Лекция 19.

Гайфуллин Сергей Александрович

МГУ

30 ноября, 2021

Лемма

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 $f | g$ если и только если $\alpha_i \leq \beta_i$ для всех i.

Следствие

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

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

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

Пример нефакториального кольца

Многочлены вида $a_0 + a_2 x^2 + \ldots + a_n x^n$.

В этом кольце $x^6 = (x^2)^3 = (x^3)^2$ и при этом и x^2 и x^3 неприводимы.

Определение

Формальная производная – это отображение $F[x] \to F[x]$, $f \mapsto f'$, определенное по правилу

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

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 $(fg)' = (x^{k+l})' = (k+l)x^{k+l-1} = kx^{k-1}x^l + lx^k x^{l-1}$.
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

$$(fg)' = \left(\sum (a_i b_j x^i x^j)\right)' = \sum a_i b_j (x^i x^j)' = \sum a_i b_j ((x^i)' x^j + x^i (x^j)') =$$
$$= \sum a_i (x^i)' \sum b_j x^j + \sum a_i x^i \sum b_j (x^j)' = f'g + fg'.$$

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

Определение

k-я производная многочлена f – это $f^{(k)} = \left(f^{(k-1)}\right)'$.
При этом $f^{(0)} = f$.

Предложение

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

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

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

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

Следствие

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

Следствие

Многочлен НОД(f, f') своими корнями имеет только кратные корни $f(x)$. Причем кратности всех корней в многочлене НОД(f, f') на 1 меньше, чем в f.

Избавление от кратных корней.

Следствие

Многочлен $\frac{f(x)}{\text{НОД}(f,f')}$ своими корнями имеет все корни $f(x)$ с кратностями 1.

Теорема (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,

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

Определение

Пусть $a_0, \ldots, a_n$ – последовательность вещественных чисел. Количество перемен знака в ней – это количество пар рядом стоящих положительных и отрицательных чисел после вычеркивания всех нулей.

Пусть нам дан многочлен $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$. Количество перемен знака в последовательности $a_0, \ldots, a_n$ обозначим через $L(f)$. Количество положительных корней с учетом кратностей обозначим через $N(f)$.

Теорема (Декарт)

1) $N(f) \equiv L(f) \pmod 2$,
2) $N(f) \leq L(f)$,
3) если f не имеет комплексных (не вещественных) корней, то $N(f) = L(f)$.

Доказательство.

1. Можем считать, что $a_n > 0$. Иначе заменим f на $-f$, при этом $L(f)$ и $N(f)$ не поменяются.
Кроме того можем считать, что $a_0 \neq 0$. Иначе $f(x)$ поделим на x^k, при этом $L(f)$ и $N(f)$ не поменяются.
Так как $a_n > 0$, число перемен знака $L(f)$ четно при $a_0 > 0$ и нечетно при $a_0 < 0$. С другой стороны $f(0) = a_0$. Будем двигаться от 0 вправо. При переходе через корень нечетной степени, знак функции $f(x)$ меняется, а через корень четной степени – не меняется. Получается, что в итоге знак поменяется, если сумма кратностей положительных корней нечетна и не поменяется, если четна. Но на бесконечности должно получиться положительное значение. Значит, сумма кратностей положительных корней четна, если $a_0 > 0$ и нечетна, если $a_0 < 0$. Пункт 1 доказан.

Доказательство.

2. Докажем, что $N(f') \geq N(f) - 1$. В самом деле, если c_i – корень f кратности k_i, то c_i – корень f кратности $k_i - 1$. Кроме того по теорема Ролля между любыми двумя корнями многочлена f есть корень f'. Суммируя, получаем нужное неравенство.
С другой стороны, $L(f') \leq L(f)$. Так как $L(f')$ – число перемен знака в последовательности $a_1, 2a_2, \dots na_n$, что равно числу перемен знака в $a_1, a_2, \dots a_n$.
Докажем пункт 2 индукцией по $n = \deg f$. База $n = 0$. Ясно.
Шаг. $N(f) \leq N(f') + 1 \leq L(f') + 1 \leq L(f) + 1$. Но так как $N(f) \equiv L(f) \pmod 2$, равенства быть не может.

Доказательство.

3. Рассмотрим $\widetilde{f}(x) = f(-x) = a_0 - a_1x + a_2x^2 - a_3x^3 + \dots$. Тогда $L(f) + L(\widetilde{f}) \leq n$. В самом деле, если все коэффициенты $a_i \neq 0$, то перемена знака в последовательности $a_0, -a_1, a_2, -a_3 \dots$ есть на i-ом месте тогда и только тогда, когда ее нет в последовательности $a_0, a_1, a_2, a_3 \dots$ То есть в этом случае $L(f) + L(\widetilde{f}) = n$. В общем же случае, когда среди a_j есть нули, заменим их на любые ненулевые числа. При этом количество перемен знака как в последовательности $a_0, a_1, a_2, a_3 \dots$, так и в последовательности $a_0, -a_1, a_2, -a_3 \dots$ может только возрасти. При этом мы попадем в предыдущий случай. То есть в этом случае $L(f) + L(\widetilde{f}) \leq n$.
С другой стороны $N(f) + N(\widetilde{f}) = n$, так как 0 – не корень. Если $N(f) < L(f)$, то $N(f) + N(\widetilde{f}) < L(f) + L(\widetilde{f}) \leq n$. Противоречие.