Лекция 3
Делимость и многочлены

▷Деление в кольце $k[x]$ ▷Евклидовы кольца ▷Ассоциированные, простые и неприводимые элементы кольца ▷НОД и китайская теорема об остатках в кольце главных идеалов ▷Многочлены как функции ▷Корни ▷Производный многочлен ▷Сепарабельность ▷Алгебраические расширения полей ▷Лемма Гаусса и критерий Эйзенштейна ▷Разложение на множители многочленов с целыми коэффициентами ▷Факториальные кольца

§1. Кольца главных идеалов.

Целостное (т. е. без делителей нуля) коммутативное кольцо с единицей, в котором все идеалы являются главными, называется *областью главных идеалов*. С точки зрения делимости все такие кольца устроены подобно кольцу $\mathbb{Z}$, и на них можно распространить все результаты, доказанные про $\mathbb{Z}$ в прошлой лекции. Мы начнём с примеров колец главных идеалов, не совпадающих с $\mathbb{Z}$.

1.1. Деление с остатком в $k[x]$. Я буду считать, что читатель умеет делить многочлены с остатком (например, "уголком"). Точное утверждение, которое в дальнейшем понадобится, можно сформулировать так:

Задача 3.1. Пусть k – произвольное поле. Для любых двух многочленов $f(x), g(x) \in k[x]$ существуют многочлены $q(x) \in k[x]$ (*неполное частное*) и $r(x) \in k[x]$ (*остаток*), такие, что:

$$\begin{aligned} &(1)\quad f(x) = q(x)\cdot g(x) + r(x) \\ &(2)\quad 0 \le \deg r \le \deg(g) - 1\ , \quad (\text{где } \deg \text{ — это степень.}) \end{aligned}$$

Этими условиями $q(x)$ и $r(x)$ определяются по f и g однозначно.

Подсказка: существование обеспечивается процедурой "деления уголком". Единственность доказывается от противного: если $q_1(x)$ и $r_1(x)$ тоже удовлетворяют условиям (1) и (2), то $r_1(x) - r(x) = g(x)\cdot(q_1(x) - q(x))$. Степень левой части $\le \deg(g) - 1$, что возможно лишь при $q_1(x) - q(x) \equiv 0$. Но тогда и $r_1 \equiv r$.

1.1.1. Предложение. *$k[x]$ — область главных идеалов.*

Доказательство. Рассуждение дословно повторяет доказательство аналогичной теоремы про кольцо $\mathbb{Z}$. Пусть $\mathfrak{I} \subset k[x]$ — нетривиальный идеал. Выберем в $\mathfrak{I}$ произвольный многочлен $d(x) \ne 0$, степень которого имеет наименьшее возможное значение среди степеней ненулувых многочленов из $\mathfrak{I}$. Тогда $\mathfrak{I} = (d)$.

Действительно, $(d) \subset \mathfrak{I}$ по построению. Чтобы доказать, что $\mathfrak{I} \subset (d)$, поделим произвольный многочлен $f \in \mathfrak{I}$ на d с остатком:

$$f = q \cdot d + r, \quad \text{где} \quad \deg r \le \deg d - 1.$$

Так как $r = f - q \cdot d \in \mathfrak{I}$, то $r \equiv 0$, ибо d имел наименьшую степень среди ненулевых многочлеов из $\mathfrak{I}$. Поэтому $f = q \cdot d \in (d)$ и $(d) = \mathfrak{I}$.
□

1.2. Евклидовы кольца. В приведённом выше доказательстве, также как и в прошлой лекции, ключевым местом является возможность деления с остатком. Можно аксиоматизировать класс колец, для которых такая возможность имеется.

1.3. Определение. *Целостное коммутативное кольцо A называется евклидовым, если существует функция λ (называемая высотой) из множества ненулевых элементов A в множество целых неотрицательных чисел, обладающая свойством $\lambda(ab) \ge \max(\lambda(a), \lambda(b))$ и такая, что $\forall\, a, b \in A,\ b \ne 0$ найдутся q и r из A такие, что $a = bq + r$ и либо $r = 0$, либо $\lambda(r) < \lambda(b)$.*

> Задача 3.2. Докажите, что всякое евклидово кольцо является областью главных идеалов.

1.3.1. Примеры. Кольцо $\mathbb{Z}$ евклидово относительно высоты, равной абсолютной величине целого числа. Кольцо $k[x]$ евклидово с высотой равной степени многочлена.

Кольцо Гауссовых чисел $\mathbb{Z}[i]$ евклидово относительно высоты $\lambda(z) \stackrel{\text{def}}{=} |z|^2$. Действительно, возможность для данных $a, b \in \mathbb{Z}[i]$ подобрать такие $q, r \in \mathbb{Z}[i]$, что $a = bq + r$ и $|r|^2 < |b|^2$, равносильна тому, что в круге радиуса < 1 с центром в комплексной точке $\dfrac{a}{b} \in \mathbb{C}$ найдётся целая точка $q \in \mathbb{Z}[i]$. Но это очевидно.

> Задача 3.3. Докажите, что кольцо $\mathbb{Z}[\vartheta]$, где ϑ – комплексный корень уравнения $\vartheta^2 + \vartheta + 1 = 0$, евклидово относительно той же высоты $\lambda(z) = |z|^2$.

Отметим, однако, что существуют кольца главных идеалов, не являющиеся евклидовыми.

1.4. Ассоциированные элементы. Пусть A — произвольное целостное кольцо. Элементы a и b из A называются *ассоциированными*, если порождённые ими главные идеалы совпадают: $(a) = (b)$. Это равносильно тому, что $a = bs$ для некоторого *обратимого* элемента $s \in A$.

Действительно, из равенств $a = bs$ и $b = as^{-1}$ следуют включения $(a) \subset (b)$ и $(b) \subset (a)$, т.е. равенство $(a) = (b)$. Наоборот, если $a \in (b)$, скажем: $a = rb$, и $b \in (a)$, скажем: $b = sa$, то $a = rb = rsa$, откуда $0 = a - rsa = a(1 - rs)$, что в виду целостности A влечёт $rs = 1$, т.е. обратимость r и s.

1.4.1. Пример: приведённые многочлены. Поскольку обратимые элементы в $k[x]$ — это константы и только они, предыдущее рассуждение показывает, что два многочлена f и g порождают один и тот же главный идеал в $k[x]$ тогда и только тогда, когда они пропорциональны, т.е. $f(x) = c \cdot g(x)$, где $c = \text{const}$.

Будем называть многочлен *приведённым*, если его старший коэффициент равен единице. Из предыдущего вытекает, что для каждого идеала $\mathfrak{I} \subset k[x]$, существует и единственен такой приведённый многочлен f, что $(f) = \mathfrak{I}$.

1.5. НОД. Пусть A — кольцо главных идеалов, и $\{a_1, a_2, \ldots, a_n\} \subset A$ — произвольный набор элементов. Элемент $d \in A$, порождающий идеал

$$(a_1, a_2, \ldots, a_n) = \{\, x_1 a_1 + x_2 a_2 + \cdots + x_n a_n \mid x_\nu \in A \text{ – любые} \,\} \subset A\ ,$$

называется *наибольшим общим делителем* элементов $a_1, a_2, \dots, a_n$ и обозначается

$$НОД\,(a_1, a_2, \dots, a_n)\ .$$

Он определяется элементами a_ν однозначно с точностью до умножения на обратимые элементы кольца, по построению, делит каждый из a_ν, представим в виде $d = x_1a_1 + x_2a_2 + \dots + x_na_n$, и тем самым, делится нацело на любой другой общий делитель всех a_ν.

Если $НОД\,(a_1, a_2, \dots, a_n)$ обратим, то элементы a_ν называются *взаимно-простыми в совокупности* . Это равносильно наличию таких $x_1, x_2, \dots, x_n \in A$, что

$$x_1a_1 + x_2a_2 + \dots + x_na_n = 1$$

1.5.1. Пример: НОД в $k[x]$. В случае $A = k[x]$ (где k – поле) неоднозначность в определении $НОД$ можно устранить, назвав наибольшим общим делителем многочленов $f_1, f_2, \dots, f_n$ *приведенный* многочлен $d(x)$, порождающий идеал $(f_1, f_2, \dots, f_n) \subset k[x]$.

Для практического нахождения $НОД\,(f, g)$ для пары $f, g \in k[x]$ имеется эффективная ппроцедура, называемая *алгоритмом Евклида.* Она заключается в построении последовательности многочленов $E_0(x),\ E_1(x),\ E_2(x),\ \dots$, определяемых рекуррентно по правилу:

$$\begin{aligned} E_0(x) &= f(x) \quad \text{(мы предполагаем, что } \deg f \geq \deg g) \\ E_1(x) &= g(x) \\ E_k(x) &= \text{остатку от деления } E_{k-1}(x) \text{ на } E_{k-2}(x). \end{aligned}$$

Нетрудно видеть, что степень многочленов E_ν строго убывает до тех пор, пока очередной $E_{k+1}(x)$ не окажется нулевым, т.е. пока $E_{k-1}(x)$ не разделится на $E_k(x)$ нацело.

Задача 3.4. Докажите, что последний ненулевой многочлен $E_k(x)$ в последовательности $E_\nu(x)$ пропорционален $НОД\,(f, g)$.

Указание. Воспользуйтесь убывающей индукцией по ν, чтобы проверить, что E_0 и E_1 делятся на последний ненулувой E_k, и соответственно, возрастающей индукцией по ν — для проверки того, что этот последний E_k делится на любой общий делитель E_0 и E_1.

Задача 3.5. Найдите многочлены $g_1(x)$ и $g_2(x)$, для которых $f_1(x)g_1(x) + f_2(x)g_2(x) \equiv 1$, если

$$\begin{aligned} f_1(x) &= x^5 - 8x^4 + 15x^3 - x^2 + 8x - 15 \\ f_2(x) &= 21x^5 + 10x^4 - 41x^3 - 41x^2 - 12x - 1. \end{aligned}$$

Задача 3.6. Распространите алгоритм Евклида на произвольное евклидоао кольцо.

1.6. Китайская теорема об остатках. Для того, чтобы распространить китайскую теорему об остатках на произвольные кольца главных идеалов, нам понадобится

1.6.1. Лемма. *Пусть $q = q_1q_2$ – произведение двух взаимно простых элементов в кольце главных идеалов A. Тогда правило $a \bmod q \longmapsto (a \bmod q_1, a \bmod q_2)$ устанавливает изоморфизм колец*

$$A/(q) \xrightarrow{\sim} \Big(A/(q_1)\Big) \oplus \Big(A/(q_2)\Big)\ .$$

Доказательство. Рассуждение будет почти таким же как в лекции 2. Корректность очевидна. Инъективность вытекает из того, что всякий $a \in A$, делящийся и на q_1 и на q_2, делится

и на $q_1q_2 = q$ (действительно, если $1 = xq_1 + yq_2$ и $a = mq_1 = nq_2$, то $a = (xn + ym)q_1q_2$). Эпиморфность проверяется непосредственно: пара классов $(a \bmod q_1, b \bmod q_2)$ является образом элемента $c = ayq_2 + bxq_1$, где, как и выше, x и y подбираются из условия $1 = xq_1 + yq_2$.
□

1.6.2. Следствие. (Китайская теорема об остатках.) *Пусть $q = q_1 \cdot q_2 \cdot \dots \cdot q_s$ – разложение на попарно неассоциированные простые множители. Тогда имеется изоморфизм колец:*

$$\frac{A}{(q)} = \frac{A}{(q_1)} \oplus \frac{A}{(q_2)} \oplus \cdots \oplus \frac{A}{(q_s)} \,,$$

заданный правилом $a \bmod q \longmapsto (a \bmod q_1, a \bmod q_2, \dots, a \bmod q_s)$.

Доказательство. Индукция по числу s взаимно-простых сомножителей.

Задача 3.7. Проверьте, что если элемент q_1 взаимно прост с каждым из элементов $q_2, q_3, \dots, q_s$, то он взаимно прост и с их произведением $\tilde{q}_2 = q_2 \cdot \dots \cdot q_s$.

Пользуясь задачей, сначала применим предыдущую лемму к паре взаимно простых элементов q_1, $\tilde{q}_2 = q_2 \cdot \dots \cdot q_s$, а затем применим индуктивное предположение к меньшему набору $q_2, q_3, \dots, q_s$. Получим композицию изоморфизмов

$$\frac{A}{(q)} \xrightarrow{\sim} \frac{A}{(q_1)} \oplus \frac{A}{(\tilde{q}_2)} \xrightarrow{\sim} \frac{A}{(q_1)} \oplus \frac{A}{(q_2)} \oplus \cdots \oplus \frac{A}{(q_s)} \,.$$

□

Задача 3.8. В случае $A = k[x]$ переформулируйте эту теорему в терминах “настоящих” остатков от деления, аналогично тому, как это было сделано в конце прошлой лекции для $A = \mathbb{Z}$.

1.7. Простота и неприводимость. Пусть A — произвольное целостное кольцо. Имеются два подхода к тому, какие элементы в A считать аналогами простых чисел. Они приводят к разным результатам, и потому для соответствующих элементов кольца используются различные названия.

Первый подход опирается на данное в n° 3.7 лекции 2 определение простого идеала. Необратимый элемент $a \in A$ называется *простым*, если идеал $(a) \subset A$ — простой, т. е. если фактор-кольцо $A/(a)$ целостное. Это означает, что из условий $bc \in (a)$ и $b \notin (a)$ следует, что $c \in (a)$. Иначе говоря, элемент $a \in A$ прост тогда и только тогда, когда произвольное произведение делится на a лишь при условии, что хотя бы один из сомножителей делится на a (ср. с Пр.3.6.1 из лекции 2).

Второй подход состоит в том, чтобы, не мудрствуя лукаво, переписать обычное школьное определение простого числа: необратимый элемент $a \in A$ называется *неприводимым* , если из разложения $a = bc$ следует, что один из сомножителей *обратим*. Например, неприводимые элементы в кольце многочленов — это в точности такие многочлены, которые нельзя разложить в произведение двух многочленов строго меньшей степени. Твакие многочлены называют *неприводимыми многочленами*.

Задача 3.9. Убедитесь, что в кольце $\mathbb{Z}$ оба понятия: простота и неприводимость совпадают и описывают в точности множество простых чисел.

В произвольном целостном кольце *из простоты следует неприводимость*. Действительно, если $a = bc$ и a прост, то либо b, либо c делится на a, скажем: $b = as$. Но тогда $a = asc$, откуда $sc = 1$ и c — обратим (мы воспользовались равенством $a(1 - sc) = 0$ и целостностью A).

Однако, бывают кольца, в которых имеются неприводимые, но не простые элементы, так что простота — это более сильное условие, чем неприводимость.

Задача 3.10. В кольце $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ найдите неприводимый, но не простой элемент.

Подсказка:$(1 + \sqrt{5})(-1 + \sqrt{5}) = 2 \cdot 2$.

1.7.1. Предложение. *Пусть A – область главных идеалов. Фактор-кольцо $A/(a)$ является полем тогда и только тогда, когда a неприводим.*

Доказательство. Проверим, что если a — неприводим, то всякий класс $[b] \neq [0]$ в $A/(a)$ обратим. Это аналогично Пр.3.6.2 из лекции 2: если $[b] \neq [0]$, то b не делится на a, а значит *НОД* (b, a) обратим (ибо все делители a либо обратимы, либо ассоциированы с a), и значит, $xa + yb = 1$ для некоторых $x, y \in A$, что означает, что $[b]$ обратим в $A/(a)$ и $[b]^{-1} = [y]$.
□

1.7.2. Следствие. *В кольце главных идеалов простота и неприводимость равносильны друг другу.*

§2. Многочлены и их корни

В этом параграфе мы применим предыдущие результаты к исследованию алгебраических свойств многочленов.

2.1. Вычисление значения многочлена в точке. Любой многочлен из $k[x]$ определяет функцию на поле k, а также на любом кольце A, содержащем поле k в качестве подкольца. Если $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ и $\lambda \in A$, то

$$f(\lambda) = \mathrm{ev}_\lambda(f) \stackrel{\mathrm{def}}{=} a_0\lambda^n + a_1\lambda^{n-1} + \cdots + a_{n-1}\lambda + a_n \in A$$

(где правая часть уже не формальный символ, но конкретный элемент кольца A) называется *значением многочлена f в точке $\lambda \in A$*. *Гомоморфизм вычисления*:

$$\mathrm{ev}_\lambda \colon\ k[x] \longrightarrow A$$

индуцирует гомоморфизм

$$\varphi \colon\ k[x] \longrightarrow A^A \colon\ f(x) \mapsto f(\lambda)$$

из кольца многочленов в кольцо A-значных функций на A. Вообще говоря, $\ker \varphi \neq 0$, т.е. разные элементы кольца многочленов могут давать одинаковые функции.

Задача 3.11. Найдите два разных многочлена над полем $\mathbb{Z}/p\mathbb{Z}$, задающиее, тем не менее, одинаковые функции на этом поле.

Гомоморфизм вычисления замечательным образом связан с делимостью. А именно, пусть $f(x) \in k[x] \subset A[x]$ —многочлен с коэффициентами из k, который можно также рассматривать и как многочлен из $A[x]$. Мы собираемся вычислять его значение в точке $a \in A$. Для этого заметим, что процедура “деления уголком” на линейный двучлен $x - a$ благополучно работает над любым коммутативным кольцом A, и позволяет представить любой многочлен $f(x) \in A[x]$ в виде

$$f(x) = (x - a) \cdot q(x) + r\ ,$$

где $q(x) \in A[x]$, а $r \in A$ – некоторая константа (называемая *остатком* по аналогии с евклидовым случаем). Вычисляя значения обеих частей в точке a, получаем:

$$f(a) = q(a) \cdot (a - a) + r = r \ .$$

2.1.1. Лемма. *Остаток от деления многочлена $f(x) \in A[x]$ на линейный двучлен $x - a$ в кольце $A[x]$ равен значению многочлена f в точке $a \in A$.*

□

2.2. Корни. Пусть A — произвольное коммутативное кольцо. Элемент $a \in A$ называется *корнем* многочлена $f(x) \in A[x]$, если $f(a) = 0$, т.е. если $f \in \ker(\mathrm{ev}_a)$. Прямо из предыдущего наблюдения мы получаем

2.2.1. Следствие. *Число $a \in A$ тогда и только тогда, является корнем многочлена $f(x) \in A[x]$, когда $f(x)$ делится нацело в кольце $A[x]$ на многочлен $(x - a)$.*

2.2.2. Следствие. *Пусть в кольце A нет делителей нуля. Если многочлен $f \in A[x]$ имеет несколько попарно-разных корней $a_1, a_2, \ldots, a_n \in A$, то он представим в виде $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) g(x)$, где $g(x) \in A[x]$.*

Доказательство. Индукция по числу корней n. Случай $n = 1$ рассмотрен в предыдущем следствии. Применяя индуктивное предположение к первым $(n - 1)$ корням $a_1, a_2, \ldots, a_{n-1}$, имеем

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_{n-1}) h(x) \ .$$

с $h(x) \in A[x]$. Подставляя $x = a_n$ получим

$$0 = (a_n - a_1)(a_n - a_2) \cdots (a_n - a_{n-1}) h(a_n) \ .,$$

что из-за целостности кольца A возможно лишь при $h(a_n) = 0$, т. е. при $h(x) = (x - a_n) g(x)$ с $g \in A[x]$.

□

2.2.3. Следствие. *Ненулевой многочлен $f \in A[x]$ не может иметь более $\deg f$ корней ни в каком целостном кольце $B \supset A$.*

□

2.2.4. Следствие. *Если многочлены f и g совпадают как функции на некотором целостном кольце, содержащем более, чем $\max(\deg f, \deg g)$ элементов, то $f = g$ и как многочлены (т.е. гомоморфизм $\varphi \colon A[x] \longrightarrow A^A$ в этом случае инъективен).*

□

Доказательство. Многочлен $f - g$, обладая слишком большим количеством корней, должен быть нулевым.

□

2.2.5. Следствие. *Пусть k – поле. Если НОД $(f, g) = 1$, то f и g не могут иметь общих корней ни в каком кольце $A \supset k$.*

Доказательство. Если НОД $(f, g) = 1$, то $f(x) \cdot v(x) + g(x) \cdot w(x) = 1$ для подходящих $v, w \in k[x]$. Вычисляя обе части в точке $a \in A$, получаем $f(a) \cdot v(a) + g(a) \cdot w(a) = 1$, т.е. $f(a)$ и $g(a)$ не могут быть равны нулю одновременно.

□

Значение этого следствия в том, что равенство $НОД\,(f,g)=1$ проверяется с помощью алгоритма Евклида вычислениями в поле k, тогда как вывод делается о любом расширении и о корнях, явного выражения для которых не требуется.

2.3. Кратные корни и производный многочлен. Число $a\in A$ называется *r-кратным корнем* многочлена $f\in A[x]$, если $f(x)=(x-a)^r\cdot g(x)$ в $A[x]$ и $g(a)\neq 0$. Корни с $r=1$ называются *простыми*, а с $r\geq 2$ — *кратными*.

Замечательно, что о наличии кратных корней многочлена $f\in A[x]$ в произвольном кольце $B\supset A$ можно судить не находя самих корней, но проделав некоторые вычисления с коэффициентами многочлена в исходном кольце A. Причина состоит в том, что известная из анализа операция дифференцирования в применении к многочленам является *алгебраической*, т. е. может быть описана в терминах четырёх алгебраических операций без использования предельного перехода.

Задача 3.12. Пусть A – любое кольцо. Убедитесь, что $\forall\, f\in A[x]$ многочлен $f(a)-f(b)\in A[a,b]$ делится нацело в $A[a,b]$ на двучлен $a-b$.

Подсказка: см. тождество (a) из зад.1.9 лекции 1.

Пусть $f(x)\in A[x]$. Обозначим через $D_f(a,b)\in A[a,b]$ частное от деления $f(a)-f(b)$ на $a-b$ в кольце $A[a,b]$. Многочлен

$$f'(x)=D_f(x,x)\in A[x]$$

называется *производным* (или *производной*) от f. Другое обозначение[1]: $\dfrac{d}{dx}f$.

Задача 3.13. Убедитесь, что если $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$, то

$$f'(x)=a_1+2a_2x+3a_3x^2+\cdots+ba_nx^{n-1}=\sum_{\nu=1}^{n}\nu a_\nu x^{\nu-1}\ ,$$

где коэффициент ν перед a_ν есть элемент простого подкольца в A, т. е. он равен $\underbrace{1+1+\cdots+1}_{\nu\text{ раз}}$.

Задача 3.14. Убедитесь, что взятие производной удовлетворяет всем известным из анализа стандартным формальным правилам дифференцирования суммы, разности, произведения, частного и композиции.

Замечание: в дальнейшеем для нас особенно важным будет *правило Лейбница*:

$$(fg)'=f'\cdot g+f\cdot g'\ .$$

Оно следует из тождества $D_{fg}(a,b)=f(a)\cdot D_g(a,b)+\cdot D_f(a,b)g(b)$.

2.3.1. Предложение. *Пусть поле k имеет характеристику нуль. Корень a многочлена $f\in k[x]$ тогда и только тогда является r-кратным корнем, когда он будет корнем $(r-1)$-той производной* $\left(\dfrac{d}{dx}\right)^r f$ *, но не будет корнем r-той производной* $\left(\dfrac{d}{dx}\right)^{r-1} f$.

Доказательство. Достаточно проверить, что максимальная степень $(x-a)$, которая делит $f'(x)$, ровно на единицу меньше максимальной степени $(x-a)$, делящей $f(x)$.

---

[1]символ $\dfrac{d}{dx}$ обычно используют для обозначения отображения из $A[x]$ в $A[x]$, сопоставляющего многочлену его производную

Пусть $f(x) = (x-a)^r g(x)$ и $g(x)$ не делится на $(x-a)$. По правилу Лейбница

$$f'(x) = r(x-a)^{r-1}g(x) + (x-a)^r g'(x) = (x-a)^{r-1}\Big(rg(x) + (x-a)g'(x)\Big)\ . \qquad (3\text{-}1)$$

Многочлен в скобках не делится на $(x-a)$, поскольку $rg(x) \neq 0$ и не делится на $(x-a)$.
□

Заметим, что в общем случае, из формулы (3-1) вытекают

2.3.2. Следствие. *Пусть A – любое коммутативное кольцо с единицей. Если $a \in A$ является r-кратным корнем многочлена $f \in A[x]$, то он является по меньшей мере $(r-1)$-кратным корнем его производной.*

□

2.3.3. Следствие. *Пусть A – любое коммутативное кольцо с единицей. Если $a \in A$ является простым корнем многочлена $f \in A[x]$, то $f'(a) \neq 0$.*

Доказательство. При $r = 1$ формула (3-1) имеет вид $f'(x) = g(x) - (x-a)g'(x)$, откуда $f'(a) = g(a) \neq 0$.
□

2.3.4. Сепарабельность. Пусть теперь k – поле. Многочлен $f \in k[x]$ называется *сепарабельным*, если он не имеет кратных корней ни в каком расширении $K \supset k$, и *несепарабельным* – в противном случае. Прямо из предыдущего следствия вытекает

2.3.5. Предложение. *Для несепарабельности $f \in k[x]$ необходимо и достаточно наличие общего корня у f и f' в некотором расширении поля k.*

2.3.6. Пример. Пусть $\mathrm{char}(k) = p > 0$ и $f(x) = x^p - 1 \in k[x]$. Так как $f'(x) = px^{p-1} = 0$ (ибо $p = \underbrace{1+1+\cdots+1}_{(p\ \text{раз})} = 0$), то f — несепарабелен. Более того, если $K \supset k$ — какое-либо расширение, где у f есть корень $\vartheta: \quad \vartheta^p = 1$, то

$$x^p - 1 = x^p - \vartheta^p = (x-\vartheta)^p\ ,$$

поскольку возведение в p-тую степень является в характеристике p гомоморфизмом. Таким образом, если в расширении K у f вообще есть корень, то он автоматически p-кратный (и единственный!).

2.3.7. Пример. Пусть $\mathrm{char}(k) = 0$. Тогда всякий неприводимый многочлен положительной степени $f(x) \in k[x]$ сепарабелен. В самом деле, $f'(x) \neq 0$ и *НОД* $(f, f') = 1$ из-за неприводимости f и неравенства $\deg f' < \deg f$. Следовательно, у f и f' нет общих корней ни в каком расширении.

2.4. Минимальный многочлен. Пусть $K \supset k$ — расширение полей. Элемент $\vartheta \in K$ называется *алгебраичным над k*, если $f(\vartheta) = 0$ для некоторого $f \in k[x]$. Приведенный многочлен f наименьшей степени, обладающий этим свойством, называется *минимальным многочленом* для ϑ над k, а его степень называется *степенью* ϑ над k.

Поскольку в поле нет делителей нуля, минимальный многочлен неприводим в $k[x]$, ибо подставляя ϑ в разложение $f(x) = g(x)h(x)$, мы должны будем иметь или $g(\vartheta) = 0$, или $h(\vartheta) = 0$, а значит, один из множителей имеет ту же степень что и f из-за минимальности f.

Опишем наименьшее подполе в K, содержащее k и ϑ. Для этого рассмотрим гомоморфизм вычисления значения в точке ϑ:

$$\mathrm{ev}_\vartheta:\ k[x] \longrightarrow K:\ f \mapsto f(\vartheta).$$

Его ядро состоит из всех $g \in k[x]$, для которых ϑ будет корнем. Как и всякий идеал в $k[x]$, $\ker(ev_\vartheta)$ является главным идеалом, а его образующей будет приведённый многочлен наименьшей степени, зануляющийся на ϑ, т. е. в точности минимальный многочленом для ϑ. Мы получаем

2.4.1. Предложение. *Минимальный многочлен элемента ϑ над k делит в $k[x]$ любой другой многочлен $g\in k[x]$, для которого ϑ является корнем.*

□

Далее, по теореме о строении гомоморфизма образ $\mathrm{im}\,(ev_\vartheta) \subset K$ изоморфен фактор-кольцу $k[x]/(f)$. Последнее является полем, поскольку f неприводим. Это, очевидно, и есть наименьшее подполе в K, содержащее k и ϑ.

2.4.2. Предложение. *Множество значений всевозможных многочленов из $k[x]$ на элементе $\vartheta\in K$ составляет поле, являющееся наименьшим подполем в K, содержащим k и ϑ. Это поле изоморфно фактор-кольцу $k[x]/(f)$, где f – минимальный многочлен элемента ϑ.*

□

2.5. Присоединение корня. Предыдущая конструкция позволяет для любого поля k и любого неприводимого многочлена $f(x) \in k[x]$ построить такое расширение $K\supset k$, в котором у f появится корень. Действительно, в качестве K можно взять фактор-кольцо $k[x]/(f)$. Т. к. f неприводим, оно является полем. Поле k вложено в него посредством ограничения канонического гомоморфизма $k[x] \xrightarrow{res_f} k[x]/(f)$ редукции по модулю f на константы $k \subset k[x]$. Корнем многочлена f является элемент $\vartheta = res_f(x)$ — образ одночлена x.

Чтобы представить себе поле $K = k[x]/(f)$ более явно, зафиксируем в каждом классе вычетов по модулю f канонического представителя – остаток от деления элементов этого класса на f. Такой остаток может быть совершенно произвольным многочленом степени $\leq \deg(f) - 1$. Тем самым, если $\deg(f) = n$, то элементы $k[x]/(f)$ взаимно-однозначно записываются в виде

$$t_0 + t_1\vartheta + \cdots + t_{n-1}\vartheta^{n-1} ,$$

где $\vartheta = x(\bmod f)$ и $t_\nu\in k$ – любые, а операции над ними в $k[x]/(f)$ — это обычное сложение и умножение многочленов по модулю соотношения $f(\vartheta) = 0$, т. е. в точности те же операции, которые были описаны нами в лекции 1 при построении поля $k[\vartheta]$ с $f(\vartheta) = 0$.

Задача 3.15. Докажите, что $\mathbb{Q}[\vartheta]$ с $\vartheta^4+\vartheta^3+\vartheta^2+\vartheta+1 = 0$ — поле и найдите $(1+\vartheta^2)^{-1}$.

Задача 3.16. Пусть неприводимый многочлен $f \in k[x]$ имеет корень α в каком-то расширении $K \supset k$. Докажите, что поле $k[x]/(f)$ вкладывается в поле K гомоморфизмом, отображающим класс $x(\bmod f)$ в α.

Существование такого расширения, в котором данный многочлен имеет корень, позволяет обернуть доказанные выше результаты о наличии общих корней у пары многочленов и о кратных корнях.

2.5.1. Следствие. *Если $f, g \in k[x]$, где k – поле, и НОД $(f, g) \neq 1$, то f и g имеют в некотором расширении общий корень.*

Доказательство. Надо перейти к расширению, в котором будет иметь корень НОД (f, g).
□

2.5.2. Следствие. *Для сепарабельности многочлена f необходимо и достаточно, чтобы НОД $(f, f') = 1$.*

2.6. Алгебраические расширения полей. Расширение $K \supset k$ называется *алгебраическим*, если все элементы поля K алгебраичны над k.

2.6.1. Пример: конечные поля. Все элементы любого конечного поля $\mathbb{F}$ алгебраичны над простым подполем. Действительно, если $\vartheta \in \mathbb{F}$, то среди степеней ϑ^0, ϑ^1, ϑ^2, … будут одинаковые, ибо $\mathbb{F}$ конечно. Если $\vartheta^k = \vartheta^m$, то ϑ — корень многочлена $x^{|m-k|} - 1 = 0$, определенного над простым подполем. Таким образом, если $\mathrm{char}\mathbb{F} = p$, то $\mathbb{F}$ получается из $\mathbb{Z}/p\mathbb{Z}$ при помощи конечного числа расширений, описанных в n° 2.5.

Задача 3.17. Докажите, что число элементов в конечном поле характеристики p равно p^n для некоторого $n \in \mathbb{N}$.

2.6.2. Пример: поле разложения многочлена. Для любого многочлена $f(x) \in k[x]$ существует расширение, в котором f полностью разлагается на линейные множители. Чтобы построить такое поле, надо присоединить к основному полю корень нелинейного неприводимого делителя f максимальной степени. В расширенном таким образом поле этот делитель станет приводимым, и тем самым, количество неприводимых делителей f максимальной степени уменьшится (либо уменьшится сама эта максимальная степень). Продолжая по индукции (т. е. присоединяя к уже построенному расширению корень неприводимого нелинейного делителя f уже над этим расширением), мы через конечное число шагов добьёмся того, что все неприводимые делители f станут линейными.

Посмтроенное таким образом расширение называется *полем разложения* многочлена f. Согласно зад.3.16, поле разложения вкладывается в любое другое поле, в котором f полностью разлагается на линейные множители. Поэтому поле разложения с точностью до автоморфизма, тождественного на исходном поле k, не зависит от произвола в своём построении, и может быть охарактеризовано[2] как *наименьшее* поле, в котором f распадается на линейные множители.

Задача 3.18. (необязательная) Пусть $K \supset k$ есть поле разложения неприводимого многочлена $f \in k[x]$. Докажите, что если какой-то неприводимый многочлен $g \in k[x]$ имеет корень в K, то он полностью разлагается в $K[x]$ на линейные множители.

Утешение: Это довольно трудная задача, и мы вернёмся к ней в последней лекции.

§3. Разложение на множители многочленов с целыми коэффициентами

3.1. Кольцо $\mathbb{Z}[x]$ Обратимыми элементами в $\mathbb{Z}[x]$, как и в $\mathbb{Z}$, являются только 1 и -1, так что коэффициенты многочленов, как правило, необратимы. Из-за этого многие факты о многочленах над полем перестают выполняться в $\mathbb{Z}[x]$.

Задача 3.19. Докажите, что идеал $(x, 2)$, порождённый в $\mathbb{Z}[x]$ многочленом x и постоянным многочленом 2, не является главным.

3.2. Лемма Гаусса. *Содержанием* $\mathrm{cont}(f)$ многочлена $f \in \mathbb{Z}[x]$ называется НОД его коэффициентов.

3.2.1. Предложение. (Лемма Гаусса) $\mathrm{cont}(fg) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$.

[2] опять таки, однозначно с точностью до изоморфизма

Доказательство. Из формулы, выражающей коэффициенты fg через коэффициенты f и g, следует, что всякий общий делитель коэффициентов f и всякий общий делитель коэффициентов g одновременно выносятся из коэффициентов fg. Поэтому $\operatorname{cont}(fg)$ делится на $\operatorname{cont}(f)\cdot\operatorname{cont}(g)$. Сокращая на это произведение, мы без ущерба для общности можем предполагать, что $\operatorname{cont}(f)=1$ и $\operatorname{cont}(g)=1$, и должны будем показать, что в этом случае и $\operatorname{cont}(fg)=1$.

Пусть это не так и $\operatorname{cont}(fg)=k\neq 1$, и p — какое-либо простое число, делящее k. Тогда p делит все коэффициенты fg, но не делит хотя бы один из коэффициентов f и хотя бы один из коэффициентов g. Рассмотрим гомоморфизм редукции по модулю p:

$$\pi_p\colon\ \mathbb{Z}\longrightarrow\mathbb{Z}/p\mathbb{Z}.$$

Он индуцирует гомоморфизм

$$\pi_p\colon\ \mathbb{Z}[x]\longrightarrow\mathbb{Z}/p\mathbb{Z}[x],$$

соответствующих колец многочленов, приводящий все коэффициенты многочлена $f(x)\in\mathbb{Z}[x]$ по модулю p:

$$\pi_p(a_0x^k+a_1x^{k-1}+\cdots+a_{k-1}x+a_k)=[a_0]_p+[a_1]_px+\cdots+[a_k]_px^k$$

(проверьте, что это гомоморфизм!). Но $\mathbb{Z}/p\mathbb{Z}[x]$, как и всякое кольцо многочленов над полем, не имеет делителей нуля, тогда как при наших предположениях $\pi_p(f)\neq 0$, $\pi_p(g)\neq 0$, но $\pi_p(f)\cdot\pi_p(g)=\pi_p(fg)=0$.

Это противоречие показывает, что $\operatorname{cont}(fg)=1$, что и требовалось.

□

3.2.2. Предложение. *Всякий многочлен $f(x)\in\mathbb{Q}[x]$ однозначно записывается в виде $f(x)=\dfrac{m}{n}\tilde f(x)$, где $\tilde f(x)\in\mathbb{Z}[x]$ – многочлен содержания 1, а $m/n\in\mathbb{Q}$ – несократимая дробь с положительным знаменателем.*

Доказательство. Существование разложения очевидно: надо привести все коэффициенты f к общему знаменателю, вынести его за скобку, затем вынести из оставшегося целочисленного многочлена *НОД* его коэффициентов и сократить возникашую в качестве множителя перед скобкой дробь.

Для доказательства единственности допустим, что $f(x)=\dfrac{m}{n}\tilde f(x)=\dfrac{r}{s}\widehat f(x)$ – два разложения с требуемыми свойствами. Умножая на ns и беря содержание обеих частей, получаем равенство $ms=nr$. Поскольку s взаимно прост с r, n будет делиться на s. Аналогично, r делится на m. Поэтому $n=s$ и $r=m$. Но тогда и $\tilde f=\widehat f$.

□

3.2.3. Следствие. *Если многочлен $f(x)\in\mathbb{Z}[x]$ раскладывается в $\mathbb{Q}[x]$ в произведение двух многочленов с рациональными коэффициентами, то он раскладывается и в $\mathbb{Z}[x]$ в произвеедение многочленов тех же степеней, но уже с целыми коэффициентами.*

Доказательство. Пусть в $\mathbb{Q}[x]$ имеется разложение $f(x)=g(x)h(x)$. В соответствии с предыдущим предложением, распишем

$$f(x)=m\tilde f(x)\quad,\qquad g(x)=\frac{p}{q}\tilde g(x)\quad,\qquad h(x)=\frac{r}{s}\tilde h(x)\,,$$

где $\operatorname{cont}(\tilde f)=\operatorname{cont}(\tilde g)=\operatorname{cont}(\tilde h)=\text{\textit{НОД}}\,(p,q)=\text{\textit{НОД}}\,(p,q)=1$. Умножая обе части равенства $f(x)=g(x)h(x)$ на qs и беря содержание, мы в следствие леммы Гаусса получим равенство

$mqs = pr$, из которого, как и ранее, вытекает, что p делится на s, а r делится на q. Таким образом равенство

$$f(x) = \frac{r}{q}\tilde{g}(x)\frac{p}{s}\tilde{h}(x)$$

доставляет искомое разложение f в $\mathbb{Z}[x]$.

□

Непосредственно из доказательства получаем

3.2.4. Следствие. *Если $f(x) \in \mathbb{Z}[x]$, а $g(x) \in \mathbb{Z}[x]$ – многочлен содержания 1, делящий $f(x)$ в $\mathbb{Q}[x]$, то $g(x)$ делит $f(x)$ и в $\mathbb{Z}[x]$.*

3.2.5. Следствие. *Множество неприводимых элементов кольца $\mathbb{Z}[x]$ состоит из простых целых констант и неприводимых над полем $\mathbb{Q}$ целочисленных многочленов содержания 1.*

3.2.6. Следствие. *Неприводимые элементы $\mathbb{Z}[x]$ просты.*

Доказательство. Надо проверить, что если gh делится на неприводимый многочлен f, то либо g либо h делится на f.

Если $f \equiv p = \text{const}$ — простое число, то либо $\text{cont}(g)$, либо $\text{cont}(h)$ делится на p (т.к. $\text{cont}(g)\text{cont}(h) = \text{cont}(gh)$ делится на p).

Если f неприводим над $\mathbb{Q}$ и $\text{cont}(f) = 1$, то либо g, либо h делится на f в $\mathbb{Q}[x]$, а значит и в $\mathbb{Z}[x]$ (по предыдущему следствию).

□

3.3. Разложение многочленов из $\mathbb{Z}[x]$ на множители над полем $\mathbb{Q}$. Все рациональные корни многочлена с целыми коэффициентами могут быть найдены при помощи конечного числа проб благодаря следующему факту:

3.3.1. Предложение. *Если несократимая дробь $a = p/q \in \mathbb{Q}$ является корнем многочлена $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \mathbb{Z}[x]$, то p делит a_0, а q делит a_n.*

Доказательство. Подставляя $x = p/q$ и приводя к общему знаменателю, получаем

$$a_0q^n + pq(\cdots) + a_np^n = 0.$$

Так как p и q взаимно просты, то p делит a_0 , а q делит a_n, что и требовалось доказать.

□

> Задача 3.20. Убедитесь, что $x^4 + 4$ раскладывается в $\mathbb{Z}[x]$ в произведением двух квадратных трёхчленов.

Эта задача показывает, что отсутствие рациональных корней вовсе не означает неприводимость многочлена с целыми коэффициентами. Вообще анализ неприводимости над полем $\mathbb{Q}$, хотя и является вполне алгоритмизуемой задачей, решаемой за конечное число шагов[3], часто оказывается очень тонким (или весьма трудоёмким) вопросом. Мы ограничимся здесь описанием двух прёмов, часто оказывающихся полезными

3.3.2. Предложение. (Критерий Эйзенштейна) *Пусть*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$$

приведённый многочлен с целыми коэффициентами. Если для некоторого простого $p \in \mathbb{Z}$ все коэффициенты a_ν делятся на p, но свободный член a_0 не делится при этом на p^2, то $f(x)$ неприводим над $\mathbb{Q}$.

[3]см. например *Б. Л. ван дер Варден. Алгебра* (М. “Наука” (1976) гл. V §32 (с. 122)).

Доказательство. Согласно лемме Гаусса достаточно доказать, что $f(x)$ не разлагается в $\mathbb{Z}[x]$ в произведение двух множителей меньшей степени. Допустим, что такое разложение $f(x) = g(x)h(x)$ существует. Как и в доказательстве теоремы Пр.3.2.1, применим к этому равенству гомоморфизм π_p приведения по модулю p. Получим равенство

$$\pi_p(f) = \pi_p(g)\pi_p(h) \qquad \text{в } \mathbb{Z}/p\mathbb{Z}[x].$$

По условию $\pi_p(f) = x^n$, т.е. состоит лишь из старшего члена. Из этого следует, что старшие коэффициенты многочленов g и h остаются ненулевыми при редукции по модулю p, а оба свободных члена зануляются (иначе произведение свободного члена на младший из ненулевых членов другого многочлена дало бы ненулевой младший член в $\pi_p(f)$ степени меньшей, чем n). Таким образом, свободные члены и у h и у g делятся на p. Но тогда свободный член у f делится на p^2, что запрещается условием.
□

3.3.3. Пример. Пусть p — простое число. Многочлен

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

называется *многочленом деления круга*, ибо его комплексные корни — это в точности все отличные от 1 корни уравнения деления единичного круга на p равных частей (см. лекцию 1). При помощи критерия Эйзенштейна докажем, что $f(x)$ неприводим в $\mathbb{Q}[x]$. Для этого заметим, что неприводимость $f(x)$ в $\mathbb{Q}[x]$ равносильна неприводимости многочлена $g(t) = f(t+1)$ в $\mathbb{Q}[t]$ (т.к. замена $x = t + 1$ обратима: $t = x - 1$). Но

$$g(t) = \frac{(t+1)^p - 1}{t} = t^{p-1} + \binom{p}{1}t^{p-2} + \binom{p}{2}t^{p-3} + \cdots + \binom{p}{p-2}t + \binom{p}{p-1}$$

удовлетворяет критерию Эйзенштейна: все его коэффициенты $\binom{p}{k}$ делятся на p, а свободный член (равный p), делясь на p, не делится на p^2. Стало быть, $g(t)$, а с ним и $f(x)$, неприводимы.

3.3.4. Приведение по простому модулю, которым мы уже много раз успешно пользовались в этой лекции, часто оказывается весьма эффективным средством при анализе разложимости целочисленного многочлена. Дело в том, что над полем $\mathbb{Z}/p\mathbb{Z}$ имеется лишь конечное число неприводимых многочленов данной степени, и при небольшой степени и малых p они могут быть легко перечислены.

Например, чтобы выяснить, разлагается ли $f(t) = t^5 + t^2 + 1$ на множители в $\mathbb{Z}[t]$, достаточно рассмотреть его над $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Если бы f был приводим над $\mathbb{Z}$, то над $\mathbb{F}_2$ он обязан был бы делится на неприводимый приведённый многочлен степени ≤ 2. Но таковых в $\mathbb{F}_2[t]$ всего три:

$$t \quad , \qquad t+1 \quad , \qquad t^2 + t + 1 \; ,$$

и деля столбиком (над $\mathbb{F}_2$) непосредственно убеждаемся, что f имеет остаток 1 от деления на каждый из этих трёх многочленов.

Помимо информации негативного характера, редукция по модулю p позволяет делать и позитивные выводы — например, определить, какими могут быть степени неприводимых делителей, и каковы классы вычетов их коэффициентов по модулю p.

3.4. Разложение над $\mathbb{R}$ и $\mathbb{C}$ В любом курсе комплексного анализа доказывается.

3.4.1. Предложение. *Всякий многочлен из $\mathbb{C}[x]$ имеет корень в $\mathbb{C}$.*

□

Несмотря на то, что эту теорему часто называют *основной теоремой алгебры*, причина, по которой она справедлива, кроется не в *алгебраических* свойствах поля $\mathbb{C}$, а в его *аналитических* свойствах[4]. Мы не будем здесь доказывать эту теорему, но отметим её алгебраические следствия.

3.4.2. Следствие. *Неприводимыми в $\mathbb{C}[x]$ являются только константы и многочлены степени 1.*

3.4.3. Следствие. *Неприводимыми в $\mathbb{R}[x]$ являются константы, многочлены степени 1 и квадратичные многочлены с отрицательным дискриминантом.*

Доказательство. Если $z = a+ib$ — комплексный корень многочлена $f(x) = f_0x^n + f_1x^{n-1} + \cdots + f_{n-1}x + f_n \in \mathbb{R}[x]$, то применяя к равенству $f(z) = 0$ гомоморфизм комплексного сопряжения (при котором вещественные числа неподвижны), получим

$$0 = \bar{0} = \overline{f(z)} = \overline{f_0z^n + f_1z^{n-1} + \cdots + f_{n-1}z + f_n} = f_0\bar{z}^n + f_1\bar{z}^{n-1} + \cdots + f_{n-1}\bar{z} + f_n = f(\bar{z}).$$

Поэтому $\bar{z} = a - ib$ также будет корнем для f. Но тогда f делится на

$$(x-z)(x-\bar{z}) = x^2 - (z+\bar{z})x + z\bar{z} = x^2 - 2\mathrm{Re}(z)x + |z|^2 = x^2 - 2ax + (a^2+b^2).$$

Следовательно, любой многочлен степени ≥ 3 приводим в $\mathbb{R}[x]$ и разлагается в произведение линейных и квадратичных. Квадратичные же многочлены приводимы тогда и только тогда, когда у них есть вещественные корни.

3.4.4. Следствие. *Комплексные невещественные корни многочленов из $\mathbb{R}[x]$ разбиваются на пары комплексно-сопряженных.*

§4. Факториальность

4.1. Разложение на неприводимые множители и нётеровость. Пусть A — целостное кольцо. С точки зрения делимости неприводимые элементы A являются теми “атомами”, из которых составляются при помощи перемножения все прочие элементы A. Действительно, если $a \in A$ не является неприводимым, то $a = b_1b_2$. Если b_1 и b_2 приводимы, скажем, $b_1 = c_1c_2$, $b_2 = c_3c_4$, то $a = c_1c_2c_3c_4$ и т.д. Как правило, этот процесс не может продолжаться бесконечно. Например, в кольце $\mathbb{Z}$ с каждым шагом строго уменьшается модуль самого большого по модулю приводимого сомножителя, в кольце $k[x_1, \ldots, x_n]$ — его степень, а в $\mathbb{Z}[x_1, \ldots, x_n]$ — и то и то параллельно. Мы получаем

4.1.1. Предложение. *В кольцах $\mathbb{Z}$, $\mathbb{Z}[x_1, \ldots, x_n]$, $k[x_1, \ldots, x_n]$ (где k — поле) любой элемент является произведением конечного числа неприводимых.*

□

Если описанный выше процесс разложения на множители не заканчивается за конечное число шагов, то он позволяет построить *бесконечную* последовательность приводимых элементов c_ν, в которой $c_{\nu+1}$ является собственным делителем c_ν при каждом ν. На языке идеалов, это означает, что главные идеалы $\mathfrak{I}_\nu = (c_\nu)$ образуют бесконечную цепочку *строго*

[4]Видимо, самый прямой способ получить основную теорему алгебры — это применить *теорему Лиувилля* к аналитической (т.е. представимой в виде суммы *абсолютно сходящеегося ряда*) фунции $1/f(x)$, где $f \in \mathbb{C}[z]$ — многочлен, про который предполагается, что у него нет корней. Теорема Лиувилля утверждает, что ограниченная аналитическая функция, определенная на всем $\mathbb{C}$ — константа.

вложенных друг в друга идеалов:

$$\mathfrak{I}_1 \subset \mathfrak{I}_2 \subset \mathfrak{I}_3 \subset \cdots .$$

4.2. Определение. *Кольцо A называется* нётеровым, *если в нём не существует бесконечных возрастающих последовательностей* строго *вложенных идеалов.*

Без употребления отрицаний нётеровость можно охарактеризовать тем, что для любой последовательности идеалов $\mathfrak{I}_\nu$, в которой $\mathfrak{I}_\nu \subset \mathfrak{I}_{\nu+1}$, можно указать номер $N \in \mathbb{N}$, начиная с которого последовательность стабилизируется, т. е. $\mathfrak{I}_\nu = \mathfrak{I}\nu + 1 \ \forall \ \nu \geq N$.

Прямо из определений получаем

4.2.1. Предложение. *В целостном нётеровом кольце любой элемент является произведением конечного числа неприводимых.*

□

Один класс нётеровых колец нам хорошо известен.

4.2.2. Лемма. *Кольцо главных идеалов* нётерово.

Доказательство. Объединение $\mathfrak{I}_\infty \stackrel{\text{def}}{=} \bigcup\limits_\nu \mathfrak{I}_\nu$ всех идеалов любой цепочки вложенных идеалов является, очевидно, идеалом (проверьте!). Обозначим через d образующую этого идеала. Эта образующая лежит в одном из идеалов $\mathfrak{I}\nu$, скажем, пусть $d \in \mathfrak{I}_N$. Тогда $\mathfrak{I}_\infty = \mathfrak{I}_N$, что и означает нётеровость.

□

4.3. Однозначность разложения. Кольцо A называется *факториальным*, если оно целостное и каждый элемент $a \in A$ разлагается в произведение конечного числа неприводимых

$$a = p_1 p_2 p_3 \ldots p_m \ ,$$

причем это разложение *единственно* с точностью до перестановки сомножителей и умножения их на обратимые элементы кольца. Иначе говоря, если $a = q_1 q_2 \ldots q_k$ — другое разложение, то $m = k$ и, возможно, после подходящей перенумерации q_ν будет ассоциирован p_ν при всех ν.

В отличие от существования разложения, единственность разложения является весьма тонким фактом. Именно поэтому основную теорему арифметики иногда называют *теоремой об однозначности разложения на простые множители*, подчеркивая именно однозначность.

4.3.1. Лемма. *Если в целостном кольце A каждый элемент является произведением конечного числа неприводимых, то A факториально тогда и только тогда, когда каждый неприводимый элемент в A прост.*

Доказательство. Пусть A факториально, q — неприводим. Надо проверить, что если ab делится на q, то или a, или b делится на q.

Пусть $ab = qr$. Разложим в этом равенстве a, b и r на неприводимые:

$$\underbrace{(p_1 \cdots p_m)}_{a} \cdot \underbrace{(p_{m+1} \cdots p_n)}_{b} = q \cdot \underbrace{(q_1 \cdots q_k)}_{r} .$$

Из единственности один из множителей в левой части ассоциирован с q. Пусть $p_1 = sq$. Тогда $a = q(sp_1 \cdots p_m)$ делится на q. Тем самым в факториальном кольце неприводимые элементы просты.

Пусть теперь дано, что в A все неприводимые элементы просты и имеется два разложения на неприводимые множители

$$p_1p_2\cdots p_k = q_1q_2\cdots q_m.$$

Так как p_1 прост, то произведение в правой части должно содержать множитель, делящийся на p. Пусть это q_1, т.е. $q_1 = sp_1$.

Задача 3.21. Убедитесь, что s — обратим.

Перенося правую часть влево и вынося общий множитель, получим, что

$$p_1(p_2\cdots p_k - sq_2\cdots q_m) = 0.$$

Так как A — целостное кольцо, получаем равенство двух разложений на неприводимые множители

$$p_2p_3\cdots p_k = (sq_2)q_3\cdots q_m,$$

состоящих из строго меньшего, чем ранее количества множителей. Продолжая так дальше, получим, что $m = n$, а соответственные сомножетели — ассоцированны. Лемма доказана. □

4.3.2. Следствие. *Кольца $\mathbb{Z}$, $k[x]$ и $\mathbb{Z}[x]$ факториальны.*

4.3.3. Следствие. *Любая область главных идеалов факториальна.*

4.3.4. Факториальность кольца многочленов. При помощи леммы Гаусса и рассуждений, аналогичных проделанным в §3, но с использованием более общих понятий, нетрудно доказать, что *кольцо многочленов $A[x]$ над любым факториальным кольцом A факториально.* В частности, факториальны кольца $\mathbb{Z}[x_1,\ldots,x_n]$ и $k[x_1,\ldots,x_n]$. Мы вернёмся к этому в лекции 8, но уже сейчас вы можете использовать эти факты при решении задач на упражнениях. Подробнее о факториальных кольцах см. в книге: Ленг С. Алгебра (стр.148-151 по изданию М.”Мир”.1968).