Упражнение 1. Пусть $d = \sqrt[3]{2}$. Рассмотрим кольцо порожденное элементами $1, d$. Показать, что данное кольцо представимо в виде

$$R = \{a + bd + cd^2 \mid a, b, c \in \mathbb{Z}\}.$$

Разрешимо ли в рамках кольца R уравнение:

$$(1 - 3d + 5d^2)x = -18 + 10d + 20d^2$$

Присутствуют ли в данном кольце делители нуля?

Решение. Очевидно, что $\langle 1 \rangle = \mathbb{Z}, \langle d \rangle = d\mathbb{Z}$. В $\langle 1, d \rangle$ лежит их сумма, т.е. $\mathbb{Z} + d\mathbb{Z}$. $\mathbb{Z} \cdot (d\mathbb{Z}) = d\mathbb{Z}$, что не добавляет новых элементов. $(d\mathbb{Z}) \cdot (d\mathbb{Z}) = d^2\mathbb{Z}$ и тогда промежуточный результат это $\mathbb{Z} + d\mathbb{Z} + d^2\mathbb{Z}$. $\mathbb{Z} \cdot d^2\mathbb{Z} = d^2\mathbb{Z}, d\mathbb{Z} \cdot d^2\mathbb{Z} = \mathbb{Z}, d^2\mathbb{Z} \cdot d^2\mathbb{Z} = d\mathbb{Z}$, поэтому больше нечего добавлять.

$$\begin{aligned} (1 - 3d + 5d^2)(a + bd + cd^2) &= -18 + 10d + 20d^2 \\ a + bd + cd^2 - 3ad - 3bd^2 - 6c + 5ad^2 + 10b + 10cd &= -18 + 10d + 20d^2 \end{aligned}$$

$$\begin{cases} a - 6c + 10b = -18 \\ b - 3a + 10c = 10 \\ c - 3b + 5a = 20 \end{cases}$$

Система не вырождена, решение есть.

Делители нуля:

$$\begin{aligned} xy &= 0 \\ (a_1 + b_1d + c_1d^2)(a_2 + b_2d + c_2d^2) &= 0 \\ a_1a_2 + a_1b_2d + a_1c_2d^2 + b_1a_2d + b_1b_2d^2 + 2b_1c_2 + c_1a_2d^2 + 2c_1b_2 + 2c_1c_2d &= 0 \end{aligned}$$

$$\begin{cases} a_1a_2 + 2b_1c_2 + 2c_1b_2 = 0 \\ a_1b_2 + b_1a_2 + 2c_1c_2 = 0 \\ a_1c_2 + b_1b_2 + c_1a_2 = 0 \end{cases}$$

Что делать с этой системой нелинейных диофантовых уравнений не очень понятно.

□

Упражнение 2. Рассмотрим кольцо многочленов $R = \mathbb{R}[x]$ и множество:

$$J = \{p \mid p \vdots x^2 + 1\}$$

Показать, что J есть идеал. Построить ${}^{R}/_{J}$. Существуют ли в ${}^{R}/_{J}$ делители нуля?

Решение. То, что J является подкольцом, очевидно.

$\triangleleft a \in R, p \cdot (x^2+1) \in J.$

$$a \cdot p \cdot (x^2+1) \in J$$

Таким образом, J — идеал.

В каждом классе из ${}^{R}\!/_{J}$ есть ровно один элемент вида $ax+b$, потому что если коэффициент при x^{n+2} ненулевой и $n \geq 0$, то такой многочлен можно представить как $(x^2+1)\cdot x^n \cdot a + p$ и тогда любой многочлен лежит в $[ax+b]$ для каких-то a и b.

Заметим, что в ${}^{R}\!/_{J}$ $[x^2+1] = [0]$, следовательно, $[x^2] = [-1]$. Итого ${}^{R}\!/_{J} = \{ax+b \mid a, b \in \mathbb{Z}\}$ со стандартным сложением и умножением таким, что $x^2 = -1$. Несложно также заметить, что ${}^{R}\!/_{J} \cong \mathbb{C}$ по гомоморфизму $[ax+b] \mapsto b + ia$.

В $\mathbb{C}$ нет делителей нуля, так что и в ${}^{R}\!/_{J}$ их нет. □

Упражнение 3. Вычислить

1. $\varphi(360)$
2. $\varphi(125)$
3. $\varphi(\varphi(12))$

Решение.

1. $\varphi(360) = \varphi(8)\cdot\varphi(9)\cdot\varphi(5) = 4\cdot(2-1)\cdot 3\cdot(3-1)\cdot 4 = 96$
2. $\varphi(125) = \varphi(5^3) = 5^2\cdot(5-1) = 100$
3. $\varphi(\varphi(12)) = \varphi(|\{1,5,7,11\}|) = \varphi(4) = |\{1,3\}| = 2$

□

Упражнение 4. Пусть $a, n \in \mathbb{Z}$ два взаимно простых числа $(a, n) = 1$. Показать, что:

$$a^{\varphi(n)} \equiv 1 \pmod n$$

Решение. Рассмотрим мультипликативную группу A взаимно простых с n чисел по модулю n. Очевидно это действительно группа. $|A| = \varphi(n)$. По теореме Лагранжа $|A| \vdots |\langle a\rangle|$, т.е. $|\langle a\rangle| \cdot k = \varphi(n)$.

$$a^{\varphi(n)} = a^{|\langle a\rangle|\cdot k}$$

Из структуры A понятно, что $\langle a\rangle$ это простой цикл и тогда $a^{|\langle a\rangle|} \equiv 1 \pmod n$.

$$a^{\varphi(n)} = 1 \pmod n$$

□