

Идеалы, факторкольца и разложение на множители

Максимальность, простота и неприводимость. В коммутативном кольце A с единицей собственный¹ идеал² $\mathfrak{a} \subset A$ называется *простым* (соотв. *максимальным*), если кольцо A/\mathfrak{a} не имеет делителей нуля (соотв. является полем). Необратимый элемент $a \in A$ называется *простым*, если идеал $(a) \subset A$ прост, и *неприводимым*, если равенство $a = rs$ влечёт обратимость r или s .

АС4♦1. Опишите все идеалы в кольцах $\mathbb{k}[x]$ и $\mathbb{k}[[x]]$, где \mathbb{k} — поле. Какие из них максимальны? Какие просты?

АС4♦2. Являются ли кольца $\mathbb{Q}[x, y]$ и $\mathbb{Z}[x]$ областями главных идеалов? Есть ли в них простые немаксимальные идеалы?

АС4♦3. Обязательно ли конечно кольцо $\mathbb{Z}[x]/(f, g)$, если $f, g \in \mathbb{Z}[x]$ а) взаимно просты в кольце $\mathbb{Q}[x]$ б*) имеют $\text{НОД}(f, g) = 1$ в кольце $\mathbb{Z}[x]$?

АС4♦4. Докажите, что каждый простой элемент неприводим.

АС4♦5. Как устроено кольцо $\mathbb{Z}[x]/(2, x^2 - 5)$? Найдите в кольце $\mathbb{Z}[\sqrt{5}] = \mathbb{Z}[x]/(x^2 - 5)$

а) непростой неприводимый элемент³

б) элемент, имеющий два различных⁴ разложения на неприводимые множители.

АС4♦6 (евклидовы кольца). Целостное коммутативное кольцо с единицей называется *евклидовым*, если на нём существует *функция высоты* $v : A \rightarrow \mathbb{Z}_{\geq 0}$ со свойствами: 1) $v(a) = 0$ если и только если $a = 0$ 2) для любых $a \in A$ и ненулевого $b \in A$ найдётся такое $q \in A$, что $v(a - bq) < v(b)$. Покажите, что а) каждое евклидово кольцо является областью главных идеалов б) высоту на евклидовом кольце можно выбрать так, чтобы⁵ $v(ab) \geq v(a)$ для всех a и всех $b \neq 0$ в) при таком выборе высоты равенство $v(ab) = v(a)$ при $a \neq 0$ равносильно обратимости b .

АС4♦7. Элементы кольца $\mathbb{Z}[i] \stackrel{\text{def}}{=} \mathbb{Z}[x]/(x^2 + 1) \simeq \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ называются *гауссовыми числами*. а) Нарисуйте в \mathbb{C} все гауссовы числа, кратные $5 - i$ б) Найдите наименьшее $n \in \mathbb{N}$, кратное заданному $a + bi \in \mathbb{Z}[i]$, если $\text{НОД}(a, b) = 1$ и в общем случае. в) Покажите, что кольцо $\mathbb{Z}[i]$ евклидово с приведённой высотой $v(z) = |z|^2$. г) Найдите $\text{НОД}(5 + 3i, 6 - 4i)$. д) Разложите $3, 5, 7, 7 + i$ на простые множители в $\mathbb{Z}[i]$. е) Какие простые $p \in \mathbb{Z}$ остаются таковыми в $\mathbb{Z}[i]$?

АС4♦8. Элементы кольца $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \mathbb{Z}[x]/(x^2 + x + 1) \simeq \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z}, \omega = e^{\frac{2\pi i}{3}}\}$ называются *числами Эйзенштейна*⁶. Покажите, что а) кольцо $\mathbb{Z}[\omega]$ евклидово с приведённой высотой $v(z) = |z|^2$ б) простое $p \in \mathbb{Z}$ имеет вид $x^2 + xy + y^2$, где $x, y \in \mathbb{Z}$, если и только если $p = 3$ или $p \equiv 1 \pmod{3}$. в) Какие простые $p \in \mathbb{Z}$ остаются таковыми в $\mathbb{Z}[\omega]$?

АС4♦9. Является ли кольцо $\mathbb{Z}[\sqrt{2}] = \mathbb{Z}[x]/(x^2 - 2) \simeq \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$ евклидовым относительно высоты $v(a + b\sqrt{2}) = |a^2 - 2b^2|$?

АС4♦10. Может ли неприводимый 1) в $\mathbb{Q}[x]$ 2) в $\mathbb{Z}[x]$ многочлен $f \in \mathbb{Z}[x]$ степени $\deg f \geq 2$ иметь а) рациональные корни б) кратные комплексные корни?

АС4♦11. Приводимы ли в $\mathbb{Q}[x]$ многочлены: а) $x^4 - 8x^3 + 12x^2 - 6x + 2$ б) $x^5 - 12x^3 + 36x - 12$?

АС4♦12. В кольце $\mathbb{Z}[x]$ разложите на неприводимые множители или докажите неприводимость многочленов: а) $x^4 + x + 1$ б) $x^5 + x^4 + x^2 + x + 2$ в) $x^6 + x^3 + 1$ г) $x^{105} - 9$.

¹Т. е. отличный от всего кольца.

²Т. е. подкольцо, содержащее вместе с каждым своим элементом и все его кратные.

³При решении этой задачи полезно понятие *нормы* $\|a + b\sqrt{5}\| \stackrel{\text{def}}{=} (a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - 5b^2$ и то, что *норменное отображение* $z \mapsto \|z\|$ является мультипликативным гомоморфизмом $\mathbb{Z}[\sqrt{5}] \rightarrow \mathbb{Z}$.

⁴Т. е. сомножители разложений нельзя привести в биективное соответствие друг с другом так, чтобы соответственные множители получались друг из друга умножением на обратимый элемент кольца.

⁵Такая высота v называется *приведённой*. Положите $v(a) = \min_{b \neq 0} v'(ab)$, где v' — произвольная высота.

⁶А также *числами* Кронекера.