1 Поля. Кольца многочленов над полями. Корни многочлена, производная

Определение 1.1 (Многочлен над полем)**.** Пусть P - поле, многочлен над полем P это выражение

$$a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$$

где $a_i \in P$

Теорема 1.2. *Множество многочелнов над полем P $P[x]$ - евклидово кольцо, где норма $\|p\|, p \in P[x]$ - степень многочлена*

Доказательство. Чтобы $P[x]$ было евклидовым по определению **??** оно должно быть ассоциативным, коммутативным кольцом с единицей, что доказывается тривиально. К тому же оно является целостным.

Теперь нужно доказать что степень многочлена является нормой, воспользуемся определением евклидово нормы **??**:

1. Степень многочлена - натуральные числа, поэтому $\|p\| = \deg p \in \omega$
2. Пусть $p(x), q(x) \in P[x]$, где $p(x), q(x) \neq 0$ и $\deg p = n, \deg q = m$. Тогда $\deg pq = n + m$, то есть $\|pq\| \geq \max(\|p\|, \|q\|)$
3. если $p(x) \neq 0$, то для любого $q(x)$ существуют $d(x)$ и $r(x)$ такие что $p(x) = d(x)q(x) + r(x)$ и $\|r\| < \|q\|$ или $r(x) = 0$. Доказательство индукцией по степени $p(x)$:

   Базис: $\deg p < \deg q$. $p(x) = 0 \cdot q(x) + p(x)$

   Индукционный шаг: для всех $\deg p : m = \deg q < \deg p < n$ верно. Показать что верно для $\deg p = n$. Пусть

   $$p(x) = a_0 + a_1 + ...a_n x^n$$

   $$q(x) = b_0 + b_1 + ...b_m x^m$$

   Мы можем отнять от $p(x)$ подходящий многочлен, после которого не останется слагаемого степени n

   $$\begin{aligned} p(x) - q(x) \cdot \frac{a_n}{b_m} x^{n-m} &= a_n x^n + p'(x) - (a_n x^n + \frac{a_n}{b_m} x^{n-m} q'(x)) \\ &= p'(x) - \frac{a_n}{b_m} x^{n-m} q'(x) \end{aligned}$$

Где $p'(x)$ и $q'(x)$ - не производные, это просто обозначение. По индукционному предположению

$$\underbrace{\underbrace{\underbrace{p'(x)}_{<n} - \frac{a_n}{b_m}x^{n-m}\underbrace{q'(x)}_{<m}}_{<n}}_{<n} = d'(x)\cdot q(x) + r(x) \quad \|r\| < \|q\|$$

Так как

$$p(x) - q(x)\cdot\frac{a_n}{b_m}x^{n-m} = d'(x)\cdot q(x) + r(x)$$

то

$$p(x) = q(x)\left(d'(x) + \frac{a_n}{b_m}x^{n-m}\right) + r(x) = q(x)\cdot d(x) + r(x) \quad \|r\| < \|q\|$$

□

Определение 1.3 (Корень многочлена)**.** Корень многочлена $p(x)$ над полем P это такой Элемент поля $a \in P$ что $p(a) = 0$

Теорема 1.4 (Теорема Безу)**.** *Если a - корень многочлена p, то $(x-a)|p(x)$*

Доказательство. Предположим обратное, тогда деление $p(x)$ на $(x-a)$ будет давать остаток

$$p(x) = d(x)(x-a) + r(x)$$

По теореме 1.2 $\|r\| < \|(x-a)\|$, и так как $\|(x-a)\| = 1$, то $\|r\| = 0$, то есть r - константа, следовательно

$$\begin{aligned} p(x) &= d(x)(x-a) + C \\ p(a) &= d(a)(a-a) + C \\ 0 &= 0 + C \end{aligned}$$

Следовательно $C = 0$, $p(x) = d(x)(x-a)$, а это и значит что $(x-a)|p(x)$ □

Определение 1.5 (Корень кратности)**.** a - корень кратности k многочлена $p(x)$, если $(x-a)^k|p(x)$

Определение 1.6 (Производная)**.** Пусть $p(x)$ - многочлен и $p(x) = \sum_{i=0}^{n} a_i x^i$ тогда его производная равна

$$p'(x) = \sum_{i=0}^{n} a_i \underbrace{1+1+\ldots+1}_{i} x^{i-1}$$

Теорема 1.7 (Свойства производных)**.** *Пусть* $p(x), q(x) \in P[x]$*, тогда*

1. $(p+q)' = p' + q'$
2. $(pq)' = p'q + pq'$

Теорема 1.8. *Пусть* $p(x) \in P[x]$, $p(a) = 0$, $k-1 \neq 0$*, тогда* a *является корнем кратности степени* k *тогда и только тогда, когда является корнем кратности степени* $k-1$ *производной этого многочлена.*

Доказательство. 1. Необходимость. Пусть a является корнем кратности степени k, тогда

$$p(x) = (x-a)^k q(x) \quad q(a) \neq 0$$

Найдём производную

$$\begin{aligned} p'(x) &= k(x-a)^{k-1} q(x) + (x-a)^k q'(x) \\ &= (x-a)^{k-1}(kq(x) + (x-a)q'(x)) \\ &= (x-a)^{k-1} S(x) \end{aligned}$$

подставляя в $S(x)$ вместо x a получаем

$$\begin{aligned} S(a) &= kq(a) + (a-a)q'(a) \\ &= kq(a) \\ &= \underbrace{q(a) + ...q(a)}_{k} \\ &= \underbrace{(1 + ... + 1)}_{k} q(a) \end{aligned}$$

Если $k \cdot 1 \neq 0$, то $k \cdot q(a) \neq 0$, следовательно a является корнем произаодной многочлена

$$p'(x) = (x-a)^{k-1} S(x)$$

2. Достаточность. Пусть $p(x) \in P[x]$ и a - корень кратности $k-1$ производной многочлена $p(x)$:

$$p'(x) = (x-a)^{k-1} s(x)$$

тогда

$$p(x) = (x-a)^m q(x) \quad q(a) \neq 0,\ m \geq 1$$

очевидно a является корнем кратности m. Найдём производную

$$\begin{aligned} p'(x) &= m(x-a)^{m-1} + (x-a)^m q'(x) = (x-a)^{k-1} s(x) \\ &= (x-a)^{m-1}(m \cdot q(x) + (x-a)q'(x)) \\ &= (x-a)^{k-1} s(x) \end{aligned}$$

Из этого следует что $m = k$, то есть a является корнем кратности k $\square$