Крайни полета

Полето F е крайно, ако $|F| < \infty$.

Твърдение 1: *Нека E е поле и F е подполе на E. Тогава E е линейното пространство над F.*

Доказателство**:**
Операцията " + " на линейни пространства е същата като в полето E. Първите четири аксиоми на лин. простр. са автоматично удовлетворени. Ако $\alpha \in F$ и $a \in E$, тогава произведението αa е произведение в смисъл на E. Ясно е, че другите четири аксиоми също ще са изпълнени и поради това твърдението е доказано.

С $\dim_F E$ означаваме размерността на E като лин. пр. над F.

Твърдение 2: *Нека L е лин. пр. над F и F е крайно поле. Ако* $\dim_F L = t$ *, тогава*
$|L| = |F|^t$

Доказателство: Нека $e_1, \ldots, e_t$ е базис на L и $x \in L$
Ако

$$x = \xi_1 e_1 + \ldots + \xi_t e_t \text{ тогава } x \xrightarrow{\varphi} (\xi_1, \ldots, \xi_t) \text{ по дефиниция.}$$

От линейната алгебра знаем, че φ задава 1-1 изображение между L и наредените t-орки елементи от F. Понеже броят на наредените t-орки от F е равен на $|F|^t$, имаме $|L| = |F|^t$. □

Твърдение 3: *Нека F е крайно поле, което има характеристика p. Ако* $\dim_{Zp} F = n$ *тогава броят на елементите на F е равен на* p^n.

Съгласно теоремата от миналата лекция , F е разширение на Z_p. Поради това означението $\dim_{Z_p} F$ е коректно. F е линейно пространство на Z_p понеже $|Z_p| = p$ желаното равенство следва от **Тв.2**.

Теорема 1: *Нека F е крайно поле и* ***char****(F) = p. Ако* $\dim_{Z_p} F = n$ *тогава*

а) всеки елемент на F е корен на полинома $x^{p^n} - x$ *;*

б) вярно е равенството $x^{p^n} - x = \prod_{a \in F} (x - a)$ *и* $\Rightarrow$ $x^{p^n} - x$ *се разлага на линейни множители над F .*

Доказателство**:** Очевидно $x = 0$ е корен на $x^{p^n} - x$. Нека $a \in F$ и $a \neq 0$. Тогава a е елемент на мултипликативната група на полето. Тъй като $|F| = p^n$ (Тв.3) редът на мултипликативната група на полето F е $p^n - 1$ и поради това $a^{p^n - 1} = e \Rightarrow a^{p^n} = a \Rightarrow a$ е корен на $x^{p^n} - x$. Нека $h(x) = \prod_{a \in F} (x - a)$. Тъй като всеки елемент на полето F е корен на полинома $x^{p^n} - x$, всеки от множителите на $h(x)$ ще дели $x^{p^n} - x$. От друга страна всеки два множителя на $h(x)$ са взаимно прости (Защо? виж лекцията за взаимно прости множители). Поради това $h(x)$ дели $x^{p^n} - x$. Понеже тези два полинома имат равни степени това означава, че единият от тях се получава от другия с умножаване на константа. Понеже и двата полинома са унитарни те трябва да съвпадат.

Теорема 2: *Нека F е поле и char(F) = p. Означаваме множеството на корените на полинома* $x^{p^k} - x$ *в F с F' (k-фиксирано естествено число). Тогава F' е подполе на F и броят на елементите на* F' *не надминава* p^k *.*

Доказателство**:**

Очевидно 0, $e \in F'$. Поради това *F'* съдържа ненулев елемент. Нека *a,* $b \in F'$, т.е. $a^{p^k} = a$ и $b^{p^k} = b$. Поради това

$$(a+b)^{p^k} = a^{p^k} + b^{p^k} = a + b \Rightarrow a + b \in F'$$ (е корен на полинома)

$$(a-a)^{p^k} = 0 = a^{p^k} + (-a)^{p^k} \Rightarrow a + (-a)^{p^k} = 0 \Rightarrow (-a)^{p^k} = -a \Rightarrow -a \in F'$$

До тук изяснихме, че *F'* е подгрупа на адитивната група, която съдържа ненулев елемент.
Очевидно е, че

$$(ab)^{p^k} = a^{p^k} \; b^{p^k} = ab \Rightarrow ab \in F'$$

Нека $a \neq 0$. $(\underbrace{aa^{-1}}_{e})^{p^k} = a^{p^k} . (a^{-1})^{p^k} \Rightarrow a(a^{-1})^{p^k} = e \Rightarrow (a^{-1})^{p^k}$ е обратен на *a*

$\Rightarrow (a^{-1})^{p^k} = a^{-1} \Rightarrow a^{-1} \in F'$

Тъй като $x^{p^k} - x$ не може да има повече от p^k корена $\Rightarrow |F'| \leq p^k$.□

Теорема 3: *За всяко естествено число k и всяко просто число p , съществува поле с* p^k *елемента.*

Долазателство**:**

Разглеждаме полето Z_p и $x^{p^k} - x \in Z_p[x]$. Съгласно следствието от теоремат на Кронекер, съществува разширение *E* на Z_p ($E \supset Z_p$), над което $x^{p^k} - x$ се разлага на линейни множители. Да означим с *F* множеството от корените на $x^{p^k} - x$ в *E*. Съгласно Теорема2, *F* е поле. Ще докажем, че полето *F* има желаните свойства т.е. $|F| = p^k$. Да забележим, че формалната производна е равна на:

$(x^{p^k} - x)' = p^k x^{p^k - 1}$ -1 , коефициентът пред $x^{p^k - 1}$ всъщност е ($p^k e$) и понеже характеристиката е равна на нула, то ($p^k e$) = 0 в Z_p . Поради това формалната производна на $x^{p^k} - x$ е равна на единица и следователно е различна от нула. Следователно този полином няма кратни коерни. И така полиномът $x^{p^k} - x$ се разлага на линейни множители в полето *E* и няма кратни корени. От тези два факта $\Rightarrow$ че броят на корените на $x^{p^k} - x$ в *E* е равен на p^k т.е. $|F| = p^k$.□

Теорема 4: *Нека F е крайно поле, char F = p и* $|F| = p^n$ *. Ако F' е подполе на F тогава* $|F'| = p^m$ *, където m дели n.*

Обратно: За всяко естествено число m, което дели n, F има подполе с p^m *елемента и то е единствено.*

Доказателство**:**

1) *F'* е подполе на *F* и $|F'| = p^m$

$F \supseteq F' \supseteq Z_p$ Ако $\dim_{F'} F = s \Rightarrow |F| = |F'|^s$ (Тв.2). Заместваме $|F'| = p^m$ и получаваме

$p^n = (p^m)^s \Rightarrow p^n = p^{ms} \Rightarrow n = ms \Rightarrow m$ дели n .

2) Нека $n = ms$

$p^n - 1 = p^{ms} - 1 = (\underbrace{p^m - 1}_{k})(\underbrace{\ldots\ldots\ldots}_{e})$

$$x^{p^n - 1} - 1 = x^{kl} - 1 = (x^k - 1)(\ldots\ldots\ldots) \qquad (*)$$

Знаем, че $x^{p^n} - x$ се разлага на линейни множители над $F \Rightarrow x^{p^n - 1} - 1$ също се разлага на линейни множители над *F*. От (*) и единстеността на разлагането на линейни множители $\Rightarrow x^k - 1$ също се разлага на лин. множители над $F \Rightarrow x^{k+1} - x$ също се разлага на лин. мн. над *F*. Но $k = p^m - 1 \Rightarrow x^{p^m} - x$ се разлага на лин. мн. над *F*. Нека *F'* е множеството на корените на $x^{p^m} - x$ в *F* . Съгасно Теорема 2 *F'* е подполе. Тъй като $x^{p^m} - x$ се разлага на линейни множители в *F* и няма кратни корени, имаме, че $|F'| = p^m$, с което съществувнето на подполето е доказано. Не е възмойно да има друго подполе с p^m елемента тъй като неговите елементи също ще бъдат корени на $x^{p^m} - x$ и ще стигнем до извода, че този полином има повече корена в разглеждното поле от своята степен, което е противоречие.