

5. ПЯТАЯ ЛЕКЦИЯ, 4 ОКТЯБРЯ 2021 Г.

5.1. Максимальные и простые идеалы.

Определение 5.1. Идеал $\mathfrak{m} \subset A$ называется *максимальным*, если он не содержится ни в каком большем идеале (не совпадающем со всем кольцом).

Определение 5.2. Идеал $\mathfrak{p} \subset A$ называется *простым*, если для любых двух элементов $a, b \in A$, таких, что $ab \in \mathfrak{p}$, верно, что либо $a \in \mathfrak{p}$, либо $b \in \mathfrak{p}$.

Пример 5.3. Простые идеалы в $\mathbb{Z}$ — это идеалы вида (p) , где p простое. Они же являются и максимальными (проверьте это!).

Предложение 5.4. 1) Идеал $\mathfrak{p}$ прост тогда и только тогда, когда $A/\mathfrak{p}$ — область целостности.

2) Идеал $\mathfrak{m}$ максимален тогда и только тогда, когда $A/\mathfrak{m}$ — поле.

Доказательство. 1) Пусть $\mathfrak{p}$ прост, $ab \in \mathfrak{p}$. Значит, a или b лежат в $\mathfrak{p}$. Рассмотрим их образы при отображении факторизации $A \rightarrow A/\mathfrak{p}$. Получим, что из $[ab] = [0]$ следует, что $[a] = [0]$ или $[b] = [0]$, что и означает, что $A/\mathfrak{p}$ целостное. Обратное утверждение доказывается точно так же.

2) Пусть $\mathfrak{m}$ максимален. Докажем, что всякий ненулевой элемент $[a] \in A/\mathfrak{m}$ обратим. Действительно, $a \notin \mathfrak{m}$. Рассмотрим идеал $a + \mathfrak{m} = \{ax + m \mid x \in A, m \in \mathfrak{m}\}$. Этот идеал содержит $\mathfrak{m}$ и не совпадает с ним (поскольку содержит ещё и a), значит, он совпадает со всем кольцом. Поэтому $1 = ax + m$ для некоторых $x \in A, m \in \mathfrak{m}$. Получаем, что в $A/\mathfrak{m}$ элемент $[x]$ есть $[a]^{-1}$, так как $[1] = [a][x] + [m] = [a][x]$. Обратное утверждение доказывается аналогично (проделайте это!). $\square$

Следствие 5.5. Всякий максимальный идеал прост.

Упражнение 5.6. Приведите пример простого, но не максимального идеала.

Оказывается, что в кольцах главных идеалов верно и обратное к следствию 5.5. Это вытекает из следующей теоремы.

Теорема 5.7. Пусть A — кольцо главных идеалов, $u \in A$ — необратимый элемент. Тогда $A/(u)$ является полем тогда и только тогда, когда u прост.

Доказательство. Пусть u не прост: $u = vw$, где v и w необратимы. Тогда в $A/(u)$ получаем: $[v][w] = [u] = [0]$, причём $[v] \neq [0]$ и $[w] \neq [0]$ — значит, $A/(u)$ не область целостности, и тем более не поле.

Обратно, пусть u прост. Это значит, что для любого $x \notin (u)$ верно, что $(x, u) = 1$, следовательно, найдутся a и b , для которых $ax + bu = 1$. Значит, в $A/(u)$ получаем, что $[a][x] = [1]$, т.е. $[a]$ обратим. $\square$

5.2. Многочлены и их корни. Пусть A — произвольное кольцо. Можно рассмотреть кольцо многочленов с коэффициентами из A :

$$A[x] = \{a_n x^n + \dots + a_1 x + a_0 \mid a_0, \dots, a_n \in A\}.$$

Если A целостное, то $A[x]$ тоже будет целостным кольцом (почему?).

Рассмотрим произвольное кольцо $B \supseteq A$, содержащее A . Пусть $b \in B$. Тогда определен гомоморфизм вычисления (по-английски *evaluation map*), действующий на многочлен $f(x) = a_n x^n + \dots + a_1 x + a_0$ следующим образом:

$$\text{ev}_b: A[x] \rightarrow B, \quad f(x) \mapsto f(b) = a_n b^n + \dots + a_1 b + a_0.$$

Если $\text{ev}_b(f) = 0$, то есть $f(b) = 0$, будем говорить, что b является *корнем* многочлена $f(x)$.

Предложение 5.8 (теорема Безу). Если $a \in B$ — корень многочлена $f(x)$, то $f(x)$ делится нацело на $x - a$ в кольце $A[x]$; иными словами, существует такой $g(x) \in A[x]$, для которого

$$f(x) = (x - a)g(x).$$

Доказательство. Поделим $f(x)$ на $g(x)$ с остатком в кольце $A[x]$ (подумайте, почему это всегда можно сделать?). Получим представление

$$f(x) = (x - a)g(x) + r,$$

где $r \in B$. Подставив $x = a$, получим, что $r = 0$. □

Следствие 5.9. Если A — целостное кольцо, а $a_1, \dots, a_k$ — различные его элементы, то многочлен $f(x)$, обращающийся в нуль во всех этих точках, делится на $(x - a_1) \dots (x - a_k)$.

Доказательство. Воспользуемся индукцией по k . База — это просто предыдущее предложение. Переход: пусть утверждение доказано для $k - 1$ элемента. Тогда

$$f(x) = (x - a_1) \dots (x - a_{k-1})h(x).$$

Подставим в это равенство $x = a_k$. Получим

$$0 = f(a_k) = (a_k - a_1) \dots (a_k - a_{k-1})h(a_k).$$

Все скобки в правой части отличны от 0, так что $h(a_k) = 0$. Значит, $h(x) = (x - a_k)g(x)$, откуда получается требуемое. □

Следствие 5.10. Если A целостное, ненулевой многочлен $f(x) \in A[x]$ степени d имеет не более d корней в любом расширении $B \supseteq A$.

Упражнение 5.11. Приведите пример кольца, не являющегося целостным, и многочлена $f(x)$ над ним, имеющего более $\deg f$ корней.

Следствие 5.12. Если многочлены $f(x)$ и $g(x)$ совпадают более чем в d точках, где $d = \max(\deg f, \deg g)$, то $f(x) \equiv g(x)$.

В частности, многочлен, равный нулю во всех точках бесконечного кольца, обязан равняться нулю. Однако для конечных колец (в частности, конечных полей) это неверно.

Пример 5.13. Многочлен $x^p - x \in \mathbb{F}_p[x]$ имеет корнем любой элемент поля $\mathbb{F}_p$ — это утверждает малая теорема Ферма. Следовательно, $x^p - x = x(x - 1) \dots (x - (p - 1))$.

Упражнение 5.14. Выведите из последнего равенства еще одно доказательство теоремы Вильсона.

5.3. Разложение на неприводимые множители многочленов с целыми коэффициентами. В этом разделе мы докажем факториальность кольца $\mathbb{Z}[x]$; иначе говоря, покажем, что всякий многочлен с целыми коэффициентами однозначно раскладывается на неприводимые множители с целыми коэффициентами.

Пусть $f(x) = a_n x^n + \dots + a_1 x + a_0$, где $a_i \in \mathbb{Z}$. Назовем *содержанием* $\text{cont } f$ многочлена $f(x)$ наибольший общий делитель его коэффициентов. Если они взаимно просты в совокупности, т.е. $\text{cont } f = 1$, будем называть f *примитивным*.

Теорема 5.15 (лемма Гаусса). Содержание произведения многочленов равно произведению содержаний:

$$\text{cont } fg = \text{cont } f \cdot \text{cont } g.$$

Доказательство. Ясно, что $\text{cont } fg : \text{cont } f$ и $\text{cont } fg : \text{cont } g$. Поэтому нужно лишь доказать, что произведение двух примитивных многочленов снова будет примитивно. Пусть f и g примитивны. Предположим, что $\text{cont } fg$ делится на какое-то простое число p .

Рассмотрим многочлены $\bar{f}, \bar{g} \in \mathbb{F}_p[x]$, коэффициенты которых — это остатки соответствующих коэффициентов по модулю p (такая операция называется *приведением по простому модулю*). Ясно, что $\overline{fg} = \bar{f} \cdot \bar{g}$. При этом все коэффициенты fg делятся на p , следовательно, $\overline{fg} = 0$. Но многочлены f и g примитивны, следовательно, у каждого из них найдется коэффициент, не кратный p . Поэтому $\bar{f} \neq 0$ и $\bar{g} \neq 0$. Это противоречит тому, что кольцо $\mathbb{F}_p[x]$ является целостным. Значит, fg примитивен. $\square$

Предложение 5.16. *Всякий многочлен с рациональными коэффициентами $f(x) \in \mathbb{Q}[x]$ однозначно записывается в виде*

$$f(x) = \frac{m}{n} \tilde{f}(x),$$

где $\tilde{f}(x) \in \mathbb{Z}[x]$ примитивен, а дробь m/n несократима.

Доказательство. Существование такого представления очевидно. Докажем единственность. Предположим, что

$$\frac{m}{n} \tilde{f}(x) = \frac{r}{s} \hat{f}(x).$$

Стало быть, $ms\tilde{f}(x) = rn\hat{f}(x)$. Возьмем содержание обеих частей, получим, что $ms = rn$. Поэтому $ms : r$. Но s и r взаимно просты, значит, $m : r$. Аналогично можно доказать, что $r : m$. Значит, $m = r$, и поэтому $n = s$. $\square$

Следствие 5.17. *Если многочлен $f(x) \in \mathbb{Z}[x]$ раскладывается на неприводимые сомножители как многочлен с рациональными коэффициентами, то он раскладывается на неприводимые сомножители той же степени с целыми коэффициентами.*

Доказательство. Предположим, что в $\mathbb{Q}[x]$

$$f(x) = g(x)h(x), \quad f(x) = m\tilde{f}(x),$$

где $m = \text{cont } f$, т.е. $\tilde{f}(x)$ примитивен.

Представим $g(x)$ и $h(x)$ в виде, указанном в предложении 5.16:

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

Взяв содержание $f(x)$ и воспользовавшись леммой Гаусса, получаем, что $mqs = pr$. Значит, $p : s$ и $r : q$. Поэтому у сомножителей в скобках в разложении

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

коэффициенты уже будут целыми, что и требовалось. $\square$

Следствие 5.18. *Если многочлен с целыми коэффициентами $f(x)$ делится на примитивный многочлен $g(x)$ в $\mathbb{Q}[x]$, то он делится на $g(x)$ и в $\mathbb{Z}[x]$ (т.е. частное этих многочленов имеет целые коэффициенты).*

Подведем итог. Мы доказали следующее утверждение.

Теорема 5.19. *Кольцо многочленов $\mathbb{Z}[x]$ факториально. Неприводимыми элементами в нем являются, во-первых, примитивные многочлены, неприводимые как элементы $\mathbb{Q}[x]$, и, во-вторых, неприводимые элементы $\mathbb{Z}$ (т.е. простые числа).*

Теорема 5.20. Второе утверждение вытекает из следствия 5.18: если многочлен из $\mathbb{Z}[x]$ неприводим как многочлен из $\mathbb{Q}[x]$, это значит, что в $\mathbb{Z}[x]$ он может делиться только на многочлен той же степени (т.е. пропорциональный ему) или нулевой степени (т.е. константу). Каждый такой многочлен пропорционален примитивному; последний и будет являться неприводимым. Тем самым каждый элемент из $\mathbb{Z}[x]$ можно представить в виде произведения неприводимых, причем единственным образом. Теорема доказана.

Приведем полезный критерий для поиска рациональных корней многочленов с целыми коэффициентами.

Предложение 5.21. Пусть несократимая дробь p/q — корень многочлена $a_n x^n + \dots + a_1 x + a_0$, где $a_i \in \mathbb{Z}$. Тогда $a_n : q$ и $a_0 : p$.

Доказательство. Подставим p/q в многочлен и домножим его на q^n . Получим следующее равенство (в целых числах):

$$a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0.$$

Все слагаемые в нем, кроме последнего, делятся на p , поэтому и $a_0 q^n : p$. Но p и q взаимно просты, то есть $a_0 : p$. Аналогично $a_n : q$. $\square$

В частности, если $a_n = 1$, мы получаем следующий результат: рациональный корень приведенного многочлена (т.е. многочлена со старшим коэффициентом 1), если он есть, обязательно будет целым числом.

В отличие от многочленов над $\mathbb{R}$ и тем более $\mathbb{C}$, неприводимые многочлены над $\mathbb{Q}$ (или, что почти то же самое, над $\mathbb{Z}$) устроены сложно, и доказательство неприводимости того или иного многочлена может быть непростой задачей. Приведем одно достаточное условие, которое иногда позволяет убедиться в неприводимости многочлена с целыми коэффициентами.

Теорема 5.22 (признак Эйзенштейна). Пусть $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ — приведенный многочлен с целыми коэффициентами, и для некоторого простого p верно, что все коэффициенты $f(x)$, кроме старшего, делятся на p , а свободный член a_0 не делится на p^2 . Тогда $f(x)$ неприводим над $\mathbb{Q}$.

Доказательство. Предположим противное: что $f(x) = g(x)h(x)$ приводим. Аналогично доказательству леммы Гаусса рассмотрим редукцию по модулю p :

$$\bar{f}(x) = x^n = \bar{g}(x) \cdot \bar{h}(x).$$

Значит, $\bar{g}(x) = x^m$ и $\bar{h}(x) = x^{n-m}$ для некоторого m , где $0 < m < n$. Поэтому свободные члены $g(x)$ и $h(x)$ делятся на p . Но отсюда следует, что a_0 делится на p^2 — противоречие. $\square$