РАЗДЕЛ 1

Кольца, типы колец, поля

1.1. Понятие кольца

Рассмотрим алгебраическую структуру $(\mathbb{Z}, +, \cdot)$, где $+$ и $\cdot$ – это обычные операции сложения и умножения чисел. Хорошо известно, что эти две операции связаны *дистрибутивным законом*: $(a+b)c = ac + bc$ для любых $a, b, c \in \mathbb{Z}$. Заметим сразу, что указанная замечательная связь операций сложения и умножения (она воспринимается нами как нечто само собой разумеющееся) не является обязательным свойством произвольных алгебраических структур. Например, в алгебраической структуре $(\mathbb{Z}, +, \diamond)$, где операция $a \diamond b$ определена при помощи соотношения $a \diamond b = a + b + ab$ и играет роль умножения, свойство дистрибутивности уже не выполняется (проверка оставляется в качестве *упражнения*). Вспомним также, что $(\mathbb{Z}, +)$ – это коммутативная группа, а $(\mathbb{Z}, \cdot)$ – полугруппа. Эти наблюдения оправдывают следующее определение.

Определение. *Пусть $\mathcal{R}$ – некоторое множество, на котором опредедены операции сложения $(+)$ и умножения $(\cdot)$. Алгебраическая структура $(\mathcal{R}, +, \cdot)$ называется кольцом, если*

- *$(\mathcal{R}, +)$ является коммутативной группой;*
- *$(\mathcal{R}, \cdot)$ – является полугруппой;*
- *операции $+$ и $\cdot$ на $\mathcal{R}$ связаны дистрибутивным законом: $(a+b)c = ac + bc$ и $a(b+c) = ab + ac$ для любых $a, b, c \in \mathcal{R}$.*

Подмножество $\mathcal{R}'$ кольца $\mathcal{R}$, само являющееся кольцом, называется подкольцом кольца $\mathcal{R}$.

Если $(\mathcal{R}, +, \cdot)$ кольцо, а $(\mathcal{R}, \cdot)$ – полугруппа с единицей, то кольцо $\mathcal{R}$ называется кольцом с единицей. Если $(\mathcal{R}, \cdot)$ – коммутативная полугруппа, то $\mathcal{R}$ называется коммутативным кольцом.

В определении кольца требуется, чтобы относительно умножения $\mathcal{R}$ было полугруппой. Это требование означает, что операция умножения в кольце должна быть ассоциативной. В ряде случае полезно рассматривать и такие алгебраические структуры $(\mathcal{R}, +, \cdot)$, в которых операция умножения может и не быть ассоциативной. В этом случае вводится понятие *неассоциативного* кольца.

В точности так же, как это делается в случае групп, проверяется справедливость следующего утверждения.

Предложение. *Пусть $\mathcal{R}$ – некоторое кольцо, а $\mathcal{R}_\ell$ при $\ell \in \Lambda$ (некоторое множество индексов) подкольца кольца $\mathcal{R}$. Тогда $\mathcal{R}_\Lambda = \bigcap_{\ell \in \Lambda} \mathcal{R}_\ell$ подкольцо кольца $\mathcal{R}$.*

Пример 1.1. $(\mathbb{Z}, +, \cdot)$ – коммутативное кольцо с единицей, $(m\mathbb{Z}, +, \cdot)$, $m \in \mathbb{N}$ – коммутативное кольцо (без единицы). Совокупность $M_n(\mathbb{R})$ вещественных $n \times n$ матриц является (некоммутативным) кольцом с единицей относительно операций матричного сложения и умножения. Аналогично можно определить кольцо матриц $M_n(\mathcal{R})$ с элементами, принадлежащими некоторому кольцу $\mathcal{R}$.

В любой аддитивной абелевой группе G можно ввести структуру кольца, если определить умножение $\cdot$ в G следующим тривиальным образом: $xy = 0$ (ноль группы G) для любых $x, y \in G$.

Пример 1.2. Если X – произвольное множество, а $\mathcal{R}$ – некоторое кольцо с единицей, то совокупность $F(X, \mathcal{R})$ функций $f : X \to \mathcal{R}$ образует кольцо относительно

операций поточечного сложения и умножения функций:

$$(f+g)(x) = f(x) + g(x), \qquad (fg)(x) = f(x)g(x), \qquad x \in X,$$

образует кольцо с единицей, причем нулем и единицей в $F(X, \mathcal{R})$ являются функции $x \mapsto 0$ и $x \mapsto 1$ соответственно (здесь 1 – единица в $\mathcal{R}$).

Установим некоторые общие свойства колец. Напомним, что через $-x$ обозначается обратный к элементу x элемент аддитивной группы кольца.

Предложение. *В произвольном кольце $\mathcal{R}$ верны равенства $0x = x0 = 0$ для любого $x \in \mathcal{R}$ и $(-a)b = a(-b) = -(ab)$ для любых $a, b \in \mathcal{R}$. В произвольном нетривиальном кольце $\mathcal{R}$ с единицей $1 \neq 0$.*

Доказательство. Первое утверждение проверяется так:

$$x = x + 0 \quad \Longrightarrow \quad x^2 = x(x+0) = x^2 + x0 \quad \Longrightarrow \quad 0 = x0,$$

равенство $0 = 0x$ проверяется аналогично. Пусть теперь $1 = 0$. Тогда для любого $x \in \mathcal{R}$ верны равенства $x = 1x = 0x = 0$, что противоречит предположению о том, что кольцо $\mathcal{R}$ нетривиально. Следовательно, $1 \neq 0$. Проверим третье свойство. Для произвольных $a, b \in \mathcal{R}$ имеем $0 = a0 = a(b-b) = ab + a(-b)$ и, следовательно, $-(ab) = a(-b)$. Оставшееся равенство проверяется аналогично. □

Замечание. Так как $-(-a) = a$, то из только что доказанного утверждения вытекает, что $(-a)(-b) = ab$ для любых $a, b \in \mathcal{R}$. Кроме того, по индукции можно легко проверить (это рекомендуется проделать в качестве *упражнения*), что для любых $a_1, \ldots, a_n \in \mathcal{R}$ и для любых $b_1, \ldots, b_m \in \mathcal{R}$ имеет место равенство

$$(a_1 + \cdots + a_n)(b_1 + \cdots + b_m) = \sum_{j=1}^{n} \sum_{k=1}^{m} a_j b_k.$$

Далее, из этой формулы вытекает, что для любого $n \in \mathbb{Z}$ и для любых элементов x, y кольца $\mathcal{R}$ имеют место соотношения $n(xy) = (nx)y = x(ny)$.

И, наконец, легко проверяется (*упражнение*), что в произвольном коммутативном кольце $\mathcal{R}$ с единицей выполняется формула *бинома Ньютона*:

$$(a+b)^n = \sum_{k=0}^{n} \mathrm{C}_n^k \, a^k b^{n-k}, \quad \text{для любых} \quad a, b \in \mathcal{R}.$$

Сравнения. Классы вычетов. Пусть $m \in \mathbb{N}$, $m > 1$. Напомним, что $m\mathbb{Z}$ – это подкольцо кольца $\mathbb{Z}$, состоящее из всех целых чисел, кратных m. Введем следующее определение.

Определение. *Два числа $n_1 \in \mathbb{Z}$ и $n_2 \in \mathbb{Z}$ называются сравнимыми по модулю m, если они имеют одинаковые остатки при делении на m. Для записи этого факта используют символ $n_1 \equiv n_2 \pmod m$.*

Другими словами, $n_1 \equiv n_2 \pmod m$ если и только если $n_1 - n_2 \in m\mathbb{Z}$. Из этого факта непосредственно выводится следующий результат, проверка которого оставляется в качестве *упражнения*.

Предложение. *Отношение $\equiv \pmod m$ на множестве $\mathbb{Z}$ является отношением эквивалентности.*

Из этого вытекает, что множество $\mathbb{Z}$ распадается на непересекающиеся подмножества – классы эквивалентности по рассматриваемому отношению. Эти классы называются *классами вычетов по модулю m*. При этом каждый класс вычетов по модулю m имеет вид

$$\{r\}_m = r + m\mathbb{Z} = \{r + km : \ k \in \mathbb{Z}\},$$

где r – целое число и, кроме того,

$$\mathbb{Z} = \{0\}_m \sqcup \{1\}_m \sqcup \cdots \sqcup \{m-1\}_m.$$

Предложение. *Пусть $n_1, n_2, k_1, k_2 \in \mathbb{Z}$ таковы, что $n_1 \equiv n_2 \pmod m$ и $k_1 \equiv k_2 \pmod m$. Тогда $n_1 \pm k_1 \equiv n_2 \pm k_2 \pmod m$ и $n_1 k_1 \equiv n_2 k_2 \pmod m$. Кроме того, $n_1 \ell \equiv n_2 \ell \pmod m$ для любого $\ell \in \mathbb{Z}$.*

Проверка. Все требуемые сравнимости непосредственно вытекают из того факта, что $x \equiv y \pmod m$ тогда и только тогда, когда $x - y \in m\mathbb{Z}$. В самом деле, пусть $n_1 - n_2 = tm$, $t \in \mathbb{Z}$ и пусть $k_1 - k_2 = sm$, $s \in \mathbb{Z}$. Тогда, например, $n_1 k_1 - n_2 k_2 = m(sn_2 + tk_2 + stm)$ и, следовательно, $n_1 k_1 \equiv n_2 k_2 \pmod m$. Остальные свойства проверяются аналогично. □

Отсюда следует, что на множестве $\mathbb{Z}/m\mathbb{Z}$ классов вычетов по модулю m можно задать операции сложения $\oplus$ и умножения $\odot$ по формулам

$$\{n\}_m \oplus \{k\}_m := \{n + k\}_m, \qquad \{n\}_m \odot \{k\}_m := \{nk\}_m.$$

Упражнение. Проверить, что множество $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ является кольцом относительно операций $\oplus$ и $\odot$. Это кольцо называют *кольцом классов вычетов* по модулю m или, чаще, просто *кольцом вычетов* по модулю m.

Если в каждом классе вычетов по модулю m выбрать минимальный неотрицательный представитель, то мы получим множество $\{0, 1, \ldots, m-1\}$, которое часто называют *полной приведенной системой вычетов* по модулю m. Ясно, что кольцо $\mathbb{Z}_m$ естественно отождествляется с этим множеством, на котором операции сложения и умножения заданы как сложение и умножение по модулю m.

1.2. Гомоморфизмы колец, идеалы колец и факторкольца

Гомоморфизмы колец.

Определение. *Пусть $\mathcal{R}_1$ и $\mathcal{R}_2$ – кольца. Отображение $f : \mathcal{R}_1 \to \mathcal{R}_2$ называется гомоморфизмом колец $\mathcal{R}_1$ и $\mathcal{R}_2$, если оно сохраняет обе операции, т.е. если для любых $x, y \in \mathcal{R}_1$ выполняются равенства*

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y),$$

где в левых частях приведенных равенств сложение и умножение выполняются в кольце $\mathcal{R}_1$, а в правых – в кольце $\mathcal{R}_2$.

Любой гомоморфизм $f : \mathcal{R}_1 \to \mathcal{R}_2$ колец $\mathcal{R}_1$ и $\mathcal{R}_2$ обладает теми свойствами, что $f(0_1) = 0_2$ и $f(nx) = nf(x)$ для всех $x \in \mathcal{R}_1$ и $n \in \mathbb{Z}$. Проверку этого свойства оставляется в качестве *упражнения*.

Для гомоморфизма $f : \mathcal{R}_1 \to \mathcal{R}_2$ колец, как и в случае гомоморфизмов групп, определяются его *ядро*

$$\operatorname{Ker} f = \{x \in \mathcal{R}_1 : \ f(x) = 0_2\}$$

и *образ*

$$\operatorname{Ran} f = f(\mathcal{R}_1) = \{y \in \mathcal{R}_2 : \ y = f(x), x \in \mathcal{R}_1\}.$$

При этом $\operatorname{Ker} f$ является подкольцом в $\mathcal{R}_1$, а $\operatorname{Ran} f$ – подкольцом в $\mathcal{R}_2$.

Далее, как и в случае гомоморфизмов групп, гомоморфизм f колец называется *мономорфизмом*, если $\operatorname{Ker} f = \{0\}$, *эпиморфизмом*, если $\operatorname{Ran} f = \mathcal{R}_2$ и *изоморфизмом*, если f является мономорфизмом и эпиморфизмом одновременно.

Другими словами, изоморфизм колец – это биективный гомоморфизм.

Упражнение. Проверить, что если $\mathcal{R}_1$ и $\mathcal{R}_2$ – кольца с единицей, а $f : \mathcal{R}_1 \to \mathcal{R}_2$ – эпиморфизм колец, то $f(1_1) = 1_2$.

Заметим, что при рассмотрении гомоморфизмов $f : \mathcal{R}_1 \to \mathcal{R}_2$ колец с единицей условие $f(1_1) = 1_2$ должно быть заложено в соответствующее определение.

Идеалы колец и факторкольца. Пусть $f : \mathcal{R} \to \mathcal{R}'$ – некоторый гомоморфизм колец $\mathcal{R}$ и $\mathcal{R}'$. Рассмотрим его ядро $\operatorname{Ker} f = \{a \in \mathcal{R} : \ f(a) = 0'\}$, где $0'$ – ноль в кольце $\mathcal{R}'$. Заметим, что $\mathcal{J} := \operatorname{Ker} f$ – это не простое подкольцо в $\mathcal{R}$, оно обладает специальными интересными свойствами. А именно, для любого $x \in \mathcal{R}$ имеют место включения

$$\mathcal{J} \cdot x = \{ax : \ a \in \mathcal{J}\} \subset \mathcal{J} \qquad \text{и} \quad x \cdot \mathcal{J} = \{xa : \ a \in \mathcal{J}\} \subset \mathcal{J}.$$

В самом деле, если $x \in \mathcal{R}$, а $a \in \mathcal{J}$, то $f(ax) = f(a)f(x) = 0'f(x) = 0'$ и $f(xa) = f(x)f(a) = f(x)0' = 0'$, откуда $xa \in \mathcal{J}$ и $ax \in \mathcal{J}$.

Понятие идеала. Если $\mathcal{J} \subset \mathcal{R}$ – подкольцо кольца $\mathcal{R}$. Обозначим через $\mathcal{J}\mathcal{R} = \{jr : \ j \in \mathcal{J}, \ r \in \mathcal{R}\}$, а $\mathcal{R}\mathcal{J} = \{rj : \ r \in \mathcal{R}, \ j \in \mathcal{J}\}$. Ясно, что в общем случае $\mathcal{J}\mathcal{R} \neq \mathcal{R}\mathcal{J}$.

Определение. *Подкольцо $\mathcal{J}$ кольца $\mathcal{R}$ называется идеалом (или, точнее, двусторонним идеалом), если $\mathcal{J}\mathcal{R} \subset \mathcal{J}$ и $\mathcal{R}\mathcal{J} \subset \mathcal{J}$. Если выполнено только условие $\mathcal{J}\mathcal{R} \subset \mathcal{J}$, то $\mathcal{J}$ называется левым идеалом кольца $\mathcal{R}$, а если выполнено только условие $\mathcal{R}\mathcal{J} \subset \mathcal{J}$, то $\mathcal{J}$ называется правым идеалом кольца $\mathcal{R}$.*

Если $\mathcal{R}$ – коммутативное кольцо, то понятия правого, левого и двустороннего идеалов совпадают.

Естественным образом возникает вопрос о том, как находить идеалы в кольцах. Пусть $\mathcal{R}$ – коммутативное кольцо, и пусть $a \in \mathcal{R}$. При этом $a\mathcal{R} = \{ax : \ x \in \mathcal{R}\}$ – будет идеалом в $\mathcal{R}$. В самом деле $(a\mathcal{R})\mathcal{R} = \{axy : \ x, y \in \mathcal{R}\} \subset \{az : \ z \in \mathcal{R}\}$ и, так как кольцо $\mathcal{R}$ коммутативное, то $\mathcal{R}(a\mathcal{R}) = \{xay : \ x, y \in \mathcal{R}\} \subset \{aw : \ w \in \mathcal{R}\}$.

Идеал вида $a\mathcal{R}$ (коммутативного) кольца $\mathcal{R}$ называется главным идеалом.

Если кольцо $\mathcal{R}$ не коммутативно, то понятие главного идеала превращается в понятие главного левого идеала. Аналогично, в случае некоммутативного кольца вводится понятие главного правого идеала.

В качестве примера главного идеала можно рассмотреть идеал $m\mathbb{Z} = \{mk : \ k \in \mathbb{Z}\}$ при $m \in \mathbb{Z}$ – множество всех целых кратных данного целого числа m.

Если рассматривать кольца $\mathcal{R}$ с единицей, то идеалами будут подгруппы аддитивной группы кольца, инвариантные относительно умножения на элементы кольца справа и слева.

Понятие факторкольца. Пусть теперь $\mathcal{R}$ – некоторое кольцо, а $\mathcal{J}$ – его (двусторонний) идеал. Рассмотрим конструкцию *факторкольца* кольца $\mathcal{R}$ по идеалу $\mathcal{J}$. Для этого мы определим следующее отношение $\sim_{\mathcal{J}}$ на множестве $\mathcal{R}$: скажем, что элементы $a \in \mathcal{R}$ и $b \in \mathcal{R}$ удовлетворяют отношению $a \sim_{\mathcal{J}} b$, если и только если $a - b \in \mathcal{J}$.

Упражнение. Проверить, что отношение $\sim_{\mathcal{J}}$ является отношением эквивалентности на $\mathcal{R}$.

На основании общих свойств отношений эквивалентности, множество $\mathcal{R}$ разбивается на непересекающиеся классы эквивалентности по отношению $\sim_{\mathcal{J}}$. Эти классы называются *классами вычетов по модулю идеала $\mathcal{J}$* (это название оправдано очевидной аналогией с классами вычетов по модулю целого числа m, которые являются классами вычетов множества $\mathbb{Z}$ по модулю идеала $m\mathbb{Z}$). Классы вычетов $\mathcal{R}$ по модулю идеала $\mathcal{J}$ обозначаются символом $a + \mathcal{J}$, где $a \in \mathcal{R}$ – представитель соответствующего класса. В этом обозначении учтено, что при построении идеалов используется аддитивная подгруппа рассматриваемого кольца.

На множестве $\mathcal{R}/\mathcal{J}$ классов вычетов по модулю идеала $\mathcal{J}$ определим операции сложения $\oplus$ и умножения $\odot$ следующим образом:

$$(a + \mathcal{J}) \oplus (b + \mathcal{J}) = (a + b) + \mathcal{J}, \qquad \text{и} \quad (a + \mathcal{J}) \odot (b + \mathcal{J}) = (ab) + \mathcal{J}.$$

Проверим, что эти операции определены корректно в том смысле, что они не зависят от выбора представителя в соответствующих классах вычетов. Пусть $a + \mathcal{J} = a' + \mathcal{J}$ и $b + \mathcal{J} = b' + \mathcal{J}$. Тогда $a' = a + j_a$, а $b' = b + j_b$, где $j_a \in \mathcal{J}$ и $j_b \in \mathcal{J}$ и, следовательно, выполняются равенства

$$(a' + \mathcal{J}) \oplus (b' + \mathcal{J}) = (a' + b') + \mathcal{J} = a + j_a + b + j_b + \mathcal{J} = \\ = a + b + (j_a + j_b + \mathcal{J}) = a + b + \mathcal{J} = (a + \mathcal{J}) \oplus (b + \mathcal{J}).$$

и, так как $aj_b \in \mathcal{J}$ и $j_a b \in \mathcal{J}$ (так как $\mathcal{J}$ – идеал),

$$(a' + \mathcal{J}) \odot (b' + \mathcal{J}) = (a'b') + \mathcal{J} = ab + aj_b + j_a b + j_a j_b + \mathcal{J} = \\ = ab + (aj_b + j_a b + j_a j_b \mathcal{J}) = ab + \mathcal{J} = (a + \mathcal{J}) \odot (b + \mathcal{J}).$$

Итак, операции $\oplus$ и $\odot$ сложения и умножения классов вычетов по модулю идеала $\mathcal{J}$ определены корректно. В дальнейшем, для сокращения обозначений, мы будем записывать операции сложения и умножения классов вычетов по модулю идеала $\mathcal{J}$ использую обычные символы операций сложения и умножения. Это не приведет ни к каким разночтениям так как из контекста всегда будет ясно, о каких операция идет речь.

Так как операции сложения и умножения над классами вычетов по модулю идеала $\mathcal{J}$ сводятся к соответствующим операциям над представителями этих классов, т.е. над элементами исходного кольца, то все аксиомы кольца выполнены для множества $\mathcal{R}/\mathcal{J}$ с операциями $+ = \oplus$ и $\cdot = \odot$. В самом деле, проверим, например, свойство дистрибутивности умножения относительно сложения. Пусть $a, b, c \in \mathcal{R}$. Тогда

$$\big((a + \mathcal{J}) + (b + \mathcal{J})\big)(c + \mathcal{J}) = ((a + b) + \mathcal{J})(c + \mathcal{J}) = (a + b)c + \mathcal{J} = (ac + bc) + \mathcal{J}$$

и, в тоже самое время,

$$\big((a + \mathcal{J})(c + \mathcal{J})\big) + \big((b + \mathcal{J})(c + \mathcal{J})\big) = (ac + \mathcal{J}) + (bc + \mathcal{J}) = (ac + bc) + \mathcal{J}.$$

Итак, множество $\mathcal{R}/\mathcal{J}$ с введенными операциями сложения и умножения классов вычетов по модулю идеала $\mathcal{J}$ является *кольцом.*

Определение. *Множество $\mathcal{R}/\mathcal{J}$ с введенными операциями сложения и умножения классов вычетов по модулю идеала $\mathcal{J}$ называется факторкольцом кольца $\mathcal{R}$ по идеалу $\mathcal{J}$.*

Замечание. Отображение $\pi : a \mapsto a + \mathcal{J}$, $a \in \mathcal{R}$ является эпиморфизмом колец $\mathcal{R} \to \mathcal{R}/\mathcal{J}$ с ядром $\operatorname{Ker} \pi = \mathcal{J}$.

Например, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ при $m \in \mathbb{Z}$ – кольцо вычетов по модулю m, а рассмотренное выше отображение $n \mapsto n_m$ – эпиморфизм колец $\mathbb{Z} \to \mathbb{Z}_m$ с ядром $m\mathbb{Z}$.

Применим теперь только что введенное понятие факторкольца к описанию всех возможных гомоморфных образов исходного кольца $\mathcal{R}$. Пусть $f : \mathcal{R} \to \mathcal{R}'$ – некоторый гомоморфизм кольца $\mathcal{R}$. Так как $\operatorname{Ran} f \subset \mathcal{R}'$, то, полагая $\mathcal{R}' = \operatorname{Ran} f$ мы, не ограничивая общности, можем считать, что f – эпиморфизм. Введем на $\mathcal{R}$ отношение $\sim_f$ следующим образом: элементы $a \in \mathcal{R}$ и $b \in \mathcal{R}$ эквивалентны, если $a - b \in \operatorname{Ker} f$. В качестве *упражнения* предлагается проверить, что $\sim_f$ – отношение эквивалентности на $\mathcal{R}$ и, что соответствующие классы эквивалентности – это классы вычетов по модулю идеала $\operatorname{Ker} f$.

Кроме того, отображение f, по определению, устанавливает биективное соответствие f' между элементами $a' \in \mathcal{R}'$ и классами вычетов по модулю $\operatorname{Ker} f$, а именно, $f'(a + \mathcal{J}) = a'$, если $f(a) = a'$. При этом для любых $a \in \mathcal{R}$ и $b \in \mathcal{R}$ справедливы равенства

$$f'((a + \mathcal{J}) + (b + \mathcal{J})) = f'((a + b) + \mathcal{J}) = f(a + b) = f(a) + f(b) = f'(a + \mathcal{J}) + f'(b + \mathcal{J})$$

и, соответственно,

$$f'((a + \mathcal{J})(b + \mathcal{J})) = f'((ab) + \mathcal{J}) = f(ab) = f(a)f(b) = f'(a + \mathcal{J})f'(b + \mathcal{J}).$$

Отсюда вытекает, что биективное отображение f' – это изоморфизм колец $\mathcal{R}/\mathcal{J}$ и $\mathcal{R}'$. Другими словами, нами установлено следующее утверждение.

Теорема 1.3. *Для любой идеала $\mathcal{J}$ кольца $\mathcal{R}$ определено факторкольцо $\mathcal{R}/\mathcal{J}$. Кольцо $\mathcal{R}/\mathcal{J}$ является гомоморфным образом кольца $\mathcal{R}$ при гомоморфизме π с ядром $\mathcal{J}$. Для любого гомоморфизма f кольца $\mathcal{R}$ справедливо соотношение* $\operatorname{Ran} f \cong \mathcal{R}/\operatorname{Ker} f$.

Замечание. Необходимо отличать произведение $(a+\mathcal{J})(b+\mathcal{J})$ классов вычетов по модулю идеала $\mathcal{J}$ от произведение множеств $a+\mathcal{J} = \{a+j : \ j \in \mathcal{J}\}$ и $b+\mathcal{J}$ в теоретико множественном смысле. В самом деле, рассмотрим в кольце $\mathbb{Z}$ идеал $8\mathbb{Z}$. Тогда $(4+8\mathbb{Z}) \odot (4+8\mathbb{Z}) = 16+8\mathbb{Z}$, а теоретико множественное произведение $A * B = \{ab : \ a \in A, \ b \in B\}$ множеств $4+8\mathbb{Z}$ и $4+8\mathbb{Z}$ равно $\{16+32s+32t+64st : \ s,t \in \mathbb{Z}\}$ а, например, число 24 принадлежит первому множеству (так как $24 = 16+8$), но не принадлежит второму (так как $24 \neq 16x$, $x \in \mathbb{Z}$).

1.3. Типы колец. Поля. Характеристика поля

Пусть $\mathcal{R}^* := \mathcal{R} \setminus \{0\}$ – множество всех ненулевых элементов кольца $\mathcal{R}$.

Отметим хорошо известное свойство целых, рациональных и вещественных чисел, которое знакомо нам из программы средней школы: если $ab = 0$ для двух чисел $a, b \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, то либо $a = 0$ либо $b = 0$. Это кажущееся естественным и всегда выполняющимся свойство на самом деле не так просто. Например, в кольце $M_n(\mathbb{R})$ оно не выполняется: легко сообразить, при каких целых индексах j, k, s, t произведение $E_{jk}E_{st}$ соответствующих матричных единиц равно нулевой матрице. Далее, в кольце $\mathbb{Z}_4$ справедливо равенство $2 \cdot 2 = 0$.

Упражнение. Показать, что множества $\mathbb{Z} \times \mathbb{Z}$ (соответственно, $\mathbb{Q} \times \mathbb{Q}$ и $\mathbb{R} \times \mathbb{R}$) являются коммутативными кольцами с единицей относительно операций $\oplus$ и $\otimes$, определенных соотношениями

$$(x,y) \oplus (u,v) = (x+u, y+v), \qquad (x,y) \otimes (u,v) = (xu, yv)$$

при $x, y, u, v \in \mathbb{Z}$ (соответственно, при $x, y, u, v \in \mathbb{Q}$ и при $x, y, u, v \in \mathbb{R}$).

Интересно отметить, что в кольцах $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q} \times \mathbb{Q}$, $\mathbb{R} \times \mathbb{R}$ имеет место равенство $(a,0) \otimes (0,b) = (0,0) = 0$.

Таким образом, примеров колец, в которых произведение ненулевых элементов может быть равно нулю достаточно много, и эти примеры не являются чем-то экзотическим. Соответственно оправдано введение следующего понятия.

Определение. *Пусть $\mathcal{R}$ – некоторое кольцо. Если $ab = 0$ при $a, b \in \mathcal{R}^*$, то a называется левым, а b правым делителями нуля в кольце $\mathcal{R}$. Если кольцо $\mathcal{R}$ коммутативно, то говорят просто о делителях нуля.*

Коммутативное кольцо с единицей и без делителей нуля называется целостным кольцом, или областью целостности.

Предложение 1.4. *Нетривиальное коммутативное кольцо $\mathcal{R}$ с единицей является целостным если и только если в $\mathcal{R}$ выполняется правило сокращения: если $a \in \mathcal{R}^*$, а $b, c \in \mathcal{R}$, то из равенства $ab = ac$ следует, что $b = c$.*

Доказательство. Пусть правило сокращения в кольце $\mathcal{R}$ выполняется. Тогда, если $ab = 0$ при $a, b \in \mathcal{R}^*$, то $ab = 0 = a0$ и, следовательно, $b = 0$. Аналогично, $ab = 0 = 0b$, откуда $a = 0$. В обоих случаях получается противоречие и, следовательно, $ab \neq 0$ при $a, b \in \mathcal{R}^*$. Обратно, если $\mathcal{R}$ – целостное кольцо, то из равенства $ab = ac$ при $a \in \mathcal{R}^*$ вытекает, что $ab - ac = a(b-c) = 0$. Далее, так как делителей нуля в $\mathcal{R}$ нет, то $b - c = 0$. Следовательно, $b = c$. $\square$

Определение. *Элемент x кольца $\mathcal{R}$ называется лево-обратимым, если существует такой элемент $x_\ell^{-1} \in \mathcal{R}$, называемый левым обратным для x, что $x_\ell^{-1}x = 1$. Аналогично, x называется право-обратимым, если существует такой элемент $x_r^{-1} \in \mathcal{R}$, называемый правым обратным для x, что $xx_r^{-1} = 1$.*

Элемент x кольца $\mathcal{R}$ называется обратимым, если существует такой элемент $x^{-1} \in \mathcal{R}$, что $xx^{-1} = x^{-1}x = 1$.

Предложение 1.5. *В коммутативных кольцах и в кольцах без делителей нуля всякий лево-обратимый элемент право-обратим и наоборот. При этом правый и левый обратные совпадают. Кроме того, обратимый элемент кольца не может быть делителем нуля.*

Доказательство. В коммутативном кольце $\mathcal{R}$ утверждение очевидно. В самом деле, пусть элемент $x \in \mathcal{R}$ лево-обратим. Следовательно, существует левый обратный x_ℓ^{-1} такой, что $x_\ell^{-1}x = 1$. Но в силу коммутативности кольца $\mathcal{R}$, $xx_\ell^{-1} = x_\ell^{-1}x = 1$ и, следовательно, элемент x_ℓ^{-1} является и правим обратным для x.

Если $\mathcal{R}$ произвольное кольцо без делителей нуля, то дело обстоит не намного сложнее. В самом деле, из существования левого обратного элемента x_ℓ^{-1} для элемента $x \in \mathcal{R}$ вытекает, что $x_\ell^{-1}x = 1$. Следовательно, $x_\ell^{-1}xx_\ell^{-1} = x_\ell^{-1}$, откуда $x_\ell^{-1}(xx_\ell^{-1} - 1) = 0$ и, так как в $\mathcal{R}$ нет делителей нуля, то $xx_\ell^{-1} - 1 = 0$. Отсюда вытекает, что $xx_\ell^{-1} = 1$, т.е. элемент x_ℓ^{-1} является право-обратным к x.

Случай, когда x право-обратим рассматривается аналогично.

Проверим теперь, что обратимый элемент кольца не является делителем нуля. В самом деле, пусть для элемента $x \in \mathcal{R}$ существует обратный x^{-1}. Тогда, если $xy = 0$, то $x^{-1}xy = 0$ и, следовательно, $y = 0$. Аналогично, если $yx = 0$, то $yxx^{-1} = 0$ и, как и раньше, $y = 0$. □

Предложение 1.6. *Пусть $\mathcal{R}$ – произвольное кольцо с единицей, а $U(\mathcal{R})$ – совокупность всех обратимых элементов из $\mathcal{R}$. Тогда $U(\mathcal{R})$ образует группу относительно операции умножения в $\mathcal{R}$.*

Доказательство. Ясно, что $1 \in U(\mathcal{R})$. Далее, если $a \in U(\mathcal{R})$, то существует $a^{-1} \in \mathcal{R}$ такой, что $aa^{-1} = a^{-1}a = 1$. Но эти два равенства можно воспринимать и как проверку обратимости элемента a^{-1} в $\mathcal{R}$ (соответствующий обратный равен a). Следовательно, $a^{-1} \in U(\mathcal{R})$. Заметим также, что операция умножения на $U(\mathcal{R})$ является ассоциативной (так как она ассоциативна на всем $\mathcal{R}$). Для завершения доказательства этого предложения нам остается проверить, что $U(\mathcal{R})$ замкнута относительно операции умножения. Пусть $a, b \in \mathcal{R}$ – обратимые элементы кольца $\mathcal{R}$, т.е. существуют $a^{-1}, b^{-1} \in \mathcal{R}$. В силу общих свойств степени,

$$(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aa^{-1} = 1, \qquad (b^{-1}a^{-1})(ab) = b^{-1}a^{-1}ab = b^{-1}b = 1$$

и, следовательно, элемент $b^{-1}a^{-1}$ – обратный элемент для ab. □

Пример 1.7. $U(\mathbb{Z}) = \{-1, 1\} = Z_2 = \langle -1 \rangle$ – циклическая группа порядка 2.

Определение. *Кольцом с делением (или телом) называется такое кольцо $\mathcal{R}$, для которого $\mathcal{R}^*$ является группой по умножению.*

Поле – это коммутативное кольцо $\mathcal{F}$ с единицей $1 \neq 0$ без делителей нуля в котором каждый элемент $x \in \mathcal{F}^*$ обратим. При этом группа $U(\mathcal{F}) = \mathcal{F}^*$ называется мультипликативной группой поля.

Таким образом, поле можно рассматривать как некий специальный "гибрид" двух абелевых групп – аддитивной и мультипликативной – связанных между собой правилом дистрибутивности. На самом деле, числовое поле это наиболее естественный с точки зрения человеческой интуиции тип числовых множеств, которые могут применяться в повседневных вычислениях. Это связано с тем, что в полях работают все

четыре арифметических действия причем так, как мы привыкли к этому, работая с множествами рациональных, вещественных или комплексных чисел.

Определение. *Пусть $\mathcal{F}$ – поле, $a \in \mathcal{F}$ и $b \in \mathcal{F}^*$. Выражение $\frac{a}{b} = a/b := ab^{-1}$ называется дробью.*

Предложение 1.8. *В произвольном поле $\mathcal{F}$ все стандартные операции с дробями (сложение, умножение, вычитание, деление) подчиняются следующим правилам:*

$$\frac{a}{b} = \frac{c}{d} \Longleftrightarrow ad = bc, \quad \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad -\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}, \quad \frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}, \quad \left(\frac{a}{b}\right)^{-1} = \frac{b}{a},$$

где $a, c \in \mathcal{F}$, $b, d \in \mathcal{F}^*$, а в последнем равенстве $a \neq 0$.

Упражнение. Доказать Предложение 1.8.

Упражнение. Проверить, что множества рациональных чисел $\mathbb{Q}$, вещественных чисел $\mathbb{R}$ и комплексных чисел $\mathbb{C}$ со стандартными операциями сложения и умножения, определенными для рациональных, вещественных и комплексных чисел соответственно, образуют поля.

Определение. *Если $\mathcal{F}$ и $\mathcal{F}'$ – поля, причем $\mathcal{F}' \subset \mathcal{F}$, то поле $\mathcal{F}'$ называется подполем поля $\mathcal{F}$, а поле $\mathcal{F}$ – расширением поля $\mathcal{F}'$.*

Например, поле рациональных чисел $\mathbb{Q}$ является подполем поля $\mathbb{R}$.

Замечание. Если $\mathcal{F}'$ – подполе поля $\mathcal{F}$, то 0 и 1 поля $\mathcal{F}'$ будут в $\mathcal{F}$ нулем и единицей.

Пусть теперь задана некоторое поле $\mathcal{F}$ и его подполе $\mathcal{F}_0$. Возьмем некоторый элемент $a \in \mathcal{F} \setminus \mathcal{F}_0$ и рассмотрим пересечение $\mathcal{F}_0(a) := \bigcap \mathcal{F}'$ всех полей $\mathcal{F}'$ таких, что $\mathcal{F}' \subset \mathcal{F}$ – подполе поля $\mathcal{F}$, $\mathcal{F}_0 \subset \mathcal{F}'$ и $a \in \mathcal{F}'$. Так как же, как и в случае пересечения семейств групп и колец проверяется, что $\mathcal{F}_0(a)$ является полем. Более того, по построению поле $\mathcal{F}_0(a)$ является минимальным подполем поля $\mathcal{F}$, содержащим $\mathcal{F}_0$ и a.

Определение. *Поле $\mathcal{F}_0(a)$ называется расширением поля $\mathcal{F}_0$ на элемент $a \in \mathcal{F} \setminus \mathcal{F}_0$. Аналогично вводится расширение $\mathcal{F}_0(a_1, \ldots, a_m)$ поля $\mathcal{F}_0$ на конечное множество элементов $a_1, \ldots, a_m \in \mathcal{F} \setminus \mathcal{F}_0$.*

Упражнение. Проверить, что $\mathbb{Q}(\sqrt{2})$ – расширение поля $\mathbb{Q}$ на элемент $\sqrt{2}$ в точности совпадает с множеством $\{p + q\sqrt{2} : \ p, q \in \mathbb{Q}\}$ операции сложения и умножения на котором заданы равенствами

$$(p_1 + q_1\sqrt{2}) + (p_2 + q_2\sqrt{2}) = (p_1 + p_2) + (q_1 + q_2)\sqrt{2},$$
$$(p_1 + q_1\sqrt{2}) \times (p_2 + q_2\sqrt{2}) = (p_1p_2 + 2q_1q_2) + (p_1q_2 + p_2q_1)\sqrt{2}.$$

Определение. *Поля $\mathcal{F}_1$ и $\mathcal{F}_2$ изоморфны, если они изоморфны как кольца.*

Замечание. В отличии от весьма содержательного (как будет ясно из последующего изложения) понятия изоморфизма полей, рассматривать гомоморфизмы полей смысла не имеет. В самом деле, пусть $f : \mathcal{F}_1 \to \mathcal{F}_2$ – гомоморфизм и пусть $\operatorname{Ker} f \neq \{0\}$. Тогда существует элемент $a \in \mathcal{F}_1^*$ такой, что $f(a) = 0$. Так как $a \neq 0$, то существует $a^{-1} \in \mathcal{F}$ и $f(1) = f(aa^{-1}) = f(a)f(a^{-1}) = 0$. Далее, для любого $b \in \mathcal{F}_1$ имеем $f(b) = f(b1) = f(b)f(1) = 0$. Таким образом, если ядро f ненулевое, то оно совпадает со всем полем $\mathcal{F}_1$.

Пример 1.9. Ранее было установлено, что все автоморфизмы аддитивной группы $\mathbb{Q}$ имеют вид $f : q \mapsto cq$, где $c \in \mathbb{Q}^*$ – некоторое ненулевое рациональное число. Соответственно, все автоморфизмы поля $\mathbb{Q}$ рациональных чисел надо искать среди таких отображений. Так как автоморфизм поля должен сохранять еще и произведение, то для любого $q \in \mathbb{Q}$, $q \neq 0$, получаем $cq^2 = f(q^2) = f(q)f(q) = c^2q^2$. Из этого видно, что $c^2 = c$ и, так как $c \neq 0$, то $c = 1$. Итак, поле рациональных чисел имеет единственный автоморфизм – тождественный.

Рассмотрим теперь автоморфизмы поля $\mathbb{R}$ вещественных чисел. Пусть $f : \mathbb{R} \to \mathbb{R}$ – автоморфизм, т.е. отображение f биективно и для любых $x, y \in \mathbb{R}$ верны равенства $f(x+y) = f(x)+f(y)$ и $f(xy) = f(x)f(y)$. Так как же, как и при вычислении автоморфизмов поля $\mathbb{Q}$ доказывается, что $f(q) = q$ для всех $q \in \mathbb{Q}$. Вспомним далее, что поле $\mathbb{R}$ упорядочено. Если $x > 0$, то $x = d^2$, $d \in \mathbb{R}$ и $f(x) = f(d^2) = (f(d))^2 > 0$. Таким образом, автоморфизм сохраняет отношение порядка на $\mathbb{R}$ – в самом деле, если $x, y \in \mathbb{R}$ и $x > y$, то $x-y > 0$ и $f(x) = f(x-y)+f(y) > f(y)$. Из этого факта и из того, что рациональные числа всюду плотны в $\mathbb{R}$ вытекает, что $f \equiv \mathrm{id}$. Проверка этого оставляется в качестве *упражнения*.

Характеристика поля. Рассмотрим снова кольцо $\mathbb{Z}_m$, $m \in \mathbb{N}$, $m > 1$. Считая m фиксированным, для произвольного $n \in \mathbb{Z}$ введем обозначение $\overline{n} = n \pmod m$. Тогда $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$, а операции сложения и умножения можно записать следующим образом: $\overline{k} + \overline{n} = \overline{k+n} = (k+n) \pmod m$ и $\overline{k} \times \overline{n} = \overline{kn} = (kn) \pmod m$. Убедимся, что в кольце $\mathbb{Z}_m$ существуют делители нуля. В самом деле, если $s, r \in \mathbb{N}$ таковы, что $sr = m$, $s > 1$, $r > 1$, то $\overline{s} \times \overline{r} = \overline{m} = \overline{0}$. Т.е. $\overline{s}$ и $\overline{r}$ – делители нуля в $\mathbb{Z}_m$. Однако такое разложение числа m в произведение возможно только если m составное число. Имеет место следующее утверждение.

Предложение 1.10. *Если p – простое число, то $\mathbb{Z}_p$ – поле.*

Доказательство. Для проверки того, что $\mathbb{Z}_p$ поле нам достаточно установить существование обратного элемента для любого элемента $\overline{n} \in \mathbb{Z}_p^*$. Заметим, что числа n и r, где $\overline{r}$ – обратный элемент для $\overline{n}$, не должны делится на p. Рассмотрим элементы

$$\overline{n}, \quad \overline{2n}, \quad \ldots, \quad \overline{(p-2)n}, \quad \overline{(p-1)n}. \tag{1.1}$$

Заметим, что все они отличны от нуля так как из $n \not\equiv 0 \pmod m$ вытекает, что $nk \not\equiv 0 \pmod m$ при $k = 1, \ldots, p-1$. Заметим далее, что все рассматриваемые элементы различны, так как если $\overline{k_1 n} = \overline{k_2 n}$ при $k_1 < k_2$, то $\overline{(k_2 - k_1)n} = 0$, а это неверно. Итак, совокупность (1.1) состоит из $p-1$ различных ненулевых элементов из $\mathbb{Z}_p$. Следовательно, в этой совокупности содержаться (причем по одному разу) все ненулевые элементы из $\mathbb{Z}_p$. В частности, существует такое $r \in \{1, 2, \ldots, p-1\}$, что $\overline{nr} = \overline{1}$. Элемент $\overline{r}$ и будет обратным к $\overline{n}$. □

На самом деле можно утверждать большее. А именно, справедливо следующее утверждение.

Теорема 1.11. *Кольцо вычетов $\mathbb{Z}_m$, $m \in \mathbb{N}$, $m > 1$, является полем если и только если m – простое число.*

В Предложении 1.10 уже установлено, что если m – простое число, то $\mathbb{Z}_m$ – поле. В самом начале этого раздела было показано, что если m составное число, то в $\mathbb{Z}_m$ имеются делители нуля. Таким образом, при составных m кольцо $\mathbb{Z}_m$ полем быть не может по определению.

Упражнение. Проверить, что если $a \in \mathbb{Z}$ – произвольное целое число, а p – простое число такое, что $p \nmid a$, то $a^{p-1} \equiv 1 \pmod p$. Это утверждение носит название *малой теоремы Ферма*.

Определение. *Подполе $\mathcal{F}_0$ поля $\mathcal{F}$ называется собственным, если $\mathcal{F}_0 \neq \mathcal{F}$. Поле, не содержащее никакого собственного подполя, называется простым.*

Теорема 1.12. *В каждом поле $\mathcal{F}$ содержится одно и только одно простое подполе $\mathcal{F}_0$. Это подполе изоморфно либо полю $\mathbb{Q}$ либо полю $\mathbb{Z}_p$ при некотором простом p.*

Доказательство. Начнем с проверки единственности простого подполя.

Пусть некоторое поле $\mathcal{F}$ содержит два различных простых поля $\mathcal{F}_1$ и $\mathcal{F}_2$. Тогда $\mathcal{F}_1 \cap \mathcal{F}_2$ будет подполем поля, а также подполем полей $\mathcal{F}_1$ и $\mathcal{F}_2$. При этом $0, 1 \in \mathcal{F}_1 \cap \mathcal{F}_2$

и, следовательно, $\mathcal{F}_1 \cap \mathcal{F}_2 \neq \varnothing$. Таким образом получено противоречие с простотой полей $\mathcal{F}_1$ и $\mathcal{F}_2$ и, следовательно, простое подполе $\mathcal{F}_0$ единственно.

Проверим теперь существование $\mathcal{F}_0$ и утверждение о его структуре. В поле $\mathcal{F}$ рассмотрим единицу и все ее кратные, т.е. элементы вида $n1$, где $n \in \mathbb{Z}$. Легко проверить, что при $n, k \in \mathbb{Z}$ имеют место равенства $(n1) + (k1) = (n+k)1$, $(n1) \times (k1) = (nk)1$. Отсюда следует, что отображение $\mathbb{Z} \to \mathcal{F}$ определенное по правилу $f(n) = n1$ является гомоморфизмом. Рассмотрим его ядро $\operatorname{Ker} f$. Найдется такое $m \in \mathbb{Z}_+$ такое, что $\operatorname{Ker} f = m\mathbb{Z}$.

Если $m = 0$, то f – мономорфизм. В этом случае дроби $(k1)/(n1)$ определены в $\mathcal{F}$ и, как несложно проверить исходя из аксиом поля, образуют в $\mathcal{F}$ некоторое подполе $\mathcal{F}_0$. При этом ясно, что $\mathcal{F}_0 \cong \mathbb{Q}$ и, что $\mathcal{F}_0$ – простое поле. Последнее вытекает из того, что наряду с 1 поле $\mathcal{F}_0$ обязано содержать все ее кратные, т.е. элементы вида $n1$, $n \in \mathbb{Z}$ и, следовательно, все дроби вида $(k1)/(n1)$, $k, n \in \mathbb{Z}$.

Пусть теперь $m > 0$. В этом случае отображение $f_1 : \mathbb{Z}_m \to \mathcal{F}$, определенное по правилу $f(\{k\}_m) = f(k)$ будет изоморфным вложением $\mathbb{Z}_m$ в $\mathcal{F}$. Это возможно однако, если и только если p – простое число (так как изоморфный образ поля обязан быть полем). Следовательно, $f_1(\mathbb{Z}_p)$ – простое подполе в $\mathcal{F}$. □

Определение. *Говорят, что поле $\mathcal{F}$ имеет характеристику ноль, если простое подполе $\mathcal{F}_0$ поля $\mathcal{F}$ изоморфно полю $\mathbb{Q}$. Далее, говорят что поле $\mathcal{F}$ имеет простую характеристику p, если его простое подполе $\mathcal{F}_0$ изоморфно полю $\mathbb{Z}_p$.*

Итак, всякое поле имеет характеристику ноль или простую характеристику. Однако часто поля характеристики ноль называют полями, имеющими бесконечную характеристику.

1.4. Единственность поля комплексных чисел

Как известно, уравнение $x^2 + 1$ не имеет корней в поле вещественных чисел $\mathbb{R}$. Применим описанную выше процедуру алгебраического расширения поля к полю $\mathbb{R}$ и элементу $j \notin \mathbb{R}$ – корню уравнения $x^2 + 1 = 0$. Получим некоторое расширение $\mathbb{R}(j)$ поля $\mathbb{R}$. Оказывается, что в этом случае верно следующее утверждение.

Теорема 1.13. *Пусть $\mathcal{F} \cong \mathbb{R}$ – поле и пусть $\widetilde{\mathcal{F}}$ – расширение поля $\mathcal{F}$, полученное присоединением корня j уравнения $x^2 + 1 = 0$ к $\mathcal{F}$. Тогда $\widetilde{\mathcal{F}} \cong \mathbb{C}$.*

Доказательство. По определению, поле $\widetilde{\mathcal{F}} = \mathcal{F}(j)$ – минимальное подполе некоторого поля $\mathcal{F}_1$, содержащего $\mathcal{F}$ и j. Рассмотрим множество $\mathcal{F}_j = \{a+jb : \ a, b \in \mathcal{F}\} \subset \mathcal{F}_1$. Первым делом заметим, что если $(a, b) \neq (a', b')$, то $a + jb \neq a' + jb'$. В самом деле, если это не так, то существует пара $(a_0, b_0) \neq (0, 0$ такая, что $a_0 + jb_0 = 0$. В этом случае, $b_0 \neq 0$ (так как иначе и $a_0 = 0$). А раз так, то $j = -a_0/b_0$, что невозможно, так как $j \notin \mathcal{F}$. Далее, заметим, что в поле $\mathcal{F}_1$ верны следующие равенства

$$(a_1+jb_1)+(a_2+jb_2) = (a_1+a_2)+j(b_1+b_2), \quad (a_1+jb_1)(a_2+jb_2) = (a_1a_2-b_1b_2)+j(a_1b_2+a_2b_1)$$

для любых $a_1 + jb_1 \in \mathcal{F}_j$ и $a_2 + jb_2 \in \mathcal{F}_j$. Из этих равенств непосредственно выводится, что $(a+jb)^{-1} = \frac{a}{a^2+b^2} + j\frac{-b}{a^2+b^2}$ для любого $a + jb \in \mathcal{F}_j^*$. Таким образом, $\mathcal{F}_j$ – это подполе поля $\mathcal{F}_1$ такое, что $\mathcal{F}_j$ содержит $\mathcal{F}$ и j. По построению поля $\mathcal{F}_j$ и в силу минимальности $\widetilde{\mathcal{F}}$ получаем, что $\widetilde{\mathcal{F}} = \mathcal{F}_j$. Пусть теперь $f : \mathcal{F} \to \mathbb{R}$ данный нам по условию изоморфизм полей. Тогда отображение $F : (a + jb) \mapsto (f(a) + if(b))$ будет, как легко проверить, изоморфизмом $\widetilde{\mathcal{F}}$ и $\mathbb{C}$. □

Интересно и полезно выразить факт единственности поля комплексных чисел в следующей форме.

Предложение 1.14. *Всякое коммутативное кольцо $\mathcal{R}$ с единицей и без делителей нуля, являющееся двумерным линейным пространством над $\mathbb{R}$, изоморфно полю $\mathbb{C}$.*

Доказательство. Без ограничения общности можно считать, что $\mathbb{R} \subset \mathcal{R}$. Из того, что $\dim_{\mathbb{R}} \mathcal{R} = 2$ следует, что существует элемент $w \in \mathcal{R} \setminus \mathbb{R}$ такой, что $\{1, w\}$ – базис линейного пространства $\mathcal{R}$. Пусть, далее, $w^2 = \alpha + 2\beta w$. При этом элемент $y = e - \beta \notin \mathbb{R}$, но $y^2 = \alpha + \beta^2 \in \mathbb{R}$. Заметим, что при этом $\gamma := \alpha + \beta^2 < 0$. В самом деле, если $\gamma \geqslant 0$, то $\sqrt{\gamma} \in \mathbb{R}$ и, следовательно, $y \in \mathbb{R}$. Так что найдется $\delta \in \mathbb{R}$, $\delta \neq 0$, такое, что $\delta^2 = -\gamma^{-1}$. Далее, из этого следует, что элемент $j := \delta y$ удовлетворяет условию $j^2 = -1$. Пусть теперь $a + bw$ – произвольный элемент из $\mathcal{R}$. Тогда $a + bw = a_1 + jb_1$, где $a_1 = (a + b\beta)$ и $b_1 = b\delta^{-1}$ и, если $a_1 = b_1 = 0$, то легко проверить, что $a = b = 0$. Так как любой элемент $\mathcal{R}$ записан в виде $a_1 + jb_1$, где $j^2 = -1$, то, аналогично тому, как это было проделано в доказательстве предыдущей теоремы, проверяется, что любой ненулевой элемент в $\mathcal{R}$ обратим. Таким образом, $\mathcal{R}$ является полем и отображение $f : a + jb \mapsto a + ib$ является, очевидно, изоморфизмом полей $\mathcal{R}$ и $\mathbb{C}$. □

Упражнение. Покажите, где в доказательстве Предложения 1.14 было использовано отсутствие делителей нуля в $\mathcal{R}$.

1.5. Делимость в кольцах, общий подход

Рассмотрим с несколько более общих позиций хорошо известные свойства делимости целых чисел. Пусть $\mathcal{R}$ — некоторое кольцо, относительно которого мы будем предполагать выполнение тех или иных свойств (например, коммутативность или целостность) при необходимости.

Определение. *Элемент $b \in \mathcal{R}$ делится на $a \in \mathcal{R}$, если существует $c \in \mathcal{R}$ такой, что $b = ac$. В этом случае также говорят, что b кратен a и пишут $a \mid b$. Если элементы $a, b \in \mathcal{R}$ таковы, что $a \mid b$ и $b \mid a$, то говорят, что a и b ассоциированы.*

Пусть элементы a и b кольца $\mathcal{R}$ ассоциированы. Тогда $b = c_1 a$ и $a = c_2 b$ для некоторых элементов $c_1, c_2 \in \mathcal{R}$. Тогда $b = c_1 a = c_1 c_2 b$ и, так как кольцо $\mathcal{R}$ целостное, то $c_1 c_2 = 1$. Отсюда вытекает, что если элементы a и b кольца $\mathcal{R}$ ассоциированы, то $b = ua$, где $u \mid 1$ – обратимый элемент в $\mathcal{R}$. Итак, ассоциированные элементы отличаются друг от друга на обратимый множитель.

Определение. *Элемент $p \in \mathcal{R}$ называется простым или неразложимым, если p необратим в $\mathcal{R}$ и его нельзя представить в виде $p = ab$, где $a, b \in \mathcal{R}$ – необратимые элементы.*

Замечание. В поле все ненулевые элементы обратимы и, следовательно, в поле нет простых элементов.

Упражнение. Проверить, что имеют место следующие свойства делимости в кольце $\mathcal{R}$. Пусть $a, b, c \in \mathcal{R}$. Тогда

(1) если $a \mid b$ и $b \mid c$, то $a \mid c$;
(2) если $c \mid a$ и $c \mid b$, то $c \mid (a \pm b)$;
(3) если $a \mid b$, то $a \mid bc$ для любого $c \in \mathcal{R}$.

Важным свойством колец является возможность разложения элементов на простые множители. В связи с этим введем следующее определение:

Определение. *Целостное кольцо $\mathcal{R}$ называется кольцом с разложением (или, более точно, кольцом с разложением на простые множители), если для любого $a \in \mathcal{R}^*$ элемент a может быть представлен в виде*

$$u \times p_1 \times \cdots \times p_m, \tag{1.2}$$

где элемент u обратим в $\mathcal{R}$, а все элементы p_j простые (но не обязательно попарно различные).

Это свойство кажется тривиальным, однако это не так.

Упражнение. Назовем комплексное число *целым алгебраическим*, если оно является корнем некоторого многочлена с целыми коэффициентами, старший коэффициент которого равен 1 (например, число $\sqrt{2}$ является целым алгебраическим, так как оно является корнем многочлена x^2-2, а число $1/\sqrt{2}$ — нет). Доказать, что совокупность всех целых алгебраических чисел образует кольцо относительно обычных операций сложения и умножения.

Упражнение. Проверить, что число $\sqrt{2}$ в кольце целых алгебраических чисел не обратимо и не допускает разложения на простые множители.

Утверждения, содержащиеся в двух вышеприведенных упражнениях, оправдывают следующее определение.

Определение. *Кольцо с разложением $\mathcal{R}$ называется факториальным кольцом (или кольцом с однозначным разложением на простые множители), если для произвольного элемента $a\in\mathcal{R}^*$ его разложение вида (1.2) единственно в том смысле, что если $up_1\times\dots\times p_m$ и $wq_1\times\dots\times q_k$ — два таких разложения элемента a, то $m=k$ и $q_j=u_jp_j$ для любого $j=1\dots m$, где u_j — некоторый обратимый элемент кольца $\mathcal{R}$.*

Установим следующее характеристическое свойство факториального кольца.

Предложение 1.15. *Кольцо с разложением $\mathcal{R}$ является факториальным кольцом если и только если для любого простого элемента $p\in\mathcal{R}$ из того, что $p\mid(ab)$ вытекает, что $p\mid a$ или $p\mid b$.*

Доказательство. Пусть $\mathcal{R}$ – факториальное кольцо и пусть $ab=pc$, где c – некоторый элемент из $\mathcal{R}$. Так как $\mathcal{R}$ факториально, то a, b и c единственным образом представляются разложениями $a=\prod_{j=1}^{J}a_j$, $b=\prod_{k=1}^{K}b_k$ и $c=\prod_{\ell=1}^{L}c_\ell$ вида (1.2). Тогда произведения $a_1\times\dots\times a_J\times b_1\times\dots b_K$ и $p\times c_1\times\dots\times c_L$ – это представления в виде (1.2) элемента ab и, следовательно, из определения факториальности кольца $\mathcal{R}$ вытекает, что p ассоциирован с одним из простых множителей a_j, $j=1\dots J$ или b_k, $k=1\dots K$. А это в точности означает, что $p\mid a$ или $p\mid b$.

Докажем теперь обратную импликацию. Воспользуемся индукцией по числу элементов в разложении (1.2). Ясно, что любое простое число представляется в виде (1.2) с одним простым и одним обратимым множителем (это непосредственно вытекает из определения простого элемента в $\mathcal{R}$). Предположим теперь, что единственность (с точностью до порядка следования и ассоциированности множителей) разложения установлена на всех чисел, имеющих в своем разложении вида (1.2) не более n простых множителей. Из этого нам необходимо заключить, что единственность будет и для разложений, в которых задействовано $n+1$ простых множителей. Пусть некоторый элемент $a\in\mathcal{R}^*$ имеет два различных разложения

$$a=\prod_{j=1}^{n+1}p_j=\prod_{k=1}^{n+1}q_k$$

вида (1.2). Тогда, из условия доказываемого предложения вытекает, что $p_{n+1}\mid q_k$ при некотором $k=1,\dots,(n+1)$. Без ограничения общности считаем, что $k=n+1$. Отсюда вытекает, что $\prod_{j=1}^{n}p_j=\prod_{k=1}^{n}q_k$. По предположению индукции из этого равенства вытекает, что $p_1,\dots,p_n$ и $q_1,\dots,q_n$ – это один и тот же набор простых элементов (с точностью до смены нумерации и ассоциированности элементов). □

Пример 1.16. Рассмотрим поле $\mathbb{Q}(\sqrt{-11})$ и содержащееся в нем целостное кольцо $\mathcal{K}=\{a+b\sqrt{-11}:\ a,b\in\mathbb{Z}\}$. Проверка того, что кольцо $\mathcal{K}$ целостное оставляется в качестве *упражнения*. Найдем обратимые элементы в $\mathcal{K}$. Пусть для элемента $\xi=a+b\sqrt{-11}\in\mathcal{K}$ существует обратный $\zeta=x+y\sqrt{-11}\in\mathcal{K}$. Тогда $\xi\zeta=(ax-11by)+(ay+bx)\sqrt{-11}=1$ и

$$ax-11by=1,\quad bx+ay=0.$$

из этих уравнений находим $x = a/(a^2+11b^2)$ и $y = -b/(a^2+11b^2)$. Заметим, что величина $N(\xi) = a^2 + 11b^2$ – это целое положительное число для любого $\xi \neq 0$ и, следовательно, элемент $x + y\sqrt{-11} \in \mathcal{K}$ только при $x \in \mathbb{Z}$ и $y \in \mathbb{Z}$. А из этого условия легко вытекает, что $a = \pm 1$, а $b = 0$. Итак, обратимыми элементами в $\mathcal{K}$ являются ± 1.

Величину $N(\xi)$ называют нормой элемента $\xi \in \mathcal{K}$.

Проверим, что $\mathcal{K}$ является кольцом с разложением. Легко проверить (это оставляется в качестве *упражнения*), что если $\xi, \xi_1, \ldots, \xi_k \in \mathcal{K}^*$ таковы, что $\xi = \pm 1 \times \xi_1 \times \cdots \times \xi_k$, то $N(\xi) = N(\xi_1) \times \cdots \times N(\xi_k)$. Так как $N(\eta) > 1$ при $\eta \in \mathcal{K}^*$, то число множителей k в разложении элемента ξ не может расти бесконечно. Следовательно, $\mathcal{K}$ является кольцом с разложением.

Однако, $\mathcal{K}$ не является факториальным кольцом. В самом деле, имеем место равенство

$$3 \times 5 = 15 = (2 + \sqrt{-11}) \times (2 - \sqrt{-11}),$$

а элементы 3 и $2 \pm \sqrt{-11}$ и 5 и $2 + \pm\sqrt{-11}$, очевидно, не ассоциированы. Остается проверить, что элементы $3, 5, 2 \pm \sqrt{-11}$ просты в $\mathcal{K}$. Проверим это на примере числа 3. Пусть существуют необратимые $\zeta_1, \zeta_2 \in \mathcal{K}$ такие, что $\zeta_1\zeta_2 = 3$. Тогда $9 = N(3) = N(\zeta_1)N(\zeta_2)$. Так как $N(\zeta_{1,2}$ – это целые числа, отличные от ± 1 (в силу необратимости ζ_1 и ζ_2), то $N(\zeta_1) = N(\zeta_2) = 3$. Следовательно, $\zeta_{1,2} = x_{1,2} + y_{1,2}\sqrt{-11}$, $x_{1,2}, y_{1,2} \in \mathbb{Z}$, где $x_{1,2}^2 + 11y_{1,2}^2 = 3$. А это уравнение целочисленных решений не имеет.

Итак, элемент $15 \in \mathcal{K}$ имеет в $\mathcal{K}$ два различных разложения на простые множители и, следовательно, кольцо $\mathcal{K}$ не факториально.

Квадратичные кольца. Пусть $d \in \mathbb{Z}$, причем $d \neq 1$ и d *свободно от квадратов*, т.е. d не делится на квадрат никакого простого числа. Легко проверить, что множество $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : \ a, b \in \mathbb{Q}\}$ является полем относительно стандартных операций сложения и умножения (комплексных) чисел (разумеется, при $d < 0$ мы полагаем $\sqrt{d} = i\sqrt{|d|}$).

Заметим, что поле $\mathbb{Q}(\sqrt{d})$ имеет только два автоморфизма: тождественный автоморфизм и автоморфизм $\phi : a + b\sqrt{d} \mapsto a - b\sqrt{d}$ (проверка этого факта оставляется в качестве упражнения).

Для любого $\alpha \in \mathbb{Q}(\sqrt{d})$ определим числа $N(\alpha) = a^2 - db^2$ (норму элемента α) и $T(\alpha) = 2a$ (след элемента α). Заметим, что $N(\alpha) = \alpha\phi(\alpha)$ и, если $d < 0$, то $N(\alpha) = \alpha\overline{\alpha}$, где черта означает обычное комплексное сопряжение.

Определим множество

$$\mathbb{Z}[\sqrt{d}] = \{\alpha \in \mathbb{Q}(\sqrt{d}) : \ N(\alpha) \in \mathbb{Z}, \ T(\alpha) \in \mathbb{Z}\}.$$

Упражнение. Проверить, что $\mathbb{Z}[\sqrt{d}]$ является кольцом (относительно операций сложения и умножения комплексных чисел) и, что это множество состоит из всех элементов поля $\mathbb{Q}(\sqrt{d})$, являющихся целыми алгебраическими числами.

Определение. *Множество $\mathbb{Z}[\sqrt{d}]$ называется квадратичным кольцом. В случае $d \geqslant 0$ это кольцо называется действительным квадратичным кольцом, а при $d < 0$ — комплексным квадратичным кольцом.*

Задача 1.1. Показать, что если $d \equiv 2 \pmod 4$ или $d \equiv 3 \pmod 4$, то $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : \ a, b \in \mathbb{Z}\}$, а если $d \equiv 1 \pmod{()4}$, то $\mathbb{Z}[\sqrt{d}] = \{\frac{a}{2} + \frac{b}{2}\sqrt{d} : \ a, b \in \mathbb{Z}, \ 2 \mid (x - y)\}$.

Заметим, что кольцо $\mathcal{K}$, определенное в примере 1.16 отличается от кольца $\mathbb{Z}[\sqrt{-11}]$.

Задача 1.2. Доказать, что кольца $\mathbb{Z}[\sqrt{d}]$ являются целостными кольцами.

Задача 1.3. Вычислить группу $U(\mathbb{Z}[\sqrt{d}])$ обратимых элементов кольца $\mathbb{Z}[\sqrt{d}]$ при $d = -1, -2, -3$. Как описать обратимые элементы в $\mathbb{Z}[\sqrt{d}]$ при общем $d < 0$?

Рассмотрим еще один пример, связанный с примером 1.16. В кольце $\mathbb{Z}[i]$ число 5 имеет два формально различных разложения:

$$(1-2i)(1+2i) = 5 = (-2-i)(-2+i)$$

Однако легко проверить, что эти разложения содержат ассоциированные множители — обратимыми элементами в $\mathbb{Z}[i]$ будут ± 1 и $\pm i$, а $1-2i = i(-2-i)$ и $(1+2i) = -i(-2+i)$.

НОД и НОК в кольцах. Пусть $\mathcal{R}$ – целостное кольцо.

Определение. *Наибольшим общим делителем двух элементов $a, b \in \mathcal{R}$ называется такой элемент $d \in \mathcal{R}$, что*

(1) $d \mid a$, $d \mid b$;
(2) *если* $c \mid a$ *и* $c \mid b$ *для некоторого* $c \in \mathcal{R}$, *то* $c \mid d$.

Наибольший общий делитель обозначается символом $\gcd(a, b)$ *или символом* $\text{НОД}(a, b)$.

Замечание. Если $\text{НОД}(a, b) = d$, то свойствами $d \mid a$, $d \mid b$ и если $c \mid a$ и $c \mid b$ для некоторого $c \in \mathcal{R}$, то $c \mid d$ обладает, наряду с d и любой ассоциированный с d элемент. Верно и обратное, если d_1 и d_2 – два наибольших общих делителя элементов a и b целостного кольца $\mathcal{R}$, то, по определению, $d_1 \mid d_2$ и $d_2 \mid d_1$, т.е. d_1 и d_2 ассоциированы. Соответственно, целесообразно обозначать символом $\text{НОД}(a, b)$ (или $\gcd(a, b)$) любой из (ассоциированных) наибольших общих делителей a и b. При таком соглашении наибольший общий делитель будет обладать следующими свойствами:

(3) $\text{НОД}(a, b) = a$ если и только если $a \mid b$;
(4) $\text{НОД}(a, 0) = 0$;
(5) $\text{НОД}(ta, tb) = t\,\text{НОД}(a, b)$;
(6) $\text{НОД}(\text{НОД}(a, b), c) = \text{НОД}(a, \text{НОД}(b, c))$.

Следующее естественное понятие, которое возникает в целостных кольцах в связи с понятием делимости – это понятие наименьшего общего кратного, которое, как и понятие наибольшего общего делителя, вводится “с точностью до ассоциированности”.

Определение. *Наименьшим общим кратным двух элементов $a, b \in \mathcal{R}$ называется такой элемент $m \in \mathcal{R}$, что*

(1) $a \mid m$, $b \mid m$;
(2) *если* $a \mid c$ *и* $b \mid c$ *для некоторого* $c \in \mathcal{R}$, *то* $m \mid c$.

Наибольший общий делитель обозначается символом $\text{НОК}(a, b)$.

Замечание. Полагая в свойстве (2) наименьшего общего кратного $c = ab$ получаем, что $\text{НОК}(a, b) \mid (ab)$.

Предложение 1.17. *Пусть для элементов a и b целостного кольца $\mathcal{R}$ существуют* $\text{НОД}(a, b)$ *и* $\text{НОК}(a, b)$. *Тогда* $\text{НОК}(a, b) = 0$ *если и только если* $a = 0$ *или* $b = 0$. *Кроме того, если* $a \neq 0$ *и* $b \neq 0$, $m = \text{НОК}(a, b)$ *и* $ab = md$, *то* $d = \text{НОД}(a, b)$.

Доказательство. Первое утверждение непосредственно вытекает из определения наименьшего общего кратного. Проверим второе утверждение. Так как $m = \text{НОК}(a, b)$, то $m = aa_1 = bb_1$ для некоторых $a_1, b_1 \in \mathcal{R}$. Следовательно, $ab = md = aa_1 d$ и $ab = md = bb_1 d$. Из этих равенств, после сокращения на a и b соответственно (напомним, что сокращение на ненулевой множитель возможно в любом целостном кольце), вытекает, что $b = a_1 d$ и $a = b_1 d$. То есть, $d \mid a$ и $d \mid b$. Итак, d – общий делитель a и b. Пусть теперь c – какой-то общий делитель a и b, т.е. $a = a_2 c$, $b = b_2 c$. Тогда $md = ab = ca_2 b$, но $a_2 b = mh$, $h \in \mathcal{R}$, так как $m = \text{НОК}(a, b)$. Отсюда $md = cmh$ и, окончательно, $d = ch$, т.е. $c \mid d$. □

Определение. *Элементы a и b целостного кольца $\mathcal{R}$ называются взаимно простыми, если* $\text{НОД}(a, b) = 1$.

Замечание. В произвольном целостном кольце опираясь только на определения наибольшего общего делителя и наименьшего общего кратного и на установленные свойства этих величин невозможно установить, существуют ли для заданных двух элементов такого кольца их НОД и НОК и, если существуют, то как их находить.

Этот вопрос сравнительно легко решается в *факториальном* кольце. Пусть $\mathcal{K}$ – факториальное кольцо. Обозначим через $\mathbb{P}(\mathcal{K})$ такое множество простых элементов из $\mathcal{K}$, что любой простой элемент из $\mathcal{K}$ ассоциирован в одним и только одним элементов множества $\mathbb{P}(\mathcal{K})$. Например, $\mathbb{P}(\mathbb{Z}) = \mathbb{P}$ – стандартное множество простых чисел (напомним, что число $p \in \mathbb{Z}_+$ называется *простым*, если оно не имеет делителей, отличных от 1 и p).

Теперь для любых двух элементов $a, b \in \mathcal{K}$ справедливы разложения

$$a = u_a p_1^{\mu_1} \times \cdots \times p_J^{\mu_J}, \qquad b = u_b p_1^{\nu_1} \times \cdots \times p_J^{\nu_J},$$

где $p_1, \ldots, p_J \in \mathbb{P}(\mathcal{K})$, $\mu_j \geqslant 0$, $\nu_j \geqslant 0$, $j = 1 \ldots J$, а $u_a \mid 1$ и $u_b \mid 1$.

Из Предложения 1.15 вытекает, что НОД(a, b) и НОК(a, b) существуют для любых элементов a и b факториального кольца $\mathcal{K}$ и, более того,

$$\text{НОД}(a, b) = p_1^{\min\{\mu_1,\nu_1\}} \times \cdots \times p_J^{\min\{\mu_J,\nu_J\}}, \quad \text{НОК}(a, b) = p_1^{\max\{\mu_1,\nu_1\}} \times \cdots \times p_J^{\max\{\mu_J,\nu_J\}}.$$

Из этих формул можно усмотреть, что элементы a и b факториального кольца $\mathcal{K}$ взаимно просты если и только если их разложения на простые множители не содержат одинаковых множителей.

Оказывается, что в факториальных кольцах имеется весьма простой и изящный алгоритм нахождения НОД и НОК, к описанию которого мы и переходим.

1.6. Евклидовы кольца и их факториальность

Определение. *Целостное кольцо $\mathcal{R}$ называется евклидовым, если каждому элементу $a \in \mathcal{R}$, $a \neq 0$, поставлено в соответствие число $\delta(a) \in \mathbb{Z}_+$ такое, что*

(1) *$\delta(ab) \geqslant \delta(a)$ для всех $a, b \in \mathcal{R}^*$;*
(2) *для любых $a \in \mathcal{R}$ и $b \in \mathcal{R}^*$ существуют $q, r \in \mathcal{R}$ такие, что $a = qb + r$ и $\delta(r) < \delta(b)$ или $r = 0$.*

Так, кольцо $\mathbb{Z}$ евклидово (можно положить $\delta(m) = |m|$ для $m \in \mathbb{Z}^*$).

Алгоритм Евклида в евклидовых кольцах. Пусть $\mathcal{R}$ – евклидово кольцо с евклидовой структурой δ. Пусть $a, b \in \mathcal{R}^*$. Тогда, применяя необходимое число раз процедуру деления с остатком и выбирая соответствующие q И r как предписано свойством (2) евклидовых колец, получим

$$\begin{array}{ll}
a = q_1 b + r_1, & \delta(r_1) < \delta(b), \\
b = q_2 r_1 + r_2, & \delta(r_2) < \delta(r_1), \\
r_1 = q_3 r_2 + r_3, & \delta(r_3) < \delta(r_2), \\
\multicolumn{2}{l}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots} \\
r_{k-2} = q_k r_{k-1} + r_k, & \delta(r_k) < \delta(r_{k-1}), \\
r_{k-1} = q_{k+1} r_k, & r_{k+1} = 0.
\end{array} \tag{1.3}$$

Это процесс в самом деле обрывается, так как последовательность $(\delta(r_j))$ – это строго убывающая последовательность положительных целых чисел, которая, заведомо, обрывается на каком-то конечном шаге и обрыв может произойти только в случае, когда очередной возникающий остаток обращается в ноль (см. еще раз свойство (2) евклидовых колец).

Предложение. $r_k = \text{НОД}(a, b)$.

Проверка. В самом деле, из того, что $r_k \mid r_{k-1}$ вытекает, что $r_k \mid r_{k-2}$. Это, в свою очередь, дает $r_k \mid r_{k-3}$. И так далее поднимаясь "вверх" по списку соотношений (1.3). В завершении этого "подъема" получим, что $r_k \mid b$ и $r_k \mid a$ соответственно. Итак, r_k – общий делитель a и b.

Пусть теперь d – некоторый общий делитель a и b. Так как $d \mid a$ и $d \mid b$ и так как $r_1 = a - q_1 b$, то $d \mid r_1$. Далее аналогично проверяется, что $d \mid r_2$. Проведя процесс "спуска" по списку соотношений (1.3) получим, что $d \mid r_j$ при $j = 1 \dots k$. Следовательно, $d \mid r_k$ и, по определению, $r_k = \text{НОД}(a, b)$. □

Определение. *Алгоритм нахождения наибольшего общего делителя, описываемый соотношениями (1.3) называется алгоритмом Евклида.*

Следующий результат весьма важен и будет часто применяться в дальнейшем.

Теорема 1.18. *В евклидовом кольце $\mathcal{R}$ любые два элемента a и b имеют наибольший общий делитель, причем существуют такие элементы $u, v \in \mathcal{R}$, что* $\text{НОД}(a, b) = au + bv$. *Кроме того, любые два элемента $a, b \in \mathcal{R}$ имеют наименьшее общее кратное, причем* $ab = \text{НОД}(a, b)\,\text{НОК}(a, b)$.

Доказательство. Существование наибольшего общего делителя вытекает из применимости алгоритма Евклида к любым двум элементам a и b евклидова кольца. Соотношение $\text{НОД}(a, b) = au + bv$ явно следует из соотношений (1.3) так как $r_1 - q_1 b$ есть линейная комбинация a и b, затем $r_2 = b - q_2 r_1 = -q_2 a + b(1 - q_1 q_2)$ снова есть линейная комбинация a и b с коэффициентами из $\mathcal{R}$. Повторяя это рассуждение k раз получим, что r_k является линейной комбинацией a и b с коэффициентами из $\mathcal{R}$.

Проверим существование наименьшего общего кратного элементов a и b. Пусть $a \neq 0$ и $b \neq 0$ и пусть $d = \text{НОД}(a, b)$. Так как $d \mid a$ и $d \mid b$, то $d \mid (ab)$ и, следовательно, существует $m \in \mathcal{R}$ такой, что $ab = dm$. Проверим, что $m = \text{НОК}(a, b)$, чем и будет завершено доказательство теоремы. Во-первых, так как $a = a_1 d$, а $ab = dm$, то $a_1 db = dm$ и, соответственно, $a_1 b = m$ (кольцо $\mathcal{R}$ целостное, что позволяет нам сокращать на ненулевой общий множитель). Таким образом $b \mid m$. Аналогично устанавливается, что $a \mid m$. Итак, m – общее кратное a и b. Пусть теперь c – некоторое общее кратное a и b, т.е. существуют $x, y \in \mathcal{R}$ такие, что $c = ax = by$. В силу утверждения первой части теоремы существуют такие $u, v \in \mathcal{R}$, что $d = au + bv$. Тогда

$$cab = cdm = c(au + bv)m = caum + cbvm = byaum + axbvm,$$

откуда, после сокращения на ab, получаем, что $c = yum + xvm = (yu + xv)m$, т.е. $m \mid c$. Из этого следует, что m – наименьшее общее кратное a и b. □

***Следствие* 1.19.** *Если элементы a и b евклидова кольца $\mathcal{R}$ взаимно просты, то существуют такие элементы $u, v \in \mathcal{R}$, что $au + bv = 1$.*

Предложение 1.20. *Пусть $\mathcal{R}$ – евклидово кольцо и пусть $a, b, c \in \mathcal{R}$. Тогда*

(1) *если* $\text{НОД}(a, b) = 1$ *и* $\text{НОД}(a, c) = 1$, *то* $\text{НОД}(a, bc) = 1$;
(2) *если $a \mid (bc)$ и* $\text{НОД}(a, b) = 1$, *то $a \mid c$;*
(3) *если $b \mid a$ и $c \mid a$ и* $\text{НОД}(b, c) = 1$, *то $(bc) \mid a$.*

Упражнение. Доказать Предложение 1.20.

Предложение 1.21. *Всякое евклидово кольцо является кольцом с разложением.*

Доказательство. Пусть $\mathcal{R}$ — евклидово кольцо. Нам необходимо показать, что любой элемент $a \in \mathcal{R}^*$ может быть представлен в виде (1.2) (возможно, не единственным образом). Предположим, что a обладает собственным делителем b, т.е. $a = bc$, где $c \in \mathcal{R}^*$, а b и c необратимые элементы. Заметим при этом, что элементы a и b не ассоциированы.

Установим, что $\delta(b) < \delta(a)$. Из свойства (1) евклидовой структуры δ непосредственно вытекает неравенство $\delta(b) \leqslant \delta(a)$ и нам остается исключить случай равенства.

Пусть $\delta(b) = \delta(a)$ и пусть элементы $q, r \in \mathcal{R}$ таковы, что $b = aq + r$ и $\delta(r) < \delta(a)$ или $r = 0$. При этом из $r = 0$ вытекает, что $b = aq$, что, вместе с равенством $a = bc$, означает ассоциированность элементов a и b. Из обнаруженного противоречия вытекает, что $r \neq 0$. Аналогично проверяется, что $1 - qc \neq 0$ (это оставляется в качестве *упражнения*). Далее оцениваем

$$\delta(a) = \delta(b) \leqslant \delta(b(1 - qc)) = \delta(b - qa) = \delta(r) < \delta(a)$$

и приходим к противоречию. Итак $\delta(b) < \delta(a)$.

Пусть теперь $a = a_1 \times a_2 \times \cdots \times a_n$, где все элементы $a_j \in \mathcal{R}$, $j = 1 \ldots n$, необратимы и пусть $b_m := a_m a_{m+1} \times \cdots \times a_n$ при $m = 1 \ldots n$. При этом элемент b_{k+1} является собственным делителем элемента b_k, $k = 1 \ldots n$ и, следовательно,

$$\delta(a) = \delta(b_1) > \delta(b_2) > \cdots > \delta(b_n) = \delta(a_n) > \delta(1).$$

Полученная строго убывающая последовательность неотрицательных целых чисел имеет длину $n \leqslant \delta(a)$. Возьмем для элемента a разложение, соответствующая последовательность $(\delta(b_k))$ для которого имеет максимальную длину. Это разложение и будет разложением на простые множители. □

Теорема 1.22. *Всякое евклидово кольцо факториально.*

Доказательство. В Предложении 1.21 выше уже установлено, что если $\mathcal{R}$ — евклидово кольцо, то $\mathcal{R}$ является кольцом с разложением. Нам необходимо доказать, что разложение произвольного элемента $a \in \mathcal{R}^*$ на простые множители единственно с точностью до порядка следования множителей и их ассоциированности.

С учетом Предложения 1.15 нам необходимо проверить, что если $p \in \mathcal{R}$ – простой и если $p \mid (bc)$ для некоторых $b, c \in \mathcal{R}$, то $p \mid b$ или $p \mid c$. Без ограничения общности считаем, что $b \neq 0$ и $c \neq 0$. Пусть $d = \text{НОД}(b, p)$. Тогда $d \mid 1$ либо d ассоциирован с p. В первом случае b и p взаимно просты и, применяя утверждение (2) Предложения 1.20 получаем, что $p \mid c$. Если же $d = up$, где $u \mid 1$, то $p \mid b$. □

Задача 1.4. Доказать, что при $d = -1, \pm 2, 3$ соответствующие квадратичные кольца $\mathbb{Z}[\sqrt{d}]$ являются евклидовыми.

Замечание. Кольцо $\mathbb{Z}[\sqrt{d}]$ является евклидовыми только при $d = -1, -2, -3, -7, -11$ и $d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, 97$. При $d = -19, -43, -67, -163$ кольцо $\mathbb{Z}[\sqrt{d}]$ не является евклидовым, но является факториальным.