ЛЕКЦИЯ 13
РАЗЛАГАНЕ НА ПОЛИНОМИТЕ В ПРОИЗВЕДЕНИЕ НА НЕРАЗЛОЖИМИ МНОЖИТЕЛИ

Ще ни е необходима следната:

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

Доказателство:

Нека $a.b = a.c$ и a не е делител на нулата. Тогава $a(b-c) = 0$. Понеже a не е делител на нулата следва $b - c = 0$, т. е. $b = c$.

Теорема 1. *Нека F е поле. Тогава всеки неконстантен полином над F може да се представи като произведение на неразложими над F полиноми. С точност до асоциираност това разлагане е единствено.*

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

Доказателство на Теорема 1:

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 такова разлагане е ясно.

Нека $f(x)$ е разложим над F, т. е.

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

От ст. $f_1(x) \geq 1$ и ст. $f_2(x) \geq 1 \Rightarrow$ ст. $f_1(x) < n$ и ст. $f_2(x) < n$. Съгласно идуктивната хипотеза $f_1(x)$ 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

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

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 $f_i(x) = c_i.g_i(x)$, $c_i \in F$, $i = 1, \dots, k$.

От $(\#) \Rightarrow f_1(x)$ дели $g_1(x)g_2(x) \dots g_s(x)$. Понеже $f_1(x)$ е неразложим от Твърдение 4 на втората част на Лекция 12 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 $g_1(x)$. Тъй като в тази ситуация $f_1(x)$ е НОД на $f_1(x)$ и $g_1(x)$ следва, че $f_1(x)$ и $g_1(x)$ не са взаимно прости. Но $f_1(x)$ и $g_1(x)$ са неразложими над F. Поради това от Твърдение 3 на втората част на Лекция 12 следва $f_1(x) = c_1 g_1(x)$. Заместваме в $(\#)$ и получаваме

$$c_1 g_1(x) f_2(x) \dots f_k(x) = g_1(x) g_2(x) \dots g_s(x).$$

Съгласно Лемата можем да съкратим на $g_1(x)$ и получаваме

$$c_1 f_2(x) \dots f_k(x) = g_2(x) \dots g_s(x) \qquad (\#\#)$$

От $(\#\#)$ следва, че $f_2(x)$ дели $g_2(x) \dots g_s(x)$. Съгласно Твърдение 4 на втората част на Лекция 12, след евентуално преномериране имаме, че $f_2(x)$ дели $g_2(x)$. Понеже $f_2(x)$ и $g_2(x)$ са неразложими, от Твърдение 3 на втората част на Лекция 12 имаме $f_2(x) = c_2 g_2(x)$. 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, след евентуално преномериране, имаме $f_i(x) = c_i.g_i(x)$, $c_i \in F$.

С това единствеността е доказана.