Коммутативные кольца, гомоморфизмы и идеалы

Терминология. Отображение $A \xrightarrow{\varphi} B$ называется *гомоморфизмом колец*[1] если $\forall\, a_1, a_2 \in A$ в кольце B выполнены соотношения $\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2)$ и $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2)$. Взаимно однозначные гомомоморфизмы называются *изоморфизмами*, а изоморфизмы на себя называются *автоморфизмами*.

А3-1. Пусть $A \xrightarrow{\varphi} B$ – ненулевой гомоморфизм коммутативных колец с единицами. Верно ли, что $\varphi(1) = 1$? Изменится ли ответ, если в B нет делителей нуля?

А3-2. Найдите все автоморфизмы

а) поля $\mathbb{C}$, оставляющие элементы из $\mathbb{R}$ неподвижными.

б)* поля $\mathbb{Q}[\sqrt[3]{2}] \stackrel{\text{def}}{=} \mathbb{Q}[x]/(x^3 - 2)$.

А3-3°. Проверьте, что *образ* $\operatorname{im}\varphi \stackrel{\text{def}}{=} \{\, b \in B \mid \exists a \in A \varphi(a) = b\,\}$ гомоморфизма колец $A \xrightarrow{\varphi} B$ является подкольцом в B, а *ядро* $\ker\varphi \stackrel{\text{def}}{=} \{\, a \in A \mid \varphi(a) = 0\,\}$ является *идеалом*[2] в A, причём $\ker\varphi = \{0\}$ тогда и только тогда, когда φ – вложение.

А3-4°. Докажите, что кольцо является полем тогда и только тогда, когда оно не имеет идеалов, отличных от (0) и самого кольца.

Китайская теорема об остатках. Прямой суммой $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ колец[3] называется кольцо, элементами которого являются упорядоченные наборы $(a_1, a_2, \ldots, a_n)$ из $a_\nu \in A_\nu$ с *покоординатным* сложением и умножением.

А3-5. Докажите, что если $m = rs$ и *НОД* $(r, s) = 1$, то $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/s\mathbb{Z}$, и выведите из этого, что если число m разложено на простые множители: $m = p_1^{k_1} \cdot \cdots \cdot p_n^{k_n}$, то имеется изоморфизм колец $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{k_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_n^{k_n}\mathbb{Z}$.

А3-6. Сформулируйте и докажите аналог предыдущей задачи для кольца многочленов $k[x]$, где k — произвольное поле.

А3-7. В кольце $\mathbb{Z}/360\mathbb{Z}$ решите уравнения **а)** $x^2 = 1$ **б)** $x^3 = 1$ **в)** $x^2 = 49$

А3-8. Опишите все многочлены $f \in \mathbb{Q}[x]$, имеющие остатки $1 + x$, $1 + x^3$ и $1 + x^5$ от деления на $1 + x^2$, $1 + x^4$ и $1 + x^8$ соответственно.

Евклидовость. Кольцо A называется *евклидовым*, если в нём нет делителей нуля и имеется *функция высоты* λ из множества ненулевых элементов A в множество целых неотрицательных чисел, обладающая свойством $\lambda(ab) \geqslant \max\big(\lambda(a), \lambda(b)\big)$ и такая, что $\forall\, a, b \in A,\ b \neq 0$ найдутся q и r из A такие, что $a = bq + r$ и либо $r = 0$, либо $\lambda(r) < \lambda(b)$. Кольцо A называется *кольцом главных идеалов*, если все идеаля в A имеют вид $(a) \stackrel{\text{def}}{=} aA = \{ax \mid x \in A\}$ с $a \in A$.

А3-9°. Убедитесь, что кольца $\mathbb{Z}$ и $k[x]$, где k – поле, евклидовы.

А3-10. Докажите, что всякое евклидово кольцо является кольцом главных идеалов.

---

[1] что такое *коммутативное кольцо с единицей* и что такое *поле* см. в каом-нибудь учебнике алгебры, например в записках лекций

[2] подкольцо $\mathfrak{i} \subset A$ называется *идеалом*, если $a\mathfrak{i} \stackrel{\text{def}}{=} \{ax \mid x \in \mathfrak{i}\} \subset \mathfrak{i} \quad \forall\, a \in A$

[3] иногда вместо «прямая сумма» говорят «прямое произведение» и пишут $A_1 \times A_2 \times \cdots \times A_n$, что более правильно с «общекатегорной» точки зрения, но в рассматриваемых нами случаях обозначает в точности то же самое

А3-11. Докажите, что кольцо $\mathbb{Z}[\omega] = \{a+b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$, где $\omega \neq 1$ – один из комплексных корней уравнеия $z^3 = 1$, является евклидовым относительно высоты $\lambda(z) = |z|^2$ и опишите множество обратимых элементов этого кольца.

А3-12. Докажите, что кольца $\mathbb{Q}[x, y]$ и $\mathbb{Z}[x]$ не являются кольцами главных идеалов.

Терминология. Идеал $\mathfrak{a}$ в коммутативном кольце A с единицей называется *простым*, если в кольце $A/\mathfrak{a}$ нет делителей нуля, и *максимальным*, — если $A/\mathfrak{a}$ – поле. Элемент $a \in A$ называется *простым*, если идеал (a) прост, и *неприводимым*, — если a не представим в виде произведения двух необратимых элементов.

А3-13°. Докажите, что максимальные идеалы просты, а простые элементы неприводимы.

А3-14. Докажите, что в евклидовом кольце простота элемента равносильна его неприводимости.

А3-15*. Глядя на равенство $2 \cdot 2 = (\sqrt{5}+1) \cdot (\sqrt{5}-1)$ в кольце $\mathbb{Z}[\sqrt{5}]$, укажите в этом кольце неприводимый непростой элемент.

А3-16°. Докажите, что простота элемента p равносильно тому, что при произвольных $a, b \in A$ элемент p делит произведение ab лишь при условии, что он делит хотя бы один из сомножителей.

А3-17°. Докажите, что идеал является максимальным тогда и только тогда, когда он не содержится ни в каком строго большем идеале, отличном от всего кольца.

А3-18. Будет ли факторкольцо $\mathbb{R}[x]/(f(x))$ полем при $f = x^4 + 1$, $f = x^3 + 1$ и $f = x^2 + 3$?

А3-19. Докажите, что многочлен $x^{p-1} + \ldots + x + 1$ неприводим над $\mathbb{Q}$ при простом $p > 1$. *Указание*: воспользуйтесь *критерием Эйзенштейна*.

А3-20. Пусть $f(x)$ - неприводимый многочлен степени n над полем $\mathbb{Z}/p\mathbb{Z}$ (p - простое число). Докажите, что фактор-кольцо $(\mathbb{Z}/p\mathbb{Z})[x]/(f)$ есть конечное поле и найдите число его элементов.

А3-21. Пусть $f, g \in \mathbb{Z}[x]$ не имеют общих делителей, отличных от ± 1. Докажите, что фактор-кольцо $\mathbb{Z}[x]/(f, g)$ конечно.

А3-22. Докажите, что в кольце главных идеалов всякий элемент является произведением конечного числа неприводимых элементов.
Указание: воспользуйтесь тем, что в кольце главных идеалов нельзя построить бесконечной возрастающей цепочки строго вложенных друг в друга идеалов.

А3-23. Докажите, что в кольце $k[x]$ многочленов над *любым* полем имеется бесконечно много неприводимых многочленов.

А3-24. В кольце $k[[x]]$ формальных степенных рядов над полем k опишите все идеалы и все максимальные идеалы.

А3-25. Гауссовы целые числа. Пусть $\Gamma = \{\, m + ni \in \mathbb{C} \mid m, n \in \mathbb{Z} \,\}$ — кольцо *целых гауссовых чисел*. Докажите, что

а) Γ – евклидово кольцо относительно высоты $\lambda(z) = |z|^2$;

б) если числа m_1 и m_2 представимы в виде суммы квадратов двух неотрицательных целых чисел, то и их произведение $m_1 m_2$ тоже представимо;

в) следующие условия на простое число $p \in \mathbb{Z}$ попарно равносильны:

(a) $p \in \mathbb{Z}$ перестаёт быть простым в Γ;

(b) p представимо в виде суммы квадратов двух неотрицательных целых чисел;

(c) -1 является квадратом в $\mathbb{Z}/p\mathbb{Z}$;

(d)* $p \not\equiv 3 \pmod 4$.

A3-26*. Докажите, что натуральное число тогда и только тогда не является квадратом и не представляется в виде суммы двух квадратов, когда в его разложении на простые множители участвует хотя бы одно простое число вида $4k + 3$ в нечётной степени.

A3-27. Существует ли в кольце гауссовых целых чисел Γ такой идеал $\mathfrak{a} \subset \Gamma$, что фактор-кольцо $\Gamma/\mathfrak{a}$ является **а)** полем характеристики 2? **б)** полем характеристики 3? (в случае положительного ответа укажите, сколько элементов может быть в этом поле).