Лекция 21.

Гайфуллин Сергей Александрович

МГУ

10 декабря, 2021

Теорема

Пусть $r = \frac{f}{g} \in F(x)$ – правильная дробь. И пусть $g = p_1^{k_1} \dots p_s^{k_s}$. Тогда существует единственное разложение

$$r = \sum_{i=1}^{s} \sum_{j=1}^{k_i} \frac{h_{ij}}{p_i^j},$$

где $\deg h_{ij} < \deg p_i$.

Было. (Доказательство существования).

Лемма

Пусть $g = g_1 g_2$, где g_1 и g_2 взаимно просты. Тогда правильную дробь $\frac{f}{g}$ можно представить в виде суммы правильных дробей $\frac{f}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2}$.

Следствие

Если $g = p_1^{k_1} \dots p_s^{k_s}$, то правильная дробь $\frac{f}{g}$ может быть представлена в виде суммы правильных дробей

$$\frac{f}{g} = \frac{f_1}{p_1^{k_1}} + \dots + \frac{f_s}{p_s^{k_s}}$$

Лемма

Правильную дробь $\frac{f}{p^k}$ можно представить в виде суммы простейших дробей

$$\frac{f}{p^k} = \frac{h_1}{p} + \frac{h_2}{p^2} + \dots + \frac{h_k}{p^k}.$$

Доказательство единственности.

Пусть $g = p_1^{k_1} \dots p_s^{k_s}$ и

$$\frac{f}{g} = \sum_{i=1}^{s} \sum_{j=1}^{k_i} \frac{h_{ij}}{p_i^j} = \sum_{i=1}^{s} \sum_{j=1}^{k_i} \frac{\widetilde{h}_{ij}}{p_i^j}.$$

Домножим это равенство на g. Получим

$$\sum_{i=1}^{s} \sum_{j=1}^{k_i} h_{ij} p_1^{k_1} \dots p_i^{k_i - j} \dots p_s^{k_s} = \sum_{i=1}^{s} \sum_{j=1}^{k_i} \widetilde{h}_{ij} p_1^{k_1} \dots p_i^{k_i - j} \dots p_s^{k_s}.$$

Перенося все в одну часть, получаем

$$\sum_{i=1}^{s} \sum_{j=1}^{k_i} (h_{ij} - \widetilde{h}_{ij}) p_1^{k_1} \dots p_i^{k_i - j} \dots p_s^{k_s} = 0. \qquad (1)$$

Продолжение доказательства единственности.

Так как не все h_{ij} равны $\widetilde{h}_{ij}$, можно выбрать такие a и b, что $h_{ab} \neq \widetilde{h}_{ab}$ и при этом $h_{ac} = \widetilde{h}_{ac}$ при $c > b$. Рассмотрим слагаемое

$$(h_{ab} - \widetilde{h}_{ab}) p_1^{k_1} \dots p_a^{k_a - b} \dots p_s^{k_s}$$

в сумме (1). Так как $\deg(h_{ab} - \widetilde{h}_{ab}) < \deg p_a$, это слагаемое не делится на $p_a^{k_a - b + 1}$. Однако все остальные слагаемые в сумме (1) делятся на $p_a^{k_a - b + 1}$. В самом деле, если $i \neq a$, то слагаемое

$$(h_{ij} - \widetilde{h}_{ij}) p_1^{k_1} \dots p_i^{k_i - j} \dots p_s^{k_s}$$

делится на $p_a^{k_a}$ и $k_a \geq k_a - b + 1$. Если же $i = a$ и $c < b$, то

$$(h_{ac} - \widetilde{h}_{ac}) p_1^{k_1} \dots p_a^{k_a - c} \dots p_s^{k_s}$$

делится на $p_a^{k_a - c}$ и $k_a - c \geq k_a - b + 1$. При $i = a$, и $c > b$ слагаемые нулевые.

Итак, в сумме (1) все слагаемые, кроме одного делятся на $p_a^{k_a - b + 1}$, а одно – нет. Противоречие с тем, что сумма равна 0.

Определение

Кольцо многочленов от переменных $x_1, \ldots, x_n$ с коэффициентами из поля F определим рекурсивно

$$F[x_1, \ldots, x_n] = F[x_1, \ldots, x_{n-1}][x_n].$$

Каждый многочлен представляется в виде конечной линейной комбинации мономов вида $x_1^{k_1} \ldots x_n^{k_n}$.

$$f(x_1, \ldots, x_n) = \sum_{0 \le k_i \le m_i} a_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n}.$$

При суммировании многочленов суммируются соответствующие коэффициенты. Произведение многочленов $f = \sum_{0 \le k_i \le m_i} a_{k_1,\ldots,k_n} x_1^{k_1} \ldots x_n^{k_n}$ и $g = \sum_{0 \le s_i \le l_i} b_{s_1,\ldots,s_n} x_1^{s_1} \ldots x_n^{s_n}$. есть многочлен $h = \sum_{0 \le p_i \le r_i} c_{p_1,\ldots,p_n} x_1^{p_1} \ldots x_n^{p_n}$, где

$$c_{p_1,\ldots,p_n} = \sum_{0 \le k_i \le p_i} a_{k_1,\ldots,k_n} b_{p_1-k_1,\ldots,p_n-k_n}.$$

Утверждение (Было)

Пусть R – область целостности. Тогда $R[x]$ – также область целостности.

Следствие.

Если R – область целостности, то $R[x_1, \ldots, x_n]$ – также область целостности.

В частности, если F – поле, то $F[x_1, \ldots, x_n]$ – область целостности.
Далее мы рассматриваем многочлены $F[x_1, \ldots, x_n]$ над полем F.

Порядок на мономах.

Сейчас наша цель – ввести порядок $\succ$ на множестве мономов, который удовлетворяет следующим свойствам.

1. для любых двух несовпадающих мономов m_α и m_β либо $m_\alpha \succ m_\beta$ либо $m_\alpha \prec m_\beta$.
2. не может быть $m_\alpha \succ m_\beta$ и $m_\alpha \prec m_\beta$.
3. из того, что $m_\alpha \succ m_\beta$ и $m_\beta \succ m_\gamma$, следует $m_\alpha \succ m_\gamma$ (транзитивность).
4. из того, что $m_\alpha \succ m_\beta$, следует $m_\alpha m_\gamma \succ m_\beta m_\gamma$ (согласованность с умножением).
5. не существует бесконечных убывающих цепочек мономов $m_1 \succ m_2 \succ m_3 \succ \dots$

Заметим, что из 3) и 4) следует свойство
4') из того, что $m_\alpha \succ m_\beta$ и $m_\gamma \succ m_\delta$, следует, что $m_\alpha m_\gamma \succ m_\beta m_\delta$.

Доказательство. $m_\alpha m_\gamma \succ m_\beta m_\gamma \succ m_\beta m_\delta$.

Лексикографический порядок.

Определение.

Определим лексикографический порядок на мономах (lex). Пусть $m_\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}, m_\beta = x_1^{\beta_1} \dots x_n^{\beta_n}$. И пусть $\alpha_1 = \beta_1, \dots, \alpha_{k-1} = \beta_{k-1}$ и $\alpha_k \neq \beta_k$. Тогда если $\alpha_k > \beta_k$, то $m_\alpha \succ m_\beta$. А если $\alpha_k < \beta_k$, то $m_\alpha \prec m_\beta$.

Предложение.

Лексикографическийй порядок удовлетворяет свойствам 1)-5).

Доказательство. Свойства 1) и 2) очевидно следуют из определения. Докажем 3). Так как $m_\alpha \succ m_\beta$, найдется k такое, что $\alpha_i = \beta_i$ при $i < k$ и $\alpha_k > \beta_k$. Так как $m_\beta \succ m_\gamma$, найдется l такое, что $\beta_i = \gamma_i$ при $i < l$ и $\beta_l > \gamma_l$. Если $k < l$, то при $i < k$ выполнено $\alpha_i = \beta_i = \gamma_i$, а также $\alpha_k > \beta_k = \gamma_k$. Если $k > l$, то при $i < l$ выполнено $\alpha_i = \beta_i = \gamma_i$, и $\alpha_l = \beta_l > \gamma_l$. Если же $l = k$, то при $i < k$ выполнено $\alpha_i = \beta_i = \gamma_i$, и $\alpha_k > \beta_k > \gamma_k$.

Продолжение доказательства.

4) Так как $m_\alpha \succ m_\beta$, найдется k такое, что $\alpha_i = \beta_i$ при $i < k$ и $\alpha_k > \beta_k$. Тогда при $i < k$ получаем $\alpha_i + \gamma_i = \beta_i + \gamma_i$, а также $\alpha_k + \gamma_k > \beta_k + \gamma_k$. Значит, $m_\alpha m_\gamma \succ m_\beta m_\gamma$.

Продолжение доказательства.

5) Проведем индукцию по n. База $n = 1$. Тогда $m_1 = x^k$. Тогда в убывающей последовательности $m_1 \succ m_2 \succ m_3 \succ \ldots$ могут встретиться только x^t при $t \leq k$. Значит, эта последовательность конечна.
Шаг индукции. Пусть свойство 5) доказано для всех $n < l$. Докажем для $n = l$. Допустим, что существует бесконечная убывающая последовательность $m_1 \succ m_2 \succ m_3 \succ \ldots$ При этом $m_1 = x_1^{\alpha_1} \ldots x_l^{\alpha_l}$. При переходе от m_i к m_{i+1} показатель степени x_1 либо не меняется, либо убывает. Следовательно, убывать он может лишь конечное число раз. Значит, найдется такое натуральное N, что начиная с m_N показатель степени x_1 не меняется. То есть при $j \geq N$ выполнено $m_j = x_1^a \widetilde{m}_j$, где $\widetilde{m}_j$ – моном от переменных $x_2, \ldots, x_l$. Однако при убывании m_j, $j \geq N$ убывают и $\widetilde{m}_j$, то есть $\widetilde{m_1} \succ \widetilde{m_2} \succ \widetilde{m_3} \succ \ldots$ – бесконечная убывающая последовательность для $n = l - 1$. Противоречие. Значит, не существует бесконечной убывающей последовательности $m_1 \succ m_2 \succ m_3 \succ \ldots$ при $n = l$.

Замечание.

Можно вместо порядка lex использовать, например, однородный лексикографический порядок deglex, который устроен следующим образом. Для того, чтобы сравнить два монома $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ и $x_1^{\beta_1} \dots x_n^{\beta_n}$ мы сперва сравниваем $\sum_{i=1}^{n} \alpha_i$ и $\sum_{i=1}^{n} \beta_i$. Если больше первая сумма, то мы говорим, что первый моном больше. Если вторая, то больше второй моном. Если же данные суммы равны, то мы сравниваем эти мономы с помощью lex.

Для такого порядка легче доказать свойство 5), так как для данного монома есть лишь конечное число мономов меньших его. (Для lex это свойство не верно при $n \geq 2$.)

Существуют и другие порядки на мономах, удовлетворяющие свойствам 1)-5). В дальнейшем, если не оговорено противного, мы будем использовать порядок lex, хотя все рассуждения подходят для любого порядка со свойствами 1)-5).

Определение.

Пусть $f = \sum a_{i_1,\ldots,i_n} x_1^{i_1} \ldots x_n^{i_n}$. Старшим мономом многочлена f называется наибольший (в смысле нашего порядка) моном $x_1^{j_1} \ldots x_n^{j_n}$, входящий в f с ненулевым коэффициентом. Обозначать старший моном f мы будем через $LM(f)$. Старший член многочлена f – это старший моном с коэффициентом (с которым он входит в f), то есть $a_{j_1,\ldots,j_n} x_1^{j_1} \ldots x_n^{j_n}$. Обозначать старший член f мы будем через $LT(f)$.

Пример.

Пусть

$$f = 3x_1^5 x_2^4 x_3^7 + 2x_1^6 x_2^3 x_3^{10} - 2x_1^6 x_2^5 x_3^3 + 8x_1 x_2^{11} x_3^9.$$

Тогда

$$LM(f) = x_1^6 x_2^5 x_3^3, \qquad LT(f) = -2x_1^6 x_2^5 x_3^3.$$

Лемма о старшем члене.

Пусть f и g – многочлены от переменных $x_1, \ldots, x_n$. Тогда $LT(fg) = LT(f)LT(g)$.

Доказательство. Пусть $f = LT(f) + c_1 m_1 + \ldots + c_s m_s$, где $c_i \in F$, m_i – мономы. При этом $m_i \prec LM(f)$. Аналогично, $g = LT(g) + d_1 l_1 + \ldots + d_r l_r$, где $d_i \in F$, l_i – мономы. При этом $l_i \prec LM(g)$. Имеем

$$fg = LT(f)LT(g) + LT(f)\sum d_j l_j + LT(g)\sum c_i m_i + \sum c_i d_j m_i l_j.$$

При этом $LM(f)LM(g) \succ LM(f)l_j$, $LM(f)LM(g) \succ LM(g)m_i$ и $LM(f)LM(g) \succ m_i l_j$. Значит, моном $LM(f)LM(g)$ строго больше остальных мономов, получающихся при произведении. То есть это будет старший моном fg, причем он войдет именно с коэффициентом из $LT(f)LT(g)$, так как остальные слагаемые не могут повлиять на этот коэффициент.