Липсва теоремата за съществуване на всички корени на полином в някакво разширение на полето.

Корени на полином. Кратни корени.

Дефиниция *(корен на полином)*:
Нека $f(x) \in F[x]$ е произволен полином. $\alpha \in F$ наричаме *корен на полинома* $f(x)$, ако е изпълнено, че:

$$f(\alpha) = 0 \quad (1)$$

α е корен на полинома $f(x)$ е равносилно на $x - \alpha \mid f(x)$. (проверява се тривиално с теоремата за деление с частно и остатък).

Дефиниция *(к-кратен корен)*:
Нека $f(x) \in F[x]$ е произволен полином. Казваме, че $\alpha \in F$ е k-кратен корен на полинома $f(x)$, ако е изпълнено, че:

$$\left|\begin{array}{lcl}(x-\alpha)^k & \mid & f(x) \\ (x-\alpha)^{k+1} & \nmid & f(x)\end{array}\right. \quad (2)$$

Производна

Дефиниция *(производна)*:
Нека $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ е произволен полином над $F[x]$. Тогава:

$$f'(x) = a_0nx^{n-1} + a_1(n-1)x^{n-2} + \cdots + a_{n-1} \quad (3)$$

наричаме *производна* на полинома $f(x)$.
Под a_0n разбираме n-кратното на a_0, т.е $\underbrace{a_0 + a_0 + \cdots + a_0}_{n}$.

Свойства

- $(cf(x))' = cf'(x)$
- $(f+g)' = f' + g'$
- $(f.g)' = f'.g + f.g'$

Доказват се тривиално от дефиницията.[1]

Твърдение:
Нека $f(x) \in F[x]$ е произволен полином. Тогава α е кратен корен (т.е поне 2-кратен) т.с.т.к. $f(\alpha) = f'(\alpha) = 0$.
Доказателство:
$|\Rightarrow|$ От $(x-\alpha)^2 \mid f(x)$ следва $f(x) = (x-\alpha)^2g(x)$. Да сметнем производната:

$$f'(x) = (x-\alpha)^2g'(x) + 2(x-\alpha)g(x) = (x-\alpha)((x-\alpha)g'(x) + 2g(x)) \quad (4)$$

Следователно α е корен и на $f'(x)$, т.е $f'(\alpha) = f(\alpha) = 0$.
$|\Leftarrow|$ $f(\alpha) = 0$, следователно $(x-\alpha) \mid f(x)$, т.е $f(x) = (x-\alpha)h(x)$. Да разделим с частно и остатък $h(x)$ на $x-\alpha$:

$$h(x) = (x-\alpha)t(x) + c \quad (5)$$

където c е константа (т.е полином от 0ва степен). Сега да разпишем $f(x)$ след което и $f'(x)$:

$$(6)$$

$$\begin{aligned} f(x) &= (x-\alpha)h(x) \\ &= (x-\alpha)((x-\alpha)t(x)+c) \\ &= (x-\alpha)^2 t(x) + (x-\alpha)c \\ f'(x) &= (x-\alpha)^2 t'(x) + 2(x-\alpha)t(x) + c \end{aligned}$$

Сега заместваме α във $f'(x)$ и получаваме:

$$\begin{aligned} f'(\alpha) &= (\alpha-\alpha)^2 t'(\alpha) + 2(\alpha-\alpha)t(\alpha) + c \\ &= 0^2 t'(\alpha) + 2.0t(\alpha) + c \\ &= c \end{aligned} \tag{7}$$

Но по условие $f'(\alpha) = 0$, следователно $c = 0$, т.е $h(x)$ се дели точно на $x - \alpha$, и от тук $(x-\alpha)^2 \mid f(x)$.

Формули на Виет

Ще напишем формули, които свързват корените на даден полином с неговите коефициенти.

Теорема *(Формули на Виет)*:
Нека $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$ е произволен полином от $F[x]$.
Нека $\beta_1, \beta_2, \cdots, \beta_n$ са всичките му корени в някакво разширение $K \supset F$. Тогава:

$$\begin{aligned} \sum_i \beta_i &= \beta_1 + \beta_2 + \cdots + \beta_n &= -\frac{a_1}{a_0} \\ \sum_{i<j} \beta_i\beta_j &= \beta_1\beta_2 + \beta_1\beta_3 + \cdots + \beta_1\beta_n + \beta_2\beta_3 + \cdots + \beta_{n-1}\beta_n &= \frac{a_2}{a_0} \\ &\vdots \\ \prod_i \beta_i &= \beta_1\beta_2\cdots\beta_n &= (-1)^n \frac{a_n}{a_0} \end{aligned} \tag{8}$$

Доказателство:
Полиномът $f(x)$ може да бъде разложен по следния начин в разширението $K \supset F$, в което се намират всичките му корени:

$$f(x) = a_0(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n) \tag{9}$$

Сега ще разкрием скобите:

$$
\begin{aligned}
f(x) &= a_0(x-\beta_1)(x-\beta_2)\cdots(x-\beta_n) \\
&= a_0x^n \\
&+ a_0x^{n-1}(-1)(\beta_1+\beta_2+\cdots+\beta_n) \\
&+ a_0x^{n-2}(+1)(\beta_1\beta_2+\cdots+\beta_{n-1}\beta_n) \\
&\vdots \\
&+ a_0(-1)^n(\beta_1\beta_2\cdots\beta_n)
\end{aligned} \tag{10}
$$

Сега просто използваме, че коефициентите на 2 полинома, които са еднакви (в нашия случай - написани по 2 различни начина) съвпадат, т.е коефициентът пред дадена степен в едното представяне е равен на коефициентът пред същата степен в другото представяне.
С това теоремата е доказана!

Забележка: Който не знае Формулите на Виет няма да мине Алгебра 2[2]

Съществуване на поле на разлагане

Теорема 1

Нека f е F[x], deg f > 0, I = (f). Тогава факторпръстенът F[x]/I е поле <=> полиномът f е неразложим над F.

Доказателство:
$|\Rightarrow|$ Нека F[x]/I е поле. Да допуснем, че f = gh g, h e F[x], deg g, deg h < deg f. Тогава f !/ g, f !/ h -> g,h !e I. Тоест f и g са ненулеви елементи от F[x]/I. От друга страна, равенството f = gh в пръстена F[x] => 0(cherta) = f(cherta) = g(cherta)h(cherta) в полето F[x]/I, което е противоречие с липсата на делители на нулата в поле => f е неразложим над F.
$|\Leftarrow|$ f е неразложим над F и 0(cherta) != g(cherta) e F[x]/I, където g е F[x]. Тогава g !e I, тоест f !/ g. Тъй като f е неразложим полином, то (f, g) = 1. Тогава съществуват полиноми u, v e F[x] : uf + vg = 1. Оттук получаваме равенството: uf + vg = 1 (всяко едно с чертичка) в пръстена F[x]/I. Като вземем предвид, че f(cherta) = 0(cherta), получаваме vg = 1 (с чертички отново) => g е обратим елемент(v(cherta)). Така всеки ненулев елемент на пръстена F[x]/I е обратим, което означава, че F[x]/I е поле.

Теорема 2

Нека f e F[x], deg f > 0. Тогава съществува разширение K на полето F, в което полиномът f има корен.
Доказателство:
Полиномът f се разлага в произведение на неразложими над F множители. Ако намерим разширение на F, в което един от тези множители има корен, то той ще бъде корен и на f. БОО можем да считаме, че полиномът f е неразложим над F.

Нека $I = (f)$ и $K = F[x]/I$.
Според Теорема 1 K е поле. Нека $\varphi : F[x] \to K$ е естественият хомоморфизъм, т.е $\varphi(g) = \bar{g} = g + I \in K$.
Нека $\bar{\varphi}$ е ограничението на φ върху F, т.е $\bar{\varphi} : F \to K$ е хомоморфизъм и $\bar{\varphi}(a) = \varphi(a) = \bar{a} \quad a \in F$.
Очевидно $\operatorname{Ker} \bar{\varphi} \neq F$, също така $\operatorname{Ker} \bar{\varphi} \lhd F$, а полето F няма нетривиални идеали, следователно $\operatorname{Ker} \bar{\varphi} = \{0\}$. Нека $F_0 = \operatorname{Im} \bar{\varphi}$. От Теоремата за Хомоморфизмите имаме, че $F / \operatorname{Ker} \bar{\varphi} \cong F_0$. Следователно $F \cong F_0$. Благодарение на този изоморфизъм считаме, че $F \leq K$. Тъй като $f \in F[x]$, в частност имаме $f \in K[x]$.
Ако $\bar{a} \in F$ следователно $\bar{a} = a$.
Тогава

$$\begin{aligned} f &= a_0 x^n + a_1 x^{n-1} + \dots + a_n \\ &= \overline{a_0}\,\overline{x}^n + \overline{a_1}\,\overline{x}^{n-1} + \dots + \overline{a_n} \\ &= \overline{a_0 x^n + a_1 x^{n-1} + \dots + a_n} \\ &= \bar{f} \\ &= \bar{0} \\ &= 0 \end{aligned} \tag{11}$$

Така полето K е разширение на полето F и a е K е корен на полинома $f \in F[x]$.

Теорема 3

Нека f e F[x], deg f = n > 0. Тогава съществува разширение L на полето F, над което f се разлага в произведение на линейни множители, т.е. всички корени на ф са в това разширение.

Доказателство:
Нека K1 е разширение на F, в което f има корен a1.
Тогава от (K - комутативен пръстен с 1 f e F[x] и a e K. Тогава f(a) = 0 когато f = (x - a)q за някой полином q от F[x]) => f = (x - a1)f1, f1 e K1[x], degf1 = n - 1. Ако degf1 > 0 K2 е разширение на K1, в което f има корен a2 => f1 = (x - a2)f2, deg f2 = n - 2 и т.н.След n стъпки f - разложен на линейни множители в последното разширение Kn = L на полето F. Елементите a1, a2, .., an на L са корени на f, а fn - старшия коефициент..

ако някой не разбира нещо по последните 3 теореми - " Записки по Алгебра групи, пръстени, полиноми " -> стр. 40/41

Footnotes

1. или може би не чак толкова - на който му е безумно интересно може да пробва и да разкаже после
2. каза Великова. Ако щете вярвайте :)