Глава VIII. Общая теория делимости

§ 1. Простые и неприводимые элементы области целостности

1°. **Основные понятия теории делимости в областях целостности.** Напомним, что областью целостности называется коммутативное ассоциативное кольцо с единицей и без делителей 0.

В предыдущих главах мы уже обсуждали основные понятия делимости. Напомним некоторые из определений и простых утверждений из главы 1. Если Λ – область целостности, и $a, b \in \Lambda$, то говорят, что a делится на b и пишут $a \div b$, если существует такой элемент $c \in \Lambda$, что $a = bc$. Множество всех элементов, делящихся на некоторый элемент $a \in \Lambda$, совпадает с главным идеалом (a) кольца Λ, порожденным элементом a.

Элементы $a, b \in \Lambda$ называются ассоциированными, если $a \div b$, $b \div a$. Для записи того, что a и b ассоциированы, мы применяем обозначение $a \sim b$. Ассоциированность элементов является отношением эквивалентности (т.е. она симметрична, рефлексивна и транзитивна). В отношении делимости ассоциированные элементы ведут себя одинаково: если $a \sim a'$, $b \sim b'$, то a делится на b тогда и только тогда, когда a' делится на b'.

Элемент $\varepsilon \in \Lambda$ называется делителем 1, или обратимым элементом кольца Λ, если $1 \div \varepsilon$. Таким образом, множество всех делителей 1 в кольце Λ совпадает с мультипликативной группой Λ^* обратимых элементов этого кольца. Напомним, что если a – любой элемент из Λ, а ε – делитель 1, то $a \sim a\varepsilon$, и обратно, если элементы a, b из области целостности Λ ассоциированы, то существует такой делитель единицы $\varepsilon \in \Lambda^*$, что $b = a\varepsilon$.

Основные понятия теории делимости удобно интерпретировать на языке идеалов. Пусть $a, b \in \Lambda$; тогда

a делится на b тогда и только тогда, когда $(a) \subseteq (b)$;

a и b ассоциированы тогда и только тогда, когда $(a) = (b)$;

a тогда и только тогда является делителем 1, когда $(a) = (1) = \Lambda$.

2°. **Простые и неприводимые элементы.** В главе 1 при построении теории делимости в кольце целых чисел мы выделили некоторые элементы, которые назвали простыми или неприводимыми. Там слова "простой" и "неприводимый" были двумя терминами для обозначения одного и того же понятия. В общем случае понятия простого и неприводимого элементов приходится различать.

Пусть Λ – область целостности; элемент $p \in \Lambda$ называется неприводимым, если $p \neq 0$, $p \notin \Lambda^*$ и у p нет делителей, отличных от делителей 1 и ассоциированных с p элементов. Иначе говоря (см. гл. I, §5), элемент $p \in \Lambda$, $p \neq 0$, $p \notin \Lambda^*$ не является неприводимым тогда и только тогда, когда существуют такие элементы $c, d \in \Lambda$, не являющиеся делителями 1 и не ассоциированные с p, что $p = cd$. Элемент $p \in \Lambda$ называется простым, если $p \notin \Lambda^*$ и из того, что произведение двух элементов $a, b \in \Lambda$ делится на p следует, что a делится на p или b делится на p. В частности, в области целостности Λ элемент 0 неприводим: если ab делится на 0, то $ab = 0$, а это в области целостности возможно лишь тогда, когда $a = 0$ или $b = 0$.

Предложение 1. *Пусть $p \neq 0$ – простой элемент области целостности Λ. Тогда элемент p неприводим.*

Доказательство. Из определения простого элемента следует, что $p \notin \Lambda^*$. Если элемент p приводим, то существуют такие элементы $c, d \in \Lambda$, не являющиеся делителями 1 и не ассоциированные с p, что $p = cd$. Но тогда произведение cd делится на простой элемент p, и потому один из элементов c, d делится на p. Пусть, например, $c \div p$; но $p = cd \div c$, так что элементы c и p ассоциированы вопреки предположению о том, что оба сомножителя c, d не ассоциированы с p.

Это утверждение не обратимо: существуют такие области целостности, в которых есть неприводимые, но не простые элементы. Примером такой области целостности является множество $\mathbb{Z}(i\sqrt{5})$ комплексных чисел вида $a + bi\sqrt{5}$, где a, b – любые целые числа. Ясно, что сумма, разность и произведение чисел такого вида – снова число такого же вида, так что $\mathbb{Z}(i\sqrt{5})$ – подкольцо поля комплексных чисел $\mathbb{C}$. Далее, $\mathbb{Z}(i\sqrt{5})$ – область целостности, потому что делителей 0 нет не только в $\mathbb{Z}(i\sqrt{5})$, но и в содержащем его поле комплексных чисел $\mathbb{C}$. Покажем, что целое число 3 – не простой, но неприводимый элемент кольца $\mathbb{Z}(i\sqrt{5})$. Действительно, $(2 + i\sqrt{5})(2 - i\sqrt{5}) = 9$ делится на 3, но оба сомножителя $2 + i\sqrt{5}$, $2 - i\sqrt{5}$ не делятся на 3 в $\mathbb{Z}(i\sqrt{5})$; таким образом, 3 – не простой элемент кольца $\mathbb{Z}(i\sqrt{5})$.

Осталось проверить, что 3 – неприводимый элемент кольца $\mathbb{Z}(i\sqrt{5})$. Пусть это не так; тогда существует разложение $3 = (a + bi\sqrt{5})(c + di\sqrt{5})$ с целыми a, b, c, d, в котором оба сомножителя отличны от ± 1. Квадраты модулей левой и правой частей предыдущего равенства совпадают, поэтому мы получаем соотношение

$$9 = (a^2 + 5b^2)(c^2 + 5d^2),$$

откуда следует,что либо оба числа a^2+5b^2, c^2+5d^2 равны 3, либо одно из них равно 9, а другое 1. Но первая возможность не осуществима, так как $a^2 + 5b^2 \geq 5 > 3$, если $b \neq 0$, а при $b = 0$ ни для какого целого числа a не выполняется равенство $a^2 + 5 \cdot 0^2 = 3$. Следовательно, одно из чисел $a^2 + 5b^2$, $c^2 + 5d^2$ равно 1; пусть это будет $a^2 + 5b^2$. Но равенство $a^2 + 5b^2 = 1$ выполняется лишь тогда, когда $a = \pm 1$, $b = 0$, т.е. когда $a + bi\sqrt{5} = \pm 1$. Полученное противоречие доказывает неприводимость числа 3 в кольце $\mathbb{Z}(i\sqrt{5})$.

3°. **Интерпретация простоты и неприводимости элементов в терминах идеалов.** Как мы видели, свойства элементов, связанные с понятием делимости, часто бывает удобно формулировать в терминах главных идеалов, порожденных этими элементами. Выясним, как перевести на язык идеалов понятия простого и неприводимого элементов. Особенно естественно это выглядит для простых элементов.

Сначала дадим одно определение. Идеал $\mathfrak{p}$ коммутативного ассоциативного кольца Λ (не обязательно главный) называется простым идеалом, если $\mathfrak{p} \neq \Lambda$ и факторкольцо $\Lambda/\mathfrak{p}$ не имеет делителей 0 (т.е. является областью целостности).

Предложение 2. *Элемент p из области целостности Λ является простым тогда и только тогда, когда простым является порожденный им главный идеал (p).*

Доказательство. Пусть π – канонический эпиморфизм кольца Λ на факторкольцо $\Lambda/(p)$; его ядро совпадает с идеалом (p). Если (p) – простой идеал, то $\Lambda/(p)$ – область целостности; из того, что произведение ab двух элементов из Λ делится на p, следует, что произведение $\pi(a)\pi(b) = \pi(ab)$ – нулевой элемент факторкольца, и потому равен 0 один из элементов $\pi(a), \pi(b)$, т.е. один из элементов a, b принадлежит $\operatorname{Ker}\pi = (p)$ и потому делится на p. Следовательно, p – простой элемент кольца Λ.

Обратно, пусть p – простой элемент кольца Λ; покажем, что идеал p простой, т.е. факторкольцо $\Lambda/(p)$ – область целостности. Пусть $\bar{a}, \bar{b} \in \Lambda/(p)$, $\bar{a}\bar{b} = 0$; покажем, что $\bar{a} = 0$ или $\bar{b} = 0$. Существуют элементы $a, b \in \Lambda$, такие что $\pi(a) = \bar{a}$, $\pi(b) = \bar{b}$; тогда $\pi(ab) = \pi(a)\pi(b) = \bar{a}\bar{b} = 0$, а значит, $ab \in \operatorname{Ker}\pi = (p)$, т.е. ab делится на p. Но p – простой элемент кольца Λ, и потому a делится на p или b делится на p; в первом случае $\bar{a} = \pi(a) = 0$, во втором – $\bar{b} = \pi(b) = 0$.

Предложение 3. *Элемент $p \neq 0$ из области целостности Λ неприводим тогда и только тогда, когда $(p) \neq \Lambda$ и всякий главный идеал (a) кольца Λ, такой что*

$(p) \subseteq (a)$ *и* $(a) \neq \Lambda$, *совпадает с* (p). *Иными словами, элемент* p *неприводим, когда идеал* (p) *является максимальным в множестве главных идеалов кольца* Λ, *не совпадающих со всем кольцом* Λ.

Доказательство. Пусть p – неприводимый элемент кольца Λ; если a – такой элемент из Λ, что $(a) \neq \Lambda = (1)$, $(a) \supseteq (p)$, то p делится на a, причем a – не делитель 1. Поскольку элемент p неприводим, отсюда следует, что a и p ассоциированы, и потому $(a) = (p)$. Обратно, пусть всякий главный идеал, содержащий (p) и не совпадающий с Λ, равен (p); если тогда a – делитель p, не являющийся делителем 1, то $\Lambda = (1) \neq (a) \supseteq (p)$, и потому $(a) = (p)$, а это значит, что делитель a элемента p ассоциирован с p.

4°. **Условие обрыва цепей делителей.** Говорят, что в области целостности Λ выполняется условие обрыва цепей делителей, если для любой последовательности элементов $a_1, a_2, \ldots$ элементов из Λ, такой, что каждый следующий элемент a_{i+1} делит предыдущий элемент a_i, найдется такой номер n, что все элементы a_m, для которых $m \geq n$, ассоциированы с a_n. Переформулировкой этого условия в терминах идеалов является следующее условие обрыва возрастающих цепей главных идеалов: для любых элементов $a_1, a_2, a_3, \ldots \in \Lambda$, таких что $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \ldots$, найдется такой номер n, что все идеалы (a_m), начиная с n-го, совпадают друг с другом.

Лемма 1. *Если в кольце* Λ *выполняется условие обрыва цепей делителей, то всякий элемент* $a \in \Lambda$, *такой что* $a \neq 0$, $a \notin \Lambda^*$, *делится хотя бы на один неприводимый в кольце* Λ *элемент.*

Доказательство. Построим цепочку элементов $a_1, a_2, \cdots \in \Lambda$ следующим образом:

1. Полагаем $a_1 = a$;

2. Пусть элемент a_i уже определен; если a_i не является неприводимым, то у a_i есть делители, не ассоциированные с a_i и не делящие 1, и мы возьмем в качестве a_{i+1} любой из таких делителей. Если же a_i – неприводимый элемент, то мы останавливаем построение.

Ясно, что в последовательности $a_1, a_2, \ldots$ каждый следующий элемент делит предыдущий и не ассоциирован с ним. Но в кольце, в котором выполняется условие обрыва цепей делителей, не существует бесконечных последовательностей, удовлетворяющих этим условиям. Следовательно, процесс построения элементов a_i останавливается через конечное число шагов, а он может остановиться только тогда, когда очередной элемент a_n окажется неприводимым. Итак, у элемента $a = a_1$ найдется неприводимый делитель a_n.

Предложение 4. *Если в кольце* Λ *выполняется условие обрыва цепей делителей, то всякий ненулевой элемент* $a \in \Lambda$ *представим в виде произведения* $a = \varepsilon p_1 \ldots p_n$, *где* ε – *делитель* 1, $n \geq 0$, *а* $p_1, \ldots, p_n$ – *неприводимые элементы кольца* Λ.

Замечание. *Сомножитель* ε *важен только в случае, если* $a = \varepsilon$ – *делитель 1. В противном случае* $n \geq 1$, *и мы можем заменить первый неприводимый сомножитель* p_1 *на ассоциированный с ним и тоже неприводимый элемент* εp_1, *и тем самым избавиться от делителя 1 в разложении элемента* a.

Доказательство. Построим цепочку ненулевых элементов $a_0, a_1, a_2, \cdots \in \Lambda$ и цепочку неприводимых элементов $p_1, p_2, \ldots$ следующим образом:

1. Полагаем $a_0 = a$;

2. Пусть $i \geq 0$ и элемент a_i уже определен. Если a_i – делитель 1, то полагаем $\varepsilon = a_i$ и останавливаем построение. Если a_i – не делитель 1, то в качестве p_{i+1} берем любой неприводимый делитель элемента a_i (такой неприводимый делитель

существует по лемме 1), а в качестве a_{i+1} – тот элемент из Λ, для которого $a_i = p_{i+1}a_{i+1}$.

Ясно, что в последовательности $a = a_0, a_1, a_2, \ldots$ каждый следующий элемент делит предыдущий и не ассоциирован с ним. Но в кольце, в котором выполняется условие обрыва цепей делителей, не существует бесконечных последовательностей, удовлетворяющих этим условиям. Следовательно, процесс построения останавливается через конечное число шагов, а он может остановиться только тогда, когда очередной элемент a_n окажется делителем 1. Тогда будут выполняться соотношения

$$a = a_0 = p_1 a_1, \;\; a_1 = p_2 a_2, \;\; \ldots \;\; a_{n-1} = p_n a_n = p_n \varepsilon,$$

из которых легко получается, что $a = \varepsilon p_1 \ldots p_n$. По нашему построению элементы $p_1, \ldots, p_n$ неприводимы, а элемент ε – делитель 1.

§ 2. Факториальные кольца

1°. **Определение факториального кольца.** У нас уже встречались кольца, в которых каждый элемент однозначно раскладывается в произведение неприводимых элементов – это кольцо целых чисел $\mathbb{Z}$ и кольцо многочленов от одной переменной над полем $k[x]$. Мы будем теперь изучать произвольные кольца, для которых выполняется аналогичное утверждение.

Область целостности Λ называется факториальным кольцом, если всякий элемент $a \in \Lambda$, $a \neq 0$ представляется в виде $a = \varepsilon p_1 \ldots p_n$, где ε – делитель 1, $n \geq 0$, а $p_1, \ldots, p_n$ – неприводимые элементы, причем это представление единственно с точностью до ассоциированности и порядка сомножителей. Последнее означает, что если $a = \delta q_1 \ldots q_m$ – другое представление того же элемента a в виде произведения делителя единицы δ и неприводимых элементов $q_1, \ldots, q_m$, то $m = n$, и можно так перенумеровать элементы $p_1, \ldots, p_n$, что $p_1 \sim q_1$, ... , $p_n \sim q_n$.

Из самого определения факториального кольца следуют некоторые важные его свойства. Пусть Λ – факториальное кольцо. Множество всех неприводимых элементов кольца Λ разбивается на классы ассоцированных элементов; произвольным образом выберем в этих классах представителей. Пусть $\{p_i\}_{i \in I}$ будет множество всех так выбранных представителей. Еще раз подчеркнем: все элементы p_i неприводимы, попарно не ассоциированы и для каждого неприводимого элемента p кольца Λ найдется такой индекс $i \in I$, что $p \sim p_i$. Заметим, что для колец $\mathbb{Z}$ и $k[x]$ нам удавалось выбрать представителей p_i каноническим образом (в первом случае это были положительные простые числа, а во втором – унитарные многочлены); для других колец это далеко не всегда возможно.

Предложение 1. *В обозначениях предыдущего абзаца каждый элемент $a \in \Lambda$, не равный 0, однозначно представляется в виде $a = \varepsilon \prod\limits_{i \in I} p_i^{s_i}$, где ε – делитель 1, а s_i – неотрицательные целые числа, почти все (т.е. все, кроме конечного числа) равные 0, так что на самом деле предыдущее произведение конечно. Далее, пусть*

$$a = \varepsilon \prod_{i \in I} p_i^{s_i}, \quad b = \delta \prod_{i \in I} p_i^{t_i} \qquad (\varepsilon, \delta \in \Lambda^*, \;\; s_i, t_i \geq 0 \text{ и почти все равны } 0).$$

Тогда

(1) *a делится на b тогда и только тогда, когда $s_i \geq t_i$ для всех $i \in I$;*
(2) *a и b ассоциированы тогда и только тогда, когда $s_i = t_i$ для всех $i \in I$;*
(3) *если a делится на b и $b \notin \Lambda^*$, то b делится хотя бы на один неприводимый элемент p_i, входящий в разложение элемента a с показателем $s_i \geq 1$;*

(4) *элемент* $d = \prod\limits_{i\in I} p_i^{\min(s_i,t_i)}$ *является наибольшим общим делителем элементов* a *и* b*;*

(5) *если* a *и* b *взаимно просты (т.е.* 1 *– их наибольший общий делитель) и произведение элемента* ab *и* n*-й степени какого-то элемента из* Λ *снова является* n*-й степенью некоторого элемента из* Λ $(n \geq 1)$*, то существуют такие элементы* $a_1, b_1 \in \Lambda$*, что* $a = \varepsilon a_1^n$*,* $b = \delta b_1^n$*.*

Доказательство. Утверждение, сформулированное в начале предложения, очевидным образом следует из факториальности. Докажем остальные утверждения.

(1) Если a делится на b, то существует элемент $c = \gamma \prod\limits_{i\in I} p_i^{u_i} \in \Lambda$, такой что $a = bc$ (здесь $\gamma \in \Lambda^*$, а u_i – неотрицательные целые числа, почти все равные 0). Тогда

$$\varepsilon \prod_{i\in I} p_i^{s_i} = a = bc = \delta \prod_{i\in I} p_i^{t_i} \cdot \gamma \prod_{i\in I} p_i^{u_i} = \delta\gamma \prod_{i\in I} p_i^{t_i+u_i},$$

откуда, в силу единственности представления элемента в виде произведения степеней неприводимых элементов p_i, следует, что $s_i = t_i + u_i \geq t_i$.

(2) Если a делится на b и b делится на a, то по (1) для любого $i \in I$ выполняются неравенства $s_i \geq t_i$, $t_i \geq s_i$.

(3) Поскольку b – не делитель 1, существует индекс $i \in I$, такой что $t_i \geq 1$. Тогда b делится на неприводимый элемент p_i; но a делится на b, и $s_i \geq t_i \geq 1$ по утверждению (1).

(4) По утверждению (1), элементы a и b делятся на d. Если элементы a и b делятся на элемент $d_1 = \gamma \prod\limits_{i\in I} p_i^{v_i}$ (где, как всегда $\gamma \in \Lambda^*$, а v_i – неотрицательные целые числа, почти все равные 0), то для всех $i \in I$ будет $v_i \leq s_i, t_i$, а потому $v_i \leq \min(s_i, t_i)$, и, значит, d делится на d_1.

(5) Если a и b взаимно просты, то для любого $i \in I$ хотя бы одно из чисел s_i, t_i равно 0. Пусть

$$\big(\gamma_1 \prod_{i\in I} p_i^{v_i}\big)^n \varepsilon\delta \prod_{i\in I} p_i^{s_i+t_i} = \big(\gamma_1 \prod_{i\in I} p_i^{v_i}\big)^n ab = \big(\gamma \prod_{i\in I} p_i^{u_i}\big)^n.$$

Тогда для любого $i \in I$ будет выполнено равенство $nv_i + s_i + t_i = nu_i$, и поскольку одно из чисел s_i, t_i равно 0 и потому делится на n, другое из этих чисел тоже делится на n. Итак, все показатели степеней s_i, t_i делятся на n, и, значит,

$$a = \varepsilon\big(\prod_{i\in I} p_i^{s_i/n}\big)^n, \quad b = \delta\big(\prod_{i\in I} p_i^{t_i}\big)^n.$$

Замечание. *Из утверждения* (4) *следует, что в факториальных кольцах для любых двух элементов* a*,* b *существует их наибольший общий делитель* d*. Однако, в отличие от колец* $\mathbb{Z}$*,* $k[x]$ *и других областей главных идеалов, он не обязательно линейно выражается через* a *и* b*, и значит, вообще говоря,* $(d) \neq (a, b)$*. Поэтому для общих факториальных колец не стоит использовать привычное обозначение* (a, b) *для наибольшего общего делителя элементов* a*,* b*; оно удобно только для колец главных идеалов.*

2°. **Длина элемента факториального кольца.** Пусть Λ – факториальное кольцо, и пусть $a \neq 0$ – элемент из Λ. Тогда существует разложение $a = \varepsilon p_1 \dots p_n$, где ε – делитель 1, а $p_1, \dots, p_n$ – неприводимые элементы; количество n неприводимых сомножителей не зависит от разложения; оно называется длиной элемента a и обозначается $l(a)$. Заметим, что длина $l(a)$ ненулевого элемента $a \in \Lambda$ всегда неотрицательна.

Лемма 1. *Пусть* a, b *– ненулевые элементы факториального кольца* Λ*. Тогда* $l(ab) = l(a) + l(b)$*. Длина* $l(a)$ *элемента* a *равна* 0 *тогда и только тогда, когда* a

– *делитель* 1. *Если* a *делится на* b, *то* $l(a) \geq l(b)$; *если же при этом* $l(a) = l(b)$, *то элементы* a *и* b *ассоциированы.*

Доказательство. Пусть $a = a = \varepsilon p_1 \dots p_n$, $b = \delta q_1 \dots q_m$, где ε, δ – делители 1, а $p_1, \dots, p_n, q_1, \dots, q_m$ – неприводимые элементы. Тогда $ab = \varepsilon\delta p_1 \dots p_n q_1 \dots q_m$, и мы видим, что $l(a) = m$, $l(b) = n$, $l(ab) = n + m = l(a) + l(b)$, и первое утверждение леммы доказано. Второе утверждение очевидно. Если a делится на b, то существует элемент $c \in \Lambda$, такой что $a = bc$; тогда $l(a) = l(b) + l(c) \geq l(b)$, и если $l(a) = l(b)$, то $l(c) = 0$ и c – делитель 1, так что $a = bc \sim b$.

3°. **Необходимые и достаточные условия факториальности кольца.**

Теорема 1. *Пусть* Λ – *область целостности. Для того, чтобы кольцо* Λ *было факториальным кольцом, необходимо и достаточно, чтобы в кольце* Λ *выполнялось условие обрыва цепей делителей и чтобы всякий неприводимый элемент кольца* Λ *был простым.*

Доказательство. Необходимость. Пусть Λ – факториальное кольцо, и пусть $a_1, a_2, \dots$ – такие элементы, что для любого $i \geq 1$ элемент a_i делится на a_{i+1}. Если все элементы a_i равны 0, то они ассоциированы. Пусть среди элементов a_i есть ненулевой элемент a_m; тогда все последующие элементы a_n, где $n \geq m$, делят a_m и потому тоже отличны от 0. По лемме 1 мы получаем невозрастающую цепочку неотрицательных целых чисел $l(a_m) \geq l(a_{m+1}) \geq l(a_{m+2}) \geq \dots$. В этой цепочке количество строгих неравенств конечно (оно не больше, чем $l(a_m)$), и потому, начиная с некоторого места, все неравенства превращаются в равенства. Таким образом, существует такой номер n, что $l(a_s) = l(a_n)$ для всех $s \geq n$. Поскольку при этом a_n делится на a_s, мы получаем, что все элементы a_s при $s \geq n$ ассоциированы с a_n. Тем самым мы доказали, что в Λ выполняется условие обрыва цепей делителей.

Пусть теперь p – любой неприводимый элемент кольца Λ; покажем, что он является простым. Пусть a, b – элементы из Λ, произведение которых делится на p. Если один из элементов a, b равен 0, то он делится на p; пусть теперь $a \neq 0$, $b \neq 0$. Существует элемент $c \in \Lambda$, такой что $ab = pc$; при этом $c \neq 0$, потому что Λ – область целостности, и поэтому $ab \neq 0$. Поскольку Λ – факториальное кольцо, элементы a, b, c раскладываются в произведения

$$a = \varepsilon p_1 \dots p_m, \qquad b = \delta p_{m+1} \dots p_n, \qquad c = \gamma q_1 \dots q_r,$$

в которых γ, δ, ϵ – делители 1, а $p_1, \dots, p_n, q_1, \dots, q_r$ – неприводимые элементы. Мы получаем равенство

$$\varepsilon\delta p_1 \dots p_m p_{m+1} \dots p_n = ab = pc = \gamma p q_1 \dots q_r;$$

из единственности (с точностью до порядка сомножителей и ассоциированности) разложения элемента факториального кольца в произведение неприводимых элементов мы получаем теперь, что найдется сомножитель p_i левой части последнего равенства, который ассоциирован с p ($1 \leq i \leq n$). Если $i \leq m$, то a делится на p, а если $i > m$, то b делится на p. Итак, мы показали, что если произведение ab двух элементов кольца Λ делится на неприводимый элемент p, то один из сомножителей a, b делится на p; а это значит, что p – простой элемент кольца Λ.

Достаточность. Пусть Λ – область целостности, в которой выполнено условие обрыва цепей делителей и в которой всякий неприводимый элемент является простым. Существование разложения $a = \varepsilon p_1 \dots p_n$ любого ненулевого элемента $a \in \Lambda$ в произведение делителя единицы ε и неприводимых элементов $p_1, \dots, p_n$

было уже доказано в предложении 1.4. Остается доказать единственность разложения; это делается буквальным повторением рассуждений, которые были использованы ранее для доказательства этого утверждения в двух частных случаях, когда Λ было кольцом целых чисел или кольцом многочленов от одной переменной над полем.

Пусть $\varepsilon p_1 \dots p_n = \delta q_1 \dots q_m$, где ε, δ – делители 1, а $p_1, \dots, p_n, q_1, \dots, q_m$ – неприводимые, а потому простые элементы кольца Λ. Для определенности будем считать $n \geq m$ (если это не так, мы просто переменим обозначения). Индукцией по m докажем, что $n = m$ и можно так перенумеровать элементы p_i, что $p_i \sim q_i$ для всех i, $1 \leq i \leq n$. Случай $m = 0$ тривиален: делитель единицы δ не может делиться на неприводимый элемент p_1, который не является делителем 1, и потому в первом разложении нет ни одного неприводимого сомножителя, т.е. $n = 0$. Пусть $m \geq 1$ и для меньших значений этого параметра утверждение уже доказано. Элемент $\varepsilon p_1 \dots p_n = \delta q_1 \dots q_m$ делится на q_1. Поскольку неприводимый элемент q_1 является простым, а делитель единицы ε не делится на q_1, один из элементов $p_1, \dots, p_n$ делится на q_1. Изменив, если надо, нумерацию элементов p_i, можем считать, что p_1 делится на q_1 и потому $p_1 \sim q_1$ (ведь у неприводимого элемента p_1 нет делителей, кроме делителей 1 и ассоциированных с p_1 элементов, а неприводимый элемент q_1 – не делитель 1). Значит, существует такой делитель единицы γ, что $p_1 = \gamma q_1$. Тогда

$$\delta q_1 q_2 \dots q_m = \varepsilon p_1 \dots p_n = \varepsilon\gamma q_1 p_2 \dots p_n.$$

Сокращая на множитель $q_1 \neq 0$, получим, что $\delta q_2 \dots q_m = \varepsilon\gamma p_2 \dots p_n$. К этому равенству применимо предположение индукции, согласно которому $m-1 = n-1$, т.е. $m = n$, и можно так перенумеровать элементы $p_2, \dots, p_n$, что $p_2 \sim q_2$, ... , $p_m \sim q_m$ (соотношение $p_1 \sim q_1$ было получено ранее).

4°. **Факториальность областей главных идеалов.** Покажем, что факториальными являются не только кольца $\mathbb{Z}$ и $k[x]$, где k – поле, но и все области главных идеалов.

Теорема 2. *Всякая область главных идеалов является факториальным кольцом.*

Доказательство. По теореме 1 достаточно показать, что в любой области главных идеалов Λ выполнено условие обрыва возрастающих цепей главных идеалов и что всякий неприводимый элемент кольца Λ является простым; это и будет сделано ниже в леммах 3 и 4.

Лемма 2. *Пусть Λ – любое коммутативное кольцо, и пусть для каждого натурального n задан идеал I_n кольца Λ, причем при $m \leq n$ идеал I_m содержится в идеале I_n. Тогда объединение всех этих идеалов $I = \bigcup\limits_{s=1}^{\infty} I_s$ является идеалом кольца Λ.*

Доказательство. Надо доказать, что если $x, y \in I$ и $a \in \Lambda$, то $ax + y \in I$. Поскольку $x, y \in I = \bigcup\limits_{s=1}^{\infty} I_s$, существуют такие индексы m, n, что $x \in I_m$, $y \in I_n$. Пусть l – любое натуральное число, такое что $m, n \leq l$; по условию $I_m, I_n \subseteq I_l$, поэтому элементы x, y принадлежат идеалу I_l, а тогда и элемент $ax + y$ принадлежит идеалу $I_l \subseteq \bigcup\limits_{s=1}^{\infty} I_s = I$.

Лемма 3. *Пусть Λ – область главных идеалов и пусть для каждого натурального n задан идеал I_n кольца Λ, причем при $m \leq n$ идеал I_m содержится в идеале I_n. Тогда существует такой номер n, что все идеалы I_m с номерами $m \geq n$ совпадают с I_n.*

Доказательство. По предыдущей лемме объединение всех этих идеалов $I = \bigcup_{s=1}^{\infty} I_s$ – идеал кольца Λ. Но все идеалы кольца Λ главные, поэтому существует такой элемент $a \in I$, что $I = (a)$. Поскольку I – объединение всех идеалов I_s, а $a \in I$, найдется такой номер n, что $a \in I_n$. Тогда, очевидно, $(a) \subseteq I_n$, и для любого $m \geq n$ мы получим

$$I_n \subseteq I_m \subseteq I = (a) \subseteq I_n,$$

откуда видно, что $I_m = I_n$.

Лемма 4. *Пусть Λ – область главных идеалов. Тогда любой неприводимый элемент p кольца Λ является простым элементом этого кольца.*

Доказательство. Надо доказать, что если a, b – такие элементы кольца Λ, что a не делится на p, а произведение ab делится на p, то b делится на p. Множество $(a, p) = \{ax + py \,|\, x, y \in \Lambda\}$ является идеалом Λ; но все идеалы кольца Λ главные, поэтому существует такой элемент $d \in (a, p)$, что $(a, p) = (d)$. Элементы $a = a \cdot 1 + p \cdot 0$, $p = a \cdot 0 + p \cdot 1$ принадлежат идеалу $(a, p) = (d)$ и потому делятся на d. Но у неприводимого элемента p нет делителей, кроме ассоциированных с p и делителей 1. Если $d \sim p$, то элемент a, который делится на d, делился бы и на ассоциированный с d элемент p, но это не так; следовательно, d – делитель 1, т.е. обратимый элемент кольца Λ. Поскольку $d \in (a, b)$, существуют такие $x, y \in \Lambda$, что $d = ax + py$; домножая обе части этого равенства на bd^{-1}, увидим, что элемент $b = (ab)d^{-1}x + pbd^{-1}y$ делится на p.

5°. **Евклидовы кольца.** Мы доказывали, что кольца целых чисел и многочленов от одной переменной над полем являются областями главных идеалов, используя то, что в этих кольцах есть деление с остатком. В этом пункте мы обобщим это рассуждение на произвольные кольца, в которых есть что-то похожее на деление с остатком.

Область целостности Λ называется евклидовым кольцом, если существует такая функция φ, сопоставляющая каждому ненулевому элементу a кольца Λ неотрицательное целое число $\varphi(a)$, что выполняется следующее свойство: если $a, b \in \Lambda$, $b \neq 0$ и a не делится на b, то существуют такие элементы $q, r \in \Lambda$, что $a = bq + r$ и $\varphi(r) < \varphi(b)$.

Упомянутые выше кольца $\mathbb{Z}$ и $k[x]$ (где k – поле) являются евклидовыми кольцами; для первого из них нашему условию удовлетворяет функция $\varphi(a) = |a|$, а для второго – функция $\varphi(f(x)) = \deg f(x)$ $(a \in \mathbb{Z},\ f(x) \in k[x])$.

Теорема 3. *Всякое евклидово кольцо является областью главных идеалов и, следовательно, факториальным кольцом.*

Доказательство. Пусть Λ – область целостности, и пусть $\varphi : \Lambda \setminus \{0\} \to \mathbb{N}_0$ – функция, удовлетворяющая условию из определения евклидова кольца. Пусть I – произвольный идеал кольца Λ. Если I состоит только из 0, то $I = (0)$ – главный идеал. Если же в I есть и ненулевые элементы, то множество неотрицательных целых чисел $\{\varphi(a) \,|\, a \in I, a \neq 0\}$ непусто, и потому в нем есть наименьший элемент n. Пусть $b \in I$ – элемент из идеала I, для которого $\varphi(b)$ принимает это наименьшее значение n; покажем, что $I = (b)$. Если $a \in I$ и a не делится на b, то существуют такие элементы $q, r \in \Lambda$, что $a = bq + r$ и $\varphi(r) < \varphi(b)$; тогда $r = a - bq \in I$, $\varphi(r) < \varphi(b) = n$, а это противоречит тому, что n – наименьший элемент множества $\{\varphi(a) \,|\, a \in I, a \neq 0\}$. Следовательно, всякий элемент $a \in I$ делится на b, т.е. $I \subseteq (b)$. Поскольку $b \in I$, верно и обратное включение $(b) \subseteq I$. Таким образом, произвольный идеал I кольца евклидова кольца Λ оказался главным идеалом.

6°. **Кольцо целых чисел Гаусса.** Целым числом Гаусса называется комплексное число $a+bi$, у которого вещественная часть a и коэффициент мнимой части b – целые числа. Будем обозначать это множество через $\mathbb{G}$. Таким образом,

$$\mathbb{G} = \{a+bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}.$$

Теорема 4. *Множество $\mathbb{G}$ целых чисел Гаусса является подкольцом поля комплексных чисел $\mathbb{C}$. Кольцо $\mathbb{G}$ евклидово, а потому факториально.*

Доказательство. Первое утверждение тривиально: если $a+bi, c+di \in \mathbb{G}$, то $a, b, c, d \in \mathbb{Z}$, и потому

$$(a+bi)\pm(c+di) = (a\pm c)+(b\pm d)i \in \mathbb{G}, \qquad (a+bi)(c+di) = (ac-bd)+(ad+bc)i \in \mathbb{G}.$$

Положим $\varphi(a+bi) = |a+bi|^2 = a^2+b^2$ и покажем, что в $\mathbb{G}$ возможно деление с остатком. Пусть $a+bi, c+di \in \mathbb{G}$, причем $c+di \neq 0$. Пусть $\alpha+\beta i$ – частное от деления $a+bi$ на $c+di$ в поле комплексных чисел $\mathbb{C}$ ($\alpha, \beta \in \mathbb{R}$). Существуют такие целые числа u, v, что $|\alpha-u|, |\beta-v| \leq 1/2$; положим $r = ((\alpha-u)+(\beta-v)i)(c+di)$. Тогда $r = (\alpha+\beta i)(c+di) - (u+vi)(c+di) = (a+bi) - (u+vi)(c+di) \in \mathbb{G}$. Далее,

$$\varphi(r) = |((\alpha-u)+(\beta-v)i)(c+di)|^2 = |(\alpha-u)+(\beta-v)i|^2|c+di|^2 =$$
$$= ((\alpha-u)^2+(\beta-v)^2)\varphi(c+di) \leq ((1/2)^2+(1/2)^2)\varphi(c+di) < \varphi(c+di).$$

Таким образом, в кольце $\mathbb{G}$ нашлись элементы $q = u+vi$, r, для которых

$$a+bi = (c+di)q + r, \qquad \varphi(r) < \varphi(c+di).$$

7°. **Делители 1 и простые элементы кольца целых чисел Гаусса.** Из теоремы 4 следует, что в кольце целых чисел Гаусса теория делимости такая же, как в кольце целых чисел; для полноты картины остается только выяснить, какие элементы этого кольца являются делителями 1 и какие элементы являются простыми (напомним, что в факториальном кольце понятия ненулевого простого элемента и неприводимого элемента совпадают). Этим мы сейчас и займемся.

Предложение 2. *Множество делителей 1 в кольце целых чисел Гаусса $\mathbb{G}$ состоит из чисел $\pm 1, \pm i$.*

Доказательство. Ясно, что $\pm 1, \pm i$ – делители 1. Если $a+bi$, где $a, b \in \mathbb{Z}$ – делитель 1 в $\mathbb{G}$, то $1 = |1|^2$ делится на $a^2+b^2 = |a+bi|^2$ в кольце $\mathbb{Z}$, и потому $a^2+b^2 = 1$. Для целых чисел a, b это возможно только при $a = \pm 1, b = 0$ или $a = 0, b = \pm 1$.

Следствие. *Если элемент $\alpha \in \mathbb{G}$ ассоциирован со своим комплексно сопряженным элементом $\bar{\alpha}$, то существует такое целое число $a \in \mathbb{Z}$, что α имеет один из видов* $\alpha = a, \quad \alpha = ai, \quad \alpha = a(1 \pm i)$.

Доказательство. Пусть $\alpha = a+bi$, где $a, b \in \mathbb{Z}$. Если $\alpha \sim \bar{\alpha}$, то существует делитель единицы ε, такой что $\bar{\alpha} = \varepsilon\alpha$. Но делителями 1 в $\mathbb{G}$ являются лишь числа ± 1, $\pm i$, поэтому выполняется одно из соотношений

$$a-bi = a+bi, \qquad a-bi = -(a+bi), \qquad a-bi = \pm i(a+bi),$$

и значит, $b = 0$, или $a = 0$, или $b = \pm a$.

В следующей лемме собраны некоторые простейшие свойства элементов из $\mathbb{G}$.

Лемма 5. (1) *Если $\alpha \in \mathbb{G}$, то $\bar{\alpha} \in \mathbb{G}$.*

(2) *Если $\alpha, \beta \in \mathbb{G}$ и α делится на β, то $\bar{\alpha}$ делится на $\bar{\beta}$.*

(3) *Если целое число $a \in \mathbb{Z}$ делится в $\mathbb{G}$ на целое число Гаусса α, то a делится в $\mathbb{G}$ и на $\bar{\alpha}$.*

(4) *Если элементы $\alpha, \beta \in \mathbb{G}$ ассоциированы, то и элементы $\bar{\alpha}, \bar{\beta}$ ассоциированы.*

(5) *Если π – простой элемент кольца $\mathbb{G}$, то $\bar{\pi}$ – простой элемент кольца $\mathbb{G}$.*

(6) *Если простое целое число $p > 0$ делится в $\mathbb{G}$ на простой элемент π кольца $\mathbb{G}$, то или p ассоциировано с π, или $p = \pi\bar{\pi}$.*

Доказательство. (1) Если $\alpha \in \mathbb{G}$, то по определению кольца $\mathbb{G}$ существуют такие целые числа $a, b \in \mathbb{Z}$, что $\alpha = a + bi$; тогда $\bar{\alpha} = a - bi \in \mathbb{G}$.

(2) Если α делится на β, то существует элемент $\gamma \in \mathbb{G}$, такой что $\alpha = \beta\gamma$; тогда элемент $\bar{\alpha} = \bar{\beta}\bar{\gamma}$ делится на $\bar{\beta}$.

(3) Если $a \in \mathbb{Z}$ делится на α, то по (2) число $a = \bar{a}$ делится на $\bar{\alpha}$.

(4) Если α делится на β, β делится на α, то по (2) $\bar{\alpha}$ делится на $\bar{\beta}$, $\bar{\beta}$ делится на $\bar{\alpha}$.

(5) Пусть π – простой элемент кольца $\mathbb{G}$. Вместе с π элемент $\bar{\pi}$ не делит 1. Если произведение элементов $\alpha, \beta \in \mathbb{G}$ делится на $\bar{\pi}$, то $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$ делится на простой элемент π, а потому одно из чисел Гаусса $\bar{\alpha}, \bar{\beta}$ делится на π, а тогда одно из чисел α, β делится на $\bar{\pi}$.

(6) Пусть положительное простое число $p \in \mathbb{Z}$ делится на простой элемент π кольца $\mathbb{G}$. Тогда по (3) число p делится также и на $\bar{\pi}$, откуда следует, что p^2 делится на $\pi\bar{\pi}$. Но $\pi\bar{\pi} = |\pi|^2$ – целое положительное число, и для произведения $\pi\bar{\pi}$ есть лишь три возможности: $\pi\bar{\pi} = p^2$, $\pi\bar{\pi} = p$, $\pi\bar{\pi} = 1$. Последний случай надо исключить, так как простой элемент π не является делителем 1. Если $\pi\bar{\pi} = p^2$, то из единственности разложения в произведение простых элементов следует, что число p остается простым и в $\mathbb{G}$ (иначе произведение двух простых элементов $\pi\bar{\pi}$ равнялось бы произведению большего числа простых элементов), и что оно ассоциировано с π и $\bar{\pi}$.

Теорема 5. *Всякий ненулевой простой элемент кольца целых чисел Гаусса $\mathbb{G}$ является делителем некоторого простого числа $p \in \mathbb{Z}$, $p > 0$. У числа 2 с точностью до ассоциированности есть единственный простой делитель $1+i$. Нечетные простые числа, сравнимые с 3 по модулю 4, остаются простыми и в $\mathbb{G}$. У нечетного простого числа, сравнимого с 1 по модулю 4 с точностью до ассоциированности есть ровно два простых делителя, комплексно сопряженных друг с другом.*

Доказательство. Пусть π – простой элемент кольца $\mathbb{G}$; тогда квадрат его модуля $n = \pi\bar{\pi}$ является целым рациональным числом и делится на π. Разложим n в произведение $p_1 \dots p_r$ простых чисел $p_s \in \mathbb{Z}$; это произведение делится на простой элемент π кольца $\mathbb{G}$, и потому на π делится один из простых сомножителей p_s.

Простое число 2 раскладывается в $\mathbb{G}$ в произведение $2 = (1+i)(1-i) = -i(1+i)^2 \sim (1+i)^2$. Нетрудно видеть, что элемент $1+i$ неприводим: если $1+i = \alpha\beta$, где $\alpha, \beta \in \mathbb{G}$, то $2 = |1+i|^2 = |\alpha|^2|\beta|^2$, и одно из положительных целых рациональных чисел $|\alpha|^2| = \alpha\bar{\alpha}$, $|\beta|^2| = \beta\bar{\beta}$ равно 1, а это значит, что одно из целых чисел Гаусса α, β – делитель 1.

Пусть теперь $p > 0$ – простое целое рациональное число, сравнимое с 3 по модулю 4. Если $\pi = a+bi$ – простой делитель p в $\mathbb{G}$, не ассоциированный с p, то по утверждению (6) леммы 5 мы получили бы, что $p = \pi\bar{\pi} = (a+bi)(a-bi) = a^2+b^2$. Но это невозможно, так как сумма квадратов четных чисел делится на 4, сумма квадратов нечетных чисел сравнима с 2 по модулю 4, а сумма квадратов четного и нечетного чисел сравнима с 1 по модулю 4; остаток же 3 при делении на 4 никогда не может появиться. Следовательно, число p ассоциировано с простым элементом π кольца $\mathbb{G}$ и потому само является простым элементом этого кольца.

Наконец, пусть $p > 0$ – простое рациональное число, сравнимое с 1 по модулю 4. Согласно результатам главы I,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p};$$

следовательно, при $p \equiv 1 \pmod 4$ число -1 является квадратичным вычетом, и поэтому существует целое число x, такое что $x^2 \equiv -1 \pmod p$. Можно считать, заменив, если надо, число x на его остаток от деления на p, что $0 < x \leq p-1$; тогда x^2+1 делится на p, но не делится на p^2, потому что $x^2+1 \leq (p-1)^2+1 = p^2-2p < p^2$.

Разложим целое число Гаусса $x+i$ в произведение простых элементов кольца $\mathbb{G}$: $x+i = \pi_1 \dots \pi_m$. Тогда $x-i = \overline{x+i} = \bar\pi_1 \dots \bar\pi_m$; элементы $\bar\pi_s$, комплексно сопряженные к простым элементам π_s, тоже являются простыми, и потому

$$x^2+1 = (x+i)(x-i) = \pi_1 \dots \pi_m \bar\pi_1 \dots \bar\pi_m$$

– разложение числа x^2+1 в произведение простых элементов кольца $\mathbb{G}$. Поскольку $\mathbb{G}$ – факториальное кольцо, по утверждению (3) предложения 1 делитель p числа x^2+1, не делящий 1, делится на один из простых сомножителей π_s или $\bar\pi_s$; по утверждению (6) леммы отсюда следует, что $p = \pi_s \bar\pi_s$.

Остается заметить, что π_s и $\bar\pi_s$ не ассоциированы; действительно, они не ассоциированы с целыми рациональными числами и потому по следствию предложения 1 их ассоциированность означала бы, что $\pi_s = a(1 \pm i)$ для некоторого целого рационального числа a, а тогда получилось бы, что $p = \pi_s \bar\pi_s = 2a^2$, что противоречит нечетности p.

Теорема 6. *Для того чтобы целое рациональное число $n > 0$ представлялось в виде суммы двух квадратов целых чисел, необходимо и достаточно, чтобы каждое простое число, сравнимое с 3 по модулю 4, входило в его каноническое разложение в произведение простых чисел с четной кратностью.*

Доказательство. Пусть $n = x^2+y^2 = (x+yi)(x-yi)$, где $x, y \in \mathbb{Z}$. Целое гауссовское число $x+yi$ раскладывается в $\mathbb{G}$ в произведение простых элементов

$$x+yi = \varepsilon q_1 \dots q_r \pi_1 \dots \pi_s,$$

где $\varepsilon = \pm 1, \pm i$, $q_1, \dots, q_r$ – простые числа, сравнимые с 3 по модулю 4, а π_j – простой делитель 2 или простого числа $p_j = \pi_j \bar\pi_j$, сравнимого по модулю 4 с 1 ($1 \leq j \leq s$). Тогда

$$n = (x+yi)(x-yi) = \varepsilon q_1 \dots q_r \pi_1 \dots \pi_s \cdot \bar\varepsilon q_1 \dots q_r \bar\pi_1 \dots \bar\pi_s = q_1^2 \dots q_r^2 p_1 \dots p_s.$$

Обратно, если $n = q_1^2 \dots q_r^2 p_1 \dots p_s$, где $p_1, \dots, p_s$ – положительные простые числа, равные 2 или сравнимые с 1 по модулю 4, а $q_1, \dots, q_r$ – простые числа, сравнимые с 3 по модулю 4, то, обозначив через π_j простой делитель в $\mathbb{G}$ числа p_j, а через $x+yi$ – произведение $q_1 \dots q_r \pi_1 \dots \pi_s$, мы получим

$$n = q_1^2 \dots q_r^2 p_1 \dots p_s = q_1 \dots q_r \pi_1 \dots \pi_s \cdot q_1 \dots q_r \bar\pi_1 \dots \bar\pi_s = (x+yi)(x-yi).$$

8°. **Пифагоровы тройки целых чисел.** В этом пункте мы покажем, как, благодаря тому, что кольцо целых чисел Гаусса факториально, можно найти все целочисленные решения уравнения $x^2+y^2 = z^2$. Тройки целых чисел x, y, z, удовлетворяющих этому уравнению, по понятным причинам называются пифагоровыми тройками.

Пусть $x, y, z \in \mathbb{Z}$, причем $z \neq 0$, и пусть $x^2+y^2 = z^2$. Обозначим через δ наибольший общий делитель целых чисел Гаусса $x+yi$, $x-yi$, так что $x+yi = \delta\alpha$, $x-yi = \delta\beta$, где α, β – тоже целые числа Гаусса. Если бы у α и β был общий нетривиальный делитель π, то элемент $\delta\pi$ был бы общим делителем $x+yi$, $x-yi$, а это противоречило бы тому, что δ – их наибольший общий делитель; поэтому α и β взаимно просты, и по предложению 1, (5) из равенства

$$z^2 = (x+yi)(x-yi) = \delta^2 \alpha\beta$$

следует, что существует такое целое число Гаусса $u+vi$ ($u, v \in \mathbb{Z}$), что $\alpha = \varepsilon(u+vi)^2$, где ε – делитель 1.

Обозначим через δ_1 целое число Гаусса $\delta\varepsilon$; тогда $x+yi=\delta_1((u+vi)^2)$. Вместе с ассоциированным с ним элементом δ элемент δ_1 является наибольшим общим делителем $x+yi$, $x-yi$, и очевидно, что $\bar{\delta}_1$ – тоже их наибольший общий делитель. Но все наибольшие общие делители двух ненулевых элементов ассоциированы, поэтому по следствию из предложения 2 существует такое целое число $a\in\mathbb{Z}$, что $\delta_1=a$, или $\delta_1=ai$, или $\delta_1=a(1\pm i)$. Рассмотрим эти каждый из этих случаев.

Если $\delta_1=a$, то $x+yi=a(u+vi)^2=a(u^2-v^2)+ia(2uv)$, откуда следует, что $x=a(u^2-v^2), y=2auv$, и для числа z получается уравнение

$$z^2=x^2+y^2=a^2((u^2-v^2)^2+(2uv)^2)=a^2(u^2+v^2)^2,$$

откуда следует, что $z=\pm a(u^2+v^2)$.

Если $\delta_1=ai$, то $x+yi=ai(u+vi)^2=-a(2uv)+a(u^2-v^2)$, откуда следует, что $x=-2auv, y=a(u^2-v^2)$, и для числа z получается то же уравнение

$$z^2=x^2+y^2=a^2((-2uv)^2+(u^2-v^2)^2)=a^2(u^2+v^2)^2,$$

откуда следует, что $z=\pm a(u^2+v^2)$.

Если $\delta_1=a(1\pm i)$, то $x+yi=a(1\pm i)(u+vi)^2$, откуда следует, что $x^2+y^2=|x+yi|^2=|a|^2|1\pm i|^2(|u+vi|^2)^2=2a^2(u^2+v^2)^2$, и для числа z получается уравнение $z^2=2a^2(u^2+v^2)^2$, которое не имеет целых рациональных решений, так как иначе число 2 было квадратом $z/(a(u^2+v^2))$.

Итак, мы доказали первую часть следующего утверждения (вторая часть тривиальна).

Теорема 7. *Если x,y,z – такие целые рациональные числа, что $x^2+y^2=z^2$, то существуют целые числа a,u,v, такие что $z=\pm a(u^2+v^2)$ и*

$$x=a(u^2-v^2),\ y=2auv \qquad \text{или} \qquad x=-2auv,\ y=a(u^2-v^2).$$

Обратно, при любых $a,u,v\in\mathbb{Z}$ по этим формулам получается решение уравнения $x^2+y^2=z^2$ в целых числах.

§ 3. Теорема Гаусса

1°. **Кольцо многочленов над факториальным кольцом. Теорема Гаусса.** До сих пор все встречавшиеся у нас факториальные кольца были областями главных идеалов (и даже евклидовыми кольцами). Естественно возникает вопрос: а существуют ли вообще факториальные кольца, в которых не все идеалы главные? Ответ на этот вопрос получается из следующей замечательной теоремы Гаусса.

Теорема 1. *Кольцо $\Lambda[x]$ многочленов над факториальным кольцом Λ снова является факториальным кольцом.*

Поскольку кольцо многочленов от n переменных является кольцом многочленов от одной переменной над кольцом многочленов от $n-1$ переменной, из теоремы Гаусса очевидной индукцией мы получаем

Следствие. *Если Λ – факториальное кольцо, то для любого натурального n кольцо многочленов над Λ от n переменных также факториально.*

В частности, факториальными являются кольца $\mathbb{Z}[x_1,\dots,x_n]$, $k[x_1,\dots,x_n]$, где k – поле. В то же время при $n\geq 1$ кольцо $\mathbb{Z}[x_1,\dots,x_n]$, а при $n\geq 2$ кольцо $k[x_1,\dots,x_n]$ не является областью главных идеалов. Например, идеал $(2,x)$ кольца $\mathbb{Z}[x]$ состоит из всех целочисленных многочленов с четным свободным членом; если бы он был главным идеалом, то порождающий этот идеал многочлен $d(x)$ был бы делителем многочлена нулевой степени 2 и многочлена первой степени x. Но среди целочисленных многочленов такими свойствами обладают лишь многочлены нулевой степени ± 1, которые не принадлежат идеалу $(2,x)$, потому что их свободный член ± 1 нечетен.

Приступим теперь к доказательству теоремы Гаусса.

2°. **Делители 1 и простые элементы кольца Λ как элементы кольца $\Lambda[x]$.** В этом пункте мы докажем два утверждения, справедливые для многочленов над любой областью целостности, а не только над факториальным кольцом.

Предложение 1. *Пусть Λ – область целостности; тогда множество $(\Lambda[x])^*$ делителей единицы кольца $\Lambda[x]$ совпадает с множеством Λ^* делителей единицы кольца $\Lambda \subset \Lambda[x]$.*

Доказательство. Ясно, что $\Lambda^* \subseteq (\Lambda[x])^*$. Пусть $f(x) \in (\Lambda[x])^*$ – делитель 1 в $\Lambda[x]$. Тогда существует такой многочлен $g(x) \in \Lambda[x]$, что $1 = f(x)g(x)$. Поскольку Λ – область целостности, степень произведения многочленов равна сумме их степеней; поэтому

$$0 = \deg 1 = \deg f(x)g(x) = \deg f(x) + \deg g(x).$$

Но оба многочлена ненулевые, поэтому их степени не меньше 0, и предыдущее равенство возможно лишь если $\deg f(x), \deg g(x) = 0$, т.е. $f(x) = a \in \Lambda$, $g(x) = b \in \Lambda$. При этом $ab = f(x)g(x) = 1$, так что $f(x) = a \in \Lambda^*$.

Следующее утверждение играет ключевую роль в доказательстве теоремы Гаусса.

Лемма 1 (лемма Гаусса). *Пусть Λ – область целостности; тогда всякий простой элемент кольца Λ остается простым и как элемент кольца $\Lambda[x]$.*

Доказательство. Пусть p – простой элемент кольца Λ, и пусть $f(x) = a_0 + a_1x + \ldots + a_nx^n$, $g(x) = b_0 + b_1x + \ldots + b_mx^m$ – такие многочлены с коэффициентами из Λ, что их произведение $f(x)g(x) = c_0 + c_1x + \ldots + c_{m+n}x^{m+n}$ делится в $\Lambda[x]$ на p. Это значит, что все коэффициенты c_i многочлена $f(x)g(x)$ делятся на p. Положим $a_i = 0$, $b_j = 0$ при $i > m$ и $j > m$. Если многочлены $f(x)$ и $g(x)$ не делятся на p в $\Lambda[x]$, то найдутся такие $s, t \geq 0$, что $a_0, \ldots, a_{s-1}$, $b_0, \ldots, b_{t-1}$ делятся на p, но a_s и b_t не делятся на p; поскольку p – простой элемент кольца Λ, из последнего условия следует, что a_sb_t не делится на p. Тогда коэффициент c_{s+t} многочлена $f(x)g(x)$ не делится на p, так как

$$c_{s+t} = a_0b_{s+t} + a_1b_{s+t-1} + \ldots + a_{s-1}b_{t+1} + a_sb_t + a_{s+1}b_{t-1} + \cdots + a_{s+t-1}b_1 + a_{s+t}b_0,$$

и в последней сумме все слагаемые, кроме a_sb_t, делятся на p, а a_sb_t на p не делится. Но мы предположили, что все коэффициенты c_i многочлена $f(x)g(x)$, в том числе, и коэффициент c_{s+t}, делятся на p. Полученное противоречие показывает, что хотя бы один из многочленов $f(x)$, $g(x)$ делится на p в $\Lambda[x]$.

3°. **Простые и неприводимые элементы кольца многочленов над факториальным кольцом.** Пусть Λ – область целостности; многочлен $f(x) \in \Lambda[x]$ называется примитивным многочленом, если единственными общими делителями всех его коэффициентов являются делители единицы кольца Λ.

Перед тем, как формулировать утверждения, доказываемые в этом пункте, напомним, что всякую область целостности Λ можно погрузить в ее поле отношений, причем всякий элемент этого поля является отношением двух элементов из Λ.

Лемма 2. *Пусть Λ – факториальная область целостности, K – ее поле отношений. Для всякого ненулевого многочлена $g(x) \in K[x]$ существует ассоциированный с ним в $K[x]$ примитивный многочлен $g_1(x) \in \Lambda[x]$.*

Доказательство. Пусть $g(x) = \dfrac{a_0}{b_0} + \dfrac{a_1}{b_1}x + \ldots + \dfrac{a_n}{b_n}x^n$, где $a_i, b_i \in \Lambda$, причем $b_i \neq 0$ для всех i, $0 \leq i \leq n$, а среди элементов a_i есть хоть один ненулевой. Положим

$b = b_0 b_1 \dots b_n$, $A_i = \dfrac{ba_i}{b_i}$ $(0 \le i \le n)$. Ясно, что все элементы A_i принадлежат Λ; поскольку Λ – область целостности, $b \neq 0$ и среди элементов A_i есть хоть один ненулевой. Кольцо Λ факториально; поэтому существует наибольший общий делитель $d \neq 0$ элементов $A_0, A_1, \dots, A_n$. Тогда элементы $c_i = A_i/d$ принадлежат Λ и у них нет общего делителя, кроме делителей 1, потому что если бы такой делитель $p \notin \Lambda^*$ нашелся, то все A_i делились бы на dp, и потому их наибольший общий делитель d делился бы на dp, что не верно, так как $d/(dp) = 1/p \notin \Lambda$. Итак, многочлен $g_1(x) = c_0 + c_1 x + \dots + c_n x^n = (b/d)g(x)$ – примитивный многочлен с коэффициентами из Λ, ассоциированный с $g(x)$.

Следующее утверждение вытекает из леммы Гаусса.

Лемма 3. *Пусть Λ – факториальная область целостности, K – ее поле отношений, и пусть $f(x), g(x) \in \Lambda[x]$, причем многочлен $g(x)$ примитивен. Если $f(x)$ делится на $g(x)$ в $K[x]$, то $f(x)$ делится на $g(x)$ уже в $\Lambda[x]$.*

Доказательство. Поскольку $f(x)$ делится на $g(x)$ в $K[x]$, существует многочлен $h_1(x) \in K[x]$, такой что $f(x) = g(x)h_1(x)$. По лемме 2 существует примитивный многочлен $h(x) = (b/d)h_1(x) \in \Lambda[x]$, ассоциированный с $h_1(x)$ в кольце $K[x]$ (здесь $b, d \in \Lambda$, $d \neq 0$). Сокращая дробь b/d на наибольший общий делитель числителя и знаменателя, добьемся того, что у b и d нет общих делителей, кроме делителей 1. У нас получилось равенство: $df(x) = bg(x)h(x)$. Если $p \in \Lambda$ – простой делитель d, то $bg(x)h(x)$ делится на p; по лемме Гаусса p является простым элементом не только кольца Λ, но и кольца $\Lambda[x]$, поэтому на p должен делиться один из множителей b, $g(x)$, $h(x)$. Но многочлены $g(x)$, $h(x)$ не могут делиться на p, так как они примитивны, и потому у коэффициентов каждого из этих многочленов не может быть общего простого делителя p. Следовательно, на p делится b, а это противоречит тому, что у b и d нет общих делителей, кроме делителей 1. Итак, у элемента $d \in \Lambda$ нет простых делителей, и поэтому элемент d обратим в Λ. Таким образом, $f(x) = (d^{-1}bh(x))g(x)$ делится на $g(x)$ в $\Lambda[x]$.

Предложение 2. *Пусть Λ – факториальная область целостности, K – ее поле отношений, и пусть $q(x) \neq 0$ – многочлен с коэффициентами из Λ. Следующие условия равносильны:*

(1) *$q(x)$ – простой элемент кольца $\Lambda[x]$;*
(2) *$q(x)$ – неприводимый элемент кольца $\Lambda[x]$;*
(3) *$q(x)$ – примитивный неприводимый в $K[x]$ многочлен, или $q(x)$ – простой элемент кольца Λ (в последнем случае $\deg q(x) = 0$).*

Доказательство. $1 \Rightarrow 2$ выполняется в любой области целостности (см. предложение 1.1).

(2) $\Rightarrow$ (3). Пусть $q(x)$ – неприводимый элемент кольца $\Lambda[x]$, и пусть сначала $\deg q(x) \ge 1$; если многочлен $q(x)$ не примитивен, то существует общий делитель $a \in \Lambda$ его коэффициентов, не принадлежащий Λ^*. Тогда a – делитель $q(x)$, причем $a \notin (\Lambda[x])^* = \Lambda^*$ и a не ассоцирован с $q(x)$, потому что $0 = \deg a \neq \deg q(x)$. Это противоречит тому, что $q(x)$ – неприводимый элемент кольца $\Lambda[x]$. Если многочлен $q(x)$ приводим в $K[x]$, то существует многочлен $f(x) \in K[x]$, такой что $1 \le \deg f(x) < \deg q(x)$ и $q(x)$ делится в $K[x]$ на $f(x)$. По лемме 2 существует примитивный многочлен $f_1(x) \in \Lambda[x]$, ассоциированный с $f(x)$ в кольце $K[x]$. Тогда $q(x)$ делится в $K[x]$ на $f_1(x) \sim f(x)$. Поскольку многочлен $f_1(x)$ примитивен, по лемме 3 $q(x)$ делится на $f_1(x)$ уже в $\Lambda[x]$; при этом $1 \le \deg f_1(x) = \deg f(x) < \deg q(x)$, так что многочлен $f_1(x)$ не ассоциирован с $q(x)$ и не является делителем 1 в $\Lambda[x]$. Это опять противоречит неприводимости $q(x)$.

Пусть теперь $\deg q(x) = 0$; тогда $a = q(x) \in \Lambda$, и если бы элемент a факториального кольца Λ не был простым, он бы не был неприводимым, и существовало бы разложение $a = bc$, в котором оба сомножителя не являются делителями 1. Но тогда по предложению 1 они не являются делителями 1 и в $\Lambda[x]$, а это значит, что $q(x) = a = bc$ – не неприводимый элемент кольца $\Lambda[x]$.

(3) $\Rightarrow$ (1). Мы уже видели, что простой элемент кольца Λ остается простым и в $\Lambda[x]$. Пусть теперь $q(x) \in \Lambda[x]$ – примитивный многочлен, неприводимый над K; покажем, что он простой, т.е. что произведение многочленов $f(x), g(x) \in \Lambda[x]$ делится на $q(x)$ лишь тогда, когда хоть один из сомножителей делится на $q(x)$. Но это сразу следует из леммы 3: поскольку $q(x)$ – неприводимый над полем K многочлен, один из многочленов $f(x), g(x)$ делится на $q(x)$ в $K[x]$, а так как $q(x)$ – примитивный многочлен, он по лемме 3 делится на $q(x)$ уже в $\Lambda[x]$.

4°. **Обрыв цепей делителей в $\Lambda[x]$.** Покажем, что цепи делителей обрываются в кольце многочленов не только над факториальным кольцом, но и в чуть более общей ситуации.

Предложение 3. *Если в области целостности Λ выполнено условие обрыва цепей делителей, то оно выполнено и в кольце многочленов $\Lambda[x]$.*

Доказательство. Пусть для каждого натурального числа i задан многочлен $f_i(x) \in \Lambda[x]$, причем для любого i многочлен $f_i(x)$ делится на многочлен $f_{i+1}(x)$. Если все многочлены $f_i(x)$ нулевые, то они ассоциированы. Пусть $f_r(x) \neq 0$; тогда все последующие многочлены $f_i(x)$ $(i \geq r)$ тоже отличны от 0. Для каждого $i \geq r$ обозначим через $a_i x^{n_i}$ старший член многочлена $f_i(x)$; это значит, что $\deg f_i(x) = n_i$, и что старшая степень переменной x входит в многочлен с коэффициентом $a_i \in \Lambda$. Как мы знаем, старший член произведения многочленов равен произведению старших членов сомножителей; поэтому из того, что при $i \geq r$ многочлен $f_i(x)$ делится на многочлен $f_{i+1}(x)$, следует, что при $i \geq r$ одночлен $a_i x^{n_i}$ делится на $a_{i+1} x^{n_{i+1}}$. Последнее условие равносильно тому, что $n_i \geq n_{i+1}$ и a_i делится на a_{i+1}.

Таким образом, у нас есть невозрастающая цепочка натуральных чисел $n_r \geq n_{r+1} \geq \ldots$ и цепочка делителей $a_r \div a_{r+1} \div \ldots$. Обе эти цепочки стабилизируются: первая – потому, что не бывает бесконечно убывающих последовательностей неотрицательных целых чисел, а вторая – потому, что в Λ выполнено условие обрыва цепей делителей. Следовательно, существует такое $m \geq r$, что при $i \geq m$ элементы a_i и a_m ассоциированы, а $n_i = n_m$. Заметим теперь, что поскольку многочлен $f_m(x)$ делится при $i \geq m$ на многочлен $f_i(x)$, то существует многочлен $h(x) \in \Lambda[x]$, такой что $f_m(x) = h(x) f_i(x)$. Пусть bx^s – старший член многочлена $h(x)$. Тогда $a_m x^{n_m} = a_i x^{n_i} \cdot bx^s$, откуда следует, что $s = n_m - n_i = 0$, а b – делитель 1, так как $a_m \sim a_i$. Следовательно, $h(x) = b \in \Lambda^* = (\Lambda[x])^*$, и потому при $i \geq m$ многочлены $f_m(x) = h(x) f_i(x)$ и $f_i(x)$ ассоциированы в $\Lambda[x]$.

5°. **Завершение доказательства теоремы Гаусса.** Согласно теореме 1 из §2, для доказательства теоремы Гаусса достаточно показать, что в кольце многочленов над факториальным кольцом выполняется условие обрыва цепей делителей, и что всякий неприводимый элемент этого кольца многочленов является и простым элементом этого кольца. Но оба этих утверждения уже получены нами в предложениях 3 и 2.