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. Идеал $I \neq K$ называется простым, если $ab \in I \Rightarrow a \in I \vee b \in I$

Определение 1.20. Идеал $I \neq K$ 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. $\square$

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. ☐

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. ☐

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 $a \sim b$ ☐

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. ☐

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 $q|a$. ☐

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, $d_1 \sim d_2$ ☐

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 $z_1, z_2 \neq 0$: $N(z_1z_2) = z_1z_2\overline{z}_1\overline{z}_2 = N(z_1)N(z_2) \geq N(z_1)$ 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 $\frac{abc}{4S} = \frac{1}{\sqrt{3}} < 1$ □

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 $k|z$. □

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, $z \sim x$ □

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, $z \sim x$ □

Утверждение 2.17. *Если z – неразложимый в $\mathbb{Z}[i]$, то $\exists p$ – простое, $N(z) = p \vee N(z) = p^2$*

Доказательство. Будет пользоваться тем фактом, что $\mathbb{Z}[i]]$ – факториальное кольцо. Тогда z – простой. $N(z) = z\overline{z}$, причем $N(z) \in \mathbb{Z}$. Разложим $N(z)$ на простые. $z\overline{z} = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$. То есть $z|p_1^{k_1} \cdots p_s^{k_s}$. но z – простое, поэтому $\exists i : z|p_i$. То есть $zx = p_i$. Обозначим $p = p_i$, оно простое. $N(z)N(x) = p^2$. Есть 3 варианта:

1. $N(x) = 1$. Тогда $N(z) = p^2$
2. $N(x) = p$. Тогда $N(z) = p$.
3. $N(x) = p^2$. Тогда $N(z) = 1$, и z обратим, а значит, не является неразложимым. Противоречие.

$\square$

Утверждение 2.18. *Если z – неразложимый в $\mathbb{Z}[\omega]$, то $\exists p$ – простое, $N(z) = p \vee N(z) = p^2$*

Доказательство. Доказательство повторяет предыдущее. Будет пользоваться тем фактом, что $\mathbb{Z}[\omega]$ – факториальное кольцо. Тогда z – простой. $N(z) = z\overline{z}$, причем $N(z) \in \mathbb{Z}$. Разложим $N(z)$ на простые. $z\overline{z} = p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$. То есть $z|p_1^{k_1}\cdots p_s^{k_s}$. но z – простое, поэтому $\exists i : z|p_i$. То есть $zx = p_i$. Обозначим $p = p_i$, оно простое. $N(z)N(x) = p^2$. Есть 3 варианта:

1. $N(x) = 1$. Тогда $N(z) = p^2$
2. $N(x) = p$. Тогда $N(z) = p$.
3. $N(x) = p^2$. Тогда $N(z) = 1$, и z обратим, а значит, не является неразложимым. Противоречие.

$\square$

Утверждение 2.19. *Если x – неразложимый элемент $\mathbb{Z}[i]$ и $N(z) = p^2$, то $z \sim p$*

Доказательство. В рамках предыдущего доказательства мы показали, что $\exists x : zx = p$. Тогда $N(z)N(x) = p^2$, но также $N(z) = p^2$, а значит, $N(x) = 1$. Значит, x – обратим и $z \sim p$ $\square$

Утверждение 2.20. *Если x – неразложимый элемент $\mathbb{Z}[\omega]$ и $N(z) = p^2$, то $z \sim p$*

Доказательство. Аналогично. $\square$

Утверждение 2.21. *Если для $z \in \mathbb{Z}[i]$ выполнено, что $N(z) = p$, где p – простое, то z неразложим.*

Доказательство. Пусть z разложим, тогда $z = z_1z_2$, причем $z_1, z_2 \notin \mathbb{Z}[i]^*$. Тогда $p = N(z) = N(z_1)N(z_2)$. Так как p простое, то либо $N(z_1) = 1$, либо $N(z_2) = 1$. Но тогда либо z_1, либо z_2 обратим. Противоречие. $\square$

Утверждение 2.22. *Если для $z \in \mathbb{Z}[\omega]$ выполнено, что $N(z) = p$, где p – простое, то z неразложим.*

Доказательство. Аналогично. $\square$

Утверждение 2.23. *Множество делителей нуля кольца K вместе с нулём не всегда образуют идеал.*

Доказательство. Рассмотрим $K = \mathbb{Z}_6$. Его множество делителей нуля (вместе с нулем) – это $\{0, 2, 3\}$. Это множество не образует даже подкольцо, так как $2 + 3 = 5 \notin \{0, 2, 3\}$ $\square$

Утверждение 2.24. *3 – разложимый элемент $\mathbb{Z}[\omega]$*

Доказательство. $(1-\omega)(1-\omega^2) = 1 - \omega - \omega^2 + \omega^3 = 2 - \omega - \omega^2 = 2 - \omega - (-1-\omega) = 3$ $\square$

Утверждение 2.25. *Если идеал $I \subset K$ содержит обратимый элемент, то $I = K$*

Доказательство. Пусть $a \in I$ – обратимый элемент. Тогда $\exists a^{-1} \in K : aa^{-1} = 1$. Из опеределения идеала $\forall x \in I : \forall y \in K : xy \in I$. Значит, $1 = aa^{-1} \in I$. Раз $1 \in I$, то и $\forall y \in K : 1 \cdot y \in I$. Значит, $K \subset I$. Но тогда $K = i$. $\square$

Утверждение 2.26. $I = (a_1, \cdots, a_k) = \{x_1 a_1 + \cdots + x_k a_k : \forall i : x_i \in K\}$ *– это минимальный по включению идеал, содержащий элементы $a_1, \cdots, a_k$.*

Доказательство. Во-первых, I – это идеал. Действительно, пусть $x \in I, y \in K$. Тогда $x = x_1 a_1 + \cdots x_k a_k$. $yx = yx_1 a_1 + \cdots + yx_k a_k \in I$. Кроме того, это подгруппа по сложению.

Пусть J – другой идеал, содержащий $a_1, \cdots, a_k$. Тогда $\forall i : \forall x \in K : xa_i \in J$. Тогда $\forall x_1, \cdots, x_k : x_1 a_1 + \cdots + x_k a_k \in J$. Но тогда $I \subset J$. Но это и означает, что I – минмальный по включению идеал, содержащий элементы $a_1, \cdots, a_k$. $\square$

Утверждение 2.27. *Идеал $(x, x+1) \subset \mathbb{Z}[x]$ не является ни простым, ни максимальным.*

Доказательство. $x \in (x, x+1), x+1 \in (x, x+1) \Rightarrow x+1-x = 1 \in (x, x+1)$. Но тогда $I = \mathbb{Z}[x]$. То есть этот идеал тривиальный. Значит, он не максимальный и не простой. $\square$

3 Вопросы сложности 3

Утверждение 3.1. *Множество $S = \{x + \sqrt{2}y : x, y \in \mathbb{Q}\}$ является кольцом.*

Доказательство. Так как $S \subset \mathbb{R}$, а $\mathbb{R}$ – кольцо, то достаточно проверить замкнутость S. Пусть $x + \sqrt{2}y \in S, a + \sqrt{2}b \in S$. Тогда $-(x + \sqrt{2}y) = -x + \sqrt{2}(-y) \in S$. $(x + \sqrt{2}y) + (a + \sqrt{2}b) = (x + a) + \sqrt{2}(y + b) \in S$. $(x + \sqrt{2}y)(a + \sqrt{2}b) = (xa + 2yb) + \sqrt{2}(ya + xb) \in S$. Получаем, что S замкнуто относительно операци. Значит S – подкольцо, значит S – кольцо. $\square$

Утверждение 3.2. *Простой элемент области целостности является неразложимым.*

Доказательство. Пусть p – простой элемент области целостности K. Пусть p – разложим, то есть $\exists a \not{in} K^*, b \notin K^* : p = ab$. Тогда $p|ab$. Значит, либо $p|a$, либо $p|b$. Пусть без ограничения общности $p|a$. Тогда $a = px$. Тогда $p = pxb$. Значит, $p(1 - xb) = 0$. Так как $p \neq 0$, то $1 - xb = 0$. Значит, $xb = 1$, и следовательно, $b \in K^*$. Противоречие. $\square$

Утверждение 3.3. *При каких $u \in \mathbb{C}$ множество $\mathbb{Z}[u] = \{a + bu : a, b \in \mathbb{Z}\}$ является областью целостности.*

Доказательство. Заметим, что $\mathbb{Z}[u] \subset \mathbb{C}$. Но в $\mathbb{C}$ делителей нуля нет, так как это поле (ну или так: пусть a – делители нуля в $\mathbb{C}$, тогда $0 = |ab| = |a||b|$. Но тогда либо $|a| = 0$, либо $|b| = 0$).

Осталось проверить, при каких u $\mathbb{Z}[u]$ замкнуто. Понятно, что $(a+bu)+(c + du) = (a + c) + (d + b)u$, то есть относительно сложения это множество всегда замкнуто. Посмотрим, что происходит при умножении: $(a + bu)(c + du) = ac+(bc+ad)u+bdu^2$. Значит, это множество замкнуто тогда и только тогда, когда $u^2 \in \mathbb{Z}[u]$. То есть $\exists r, s : u^2 = r + su$. Заметим, что если u – корень $u^2 = r + su$, то и $\overline{u}$ это тоже корень $u^2 = r + su$. Тогда по теореме Виета это означает, что $u + \overline{u} = 2\Re u \in \mathbb{Z}, u \cdot \overline{u} = |u|^2 \in \mathbb{Z}$ $\square$

Утверждение 3.4.

$$\mathbb{Z}[ni]^* = \begin{cases} \{1, -1, i, -i\}, n = 1, \\ \{1, -1\}, n > 1. \end{cases}$$

Доказательство. Заметим, что если z – обратимый, то $|z|^2|z^{-1}|^2 = |zz^{-1}|^2 = |1|^2 = 1$. Если $z, z^{-1} \in \mathbb{Z}[ni]$, то $|z|^2, |z^{-1}|^2 \in \mathbb{Z}$. Произведение двух положительных чисел из $\mathbb{Z}$ дает единицу, если оба числа это единица. Значит, обратимыми могут быть только элементы с нормой 1. Просто переберём все элементы из $\mathbb{Z}[ni]$ с нормой 1 и посмотрим, какие из них обратимы. $\square$

Утверждение 3.5. $\mathbb{Z}[\omega]^* = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$

Доказательство. Рисуем $\mathbb{Z}[\omega]$ на листочке и внимательно смотрим, использую соображения из предыдущего доказательства. $\square$

Утверждение 3.6. $\mathbb{Z}[3i]$ *не факториально.*

Доказательство. $3i\cdot(-3i) = 9 = 3\cdot3$. Докажем, что $3, 3i, -3i$ неразложимы. Пусть не так, и скажем, $3 = z_1z_2$, причем ни z_1, ни z_2 не обратимы, а следовательно $N(z_1) > 1, N(z_2) > 1$. Тогда $9 = N(z_1)N(z_2)$. Понятно, что тогда $N(z_1) = 3, N(z_2) = 3$. Но $N(z) = a^2 + 9b^2$. Легко показать, что $N(z) \neq 3$ при любых a, b. Ну или можно нарисовать $\mathbb{Z}[3i]$ и убедиться в этом при помощи геометрии. Оба варианта являются правильными. Аналогично делаем с $3i$ и $-3i$ $\square$

Утверждение 3.7. *$\mathbb{Z}[\sqrt{3}i]$ не факториально.*

Доказательство. $4 = 2 \cdot 2 = (1-\sqrt{3}i)(1+\sqrt{3}i)$. $N(2) = N(1-\sqrt{3}i) = N(1+\sqrt{3}i) = 4$. Покажем, что элемент с нормой 4 неразложим. $4 = N(z_1) \cdot N(z_2)$. Тогда $N(z_1) = N(z_2) = 2$. Но элементов с такой нормой в $\mathbb{Z}[\sqrt{3}i]$ нет. □

Утверждение 3.8. *Если $N(ab) = N(a)$, и $a, b \neq 0$, то b – обратим*

Доказательство. Разделим a на ab с остатком. Тогда $\exists q, r : a = abq + r$. Пусть $r \neq 0$. Тогда $N(r) < N(ab) = N(a)$. Но $r = a - abq = a(1-bq)$, следовательно $a|r$. Тогда $r = xa$. $N(r) = N(xa) \geq N(a)$. Но мы получили противоречие, ведь $N(a) \leq N(xa) = N(r) < N(ab) = N(a)$. Значит $r = 0$. Но тогда b – обратимый □

Утверждение 3.9. *Если b – обратим, то $N(ab) = N(a)$*

Доказательство. Из свойства нормы: $N(ab) \geq N(a)$. Докажем, что $N(a) \geq N(ab)$. Так как b – обратимый, то $a = abb^{-1}$. Тогда Из свойства нормы $N(a) = N(abb^{-1}) \geq N(ab)$. Конец. □

Утверждение 3.10. *Если p – простое целое число, причем $p = 4k+3$, то p – неразложимый элемент в $\mathbb{Z}[i]$*

Доказательство. Пусть не так. Тогда $\exists z_1, z_2 \notin \mathbb{Z}[i]^* : p = z_1 z_2$. Посмотрим на норму p: $p^2 = N(z_1)N(z_2)$. Понятно, что без ограничения общности есть два варианта:

1. $N(z_1) = N(z_2) = p$. Но такого быть не может, т.к. $N(z_1) = a^2 + b^2 \not\equiv 3 \mod 4$

2. $N(z_1) = 1, N(z_2) = p^2$. Но тогда z_1 обратимый, и мы опять пришли к противоречию.

Значит, p неразложимый. □

Утверждение 3.11. *Если p – простое целое число вида $4k+1$, то p – разложимый элемент в $\mathbb{Z}[i]$*

Доказательство. Предположим противное, пусть p – неразложимый, а следовательно, простой, так как $\mathbb{Z}[i]$ – факториально.

Заметим, что -1 является квадратичным вычетом по модулю p (другими словами, $\exists a : a^2 \equiv -1 \mod p$). Это можно понять, посчитав символ Лежандра $\left(\frac{-1}{p}\right)$. Но есть и другой вариант доказательства. Мы знаем, что $\forall a : a^{p-1} \equiv 1 \mod p$ из малой теоремы Ферма. Тогда $(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0 \mod p$. Мы знаем, что у этого многочлена $p-1$ корень, а у $a^{\frac{p-1}{2}} - 1 \equiv 0 \mod p$ не может быть больше $\frac{p-1}{2}$ корней (так как $\mathbb{Z}[p]$ – это поле). Тогда $\exists a : a^{\frac{p-1}{2}} \equiv -1 \mod p$. Если положить $x = a^k$, то $x^2 = a^{2k} = a^{\frac{p-1}{2}} \equiv -1 \mod p$. Значит, -1 является квадратичным вычетом по модулю p. Тогда $x^2 + 1 = (x-i)(x+i) \equiv 0 \mod p$. Так как p простое, то либо $p|x+i$, либо $p|x-i$. Но оба этих утверждения неверны (это доказывалось в 2.14) □

Утверждение 3.12. *Натуральное число представимо в виде суммы двух квадратов (целых чисел) тогда и только тогда, когда любое простое число вида $4k+3$ входит в его разложение на простые множители в чётной степени.*

Доказательство. Пусть число m представимо в виде суммы двух квадратов, тогда $\exists z : m = z\overline{z}$. Разложим z на простые. Пусть $z = p_1 \cdots p_s$. Тогда $m = (p_1\overline{p}_1)\cdots(p_s\overline{p}_s)$. Почему в этом разложении простые вида $4k+3$ входят в чётных степени? Давайте это проверим, путь для некоторого k простое $4k+3$ входит в разложение m на простые, тогда $4k+3|m$. Так как $4k+3$ простое над $\mathbb{Z}[i]$, то либо $\exists i : 4k+3|p_i$, либо $\exists i : 4k+3|\overline{p}_i$. Пусть без ограничения общности $4k+3|p_i$, то есть $(4k+3)x = p_i$. Но p_i – простое (и $\overline{p}_i$). Тогда они неразложимы, а тогда x – обратимо. Но тогда $p_i \sim 4k+3$. Но $N(p_i) = p_i\overline{p}_i = (4k+3)^2$. Значит, эта скобка $(p_i\overline{p}_i) = (4k+3)^2$. Поделим m на $(4k+3)^2$ и продолжим доказательство по индукции. В результате, все простые вида $(4k+3)$, которые нам удастся вынести, будут всегда выносится в чётной степени.

Пусть теперь наоборот, m таково, что простые вида $4k+3$ входят в его разложение в чётной степени. То есть $m = p_1^2 \cdots p_s^2 q_1 \cdots q_r$. Причем $p1, \cdots, p_s$ – простые вида $4k+3$, а $q_1, \cdots, q_r$ – простые вида $4k+1$. Докажем, что $\forall i \in \{1, \cdots, r\} : \exists z_i : q_i = z_i \cdot \overline{z}_i$. Действительно, q_i – это простое вида $4k+1$. Оно разложимо над $\mathbb{Z}[i]$. Тогда $q_i = uv$, тогда $q_i^2 = N(q_i) = N(u)N(v)$. Но $N(u) > 1, N(v) > 1$. Тогда $u\overline{u} = N(u) = q_i, v\overline{v} = N(v) = q_i$. Тогда можно переписать разложение для m в виде: $m = p_1^2 \cdots p_s^2(z_1\overline{z}_1)\cdots(z_r\overline{z}_r)$. Если положить $z = p_1 \cdots p_s z_1 \cdots z_r$, то $m = z\overline{z} = N(z)$, а значит m представляется как сумма квадратов. □

Утверждение 3.13. *Пусть p – простое целое число вида $p = 3k+1$. Тогда p разложим в $\mathbb{Z}[\omega]$*

Доказательство. Сначала докажем, что -3 является квадратичным вычетом по модулю p используя символ Лежандра: $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. Здесь мы воспользовались квадратичным законом взаимности и критерием Эйлера для квадратичных вычетов. Значит, $\exists c : c^2 + 3 = (c - \sqrt{3}i)(c + \sqrt{3}i) \equiv 0 \mod p$. Но $\sqrt{3}i = 2\omega + 1$. Тогда $p|(c+1+2\omega)(c-1-2\omega)$. Если бы p было простым, то либо $p|(c+1+2\omega)$, либо $p|(c-1-2\omega)$. Но это не так (показано в 2.14) □

Утверждение 3.14. *Если p – простое число вида $p = 3K + 2$, то p – неразложимый элемент $\mathbb{Z}[\omega]$*

Доказательство. Пусть не так и $p = z_1z_2$, причем $N(z_1) > 1, N(z_2) > 1$. Тогда $p^2 = N(z_1)N(z_2)$. Это возможно, если только если $N(z_1) = N(z_2) = p$. Узнаем, можно ли найти такие $a, b : a^2 - ab + b^2 = p = 3k+2$. Посмотрим на это равенство по модулю 3. Тогда $2 \equiv a^2 - ab + b^2 \equiv a^2 + 2ab + b^2 \equiv (a+b)^2 \mod 3$. Но 2 – не квадратичный вычет по модулю 3. Значит, таких a, b найти не удастся, значит, p – неразложимый. □

Утверждение 3.15. *Кольцо* $\mathbb{Z}$ *является евклидовым с нормой* $N(z) = |z|$

Доказательство. Проверяем свойства:

1. $|ab| = |a||b| \geq |a|$
2. $\forall a, b : \exists q = \lfloor \frac{a}{b} \rfloor, r = a - qb : a = bq + r$, причем либо $r = 0$, либо $N(r) < N(b)$

$\square$

Утверждение 3.16. *Евклидово кольцо является кольцом главных идеалов, в частности,* $\mathbb{Z}$ *является кольцом главных идеалов.*

Доказательство. Рассмотрим идеал I евклидова кольца K. Если $I = \{0\}$, то он главный. Иначе в I есть ненулевые элементы. Выберем x – элемент I с минимальной нормой. Рассмотрим $y \in I$. Поделим y на x с остатком. $y = qx + r$, где $q \in K$. Тогда $r = y - qx \in I$. Если $r = 0$, то любой $y \in I$ представляется в виде $y = qx$, и тогда $I \subset (x)$. Если $r \neq 0$, тогда $N(r) < N(x)$. Но $r \in I$ и это противоречит выбору x как элементу с минимальной нормой. Значит $I \subset (x)$, но с другой стороны $(x) \subset I$, так как $x \in I$. Получили, что I – главный. $\square$

Утверждение 3.17. *Если* K *– поле, то* $K[x]$ *– евклидово.*

Доказательство. Введём норму $N(p) = \deg p$. Тогда $\deg fg = \deg(a_n x^n + \dots + a_0)(b_m x^m + \dots + b_0) = \deg(a_n b_m x^{n+m} + \dots) = \deg f + \deg g \geq \deg f$. Второе свойство следует из алгоритма деления многочленов столбиком: в результате деления степень остатка всегда меньше степень делителя, ведь иначе мы можем продолжить алгоритм. $\square$

Утверждение 3.18. $\mathbb{Z}[i]$ *евклидово*

Доказательство. Аналогично 2.13 $\square$

Утверждение 3.19. $\mathbb{Z}[\omega]$ *евклидово*

Доказательство. Доказательство содержится в 2.13 $\square$

Утверждение 3.20. *Пусть* $I, J \subset K$ *– идеалы, тогда* $I + J = \{i + j : i \in I, j \in J\}$ *– идеал в* K

Доказательство. Проверяем замкнутость: пусть $i_1 + j_1 \in I + J, i_2 + j_2 \in I + J, k \in K$. Тогда $(i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2) \in I + J, -(i_1 + j_1) = (-i_1) + (-j_1) \in I + J, k(i_1 + j_1) = (ki_1) + (kj_1) \in I + J$ $\square$

Утверждение 3.21. *Пусть* $I, J \subset K$ *– идеалы, тогда* $I \cap J$ *– идеал в* K*.*

Доказательство. Проверяем замкнутость: пусть $x, y \in I \cap J, k \in K$. Тогда $x \in I, x \in J, y \in I, y \in J$. Тогда $x + y, -x, kx \in I, J$ Тогда $x + y, -x, kx \in I \cap J$ $\square$

Утверждение 3.22. *Пусть $I \subset K$ – идеал, тогда радикал $\sqrt{I} = \{a \in K : \exists m \in \mathbb{N} : a^m \in I\}$ тоже является идеалом*

Доказательство. Пусть $x, y \in \sqrt{I}, k \in K$. Пусть $m : x^m \in I, n : y^n \in I$. Тогда $(x+y)^{n+m} \in I$. Значит, $(x+y) \in \sqrt{I}$. Кроме того, $(ky)^m = k^m y^m \in I$. Значит, $ky \in \sqrt{I}$. $(-x)^n = (-1)^n x^n \in I$. Тогда $(-x) \in \sqrt{I}$ □

Утверждение 3.23. *Пусть $K \neq \{0\}$. Тогда K является полем тогда и только тогда, когда K не содержит нетривиальных идеалов.*

Доказательство. Пусть K – поле, а $I \subset K$ – идеал, причем $I \neq \{0\}$. Тогда $\exists x \neq 0 \in I$. Но в этом случае x – обратимый. Тогда $x^{-1}x = 1 \in I$. А значит $I = K$.

Наоборот, пусть K не содержит нетривиальных идеалов. Рассмотрим $x \neq 0 \in K$. $(x) \neq \{0\} \Rightarrow (x) = K$. Тогда $\exists b : bx = 1 \in (x)$. Тогда x – обратимый. □

Утверждение 3.24. *Пусть K – область целостности. Тогда идеал (x) простой тогда и только тогда, когда элемент x простой.*

Доказательство. Пусть (x) – простой. Тогда $(x) \neq \{0\}$ Значит, $x \neq 0$. Кроме того, $(x) \neq K$, значит x не обратимый. Пусть $x|ab$. Тогда $kx = ab$. Тогда $ab \in (x)$. Так как (x) – простой, то либо $a \in (x)$, либо $b \in (x)$. Это означает, что либо $a = ux$, либо $b = vx$. Значит, $x|a$, либо $x|b$.

Пусть x – простой. Тогда он не ноль и не обратимый, тогда $(x) \neq \{0\}, (x) \neq K$. Пусть $ab \in (x)$. Тогда $ab = kx$. Тогда $x|ab$. Так как x – простой, то либо $x|a$, либо $x|b$. Тогда либо $a = ux$, либо $b = vx$. Тогда либо $a \in (x)$, либо $b \in (x)$. □

Утверждение 3.25. *Идеал $(5, x^2+4) \subset \mathbb{Z}[x]$ не простой и не максимальный.*

Доказательство. Пользуемся тем фактом, что I – максимальный идеал в $K \Leftrightarrow K/I$ – поле, I – простой идеал в $K \Leftrightarrow K/i$ – область целостности. $\mathbb{Z}[x]\big/(5, x^2+4) \cong \mathbb{Z}_5[x]\big/(x^2+4)$. Но $x^2+4 = (x-2)(x+2)$, $x^2+4 \in (x^2+4), x-2 \notin (x^2+4), x+2 \notin (x^2+4)$ и идеал (x^2+4) не простой в $\mathbb{Z}_5[x]$. Тогда $\mathbb{Z}_5[x]\big/(x^2+4)$ – не область целостности и не поле, а значит, $(5, x^2+4)$ – не простой и не максимальный. □

Утверждение 3.26. *Идеал $(x^2+1, x+2)$ простой и максимальный.*

Доказательство. $(x^2+1, x+2) = (x^2+1-x(x+2), x+2) = (1-2x, x+2) = (1-2x+2(x+2), x+2) = (5, x+2)$. Аналогично, $\mathbb{Z}[x]\big/(5, x+2) \cong \mathbb{Z}_5[x]\big/(x+2)$. Рассмотрим гомоморфизм $\varphi : \mathbb{Z}_5[x] \mapsto \mathbb{Z}_5$ устроенный таким образом $\varphi(p) = p(-2)$. Тогда $Im\varphi = \mathbb{Z}_5$, $Ker\varphi = (x+2)$. По основной теореме о гомоморфизмах $\mathbb{Z}_5[x]\big/(x+2) \cong \mathbb{Z}_5$, а это поле. Значит, идеал простой и максимальный. □

Утверждение 3.27. *Пусть многочлен* $n = const \in \mathbb{Z}[x]$ *(*$\deg n = 0$*). Тогда* n *– неприводим в* $\mathbb{Z}[x]$ *тогда и только тогда, когда* n *– простой в* $\mathbb{Z}$*.*

Доказательство. Пусть n – неприводим в $\mathbb{Z}[x]$ и n – не простой в $\mathbb{Z}$. Тогда $n = pq$ в $\mathbb{Z}$. Но тогда $n = pq$ в $\mathbb{Z}[x]$. Причем p и q необратимы. Противоречие. Значит n – протой.

Пусть теперь n – простой в $\mathbb{Z}$ и n – приводим в $\mathbb{Z}[x]$. Тогда $\exists f, g \in \mathbb{Z}[x]$: $fg = n$. Но $\deg fg = \deg f + \deg g = 0$. Значит, $f = const, g = const$. Но тогда n приводим в $\mathbb{Z}$, а значит, не простой. Противоречие. $\square$