8 Лекция 29.04

Доказательство теоремы о гомоморфизме для колец. Проверим, что умножение сохраняется, то есть $\psi((a+I)(b+I)) = \psi(a+I)\psi(b+I)$.

$$\psi((a+I)(b+I)) = \psi(ab+I) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(a+I)\psi(b+I)$$

где $\varphi(ab) = \varphi(a)\varphi(b)$ выполняется из-за того, что φ — гомоморфизм. □

Пример. $R = F(M,S)$ (R — кольцо). Зафиксируем $m_0 \in M$. Определим $\varphi : R \to S, f \mapsto f(m_0)$. Этот гомоморфизм сюръективен, потому что можно выбрать любую функцию, т.ч. $\forall s \in S : f(m_0) = s$. $\ker\varphi = \{f \in R \mid f(m_0) = 0\} = I_{m_0}$. Тогда по теореме о гомоморфизме $\operatorname{Im}\varphi = S \cong F(M,S)/\ker\varphi = F(M,S)/I_{m_0}$.

Далее считаем, что R — не обязательно коммутативное кольцо.

Определение 50. *R простое, если в нем нет нетривиальных двусторонних идеалов.*

Факт 3. Любое поле является простым кольцом.

Определение 51. *Центр кольца R это $Z(R) = \{a \in R \mid \forall b \in R : ab = ba\}$.*

Теорема 11. *Пусть K — поле, $R = M_n(K)$. Тогда*

1. *$Z(M_n(K)) = \{\lambda E \mid \lambda \in K\}$.*
2. *R — простое кольцо.*

Доказательство. (1) очевидно. Для доказательства (2) нужно вспомнить, что

$$E_{ij}E_{kl} = \begin{cases} 0, \text{ если } j \neq k \\ E_{il}, \text{ иначе} \end{cases}$$

Пусть I — двусторонний идеал в R. Если он нулевой, то все доказано. Иначе $\exists X \in I, X \neq 0 : X = (x_{ij})$. Тогда $\exists k,l : x_{kl} \neq 0$. Будем унможать X на матричные единицы. Рассмотрим $E_{ik}XE_{lj}$:

$$E_{ik}XE_{lj} = E_{ik}\left(\sum_{p,q=1}^{n} x_{pq}E_{pq}\right)E_{lj} = E_{ik}\left(\sum_{p=1}^{n} x_{pl}E_{pj}\right) = x_{kl}E_{ij} \in I$$

Умножим $x_{kl}E_{ij}$ на $x_{kl}^{-1}E$. Тогда $\forall i,j : E_{ij} \in I$. Получаем, что $\sum_{i,j} a_{ij}E_{ij}$, то есть произвольная матрица лежит в I, что и требовалось. □

Многочлены от многих переменных Пусть K — произвольное поле. Множество многочленов от n переменных $x_1 \dots, x_n$ обозначается как $K[x_1,\dots,x_n]$. Любая функция $f \in K[x_1,\dots,x_n]$ выражается как $\sum a_{i_1,\dots,i_n}x^{i_1}\dots x^{i_n}$ (сумма конечна), где $\forall j : i_j \geq 0$.

Определение 52. *$f(x_1,\dots,x_n)$ — симметрический, если $\forall \tau \in S_n : f(x_{\tau(1)},\dots,x_{\tau(n)}) = f(x_1,\dots,x_n)$.*

Пример. $f(x_1, \dots, x_4) = x_1x_2 + x_2x_3 + x_3x_4$ не является симметрическим, можно взять $\tau = (13)$. На наборе $f(1,0,0,1) = 0$, но $f(0,0,1,1) = 1$.

Пример (Степенные суммы)**.** Определим

$$s_k(x_1, \dots, x_n) = x_1^k + \dots + x_n^k \ (k \geq 0)$$

Пример (Элементарные симметрические многочлены)**.** Определим

$$\sigma_1 = x_1 + \dots + x_n$$

$$\sigma_k = \sum_{i_1 < \dots < i_k} x_{i_1} \dots x_{i_k}$$

$$\sigma_n = x_1 \dots x_n$$

Пример (Определитель Вандермонда)**.**

$$V(x_1, \dots, x_n) = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ x_1^2 & x_2^2 & \dots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{pmatrix} = \prod_{i<j} (x_j - x_i)$$

Если возвести в квадрат, то получим симметрический многочлен $V^2(x_1, \dots, x_n)$.

Теперь наша цель — описать все симметрические многочлены.

Факт 4. Сумма и произведение симметрических многочленов — симметричны. Как следствие, $f_1(x_1, \dots, x_n)$, $\dots$, $f_k(x_1, \dots, x_n)$ — симметрические, а $F(y_1, \dots, y_k)$ — произвольный многочлен, то $F(f_1, \dots, f_k)$ — симметрический многочлен.

Теорема 12 (Основная теорема о симметрических многочленах)**.** *Для произвольного симметрического многочлена $f(x_1, \dots, x_n)$ существует единственный многочлен $F(y_1, \dots, y_n) : f = F(\sigma_1, \dots, \sigma_n)$.*

Пример. Возьмем $s_2 = x_1^2 + \dots + x_n^2 = (x_1 + \dots + x_n)^2 - 2\sigma_2 = \sigma_1^2 - 2\sigma_2$. Получаем, что $F(y_1, \dots, y_n) = y_1^2 - 2y_2$.

Доказательство. Введем на множестве одночленов лексикографический порядок. Скажем, что одночлен $\alpha x^{i_1} \dots x_n^{i_n} < \beta x^{j_1} \dots x_n^{j_n}$, если $\exists k, \forall m < k : i_m = j_m, i_k < j_k$.

Замечание 10. *1) Если $u < v$, $w \in \mathcal{M}_n$, то $uw < vw$.*

2) Если $u \leq v, v \leq w$, то $u \leq w$.

Определение 53. *Старшим членом $f(x_1, \dots, x_n)$ называется ненулевой член $f(x_1, \dots, x_n)$, который больше всех остальных ненулевых членов в лексикографическом порядке. Обозначается как $L(f)$ (от слова leading term).*

Лемма 9 (О старшем члене)**.** $L(fg) = L(f)L(g)$.

Доказательство леммы о старшем члене. Пусть u входит в f : $u \leq L(f)$. Аналогично v входит в g : $v \leq L(g)$. В fg все члены вида uv. Тогда $u \leq L(f), v \leq L(g) \Rightarrow uv \leq L(f)v \leq L(f)L(g)$. Также заметим, что равенство в обоих неравенствах возможно только если $u = L(f), v = L(g)$. Тогда $L(f)L(g)$ — старший член. □

□