Алгебра 11

Igor Engel

1

Теорема 1.1. Пусть $p \in \mathbb{P}$, G - группа, $|G| \vdots p$.
Тогда $\exists x \in G \quad \operatorname{ord} x = p$.

Доказательство. Пусть $X = G^p$.
$Y = \{(a_0, \dots, a_{p-1}) \in X \mid a_0 \dots a_{p-1} = e\}$.
Ввердём действие $\mathbb{Z}/p \curvearrowright Y$.

$$k(a_0, \dots, a_{p-1}) \to (a_k, \dots, a_{i+k} \mod p, a_{k-1}.$$

Сопряжением с элементом a_0 можно показать, что тождество сохраняется
Рассмотрим множество неподвижных точек при $k = 1$:
Это $(a_0, a_0, \dots, a_0)$. По условию в Y, получаем что $a_0^p = e$.
Тогда существует два случая: $a_0 = e$, или $\operatorname{ord} a_0 = p$.
Покажем что точки второго типа существуют, посчитаем количетсво элементов:
Заметим, что последний элемент любого элемента Y определяется однозначно через предыдущие. Тогда

$$|Y| = n^{p-1} \vdots p.$$

Разобьём Y на орбиты:

$$|Y| = \sum_x |O_x|.$$

$|O_x|$ может быть либо 1, либо p, поэтому $|Y| = r + kp$, так-как $|Y| \vdots$, то $r = k'p$, $k' \neq 0$, так-как $|O_e| = 1$, значит существует хотя-бы одна нетривиальная неподвижная точка. $\square$

Определение 1.1. X - множество, G - группа, $G \curvearrowright X$.
Тогда X/G - множество всех орбит.

Определение 1.2. Множество неподвижных точек элемента g:

$$\operatorname{Fix} g = \{x \in X \mid gx = x\}.$$

Лемма 1.2.1 (Лемма (Не) Бернсайда)**.** G - конечная группа, X - конечное множество, $G \curvearrowright X$.
Тогда:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix} g|.$$

Доказательство. Рассмотрим множество $Y = \{\langle g, x\rangle \in G \times X \mid gx = x\}$.

$$|Y| = \sum_{g\in G} |\operatorname{Fix} g|.$$

$$|Y| = \sum_{x\in X} |\operatorname{Stab} x| = \sum_{x\in X} \frac{|G|}{|O_x|} = |G| \sum_{x\in X} \frac{1}{|O_x|} = |G| \sum_{O\in X/G} \sum_{x\in O} \frac{1}{|O|} = |G||X/G|.$$

$$|Y| = \sum_{g\in G} |\operatorname{Fix} g| = |G||X/G| \implies |X/G| = \frac{1}{|G|} \sum_{g\in G} |\operatorname{Fix} g|.$$ □

2 Теория Колец

Определение 2.1. R - кольцо, $a \in R$ называется делителем нуля, если $\exists b \neq 0 \in R \quad ab = 0$.
$a \in R$ называется нильпотентным, если $\exists n \in \mathbb{N} \quad a^n = 0$.

Лемма 2.1.1. В R нет нетривиальных делителей нуля тогда и только тогда, когда $\forall c \neq 0 \quad \forall a, b \quad ac = bc \implies a = b$.

Доказательство.

$$ac = bc \implies ac - bc = 0 \implies (a-b)c = 0.$$

.
Если делителей нуля нет, то $a - b = 0 \implies a = b$.
Если $a - b \neq 0$, но утверждение выполнено, то $c = 0$. □

Определение 2.2. Кольцо R называется областью целостности, если в нём нет нетривиальных делителей нуля.

Определение 2.3. Пусть $a, b \in R$, тогда

$$a \,\vdots\, b \iff \exists c \in R \quad a = bc.$$

Определение 2.4. Пусть $a, b \in R$, тогда a ассоциированно с b ($a \sim b$), если $a \,\vdots\, b$ и $b \,\vdots\, a$.

Лемма 2.4.1. Пусть $a, b \in R$, тогда следующие утверждения эквивалентны:

1. $a \sim b$
2. $\exists \varepsilon \in R^* \quad a = \varepsilon b$

Доказательство. $2 \implies 1$: $a = \varepsilon b$, $b = \varepsilon^{-1} a$.
$1 \implies 2$: $a = bc_1$, $b = ac_2$, $a = ac_2c_1$, тогда либо $a = 0$, либо $c_1 = c_2^{-1}$. □

Лемма 2.4.2. Ассоциированность - отношение эквивалентности на R

Доказательство. Рефлексивность и симметричность очевидны.
$a \vdots b$, $b \vdots a$, $b \vdots c$, $c \vdots b$.
Из 1 и 3 следует $a \vdots c$, из 2 и 4 - $c \vdots a$. $\square$

Определение 2.5. $d \in R$ называется наибольшим общим делителем a и b, и обозначается (a, b), если $a \vdots d$, $b \vdots d$ и

$$\forall d' \in R \quad \begin{cases} a \vdots d' \\ b \vdots d' \end{cases} \implies d \vdots d'.$$

Лемма 2.5.1. Пусть $a, b \in R$, Если существет (a, b), то он определён однозначно с точностью до ассоциированности.

Доказательство. Пусть d, d' - два простых делителя. Тогда $d \vdots d'$ и $d' \vdots d$. $\square$

Определение 2.6. Элемент $p \in R$ называется простым, если $p \notin R^*$, $p \neq 0$ и

$$ab \vdots p \implies \left[\begin{array}{l} a \vdots p \\ b \vdots p \end{array}\right..$$

Определение 2.7. Элемент $p \in R$ называется неприводимым, если $p \notin R^*$, $p \neq 0$ и

$$p = ab \implies \left[\begin{array}{l} a \sim p \\ b \sim p \end{array}\right..$$

Лемма 2.7.1. Если $p \in R$ простой, то он неприводимый.

Доказательство. Предположим что $p = ab$.
Заметим, что $ab \vdots p$, значит либо a либо b делится на p. Предположим что $a \vdots p$.
Так-же $p \vdots a$, а значит $a \sim p$ $\square$

Определение 2.8. R - кольцо. $R[x]$ - кольцо многочленов над R.
$f \in R[x]$, степень многочлена $\deg f$ - индекс последнего ненулевого элемента. Старший коэффициент - последний ненулевой элемент.
$\deg 0 = -\infty$

Лемма 2.8.1.

$$\deg fg \leq \deg f + \deg g.$$

Если R - область целостности, то $\deg fg = \deg f + \deg g$.

Лемма 2.8.2. Пусть $\deg f = n$, $\deg g = m$.
Тогда $fg[n + m] = f[n]g[m]$.
Если $f[n]$ и $f[m]$ - не делители нуля, то $\deg fg = \deg f + \deg g$.

Лемма 2.8.3. Если R - область целостности, то $R[x]$ - тоже область целостности.

Лемма 2.8.4. R - область целостности, тогда $(R[x])^* = R^*$.