Алгебра 3 Кузнецов

1 Листок 1. Нётеровы кольца

1. R нёторово. Покажем, что $R[[x]]$ тоже нётерово. Пусть J — идеал в $R[[x]]$. Пусть $\mathfrak{a}(n) = \{a_n \in R \colon \exists p = a_n x^n + a_{n+1}x^{n+1} + \ldots \in J\}$. Ясно, что $\mathfrak{a}(0) \subseteq \mathfrak{a}(1) \subseteq \mathfrak{a}(2) \subseteq \ldots$ — идеалы в R. Поэтому из нётеровости R следует, что при некотором $d \in \mathbb{N}$ имеет место

   $$\mathfrak{a}(n) = \mathfrak{a}(d) \;\; \forall n \geq d.$$

   Найдём образующие каждого идеала $\mathfrak{a}(n)$ при $n \leq d$ и выберем соответствующие степенные ряды в $R[[x]]$ для каждой образующей (для $a \in \mathfrak{a}(n)$ выбираем степенной ряд вида $a_n x^n + \ldots$). Вся эта совокупность образующих и порождает идеал J. Если степенной ряд в J начинается со степени меньше d, то вычитаниями приводим его к начинающемуся со степени не меньше d. А для ряда, начинающегося со степени не меньше d, проводим аналог деления с остатком на степенные ряды, соответствующие образующим $\mathfrak{a}(d)$. Только в отличие от деления многочленов этот процесс бесконечный. В результате такого деления получаем представление степенного ряда в виде суммы произведений некоторых степенных рядов на степенные ряды, соответствующие образующим $\mathfrak{a}(d)$.

2. Конечно порождённый модуль над нётеровым кольцом нётеров. Пусть R — нётерово кольцо, M — нётеров модуль над R. Если M не нётеров, то существует бесконечная последовательность $b_1, b_2, \ldots$ элементов M, такая, что ни один из b_k не выражается как линейная комбинация с коэффициентами из R предыдущих b_i. Записывая b_k как линейные комбинации образующих модуля M $a_1, \ldots, a_N$, получаем, что есть бесконечная последовательность векторов из R^N, такая, что ни один из них не является линейной комбинацией предыдущих с коэффициентами из R. Индукцией по N показываем, что это не так.

3. M — нётеров R-модуль. $\mathfrak{a}$ — аннигиляционный идеал в R. Покажем, что $R/\mathfrak{a}$ — нётерово кольцо.

   $R/\mathfrak{a}$ действует на M так, что ни один его элемент кроме нуля не действует на M нулём.

   Можно считать сразу, что R действует на M так, что ни один элемент, кроме нуля, не действует нулём, и показывать, что R — нётерово кольцо.

   Пусть $m_1, \ldots, m_n$ — порождают M над R. Допустим, M не нёторово. Тогда есть идеал I в R, который не конечно порождён.

Выбираем последовательность $i_1, i_2, \ldots, i_k$, такую, что i_{k+1} не содержится в идеале, порождённом $i_1, \ldots, i_k$, для любого k. Рассматриваем векторы в M^n:

$$\begin{pmatrix} i_1 m_1 \\ \vdots \\ i_1 m_n \end{pmatrix}, \ldots, \begin{pmatrix} i_k m_1 \\ \vdots \\ i_k m_n \end{pmatrix}, \ldots$$

Лемма 1.1. *Если M — нётеров R-модуль, то в любой последовательности векторов из M^n какой-то вектор будет линейной комбинацией предыдущих. Иначе говоря, M^n — нётеров модуль.*

Эта лемма следует из следующей.

Лемма 1.2. *Если M и N — нётеровы R-модули, то $M \times N$ — нётеров R-модуль.*

Proof. Если это не так, то существует бесконечная последовательность

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \ldots, \begin{pmatrix} x_k \\ y_k \end{pmatrix}, \ldots$$

в которой каждый элемент не является линейной комбинацией (с коэффициентами из R) предыдущих. Сначала за счёт нётеровости обнулим первую компоненту, затем вторую. □

Применяя лемму к нашей ситуации, получаем при некотором k равенство

$$\begin{pmatrix} i_k m_1 \\ \vdots \\ i_k m_n \end{pmatrix} = r_1 \begin{pmatrix} i_1 m_1 \\ \vdots \\ i_1 m_n \end{pmatrix} + \ldots + r_{k-1} \begin{pmatrix} i_{k-1} m_1 \\ \vdots \\ i_{k-1} m_n \end{pmatrix}.$$

А отсюда получаем, что $i_k - r_1 i_1 - \ldots - r_{k-1} i_{k-1}$ действует нулём на M. Значит, это 0. Противоречие.

4. а) Нуль на всех координатных плоскостях. Образующая xyz. Если содержатся члены, которые не содержат одну из переменных, например, z, то $p(x,y) + zq(x,y)$ на плоскости $z = 0$ не тождественный ноль.

   б) Нуль на всех координатных прямых. Координатные прямые:

   $$x = y = 0, x = z = 0, y = z = 0.$$

   xy, yz, zx — образующие. Как только есть члены, зависящие только от одной переменной, например $p(x)$, то мы получаем не тождественный ноль на $y = z = 0$.

   в) Нуль на t^2, t^3, t^4. $z - x^2, y^2 - x^3$. Допустим, многочлен обращается в 0 на (t^2, t^3, t^4). Тогда его можно представить в виде

   $$(z - x^2)p(x,y) + q(x,y),$$

и при этом $q(x,y)$ обращается в ноль на (t^2,t^3). А это ровно когда $y^2=x^3$. Делим на y^2-x^3, получаем в остатке многочлен степени не выше 1 по y. Это многочлен вида $yr(x)+u(x)$, причём он обращается в 0 когда $y^2=x^3$. Заменяем y на $-y$, и он уже не обращается в 0, если не был нулевым тождественно.

г)

5. а) Кольцо полиномов, инвариантных относительно действия группы диэдра D_n. Положим $z=x+iy$ и будем рассматривать полиномы $p(z,\overline{z})$. Наш полином должен быть инвариантен относительно сопряжения и умножения z на $e^{2\pi i/n}$. Инвариантами должны быть и его однородные компоненты. Из
$$\frac{1}{n}\sum_{k=0}^{n} p(e^{2\pi i}z,\overline{e^{2\pi i}z})=p(z,\overline{z})$$
получаем, что $z^k\overline{z}^l$ не усредняется в 0 только при $k-l$ делящемся на n. Из инвариантности относительно сопряжения получаем, что наш многочлен представляется в виде суммы членов вида $a(z^k\overline{z}^l+z^l\overline{z}^k)$ с $k-l$ делящимся на n. Значит, образующие $z\overline{z}$ и $z^n+\overline{z}^n$.

Есть ли между этими образующими какие-либо соотношения? Допустим, $p(z\overline{z},z^n+\overline{z}^n)=0$. Представим себе p как многочлен h от $z^n+\overline{z}^n$ с коэффициентами-многочленами от $z\overline{z}$. Старший член
$$q_m(z\overline{z})(z^n+\overline{z}^n)^m.$$
Возьмём $z=re^{i\phi}$. Получаем, что многочлен $h(r^{2n})$ имеет бесконечно много корней (вида $2r^n cos(n\phi)$). Значит, этот многочлен нулевой при всех r. А значит, его старший коэффициент нулевой как многочлен от $z\overline{z}$.

б) Кольцо полиномов, инвариантных относительно действия группы вращений правильного n-угольника.

Как и в предыдущем пункте, получаем, что наш многочлен представляется в виде суммы членов вида $az^k\overline{z}^l$ с $k-l$ делящимся на n. Образующие $1,z\overline{z},z^n,\overline{z}^n$. Соотношение: $(z\overline{z})^n=z^n\overline{z}^n$. Почему нет других соотношений?

6. а) Идеал в $\mathbb{C}[x_1,x_2,x_3]^{\mathbb{S}_3}$, состоящий из функций, обращающихся в 0 при $x_1=x_2$.

Пусть $p(x_1,x_2,x_3)$ принадлежит идеалу. Разделим с остатком p на x_1-x_2 как многочлены от x_1. Получим равенство
$$p(x_1,x_2,x_3)=(x_1-x_2)q(x_1,x_2,x_3)+r(x_2,x_3).$$
Получается, $r(x_2,x_3)$ обращается в 0 при $x_1=x_2$. Значит, он тождественно нулевой. Разделим q на x_1-x_2 с остатком. Получим
$$p(x_1,x_2,x_3)=(x_1-x_2)^2q_1(x_1,x_2,x_3)+(x_1-x_2)r_1(x_2,x_3).$$
Перестановка x_1 и x_2 не меняет многочлена. Поэтому
$$(x_1-x_2)^2q_1(x_1,x_2,x_3)+(x_1-x_2)r_1(x_2,x_3)=(x_1-x_2)^2q_1(x_2,x_1,x_3)+(x_2-x_1)r_1(x_1,x_3).$$

Переносим члены в другие части, получаем:

$$(x_1-x_2)^2(q_1(x_1,x_2,x_3)-q_1(x_2,x_1,x_3)) = (x_2-x_1)(r_1(x_1,x_3)+r_1(x_2,x_3)).$$

Сокращаем на $x_1 - x_2$:

$$(x_2 - x_1)(q_1(x_1, x_2, x_3) - q_1(x_2, x_1, x_3)) = r_1(x_1, x_3) + r_1(x_2, x_3).$$

Подставляя $x_1 = x_2$, получаем $r_1 = 0$. Итак,

$$p(x_1, x_2, x_3) = (x_1 - x_2)^2 q_1(x_1, x_2, x_3).$$

Аналогично, p делится на $(x_2-x_3)^2$ и на $(x_1-x_3)^2$. Значит, он делится на $(x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2$. Это и есть порождающий элемент идеала.

2 Листок 2. Факториальные кольца

1. в) Пусть $g(x) = f(x + m)$. Тогда g — тоже многочлен с целыми коэффициентами.
$$g\left(\frac{p}{q} - m\right) = f\left(\frac{p}{q}\right) = 0.$$
Значит, $\frac{p-mq}{q}$ — корень g. Кроме того, $g(0) = f(m)$. Из пункта а) получаем нужное.

2. Определитель неприводим. Допустим, мы представили наш определитель как произведение двух скобок. Рассмотрим произвольный элемент матрицы x_{ij}. Рассматривая наши многочлены как многочлены от x_{ij} (с коэффициентами из большего кольца), получаем, что x_{ij} содержится ровно в одной из скобок (иначе у нас будет некоторая большая степень x_{ij}), причём содержится в первой степени. x_{ij} и $x_{i'j}, i \neq i'$ находятся в одной скобке, иначе бы в определитель входило их произведение. Итак, каждый столбец входит целиком в одну скобку. Но так же и каждая строчка. А такого быть не может, ибо тогда все переменные входили бы в одну скобку.

3. а) Надо взять в роли p в критерии Эйзенштейна $x - \alpha \in \mathbb{C}[x]$, где α — некратный корень $x^3 + px + q$. Поскольку $x^3 + px + q$ не имеет вид $(x - u)^3$, то у него есть некратный корень.

   б) Рассматриваем как многочлен от y $xy^3 + (1 - x)y + (x^2 - 1)$ и применяем критерий Эйзенштейна с $x - 1$ в роли p.

   в) Что-то неверное.

4. а) Пусть $h_1, h_2, \ldots, h_k$ — однородные порождающие идеала $\mathfrak{a}$. f - некоторый элемент идеала. $f = g_1h_1 + \ldots + g_kh_k, g_i \in \mathbb{C}[x_1, \ldots, x_n]$. Представляя g_i в виде суммы однородных компонент и группируя слагаемые одинаковых степеней, получаем представление f в виде суммы однородных полиномов, лежащих в идеале.

5. Если множеством нулей идеала $\mathfrak{a}$ является начало координат, то по теореме Гильберта о нулях каждый $x_1, \ldots, x_n$ в какой-то степени лежит в идеале. Поэтому там лежат все однородные многочлены достаточно высокой степени.

   В другую сторону: в идеале лежат $x_1^N, \ldots, x_n^N$ при достаточно большом N, а множество их общих нулей — только начало координат. Поскольку идеал не единичный, есть хотя бы один общий ноль. Значит, это начало координат.

6. а) Ясно из лекции, что факториально.

   б) $\mathbb{Q}[x,y]/(x^3-2) = \mathbb{Q}[\sqrt[3]{2}][y]$. Заметим, что в $\mathbb{Q}[\sqrt[3]{2}]$ все элементы кроме нуля обратимы, т.е. это поле. Действительно, пусть $\alpha \in \mathbb{Q}[\sqrt[3]{2}]$. Тогда $\alpha, \alpha^2, \alpha^3, \ldots$ — всё элементы этого кольца, и они линейно зависимы над полем $\mathbb{Q}$, поскольку наше кольцо имеет базис $(1, \sqrt[3]{2}, \sqrt[3]{4})$ над $\mathbb{Q}$. А тогда

$$u_0\alpha^k + u_1\alpha^{k+1} + \ldots + u_n\alpha^{k+n} = 0, k \geq 1, u_i \in \mathbb{Q}, u_0 \neq 0, u_n \neq 0.$$

   Отсюда

$$u_0 + u_1\alpha + \ldots + u_n\alpha^n = 0,$$
$$\alpha(u_1 + \ldots + u_n\alpha^{n-1}) = -u_0,$$

   и α обратим. Значит, $\mathbb{Q}[\sqrt[3]{2}]$ — поле, и $\mathbb{Q}[\sqrt[3]{2}][y]$ факториально.

   в) Пусть $p_1, \ldots, p_r$ — все простые множители N. Обратимые (единицы) в рассматриваемом кольце — это все вида $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \alpha_i \in \mathbb{Z}$. Неприводимыми элементами будут все остальные (кроме $p_1, \ldots, p_r$) простые числа. Ясно, что кольцо факториально.

   г) В $\mathbb{Z}_p$ неприводимые — это p. Любой элемент однозначно раскладывается на произведение нескольких p и обратимый элемент вида $\sum\limits_{k=0}^{\infty} a_k p^k, a_0 \neq 0, 0 \leq a_i \leq p-1$.

   д) Кольцо $\mathbb{Z}[\sqrt{-1}]$. Факториально, поскольку в нём есть алгоритм Евклида. Мы можем делить с остатком одно число на другое, а именно, если у нас есть x, y из кольца и $0 < \|y\| < \|x\|$, то одно из чисел $y, -y, iy, -iy$ образует на комплексной плоскости угол с x меньше 45 градусов (а значит, меньше 60 градусов). Отсюда следует, что (обозначив это число через y_1)

$$\|x - y_1\| < \|x\|.$$

   Действительно, в треугольнике, образованном векторами x, y_1, $x - y_1$ угол против стороны $x - y_1$ меньше 60 градусов. Значит, угол против большей из двух других сторон (а это x) больше 60 градусов. Значит, и выполнено неравенство $\|x - y_1\| < \|x\|$ (против большей стороны лежит больший угол).

   е) $\mathbb{Z}[\sqrt{-3}]$. Имеем, как на лекции:

$$4 = 2 \times 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

3 Листок 3

1. Для $n = 1$ легко (у многочлена от одной переменной не может быть слишком много корней), а дальше индукция. Рассматриваем многочлен как многочлен от x_n, есть набор чисел, при которых его старший коэффициент ненулевой. Подставляем эти числа. Тогда при некотором x_n многочлен ненулевой (случай $n = 1$).

2. а) Однородный неприводимый многочлен второй степени в $\mathbb{C}[x, y]$. Не существует. Если это многочлен $f(x, y) = ax^2 + 2bxy + cy^2$, то, рассматривая отдельно случаи $a = 0$ и $c = 0$, имеем

$$f(x, y) = cx^2 h\left(\frac{y}{x}\right) = cx^2 \left(\frac{y}{x} - \alpha_1\right)\left(\frac{y}{x} - \alpha_2\right) = c(y - \alpha_1 x)(y - \alpha_2 x).$$

б) Многочлен $x^2 + y^2 + z^2$ неприводим. Допустим,

$$x^2 + y^2 + z^2 = (\alpha_1 x + \beta_1 y + \gamma_1 z)(\alpha_2 x + \beta_2 y + \gamma_2 z).$$

Тогда $\alpha_1\alpha_2 = \beta_1\beta_2 = \gamma_1\gamma_2 = 1$. Можно считать $\alpha_1 = 1$. Тогда имеем разложение

$$x^2 + y^2 + z^2 = (x + \beta y + \gamma z)\left(x + \frac{1}{\beta} y + \frac{1}{\gamma} z\right).$$

Из этого разложения получаем $\beta + 1/\beta = 0, \gamma + 1/\gamma = 0, \beta/\gamma + \gamma/\beta = 0$. Отсюда $\beta = \pm i, \gamma = \pm i$, а тогда равенство $\beta/\gamma + \gamma/\beta = 0$ не может выполняться.

3.

4. а)

$$\begin{cases} xy = 0, \\ y^3 + y^2 = 0; \end{cases}$$

$$\begin{cases} xy = 0, \\ y^3 + y^2 = 0; \end{cases}$$

$$\begin{cases} xy = 0, \\ y^2(y + 1) = 0; \end{cases}$$

Имеем два варианта: либо $y = 0$, либо $x = 0, y = -1$. Это и есть неприводимые компоненты. Осталось найти радикал идеала. Это многочлены, зануляющиеся на $y = 0$ и в точке $x = 0, y = -1$. На $y = 0$ зануляются все из идеала (y) и только они, то есть наш многочлен должен делиться на y. В точке $x = 0, y = -1$ зануляются многочлены из идеала $(x, y + 1)$. Наш радикал — это идеал $(xy, y(y + 1))$.

5. Доказываем индукцией по n. База индукции: $n = 2$. $I \subseteq \mathfrak{a}_1 \cup \mathfrak{a}_2$. Допустим, I не содержится ни в $\mathfrak{a}_1$, ни в $\mathfrak{a}_2$. Тогда существует элемент $x \in I$, такой, что $x \notin \mathfrak{a}_2$. Тогда $x \in \mathfrak{a}_1$. Также существует $y \in I$, такой,

что $y \notin \mathfrak{a}_1$. Тогда $y \in \mathfrak{a}_2$. Рассмотрим элемент $x+y$. Он лежит в I, но он не может лежать ни в $\mathfrak{a}_1$, ни в $\mathfrak{a}_2$. Противоречие.

Индукционный переход. Будем следовать указанию. Предположим, что для меньших n чисел утверждение выполнено, а в нашем случае — нет. Тогда каждое $\mathfrak{a}_i$ не лежит в объединении остальных $\mathfrak{a}_k$, и существуют $a_i \in I, i = 1, \ldots, n$, такие, что $a_i \notin \mathfrak{a}_j$ при $i \neq j$. Если бы такое a_i при некотором i не существовало, то мы бы могли выбросить $\mathfrak{a}_i$, обойтись меньшим числом идеалов $\mathfrak{a}_k$ и применить предположение индукции.

Рассмотрим теперь элемент $x = a_1 \ldots a_{n-1} + a_n$. Он лежит в идеале I. Значит, он лежит в некотором идеале $\mathfrak{a}_k$. Если $k < n$, то $a_n \in \mathfrak{a}_k$ — противоречие. Значит, $x \in \mathfrak{a}_n$. Но тогда $a_1 \ldots a_{n-1} \in \mathfrak{a}_n$. А это противоречит простоте идеала $\mathfrak{a}_n$, ведь ни один из множителей в нём не лежит.

4 Листок 4

1. Минимальные многочлены.

а) $5+3i$ над $\mathbb{R}$. Имеем

$$(x-(5+3i))(x-(5-3i)) = x^2 - 10x + 34.$$

Ясно, что меньшей степени быть не может, т.к. меньше только степень 1, а $5+3i$ не является действительным числом.

б)$\sqrt{3}+\sqrt{5}$ над $\mathbb{Q}$. Имеем

$$(x-(\sqrt{5}+\sqrt{3}))(x+(\sqrt{5}+\sqrt{3}))(x-(\sqrt{5}-\sqrt{3}))(x+(\sqrt{5}-\sqrt{3})) =$$
$$= (x^2-(\sqrt{5}+\sqrt{3})^2)(x^2-(\sqrt{5}-\sqrt{3})^2) = (x^2-8-2\sqrt{15})(x^2-8+2\sqrt{15}) =$$
$$= (x^2-8)^2 - 60.$$

5 Листок 5