Корени на полиномите. Формули на Виет. Кратни корени.

Нека F е поле, $f(x) \in F[x]$ е такъв полином, че $\deg f \geq 1$. Интересува ни дали съществува разширение K на F, съдържащо елемент $\alpha \in K$, такъв че $f(\alpha) = 0$. Такъв елемент α се нариа *корен* или *нула* на полинома $f(x)$.

Твърдение 1 (Безу). *Нека K е поле, $f(x) \in K[x]$ и $\alpha \in K$. Тогава $f(\alpha) = 0 \iff x - \alpha$ дели $f(x)$.*

Доказателство. Според теоремата за деление на полиноми с частно и остатък съществуват $q(x), r(x) \in K[x]$, такива че

$$(*) \quad f(x) = (x - \alpha)q(x) + r(x)$$

и $\deg r < \deg(x - \alpha) = 1$. Последното означава, че или $\deg r = 0$ и $r \in K \backslash \{0\}$, или $\deg r = -\infty$ и $r = 0$. И в двата случая $r \in K$. Замествайки $x = \alpha$ в равенство $(*)$, получаваме, че $f(\alpha) = r$. Сега вече α е корен на $f(x) \iff r = 0 \iff f(x) = (x - \alpha)q(x) \iff (x - \alpha) \mid f(x)$. $\square$

Както видяхме досега, пръстенът на целите числа и пръстенът на полиномите над поле много си приличат. Знаем, че в $\mathbb{Z}$ всеки идеал има вида $m\mathbb{Z} = \{mz \mid z \in \mathbb{Z}\}$ за $m = 0, 1, \ldots$. При $m \geq 2$ имаме, че факторпръстенът $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ е поле, тогава и само тогава, когато m е просто число. След малко ще видим аналогичен резултат в полиномиален пръстен над поле. Както вече видяхме според теоремата за разлгане на полиноми в произведение на неразложими, неразложимите полиноми изпълняват подобна на ролята на простите числа в пръстена $\mathbb{Z}$. Всичко това ни кара да очакваме, че е вярна следната

Теорема. *Нека F е поле, $p(x) \in F[x]$ и $I = (p)$ е главният идеал в полиномиалния пръстен, породен от p. Нека $\deg p \geq 1$. Тогава факторпръстенът $F[x]/I$ е поле, точно когато $p(x)$ е неразложим над F полином.*

Доказателство. Нека $K = F[x]/I = \{g(x) + I \mid g(x) \in F[x]\}$. Ясно е, че K е комутативен пръстен с единичен елемент $1 + I$.

Необходимост: нека K е поле. Тогава всеки ненулев негов елемент е обратим. Да допуснем, че полиномът p е разложим. Това означава, че $\exists g(x), h(x) \in F[x]$, такива че $p(x) = g(x)h(x)$ и $\deg g, \deg h < \deg p$. От $\deg g < \deg p$ следва, че $p \nmid g$ и следователно $g \notin I$, т.е. $g + I \neq I$. Поради същите причини и $h + I \neq I$. Така $g + I$ и $h + I$ са ненулвеи елементи на K. Същевременно обаче имаме, че $(g + I) \cdot (h + I) = gh + I = p + I = I$, защото $p \in I$. Това означава, че $g + I$ и $h + I$ са делители на нулата в K и K няма как да е поле. Противоречието доказва, че p трябва да е неразложим полином.

Достатъчност: нека $p(x)$ е неразложим над F полином. Нека $g + I \in K (g \in F[x])$ е ненулев елемент, т.е. $g+I \neq I$, което означава $q \notin I$. В такъв случай $p \nmid g$ и в комбинация с факта, че p е неразложим, получаваме, че $(p, g) = 1$. За тях е изпълнено тъждеството на Безу $up + vg = 1$ за пододящи полиноми $u(x), v(x) \in F[x]$. Т.к. $up \in (p) = I$, то получаваме $(v + I) \cdot (g + I) = vg + I = vg + (up + I) = up + vg + I = 1 + I$. С други думи произволен елемент $g + I \in K$ е обратим с $(g + I)^{-1} = v + I$. Така K е поле. □

Следващата теорема излагаме без доказателство.

Теорема 2. *Нека F е поле, а $f \in F[x]$ е полином с $\deg f \geq 1$. Тогава съществува разширение $K \geq F$ и елемент $\alpha \in K$, такъв че $f(\alpha) = 0$ (т.е. $f(x)$ има поне един корен в K).*

Следствие 1. *Нека F е поле, $f(x) \in F[x]$ е такъв, че $\deg f = n \geq 1$ и има старши коефициент a_0. Тогава съществува разширение L на F и елементи $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, които не са непременно различни, такива че*

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n).$$

Доказателство. Според Теорема 2 съществува разширение $K_1 \geq F$ и елемент $\alpha_1 \in K_1$, такъв че $f(\alpha_1) = 0$. Сега, според Твърдение 1 $(x - \alpha_1) \mid f(x)$, т.е. $f(x) = (x - \alpha_1)f_1(x)$, където $f_1(x) \in K_1[x]$. Ако $\deg f_1 \geq 1$, то съществува разширение $K_2 \geq K_1 (\geq F)$, и елемент $\alpha_2 \in K_2$, такъв че

$f_1(\alpha_2) = 0$. Тогава $(x - \alpha_2) \mid f_1(x)$, т.е. $f_1(x) = (x - \alpha_2)f_2(x)$, където $f_2(x) \in K_2[x]$. Дотук $f(x) = (x - \alpha_1)(x - \alpha_2)f_2(x)$. Продължавайки по същия начин, след n стъпки намираме разширение $K_n \geq K_{n-1}$ и елемент $\alpha_n \in K_n$, такива че $f(x) = (x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)f_n(x)$, където $f_n(x) \in K_n[x]$. Т.к. на всяка стъпка степента $\deg f_i$ е с i по-малка от $\deg f = n$, то $\deg f_n = 0$ или с други думи $f_n \in K_n$ е константа. Сега от принципа за сравняване на коефициентите директно следва, че $f_n = a_0$. Полагаме $L = K_n$ и $\alpha_1, \alpha_2, \dots, \alpha_n \in L$, а

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n).$$

□

Нека L_0 е сечението на всички подполета на L, съдържащи едновременно F и елементите $\alpha_1, \alpha_2, \dots, \alpha_n$. Ясно е, че така L_0 е най-малкото подполе, което ги съдържа. То се нарича *поле на разлагане на полинома $f(x)$ над F*. В сила е, че всеки две полета на разлагане на полином $f(x) \in F[x]$ над F са изоморфни.

Да разгледаме полиномът над поле F

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in F[x]$$

с ненулев старши коефициент $a_0 \neq 0$ и степен $\deg f = n \geq 1$. Нека $\alpha_1, \alpha_2, \dots, \alpha_n$ са всички корени на $f(x)$, лещажи в някакво разширение $K \geq F$. Следстиве 1 ни дава, че

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n).$$

Използваме принципа за сравняване на коефициентите:

$$\begin{aligned}
x^n: &\quad a_0 = a_0;\\
x^{n-1}: &\quad a_1 = a_0(-\alpha_1 - \alpha_2 - \dots - \alpha_n);\\
x^{n-2}: &\quad a_2 = a_0(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n);\\
&\dots\\
x^0: &\quad a_n = a_0(-\alpha_1)(-\alpha_2)\dots(-\alpha_n),
\end{aligned}$$

което ни дава следните връзки между корените на $f(x)$ и неговите коефициенти:

$$\begin{aligned}
\alpha_1 + \alpha_2 + \cdots + \alpha_n &= -\frac{a_1}{a_0}, \\
\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n &= \frac{a_2}{a_0}, \\
&\dots \\
\alpha_1\alpha_2 \dots \alpha_n &= (-1)^n \cdot \frac{a_n}{a_0}.
\end{aligned}$$

Тези равенства се наричат *формули на Виет.* Те са n на брой и ги записваме накратко така

$$\sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \alpha_{i_1}\alpha_{i_2} \dots \alpha_{i_k} = (-1)^k \cdot \frac{a_k}{a_0}$$

за $k = 1, 2, \dots, n$.

Нека $f(x) \in F[x]$ е полином над полето F от степен $\deg f = n \geq 1$. Нека α е корен на $f(x)$ $(\alpha \in K \geq F)$. Казваме, че α е *k-кратен корен на* f, ако $(x-\alpha)^k \mid f(x)$, но $(x-\alpha)^{k+1} \nmid f(x)$ (делимостта е в $K[x]$). Ясно е, че $k \in \mathbb{N}$ като $1 \leq k \leq n$. Ако $k \geq 2$, казваме, че α е кратен корен, а ако $k = 1$, казваме че α е прост корен.

Нека $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in F[x]$. Полиномът

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + 2a_{n-2}x + a_{n-1} \in F[x]$$

се нарича *производна на полинома* f. Ако $\operatorname{char} F = 0$, то $na_0 \neq 0$ и $\deg f' = n - 1$. Ако $\operatorname{char} f = p$ за някое просто число p, то в случай, че $p \mid n$ имаме $na_0 = 0$ и тогава $\deg f' < n - 1$.

<u>Свойства:</u>
1. $(f(x) + g(x))' = f'(x) + g'(x)$,
2. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

За $k \in \mathbb{N}, k \geq 2$ дефинираме k-та производна на $f(x)$ като $f^{(k)}(x) = \left(f^{(k-1)}(x)\right)'$.

Забележка 1: НОД на два полинома не се променя при разширение на полето F. Наистина, нека $f, g \in F[x]$, и $d \in F[x]$ е такъв, че $d = (f, g)$. Нека $K \geq F$ е разширение на F и в пръстена $K[x]$ НОД на f и g е полиномът $d_1 \in K[x]$. Ако разглеждаме d като полином от $K[x]$, то веднага получаваме, че $d \mid d_1$. Освен това от тъждеството на Безу съществуват полиноми $u, v \in F[x]$, такива че $uf + vg = d$. Понеже $d_1 \mid f$ и $d_1 \mid g$, то d_1 дели цялата лява страна на тъждеството. Това означава, че d_1 дели и дясната страна, т.е. $d_1 \mid d$. Така $d_1 = d$. (Равенството се достига благодарение на уговорката за еднозначност на НОД.)

Забележка 2: Полиномите $f, g \in F[x]$ не са взаимно прости $\iff$ f и g имат общ корен (в някакво разширение $K \geq F$). Необходимост: нека $(f, g) = d \neq 1$, т.е. $\deg d \geq 1$. Тогава съществува разширение $K \geq F$ и елемент $\alpha \in K$, който анулира d, т.е. $d(\alpha) = 0$. Но $d \mid f$ и $d \mid g$ и оттук следва, че $f(\alpha) = 0$ и $g(\alpha) = 0$, т.е. α е общ корен за f и g. Достатъчност: нека f и g имат общ корен $\alpha \in K \geq F$. В $K[x]$ е изпълнено, че $(x - \alpha) \mid f$ и $(x\alpha) \mid g$. Оттук следва, че ако $d \in K[x]$ е НОД на f и g, то $(x - \alpha) \mid d$. Според Забележка 1 d се запазва и като НОД на f и g в $F[x]$, което означава, че $\deg d \geq 1$ и оттук $(f, g) = d \neq 1$.

Забележка 3: Ако f и g имат общ корен и g е неразложим над F, то $g \mid f$. Наистина, според Забележка 2 имаме, че $(f, g) \neq 1$, но g е неразложим и тогава $g \mid f$.

Твърдение 2. *Полиномът $f(x) \in F[x]$ има кратен корен $\iff$ $f(x)$ има общ корен с производната си $f'(x)$.*

Доказателство. Нека $K \geq F$ и $\alpha \in K$. Делим $f(x)$ на $(x - \alpha)^2$ с частно и остатък, т.е.

$$f(x) = (x - \alpha)^2 q(x) + r(x)$$

за $q(x), r(x) \in K[x]$ и $\deg r < \deg(x - \alpha)^2 = 2$. Това означава, че $r(x)$ е полином от вида

$$r(x) = ax + b$$

за $a, b \in K$ и така достигаме до

$$f(x) = (x - \alpha)^2 q(x) + ax + b.$$

При $x = \alpha$ получаваме $f(\alpha) = a\alpha + b$. Нека сега да разгледаме производната на полинома

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) + a.$$

При $x = \alpha$ нейната стойност е $f'(\alpha) = a$, с което определихме старшия коефициент на $r(x)$. Сега $b = f(\alpha) - a\alpha = f(\alpha) - \alpha f'(\alpha)$, което напълно определя полинома $r(x) = ax + b$ при произволен елемент $\alpha \in K$. Сега имаме, че някое $\alpha \in K$ е кратен корен на $f(x) \iff (x-\alpha)^2 \mid f \iff r(x) = 0 \iff a = b = 0 \iff f(\alpha) = 0$ и $f'\alpha) = 0$. $\square$

Твърдение 3. *Нека F е поле с характеристика $\operatorname{char} F = 0$, $f(x) \in F[x]$, а α е елемент от разщирението $K \geq F$. Ако α е k-кратен ($k \geq 1$) корен на $f(x)$, то α е $(k-1)$-кратен корен на $f'(x)$, α е $(k-2)$-кратен корен на $f''(x)$,...,α е прост корен на $f^{(k-1)}(x)$ и α не е корен на $f^{(k)}(x)$.*

Доказателство. Достатъчно е да докажем за $f'(x)$. Останалото влиза в сила според правилото $f^{(k)}(x) = \left(f^{(k-1)}(x)\right)'$. И така, нека α е k-кратен корен на $f(x)$. Това означава, че $(x-\alpha)^k \mid f$ и $(x-\alpha)^{k+1} \nmid f$. Оттук $f(x) = (x-\alpha)^k g(x)$ за $g(x) \in K[x]$ и $(x-\alpha) \nmid g$, т.е. α не е корен на g. Имаме, че $\operatorname{char} K = \operatorname{char} F = 0$ и следователно $f'(x) = k(x-\alpha)^{k-1}g(x) + (x-\alpha)^k g'(x) = (x-\alpha)^{k-1}\left(kg(x) + (x-\alpha)g'(x)\right)$. Означаваме $h(x) = kg(x) + (x-\alpha)g'(x) \in K[x]$ и по този начин $f'(x) = (x-\alpha)^{k-1}h(x)$. Имаме, че $(\alpha) = kg(\alpha)$ като $g(\alpha) \in K\backslash\{0\}$, $k \in \mathbb{N}$ и $\operatorname{char} K = 0$ и следователно $kg(\alpha) \neq 0$, т.е. $h(\alpha) \neq 0$ и α не е корен на $h(x)$. Ако $k = 1$, то $f'(x) = h(x)$ и $f'(\alpha) = h(\alpha) \neq 0$. Това означава, че ако α е прост корен на $f(x)$, тоα не е корен на $f'(x)$. Нека сега $k \geq 2$. Тогава $f'(x) = (x-\alpha)^{k-1}h(x)$ и $(x-\alpha)^{k-1} \mid f'(x)$. От друга страна $(x-\alpha) \nmid h(x)$, защото α не е корен на $h(x)$ и следователно е изпълнено също и че $(x-\alpha)^{k-1} \nmid h(x)$. Това означава, че α е $(k-1)$-кратен корен на $f'(x)$ и теоремата е доказана. $\square$

Следствие 2. *Нека $f(x) \in F[x]$ е полином над полето F, което има характеристика $\operatorname{char} F = 0$. Елементът α на разширението $K \geq F$ е k-кратен корен на $f(x) \iff$ изпълнени са условията*

$$(*) \quad f(\alpha) = f'(\alpha) = \cdots = f^{(k-1)}(\alpha) = 0 \text{ и } f^{(k)}(\alpha) \neq 0.$$

Доказателство. $\Rightarrow$) Нека α е k-кратен корен на $f(x)$. Тогава от Твърдение 3 следва, че $f(\alpha) = f'(\alpha) = \cdots = f^{(k-1)}(\alpha) = 0$ и $f^{(k)}(\alpha) \neq 0$.

$\Leftarrow$) Нека са изпълнени условията $(*)$ и нека l е кратността на α като корен на $f(x)$. От Твърдение 3 имаме, че $f(\alpha) = f'(\alpha) = \cdots = f^{(l-1)}(\alpha) = 0$ и $f^{(l)}(\alpha) \neq 0$. Щом са изпълнени условията $(*)$, значи $l = k$ и α е k-кратен корен на $f(x)$. $\square$

Пример:
Да се намерикратността k на числото $\alpha = 1$ като корен на полинома

$$f(x) = x^5 - 5x^3 + 5x^2 - 1 \in \mathbb{Q}[x].$$

Имаме, че $f(1) = 1 - 5 + 5 - 1 = 0$ и следователно $\alpha = 1$ е корен на $f(x)$. Производната на $f(x)$ е

$$f'(x) = 5x^4 - 15x^2 + 10x.$$

Имаме, че $f'(1) = 5-15+10 = 0$ и следователно дотук 1 е поне двукратен корен. Втората производна е

$$f''(x) = 20x^3 - 30x + 10.$$

Имаме, че $f''(1) = 20 - 30 + 10 = 0$ и по този начин 1 е поне трикратен корен на $f(x)$. Третата прозиводна е

$$f'''(x) = 60x^2 - 30.$$

Имаме, че $f'''(1) = 60-30 = 30 \neq 0$ и 1 не е неин корен. Така окончателно получихме, че $\alpha = 1$ е трикратен корен на $f(x)$.