1 Гомоморфизмы группы

Определение 1.1 (Факторгруппа)**.** Рассмотрим группу G и ее нормальную подгруппу H. Пусть G/H — множество смежных классов G по H. Определим в G/H операцию умножения по следующему правилу: $aH \cdot bH = (ab)H$

Теорема 1.1. *Определение произведения смежных классов корректно. То есть произведение смежных классов не зависит от выбранных представителей a и b*

Доказательство. Пусть $aH, bH \in G/H$, $a_1 = a \cdot h_a \in aH$, $b_1 = b \cdot h_b \in bH$. Докажем, что $abH = a_1 b_1 H$. Достаточно показать, что $a_1 \cdot b_1 \in abH$.

В самом деле, $a_1 \cdot b_1 = a \cdot h_a \cdot b \cdot h_b = a \cdot b \cdot (b^{-1} \cdot h_a \cdot b) \cdot h_b$. Элемент $h = (b^{-1} \cdot h_a \cdot b)$ лежит в H по свойству нормальности H. Следовательно, $a \cdot b \cdot h \cdot h_b \in abH$. □

Теорема 1.2. *Если G и H - группа, $h : G \to H$ и $h(a * b) = h(a) * h(b)$, то h - гомоморфизм*

Доказательство. $h(e) = h(e * e) = h(e) * h(e)$

$h(e)$ - идемпотент в $\mathcal{H}$, следовательно $h(e) = e$

$$h(a^{-1}) = h(a^{-1}) * e = h(a^{-1}) * h(a) * (h(a))^{-1} = \\ h(a^{-1} * a) * (h(a))^{-1} = h(e) * (h(a))^{-1} = e * (h(a))^{-1} = (h(a))^{-1}$$

□

Определение 1.2 (Порождённая конгруэнтность)**.** Конгруэнтность порождённая h - если $a \equiv b \Leftrightarrow h(a) = h(b)$ - конгруэнтность, то $h[A] = {}^{A}/_{\equiv}$

Теорема 1.3. *Если $h : G \to H$ - гомоморфизм, $\equiv$ - конгруэнтность порождённая h, то классы эквивалентные e в G являются нормальными подгруппами*

Доказательство. Пусть $a, b \in f \Rightarrow ab^{-1} \in f$, $a \equiv e$, $b \equiv e$, $b^{-1} \equiv e^{-1} \equiv e$, $ab^{-1} \equiv ee \equiv e$

$$a\{b \in \mathcal{G} : b \equiv e\} \ni c$$
$$aba^{-1} \in \{b \in \mathcal{G} : b \equiv e\}a \ni c$$

$$c = ab = abe = aba^{-1}a$$

$$b \equiv e \quad a \equiv a \quad a^{-1} \equiv a^{-1}$$
$$aba^{-1} \equiv aea^{-1} = e$$
$$aba^{-1} \equiv e$$
$$aba^{-1}a = abe = ab = c$$

□

"И в обратную сторону". Хотя я в душе не знаю как в эту получилось.

Определение 1.3 (Ядро подгруппы)**.** Ядро подгруппы - множество элементов эквивалентных e. $\operatorname{Ker} h$

Теорема 1.4. *G - группа, H - нормальная подгруппа, $a \equiv b \Leftrightarrow a$ и b принадлежат одному левому классу, то $\equiv$ - конгруэнтность*

Доказательство. Пусть $a \equiv b$, $c \equiv d$, надо доказать

1. $ac \equiv bd$
2. $a^{-1} \equiv b^{-1}$ (зачем)

1.

$$\begin{aligned} &a, b \in x\mathcal{H} && a = xh_a, b = xh_b \\ &c, d \in y\mathcal{H} && c = yh_c, d = yh_d \end{aligned}$$

$ac = xh_a \cdot yh_c$, $h_a y = yh'$, $h_a y \in \mathcal{H}y = y\mathcal{H}$

$$\left.\begin{aligned} ac = xh_a y h_c = xy\underbrace{h'h_c}_{\in\mathcal{H}} \in xy\mathcal{H} \\ bd = xh_b y h_d = xy\underbrace{h''h_d}_{\in\mathcal{H}} \in xy\mathcal{H} \end{aligned}\right\} \text{эквивалентные}$$

$h_b y = yh''$, $h_b y \in \mathcal{H}y = y\mathcal{H}$

2.

$$\begin{aligned} &h_a && h_b \\ &h_a^{-1} && h_b^{-1} \\ &\mathcal{H}x^{-1} && \mathcal{H}x^{-1} \end{aligned}$$

$a^{-1}, b^{-1} \in x^{-1}\mathcal{H}$

$\square$

Определение 1.4 (щито)**.** $\mathcal{G}$ - группа, $\mathcal{H}$ - нормальная подгруппа, $\equiv$ - отношение конгруэнтности. Тогда ${}^{\mathcal{G}}/_{\equiv} = {}^{\mathcal{G}}/_{\mathcal{H}}$

Следствие 1.1. *Если $h : \mathcal{G} \to \mathcal{H}$ - гомоморфизм, тогда $h[\mathcal{G}] = {}^{\mathcal{G}}/_{\operatorname{Ker} h}$*

Доказательство. $h[\mathcal{G}] = {}^{\mathcal{G}}/_{\equiv} = {}^{\mathcal{G}}/_{\operatorname{Ker} h}$ $\square$

Пример 1.1.

$$\mathcal{D}_3 = \{e, r_1, r_2, s_1, s_2, s_3\}$$

$\langle r_1 \rangle$ - *подгруппа вращений*

$\langle r_1 \rangle$

$S_1\langle r_1 \rangle$

Таблица умножения (ЧЕГО???)

	$\langle r_1 \rangle$	$S_1\langle r_1 \rangle$
$\langle r_1 \rangle$	$\langle r_1 \rangle$	$S_1\langle r_1 \rangle$
$S_1\langle r_1 \rangle$	$S_1\langle r_1 \rangle$	$\langle r_1 \rangle$

Пример 1.2. $(\mathbb{R}, +) \supseteq (\mathbb{Z}, +)$

$a + \mathbb{Z}$

$ba \in \mathbb{Z}$

$a + \mathbb{Z} = b + \mathbb{Z}$

$a \in [0, 1)$

$(a + \mathbb{Z}) + (b + \mathbb{Z}) = (a + b) = (a + b) \mod 1$

$\mathbb{C}_1 = \{z \in \mathbb{C}, |z| = 1\}, (\mathbb{C}_1, \cdot)$

$h(x) = e^{2nix}$

$x \in \mathbb{R} = e^{2nix} \in \mathbb{C}_1$

$h(x + y) = e^{2ni(x+y)} = e^{2nix}e^{2niy} = h(x)h(y)$

$h : (\mathbb{R}, +) \to (\mathbb{C}, \cdot)$

$r \in \operatorname{Ker} h \Leftrightarrow r \equiv e$

$h(r) = h(e)$

$h(r) = h(0)$

$e^{2nix} = e^{2nix} = 1$

$e^{2nix} = 2n \cdot k, k \in \mathbb{Z}$

$r \in \mathbb{Z}$

$\operatorname{Ker} h \in \mathbb{Z}$

Определение 1.5. $\mathcal{G}$ - группа, A - множество, образующее группу, тогда определяющим соотношением называют равенство вида $t(a) = s(a)$, где t, s - термы, $a \in A$

Пример 1.3. $A = \{a, b\}$, $a^2 = b^2$, $a^3 b = ba$

Определение 1.6. A - множество элементов, X - множество определяющих соотношений. Группа, порождённая A и X - $\mathcal{G}$ такач, что

1. образована при помощи A
2. в $\mathcal{G}$ выполняются все определяющие соотношения из X
3. любая группа $\mathcal{H}$, удовлетворяющая условиям 1 и 2 является гомоморфным множеством $\mathcal{G}$

Пример 1.4.

$$\mathcal{D}_3 = \{e, r_1, r_2, s_1, s_2, s_3\}$$

$A = \{r_1, s_1\}$, $\langle A \rangle = \mathcal{D}_3$

$$\left[\begin{array}{l} r_1^3 = e \\ r_1 s_1 = s_1 r_1^2 \\ s_1^2 = e \end{array}\right.$$

$\mathcal{H}$ порождена A

$*$ - одноместная операция

$\mathcal{H}$?????? ??? слова, состоящие из $r_1, s_1, r_1^{-1}, s_1^{-1}$, пусть в $\mathcal{H}$ выполнены определяющие соотношения X

$$\begin{array}{lll} r_1^3 = e & r_1^{-1} = r_1^2 & r_1^{-1} = r_1 r_1 \\ s_1^2 = e & s_1^{-1} = s_1 & s_1^{-1} = s_1 \end{array}$$

$s_1 ... s_1 r_1 ... r_1$

$s_1^n r_1^m$

$s_1^n = s_1^{n \mod 2}$

$r_1^m = r^{m \mod 3}$

r_1^0	$s_1 r_1^0$
r_1^0	$s_1 r_1^0$
r_1^0	$s_1 r_1^0$

Теорема 1.5. *Для любого множества A и множества определяющих соотношений X существует группа, образованная A и X*

Доказательство. Пусть $A' = A \cup \{a{-}1 : a \in A^{\}}$. Нужно проверить три свойства

1. Если M - свободный моноид образованный $A'(M$ - множество слов алфавита A' с конкатенацией), M' - моноид, порождённый A', то M' - гомоморфный образ M. $u, v \in M$, $u \equiv v \Leftrightarrow h(u) = h(v)$ для любого гомоморфизма $h : M \to \mathcal{G}$. $\mathcal{G}$ - группа, порождённая A в которой ??? X.

   Надо доказать что $\equiv$ является конгруэнтностью

   (a) $a \equiv a$

   (b) $a \equiv b \Rightarrow b \equiv a$

   (c) $a \equiv b, b \equiv c \Rightarrow a \equiv c$

   Пусть $a \equiv b$, $c \equiv d$, то есть $h(a) = h(b)$, $h(c) = h(d)$, тогда, так как h является гомоморфизмом

   $$h(ac) = h(a)h(c) = h(b)h(d) = h(bd)$$

   следовательно $ac \equiv bd$ и $\equiv$ - конгруэнтность

   Пусть группа $F = {}^{M}/_{\equiv}$, $\widehat{a} \in F$, $a = u_1...u_n$, $b = u_n^{-1}...u_1^{-1}$, $a, b \in M$

   $h(a) = h(u_1)...h(u_n)$

   $h(b) = h(u_n^{-1})...h(u_1^{-1})$

   $h(ab) = h(u_1)...h(u_n)h(u_n^{-1})...h(u_1^{-1}) = e$

   $\widehat{a}\widehat{b} = \widehat{e}$

   F порождается A

2. Доказать $t(\overline{a}) = s(\overline{a}) \in X$

   $h(t(a_1, ..., a_n)) = t(h(a_1), ..., h(a_n)) = s(h(a_1), ..., h(a_n)) = h(s(a_1, ..., a_n))$
   $t(\overline{a}) \equiv s(\overline{a}) \Rightarrow \widehat{t(\overline{a})} = widehats(\overline{a}) \Rightarrow t(\widehat{a_1}, ..., \widehat{a_n}) = s(\widehat{a_1}, ..., \widehat{a_n}$

3. Из чего следует?

и WTF в общем □

Пример 1.5. *Про пирамиду рубика. Конём.*

Пример 1.6. *Дана "головоломка"*

1	2
3	4

Построить группу $\mathcal{G}$
a - перестановка двух столбцов
b - перестановка строк

e: $\begin{array}{|c|c|}\hline 1 & 2 \\ \hline 3 & 4 \\ \hline\end{array}$ a: $\begin{array}{|c|c|}\hline 2 & 3 \\ \hline 4 & 1 \\ \hline\end{array}$ b: $\begin{array}{|c|c|}\hline 3 & 4 \\ \hline 1 & 2 \\ \hline\end{array}$ ab: $\begin{array}{|c|c|}\hline 4 & 1 \\ \hline 2 & 3 \\ \hline\end{array}$

$a^2 = e,\ b^2 = e,\ ab = ba$

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ba	e	a
ab	ab	b	a	e

$\mathcal{G} = (\{e, a, b, ab\}, \circ)$

Пример 1.7. *Таблица 8x8. Конём.*

Пример 1.8. $Z = 1, -1$

Пример 1.9.

Пример 1.10.

Пример 1.11.

Пример 1.12.

Определение 1.7. Если $X = \emptyset$, то $^{M}/_{\equiv}$ - свободная группа порождённая A

Следствие 1.2. *Любая группа порождённая A - гомоморфный образ свободной группы*

Определение 1.8. $\mathcal{G}$ - группа, $S \neq \emptyset$. Действие группы $\mathcal{G}$ на S - это отображение $h : S \times \mathcal{G} \to S$ и

1. $h(S, e) = S$
2. $h(h(S, a), b) = h(S, ab)$

Эти два условия по другому:

1. $Se = S$
2. $(Sa)b = S(ab)$

Пример 1.13. *$\mathcal{G}$ действует на себя правыми умножениями*

Определение 1.9. Сопряжение - действие группы $\mathcal{G}$ на себя или множество подмножеств $P(\mathcal{G}) : h(S, a) = a^{-1}Sa$

Теорема 1.6. *Сопряжение - действие*

Доказательство. Проверим условия сопряжения

1. $e^{-1}Se = eSe = S$
2. $h(h(S, a)b) = h(a^{-1}Sa, b) = b^{-1}a^{-1}Sab = (ab)^{-1}Sab = h(S, ab)$
   $a^{-1}Aa = A \subseteq \mathcal{G}$

□

Теорема 1.7. *Любая подгруппа при сопряжении переходит в подгруппу*

Доказательство. Пусть A - подгруппа $\mathcal{G}$ □

Теорема 1.8. *Пусть A - подгруппа, то A неподвижна при всех сопряжениях тогда и только тогда когда A - нормальная подгруппа*

Доказательство.

- $\Rightarrow a^{-1}Aa = a \Rightarrow aa^{-1}Aa = aA \Rightarrow Aa = aA$
- $\Leftarrow Aa = aA \Rightarrow a^{-1}Aa = a^{-1}aA \Rightarrow a^{-1}Aa = A$

□

Определение 1.10 (Стабилизатор)**.** $\mathcal{G}$ действует на S, $s \in S$. Стабилизатор s - $\operatorname{stab} s = \{a \in \mathcal{G}, h(s, a) = s\}$

Теорема 1.9. $\operatorname{stab} s$ *- подгруппа $\mathcal{G}$*

Доказательство. пусть $b, c \in \operatorname{stab} s$, тогда □

Определение 1.11 (Орбита)**.** Пусть G действует на S, $s \in S$. Орбита s - $\operatorname{orb} s = \{sa : a \in G\}$

Теорема 1.10. *Орбиты - классы эквивалентности*

Теорема 1.11. *Количество элементов орбиты равняется индексу стабилизатора*

Теорема 1.12 (Формула орбит)**.** *G действует на множестве S, тогда* $|S| = \sum\limits_{\text{орбиты}} \dfrac{\operatorname{ord} G}{\operatorname{ord} q_0}$

Следствие 1.3. *Если $\operatorname{ord} G = p^k$, p - простое, то $Z \neq \{e\}$*