Разлагане на полиномите в произведение на неразложими множители

Ще не е необходима следната:

Лема:
Във всеки пръстен може да се съкращава на множител, който не е делител на нулата.

Д-во:
Нека a.b = a.c и а не е делител на нулата тогава a(b – c) = 0. Понеже а не е делител на нулата следва b – c = 0, т.е. b = c

Теорема:
Нека F *е поле. Тогава всеки неконстантен полином над* F *може да се представи като произведение на неразложими над* F *полиноми. С точност до константен множители това разлогане е единствено.*

Забележка:
Ако полиномът е неразложим ще считаме, че той е произведение на един неразложим множител. Поради това за неразложими полиноми теоремата е изпълнена.

Д-во:
1. Съществуване
Индукция по степента на f(x), ст.f(x) = n
База n = 1. От ст.f(x) = 1 следва,че f(x) е неразложим над F и съществуването на разлагането е очевидно.
Нека $n \geq 2$
Ако f(x) е неразложим над F, съществуването на такъва разлагане е ясно.
Нека f(x) е разложим над F, т.е.

$$f(x) = f_1(x).\ f_2(x), \text{ където } f_i(x) \in F[x],\ i = 1,2 \text{ и ст.} f_i(x) \geq 1. \qquad (*)$$

От ст.$f_1(x) \geq 1$ и ст.$f_2(x) \geq 2 \Rightarrow$ ст.$f(x) < n$ и ст.$f_2(x) < n$
За $f_1(x)$ и $f_2(x)$ можем да приложим индуктивната хипотеза $\Rightarrow$ $f_1(x)$ и $f_2(x)$ се разлагат в произведение на неразложими над F полиноми. Като заместим в (*) тези разлагания за $f_1(x)$ и $f_2(x)$ се получава желаното разлагане на f(x).
2. Единственост
Нека

$$f(x) = f_1(x) \ldots f_k(x) = g_1(x) \ldots g_s(x), \qquad (\#)$$

където $f_i(x)$ и $g_j(x)$ са неразложими над F. Трябва да се докаже, че k = s и че след евентуално преномериране на полиномите имаме $f_i(x) = c_i.g_i(x)$, i = 1, . . , k

От (#) $\Rightarrow$ $f_1(x)$ дели $g_1(x)g_2(x) \ldots g_s(x)$. Понеже f(x) е неразложим от Твърдение 3 следва, че $f_1(x)$ дели някой от $g_1(x)$, $g_2(x)$, . . . , $g_s(x)$. След евентуално преномериране на $g_1(x)$, $g_2(x)$, . . ., $g_s(x)$ ще имаме, че $f_1(x)$ дели $g_1(x)$. Но $f_1(x)$ и $g_1(x)$ са неразложими над F. Поради това от Твърдение 2 следва c_1. $f_1(x) = g_1(x)$. Заместваме в (#) и получаваме

$$f_1(x) \ldots f_k(x) = c_1 f_1(x) g_2(x) \ldots g_s(x).$$

Съгласно Лемата можем да съкратим на $f_1(x)$ и получаваме

$$f_2(x) \ldots f_k(x) = g_2(x) \ldots g_s(x) \qquad (\#\#)$$

От (##) следва, че $f_2(x)$ дели $c_1 f_1(x) g_2(x) \ldots g_s(x)$. След евентуално преномериране се получава, че $f_2(x)$ дели $g_2(x)$. Понеже $f_2(x)$ и $g_2(x)$ са неразложими от Твърдение 2 имаме c_2. $f_2(x) = g_2(x)$. Заместваме в (##) и съкращаваме на $f_2(x)$ и т.н. Не е възможно k < s, защото като приложим тази процедура няколко пъти ще получим отляво константа, а отдясно полином, който не е константа.

Не е възможно k > s по аналогични съображения. Следователно k = s. На всеки етап имаме $g_i(x) = c_i.f_i(x)$.
С това единствеността е доказана□

Канонично разлагане

Определение:

Казваме, че ненулевият полином f(x) *е унитарен, ако коефициента пред най-високата степен е равен на единица, т.е.* $f(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + x^n$

Нека $f(x) = f_1(x) \ldots f_к(x)$ е разлагане 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

$$f(x) = A\,\varphi_1(x) \ldots \varphi_к(x) \text{ , където } A = A_1....A_к \qquad (1)$$

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

$$f(x) = B\varphi_1(x) \ldots \varphi_s(x) \qquad (2)$$

От (1) и (2) следва A=B и

$$(1/A)f(x) = \varphi_1(x) \ldots \varphi_к(x) = \psi_1(x) \ldots \psi_s(x)$$

От Теоремата следва к = 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

$$f(x) = A(\varphi_1(x))^{l_1} \ldots (\varphi_t(x))^{lt} \qquad (3)$$

, където $\varphi_i(x)$ са неразложими 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. Като отделим в (3) множителите от първа степен (ако има такива) получаваме

$$f(x) = (x - \alpha_1)^{l_1} \ldots (x - \alpha_s)^{ls}(\varphi_{s+1}(x))^{ls+1} \ldots (\varphi_t(x))^{lt} \qquad (4)$$

, където $ст.\varphi_i(x) \geq 2$, $i = s+1, \ldots, t$
От (4) става ясно, че $\alpha_1 \ldots \alpha_s$ са корени на f(x) в основното поле F
Освен $\alpha_1 \ldots \alpha_s$ f(x) няма други корени в F. Наистина ако $\beta \neq \alpha_i$, $i = 1, \ldots, s$ е корен имаме

$$f(\beta) = (\beta - \alpha_1)^{l1} \ldots (\beta - \alpha_s)^{ls}(\varphi_{s+1}(\beta))^{ls+1} \ldots (\varphi_t(\beta))^{lt} = 0$$

Съгласно Твърдение 4, $\varphi_i(\beta) \neq 0$. Понеже няма делители на нулата трябва $\beta = \alpha_i$ за някое i, което е противоречие.

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

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 α_i има кратност по-голяма или равна на l_i. От единствеността на каноничния вид следва, че α_i има кратност точно l_i
От (4) имаме

$$l_1 + l_2 + \ldots + l_s \leq \text{ст.f(x)} \qquad (5)$$

Неравенството (5) означава, че броят корените на един полином в оснавното поле, като всеки корен се отчита толкова пъти колкото е неговата кратност, е по-малка или равна на ст.f(x). Това твърдение обобщава доказано по-рано твърдение, според което броят на различните корени на един полином над дадено поле не надминава неговата степен.

Определение
Нека е даден полинома

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n .$$

Полиномът

$$f'(x) \underset{def}{=} a_0 + a_1 x + \ldots + a_n x^n$$

се нарича формална производна на полинома f(x).

Лесно се проверява, че за формалната производна са изпълнени обичайните 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*

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

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

$$f(x) = (x-\alpha)g(x) \qquad (1)$$

От (1) 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 (1) 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 κ тогава $f(x)=(x-\alpha)^{\kappa} g(x)$. От това равенство очевидно следва

$$f(\alpha) = f'(\alpha) = \ldots = f^{(\kappa-1)}(\alpha) = 0.$$

Следователно тези равенства са необходимо условие α да има кратност поне 2.
При $\kappa \geq 3$ 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 $f(x) \in F[x]$

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n \ , a_n \neq 0 \qquad (1)$$

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

$$f(x) = \alpha_0 (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \ . \qquad (2)$$

Като сравним коефициентите в равенствата (1) и (2) получаваме:

$$\alpha_1 + \ldots\ldots\ldots + \alpha_n = -\frac{a_{n-1}}{a_n}.$$

$$\alpha_1\alpha_2 + \ldots\ldots\ldots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n}.$$

$$\alpha_1\alpha_2\alpha_3 + \ldots\ldots\ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n = -\frac{a_{n-3}}{a_n}.$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\alpha_1\alpha_2\ldots\alpha_{n-1} + \ldots\ldots\ldots + \alpha_2\ldots\alpha_{n-1}\alpha_n = (-1)^{n-1}\frac{a_1}{a_n}.$$

$$\alpha_1\alpha_2\ldots\ldots\alpha_n = (-1)^n \frac{a_0}{a_n}.$$

Получените равенства се наричат формули на Виет.