ЛЕКЦИЯ 27
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 $I \lhd F[x]$, $I \neq \{0\}$. 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 $I = (f(x))$.

Доказателство:

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. Тъй като $g(x)$, $f(x) \in I$, от $r(x) = g(x) - f(x).q(x)$, следва че $r(x) \in I$. Това е противоречие, понеже $r(x)$ е полином от идеала I с по-ниска степен от $f(x)$.

Теоремата е доказана.

Забележка. *Пораждащият полином на даден ненулев идеал на $F[x]$ не е определен еднозначно. От Теорема 1 следва обаче, че всеки два пораждащи полинома се делят взаимно и поради това са асоциирани.*

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

Доказателство:

Полагаме $(f(x)) = I$. Понеже $f(x)$ е неразложим, ст. $f(x) \geq 1$. От това, че $F[x]$ е комутативен пръстен, следва че $K = F[x]/I$ също е комутативен пръстен. Съгласно Теорема 1 всеки ненулев полином от I има степен по-голяма или равна на ст. $f(x)$. Следователно в I няма ненулеви константи. Поради това единичният елемент e на F не принадлежи на I. Това означава, че съседният клас $e + I \neq I$ (ненулев елемент на K). Освен това

$$(h(x) + I)(e + I) = h(x).e + I = h(x) + I.$$

Следователно $e+I$ е единица на пръстена K, която е различна от нулевия елемент I на K. И така факторпръстенът K 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. $g(x)+I \neq I$. Тогава $g(x) \notin I$. Съгласно Теорема 1 $g(x)$ 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 $e = f(x)u(x) + g(x)v(x)$. Тогава имаме

$$e + I = f(x)u(x) + g(x)v(x) + I = (f(x)u(x) + I) + (g(x)v(x) + I)$$

Понеже $f(x)u(x) \in I$, имаме $f(x)u(x) + I = I$ и получаваме

$$e + I = g(x)v(x) + I = (g(x) + I)(v(x) + I).$$

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 $F \xrightarrow{\varphi} F'$ което изобразява сумата в сума и произведението в произведение, т. е.*

$$\text{ако } a \xrightarrow{\varphi} a' \text{ и } b \xrightarrow{\varphi} b',$$

тогава

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

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) ако $a,\ b \in F'$, тогава $ab \in F'$;

3) ако $a \in F'$, $a \neq 0$, тогава $a^{-1} \in F'$.

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

Доказателство:

(самостоятелно)

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

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

Доказателство:

Полагаме $(f(x)) = I$. Дефинираме

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

Понеже ст. $f(x) \geq 1$ и всеки елемент на I се дели на $f(x)$ следва, че в I няма ненулеви константи. Поради това ако $a,\ b \in F$ и $a \neq b$, т. е. $a - b \neq 0$, имаме $a - b \notin I$. Ето защо $a + I \neq b + I$. По този начин изясняхме, че в F' няма повторения и поради това F' е подмножество на полето $K = F[x]/I$. Лесно се проверява, че F' е подполе на K. Наистина, първите две условия за подполе са изпълнени по очевиден начин, а третото условие е изпълнено поради равенството $(a+I)^{-1} = a^{-1} + I$.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

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

и

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

Следователно 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 $f(x) \in F[x]$ съществува поле K, разширение на F, в което $f(x)$ има корен.*

Доказателство:

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 на F. Поради това предполагаме, че $f(x)$ е неразложим над F. Тогава фактопръстенът $K = F[x]/(f(x))$ е поле (съгласно Теорема 2). Съгласно Твърдение 2, K е разширение на F. Ще докажем, че $f(x)$ има корен в K, по-точно ще докажем, че съседният клас $x + I \in K = F[x]/(f(x))$ е корен на $f(x)$.

Полагаме $(f(x)) = I$. Нека $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_i \in F$, $i = 1$, $2,\ldots, n$. Разглеждан като полином над K, съгласно доказателството на Твърдение 2, $f(x)$ има вида:

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

Разглеждаме

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

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

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

Като съберем тези равенства ще получим:

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

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

Получихме, че $f(x + I) = f(x) + I$. Понеже $f(x) \in I$, имаме $f(x + I) = I$. Тъй като I е нулевия елемент на K, $x + I$ е корен на $f(x)$ в полето K.

Теоремата е доказана.

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

Доказателство:

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 $n \geq 2$:

Съгласно Теорема 3 съществува разширение E на F, в което $f(x)$ има корен α_1. Тогава

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

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

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

От последното равенство и (*) получаваме

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

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