Задачи по алгебраическим структурам (SE). 2

Далее следует напоминание необходимого для решения задач материала лекций.

• Пусть K — поле и $f \in K[x] \setminus \{0\}$; кольцо $K[x]/f$ есть кольцо остатков по модулю многочлена f; как множество это кольцо есть $\{b \in K[x] \mid \deg b < \deg f\}$, бинарные операции на нем суть сложение и умножение многочленов по модулю многочлена f. Имеют место следующие факты:

1. если $|K| < \infty$, то $|K[x]/f| = |K|^{\deg f}$ (это очевидно);

2. $\forall\, b \in K[x]/f \ \big(b \in (K[x]/f)^\times \Leftrightarrow \gcd(b, f) = 1\big)$ (данный факт мы принимаем без доказательства; аналогичный факт для колец $\mathbb{Z}/n$, где $n \in \mathbb{N}$, был доказан в лемме об обратимых остатках).

• Пусть K — поле и $f \in \mathrm{Irr}(K[x])$; тогда $(K[x]/f)^\times = (K[x]/f) \setminus \{0\}$ (это следует из второго факта) и, значит, $K[x]/f$ — поле (этот факт аналогичен тому, что если $p \in \mathbb{P}$, то $\mathbb{Z}/p$ — поле). Примеры:

$\mathbb{F}_2[x]/(x^2 + x + 1) = \{0, 1, x, x + 1\}$ — поле порядка 4;

$\mathbb{F}_2[x]/(x^3 + x + 1) = \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$ — поле порядка 8;

$\mathbb{F}_3[x]/(x^2 + 1) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$ — поле порядка 9.

• На лекции шла речь о следующей лемме.

Пусть K — поле и $f \in K[x]$; тогда

1. $\forall\, c \in K \ \big(f(c) = 0 \Leftrightarrow$ (многочлен $x - c$ делит многочлен f)$\big)$;

2. $f \neq 0 \Rightarrow |\{c \in K \mid f(c) = 0\}| \leq \deg f$.

• Пусть K — поле, $f \in K[x]$ и $\deg f \in \{2, 3\}$; тогда $f \in \mathrm{Irr}(K[x])$, если и только если $\forall\, c \in K \ (f(c) \neq 0)$ (это следует из пункта 1 леммы). Данный факт нужно использовать в решении задачи 16.

Задачи

(**2**) 12. Обозначим через G группу $(\mathbb{F}_3[x]/(x^2 + 1))^\times$.

а) Проверьте явно, что $G \cong \mathrm{C}_8$. б) Перечислите все подгруппы группы G.

(**2**) 13. Обозначим через G группу $(\mathbb{F}_2[x]/x^4)^\times$.

а) Перечислите все элементы группы G. б) Докажите, что $G \cong \mathrm{C}_2 \times \mathrm{C}_4$.

(**3**) 15. Пусть R — коммутативное кольцо, $p \in \mathbb{P}$ и $\underbrace{1 + 1 + \ldots + 1}_{p \text{ слагаемых}} = 0$ в кольце R (этими свойствами обладают, например, поле $\mathbb{F}_p$ и кольца $\mathbb{F}_p[x]/f$, где $f \in \mathbb{F}_p[x]$); докажите, что $\forall\, r, s \in R \ \big((r + s)^p = r^p + s^p\big)$.

(**3**) 16. Для любых $p \in \mathbb{P}$ и $n \in \mathbb{N}_0$ обозначим через $\mathrm{Irr}_{p,n}$ множество $\{f \in \mathrm{Irr}(\mathbb{F}_p[x]) \mid \deg f = n \wedge (\text{старший коэффициент многочлена } f) = 1\}^{(\star)}$. Пусть $p \in \mathbb{P}$; докажите, что $|\mathrm{Irr}_{p,2}| = \frac{p^2 - p}{2}$ и $|\mathrm{Irr}_{p,3}| = \frac{p^3 - p}{3}$.

(**4**) 17. а) Пусть G — группа; докажите, что следующие свойства эквивалентны:

• $\forall\, H \subseteq G \ \big((HH \subseteq H \wedge H \neq \varnothing) \Rightarrow H \leq G\big)$; • порядки всех элементов группы G конечны.

б) Пусть G — группа, $H \trianglelefteq G$ и порядки всех элементов группы H и группы G/H конечны; докажите, что порядки всех элементов группы G конечны.

Указания к задачам

12. а) Укажите какой-либо порождающий элемент группы G.

б) Используйте пункт а и первую теорему о подгруппах циклической группы.

13. а) Используйте то, что если K — поле, $f \in K[x] \setminus \{0\}$, то $\forall\, b \in K[x]/f \ \big(b \in (K[x]/f)^\times \Leftrightarrow \gcd(b, f) = 1\big)$.

б) Укажите такие подгруппы F и H группы G, что $F \cong \mathrm{C}_2$, $H \cong \mathrm{C}_4$ и подгруппы F и H удовлетворяют условиям теоремы о прямом произведении, а затем используйте эту теорему.

15. Сначала докажите, что формула бинома Ньютона верна в любом коммутативном кольце.

17. Это задача по теории групп (она не связана с кольцами); для того, чтобы ее решить, нужно понимать, что такое подгруппа, порядок элемента и факторгруппа. Пункты а и б независимы.

$^{(\star)}$Примеры: $\mathrm{Irr}_{2,2} = \{x^2 + x + 1\}$, $\mathrm{Irr}_{2,3} = \{x^3 + x + 1, x^3 + x^2 + 1\}$ и $\mathrm{Irr}_{3,2} = \{x^2 + 1, x^2 + x + 2, x^2 + 2x + 2\}$.