Лекция 6

6.1 Единственность разложения на неприводимые множители

Определение 6.1: Пусть $f \in k[x_1, \dots, x_n]$. Многочлен f называется неприводимым над k $\Leftrightarrow$ когда $f \notin k$ и f не является произведением двух непостоянных многочленов из $k[x_1, \dots, x_n]$.

Очевидно, что любой непостоянный многочлен может быть разложен в произведение непривод-х.

Теорема 6.1: Пусть $f \in k[x_1, \dots, x_n]$ неприводима над k, т.ч. f делит произведение gh, где $g, h \in k[x_1, \dots, x_n]$. Тогда f делит либо g, либо h.

Доказательство: Индукцией по количеству переменных. Пусть многочлены f, g и $h \in k[x]$. Рассмотрим $p = \gcd(f, g)$. Если $p \notin k$, то в силу неприводимости многочлена f, он может быть записан в виде $f = ap$, где $a \in k$. В этом случае f делит g. Если же $p \in k$, то можно считать, что $p = 1$. Тогда для некоторых $A, B \in k[x]$ имеется равенство $Af + Bg = 1$, умножив которое на h, получим

$$h = h(Af + Bg) = Ahf + Bgh,$$

т.е. f делит h. База индукции доказана.

Предположим, что теорема верна в кольцах многочленов от $n-1$ переменной. Сперва докажем утверждение

(*) Если $u \in k[x_2, \dots, x_n]$ неприводим и делит произведение gh, где $g, h \in k[x_1, \dots, x_n]$, то многочлен u делит либо g, либо h.

Для доказательства (*) перепишем g и h в виде

$$g = \sum_{i=0}^{l} a_i x_1^i \quad \text{и} \quad h = \sum_{i=0}^{m} b_i x_1^i,$$

где $a_i, b_i \in k[x_2, \dots, x_n]$. Многочлен u делит $g \Leftrightarrow u$ делит каждый a_i. Аналогично для многочлена h. Предположим, что u не делит ни g, ни h. Тогда существуют значения индексов $i, j \geq 0$, т.ч. ни a_i не делится на u, ни b_j не делится на u. Пусть i_0, j_0 — это наименьшие индексы с таким свойством. Рассмотрим коэффициент при $x_1^{i_0+j_0}$ в произведении gh:

$$c_{i_0+j_0} = (a_0 b_{i_0+j_0} + a_1 b_{i_0+j_0-1} + \dots + a_{i_0-1} b_{j_0+1}) + a_{i_0} b_{j_0} + (a_{i_0+1} b_{j_0-1} + \dots + a_{i_0+j_0} b_0).$$

В силу выбора i_0 многочлен u делит каждое слагаемое в первой скобке, а в силу выбора j_0 — каждое слагаемое во второй скобке. Многочлен u не делит ни a_{i_0}, ни b_{j_0}, тогда по предположению индукции в силу своей неприводимости u не делит и $a_{i_0} b_{j_0}$. То есть u не делит $c_{i_0+j_0}$, а значит не делит gh. Полученное противоречие доказывает утверждение (*).

Перейдём к общему случаю: пусть f делит $g \cdot h$, где f, g и $h \in k[x_1, \dots, x_n]$. Если f не зависит от x_1, то утверждение доказано. Далее полагаем, что f не является постоянным по x_1.

Заметим, что f остаётся неприводимым, если трактовать его как элемент кольца $k(x_2, \dots, x_n)[x_1]$, где $k(x_2, \dots, x_n)$ — поле рациональных функций от $x_2, \dots, x_n$. Действительно, предположим, что $f = AB$, где $A, B \in k(x_2, \dots, x_n)[x_1]$. Для неприводимости нужно показать, что A или B нулевой степени по x_1. Обозначим через $d \in k[x_2, \dots, x_n]$ — произведение знаменателей в A и B. Тогда $\tilde{A} := dA$, $\tilde{B} := dB$ лежат в $k[x_1, \dots, x_n]$, а значит в кольце $k[x_1, \dots, x_n]$

$$d^2 f = \tilde{A}\tilde{B}.$$

Запишем d^2 как произведение неприводимых множителей из $k[x_2, \dots, x_n]$. По утверждению (*) они делят $\tilde{A}$ или $\tilde{B}$. Сократив их в последнем равенстве, получим в $k[x_1, \dots, x_n]$ равенство

$$f = \tilde{A}_1 \tilde{B}_1.$$

Так как f неприводим в $k[x_1, \dots, x_n]$, то либо $\tilde{A}_1$, либо $\tilde{B}_1$ постоянен. Заметим, что многочлены $\tilde{A}_1, \tilde{B}_1$ получены из A и B делением и умножением на различные элементы $k[x_2, \dots, x_n]$. Следовательно, либо A, либо B не зависит от x_1.

Пусть f неприводим в $k(x_2, \dots, x_n)[x_1]$, тогда согласно базе индукции многочлен f делит g или h в $k(x_2, \dots, x_n)[x_1]$. Для определённости будем считать, что $g = Af$ для некоторого $A \in k(x_2, \dots, x_n)[x_1]$. Домножая последнее равенство на знаменатель d элемента A, получим в $k[x_1, \dots, x_n]$

$$dg = \tilde{A} f.$$

Так как $d \in k[x_2, \dots, x_n]$, то по (*) каждый неприводимый множитель d делит либо $\tilde{A}$, либо f. Последнее невозможно, т.к. f неприводим и положительной степени по x_1. Тогда, проводя сокращения в последнем равенстве, получим, что f делит g. ◀

Следствие: Пусть $f, g \in k[x_1, \dots, x_n]$ положительной степени по x_1. Тогда многочлены f и g имеют общий множитель в $k[x_1, \dots, x_n]$ положительной степени по x_1 тогда и только тогда, когда они имеют общий множитель в $k(x_2, \dots, x_n)[x_1]$

Доказательство: Пусть f, g имеют общий множитель h в $k[x_1, \dots, x_n]$, т.ч. $\deg_{x_1} h > 0$. Тогда у них есть общий множитель и в большем кольце $k(x_2, \dots, x_n)[x_1]$.

Обратно, пусть у f и g есть общий множитель в $k(x_2, \dots, x_n)[x_1]$. Тогда для некоторых $\tilde{f}_1, \tilde{g}_1 \in k(x_2, \dots, x_n)[x_1]$ имеем

$$f = \tilde{h}\tilde{f}_1 \quad \text{и} \quad g = \tilde{h}\tilde{g}_1.$$

Обозначим через $d \in k[x_2,\dots,x_n]$ общий знаменатель $\tilde{h}$, $\tilde{f}_1$ и $\tilde{g}_1$. Тогда

$$h = d\tilde{h}, \quad f_1 = d\tilde{f}_1, \quad g_1 = d\tilde{g}_1$$

— многочлены из $k[x_1,\dots,x_n]$, и в кольце $k[x_1,\dots,x_n]$ имеются равенства

$$d^2 f = h f_1, \quad d^2 g = h g_1.$$

Так как $\tilde{h} = h/d$ имеет положительную степень по x_1, то у h существует неприводимый множитель положительной степени по x_1. Поскольку h_1 делит $d^2 f$, то h_1 делит либо d^2, либо многочлен f. Замечая, что $d^2 \in k[x_2,\dots,x_n]$, получаем, что h_1 делит f в $k[x_1,\dots,x_n]$. Аналогично доказывается, что h_1 делит g.

Теорема 6.2: Каждый непостоянный $f \in k[x_1,\dots,x_n]$ может быть представлен в виде

$$f = f_1 \cdot f_2 \cdot \ldots \cdot f_r,$$

где f_i неприводимы над k. Более того, если $f = g_1 \cdot g_2 \cdot \ldots \cdot g_s$ — другое такое разложение, то $r = s$ и f_i-ые с точностью до перестановки совпадают с g_i-ми, умноженными на ненулевые элементы k.

Доказательство: (а) Из теоремы 6.1 следует, что, если f неприводим и делит произведение $h_1 \cdot \ldots \cdot h_s$, то f делит некоторый h_i.

(б) Существование разложения очевидно. Пусть $f = f_1 \cdot \ldots \cdot f_r = g_1 \cdot \ldots \cdot g_s$, где f_i-ые и g_j-ые неприводимы. Если $r = s$, то в силу (а)

f_1 делит $g_{i_1} \in \{g_1, \dots, g_s\}$, где в силу неприводимости $\frac{g_{i_1}}{f_1} \in k$;

f_2 делит $g_{i_2} \in \{g_1, \dots, g_s\} \setminus \{g_{i_1}\}$, где в силу неприводимости $g_{i_2}/f_2 \in k$;

… … …

f_r делит $g_{i_r} \in \{g_1, \dots, g_s\} \setminus \{g_{i_1}, \dots, g_{i_{r-1}}\}$, где в силу неприводимости $g_{i_r}/f_r \in k$.

Если же $r > s$, то, проводя сокращения в равенстве $f_1 \cdot \ldots \cdot f_r = g_1 \cdot \ldots \cdot g_s$, получим противоречие с неприводимостью g_j-х.

6.2 Результанты

Пусть многочлены

$$f(x) = a_0 x^l + a_1 x^{l-1} + \ldots + a_l$$

$$g(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m$$

из $k[x]$ имеют степень l и m, соответственно.

Утверждение 6.1: Многочлены f и g имеют общий множитель тогда и только тогда, когда существует многочлен $A \in k[x]$ степени $< l+m-1$, к-ый делится на оба многочлена (иными словами, когда пр-ва многочленов степени $l+m-1$, делящихся по отдельности на f и g, имеют нетривиальное пересечение).

Последнее эквивалентно линейной зависимости многочленов

$$f,\ xf,\ \dots,\ x^{m-1}f,\ g,\ xg,\ \dots,\ x^{l-1}g,$$

или тому, что матрица размерности $(l+m)\times(l+m)$

$$Syl(f,g,x) := \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & a_0 & b_2 & b_1 & \ddots & b_0 \\ \vdots & a_2 & \ddots & a_1 & \vdots & b_2 & \ddots & b_1 \\ a_l & \vdots & & a_2 & b_m & \vdots & & b_2 \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & a_l & & & \ddots & b_m \end{pmatrix}$$

имеет нулевой определитель $Res(f,g,x) := \det(Syl(f,g,x))$, который называется **результантом** многочленов f и g.

Предложение 6.1: Пусть $f,g \in k[x_1,\dots,x_n]$ – многочлены положительной степени по x_1. Тогда

(i) $Res(f,g,x_1) \in \langle f,g\rangle \cap k[x_2,\dots,x_n]$.

(ii) $Res(f,g,x_1) = 0 \Leftrightarrow$ когда f и g имеют общий множитель в $k[x_1,\dots,x_n]$ положительной степени по x_1.

Доказательство: Из определения определителя следует, что $Res(f,g,x_1) \in k[x_2,\dots,x_n]$. Известно, что существуют $A,B \in k[x_2,\dots,x_n][x_1]$, т.ч. $Af + Bg = Res(f,g,x_1)$, т.е. $Res(f,g,x_1) \in \langle f,g\rangle$.

Докажем (ii). Заметим, что для $f,g \in k[x_1,\dots,x_n]$ результант $Res(f,g,x_1) = 0$ $\Leftrightarrow$ когда f и g имеют общий множитель в кольце $k(x_2,\dots,x_n)[x_1]$ положительной степени по x_1. Тогда по следствию из теоремы 6.1 f и g имеют общий множитель в $k[x_1,\dots,x_n]$ положительной по x_1 степени. ◀

Следствие: Если $f,g \in \mathbb{C}[x]$, то результант $Res(f,g,x) = 0 \Leftrightarrow$ когда f и g имеют общий корень в $\mathbb{C}$.

Многочлены $f,g \in \mathbb{C}[x_1,\dots,x_n]$ положительной по x_1 степени можно записать в виде

$$f = a_0x_1^l + a_1x_1^{l-1} + \dots + a_l,$$
$$g = b_0x_1^m + b_1x_1^{m-1} + \dots + b_m,$$

где $a_i, b_j \in \mathbb{C}[x_2,\dots,x_n]$.

Предложение 6.2: Пусть $f,g \in \mathbb{C}[x_1,\dots,x_n]$ имеют степень l, m по x_1, соответственно, и пусть $c = (c_2,\dots,c_n) \in \mathbb{C}^{n-1}$, т.ч.

(i) $f(x_1,c) \in \mathbb{C}[x_1]$ имеет степень l.

(ii) $g(x_1,c) \in \mathbb{C}[x_1]$ имеет степень $p \le m$.

Тогда для многочлена $h = Res(f,g,x_1) \in \mathbb{C}[x_2,\dots,x_n]$ справедливо

$$h(c) = a_0(c)^{m-p}\, Res(f(x_1,c), g(x_1,c), x_1).$$

Доказательство: Подставив точку $c=(c_2,\dots,c_n)\in\mathbb{C}^{n-1}$ в результант, записанный в виде определителя, получим выражение

$$h(c)=\det\begin{pmatrix} a_0(c) & & & b_0(c) & & \\ \vdots & \ddots & a_0(c) & \vdots & \ddots & b_0(c) \\ a_\ell(c) & & \vdots & b_m(c) & & \\ & \ddots & a_\ell(c) & & \ddots & b_m(c) \end{pmatrix}.$$

Если $p=m$, то $h(c)=\mathrm{Res}(f(x_1,c),g(x_1,c),x_1)$. При $p<m$ указанный определитель перестаёт быть результантом многочленов $f(x_1,c)$ и $g(x_1,c)$. Однако, последовательно раскладывая его p раз по первой строке, мы придём к требуемому соотношению. ◀

Теорема 5.2 (об продолжении) Пусть $I=\langle f_1,\dots,f_s\rangle\subset\mathbb{C}[x_1,\dots,x_s]$, для всех $1\le i\le s$ образующие идеала записываются в виде

$$f_i=g_i(x_2,\dots,x_n)x_1^{N_i}+\text{члены, в которых степень } x_1<N_i,$$

где $N_i\ge 0$ и $g_i\in\mathbb{C}[x_2,\dots,x_n]$ ненулевой. Тогда, если частное решение $c=(c_2,\dots,c_n)\in\mathbb{V}(I_1)$, т.ч. $(c_2,\dots,c_n)\notin\mathbb{V}(g_1,\dots,g_s)$, то существует $c_1\in\mathbb{C}$, для которого $(c_1,c_2,\dots,c_n)\in\mathbb{V}(I)$.

Доказательство: Рассмотрим гомоморфизм колец

$$\mathbb{C}[x_1,\dots,x_n]\to\mathbb{C}[x_1],$$
$$f(x_1,\dots,x_n)\mapsto f(x_1,c).$$

Заметим, что образ I отн-но этого гомоморфизма является идеалом в $\mathbb{C}[x_1]$. Это вытекает из того, что гомоморфизм действует тождественно на подкольце $\mathbb{C}[x_1]$.

Поскольку кольцо $\mathbb{C}[x_1]$ является кольцом главных идеалов, то образ идеала

$$\{f(x_1,c):f\in I\}=\langle u(x_1)\rangle,$$

где $u(x_1)$ лежит в образе. Если $u(x_1)$ не постоянный, то по основной теореме алгебры найдётся $c_1\in\mathbb{C}$, т.ч. $u(c_1)=0$. Тогда $f(c_1,c)=0$ для всех $f\in I$, и, следовательно, точка $(c_1,c)\in\mathbb{V}(I)$.

Если $u_1(x)$ нулевой многочлен, то $f_i(x_1,c)=0$ для всех $i\in\{1,s\}$, тогда $g_i(c)=0$ для всех $i\in\{1,s\}$, т.е. $c\in\mathbb{V}(g_1,\dots,g_s)$. Противоречие.

Предположим, что $u(x_1)=u_0$ – ненулевая константа из k. Тогда существует $f\in I$, т.ч. $f(x_1,c)=u_0$. По условию теоремы $c\notin\mathbb{V}(g_1,\dots,g_s)$, т.е. $g_i(c)\neq 0$ для некоторого i. Рассмотрим $h=\mathrm{Res}(f_i,f,x_1)$, по предложению 6.2

$$h(c)=g_0(c)^{\deg f}\,\mathrm{Res}(f_i(x_1,c),f(x_1,c),x_1),$$

где $f(x_1,c)=u_0$. Легко заметить, что $\mathrm{Res}(f_i(x_1,c),u_0,x_1)=u_0^{N_i}$, т.е. $h(c)\neq 0$. В силу $f_i,f\in I$ по предложению 6.1 $h\in I_1$, но тогда $h(c)=0$, т.к. $c\in\mathbb{V}(I_1)$. ◀