Алгебра 6

Igor Engel

1

Теорема 1.1.

$$\forall g \in G \quad \exists! f : \mathbb{Z} \mapsto G \quad f(1) = g.$$

f - гомомоморфизм

Доказательство. Докажем единственность:

$$f(0) = 0.$$

$$f(1) = g.$$

$$f(2) = f(1+1) = g^2.$$

$$f(n-1) = g^{n-1}.$$

Существование теперь тривиально □

Теорема 1.2.

$$\forall g \in G \quad \exists! f : \mathbb{Z}/\operatorname{ord} g \mapsto \langle g \rangle.$$

Определение 1.1.

$$X \subset G.$$

Если $G = \langle X \rangle$, то X порождает G. X - порождающее множество G.
Если X кончно, то его элементы порождают G.
Если $|X| = 1$, то G - циклическая группа.

Лемма 1.1.1.

$$H \subset \mathbb{Z}.$$

H - циклическая.

Доказательство. Если $H = \{0\}$ утверждение тривиально.

$$\exists n \in \mathbb{Z} \quad H = n\mathbb{Z}.$$

Подобное утверждение было доказанно ранее. □

Лемма 1.1.2.
$$g^n = e.$$
$$n \vdots (\operatorname{ord} g = m).$$

Доказательство.
$$\begin{aligned} &g^n = e \\ &\iff g^{mq+r} = e \\ &\iff g^{mq} g^r = e \\ &\iff (g^m)^q g^r = e \\ &\iff e g^r = e \\ &\iff g^r = e \\ &\iff r = 0 \\ &\iff n \vdots m \end{aligned}$$
□

2 Смежные классы и Теорема Лагранжа

Определение 2.1. Заведём отношение $\sim_H$: $g_1 \sim_H g_2 \iff \exists h \in H \quad g_1 = g_2 h$.

Теорема 2.1. $\sim_H$ - отношение эквивалентности

Доказательство. Рефелексивность: $e \in H \implies g_1 = g_1 e$
Симметричность: $h^{-1} \in H \implies g_2 = g_1 h^{-1}$ Транзитивность:
$$g_1 = g_2 h_1$$
$$g_2 = g_3 h_2.$$
$$g_1 = g_2 h_2 h_1.$$
□

Рассмотрим классы эквивалентности:

Определение 2.2.
$$gH = \{gh \mid h \in H\}.$$
gH - левый смежный класс элемента g относительно H.
$$G = \bigsqcup_{g \in G} gH.$$

Лемма 2.2.1.
$$f : H \mapsto gH.$$
$$f(h) = gh.$$
f - биекция.

Доказательство. Построим обратное отображение:

$$F(gh) = g^{-1}gh = h.$$

$\square$

Определение 2.3. Множество всех левых смежных классов: G/H.

Определение 2.4. G - группа. $|G|$ - порядок G, это количество элементов в ней. $|G/H| = [G : H]$ - индекс H внутри G.

Теорема 2.2 (Теорема Лагранжа)**.** H - подгруппа G.
$|H|$ конечен
$[G : H]$ конечен.

$$|G| = [G : H]\,|H|.$$

Доказательство. G разбивается на классы смежности, которых $[G : H]$.
Так-как из H в gH есть биекция, $|H| = |gH|$.

$\square$

Лемма 2.2.1.

$$|G| \,\vdots\, |H|.$$

Лемма 2.2.2.

$$\forall g \in G \quad |G| \,\vdots\, \operatorname{ord} g.$$

Доказательство.

$$\operatorname{ord} g = |\,\langle g \rangle\,|.$$

$\langle g \rangle$ - подгруппа. $\square$

Лемма 2.2.3.

$$|G| = n \implies g^n = e.$$

Доказательство.

$$n \,\vdots\, \operatorname{ord} g \implies g^n = (g^{\operatorname{ord} g})^{\frac{n}{\operatorname{ord} g}} = e.$$

$\square$

Лемма 2.2.4 (Теорема Эйлера)**.**

$$G = (\mathbb{Z}/n)^*\,.$$

$$a \in (G)\,.$$

$$\varphi(n) = |G|.$$

$$a^{\varphi(n)} = 1.$$

Определение 2.5. $\varphi(n)$ - функция Эйлера.

Лемма 2.5.1. p - простое.
$\varphi(p) = p - 1$.

Доказательство. Все элементы в $\mathbb{Z}/p$ кроме нуля обратимы. $\square$

Лемма 2.5.2. p - простое.
$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Лемма 2.5.3. Пусть $n = \prod\limits_{i=1}^{\infty} p_i^{\alpha_i}$
$\varphi(n) = \prod\limits_{i=1}^{\infty} \varphi(p_i^{\alpha_i}) = \prod\limits_{i=1}^{\infty} p_i^{\alpha_i} - p_i^{\alpha_i - 1} = n \prod\limits_{i=1}^{\infty} (1 - \frac{1}{p})$

Теорема 2.3 (Малая теорема Ферма)**.**

$$a^{p-1} \equiv 0 \mod p.$$

Доказательство. Если $a \equiv 0 \mod p$ утверждение тривиально.
$\varphi(p) = p - 1$, значит утверждение следует из теоремы Эйлера. $\square$

Теорема 2.4. Пусть $|G| = p$.
Тогда G - циклическая.

Доказательство. У G не может быть собственных подгрупп, значит, любой элемент кроме нейтрального порождает всю группу. $\square$