Лекция 22, 28.02.24

Опр: $\varphi: K_1 \to K_2$ – гомоморфизм

$\operatorname{Ker}\varphi = \{r \in K_1 \mid \varphi(r) = 0\} \subseteq K_1$ – ядро

$\operatorname{Im}\varphi = \{\varphi(r) \mid r \in K_1\} \subseteq K_2$ – образ.

Лемма 1: $\operatorname{Ker}\varphi$ – всегда идеал в K_1, где $\varphi: K_1 \to K_2$ – гом-зм колец.

□ φ – гом-зм колец $\Rightarrow$ φ – гом-зм групп $(K_1, +)$ и $(K_2, +)$ $\Rightarrow$

$\Rightarrow$ $\operatorname{Ker}\varphi$ – подгруппа в $(K_1, +)$ – доказано ранее.

Покажем, что $\forall a \in \operatorname{Ker}\varphi$ $\forall r \in K_1$ ar и $ra \in \operatorname{Ker}\varphi$.

$$\left.\begin{aligned} \varphi(ar) &= \varphi(a)\cdot\varphi(r) = 0\cdot\varphi(r) = 0 \\ \varphi(ra) &= \varphi(r)\cdot\varphi(a) = \varphi(r)\cdot 0 = 0 \end{aligned}\right\} \Rightarrow ar \text{ и } ra \in \operatorname{Ker}\varphi$$

$\Rightarrow$ по опр. $\operatorname{Ker}\varphi$ явл. идеалом ■

Лемма 2. $\operatorname{Im}\varphi$ – подкольцо в K_2

□ Если $a, b \in \operatorname{Im}\varphi$, то $\exists a', b' \in K_1$: $\varphi(a') = a$, $\varphi(b') = b$

$\Rightarrow$ 1) $a - b = \varphi(a') - \varphi(b') = \varphi(a' - b')$ ($\operatorname{Im}\varphi$ – подгруппа по слож.)

2) $a\cdot b = \varphi(a')\cdot\varphi(b') = \varphi(a'\cdot b')$ ($\operatorname{Im}\varphi$ – замкн. по умн.) $\Rightarrow ab \in \operatorname{Im}\varphi$

$\Rightarrow$ по критерию подкольца $\operatorname{Im}\varphi$ явл. подкольцом в K_2. ■

Теорема о гом-зме колец:

Пусть $\varphi: K_1 \to K_2$ – гом-зм колец.

Тогда $K_1/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

□ Обозначим $\operatorname{Ker}\varphi = I$ - идеал по лемме 1 $\Rightarrow$

$\Rightarrow$ факторкольцо K_1/I - задано корректно.

$\operatorname{Im}\varphi$ - подкольцо в K_2 по лемме 2.

Рассмотрим отображение колец: $\tau : K_1/I \to \operatorname{Im}\varphi$, где $\tau(a+I) = \varphi(a)$

Из док-ва теоремы о гом-зме групп τ - изоморфизм групп по сложению $(K_1/I, +)$ и $(\operatorname{Im}\varphi, +)$. (т.к. τ корректно задано, является гомоморфизмом и биективно).

Осталось проверить, что τ „уважает" умножение.

$$\tau((a+I)(b+I)) \overset{\text{по опр. умн. см.кл.}}{=} \tau(a\cdot b + I) \overset{\text{по опр } \tau}{=} \varphi(ab) = \varphi(a)\cdot\varphi(b) = \tau(a+I)\cdot\tau(b+I)$$

Таким образом, τ уважает слож. и умн. и биективно $\Rightarrow$

$\Rightarrow \tau$ - изоморфизм колец $\Rightarrow K_1/\operatorname{Ker}\varphi \overset{\tau}{\cong} \operatorname{Im}\varphi$ ■

Поле, характеристика поля

Опр: Пусть P - поле. Тогда его <u>характеристикой</u> $\operatorname{char} P$ наз-ся наименьшее натуральное число q, такое что $\underbrace{1 + \ldots + 1}_{q \text{ раз}} = 0$.

Если такого $q \in \mathbb{N}$ не существует, то полагают $\operatorname{char} P = 0$.

Пример: $\operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = \operatorname{char} \mathbb{Q} = 0$.

$\mathbb{Z}_p$ - кольцо вычетов по простому модулю p.

Оно явл. полем. $\operatorname{char} \mathbb{Z}_p = p$.

Утв: $\mathbb{Z}_p$ (кольцо вычетов по $\operatorname{mod} p$) явл. полем $\Leftrightarrow$ p - простое число.

□ „⇐" Дано: p - простое. Док-ть: $\mathbb{Z}_p$ - поле.

$\mathbb{Z}_p$ - коммут. кольцо с единицей.

Достаточно показать, что $\forall a \in \mathbb{Z}_p,\ a \neq 0$ $\exists$ обрат. по умножению.

Если p - простое, то числа $1, 2, \ldots, p-1$ вз. просты с p.

$\Rightarrow \forall a \in \mathbb{Z}_p,\ a \neq 0 \quad НОД(a, p) = 1.$

$\Rightarrow$ по следствию из алгоритма Евклида для $\mathbb{N}$:

$\exists u, v \in \mathbb{N}: \quad a \cdot u + \underbrace{p \cdot v}_{\equiv 0 \bmod p} = 1 \Rightarrow a \cdot u \equiv 1 \bmod p \Rightarrow \bar{a} \cdot \bar{u} = \bar{1}$ для

классов вычетов $\Rightarrow \bar{u}$ - обратный к $\bar{a}$ в $\mathbb{Z}_p$, т.е. он $\exists$ ег.

„⇒" Дано: $\mathbb{Z}_p$ - поле. Док-ть: p - простое.

ПП: $p = l \cdot k$ - составное число $(1 < l, k < p)$.

$\Rightarrow \bar{l} \cdot \bar{k} = \bar{p} = \bar{0}$ для классов вычетов $\Rightarrow \bar{l}$ и $\bar{k}$ - делители 0

$\Rightarrow$ они не обратимы (т.к. если $\exists\, l^{-1}$: $\underbrace{l^{-1} \cdot l}_{1} \cdot k = 1 \cdot k = k = l^{-1} \cdot 0 = 0$

$\Rightarrow k = 0$ и l - не делитель 0) $\Rightarrow$ противоречие с опр. поля. ∎

Замечание: $\forall$ поле характеристики 0 бесконечно.

□ $1,\ 1+1,\ \ldots,\ \underbrace{1 + \ldots + 1}_{k \text{ раз}},\ \ldots$ - это все различные числа, т.к.

если $\underbrace{1 + \ldots + 1}_{k} = \underbrace{1 + \ldots + 1}_{l}$, $k < l \Rightarrow \underbrace{1 + \ldots + 1}_{l-k>0} = 0 \Rightarrow \operatorname{char} > 0$

$\Rightarrow$ противоречие $\Rightarrow$ мы имеем как минимум счётное

число элементов. ∎

Утв:

$$\operatorname{char} P = \begin{cases} 0 \\ p - \text{простое число} \end{cases}$$

(характеристика поля либо 0, либо простое число).

□ Док: Предположим, что $\operatorname{char} P = m \cdot k = p \neq 0$, где $1 < m, k < p$, $m, k \in \mathbb{N}$

$0 = \underbrace{1 + \ldots + 1}_{p \text{ раз}} \overset{\text{дистриб.}}{=} \underbrace{(1 + \ldots + 1)}_{m \text{ раз}} \underbrace{(1 + \ldots + 1)}_{k \text{ раз}}$, но $\operatorname{char} P = p$ – минимальное число раз, которое нужно сложить 1 с собой, чтобы получить 0 $\Rightarrow \underbrace{1 + \ldots + 1}_{m} \neq 0$ и $\underbrace{1 + \ldots + 1}_{k} \neq 0 \Rightarrow$

$\Rightarrow$ есть делители 0 $\Rightarrow$ они необратимы $\Rightarrow$ W с опр. поля ■

Замечание: Пересечение двух подполей одного и того же поля снова явл. подполем.

Опр: В $\forall$ поле $\exists$ет наименьшее по вложению подполе. Оно наз. простым подполем.

Утв: Пусть P – поле, P_0 – его простое подполе.

Тогда 1) Если $\operatorname{char} P = p > 0$, то $P_0 \cong \mathbb{Z}_p$

2) Если $\operatorname{char} P = 0$, то $P_0 \cong \mathbb{Q}$.

□ Рассмотрим цикл. группу по сложению, порождённую „единицей" (нейтр. элементом по умножению)

$\langle 1 \rangle \subseteq (P, +)$ – адд. группа поля

т.е. это эл-ты вида $\underbrace{1 + 1 + \ldots + 1}_{k}$, либо $\underbrace{(-1) + \ldots + (-1)}_{l}$

Заметим, что $\langle 1 \rangle$ подкольцо (замкнуто по умножению по дистриб.)

И т.к. $\forall$ подполя в P содержит 1, то $\langle 1 \rangle \subseteq P_0$

1) $\operatorname{char} P = p > 0 \Rightarrow \langle 1 \rangle \cong \mathbb{Z}_p$ (т.к. $\operatorname{ord}(1) = p$)

(т.к. все цикл. группы одного порядка изоморфны)

$\Rightarrow \langle 1 \rangle \cong \mathbb{Z}_p \subseteq P_0$, но P_0 - наименьшее подполе, и $\mathbb{Z}_p$ явл. полем (по утв.)

$\Rightarrow \mathbb{Z}_p \cong P_0$

2) $\operatorname{char} P = 0 \Rightarrow \langle 1 \rangle \cong \mathbb{Z}$ ($\langle 1 \rangle \subseteq P_0$)

Но в поле должны быть и обратные по умножению, и все возможные произведения элементов, т.е. эл-ты вида $a \cdot b^{-1} = \frac{a}{b}$, где $a, b \in \mathbb{Z}$, $b \neq 0$ ($a, b \in \langle 1 \rangle$)

$\Rightarrow$ это мн-во $\cong \mathbb{Q}$ (т.к. есть все рац. числа)

$\mathbb{Q}$ - это минимальное подполе, т.к. оно порождено только „1"

$\Rightarrow P_0 \cong \mathbb{Q}$ ■

Опр: Если P_1 - подполе в P_2, то говорят, что P_2 - это <u>расширение поля</u> P_1.

Пример: 1) $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ (вещ. числа - расш. рац., компл. - расш. вещ.)

2) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ - поле

Замечание: $\forall$ поле явл. расширением своего простого подполя (и характеристика у них одинаковая).

Опр. Эл-т $\alpha \in P_2$ наз. <u>алгебраическим эл-том</u> над полем P_1, где P_2 - расш. P_1, если $\exists f(x) \not\equiv 0$ $f(x) \in P_1[x]$, такой что $f(\alpha) = 0$. $f(x)$ - многочлен с коэф. из P_1.

Пример: 1) $P_1 = \mathbb{Q}$, $P_2 = \mathbb{R}$

$f(x) = x^2 - 2 \in \mathbb{Q}[x] \Rightarrow \alpha = \sqrt{2}$ - алгебраическое над $\mathbb{Q}$ ($\sqrt{2} \in \mathbb{Q} = P_1$)

2) $P_1 = \mathbb{R}$, $P_2 = \mathbb{C}$

$f(x) = x^2 + 1 \in \mathbb{R}[x] \Rightarrow i \in \mathbb{C}$ - алгебраическое число над $\mathbb{R}$

Опр: Если такого мн-на не $\exists$ет, то число наз. трансцендентным.

Пример: π, e.