Гомоморфизм и изоморфизм в группах. Факторгруппы: теорема о гомоморфизме.

1 Гомоморфизм и изоморфизм

Определение 1.1. *Гомоморфизмом из группы* $G = (M, \cdot)$ *в группу* $G' = (M', \circ)$ *будем называть такое отображение* $\varphi\colon G \to G'$, *что*

$$\forall a, b, \in G \hookrightarrow \varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$$

Образ гомоморфизма $Im\varphi = \varphi(G) = \{\varphi(a) \mid a \in G\} \subset G'$

1.1 Свойства гомоморфизма

- $\varphi(e) = e'$

  Доказательство.
  $$\varphi(a \cdot e) = \varphi(a) \circ \varphi(e) = \varphi(a) = \varphi(e \cdot a) = \varphi(e) \circ \varphi(a)$$
  $\square$

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

  Доказательство.
  $$\varphi(a \cdot a^{-1}) = \varphi(a^{-1} \cdot a) = \varphi(e) = e' = \varphi(a) \circ \varphi(a^{-1}) = \varphi(a^{-1}) \circ \varphi(a)$$
  $\square$

- Порядок $\varphi(a)$ является делителем порядка a

  Доказательство. Пусть $m = ord(a)$. Тогда
  $$\varphi(a^m) = \varphi(e) = e'$$
  Но
  $$\varphi(a^m) = (\varphi(a))^m$$
  Получаем
  $$(\varphi(a))^m = e' \implies ord(\varphi(a)) \mid m$$
  $\square$

Теорема 1.1. $Im\varphi < G'$

Доказательство. По определению образа гомоморфизма:

$$\forall c, d \in Im\varphi \quad \exists a, b \in G : \quad \varphi(a) = c, \quad \varphi(b) = d$$

Рассмотрим $c \circ d^{-1}$:

$$c \circ d^{-1} = \varphi(a) \circ (\varphi(b))^{-1} = \varphi(a) \circ \varphi(b^{-1}) = \varphi(a \cdot b^{-1}) \in Im\varphi$$

Тогда по критерию подгруппы получаем:

$$Im\varphi < G'$$

$\square$

Определение 1.2. *Ядро гомоморфизма* $Ker\varphi = \{g \mid g \in G,\ \varphi(g) = e' \in G'\}$

Теорема 1.2. $Ker\varphi \triangleleft G$

Доказательство.

1. Покажем, что $Ker\varphi < G$. Действительно:

$$\forall a, b \in Ker\varphi \hookrightarrow \varphi(a \cdot b^{-1}) = \varphi(a) \circ \varphi(b^{-1}) = e' \circ (e')^{-1} = e'$$

   Тогда:

$$\forall a, b \in Ker\varphi \hookrightarrow a \cdot b^{-1} \in Ker\varphi$$

   Значит окончательно по критерию подгруппы:

$$Ker\varphi < G$$

2. Покажем, что $Ker\varphi \triangleleft G$. В самом деле, $\forall g \in G,\ \forall h \in Ker\varphi$:

$$\varphi(g \cdot h \cdot g^{-1}) = \varphi(g) \circ \varphi(h) \circ \varphi(g^{-1}) = \varphi(g) \circ \varphi(g^{-1}) = e'$$

   Тогда получаем:

$$\forall g \in G,\ \forall h \in Ker\varphi \hookrightarrow g \cdot h \cdot g^{-1} \in Ker\varphi$$

   Из этого по теореме об эквивалентном определении нормальной подгруппы получаем требуемое.

□

Определение 1.3. *Сюръективным гомоморфизмом из группы G <u>на</u> G' будем называть гомоморфизм $\varphi\colon G \to G'$, являющийся сюръекцией, то есть:*

$$\forall b \in G'\ \exists a \in G :\ \ \varphi(a) = b$$

Ясно, что при этом

$$Im\varphi = G'$$

Определение 1.4. *Изоморфизм — гомоморфизм, являющийся биекцией (обозначается $\cong$)*

2 Факторгруппы: теорема о гомоморфизме

Определение 2.1. *Пусть $H \triangleleft G$. Рассмотрим смежные классы (для определённости левые, естественным образом по H). Введем операцию*

$$(a \cdot H) * (b \cdot H) = (a \cdot b) \cdot H$$

Лемма 2.1. *Множество смежных классов относительно данной операции образуют группу, называемую факторгруппой группы G по нормальной подгруппе H и обозначаемую G/H.*

Доказательство. Действительно, выполнены все аксиомы группы:

1. Ассоциативность:

$$\forall a, b, c \in G \hookrightarrow \begin{cases} ((a \cdot H) * (b \cdot H)) * (c \cdot H) = ((a \cdot b) \cdot H) * (c \cdot H) = (a \cdot b \cdot c) \cdot H \\ (a \cdot H) * ((b \cdot H) * (c \cdot H)) = (a \cdot H) * ((b \cdot c) \cdot H) = (a \cdot b \cdot c) \cdot H \end{cases}$$

2. $e \cdot H = H$ — нейтральный элемент:

$$\forall a \in G \hookrightarrow (a \cdot H) * (e \cdot H) = (a \cdot e) \cdot H = a \cdot H$$

Если $n \cdot H$ и $e \cdot H$ — нейтральные элементы, то

$$(n \cdot H) * (e \cdot H) = n \cdot H = e \cdot H$$

3. Существование обратного:

$$\forall a \in G \hookrightarrow (a \cdot H) * (a^{-1} \cdot H) = (a \cdot a^{-1}) \cdot H = e \cdot H = H$$

□

Замечание 2.1. *Нормальность подгруппы H нужна для корректности, то есть для независимости представителя.*
Действительно, если рассмотреть представителя $a \in G$ и смежный класс $a \cdot H$, а затем взять $a_1 \in a \cdot H$, то

$$a_1 \cdot H = a \cdot H$$

По аналогии рассматривая смежный класс $b \cdot H$ с представителем $b \in G$, получим, что для элемента $b_1 \in b \cdot H$ выполнено:

$$b_1 \cdot H = b \cdot H$$

Это следует из того, что смежные классы не пересекаются или совпадают.
Было бы неловко, если бы

$$(a \cdot H) * (b \cdot H) = (a \cdot b) \cdot H \neq (a_1 \cdot b_1) \cdot H = (a_1 \cdot H) * (b_1 \cdot H)$$

Для того, чтобы таких печальных ситуаций не происходило, требуется нормальность подгруппы H. Проверим, что при соблюдении нормальности все будет хорошо, доказав нижеследующую лемму.

Лемма 2.2. *Если*

$$H \triangleleft G, \quad a, b \in G, \quad a_1 \in a \cdot H, \quad b_1 \in b \cdot H$$

то

$$a_1 \cdot b_1 \in (a \cdot b) \cdot H$$

Доказательство.

$$\begin{cases} a_1 \in a \cdot H \iff \exists h_a \in H : a_1 = a \cdot h_a \\ b_1 \in b \cdot H \iff \exists h_b \in H : b_1 = b \cdot h_b \end{cases} \tag{1}$$

Отсюда

$$a_1 \cdot b_1 = a \cdot h_a \cdot b \cdot h_b$$

Так как $H \triangleleft G$, то

$$\forall h_a \in H \; \exists \widetilde{h} \in H : \; h_a \cdot b = b \cdot \widetilde{h}$$

Заменяя в (1) $h_a \cdot b$ на $b \cdot \widetilde{h}$, окончательно получим:

$$a_1 \cdot b_1 = a \cdot h_a \cdot b \cdot h_b = a \cdot b \cdot \widetilde{h} \cdot h_b \in (a \cdot b) \cdot H$$

□

Теорема 2.1. *Рассмотрим факторгруппу $G/Ker\varphi$. Два элемента группы G содержатся в одном смежном классе по $Ker\varphi$ тогда и только тогда, когда их образы совпадают.*

Доказательство.

- ($\Longrightarrow$): Пусть $a, b \in g \cdot Ker\varphi$. Тогда:

$$\exists h_a, h_b \in Ker\varphi : \begin{cases} a = g \cdot h_a \\ b = g \cdot h_b \end{cases}$$

Значит по определению гомоморфизма:

$$\begin{cases} \varphi(a) = \varphi(g \cdot h_a) = \varphi(g) \circ \varphi(h_a) = \varphi(g) \circ e' = \varphi(g) \\ \varphi(b) = \varphi(g \cdot h_b) = \varphi(g) \circ \varphi(h_b) = \varphi(g) \circ e' = \varphi(g) \end{cases}$$

- ($\Longleftarrow$): Пусть $a, b \in G : \varphi(a) = \varphi(b)$. Тогда:

$$\varphi(a \cdot b^{-1}) = \varphi(a) \circ (\varphi(b))^{-1} = e'$$

Отсюда:

$$a \cdot b^{-1} \in Ker\varphi$$

Значит:

$$a = (a \cdot b^{-1}) \cdot b \in (Ker\varphi) \cdot b = b \cdot (Ker\varphi)$$

При этом очевидно, что:

$$a \in a \cdot Ker\varphi$$

Значит в силу того, что смежные классы не пересекаются или совпадают, получаем:

$$a \cdot Ker\varphi = b \cdot Ker\varphi$$

□

Теорема 2.2. ~~*Гомоморфный образ группы до победы коммунизма изоморфен факторгруппе по ядру гомоморфизма*~~ $Im\varphi \cong G/Ker\varphi$

Доказательство. Из теоремы 2.1 получаем, что между $Im\varphi$ и $G/Ker\varphi$ существует биекция f:

$$f\colon \varphi(g) \to g \cdot Ker\varphi$$

Тогда

$$f(\varphi(g)) = g \cdot Ker\varphi$$

При этом под $g \cdot Ker\varphi$ теперь понимается не множество, а смежный класс как один элемент. Далее заметим, что с одной стороны:

$$f(\varphi(a) \circ \varphi(b)) = f(\varphi(a \cdot b)) = (a \cdot b) \cdot Ker\varphi$$

С другой стороны:

$$f(\varphi(a)) * f(\varphi(b)) = (a \cdot Ker\varphi) * (b \cdot Ker\varphi) = (a \cdot b) \cdot Ker\varphi$$

Тогда тривиально видеть, что:

$$f(\varphi(a) \circ \varphi(b)) = f(\varphi(a)) * f(\varphi(b))$$

Получили, что f есть биективный гомоморфизм. Значит f есть изоморфизм, что и требовалось. □