Гимназия 1543, 10-В класс, 23 октября.

Гомоморфизмы.

Пусть G_1, G_2 — группы. *Гомоморфизмом* $\varphi: G_1 \to G_2$ называется произвольное *мультипликативное* отображение группы G_1 в группу G_2. Под словом мультипликативность мы понимаем, что $\varphi(a \circ b) = \varphi(a) \circ \varphi(b)$. Отметим, что в этом выражении символом $\circ$ обозначены групповые операции в разных группах: слева — в G_1, справа — в G_2. Приведём примеры гомоморфизмов.

1) Тождественный гомоморфизм; $\varphi: G \to G$, $\varphi(a) = a$.

2) Аннулирующий гомоморфизм; $\varphi: G \to G$, $\varphi(a) = e$.

3) Чётность подстановки; $\varphi: S_n \to \mathbb{Z}_2$, $\varphi(\sigma)$ равно 0, если подстановка σ чётная, и 1, если σ нечётная.

4) Остаток по модулю k; $\varphi: \mathbb{Z} \to \mathbb{Z}_k$, $\varphi(n) = n \bmod k$.

С каждым гомоморфизмом $\varphi: G_1 \to G_2$ связаны две важные подгруппы: *ядро* $\ker\varphi \leqslant G_1$ и *образ* $\operatorname{Im}\varphi \leqslant G_2$ гомоморфизма. Разберём каждое из этих двух понятий по отдельности.

Ядром гомоморфизма называется полный прообраз нейтрального элемента. Докажем, что ядро — группа. Пусть a и b лежат в $\ker\varphi$.

Замкнутость: $\varphi(ab) = \varphi(a)\varphi(b) = ee = e$.

Наличие нейтрального элемента: $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$, значит $\varphi(e) = e$ и, следовательно, $e \in \ker\varphi$.

Наличие обратного для a элемента: $e = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) = \varphi(a^{-1})$, откуда следует $a^{-1} \in \ker\varphi$.

Образом гомоморфизма называется образ группы G_1. Докажем, что образ гомоморфизма — группа. Пусть a и b лежат в $\operatorname{Im}\varphi$. Обозначим через c и d какие-нибудь прообразы a и b соответственно.

Замкнутость: $ab = \varphi(c)\varphi(d) = \varphi(cd)$, поэтому $ab \in \operatorname{Im}\varphi$.

Наличие нейтрального элемента: $\varphi(e) = e$, значит $e \in \operatorname{Im}\varphi$.

Наличие обратного для a элемента: $\varphi(c^{-1})a = \varphi(c^{-1})\varphi(c) = \varphi(c^{-1}c) = \varphi(e) = e$, значит $\varphi(c^{-1})$ обратен к a.

Подгруппа H группы G, являющаяся ядром некоторого гомоморфизма φ, называется *нормальной* или *нормальным делителем группы* G. Образ φ обозначается G/H и называется *факторгруппой группы* G *по подгруппе* H. Образы разных гомоморфизмов с одинаковым ядром изоморфны (это будет доказано чуть позже), поэтому определение факторгруппы корректно. Перед тем, как приводить примеры, дадим удобный критерий нормальности подгруппы.

Критерий нормальности: H нормальна в G тогда и только тогда, когда $\forall h \in H$, $\forall a \in G$ выполенено $a^{-1}ha \in H$ (что, очевидно, равносильно равенству правого и левого смежных классов $Ha = aH$).

1) Пусть H нормальна в G, т.е. $H = \ker\varphi$. Заметим, что $\varphi(a^{-1}ha) = \varphi(a^{-1})\varphi(h)\varphi(a) = \varphi(a^{-1})\varphi(a) = \varphi(e) = e$.

2) Пусть $\forall h \in H$, $\forall a \in G$ выполенено $a^{-1}ha \in H$. Будем строить гомоморфизм φ, ядром которого будет являться H. Вспомним, что группу G можно представить, как дизъюнктное объединение смежных классов элементов G: $G = \{a_\alpha H\}_{\alpha\in I}$, $a_\alpha \in G$. Введём на индексном множестве I групповую структуру. Паре индексов α, β сопоставим такой (единственный!) индекс $p(\alpha,\beta) \in I$, что $a_\alpha a_\beta \in a_{p(\alpha,\beta)}H$. Докажем, что такая операция обладает всеми нужными свойствами (в доказательстве буквой h будем обозначать элементы H).

Ассоциативность: $a_{p(\alpha,\beta)}a_\gamma = a_\alpha a_\beta h_1 a_\gamma = a_\alpha a_\beta a_\gamma h_2 = a_\alpha a_{p(\beta,\gamma)} h_3 h_2$. Левый член цепочки лежит в смежном классе элемента $a_{p(p(\alpha,\beta),\gamma)}$, а правый — в смежном классе элемента $a_{p(\alpha,p(\beta,\gamma))}$. Значит, смежные классы этих элементов совпадают, и, следовательно, $p(p(\alpha,\beta),\gamma) = p(\alpha,p(\beta,\gamma))$.

Наличие нейтрального элемента: пусть $e \in a_\omega H$. Заметим, что смежный класс элемента $a_{p(\omega,\alpha)}$ содержит произведение $a_\omega a_\alpha$. Но $a_\omega \in H$, поэтому смежный класс элемента $a_{p(\omega,\alpha)}$ содержит также и a_α. Значит, $p(\omega,\alpha) = \alpha$.

Наличие обратного для α элемента: пусть $a_\alpha^{-1} \in a_\beta H$. Рассмотрим $a_{p(\alpha,\beta)}$. Смежный класс этого элемента содержит произведение $a_\alpha a_\beta = a_\alpha a_\alpha^{-1} h = h$. h, очевидно, содержится в смежном классе a_ω, поэтому $p(\alpha,\beta) = \omega$.

Теперь можно построить гомоморфизм φ. Будем отображать G в I так, что $\varphi(a_\alpha H) = \{\alpha\}$. Докажем, что это гомоморфизм. Пусть $x \in a_\alpha H$, $y \in a_\beta H$. Тогда $\varphi(xy) = \varphi(a_\alpha h_1 a_\beta h_2) = \varphi(a_\alpha a_\beta h_3 h_2) = p(\alpha,\beta) = p(\varphi(x),\varphi(y))$. Поэтому φ является гомоморфизмом. Ядром φ, очевидно, является класс $a_\omega H = H$.

Заметим заодно, что мы доказали ещё и корректность определения факторгруппы. Ведь образы всех гомоморфизмов ψ с ядром H изоморфны группе I (изоморфизмом является отображение $\varphi\circ\psi^{-1}$, где под ψ^{-1} понимается любое из отображений $G' \to G$, ставящее в соответствие элементу группы G' какой-то из его прообразов).

Теперь обещанные примеры.

1) Тождественный гомоморфизм имеет тривиальное ядро. Образ его — вся группа.

2) Аннулирующий гомоморфизм имеет ядро, равное всей группе. Образ такого гомоморфизма — тривиальная группа.

3) Чётность подстановки аннулирует все чётные подстановки. Ядро — A_n. Образ $S_n/A_n = \mathbb{Z}_2$.

4) Остаток по модулю k обращает в нуль все числа, кратные k (т.е. элементы группы $k\mathbb{Z}$ целых кратных k чисел по сложению). Образ этого гомоморфизма $\mathbb{Z}_k$. Отсюда обозначение $\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}$.

5) Повороты плоскости являются нормальным делителем группы движений плоскости. Действительно, если сделать некое движение, затем поворот, затем движение, обратное первому, получим поворот. Факторгруппа по этому нормальному делителю — множество всевозможных параллельных переносов и скользящих симметрий относительно одного фиксированного семейства параллельных прямых.