K-поле 1) $L \supset K$
2) $L \ni \alpha$ $p(\alpha)=0$
3) k-мин n $\int \Pi_k$

мы доказали $\overset{?}{\Leftarrow}$ Π_0-св-ть

Т-ма: Построим $L := K[x]/\langle p(x)\rangle$, тогда L-поле, удовлетв. усл. 1,2,3) $\Leftrightarrow a, b, \beta$)

а) $L \supset K$? , $\tilde{K} = \{\tilde{c} \mid c \in K\} \Rightarrow$

тогда $\tilde{K} \simeq K$, соотв: $c \leftrightarrow \tilde{c}$, оно взаимнооднозн:

$\tilde{c} = \tilde{c'} \Leftrightarrow p(x) \mid (c-c')$, так как $c, c' \in K \Rightarrow \deg(c-c') \le 0$
или $p(x) \ge 1 \Rightarrow c - c' \equiv 0 \Rightarrow c = c'$

в соотв. с операц. (сохр. соотв): $\widetilde{c \pm c'} = \tilde{c} \pm \tilde{c'}$
$\widetilde{c \cdot c'} = \tilde{c} \cdot \tilde{c'}$

$\tilde{K} \simeq K$, $\tilde{K}$ - подполе в L

далее не различаем эл-ты $\tilde{c}$ и c, $c \in K$

б) Пусть $p(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_n x^n$, где $c_i \in K$, $n \ge 1$

Докуж: Положим $\alpha = \tilde{x} \in L$, тогда $p(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \dots c_n\alpha^n =$

$= \tilde{c_0} + \tilde{c_1}\tilde{x} + \dots + \tilde{c_n}\tilde{x^n} = \widetilde{c_0 + c_1 x + \dots + c_n x_n} = \tilde{p}(x) = \tilde{0} \Rightarrow$

$p(\alpha) = 0 \Rightarrow \alpha$ - корень

в) Пусть $f(x) \in K[x]$, разделим f на p с остатком:

$f = p \cdot h + r$, $\deg r < \deg p \Rightarrow \tilde{f} = \widetilde{ph + r} = \tilde{p}\tilde{h} + \tilde{r} = \tilde{0}\cdot\tilde{h} + \tilde{r} = \tilde{r}$

Если $r(x) = r_0 + r_1 x + \dots + r_{n-1}x^{n-1}$, $r_i \in K$, то $\tilde{r}(x) = r_0 + r_1\alpha + \dots + r_{n-1}\alpha^{n-1}$

Если L'-подполе L и $L' \supset K$ и $\alpha \Rightarrow L' \ni \tilde{r} = \tilde{f} \Rightarrow$
$\Rightarrow L'$ содержит $L \Rightarrow L' \equiv L$, L - min подполе из L с усл a, b, β

ч. т. д

Следствие: L - вект. пр-во над K с базисом $1, \alpha, \alpha^2 \dots \alpha^{n-1}$, где $n = \deg p(x)$
$\Rightarrow$ размерность $\dim_K L = n$. $\left[\,|K| = q \Rightarrow |L| = q^n\,\right] \leftarrow \Pi_k$ $L \simeq K$

Доказательство: надо только проверить независимость $1, \alpha, \alpha^2 \dots \alpha^{n-1}$ Если: $r_0 + r_1\alpha + \dots r_{n-1}\alpha^{n-1} = \tilde{0}$, $r_i \in K \Rightarrow$

$\Rightarrow r(x) \mid r_0 + r_1 x + \dots r_{n-1}x^{n-1} \Rightarrow r_i = 0 \ \forall i \Rightarrow$ л.н. $1, \alpha, \dots \alpha^{n-1}$
$\deg = n$ $\deg < n$

ч. т. д

ПРИМЕР: построим поле из 4х элементов:

пусть $K = \mathbb{Z}_2^* = \{0, 1\}$, $p(x) = x^2 + x + 1 \in K[x]$, утв-ся, что он неприв!

т.к. $p(x)$ не имеет корней в K $\quad p(0) = 1$, $p(1) = 1$

Пусть $L = K[x] / \langle x^2 + x + 1 \rangle = \{ z_0 + z_1 \cdot \alpha \mid z_0, z_1 \in K \} =$

$= \{0, 1, \alpha, \alpha + 1\} \Rightarrow \alpha^2 + \alpha + 1 = 0$

$\alpha^2 = -\alpha - 1 \overset{\mathbb{Z}_2}{=} \alpha + 1$

+	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

·	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

$(\alpha+1)^2 = \alpha^2 + 2\alpha + 1$

координатное соответствие

$0 \leftrightarrow 00$

$1 \leftrightarrow 10$

$\alpha \leftrightarrow 01$

$\alpha+1 \leftrightarrow 11$

ПОРЯДОК, ЕДИНСТВЕННОСТЬ и '$\exists$-ИЕ' КОНЕЧНЫХ ПОЛЕЙ

ТЕОРЕМА: $\forall$ конеч. поле имеет порядок p^n, где p-прост. число, а n-натуральное.

Наоборот: для $\forall$ пр. p и нат. n $\exists!$ (с точ. до $\cong$) поле порядка p^n

ст. обозначение: $GF(p^n)$ (Галуа) $\vee$ $\mathbb{F}_{p^n}$

док-во: 1) порядок Пусть F-кон. поле, тогда F имеет хар-ку $p > 0$: $\underbrace{1+1+\dots+1}_{p\text{-min}} = 0$, $\Rightarrow p$-простое.

Тогда $\exists$ кон-во $K = \{0, 1, 1+1, \dots, \underbrace{1+1+\dots+1}_{p-1}\}$ - образует подполе в $F \cong \mathbb{Z}_p$

т.к. опр. умн. в K задается операцией сложения и законом дистрибутивности

Поле F рассм. как вект. прво над подполем K;

Поскольку F конечный базис над K:

$e_1, e_2 \dots e_n$, тогда:

$F = \{\alpha_1 e_1 + \dots + \alpha_n e_n\} \mid \alpha_i \in K$ - однор. прогр. $\times K^n$ г/з базис.

$\Rightarrow |F| = |K|^n = p^n$

2) '!-ость' Пусть $\mathcal{F}$ - кон поле хар. p^n p-простое.

Тогда $K^* = \mathcal{F} \setminus \{0\}$ - мультипл. поле хар p^n-1 и абелева циклическая, в частности

$\alpha \neq 0 \Rightarrow \alpha^{p^n-1} = 1 \Rightarrow \alpha^{p^n} = \alpha \leftarrow \forall \alpha \in \mathcal{F}$ (и для 0)

$\Rightarrow \mathcal{F}$ служит в кач-ве корней многочлена $x^{p^n} - x \in \mathbb{Z}_p[x]$

Т.к. $|\mathcal{F}| = p^k$ а $\deg(x^{p^n} - x) = p^n \Rightarrow$ то $\mathcal{F}$ совп. с мн-ом корней многочлена из $\mathbb{Z}_p[x]$

[K, $f(x)$, корни $f(x) \subset \underset{min}{L}$ | $K \subset L \Rightarrow L$ - поле разл. для $f(x)$]

Следовательно $\mathcal{F}$ - поле разл. $x^{p^n} = x$ над $\mathbb{Z}_p$ и оно задается мн-ом однозначно

3) Пусть L - поле разл. мн-на $x^{p^n} = x$ над $\mathbb{Z}_p$

$$\mathcal{F} = \left\{ \alpha \in L \mid \alpha^{p^n} = \alpha \right\}$$

Тогда $\mathcal{F}$ - подполе в L.

Действительно, $\mathrm{char} L = p$ и поэтому $(\alpha \pm \beta)^p = \alpha^p \pm \beta^p$ (*)

$(\alpha\beta)^p = \alpha^p \beta^p$

$(\alpha/\beta)^p = \alpha^p/\beta^p$

$(\alpha \pm \beta)^p = \sum \binom{p}{k} \alpha^k \beta^{p-k}$;

$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\dots(p-k+1)}{k!} \Rightarrow p \mid \binom{p}{k} \Rightarrow \binom{p}{k} = 0$ в поле L

Автоморфизм Фробениуса

Если $\alpha^{p^n} = \alpha$ $\beta^{p^n} = \beta \Rightarrow (\alpha \pm \beta)^{p^n} \underset{(*)}{=} \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$

$(\alpha \cdot \beta)^{p^n} = \alpha \cdot \beta$, как и частное

Таким образом:

+	−	·	÷	-1	0	1

→ замкнутость $\Rightarrow$ $\Rightarrow \mathcal{F}$ - подполе

Т.к. L - поле разл. $x^{p^\alpha} = x$ $p : L = F$

Осталось найти число эл-ов $|\mathcal{F}|$ мн-ва $x^{p^n} = x$ взаимн. с пр-ой $(x^{p^n} - x)' = \underbrace{p^n}_{0} \cdot x^{p^n-1} - 1 = -1$ (const)

// если мн-н $\perp$ пр-ой $\Rightarrow$ все корни различны $\Rightarrow$ $\Rightarrow x^{p^n} - x$ не имеет кр. корней и их число p^n $\Rightarrow |\mathcal{F}| = p^n$

Теор. Доказана

ПОЛЕ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА

ТЕОРЕМА: $\forall$ K - пр-е поле $f(x)$ - мн-н над $K[x]$ ст $f(x) \geq 1$ $\Rightarrow$ $\exists$ поле F со св-ми:

а) $F \supset K$ как подполе
б) F сод-т все корни $f(x)$
в) F - min соотв а) и б)

св-ми а, б, в поле F опр. однозначно (с т. до $\simeq$) - это "поле разл. мн-на $f(x)$ над полем K"

доказ-во: 1) '$\exists$ мн' - индукция по ст. (n)

$n=1$: $F=K$

$n>1$: Тогда $f(x)$ разл в пр-ве нер. мн-б над K ? способом выберем $p(x)$ над $K[x]$ | $p(x)$ неразл. в $K[x]$, $p(x) \mid f(x)$

{ по теор. Кронекера $\exists$! мн L | $L \supset K$, $L \ni \alpha$ и L min

теперь можно в кольце $L[x]$ $(x-\alpha) \mid p(x) \Rightarrow (x-\alpha) \mid f(x)$

пусть $g(x) = \frac{f(x)}{x-\alpha} \in L[x]$

ст. $g(x) = n-1$

по пред.-ию над $\exists$ поле F со св-ми:

$$\begin{cases} F \supset L \text{ как подполе} \\ F \supset \text{все корни } g(x) \\ F - \min \end{cases}$$

$$\Rightarrow \begin{cases} F \supset K \text{ как подполе} \\ F \supset \text{все корни } f(x) \\ F - \min \end{cases}$$

2) '!-ость' Факторизуем $p(x) \mid f(x)$ $p(x)$ - неразложимый

K, $p(x) \Rightarrow L$, $\frac{f(x)}{p(x)(x-\alpha)}$ инд. $\Rightarrow F$!

Время F, в нем есть K, и F будет делитель $p(x) \Rightarrow$ есть α

$L = (K, \alpha)$ - одн-но по инд. стр-ю F.

ПОДПОЛЯ КОНЕЧНЫХ ПОЛЕЙ

ТЕОРЕМА: $F_{p^d} \leq F_{p^n} \Leftrightarrow d \mid n$

нужна ЛЕММА 1: $X^k - 1 \mid X^n - 1 \Leftrightarrow k \mid n$ в $\mathbb{Z}[x]$

Доказат-во: пусть $n = kq + r$, $r < k$ $\Rightarrow$

$$X^n - 1 = X^{kq+r} - 1 = X^{kq+r} - X^r + X^r - 1$$

$= x^r[(x^k)^q - 1] + x^r - 1$, т.к. $a^q - 1 = (a-1)(a^{q-1} + a^{q-2} + \dots + 1) \Rightarrow$

$\Rightarrow$ при $a = x^k$ получаем

$$x^n - 1 = (x^k - 1)\,Q(x) + x^r - 1 \qquad Q(x) \in \mathbb{Z}[x]$$

$$x^k - 1 \mid x^n - 1 \iff r = 0 \iff r \mid n$$

лемма 2 $\forall$ p (нечетн.) простое число $\Rightarrow$

$$p^k - 1 \mid p^n - 1 \iff k \mid n$$

док-во: по лемме 1 (при $x = p$): $p^n - 1 = (p^k - 1)\underbrace{Q(p)}_{\in \mathbb{Z}} + p^r - 1 \Rightarrow$

пусть: $0 \le p^r - 1 < p^k - 1$

отсюда: $p^k - 1 \mid p^n - 1 \Rightarrow p^r - 1 = 0 \Rightarrow r = 0 \Rightarrow k \mid n$

док-во теоремы

По теореме о конечных полях, поле порядка p^k совпадает с полем корней мн-на $x^{p^k} - x$ над $\mathbb{F}_p$

тогда $\mathbb{F}_{p^k} \le \mathbb{F}_{p^n} \iff x^{p^k} - x \mid x^{p^n} - x \iff$

$\iff x^{p^k - 1} - 1 \mid x^{p^n - 1} - 1$ (по лемме 1)

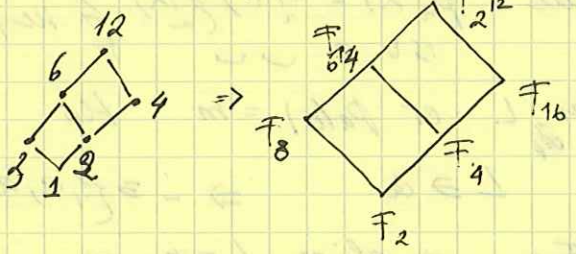
$\iff p^k - 1 \mid p^n - 1 \iff$ по л. 2 $\iff k \mid n$

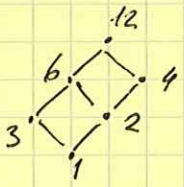
ч.т.д.

ПРИМЕР Найдем реш. подполей поля $\mathbb{F}_{2^{12}}$: Имеем.

$$\mathbb{F}_{2^k} \le \mathbb{F}_{2^{12}} \iff k \mid 12$$

решётка подполей собств. с реш. делителей числа 12.





ЧИСЛО НЕРАЗЛОЖИМЫХ, НОРМИРОВАННЫХ МНОГОЧЛЕНОВ СТ. n НАД $\mathbb{Z}_p$ (ННМ)

ТЕОРЕМА N_n – число н.нм ст. n над $\mathbb{Z}_p$ равно:

$$N_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$$

доказательство:

нужна:

ЛЕММА Для $\forall n \in \mathbb{N}$ $\exists$ неразл. норм. мн-н ст. n с коэфф. из $\mathbb{Z}_p$

док-во: Пусть $\mathbb{F}_{p^n}$ – поле порядка p^n, оно $\exists$ по теор о конечных полях, его мульт. гр. циклическая

$$\mathbb{F}_{p^n}^* = \langle a \rangle \quad , a \in \mathbb{F}_{p^n}^* \; a \neq 0$$

Пусть $P_a(x)$ – норм. мн-н наим. степени с коэффициентами из $\mathbb{Z}_p = \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$, аннулирующий эл-т a.

Так как $\mathbb{F}_{p^n}$ – бин. пр-во разм. n над $\mathbb{Z}_p$

То система $1, a, a^2 \dots a^n$ – л.з. над $\mathbb{Z}_p$

$\Rightarrow \exists \alpha_0 \alpha_1 \dots \alpha_n$ (не все $= 0$) $\alpha_0 \cdot 1 + \alpha_1 a + \dots + \alpha_n a^n = 0$ $\exists \alpha_i \neq 0$

мн-н $\alpha_0 + \alpha_1 x + \dots \alpha_n a^n$ аннулирует эл-т a отличен от 0.

Тогда $\deg P_a(x) \leq n$, если $\deg P_a(x) = n = m < n$ то по лемм Кронекера можно утв, $\exists$ поле $L \supset \mathbb{Z}_p$ $L \ni a$ и $L(a) = 0$ L min (поскольку $P_a(x)$ – неразложим над $\mathbb{Z}_p$

// если $P_a(x) = P_1(x) P_2(x)$ не разл.

$\deg$ = ∪ ∪ ∨

$\dim_{\mathbb{Z}_p} L = \deg P_a(x) = m$ т.о

$L \ni a \Rightarrow L \ni \{1, a, a^2 \dots\} = \mathbb{F}_{p^n}^*$

$L \supseteq \mathbb{F}_{p^n}$, $\Rightarrow \dim_{\mathbb{Z}_p} L = n$ →

$\Rightarrow \deg P_a(x) = n$