ЛЕКЦИЯ 29
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 „$+$“ 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 $e_1, e_2, \ldots, e_t$ е базис на L и $x \in L$.

Ако

$$x = \xi_1 e_1 + \xi_2 e_2 + \cdots + \xi_t e_t \text{ тогава дефинираме } x \xrightarrow{\varphi} (\xi_1,\ \xi_2, \ldots,\ \xi_t)\,.$$

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 $\dim_{\mathbb{Z}_p} F = n$, тогава броят на елементите на F е равен на p^n.*

Съгласно теоремата от миналата лекция, F е разширение на $\mathbb{Z}_p$. Поради това F е линейно пространство над $\mathbb{Z}_p$ и означението $\dim_{\mathbb{Z}_p} F$ е коректно. Понеже $|\mathbb{Z}_p| = p$, желаното равенство следва от Твърдение 2.

Теорема 1. *Нека F е крайно поле,* $\mathrm{char}\,(F) = p$ *и* $\dim_{\mathbb{Z}_p} F = n$. *Тогава*
а) Всеки елемент на F е корен на полинома $x^{p^n} - x = 0$;
б) Вярно е равенството $x^{p^n} - x = \prod_{a \in F} (x - a)$.

Доказателство:

Очевидно $x = 0$ е корен на $x^{p^n} - x = 0$. Нека $a \in F$ и $a \neq 0$. Тогава a е елемент на мултипликативната група на полето. Тъй като $|F| = p^n$ (Твърдение 3) редът на мултипликативната група на полето F е $p^n - 1$. Съгласно Лекция 22, Следствие 2, имаме $a^{p^n - 1} = e$, откъдето $a^{p^n} = a$ и следователно a е корен на $x^{p^n} - x$. С това (а) е доказано. 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 $h(x)$ дели $x^{p^n} - x$ и ще участва в каноничното разлагане на $x^{p^n} - x$ над F. Поради това $h(x)$ дели $x^{p^n} - x$ (до този извод можем да стигнем и с помощта на Твърдение 6 на Лекция 12). Понеже тези два полинома имат равни степени, те са асоциирани. Понеже и двата полинома са унитарни те съвпадат.

Теорема 2. *Нека F е поле и* $\mathrm{char}\,(F) = p$. *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 му 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 $b^{p^k} = b$. Тогава от миналата лекция (Твърдение 6) имаме

$$(a + b)^{p^k} = a^{p^k} + b^{p^k} = a + b.$$

Следователно

$$a + b \in F'.$$

От равенствата

$$0 = (a - a)^{p^k} = a^{p^k} + (-a)^{p^k} = a + (-a)^{p^k},$$

виждаме че

$$(-a)^{p^k} = -a \text{ и } -a \in F'.$$

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

$$(ab)^{p^k} = a^{p^k} b^{p^k} = ab, \text{ откъдето } ab \in F'.$$

Нека $a \neq 0$. Тогава

$$e = (aa^{-1})^{p^k} = a^{p^k} (a^{-1})^{p^k} = a(a^{-1})^{p^k}.$$

Следователно $(a^{-1})^{p^k} = a^{-1}$ и $a^{-1} \in F'$. Доказахме, че F' е подполе на F. Тъй като $x^{p^k} - x$ не може да има повече от p^k корена в F, следва че $|F'| \leq p^k$.

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

Доказателство:

Разглеждаме полето $\mathbb{Z}_p$ и $x^{p^k} - x \in \mathbb{Z}_p[x]$. Съгласно следствието от теоремата на Кронекер, съществува разширение E на $\mathbb{Z}_p$ ($E \supset \mathbb{Z}_p$), 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 Теорема 2, F е поле. Ще докажем, че $|F| = p^k$. Нека $\overline{1}$ е единицата на $\mathbb{Z}_p$. Тогава $x^{p^k} - x = \overline{1}x^{p^k} - \overline{1}x$ и формалната производна на този полином е равна на $(p^k\overline{1})x^{p^k-1} - \overline{1} = -\overline{1} \neq 0$, понеже в $\mathbb{Z}_p$ имаме $p\overline{1} = 0$. Съгласно Лекция 14, този полином няма кратни корени. И така полиномът $x^{p^k} - x$ се разлага на линейни множители над полето E и няма кратни корени. От тези два факта следва, 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,* $\operatorname{char} F = p$ *и $|F| = p^n$.*

а) Ако F' е подполе на F, тогава $|F'| = p^m$, където m дели n;

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

Доказателство:

Доказателство на а)

Ясно е, че $\operatorname{char}(F') = p$. Поради това $F' \supseteq \mathbb{Z}_p$. Ако $\dim_{\mathbb{Z}_p} F' = m$, тогава съгласно Твърдение 3, $|F'| = p^m$. Нека $\dim_{F'} F = s$. От Твърдение 2 имаме $|F| = |F'|^s$. Следователно $|F| = p^{ms}$, откъдето $p^n = p^{ms}$ и $n = ms$, т. е. m дели n.

Доказателство на б)

Нека m е естествено число и $n = ms$, където s също е естествено число. Нека F' е множеството на корените на $x^{p^m} - x$ в F. Съгласно Теорема 2, F' е подполе на F. Ще докажем, че $|F'| = p^m$. За тази цел ще докажем, че $x^{p^m} - x$ се разлага на линейни множители над F. От $n = ms$ имаме

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

От това равенство, получаваме

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

От Теорема 1 става ясно, че лявата част на (*) се разлага на линейни множители над F. От единствеността на каноничното разлагане на $x^{p^n-1}-1$ над полето F и (*) следва, че x^k-1 също се разлага на линейни множители над F. Поради това

$$x(x^k-1) = x^{k+1} - x = x^{p^m} - x$$

също се разлага на линейни множители над F. Понеже $x^{p^m} - x$ няма кратни корени в F (виж доказателството на Теорема 3) следва, че $|F'| = p^m$.

Да допуснем сега, че освен F' полето F има и друго подполе $F'' \neq F'$ с $|F''| = p^m$. Тогава $|F' \cup F''| > p^m$. Съгласно Теорема 1, елементите на F'' също са корени на $x^{p^m} - x$. Стигнахме до извода, че $x^{p^m} - x$ има в полето F повече от p^m корена, което е противоречие.