

ЛЕКЦИЯ 20

Непосредственно из факториальности кольца многочленов над полем следует.

**Лемма 1.** Пусть  $f, g \in F[z]$ , где  $F$  – поле. И пусть  $f = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ ,  $g = p_1^{\beta_1} \dots p_m^{\beta_m}$ . Тогда  $f|g$  если и только если  $\alpha_i \leq \beta_i$  для всех  $i$ .

**Следствие 1.** Пусть  $f, g \in F[z]$  и пусть  $f = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ ,  $g = p_1^{\beta_1} \dots p_m^{\beta_m}$ . Тогда

$$\text{НОД}(f, g) = p_1^{\min\{\alpha_1, \beta_1\}} \dots p_m^{\min\{\alpha_m, \beta_m\}}.$$

$$\text{НОК}(f, g) = p_1^{\max\{\alpha_1, \beta_1\}} \dots p_m^{\max\{\alpha_m, \beta_m\}}.$$

**Определение 1.** Формальная производная – это отображение  $F[x] \rightarrow F[x]$ ,  $f \mapsto f'$ , определенное по правилу

$$a_n x^n + \dots + a_0 = n a_n x^{n-1} + \dots + a_1.$$

**Свойства производной.**

1)  $(f + g)' = f' + g'$ .

2)  $(\lambda f)' = \lambda f'$ .

3)  $(fg)' = f'g + fg'$ . (правило Лейбница.)

Докажем это. Сперва докажем для  $f = x^k$  и  $g = x^l$ . Тогда  $(fg)' = (x^{k+l})' = (k+l)x^{k+l-1} = kx^{k-1}x^l + lx^kx^{l-1}$ .

В общем случае  $f = \sum a_i x^i$ ,  $g = \sum b_j x^j$ . Тогда  $fg = \sum (a_i b_j x^i x^j)$  и

$$\begin{aligned} (fg)' &= \left( \sum (a_i b_j x^i x^j) \right)' = \sum a_i b_j (x^i x^j)' = \sum a_i b_j ((x^i)' x^j + x^i (x^j)') = \\ &= \sum a_i (x^i)' \sum b_j x^j + \sum a_i x^i \sum b_j (x^j)' = f'g + fg'. \end{aligned}$$

4)

$$(f_1 \dots f_k)' = \sum_{i=1}^k \left( \prod_{j \neq i} f_j \right) f_i'.$$

**Упражнение.** Вывести это из правила Лейбница.

5)  $(f^k)' = k f^{k-1} f'$ .

**Определение 2.**  $k$ -я производная многочлена  $f$  – это  $f^{(k)} = (f^{(k-1)})'$ .

При этом  $f^{(0)} = f$ .

**Предложение 1.** Пусть  $F$  – поле нулевой характеристики. Число  $c \in F$  является корнем кратности  $k$  многочлена  $f \in F[x]$  тогда и только тогда, когда  $f^{(0)}(c) = \dots = f^{(k-1)}(c) = 0$  и  $f^{(k)}(c) \neq 0$ .

*Доказательство.* Пусть  $f(x) = b_k(x-c)^k + \dots + b_n(x-c)^n = (x-c)^k g(x)$ . Тогда при  $m < k$  докажем, что  $f^{(m)}$  делится на  $(x-c)^{k-m}$ . База  $m = 0$ . Шаг

$$f^{(m)}(x) = (f^{(m-1)}(x))' = ((x-c)^{k-m+1} h(x))' = (k-m+1)(x-c)^{k-m} h + (x-c)^{k-m+1} h'.$$

С другой стороны  $f^{(k)}(x) = k! b_k + (x-c) \cdot s(x)$ . И потому  $f^{(k)}(c) \neq 0$ . □

**Следствие 2.** Пусть  $c$  – корень кратности  $k > 0$  многочлена  $f(x)$ . Тогда  $c$  – корень кратности  $k-1$  многочлена  $f'(x)$ .

**Следствие 3.** Многочлен  $\text{НОД}(f, f')$  своими корнями имеет только кратные корни  $f(x)$ . Причем кратности всех корней в многочлене  $\text{НОД}(f, f')$  на 1 меньше, чем в  $f$ .

**Следствие 4** (Избавление от кратных корней). Многочлен  $\frac{f(x)}{\text{НОД}(f, f')}$  своими корнями имеет все корни  $f(x)$  с кратностями 1.

**Теорема 1** (Формула Тейлора для многочлена). Пусть  $F$  – поле нулевой характеристики, тогда

$$f(x) = \sum_{i=0}^{\deg f} \frac{f^{(i)}(c)}{i!} (x-c)^i.$$

*Доказательство.* Мы знаем, что

$$f(x) = \sum_{i=0}^{\deg f} b_i(x-c)^i.$$

При этом

$$f(x)^{(i)} = i!b_i + (x-c) \cdot h(x).$$

То есть  $f^{(i)}(c) = i!b_i$ , значит,

$$b_i = \frac{f^{(i)}(c)}{i!}.$$

□

### Многочлены от нескольких переменных.

**Определение 3.** Кольцо многочленов от переменных  $x_1, \dots, x_n$  с коэффициентами из поля  $F$  определим рекурсивно

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

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

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

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

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

**Утверждение 1** (Было). Пусть  $R$  – область целостности. Тогда  $R[x]$  – также область целостности.

**Следствие 5.** Если  $R$  – область целостности, то  $R[x_1, \dots, x_n]$  – также область целостности.

В частности, если  $F$  – поле, то  $F[x_1, \dots, x_n]$  – область целостности.

Далее мы рассматриваем многочлены  $F[x_1, \dots, x_n]$  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  $m_\alpha$  и  $m_\beta$  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.*  $m_\alpha m_\gamma \succ m_\beta m_\gamma \succ m_\beta m_\delta$ . □

**Определение 4.** Определим *лексикографический порядок* на мономах (lex). Пусть

$$m_\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}, \quad m_\beta = x_1^{\beta_1} \dots x_n^{\beta_n}.$$

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 2.** Лексикографический 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  $\alpha_k > \beta_k > \gamma_k$ .

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,  $m_\alpha m_\gamma \succ m_\beta m_\gamma$ .

5) Проведем индукцию по  $n$ . База  $n = 1$ . Тогда  $m_1 = x^k$ . Тогда в убывающей последовательности  $m_1 \succ m_2 \succ m_3 \succ \dots$  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  $m_1 \succ m_2 \succ m_3 \succ \dots$ . При этом  $m_1 = x_1^{\alpha_1} \dots x_l^{\alpha_l}$ . 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  $m_j = x_1^q \tilde{m}_j$ , где  $\tilde{m}_j$  – моном от переменных  $x_2, \dots, x_l$ . Однако при убывании  $m_j$ ,  $j \geq N$  убывают и  $\tilde{m}_j$ , то есть  $\tilde{m}_1 \succ \tilde{m}_2 \succ \tilde{m}_3 \succ \dots$  – бесконечная убывающая последовательность для  $n = l - 1$ . Противоречие. Значит, не существует бесконечной убывающей последовательности  $m_1 \succ m_2 \succ m_3 \succ \dots$  при  $n = l$ .  $\square$

*Замечание 1.* 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 5.** Пусть  $f = \sum a_{i_1, \dots, i_n} x_1^{i_1} \dots x_n^{i_n}$ . *Старшим мономом* многочлена  $f$  называется наибольший (в смысле нашего порядка) моном  $x_1^{j_1} \dots x_n^{j_n}$ , 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  $a_{j_1, \dots, j_n} x_1^{j_1} \dots x_n^{j_n}$ . Обозначать старший член  $f$  мы будем через  $LT(f)$ .

**Пример 1.** 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

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

**Лемма 2** (о старшем члене). Пусть  $f$  и  $g$  – многочлены от переменных  $x_1, \dots, x_n$ . Тогда

$$LT(fg) = LT(f)LT(g).$$

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