое произведение своих подгрупп, изоморфных G_i.

Определение 19.4. *Прямым произведением* групп $G_1, \dots, G_k$ называется множество последовательностей $(g_1, \dots, g_k)$, где $g_i \in G_i$, с покомпонентными операциями умножения и взятия обратного. Обозначение: $G_1 \times \dots \times G_k$.

Ясно, что такие операции задают на $G_1 \times \dots \times G_k$ структуру группы, единицей которой является набор $(e, \dots, e)$. Кроме того, каждая из групп G_i вкладывается в $G_1 \times \dots \times G_k$ как подгруппа: $g_i \mapsto (e, \dots, e, g_i, e, \dots, e)$, где неединичный элемент стоит на i-м месте. Тогда $G_1 \times \dots \times G_k$ есть прямое произведение своих подгрупп G_i в смысле первого определения.

Пример 19.5. Группа ненулевых комплексных чисел $\mathbb{C}^*$ раскладывается в прямое произведение групп $\mathbb{R}_+ \times U(1)$, где $U(1)$ — группа комплексных чисел единичного модуля. Это не что иное, как представление комплексного числа в тригонометрической форме: $z = re^{i\varphi}$ (для ненулевого числа это представление единственно).

Пример 19.6. Каждое движение плоскости может быть представлено, причем единственным образом, в виде композиции параллельного переноса и ортогонального преобразования (сохраняющего начало координат). Однако это не прямое произведение, т.к., например, подгруппа ортогональных преобразований не является нормальной в группе всех движений (или, иначе говоря, ортогональные преобразования не коммутируют с параллельными переносами). Зато оказывается, что это является разложением в так называемое *полупрямое произведение*, о котором речь пойдёт дальше.

19.2. **Автоморфизмы групп.**

Определение 19.7. *Автоморфизм* группы — это её изоморфизм на себя.

Пример 19.8. Отображение $A \mapsto (A^T)^{-1}$ является автоморфизмом группы матриц.

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

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

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

Итак, у нас имеется отображение $G \to \operatorname{Aut} G$ (каждому элементу группы $g \in G$ сопоставляется внутренний автоморфизм $a(g) \in \operatorname{Aut} G$). 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 $\operatorname{Int} G \cong G/Z(G)$.

Пример 19.9. При $n \geq 3$ центр симметрической группы S_n тривиален. Поэтому $\operatorname{Int} S_n \cong S_n$. Можно доказать, что при $n \neq 6$ никаких других автоморфизмов у S_n нет, а при $n = 6$ подгруппа $\operatorname{Int} G \subset \operatorname{Aut} G$ имеет индекс 2.

Пример 19.10. Найдём группу $\operatorname{Aut} \mathbb{Z}_n$. Пусть $\varphi \in \operatorname{Aut} \mathbb{Z}_n$, $\varphi(\overline{1}) = \overline{k}$. Тогда

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

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