

Деление с остатком и разложение на множители

- Аз♦1. Пусть K — любое коммутативное кольцо с единицей, и $g \in K[x]$. Покажите, что
- а) для любого $f \in K[x]$ с обратимым старшим коэффициентом существуют такие $q, r \in K[x]$, что $g = fq + r$ и либо $\deg r < \deg f$, либо $r = 0$
 - б) для любого $a \in K$ существует такой $q \in K[x]$, что $g(x) = q(x) \cdot (x - a) + g(a)$ в $K[x]$
 - в) существует коммутативное кольцо $R \supseteq K$ с той же единицей, что у K , такое что g полностью разлагается в $R[x]$ на множители степени ≤ 1 .
- Аз♦2. Может ли неприводимый многочлен $f \in \mathbb{Z}[x]$ степени ≥ 2 иметь
- а) рациональные корни? б) кратные комплексные корни?
- Аз♦3. Пусть многочлены $f_1, f_2, \dots, f_s \in \mathbb{Q}[x]$ попарно взаимно просты, и $F = f_1 f_2 \dots f_s$. Постройте изоморфизм колец $\mathbb{Q}[x]/(F) \simeq \prod_v \mathbb{Q}[x]/(f_v)$ и найдите в $\mathbb{Q}[x]$ все многочлены с остатками $1 + x$, $1 + x^3$ и $1 + x^5$ от деления на $1 + x^2$, $1 + x^4$ и $1 + x^8$ соответственно.
- Аз♦4. В кольце $\mathbb{Z}/(360)$ найдите все решения уравнений а) $x^2 = 1$ б) $x^3 = 1$ в) $x^2 = 49$.
- Аз♦5. Пусть \mathbb{F}_q — конечное поле. Верно ли, что любая функция $\mathbb{F} \rightarrow \mathbb{F}$ является многочленом? Могут ли разные многочлены задавать одинаковые функции?
- Аз♦6. Будет ли полем а) $\mathbb{R}[x]/(x^4 + 1)$ б) $\mathbb{Q}[x]/(x^4 + 1)$ в) $\mathbb{Q}[x]/(x^2 - 3)$?
- Аз♦7. Приводимы ли в $\mathbb{Q}[x]$ многочлены: а) $x^4 - 8x^3 + 12x^2 - 6x + 2$ б) $x^5 - 12x^3 + 36x - 12$.
- Аз♦8*. В кольце $\mathbb{Z}[x]$ разложите на неприводимые множители или докажите неприводимость многочленов: а) $t^4 + t + 1$ б) $t^5 + t^4 + t^2 + t + 2$ в) $t^6 + t^3 + 1$.
- Аз♦9 (Евклидовы кольца). Целостное¹ коммутативное кольцо A называется *евклидовым*, если на нём задана функция $v : A \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ (*евклидова норма*) со свойствами: (1) $\forall a, b \in A \ v(ab) \geq v(a)$ (2) $\forall b \neq 0 \ \exists q, r \in A : a = bq + r$ и при этом либо $r = 0$, либо $v(r) < v(b)$. Покажите, что для любых элементов a, b евклидова кольца A
- а) $v(ab) = v(a) \iff b$ обратим
 - б) среди общих делителей a и b имеется единственный с точностью до умножения на обратимые элементы кольца делитель наибольшей нормы², и он делится на все общие делители
 - в) (алгоритм Евклида) при $v(a) > v(b)$ $\text{нод}(a, b)$ совпадает с последним ненулевым элементом последовательности r_n , в которой $r_1 = a, r_2 = b$ и $r_n = r_{n-2} - q_{n-1}r_{n-1}$ при $n > 2$ это (любой) удовлетворяющий свойствам (1) и (2) остаток от деления r_{n-2} на r_{n-1}
 - г) $\text{нод}(a, b) = ax + by$ для подходящих $x, y \in A$; подберите такие x, y и найдите $\text{нод}(a, b)$ для $(a, b) = (8\ 385\ 403, 2\ 442\ 778)$ в кольце \mathbb{Z} и $(a, b) = (x^5 - 1, x^4 + x^2 + 1)$ в кольце $\mathbb{Q}[x]$
- Аз♦10. Покажите, что гауссовы кольца а) $\mathbb{Z}[i], i^2 = -1$, б) $\mathbb{Z}[\omega], \omega^2 + \omega = -1$, евклидовы.
- Аз♦11. Покажите, что любой идеал в евклидовом кольце является главным.
- Аз♦12. Являются ли $\mathbb{Q}[x, y]$ и $\mathbb{Z}[x]$ кольцами главных идеалов?
- Аз♦13. Пусть общие делители $f, g \in \mathbb{Z}[x]$ исчерпываются ± 1 . Обязательно ли конечно фактор кольцо $\mathbb{Z}[x]/(f, g)$?
- Аз♦14. Пусть \mathbb{k} — любое (возможно, конечное) поле. Бесконечно ли множество неприводимых многочленов в $\mathbb{k}[x]$?
- Аз♦15. Найдите а) все неприводимые многочлены степени ≤ 5 в $\mathbb{F}_2[x]$ б) все неприводимые многочлены степени 2 в $\mathbb{F}_3[x]$ в) число неприводимых многочленов степени 3 и 4 над $\mathbb{Z}/(3)$.
- Аз♦16. Пусть $p \in \mathbb{N}$ — простое, и $f \in \mathbb{F}_p[x]$ — неприводимый многочлен степени n . Сколько элементов в факторе $\mathbb{F}_p[x]/(f)$? Является ли он полем?
- Аз♦17*. Покажите, что для каждого $n \in \mathbb{N}$ и простого p имеется поле из p^n элементов.

¹т. е. с единицей и без делителей нуля

²он называется *наибольшим общим делителем* и обозначается $\text{нод}(a, b)$

№	дата сдачи	имя и фамилия принявшего	подпись принявшего
1а			
б			
в			
2а			
б			
3			
4а			
б			
в			
5			
6			
7а			
б			
8а			
б			
в			
9а			
б			
в			
г			
10а			
б			
11			
12			
13			
14			
15а			
б			
в			
16			
17			