ЛЕКЦИЯ 14
КАНОНИЧНО РАЗЛАГАНЕ. КРАТНИ КОРЕНИ. ФОРМУЛИ НА ВИЕТ

Определение. *Казваме, че полиномът от n-та степен $f(x)$ е унитарен, ако коефициентът пред n-тата степен на x е равен на единица, т. е. $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$.*

Нека
$$f(x) = f_1(x) \dots f_k(x)$$
е разлагане на $f(x)$ на неразложими полиноми над полето F. Ако A_i е коефициентът пред най-високата степен на $f_i(x)$ тогава имаме $f_i(x) = A_i\varphi_i(x)$, където $\varphi_i(x)$ е неразложим и унитарен полином. От първоначалното разлагане получаваме

$$f(x) = A\varphi_1(x) \dots \varphi_k(x), \text{ където } A = A_1 \dots A_k \tag{1}$$

Следователно всеки полином може да се представи като произведение на константа и неразложими унитарни полиноми. Това представяне е единствено в буквален смисъл. Наистина ако освен (1) е изпълнено и

$$f(x) = B\psi_1(x) \dots \psi_s(x), \tag{2}$$

където $\psi_i(x)$ са неразложими над F и унитарни полиноми. Като сравним коефициентите пред най-високата степен на x от (1) и (2), получаваме $A = B$ и
$$\frac{1}{A}\,f(x) = \varphi_1(x) \dots \varphi_k(x) = \psi_1(x) \dots \psi_s(x).$$
От Теорема 1 следва $k = s$ и след преномериране $\varphi_i(x) = c_i\psi_i(x)$. Понеже $\varphi_i(x)$ и $\psi_i(x)$ са унитарни следва $c_i = 1$, с което единствеността е доказана.

В (1) може да има повтарящи се множители. Като групираме повтарящите се множители се получава

$$f(x) = A(\varphi_1(x))^{l_1} \dots (\varphi_t(x))^{l_t}, \tag{3}$$

където $\varphi_i(x)$, $i = 1, \dots, t$ са неразложими над F унитарни и различни полиноми. Равенството (3) се нарича *канонично разлагане* на $f(x)$. Тъй като разлагането (1) е единствено в буквален смисъл, каноничното разлагане (3) също е единствено в буквален смисъл.

Забележка. *Каноничното разлагане на даден полином зависи от основното поле, тъй като над някое разширение на основното поле е възможно някои от полиномите в (3) да се разложи.*

Като отделим в (3) множителите от първа степен (ако има такива) получаваме

$$f(x) = A(x-\alpha_1)^{l_1} \dots (x-\alpha_s)^{l_s} (\varphi_{s+1}(x))^{l_{s+1}} \dots (\varphi_t(x))^{l_t}, \tag{4}$$

където ст. $\varphi_i(x) \geq 2$, $i = s+1, \dots, t$.

От (4) става ясно, че $\alpha_1, \dots, \alpha_s$ са корени на $f(x)$ в основното поле F. Освен $\alpha_1, \dots, \alpha_s$ $f(x)$ няма други корени в F. Наистина, ако $\beta \in F$ е корен на $f(x)$, тогава имаме

$$f(\beta) = A(\beta-\alpha_1)^{l_1} \dots (\beta-\alpha_s)^{l_s} (\varphi_{s+1}(\beta))^{l_{s+1}} \dots (\varphi_t(\beta))^{l_t} = 0$$

Съгласно Твърдение 5 от Лекция 12, $\varphi_i(\beta) \neq 0$, $i = s+1, \dots, t$. Понеже няма делители на нулата за някое i трябва $\beta = \alpha_i$.

Определение. *Нека k е естествено число. Казваме, че $\alpha \in F$ е k-кратен корен на $f(x) \in F[x]$, ако $f(x)$ се дели на $(x-\alpha)^k$, но $f(x)$ не се дели на $(x-\alpha)^{k+1}$.*

Корените, които имат кратност единица се наричат *прости* корени, т. е. α е прост корен на $f(x)$, ако $f(x)$ се дели на $(x-\alpha)$, но не се дели на $(x-\alpha)^2$.

От (4) става ясно, че коренът α_i има кратност по-голяма или равна на l_i. От единствеността на каноничния вид следва, че $f(x)$ не се дели на $(x-\alpha_i)^{l_i+1}$ и следователно α_i има кратност точно l_i.

От (4) имаме

$$l_1 + l_2 + \dots + l_s \leq \text{ст.}\, f(x) \tag{5}$$

От неравенството (5) става ясно, че е вярна следната

Теорема 1. *Нека F е поле и $f(x) \in F[x]$ е ненулев полином. Тогава броят на корените на $f(x)$ в полето F, като всеки корен се брои толкова пъти колкото е неговата кратност, не надминава неговата степен.*

Тази теорема обобщава доказано по-рано твърдение, според което броят на различните корени на един полином над дадено поле не надминава неговата степен. Ще отбележим, че равенство в (5) се достига само когато в каноничното разлагане (4) участват единствено неразложими полиноми от първа степен, т. е. когато в (4) имаме $s = t$.

Определение. *Нека е даден полинома*

$$f(x) = a_0 + a_1x + \cdots + a_nx^n.$$

Полиномът

$$f'(x) \stackrel{\text{def}}{=} 0 + a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1}$$

се нарича формална производна на полинома $f(x)$.

Лесно се проверява, че за формалната производна са изпълнени следните обичайни равенства за производна на функция:

$$(f+g)' = f' + g'$$
$$(fg)' = f'g + fg'$$

Твърдение. *Нека F е поле. Елементът $\alpha \in F$ е корен с кратност по-голяма или равна на 2 на ненулевия полином $f(x) \in F[x]$ тогава и само тогава, когато*

$$f(\alpha) = f'(\alpha) = 0.$$

Доказателство:

1) Нека α е корен с кратност по-голяма или равна на 2. Тогава $f(x) = (x-\alpha)^2 g(x)$. Поради това

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

Следователно $f(\alpha) = f'(\alpha) = 0$.

2) нека $f(\alpha) = f'(\alpha) = 0$. От $f(\alpha) = 0$ имаме

$$f(x) = (x-\alpha)g(x) \tag{6}$$

От това равенство получаваме

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

Понеже $f'(\alpha) = 0$, получаваме $g(\alpha) = 0$ и $g(x) = (x - \alpha)t(x)$. Като заместим в (6), получаваме

$$f(x) = (x - \alpha)^2 t(x).$$

Следователно α е корен на $f(x)$ с кратност поне 2.

Ако α е корен на $f(x)$ с кратност по-голяма или равна на k, тогава $f(x) = (x - \alpha)^k g(x)$. От това равенство лесно следва

$$f(\alpha) = f'(\alpha) = \cdots = f^{(k-1)}(\alpha) = 0.$$

Следователно тези равенства са необходимо условие коренът α да има кратност поне k. При $k \geq 3$ това условие не е достатъчно. Ако полето F е числово това условие обаче е необходимо и достатъчно.

Формули на Виет

Нека F е поле и $f(x) \in F[x]$

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad a_n \neq 0 \tag{1}$$

Нека E е разширение на полето F над което $f(x)$ се разлага на линейни множители:

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n). \tag{2}$$

Това, че (2) е разлагане над E означава, че коефициентите на множителите принадлежат на E, т. е. $\alpha_1, \ldots, \alpha_n \in E$.

Съществуването на полето E ще докажем в следващите лекции. Като сравним коефициентите на $f(x)$ в равенствата (1) и (2) получаваме:

$$\begin{aligned}
&\alpha_1 + \cdots + \alpha_n = -\frac{a_{n-1}}{a_n} \\
&\alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n} \\
&\alpha_1\alpha_2\alpha_3 + \cdots + \alpha_{n-2}\alpha_{n-1}\alpha_n = -\frac{a_{n-3}}{a_n} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\alpha_1\alpha_2\ldots\alpha_{n-1} + \cdots + \alpha_2\ldots\alpha_{n-1}\alpha_n = (-1)^{n-1}\frac{a_1}{a_n} \\
&\alpha_1\alpha_2\ldots\alpha_n = (-1)^n\frac{a_0}{a_n}
\end{aligned}$$

Получените равенства се наричат формули на Виет. От тези формули става ясно, че макар корените $\alpha_1, \ldots, \alpha_n$ да са от разширението E, имаме $\alpha_1 + \cdots + \alpha_n \in F$, $\alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n \in F$, $\ldots$, $\alpha_1\alpha_2\ldots\alpha_n \in F$.