Дефиниция

Крайно поле е поле с краен брой елементи.

Примери: $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_p$, където p е просто.

Теорема (крайно поле)

Нека F е поле и $|F| < \infty$. Тогава $|F| = p^k$, за някое просто число p.

Доказателство:
$\mathrm{char}\ F = p$ - просто (ако не е просто тогава за делителите му n, m ще е изпълнено, че n и m-кратните на 1 ще бъдат делители на 0).
Тогава съществува $F_0 \subseteq F$, такова че $F_0 \cong \mathbb{Z}_p$ (просто взимаме k-кратните на 1).
Може да разглеждаме F като линейно пространство над полето $\mathbb{Z}_p$.

- за произволни $a, b \in F$ имаме $a + b \in F$ (защото F е поле)
- съществува нулев елемент по отношение на събирането както и противоположен елемент по отношение на събирането (защото F е поле).
- събирането е асоциативно и комутативно
- за произволни $a \in F \& \alpha \in \mathbb{Z}_p$ имаме, че $\alpha a \in F$
- изпълнени са двата дистрибутивни закона

Т.е видяхме, че F е също и линейно пространство над $\mathbb{Z}_p$.
Нека $\dim_{\mathbb{Z}_p} F = k < \infty$. Тогава съществува базис $e_1, e_2, \cdots, e_k \in F$, такъв че всеки елемент от F може да се представи като $\alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_k e_k$, където $\alpha_i \in \mathbb{Z}_p$.

Т.е вече може да 'преброим' елементите на F, като видим колко различни координати могат да се образуват:

$$|F| = |\{(\alpha_1, \alpha_2, \cdots, \alpha_k) | \alpha_i \in \mathbb{Z}_p\}| = p^k \quad (1)$$

Твърдение (->)

Нека F е крайно поле и $|F| = p^k$. Тогава елементите на полето F са всички корени на уравнението $x^{p^k} - x \in \mathbb{Z}_p[x]$.

Доказателство:
Нека $\alpha \in F^*$ (т.е α е произволен ненулев елемент).
С $o(\alpha)$ ще бележим мултипликативния ред на α, т.е $o(\alpha) = s$, ако $\alpha^s = 1$ и s е минимално.
Ако $o(\alpha) = s$ имаме, че $s \mid |F^*|$ (защото F^* е група, и мултипликативната група породена от α е подгрупа на $|F^*|$, следователно реда на подгрупата дели реда на цялата група).
Т.е $s \mid p^k - 1$. Това означава, че $\alpha^{p^k - 1} = 1$ (защото повдигаме α на степен, кратна на мултипликативния му ред).
Казано по друг начин горното означава, че α е корен на уравнението $x^{p^k-1} - 1$.
Тъй като полинома $x^{p^k-1} - 1$ има точно $p^k - 1$ корена, колкото са и елементите на мултипликативната група F^*, следователно всички корени са точно елементите на F^*.
За да включим и нулевия елемент към корените (за да получим полином, чиито корени са елементите на F) трябва да умножим по x:

$$f(x) = x(x^{p^k-1} - 1) = x^{p^k} - x \quad (2)$$

Тъй като корените на $f(x)$ са точно p^k на брой, това означава че всеки елемент на полето е корен на уравнението и обратно.
От тук - всеки две полета с равен брой елементи - p^k са изоморфни (защото елементите им са всички корени на един и същи полином $x^{p^k} - x$).

Дефиниция *(степен на разширение)*

Ако $|F| = p^k$, то k се нарича *степен на разширение*.

Сега ще докажем обратното твърдение:

Твърдение (<-)

За всяко просто p и естествено s съществува поле с точно p^s елемента.

Доказателство:

Нека $g(x) = x^{p^s} - x \in \mathbb{Z}_p[x]$.
Да разгледаме разширението с корените на полинома $L \supseteq \mathbb{Z}_p$.
Нека $F_0 = \{\alpha | g(\alpha) = 0\} \subseteq L$.
Ще докажем, че $|F_0| = p^s$.

скрии

> на лекции не е доказано - аз обаче въобще не видях очевидна причина това да е така. (проблема идва от евентуални кратни корени)

Ами да допуснем, че $g(x)$ има кратен корен α. Това означава, че $g(\alpha) = g'(\alpha) = 0$.
Ще разпишем само g':

$$g'(\alpha) = (1.p^s)\alpha^{p^s-1} - 1 = (0)\alpha^{p^s-1} - 1 = -1 \tag{3}$$

Обръщам внимание, че $1.p^s$ е p^s-кратното на 1 (защото такава е дефиницията на производна), т.е 1 събрано p^s пъти само със себе си. Да обаче полето $\mathbb{Z}_p$ (над което е полинома g, и полинома g') има характеристика p, следователно p^s-кратното на 1 е 0. От тук виждаме, че производната g' е константата -1, следователно няма кратни корени (защото производната въобще няма корени).

Сега остава да докажем че F_0 е поле. Ще го направим като докажем, че F_0 е подполе на L.
За всички корени α на $g(x)$ е изпълнено $\alpha^{p^s} = \alpha$ (просто записано по друг начин $g(\alpha) = 0$).
Нека α, β са произволни корени на $g(x)$. Ще докажем, че може да ги вадим, умножаваме и намираме обратен елемент:

- **умножение**: $(\alpha\beta)^{p^s} = \alpha^{p^s}\beta^{p^s} = \alpha\beta$, следоватено $\alpha\beta \in F_0$
- **взимане на обратен**: Нека $\beta \neq 0$. Тогава $(\beta^{-1})^{p^s} = (\beta^{p^s})^{-1} = \beta^{-1}$, следователно $\beta^{-1} \in F_0$
- **изваждане**: Понеже $\mathrm{char}\, L = p$ имаме, че $(\alpha + \beta)^p = \alpha^p + \beta^p$ (просто разписваме с биномни коефициенти (и имаме предвид, че коефициента значи колко пъти събираме променливата, а не умножение в полето)). Сега вече тривиално

(4)

$$
\begin{aligned}
(\alpha-\beta)^{p^s} &= \underbrace{\Big(\Big((\alpha-\beta)^p\Big)^p\cdots\Big)^p}_{s} \\
&= \underbrace{\Big(\Big((\alpha^p-\beta^p)^p\Big)^p\cdots\Big)^p}_{s-1} \\
&= \underbrace{\Big(\Big(((\alpha^p)^p-(\beta^p)^p)^p\Big)^p\cdots\Big)^p}_{s-2} \\
&\vdots \\
&= \alpha^{p^s}-\beta^{p^s}
\end{aligned}
$$

Следователно F_0 е подполе на L, т.е самото то е поле. Следователно съществува поле с p^s елемента!

Теорема (мултипл. група на крайно поле е циклична)

Нека F е поле и $|F|=p^s$. Ще докажем, че мултипликативната група F^* на крайно поле е циклична.

Доказателство:
Нека $\alpha\in F^*$ е елемента на мултипликативната гурпа с максимален ред (относно умножението).
Тогава $o(\alpha)=r$ и $r\mid |F^*|$, следователно $r\leq |F^*|$.
Нека $\beta\in F^*$ е произволен елемент. Ще докажем, че $o(\beta)=t\mid r$.
Допускаме, че $t\nmid r$, т.е $d=(t,r)>1$. Нека $t=dt_1$.
Тогава $o(\beta^d)=t_1>1$.
Да пресметнем реда на $\alpha\beta^d$: $o(\alpha\beta^d)=o(\alpha)o(\beta^d)=t_1r>r$.[1] Противоречие (получихме елемент с по-голям ред от r).

Доказахме, че за всяко $\beta\in F^*$ имаме $o(\beta)\mid r$, следователно всички елементи от F^* са корени на полинома x^r-1. Но той има най-много r корена, следователно $|F^*|\leq r$. Получихме, че $r=|F^*|$, следователно $\langle\alpha\rangle=F^*\cong\mathbb{C}_{|F^*|}$[2]

Дефиниция (примитивни елементи)

Пораждащите елементи на мултипликативната група се наричат *примитивни*.

Теорема (за броя елементи на подполе)

1. Ако F е поле, $|F|=p^s$ и G е подполе на F, тогава $|G|=p^k$, където $k\mid s$.
2. Ако F е поле, $|F|=p^s$ и $t\mid s$, тогава съществува подполе $G\subseteq F$, такова че $|G|=p^t$.

Доказателство:
1. Нека $G \subseteq F$ е подполе. Тогава може да разглеждаме F като линейно пространство над G. Тогава ако $\dim_G F = m$ то $|F| = |G|^m$, следователно $p^s = (p^k)^m$, откъдето $s = mk \Rightarrow k \mid s$.
2. Нека $|F| = p^s$ и $t \mid s$, следователно $s = t.m$.
Мултипликативната група на F - F^* има точно $p^s - 1$ елемента.
Понеже $p^t - 1 \mid p^{tm} - 1 = p^s - 1$, можем да си изберем елемент $\beta = \alpha^m$, който да има ред $p^t - 1$ (ако $\langle \alpha \rangle = F^*$). Следователно $\langle \beta \rangle = H$ е група с $p^t - 1$ елемента.
За всяко $\gamma \in H$ имаме, че $\gamma^{p^t-1} = 1$, т.е γ е корен на полинома $x^{p^t-1} = 1$. (в обратната посока също).
Следователно $H \cup \{0\}$ е полето на разлагане на $x^{p^t} - x$. И освен това има точно p^t елемента.

Footnotes

1. $o(ab) = o(a)o(b)$ - това било от 'задачките' за ред на елементи - който иска да го докаже
2. това последното са $|F^*|$-тите корени на единицата

page revision: 1, last edited: 1 Jul 2009, 01:27 (1467 days ago)