# Идеали в пръстен на полиномите над дадено поле. Теорема на Кронекер. Съществуване на поле на разлагане на линейни множители

**Теорема 1:**
*Нека F е поле и I е ненулев идеал в F[x] , $I \neq \{0\}$.*
*Нека f(x) е ненулев полином от I, който има най-ниска възможна степен. Тогава*

$$g(x) \in I \Leftrightarrow g(x) \text{ се дели на } f(x).$$

*Полиномът f(x) се нарича пораждащ полином на идеала I и пишем I=(f(x)).*

Д-во:
1) нека g(x) се дели на f(x). Тогава g(x) = f(x).h(x) понеже $f(x) \in I$, следва $g(x) \in I$.

2) нека $g(x) \in I$. Представяме g(x) = f(x): q(x) + r(x), където ст.r(x) < ст.f(x) или r(x) = 0. Да допуснем, че g(x) не се дели на f(x). Тогава r(x) е ненулев полином и имаме r(x) = g(x) – f(x).q(x). Тъй като g(x), $f(x) \in I$ ,следва че $r(x) \in I$. Това е противоречие, понеже r(x) е полином от идеал с по-ниска степен от f(x).

Теоремата е доказана.□

**Теорема 2:**
*Нека F е поле и $f(x) \in F[x]$ и f(x) е неразложим над F.*
*Тогава факторпръстенът K = F[x] / (f(x)) е поле.*

Д-во:
Полагаме (f(x)) = I.
От това, че F[x] е комутативен пръстен $\Rightarrow$ K = F[x] / I също е комутативен пръстен. Съгласно Теорема1 всеки ненулев полином от I има степен по-голяма или равна на ст.f(x). Следователно в I няма константи, поради това единичният елемент $\boldsymbol{e}$ на F не принадлежи на I. Това означава, че съседният клас $\boldsymbol{e} + I \neq I$ (ненулев елемент на F[x]). Освен това

$$(h(x) + I)(\boldsymbol{e} + I) = h(x).\ \boldsymbol{e} + I = h(x) + I$$

следователно $\boldsymbol{e}$ + I е единица на пръстена K, която е различна от нулевия елемент на K. И така факторпръстена F[x] / I е комутативен пръстен с единица. Остава да докажем, че всеки ненулев елемент на K е обратим.

Нека $g(x) + I \in K$ е ненулев елемент, т.е. $g(x) + I \neq I$ или $g(x) \notin I$. Съгласно Теорема1 g(x) не се дели на f(x). Понеже f(x) е неразложим следва, че ( f(x),g(x) ) = 1. Тъй като ( f(x),g(x) ) = 1 съществуват $u(x),v(x) \in F[x]$ такива, че $\boldsymbol{e} = f(x)u(x)+g(x)v(x)$. Тогаво имаме съседния клас

$$\boldsymbol{e} + I = f(x)u(x) + g(x)v(x) + I$$

Понеже $f(x)u(x) \in I$ , от последното равенство получаваме

$$\boldsymbol{e} + I = g(x)v(x\ ) + I = (g(x) + I)(v(x) + I\ ).$$

От тук става ясно, че съседният клас g(x) + I е обратим и $(g(x) + I)^{-1} = v(x) + I$.
Теоремата е доказана. □

**Определение:**
*Нека F и F' са полета. Казваме, че тези полета са изоморфни, ако съществува 1-1 изображение φ* $F \xrightarrow{\varphi} F'$ *със следните свойства:*

$$от\ a \xrightarrow{\varphi} a'\ \ и\ b \xrightarrow{\varphi} b'$$

*следва, че*

$$a + b \xrightarrow{\varphi} a' + b' \quad и \quad ab \xrightarrow{\varphi} a'b'.$$

*φ се нарича изоморфизъм между полетата F и F'.*

**Определение:**
*Нека F е поле и F' е подмножество на F. Казваме,че F' е подполе на F, ако са изпълнени следните условия:*
1) *F' е подгрупа на адитивната група на F и F' съдържа поне един ненулев елемент*
2) *от a, b∈F', следва, че ab∈F'.*
3) *от a∈F', a ≠ 0, следва, че* $a^{-1} \in F'$.

**Твърдение 1:**
*Подполетата наследяват операциите на полето и относно наследените операци, подполетата също са полета.*

Д-во: (самостоятелно)

Ако F' е подполе на F, казваме също, че полето F е разширение на полето F'.

**Твърдение 2:**
*Нека F е поле, f(x) ∈ F[x] и f(x) е неразложим над полето F. Тогава полето K = F[x] / (f(x)) е разширение на полето F.*

Д-во:
Полагаме (f(x)) = I. Дефинираме

$$F' = \{a + I \mid a \in F\}.$$

Понеже ст.f(x)≥1 и всеки елемент на I се дели на f(x) следва, че в I няма ненулеви константи. Поради това ако a, b∈ $F$ и a≠ b, т.е. a - b≠ 0, имаме a - b∉I. Ето защо a + I≠ b + I. По този начин изяснихме, че в $F'$ няма повторения и поради това F' е подмножество на полето K = $F[x]/I$. Очевидно е, че F' е подполе на K. Разглеждаме изображението:

$$a \xrightarrow{\varphi} a + I, \text{ за всяко } a \in F.$$

Понеже в F' няма повторения , φ е 1-1 изображение между F и F'. Освен това

$$a + b \xrightarrow{\varphi} (a + b) + I = (a + I) + (b + I)$$
$$ab \xrightarrow{\varphi} ab + I = (a + I)(b + I)$$

φ е изоморфизъм между F и F'.

Като отъждествим елементите на подполето F' с елементите на полето F в смисъл на изоморфизма φ, получаваме, че K е разширение на F.□

**Теорема 3 (Теорема на Кронекер).**
*Нека F е поле. За всеки неконстантен полином f(x)∈F[x] съществува разширение K на F, в което f(x) има корен.*

Д-во:
Тъй като всеки неконстантен полином може да се представи като произведение на неразложими полиноми, достатъчно е да докажем,че поне един от тези неразложими множители има корен в някакво разширение. Поради това предполагаме, че f(x) е неразложим над F.
Тогава фактопръстенът K = $F[x]/(f(x))$ е поле (съгласно Теорема2). Съгласно Твърдение2, K е разширение на F. Ще докажем,че f(x) има корен в K, по-точно ще докажем ,че съседният клас x + I ∈ K = $F[x]/(f(x))$ е корен на f(x).
Полагаме (f(x)) = I. Нека $f(x) = a_0 + a_1x + \ldots + a_nx^n$ , $a_i \in F$, i = 1…n. Разглеждаме като полином над K f(x) има вида :

$$f(x) = (a_0 + I) + (a_1 + I)x + (a_2 + I)x^2 + \ldots\ldots + (a_n + I)x^n.$$

имаме

$$f(x + I) = (a_0 + I) + (a_1 + I)(x + I) + (a_2 + I)(x + I)^2 + \ldots\ldots + (a_n + I)(x + I)^n.$$

Тъй като $(x + I)^k = x^k + I$ (по дефиниция), имаме

$$(a_k + I)(x + I)^{\kappa} = (a_k + I)(x^k + I) = a_kx^k + I \text{ , } k = 0\ldots..n.$$

Като съберем тези равенства ще получим:

$$f(x + I) = (a_0 + I) + (a_1x + I) + (a_2x^2 + I) + \ldots\ldots + (a_nx^n + I) =$$

$$= \sum_{k=0}^{n} (a_{\kappa} + I)(x + I)^k = a_0 + a_1x + \ldots + a_nx^n + I = f(x) + I.$$

Получаваме, че f(x + I) = f(x) +I. Понеже f(x)∈I имаме f(x + I) = I. Следователно x + I е корен на f(x) в полето K.
Теоремата е доказана.□

**Следствие:**
*Нека F е поле. За всеки неконстантен полином f(x)∈F[x], съществува разширение K на полето F, над което f(x) се разлага на линейни множители.*

Д-во:
Индукция по ст.f(x) = n.
База на индукцията при n = 1.
В тази ситуация f(x) е линеен и в качеството на желаното разширение можем да вземем самото поле F.

Нека n ≥ 2:
Съгласно Теорема3 съществува разширение E на F, в което f(x) има корен $\alpha_1$. Тогава

$$f(x) = (x - \alpha_1)g(x), \text{ където } \alpha_1 \in E \text{ и } g(x) \in E[x]. \qquad (*)$$

Имаме ст.$g(x) = n-1 \geq 1$. Съгласно индуктивната хипотеза, съществува разширение K на E, над което g(x) се разлага на линейни множители:

$$g(x) = A(x - \alpha_2)\ldots\ldots(x - \alpha_n) \text{ , където } A, \alpha_2, \ldots, \alpha_n \in K.$$

От последното равенство е (*) получаваме

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

Получихме, че f(x) се разлага на линейни множители над разширението K, с което следствието е доказано.□