Независимый Московский Университет

Алгебра – II

Второй курс, осенний семестр 1999/2000 г.
Лекция 1

В ближайшее время мы будем заниматься *коммутативной алгеброй*. Слово «кольцо» будет обозначать коммутативное ассоциативное кольцо с единицей, «подкольцо» — подкольцо, содержащее единицу, «гомоморфизм колец» — гомоморфизм колец, переводящий единицу в единицу.

1. Факториальные кольца. Напомню, что *факториальным кольцом* называется область целостности, в которой любой ненулевой необратимый элемент можно однозначно разложить на простые (неприводимые) множители. Однозначность понимается с точностью до перестановки сомножителей и умножения их на обратимые элементы кольца.

Определение 1. Пусть R — кольцо. Идеал $\mathfrak{p} \subseteq R$ называется *простым*, если для любых $a, b \in R \setminus \mathfrak{p}$ их произведение ab не лежит в идеале $\mathfrak{p}$. Другими словами, идеал $\mathfrak{p}$ называется простым, если $R/\mathfrak{p}$ — область целостности.

Упражнение 1. Докажите, что любой максимальный идеал прост.

Теорема 1. *Пусть R — область целостности, в которой у каждого необратимого элемента существует хотя бы одно разложение на простые множители. Тогда кольцо R факториально в том и только в том случае, если для любого простого элемента $p \in R$ соответствующий главный идеал (p) прост.*

Доказательство. Вспомним, как доказывается факториальность любого кольца главных идеалов. Однозначность разложения на простые множители в кольце главных идеалов выводится из единственного нетривиального утверждения: если ab делится на p и p — простой элемент, то либо a делится на p, либо b делится на p. Это и есть утверждение о том, что идеал (p) прост. Остаток доказательства факториальности очевидным образом переносится на случай любого кольца, в котором существует разложение на простые множители.

То, что в факториальном кольце идеал, порождённый простым элементом, прост, проверьте сами. $\square$

Определение 2. Пусть R — факториальное кольцо. *Содержанием* $d(f)$ многочлена $f(x) \in R[x]$ называется наибольший общий делитель всех коэффициентов этого многочлена. Если $d(f)$ — обратимый элемент R, то многочлен f называется *примитивным*.

Теорема 2 (Лемма Гаусса). *Пусть R — факториальное кольцо и $f, g \in R[x]$. Тогда $d(fg) = d(f) \cdot d(g) \cdot \varepsilon$, где ε — некоторый обратимый элемент кольца R. В частности, произведение примитивных многочленов — снова примитивный многочлен.*

Доказательство. Пусть оба многочлена $f(x) = \sum a_k x^k$ и $g(x) = \sum b_m x^m$ примитивны, а p — простой элемент кольца R. Найдем наименьшие индексы i и j, для которых a_i и b_j не делятся на p. Тогда, как легко убедиться, коэффициент при x^{i+j} у многочлена fg не делится на p. Так как это выполнено для любого простого p, мы заключаем, что многочлен fg примитивен.

Для доказательства леммы Гаусса в общем случае (когда многочлены f и g не обязательно примитивны) достаточно вынести $d(f)$ и $d(g)$ за скобки и свести, тем самым, задачу к разобранному выше частному случаю. □

Следствие 2.1. *Пусть R — факториальное кольцо, $\mathbb{F}$ — его поле частных. Многочлен из $R[x]$ не раскладывается в произведение многочленов из $R[x]$ меньшей степени тогда и только тогда, когда он неприводим в $\mathbb{F}[x]$.*

Следствие 2.2. *Пусть R — факториальное кольцо, $\mathbb{F}$ — его поле частных, $f, g \in R[x]$, $d(g) = 1$. Многочлен f делится на многочлен g в кольце $R[x]$ тогда и только тогда, когда f делится на g в $\mathbb{F}[x]$.*

Теорема 3 (Признак Эйзенштейна). *Пусть $f(x) = \sum a_k x^k \in R[x]$ — многочлен степени $n > 0$, причем для некоторого простого $p \in R$ коэффициент a_n не делится на p, коэффициенты $a_0, \ldots, a_{n-1}$ делятся на p, но коэффициент a_0 не делится на p^2. Тогда многочлен $f(x)$ неприводим над $\mathbb{F}$.*

Доказательство. Предположим, что многочлен $f(x)$ приводим над $\mathbb{F}$ и, следовательно, над R. Тогда имеет место равенство

$$f(x) = \left(\sum_{i=0}^{k} b_i x^i\right) \cdot \left(\sum_{j=0}^{m} c_j x^j\right)$$

для некоторых $b_0, \ldots, b_k, c_0, \ldots, c_m \in R$, причем $k + m = n$ и $k, m > 0$. Найдем наименьшие индексы i и j, для которых b_i и c_j не делятся на p (такие существуют, поскольку a_n не делится на p). Из тех же соображений, что и в доказательстве леммы Гаусса, получаем, что $i = k$ и $j = m$. Но тогда коэффициент $a_0 = b_0 c_0$ должен делиться на p^2, в противоречии с условием. □

Пример 1. Рассмотрим многочлен

$$f(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1} \in \mathbb{Z}[x]$$

(p — простое число). Докажем, что этот многочлен неприводим. Для этого достаточно доказать, что неприводим многочлен

$$f(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1}.$$

Но к этому многочлену применим критерий Эйзенштейна, ибо его старший коэффицент равен 1, а все остальные, очевидно, делятся на p, причем свободный член равен p.

Теорема 4. *Кольцо многочленов $R[x]$ над факториальным кольцом R факториально.*

Доказательство. Из следствия 2.1 легко вывести, что простые элементы кольца $R[x]$ бывают двух типов: простые элементы кольца R, рассматриваемые как многочлены нулевой степени, и многочлены с содержанием 1, неприводимые в $\mathbb{F}[x]$.

Если p — простой элемент кольца R, то $R[x]/pR[x] \simeq (R/pR)[x]$ — область целостности, поэтому главный идеал $pR[x] \subset R[x]$ прост.

Пусть произведение двух многочленов $f, g \in R[x]$ делится на многочлен h с содержанием 1, неприводимый над $\mathbb{F}$. Поскольку кольцо $\mathbb{F}[x]$ факториально, то один из многочленов f и g делится на h в $\mathbb{F}[x]$. Согласно следствию 2.2 один из многочленов f и g делится на h и в $R[x]$. Таким образом, идеал $(h) \subset R[x]$ прост.

Очевидно, что разложение на простые множители в $R[x]$ существует. Мы убедились, что любой простой элемент кольца $R[x]$ порождает простой идеал. По теореме 1 отсюда следует, что кольцо $R[x]$ факториально. □

Следствие 4.1. *Кольцо $\Bbbk[x_1, \ldots, x_n]$ многочленов от n переменных над полем $\Bbbk$ является факториальным.*

2. Нётеровы кольца.

Теорема 5. *Следующие два условия на кольцо R равносильны:*

- **(А):** *Любой идеал $I \subseteq R$ порождён конечным множеством элементов.*
- **(Б):** *Любая возрастающая цепочка идеалов $I_1 \subseteq I_2 \subseteq \ldots$ стабилизируется, то есть найдётся такое $n \in \mathbb{N}$, что $I_{k+1} = I_k$ для любого $k \geqslant n$. Другими словами, не существует бесконечной строго возрастающей цепочки идеалов.*

Доказательство. Пусть всякий идеал в кольце R конечнопорождён. Рассмотрим бесконечную возрастающую цепочку идеалов $I_1 \subseteq I_2 \subseteq \ldots$. Положим $I = \bigcup_{k=1}^{\infty} I_k$. Ясно, что I является идеалом. Пусть он порождён элементами $a_1, \ldots, a_s$. Каждый из этих элементов содержится в каком-то из идеалов I_k. Поскольку эти идеалы образуют возрастающую цепочку, то найдётся такое $n \in \mathbb{N}$, что $a_1, \ldots, a_s \in I_n$. Но тогда $I_n \supseteq I$, следовательно $I_n = I$ и $I_{k+1} = I = I_k$ для любого $k \geqslant n$.

Пусть, наоборот, в кольце R есть идеал I, не являющийся конечнопорождённым. Выберем в нем элемент a_1. Так как I не порождается конечным множеством элементов, то в I существует элемент a_2, не лежащий в (a_1). Продолжая это построение по индукции, находим для каждого натурального числа k элемент a_k, не лежащий в идеале $(a_1, \ldots, a_{k-1})$. Положим $I_k = (a_1, \ldots, a_k)$. Ясно, что идеалы I_k образуют бесконечную строго возрастающую цепочку идеалов. □

Определение 3. Кольцо, удовлетворяющее равносильным условиям из теоремы 5, называется *нётеровым*.

Упражнение 2. Доказать, что если R — нётерова область целостности, то любой необратимый элемент кольца R можно разложить в произведение простых элементов. Таким образом, нётерова область целостности является факториальным кольцом тогда и только тогда, когда каждый её простой элемент порождает простой идеал.

Теорема 6. *Любой подмодуль N конечнопорождённого модуля M над нётеровым кольцом R конечнопорождён.*

Доказательство. Следующие две леммы, справедливые для модулей над любым кольцом, докажите сами.

Лемма 6.1. *Любой фактормодуль конечнопорождённого модуля конечнопорождён.*

Лемма 6.2. *Если подмодуль конечнопорождён и фактор по нему конечнопорождён, то и весь модуль конечнопорождён.*

Для доказательства теоремы воспользуемся индукцией по числу образующих модуля M. Если M — циклический модуль (то есть порождённый одним элементом), то он изоморфен фактормодулю вида R/I, где R рассматривается как модуль над собой, а $I \subseteq R$ — подмодуль (то есть идеал). Тогда N имеет вид J/I, где J — идеал, содержащий I. Поскольку кольцо R нётерово, то J конечнопорождён. По лемме 6.1 и фактормодуль J/I конечнопорождён.

Пусть M порождён n элементами $a_1, \ldots, a_n$. Обозначим через $\tilde{M}$ подмодуль модуля M, порождённый элементами $a_1, \ldots, a_{m-1}$. Положим $\tilde{N} = N \cap \tilde{M}$. По предположению индукции модуль $\tilde{N}$ конечнопорождён. Фактормодуль $N/\tilde{N}$ естественно вкладывается в циклический модуль $M/\tilde{M}$. Мы уже доказали, что всякий подмодуль циклического модуля конечнопорождён. По лемме 6.2 отсюда следует, что и модуль N конечнопорождён. □

Теорема 7. *Кольцо многочленов $R[x]$ над нётеровым кольцом R тоже нётерово.*

Доказательство. Пусть $I \subseteq R[x]$ — идеал. Положим $I_k = I \cap R[x]_k$, где через $R[x]_k$ обозначенно множество многочленов степени не большей k. Обозначим через J_k множество старших коэффициентов многочленов из I_k. Ясно, что J_k образуют возрастающую цепочку идеалов кольца R. Так как R — нётерово кольцо, эта цепочка стабилизируется, то есть найдётся такое натуральное число n, что $J_k = J_n$ при $k > n$. Отсюда следует, что $I = R[x]I_n$. С другой стороны, I_n — конечнопорождённый модуль (как подмодуль конечнопорождённого R-модуля $R[x]_n$). Множество образующих I_n как R-модуля порождает I как идеал в $R[x]$. □

Следствие 7.1 (Теорема Гильберта о базисе). *Кольцо $\Bbbk[x_1, \ldots, x_n]$ многочленов от n переменных над полем $\Bbbk$ является нётеровым.*