Звездочками помечены задачи, которые мы еще будем проходить, их делать не нужно.

Домашнее задание

1. Найдите порядок элементов α и $2\alpha - 1$ в поле $\mathbb{F}[\alpha]$, где α корень многочлена $x^2 + 3x + 3$.

2. Для кольца $\mathbb{k} = \mathbb{F}_5[\alpha]$, где α — корень многочлена $x^3 + 3x - 2$ выполните задания:

а) Докажите, что $\mathbb{k}$ — поле.

***б) Найдите порядок элемента $\alpha^2 + 2$ и его минимальный многочлен.

***в) Найдите все корни многочлена $x^3 + 3x - 2$.

г) Найдите $(\alpha + 3)^{-1}$.

3. Постройте поле из 49 элементов и найдите в нем элемент порядка

а) 3, б) 4, в) 6.

Задачу можно сильно упростить, выбрав «удобный» многочлен для построения поля.

4. ***В поле $\mathbb{F}_2[\alpha]$, где α — корень многочлена $p(x) = x^4 + x + 1$, найдите минимальный многочлен элемента $\alpha^3 + 1$ и все его корни.

5. Докажите, что $\mathbb{F}_5[x]/(x+2) \cong \mathbb{F}_5$.

6. Найдите мультипликативную группу и идемпотенты кольца $\mathbb{F}_2[\alpha]$, где α — корень многочлена $x^3 + 1$.

7. Найдите порядок мультипликативной группы кольца $\mathbb{F}_3[\alpha]$, где α — корень многочлена $x^3 + x + 1$

8. ***Рассмотрим отображение $\varphi : \mathbb{F}_3[x] \to GL(2, \mathbb{F}_3)$, заданное так:

$$\varphi(p) = p\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$$

Докажите, что $Im(\varphi)$ — поле.

9. Определите количество неприводимых многочленов второй степени над $\mathbb{F}_p$, где:

а) $p = 2$,

$\mathbb{F}_{11}$ 1, 2, 5, 10

б) $p = 3$,

в) p — произвольное простое число.

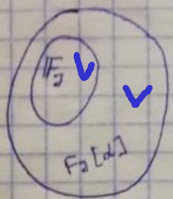
10. Постройте поле $\Bbbk$, не содержащее подполей, в котором существует элемент t порядка 5. Найдите этот элемент.

11. Постройте поле $\Bbbk$, содержащее одно подполе $\mathbb{L}$ и элемент $t \notin \mathbb{L}$ порядка 4. Найдите этот элемент.

12. Постройте поле $\Bbbk$, содержащее более одного подполя и элемент t порядка 5, не содержащийся ни в одном подполе. Найдите этот элемент.

13. ***Найдите все корни многочлена x^2+3x+1, принадлежащие $GL(2, \mathbb{F}_7)$.

$\mathbb{F}_7[x]/(x^2+1) = \mathbb{F}_7[\alpha]$, где α — корень x^2+1



$\alpha^2 = -1$

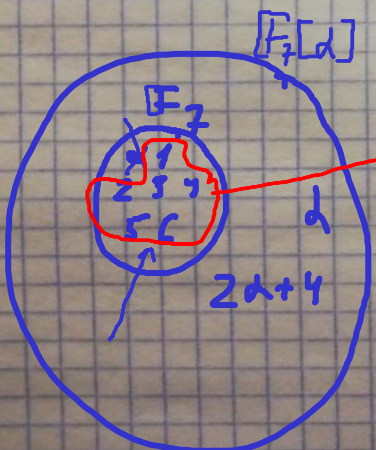
$\alpha^4 = 1 \Rightarrow \operatorname{ord}\alpha = 4$

Порядки $\mathbb{F}_7[\alpha]$: 1, 2, 3, 4, 6, 8, 12, 16, 48, 24

Порядки $\mathbb{F}_7$: 1, 2, 3, ~~4~~, ~~5~~, 6

$2^3 = 1$

$3^6 = 1$

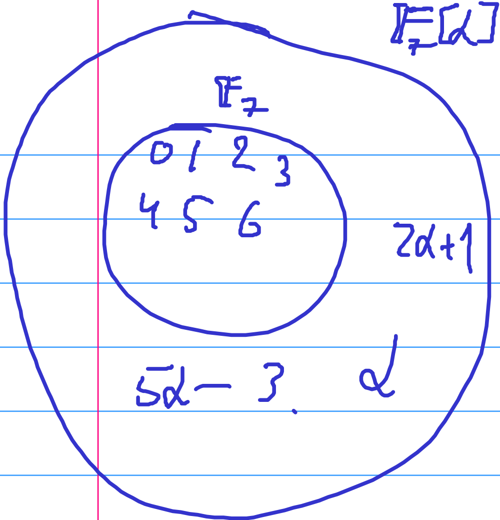


$t^6 = 1$

$t^6 - 1$

$t^{p-1} \equiv 1 \pmod p$

$\alpha^2+1=0$



$\mathbb{K}, V$

$\mathbb{K} \times V \to V$

$\mathbb{K} = \mathbb{F}_7$

$\boxed{V} = \mathbb{F}_7[\alpha]$

2

$1, \alpha$ — базис.

$\mathbb{C} = \mathbb{R}[i]$

$i^2+1=0$

$$\mathbb{F}_5[x] \big/ (x+2) \cong \mathbb{F}_5$$

$A \xrightarrow{\varphi} B$ $\qquad$ $A / \ker\varphi \cong \operatorname{Im}\varphi$

$A = ?$ $\qquad$ φ — ?

$\ker\varphi = (x+2)$

$\operatorname{Im}\varphi = \mathbb{F}_5$

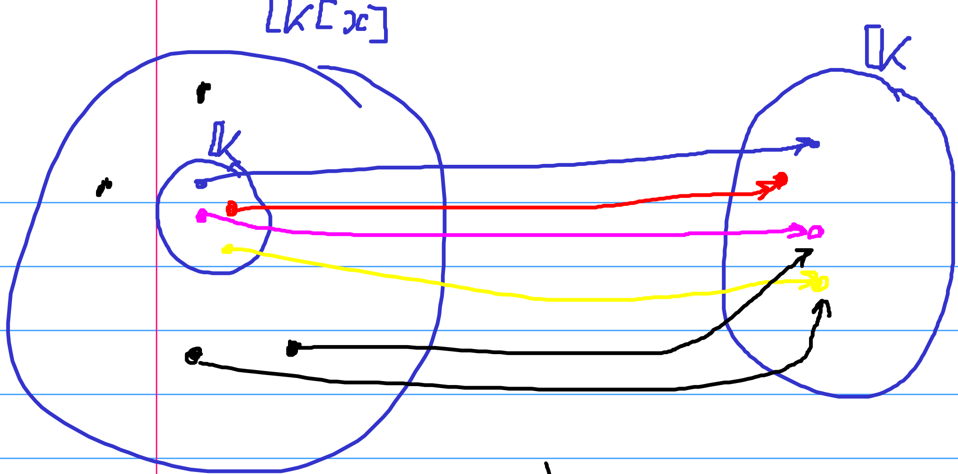
$A = \mathbb{F}_5[x]$ $\qquad$ $\varphi(u(x)) = u(3)$

$\ker\varphi = \{ f(x)\,(x+2) \} = (x+2)$.

$\mathbb{K}[x]$ $\qquad$ $\varphi(u(x)) = u(a)$

$a \in \mathbb{K}$

$\mathbb{K} \xrightarrow{\varphi} \mathbb{K}, \ \varphi = \mathrm{Id}$



$$7(5) = 7$$

$\mathbb{F}_2[\alpha]$, α – корень $x^3+1=\underline{(x+1)}\,\underline{(x^2+x+1)}$

$$\boxed{\alpha^3 = -1.}$$

$$\mathbb{F}_2[\alpha] = \underset{1}{\mathbb{F}_2[\beta]} \times \underset{3}{\mathbb{F}_2[\gamma]}, \quad \begin{array}{l} \beta+1=0 \\ \underline{\gamma^2+\gamma+1=0} \end{array}$$

$$\left|\mathbb{F}_2[\alpha]^*\right| = 1\cdot 3 = 3$$

$$\alpha^3 = 1 \Rightarrow \boxed{\alpha\cdot\alpha^2 = 1}$$

$$(\alpha+1)t(\alpha) + (\alpha^2+\alpha+1)u(\alpha) = 1.$$

$$t(\alpha) = \alpha \qquad u(\alpha) = 1$$

$$(\alpha+1)\alpha = e_1 \qquad (\alpha^2+\alpha+1) = e_2$$

$$\mathbb{F}_3[x]/(x^3+x+1) \cong$$

$$x^3+x+1 = (x-1)(x^2+x+2)$$

$$\cong \underbrace{\mathbb{F}_3[x]/(x-1)}_{\text{поле из 3 эл}} \times \underbrace{\mathbb{F}_3[x]/(x^2+x+2)}_{\text{поле из 9 эл.}}$$

2 обр   8 обр

(a, b)

$$2 \times 8 = \boxed{16}$$

№ 9.8) Всего многочленов II ст:

$p^3 - p^2$

Всего одночленов I степени: с. 1 перед x

$x + a \sim p$

$x^2 + ax + b$ p штук

попарных произв. I степени

$(p-1)p^2$

$C_p^2 = \frac{p!}{2!(p-2)!}$ — перед x стоит 1

$(x-a)(x-b)$ домножим $C_p^2 \cdot (p-1)$

$a \neq b$. еще надо учесть элементы вида

$C_p^2 + p$ x^2; $(x+1)^2$ ... — их всего $p \cdot (p-1)$

$$\boxed{p^3 - p^2 - C_p^2(p-1) - (p^2 - p)}$$

$p = 2$: $4 - 1 - 2 = 1$

$p = 3$: $18 - 3 \cdot 2 - 6 = 6$

$x^2 + ax + b$.

$$\boxed{\frac{p(p-1)}{2} + p}$$

приб.

$\mathbb{F}_5$: $(x+1)^2 = x^2 + 2x + 1$

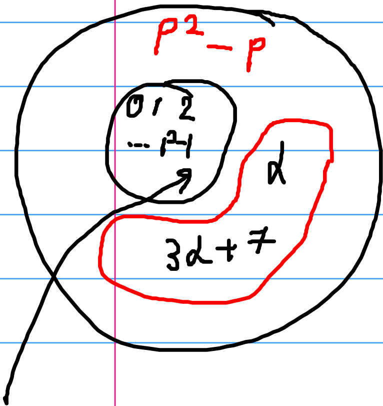
$(x+4)^2 = x^2 + 3x + 1$

$$p^2 - \frac{p^2 - p + 2p}{2} = \frac{2p^2 - p^2 - p}{2} =$$

$$= \boxed{\frac{p^2 - p}{2}} \; C_p^2$$

непр. мн-н степени 2 над $\mathbb{F}_p$.

$\mathbb{F}_p[\alpha]$ α — корень непр мн-на степени 2 $u(x)$



$$|\mathbb{F}_p[\alpha]| = p^2$$

$a\alpha + b,\quad a, b \in \mathbb{F}_p$

$$t \in \mathbb{F}_p[\alpha] \setminus \mathbb{F}_p$$

$$\mathbb{F}_p[\alpha]^* = \{1, t, t^2, t^3, \dots\}$$

$$|\mathbb{F}_p[\alpha]^*| = p^2 - 1$$

т.к. p^2-1 — порядок м.г. $\Rightarrow$ любой эл-т в степени p^2-1 равен 1. $\Rightarrow$ все они являются корнями многочлена

$$x^{p^2-1} - 1 = (x-1)(x-2)\dots(x-(p-1))(x-\alpha)\dots$$

$$\frac{p^2-p}{2} = C_p^2$$

11. $\mathbb{F}_3[x]/(x^2+1)$

$\alpha^2=2$

$\alpha^4=1$

$a\alpha+b$

$1, \alpha$

$\mathbb{F}_3[\alpha] \quad \alpha^2+1=0$

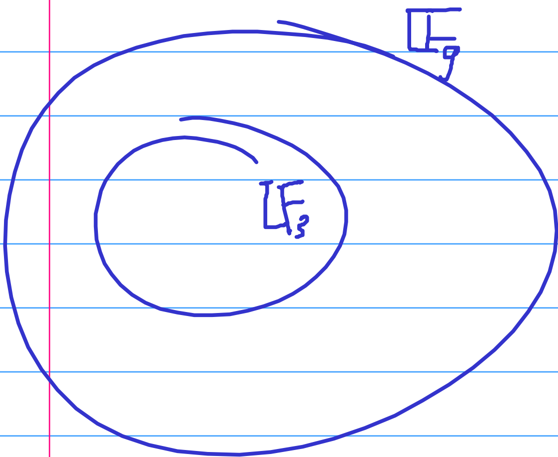
$\alpha^2=-1$

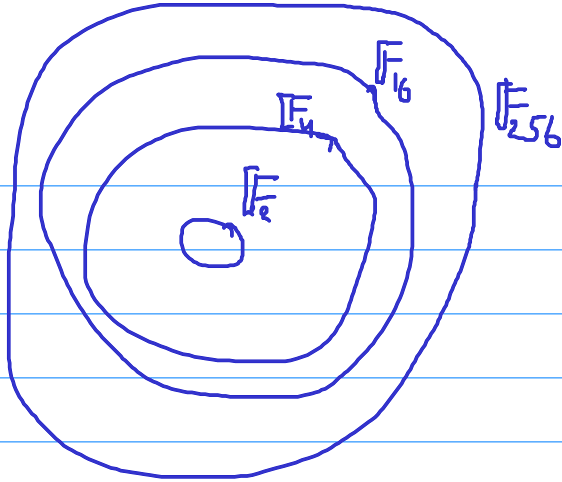
$\alpha^4=1.$

$|\mathbb{K}^*|$ делит 8

$|\mathbb{K}^*| = 1, \cancel{2}, 4, \cancel{8}$

$\cancel{\mathbb{F}_2} \quad \mathbb{F}_3 \quad \cancel{\mathbb{F}_5} \quad \mathbb{F}_9$





$\mathbb{F}_{16}$
$\mathbb{F}_4$
$\mathbb{F}_2$
$\mathbb{F}_{256}$

$\mathbb{K} \supset \mathbb{L} \supset \mathbb{P}$
$\uparrow$
a, ord $a = 5$

p^n

$p = 2^4 = 16$

$\mathbb{F}_{16}$ — ? 15

Строим поле из 4 эл-та

$\mathbb{F}_2[\alpha]$, $\boxed{\alpha^2+\alpha+1=0}$ $= \mathbb{F}_4$

Строим поле из 16 эл-тов

$\underbrace{\mathbb{F}_4[\beta]}$

$x^2 + ax + b$
$a, b \in \mathbb{F}_4$

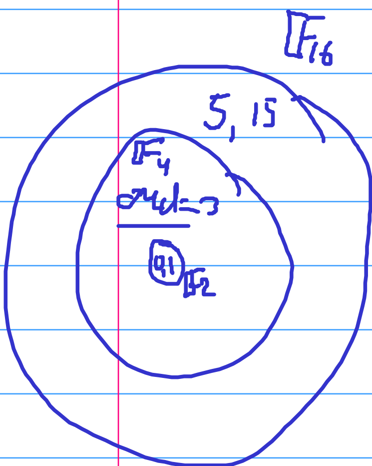
$\boxed{x^2 + \alpha x + 1}$

$0 \Rightarrow 1$
$1 \to \alpha$

$\alpha \Rightarrow \cancel{\alpha^2} + \cancel{\alpha^2} + 1 = 1$

$\alpha + 1 \Rightarrow (\alpha+1)^2 + \alpha(\alpha+1) + 1 =$
$= \cancel{\alpha^2+1} + \cancel{\alpha^2} + \alpha + \cancel{1} = \alpha$

$\beta^2 + \alpha\beta + 1 = 0$
$\underbrace{\beta^2 = \alpha\beta + 1}$



$\beta^3 = \beta(\alpha\beta + 1) =$
$= \alpha\beta^2 + \beta =$
$\alpha(\alpha\beta + 1) + \beta =$
$= \alpha^2\beta + \alpha + \beta =$
$= (\alpha+1)\beta + \alpha + \beta =$
$= \underbrace{\alpha\beta + \alpha}$

$\mathbb{F}_2[\alpha]$ $\alpha^4 + \alpha + 1 = 0$

$\mathbb{F}_{16} : \mathbb{F}_2$

4

$1, \alpha, \beta, \alpha\beta$

$\mathbb{F}_{16} = \mathbb{F}_4[\beta]$ $\quad \beta^2 = \alpha\beta + 1$

$\mathbb{F}_4 = \mathbb{F}[\alpha],\ \alpha^2 = \alpha + 1$

$\alpha \quad \alpha + 1$

$\mathbb{F}_2$

$0 \quad 1$

β

$\beta + 1$

$\beta + \alpha$

$\alpha\beta$

$\alpha\beta + 1$

$\alpha\beta + \alpha$

$\alpha\beta + \alpha + 1$

$\beta + \alpha + 1$

$\alpha\beta + \beta + 1$

$\alpha\beta + \beta$

$\alpha\beta + \alpha + \beta$

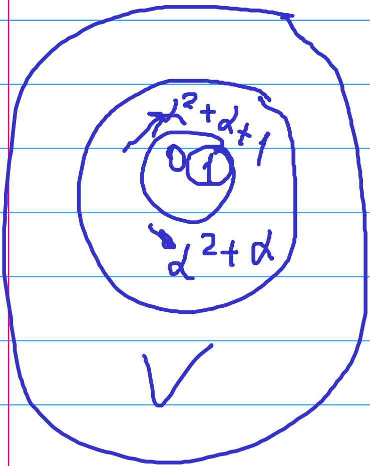
$\alpha\beta + \alpha + \beta + 1$

$\boxed{a\alpha\beta + b\alpha + c\beta + d}$

$\Sigma, \alpha^5 \beta^{10} \ldots\ldots$

$\mathbb{F}_2[\alpha]$ $\quad \alpha^4=\alpha+1$ $\qquad$ 5, 15

$$\alpha^5 = \boxed{\alpha^2+\alpha.}$$



$$\alpha^{15}=1$$

$$(\alpha^5)^3=1$$

$\mathbb{F}_5[\alpha]$ $\qquad \alpha^3+3\alpha-2=0 \qquad \alpha^3=2\alpha+2$

$x^3+3x-2.$

$$\Phi(t)=t^5$$

<u>α — корень</u>, <u>$\Phi(\alpha)$ — тоже</u>, <u>$\Phi(\Phi(\alpha))$ — тоже</u>

$$\Phi(at)=a^5t^5=at^5=a\,\Phi(t)$$

$a\in\mathbb{F}_5$ $\qquad \Phi(u+v)=(u+v)^5=u^5+v^5=\Phi(u)+\Phi(v)$

$$\Phi(\alpha^3+3\alpha-2)=\Phi(0)=0$$

$$\Phi(\alpha^3)+3\Phi(\alpha)-\Phi(2)=0$$

$$(\Phi(\alpha))^3+3\Phi(\alpha)-2=0$$

x^3+3x-2

$\alpha,\ \alpha^5,\ (\alpha^5)^5$

$\alpha^5 = \alpha^2\alpha^3 = \alpha^2(2\alpha+2) = 2(\alpha^3+\alpha^2) = 2(2\alpha+2+\alpha^2)$

$= 2\alpha^2 - \alpha - 1$