Лекция 24 сентября 2020

Кольца вычетов $\mathbb{Z}/(n)$

класс $[k]$ обратим в $\mathbb{Z}/(n) \Leftrightarrow$ НОД$(k,n)=1$

⇙

$1 = kx + ny$ с целыми x, y

$[1] = [k][x]$ в $\mathbb{Z}/(n)$

Все ненулевые элементы в $\mathbb{Z}/(n)$ обратимы $\Leftrightarrow$ $n = p$ - простое число.

$\forall p$-простого $\mathbb{Z}/(p)$ - поле.

$$\underbrace{1+1+\ldots+1}_{p} = [p] = 0$$

в $\mathbb{Z}/(p)$ напишем формулу бинома:

$$(a+b)^p = \sum_{k=0}^{p} a^k b^{p-k} \cdot \binom{p}{k}$$

сумма $\binom{p}{k}$ единиц поля $\mathbb{Z}/(p)$

=

$$\left[\begin{array}{l} \dfrac{p!}{k!(p-k)!} \text{ при } k \neq 0, p \\ \text{делится на } p. \end{array}\right.$$

p взаимно просто с $1, 2, \ldots, p-1 \Rightarrow$

p взаимно просто с $k!(p-k)!$

$$\underset{\Rightarrow}{p}\cdot\underbrace{(p-1)\cdot\ldots\cdot 1}\ \vdots\ k!(p-k)! \Rightarrow$$

$$(p-1)\cdot\ldots\cdot 1\ \vdots\ k!(p-k)!$$

класс $\binom{p}{k}$ в $\mathbb{Z}/(p)$ нулевой при $k \neq 0, p$.

В поле $\mathbb{F}_p \cong \mathbb{Z}/(p)$ бином раскрывается по формуле $(a+b)^p = a^p + b^p$

Следствие (малая теорема Ферма):

$$[a]^p = (\underbrace{[1]+\ldots+[1]}_{a\text{ раз}})^p = \underbrace{[1]^p+\ldots+[1]^p}_{a\text{ раз}} = [a]$$

$$\forall a \in \mathbb{Z} \quad a^p \equiv a \pmod p.$$

Определение: Пусть A и B — абелевы группы (с операцией $+$). Отображение $\varphi: A \to B$ называется гомоморфизмом, если $\varphi(a_1+a_2) = \varphi(a_1)+\varphi(a_2)$ $\forall a_1, a_2 \in A$

Формальные следствия определения:

(1) $\varphi(0) = 0$, т.к. $\varphi(0) = \varphi(0+0) = \varphi(0)+\varphi(0)$

$\downarrow \quad -\varphi(0)$

$$0 = \varphi(0)$$

(2) $\varphi(-a) = -\varphi(a)$, т.к. $\underline{\varphi(a)} + \underline{\varphi(-a)} =$
$= \varphi(a-a) = \varphi(0) = 0$

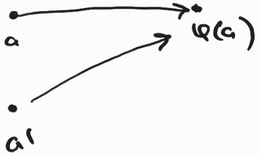
Образ $\operatorname{im}\varphi = \varphi(A) \subset B$ это подгруппа.

Факт: каждый непустой слой любого гомоморфизма абелевых групп находится в биекции со слоем над $\underline{\underline{0}}$

$$A \xrightarrow{\varphi} B$$

Слой над нулём $\ker\varphi = \varphi^{-1}(0) = \{a \in A \mid \varphi(a) = 0\}$ называется ядром

Факт: $\varphi^{-1}(\varphi(a)) = a + \ker\varphi =$
$= \{a + x \mid \varphi(x) = 0\}$



$$\varphi(a) = \varphi(a')$$
$$\Updownarrow$$
$$\varphi(a - a') = 0$$
$$\Updownarrow$$
$$a - a' \in \ker\varphi$$

т.е. $a' \in \underline{\underline{a + \ker\varphi}}$

Следствие: гомоморфизм инъективен $\Leftrightarrow$ $\ker\varphi = \{0\}$.

Пусть A и B – кольца. Отображение $\varphi: A \to B$ называется **гомоморфизмом колец**, если $\varphi(a_1+a_1) = \varphi(a_1)+\varphi(a_2)$

$$\varphi(a_1 a_2) = \varphi(a_1)\cdot\varphi(a_2)$$

φ обладает всеми свойствами гомомор. абелевых групп.

Предупреждение: Вообще говоря

$\varphi(1) \neq 1$: $\mathbb{Z}/(2) \to \mathbb{Z}/(6)$

$$[1] \longmapsto [3]$$

$$[1]+[1]=0 \longrightarrow [3]+[3]=0$$

$$[1]\cdot[1]=[1] \longrightarrow [3]\cdot[3]=[3]$$

Факт: Если кольцо B **целостное** (т.е. в B нет делителей нуля, кроме нуля), то $\varphi(1)=1$ $\forall$ ненулевого гомоморфизма $A \xrightarrow{\varphi} B$

Док-во:

$$\varphi(1) = \varphi(1\cdot 1) = \varphi(1)\varphi(1)$$

$$\varphi(1) - \varphi(1)\varphi(1) = 0$$

$$\varphi(1)(1-\varphi(1)) = 0$$

либо $\varphi(1)=0 \Rightarrow \varphi\equiv 0$, т.к. $\varphi(a)=\varphi(a\cdot 1)=\varphi(a)\varphi(1)=0$

$\boxed{\text{либо } \varphi(1)=1}$

$\varphi\equiv 0 \Leftrightarrow \varphi(1)=0$

Факт: Если $\mathbb{K}$ - поле, то любой ненулевой гомоморфизм $\mathbb{K}\xrightarrow{\varphi}B$ инъективен.

Док-во: Если φ не инъективен, то $\ker\varphi\neq 0 \Rightarrow \exists\, a\neq 0 : \varphi(a)=0$

$$\forall b \quad \varphi(b)=\varphi(a\cdot a^{-1}b)=\varphi(a)\varphi(a^{-1}b)=0$$

Важный пример: Пусть $\mathbb{K}$ - любое поле. $\xi: \mathbb{Z}\longrightarrow\mathbb{K}$

$$1\longmapsto 1$$

$$n\longmapsto \pm\underbrace{(1+\dots+1)}_{|n|}$$

$+$ если $n>0$

$-$ если $n<0$

1 случай: $\ker\xi\neq 0\ \exists n\in\mathbb{N}: \underbrace{1+\dots+1}_{n}=0$ в $\mathbb{K}$

Наименьшее такое n простое!

$$\underbrace{1+\dots+1}_{km}=\underbrace{(1+\dots+1)}_{k}\underbrace{(1+\dots+1)}_{m}$$

Оно называется характеристикой поля $\mathbb{K}$: $\operatorname{char}\mathbb{K}$

Для таких $\mathbb{K}$ гомоморфизм g пропускается через $\mathbb{Z}/(p)$

$$\begin{tikzcd} z \arrow[d] & \mathbb{Z} \arrow[r, "g"] \arrow[d, two heads] & \mathbb{K} & \\ {[z]} & \mathbb{Z}/(p) \arrow[ur] & {[z]} \arrow[r] & g(z) \end{tikzcd}$$

корректно определено

$$[z_1]=[z_2] \Rightarrow g(z_1)=g(z_2)$$

$$z_2=z_1+p\cdot m \qquad g(z_2)=g(z_1)+\underbrace{g(p)}_{0}g(m)$$

Образ g – это поле изоморфное $\mathbb{Z}/(p)$.

простое подполе в $\mathbb{K}$ = наименьшее по включению подполе в $\mathbb{K}$.

||

всё что можно получить из $1 \in \mathbb{K}$ при помощи сложений, вычитаний, умножений и делений.

В любом поле характеристики p отображение $F_p : x \longmapsto x^p$ является гомоморфизмом.

$$(x_1x_2)^p = x_1^p x_2^p$$

$$(x_1+x_2)^p = x_1^p + x_2^p$$

Гомоморфизм Фробениуса

$\Uparrow$

$\underbrace{1+\dots+1}_{\binom{p}{k}} = 0$ при $k \neq 0, p$.

Любой ненулевой гомоморфизм поля в себя тождественно действует на простом подполе: $\pm\frac{1+\dots+1}{1+\dots+1}$

$$\varphi\left(\pm\frac{1+\dots+1}{1+\dots+1}\right) = \pm\frac{1+\dots+1}{1+\dots+1}$$

т.к. $\varphi(1) = 1$.

---

2 случай: $\forall n \in \mathbb{Z} \quad \underbrace{1+\dots+1}_{n} \neq 0$

$\boxed{\ker \xi = 0}$

$$\xi : \mathbb{Z} \to \mathbb{K}$$
$$n \mapsto \underbrace{1+\dots+1}_{n}$$

ξ – вложение и продолжается до вложения $\xi : \mathbb{Q} \to K$

$$\frac{m}{n} \longmapsto \frac{\xi(m)}{\underset{\neq 0}{\xi(n)}}$$

простое подполе в K изоморфно $\mathbb{Q}$ и совпадает с $\operatorname{im} \xi$.

Говорят, что $\operatorname{char} \mathbb{K} = 0$

K - поле характеристики 0.