Здесь мы всегда считаем что $R = (R; +, \cdot\,; 0_R, 1_R)$ *— коммутативное кольцо с единицей*

Некоторые Определения

Определение 1. *Элемент* $a \in R$, $a \neq 0$ *называется* делителем нуля *если существует* $b \in R$, $b \neq 0$ *такой что* $ab = 0$.

Определение 2. R *называется* областью целостности (ID = integral domain) *если в* R *нет делителей нуля;* $ab = 0 \implies a = 0$ *или* $b = 0$.

Определение 3. R *называется* полем *если любой* $a \in R$, $a \neq 0$, *имеет обратный элемент по умножению, т.е.,* $\exists b : ab = 1_R$, $b := a^{-1}$.

Определение 4. *Подкольцо* $I < R$ *называется* идеалом *если* $\forall a \in R, r \in I \implies ar \in I$, *мы будем это обозначать как* $I \triangleleft R$.

Определение 5. *Идеал* $I \triangleleft R$ *называется* конечно порожденным *если* $\exists r_1, \ldots, r_n \in R$ *такие что*

$$I = \langle r_1, \ldots, r_n \rangle = \{a_1 r_1 + \cdots a_n r_n \mid a_i \in R\}.$$

Идеал $I \triangleleft R$ *называется* главным *если* $I = \langle r \rangle$ *для некоторого* $r \in R$.

Определение 6. *Идеал* $\mathfrak{m} \triangleleft R$ *называется* максимальным *если* $\mathfrak{m} \neq R$, *и для любого* $J \triangleleft R$, $\mathfrak{m} \subseteq J \subseteq R$, $J = \mathfrak{m}$ *или* $J = R$.

Определение 7. $R = ID$ *(т.е., область целостности* R*) называется* кольцом главных идеалов (PID = principal ideal domain) *если любой идеал в* R *главный.*

Определение 8. *Мы говорим что* $a|b$ *если* $b = ka$ *для некоторого* $k \in R$. *На языке идеалов,* $\langle b \rangle \subseteq \langle a \rangle$.

Определение 9. *Элемент* $p \in R$, $p \neq 0$, $p \notin R^\times$ *называется* простым *если* $p|ab \implies p|a$ *или* $p|b$.

Определение 10. *Элемент* $q \in R$, $q \neq 0$, $q \notin R^\times$ *называется* неприводимым *если* $p = ab \implies a \in R^\times$ *или* $b \in R^\times$.

Задачи на определения

Задача 1. *В кольце* $\mathbb{Z}_{12}$ *опишите все обратимые, непривдимые, и простые элементы.*

Задача 2. *Покажите что если* $R = ID$ *и* $p \in R$ *простой, то* p *неприводимый.*

Задача 3. *Покажите что если* $R = PID$ *и* $q \in R$ *неприводимый, то* q *простой.*

Задача 4. *Покажите что если* $R = PID$ *и* $q \in R$ *неприводимый, то* $\mathfrak{m} = \langle q \rangle$ *максимальный идеал.*

Задача 5. *Покажите что* $\mathfrak{m}$ *максимальный идеал тогда и только тогда когда* $R/\mathfrak{m}$ *поле.*

Факты

Кольца $\mathbb{Z}$ и $\mathbb{F}[x]$, где F - поле, являются Евклидовыми (алгоритм Евклида и деление с остатком). Любое Евклидово кольцо есть кольцо главных идеалов, $ED \implies PID$.

Задачи

Задача 6. *Можно показать что многочлен* $f(x) = x^3 + 3x + 3 \in \mathbb{Q}[x]$ *неприводим. Тогда* $\mathfrak{m} = \langle f \rangle$ *максимален и* $\mathbb{Q}[x]/\mathfrak{m}$ *— поле:*

$$\mathbb{F} = \mathbb{Q}[x]/\langle x^3+3x+3 \rangle = \left\{[c_0 + c_1 x + c_2 x^2] = [c_0] + [c_1][x] + [c_1][x]^2 = c_0 + c_1\alpha + c_2\alpha^2\right\} = \mathrm{Span}_{\mathbb{Q}}\{1, \alpha, \alpha^2\},$$

где $\alpha = [x]$ *и мы пишем* $[c_i], c_i \in \mathbb{Q}$ *просто как* c_i *(и.е.,* $\mathbb{Q} < \mathbb{F}$*). Найдите в этом поле* α^{-1}, $(1+\alpha)^{-1}$, $(1+\alpha^2)^{-1}$ *(в виде линейной комбинации* $c_0 + c_1\alpha + c_2\alpha^2$*). Подсказка: используйте алгоритм Евклида.*

Задача 7. *Постройте минимальное расширение поля* $\mathbb{Q}$ *в котором многочлен* $f(x) = x^2 + 2$ *имеет корень. Разложите его на множители.*

Задача 8. *Постройте минимальное расширение* $\mathbb{L}$ *поля* $\mathbb{Q}$ *в котором многочлен* $f(x) = x^3 - 5$ *имеет корень. Разложите его на множители. Теперь постройте минимальное расширение* $\mathbb{E}$ *поля* $\mathbb{L}$ *в котором этот многочлен раскладывается на линейные множители.*