1 Определения

Определение 1.1. Кольцо – это тройка $(R, +, *)$, где R – непустое множество, $+, * : R^2 \mapsto R$, такая что $(R, +)$ – абелева группа, а также выполнена дистрибутивность умножения $*$ относительно сложения $+$ слева и справа. Нейтральный элемент относительно сложения обозначается 0

Кольцо с единицей – это кольцо, в котором относительно умножения есть нейтральный элемент, обозначаемый 1: $1 * a = a * 1 = 1$

Ассоциативное кольцо – это кольцо, в котором выполнена ассоциативность операции умножения: $a * (b * c) = (a * b) * c$

Коммутативное кольцо – это кольцо, в котором выполнена коммутативность операции умножения $a * b = b * a$, а также присутствует единица и выполнена ассоциативность.

Определение 1.2. Элемент $a \neq 0$ ассоциативного кольца с единицей R называется обратимым, если $\exists a^{-1} \in R : a^{-1} * a = a * a^{-1} = 1$

Определение 1.3. Элемент $0 \neq a \in R$ называется делителем нуля, если $\exists 0 \neq b \in R : ab = 0$

Определение 1.4. Для кольца K множество его обратимых элементов обозначается K^*

Элементы a и b называются ассоциированными, если $\exists c \in K^* : a = cb$

Определение 1.5. Коммутативное кольцо без делителей нуля называется областью целостности.

Определение 1.6. Ненулевой необратимый элемент a области целостности называется неразложимым, если из того, что он представляется в виде $a = bc$, следует, что либо b либо c обратим.

Определение 1.7. Ненулевой необратимый элемент p называется простым, если из того, что $p|ab$ следует, что либо $p|a$ либо $p|b$

Определение 1.8. Евклидово кольцо – это область целостности K с определенной на ней функцией евклидовой нормы $N : K \setminus \{0\} \mapsto \mathbb{N}_0$:

1. $\forall a, b \in K \setminus \{0\} : N(a) \leq N(ab)$
2. $\forall a, b \in K \setminus \{0\} : \exists q, r : a = qb + r, N(r) < N(b)$

Определение 1.9. Пусть K – область целостности. Тогда элемент $z \in K$ называется наибольшим общим делителем элементов $a, b \in K$ (обозначается как (a, b)), если $z|a, z|b$ и $\forall z' : z'|a, z'|b$ выполнено, что $z'|z$

Определение 1.10. Пусть R_1 и R_2 – кольца. Отображение $\varphi : R_1 \mapsto R_2$ наызвается гомоморфизмом колец, если:

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\varphi(a * b) = \varphi(a) * \varphi(b)$

Определение 1.11. Подмножество $R \subset K$ называется подкольцом, если оно замкнуто относительно умножения и является подгруппой по сложению.

Определение 1.12. Подкольцо R коммутативного кольца K называется идеалом, если оно замкнуто относительно умножения на элемент из K, то есть $\forall r \in R, k \in K : rk \in R$

Определение 1.13. Тривиальным называют идеал, либо совпадающий со всем кольцом, либо состоящий из одного элемента (нейтрального элемента по сложению)

Определение 1.14. Идеал I коммутативного кольца K называется порожденным элементами $x_1, \cdots, x_n$ (обозначение $I = (x_1, \cdots, x_n)$), если $I = \{a_1 * x_1 + a_2 * x_2 + \cdots + a_n * x_n | \forall i : a_i \in K\}$

Определение 1.15. Идеал конечнопорожден, если он порожден конечным числом элементов.

Определение 1.16. Идеал называется главным, если он порожден одним элементом.

Определение 1.17. Кольцо называется кольцом главных идеалов (КГИ), если в нём все идеалы главные.

Определение 1.18. Область целостности называется факториальным кольцом, если в нём любой ненулевой элемент либо обратим, либо с точностью до перестановки и домножения на обратимые представляется в виде произведения неразложимых.

Определение 1.19. Нетривиальный идеал I называется простым, если $ab \in I \Rightarrow a \in I \vee b \in I$

Определение 1.20. Нетривиальный идеал I называется максимальным, если не существует другого нетривиального идеала, содержащего I

2 Вопросы сложности 2

Утверждение 2.1. *В коммутативном кольце элемент не может иметь двух различных обратных*

Доказательство. Пусть K – коммутативное кольцо, $a \in K$ – ненулевой элемент этого кольца, a_1, a_2 – два различных обратных элемента к нему. Тогда, с одной стороны $a_1 a a_2 = a_1(a a_2) = a_1$, а с другой стороны $a_1 a a_2 = (a_1 a) a_2 = a_2$. Получили, что $a_1 = a_2$. Противоречие. □

Утверждение 2.2. *Пусть R – кольцо с единицей, причем $|R| > 1$. Тогда в этом кольце $1 \neq 0$*

Доказательство. Пусть $a \in R$. Докажем, что $a \cdot 0 = 0$. Воспользуемся тем, что $0 = 0 + 0$ (это прямое следствие аксиом кольца), а также дистрибутивностью:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

Если добавить к обоим частям равнества обратный по сложению $-(a \cdot 0)$, то получим, что $a \cdot 0 = 0$.

Пусть теперь $1 = 0$. Поскольку $|R| > 1$, то можно найти такой $a \in R$, что $a \neq 0$. Тогда $a \cdot 1 = 0$ из выше доказанного. С другой стороны, поскольку 1 – нейтральный элемент по умножению, $a \cdot 1 = a$. Тогда $a = 0$. Но мы выбирали a так, что $a \neq 0$. Противоречие. $\square$

Утверждение 2.3. *Пусть R – ассоциативное кольцо с единицей. a – обратимый элемент в R. Тогда a не может быть делителем нуля.*

Доказательство. Пусть $\exists b \neq 0 : ab = 0$. Умножим последнее равенство на a^{-1}. Тогда $0 = a^{-1}ab = (a^{-1}a)b = b$. Получили, что $b = 0$. Противоречие. $\square$

Утверждение 2.4. *Пусть K – область целостности, пусть $a, b, c \in K$, причем $c \neq 0$. Тогда $ac = bc \Rightarrow a = b$*

Доказательство. $ac = bc \Leftrightarrow ac - bc = 0 \Leftrightarrow (a - b)c = 0$. Поскольку K – область целостности, то либо $c = 0$, либо $a - b = 0$. Но первое противоречит условию, поэтому верно второе, то есть $a = b$. $\square$

Утверждение 2.5. $S = \{\frac{p}{q} \in \mathbb{Q} : (p, 1) = 1, q|n\}$ *не является подкольцом* $\mathbb{Q}$

Доказательство. Пусть $n = 12$, $\frac{1}{4} \in S, \frac{1}{6} \in S$. Но их произведение $\frac{1}{4} \cdot \frac{1}{6} = \frac{1}{24} \notin S$. Получили, что S не замкнуто относительно умножения. $\square$

Утверждение 2.6. *Пусть p – простое, $S = \{\frac{a}{b} \in \mathbb{Q} : (a, b) = 1, \not{p}|b\}$. Тогда S – подкольцо в $\mathbb{Q}$*

Доказательство. Проверяем замкнутость относительно операций. Пусть $\frac{a}{b} \in S, \frac{c}{d} \in S$, причем $/p|b, /p|d$ $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, причем $/p|bd$. Действительно, пусть $p|bd$. Так как p простое, то либо $p|b$, либо $p|d$. А это не так. Поскольку $\not{p}|bd$, то и после сокращения дроби $\frac{ad+bc}{bd}$ на некоторое число e, $\not{p}|\frac{bd}{e}$. Действительно, воспользуемся ОТА: пусть $bd = p_1 p_2 \cdots p_k$, причем в этом разложении нет числа p. Но тогда после сокращения, в разложении числа bd могут лишь исчезнуть некоторые p_i, но не появится p.

Аналогично с произведением. Понятно также, что все обратные к $\frac{a}{b}$ в S лежат, ведь это просто $\frac{-a}{b}$ $\square$

Утверждение 2.7. *Пусть p – простое, $S = \{\frac{a}{b} \in \mathbb{Q} : (a, b) = 1, \exists n \in \mathbb{N}_0 : b = p^n\}$. Тогда S – подкольцо в $\mathbb{Q}$*

Доказательство. Проверяем замкнутость операций, пусть $\frac{a}{p^n} \in S, \frac{b}{p^m} \in S$. Без ограничения общности, $m > n$.

Тогда $\frac{a}{p^n} + \frac{b}{p^m} = \frac{ap^{m-n}+b}{p^m}$. После сокращения последней дроби её знаменатель останется степенью p. Аналогично с произведением. Обратные ко всем элементам также лежат. $\square$

Утверждение 2.8. *Множество обратимых элементов ассоциативного кольца с единицей является группой по умножению и называется мультипликативной группой кольца*

Доказательство. Пусть K^* – это множество всех обратимых элементов ассоциативного кольца с единицей K. Понятно, что для этих элементов выполняется ассоциативность, ведь она наследуется из кольца K. Кроме того, $1 \in K^*$, ведь 1 – обратимый элемент. И последнее: если a – обратим, то a^{-1} тоже обратим. В итоге мы доказали, что K^* – группа. $\square$

Утверждение 2.9. $a \sim b \Leftrightarrow a|b \wedge b|a$

Доказательство. Пусть $a \sim b$. Тогда $\exists c \in K^* : a = bc$. Тогда $b|a$. Кроме того, $c^{-1}a = b$, то есть $a|b$.

Наоборот, пусть $a|b, b|a$. Понятно, что тогда $a \neq 0, b \neq 0$. Тогда $b = ca, a = db$. Тогда $b = cdb$. Сокращая на b получаем, что $cd = 1$, а это означает, что c и d – обратимые, то есть $a \sim b$ $\square$

Утверждение 2.10. *Если a – неразложим, а $b \sim a$, то b – неразложим.*

Доказательство. Пусть b – разложимый элемент, то есть $\exists c, d \notin K^* : b = cd$. Но $a = eb$, причем $e \in K^*$. Тогда $a = ecd$. Но $ec \notin K^*$. Действительно, пусть $ec \in K^*$. $e^{-1} \in K^*$. Тогда $c \in K^*$, а это не так. Получили разложения для a на необратимые элементы. $\square$

Утверждение 2.11. *Пусть p – простой, $p \sim q$. Тогда q тоже простой.*

Доказательство. Пусть $q|ab, q = cp, c \in K^*$. Тогда $ab = dq = cdp$. Тогда $p|ab$. Тогда либо $p|a$, либо $p|b$. Пусть, без ограничения общности, $p|a$. Тогда $a = ep = ec^{-1}q$. Но тогда $q|a$. $\square$

Утверждение 2.12. *Пусть $d_1 = (a, b), d_2 = (a, b)$. Тогда $d_1 \sim d_2$*

Доказательство. Поскольку d_1 – наибольший общий делитель, а d_2 – общий делитель, то $d_2|d_1$. Аналогично, $d_1|d_2$. По критерию ассоциированности, $d_1 \sim d_2$ $\square$

Утверждение 2.13. $\mathbb{Z}[\omega]$ *– евклидово кольцо с нормой $N(a + b\omega) = a^2 + b^2 - ab$*

Доказательство. Заметим, что $|a + b\omega|^2 = (a + b\omega) \cdot (a + b\overline{\omega}) = a^2 + ab(\omega + \overline{\omega}) + b^2\omega\overline{\omega} = a^2 + b^2 - ab = N(a + b\omega) \geq 1$, при $(a, b) \neq 0$

Тогда для $z_1, z_2 \neq 0$: $N(z_1 z_2) = z_1 z_2 \overline{z}_1 \overline{z}_2 = N(z_1)N(z_2) \geq N(z_1)$ и первое свойство нормы выполнено.

Теперь нужно сказать пару слов, про то, как мы делим элементы в $\mathbb{Z}[\omega]$ (то есть как для любых двух $a, b \in \mathbb{Z}[\omega]$ выбрать $q, r \in \mathbb{Z}[\omega]$ так, что $a = bq + r$, причем $N(r) < N(b)$)

Положим $q = \left[\frac{a}{b}\right]$ – ближайшую к $\frac{a}{b}$ точку из $\mathbb{Z}[\omega]$, $r = b * \left(q - \frac{a}{b}\right) = b * \left(\left[\frac{a}{b}\right] - \frac{a}{b}\right) = bq - a$. Если мы докажем, что $\left|\left[\frac{a}{b}\right] - \frac{a}{b}\right| < 1$, это будет означать, что $N(r) < N(1)N(b) = N(b)$. Для этого докажем, что расстояние вообще от любой точки из $\mathbb{C}$ до ближайшей точки $\mathbb{Z}[\omega]$ удовлетворяет требуемому неравенству. Рассмотрим $z \in \mathbb{C}$. Для неё в $\mathbb{Z}[\omega]$ есть три ближайшие точки z_1, z_2, z_3, образующие треугольник вокруг z. Любой такой треугольник является равносторонним со стороной 1. Докажем, что $f(z) = \max_z \min\{|z_1 - z|, |z_2 - z|, |z_3 - z|\} < 1$. Но максимум достигается, когда все $|z_i - z|$ равны. Тогда точка z – центр описанной окружности вокрут треугольника, а $f(z)$ – то радиус описанной окружности, который находится по формуле $\frac{abc}{4S} = \frac{1}{\sqrt{3}} < 1$ $\square$

Утверждение 2.14. *В области целостности $\mathbb{Z}[u]$ элемент $z = a + bu$ делится на $k \in \mathbb{Z}$ тогда и только тогда, когда a и b делятся на k.*

Доказательство. Пусть $k|z$. Тогда $a + bu = z = k(x + yu) = kx + kyu$. Пусть $u = c + di$. Тогда $a + bc + bdi = kx + kyc + kydi$. Два компексных числа равны, если равны их мнимые и действительные части, поэтому

$$\begin{cases} a + bc = kx + kyc, \\ bd = kyd \end{cases}$$

Считаем, что $d \neq 0$, в противном случае утверждение не верно (например, $2|1 + 3 = 4$, но неверно, что $2|1, 2|3$). Тогда $b = ky, a = kx$. Значит, a и b делятся на k.

Пусть наоборот, a и b делятся на k. Тогда $b = ky, a = kx$. $z = a + bu = k(x + uy)$. Тогда $k|z$. $\square$

Утверждение 2.15. *В $\mathbb{Z}[\omega]$ если $z|x, |z| = |x|$, то $z \sim x$*

Доказательство. $x = zy$, причем $|x| = |z||y|$, а значит, $|y| = 1$. Но в $\mathbb{Z}[\omega]$ все такие z, что $|z| = 1$ обратимы, следовательно, $z \sim x$ $\square$

Утверждение 2.16. *В $\mathbb{Z}[i]$ если $z|x, |z| = |x|$, то $z \sim x$*

Доказательство. $x = zy$, причем $|x| = |z||y|$, а значит, $|y| = 1$. Но в $\mathbb{Z}[i]$ все такие z, что $|z| = 1$ обратимы, следовательно, $z \sim x$ $\square$