5) n - просто $\Rightarrow \mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{\bar{0}\}$

$\bar{x}^2 = \bar{1}$ за $x = \bar{1}$ или $x = -\bar{1}$

$\Leftrightarrow n \mid (x^2 - 1)$

- Единствения елемент от ред 2 е -1

$(\overline{n-1})! = \bar{1} \cdot \bar{2} \cdot \ldots \cdot (\overline{n-1}) = \bar{1} \pmod{n}$

- Останалите ел. от $\bar{2}$ -- $\overline{n-2}$ са > 2 $\Rightarrow$ нито един от тях не съвпада със своя обратен.

- Множ. се разбива на двойки (ел. нетривия обратен, ел. нейн обратен, ...)

$\bar{1} \cdot \bar{3} \cdot \bar{4} \cdot \ldots \cdot (\overline{n-2}) = \bar{1} \pmod{n}$

Т-ма на Уилсън $(n-1)! \equiv -1 \pmod{n}$ - само за n-просто.

Т-ва: Нека $K \subset M$ и M - крайни

$K < M \Leftrightarrow$ { (1) $a - b \in K, \forall a, b \in K$; (2) $ab \in K, \forall a, b \in K$

2 к.:

Ако са изпълнени (1) и (2), от (1) $\Rightarrow K$ подгрупа на $(M, +)$

(2) $\Rightarrow$ "$\cdot$" е бинарна за K.

10.

Опр: Характерист. на тяло: Нека F - тяло. Казваме, че F има характеристика $k \neq 0$ (записваме $\mathrm{char}\, F = k$) ако k е най-малкото естествено число, за което k - кратното на 1 е равно на 0. (т.е. $k1 = \underbrace{1 + 1 + \ldots + 1}_{k} = 0$) и казваме че $\mathrm{char}\, F = 0$, ако $\forall k \in \mathbb{N}$: $k1 = \overbrace{1 + \ldots + 1}^{k} \neq 0$

Забележка: k - характеристика е реда на единицата разглеждана като елемент на адитивната група?

Т-ма: (Характеристика на всяко тяло е просто число или 0) $\equiv$ F - тяло $\Rightarrow \mathrm{char}\, F$ е или 0 или просто число.

→ (съставно число m)

Док: // Допускаме, че $\operatorname{char} F = m = k \cdot s$ $(k > 1, s > 1)$ $(k < m,\ s < m)$

Това означава: $\Rightarrow 0 = m1 = ks1 = \underbrace{1+1+\dots+1}_{k \cdot s} = \underbrace{(1+\dots+1)}_{s} + \dots + \underbrace{(1+\dots+1)}_{s} =$ (k пъти)

$= \underbrace{s1 + s1 + \dots + s1}_{k} = (k1)(s1) = \underbrace{(1+1+\dots+1)}_{k=a}\underbrace{(1+\dots+1)}_{s=b} = \underbrace{1(s1) + 1(s1) + \dots + 1(s1)}_{k}$

$\Rightarrow 0 = a \cdot b$ и $a \neq 0, b \neq 0$

$(k < m \Rightarrow k1 \neq 0) \Rightarrow a, b$ са делители на 0.

$a, b \in F$ - поле $\Rightarrow a, b$ - обратими (!) $\Rightarrow$ b участва в ед. умножение с $\Rightarrow$ чие е очит просто число. хем съставен хем обратен.

Опр. Просто поле Полето F - се нарича просто ако няма собствени подполета.

Кр за просто поле: $\forall p \ \bar{m} = \underbrace{\bar{1} + \bar{1} + \dots + \bar{1}}_{m}$ p-просто $\}$

Тв $K \subset F$ и F-поле то K-подполе $\Leftrightarrow$ $\begin{cases} (1)\ a - b \in K \\ (2)\ ab \in K \\ (3)\ a^{-1} \in K \ \forall a \neq 0, a \in K \end{cases}$

Свойство Ако F-поле и $\bigcap F_i = T$ - просто поле F_i - подполета на F

↳**Следствие** Всяко поле съдържа единствено просто подполе

Опред. за Изоморфизъм F_1, F_2 - полета. Казваме че $F_1 \cong F_2$ когато $\exists \varphi : F_1 \to F_2$ със свойства: 1) $\varphi(a+b) = \varphi(a) + \varphi(b)$

2) $\varphi(ab) = \varphi(a)\varphi(b)$

$\Rightarrow \varphi$ - изоморфизъм и F_1, F_2 - изоморфни полета. 3) φ - биекция $\Rightarrow$

Тв Ако F-просто поле тогава:

а) ако $\operatorname{char} F = p \Rightarrow F \cong \mathbb{Z}_p$

б) ако $\operatorname{char} F = 0 \Rightarrow F \cong \mathbb{Q}$

Док: //

а) $\operatorname{char} F = p$ → означава, че $0, 1, 1+1, 3 \cdot 1, \dots (p-1)1$ → различни ел. в F (разлагаме четно себе)

$\varphi : \mathbb{Z}_p \to F$, $\varphi(\bar{a}) = a \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{a}$ $\boxed{p1 = 0}$

от опр. за полета

(1) $\varphi(\bar{a} + \bar{b}) = \varphi(\bar{r}) = \underbrace{1+\dots+1}_{r} = \underbrace{1+\dots+1}_{r} + \underbrace{1+\dots+1}_{sp=0} = (sp + r)1 = a + b =$

$\bar{a} + \bar{b} = \bar{r}$, $r \equiv a + b \pmod p$

$\lrcorner sp = a + b$

$= a1 + b1 = \varphi(\bar{a}) + \varphi(\bar{b})$

в) $\varphi(\bar{a}\bar{b}) = \varphi(\bar{r}_1) = (r_1 1 = r_1 1 + pk\,1 = (r_1 + pk)1 = (ab)1 = (a1)(b1) = \varphi(\bar{a})\cdot\varphi(\bar{b})$

$\bar{r}_1 = \bar{a}\bar{b}$, $r_1 \equiv ab \pmod p$ $\quad ab = r_1 + pk$

Нека $F_1 = \varphi(\mathbb{Z}_p) = \{0, 1, 2\cdot 1, 3\cdot 1, \ldots (p-1)1\}$

Ще док. че F_1 е тяло:

- $a1 + b1 = (a+b)1 = (r+ps)1 = r1 + \underbrace{s(p1)}_{=0} = r1 \in F_1$

  $a+b = r+ps$, $0 \le r < p$

- $a1 \cdot b1 = (ab)1 = (r_1 + kp)1 = r_1 1 + \underbrace{k(p1)}_{=0} = r_1 1 \in F_1$

  $ab = r_1 + kp$

ако $0 \le a < p$

$a\cdot 1 + (p-a)1 = p\cdot 1 = 0$

$a1 \neq 0 \Rightarrow (a, p) = 1$ | от ун. Безу | $= ua + vp$

$1 \cdot 1 = (u1)(a1) + \underbrace{(v1)(p1)}_{=0}$

$1 = (u1)(a1) \Rightarrow (u1) = (a1)^{-1}$

$\Rightarrow F_1$ - поле (тяло от F - (у)простО поле, щото съдържа $\mathbb{Z}_p$)

$\Rightarrow F_1 = F = \varphi(\mathbb{Z}_p) \Rightarrow \varphi$ - сюрекция

$\Rightarrow \varphi$ - изоморфизъм $\Rightarrow$ избр $F \cong \mathbb{Z}_p$

б) сл. $F = 0$ (колко ч-ла събираме 1 сам със себе си, щом ще се получи нулев ел)

$0, 1, 21, 31, \ldots, n1, \ldots$ - различни помежду си

$-1, 2(-1), \ldots$

$\{k1 \mid k \in \mathbb{Z}\}$ - тези ел са различни помежду си от аксиома 2 ↗ (равенството може да се докаже)

разглеждане: $(k1)(m1)^{-1} = \left(\frac{k}{m}\right)1 \neq 0$

$(k1)(m1)^{-1} = (s1)(t1) \iff (k1)(t1) = (s1)(m1)$

$\left(\frac{k}{m} = \frac{s}{t} \iff kt = ms\right)$

$\varphi: \mathbb{Q} \to F$

деф: $\varphi\left(\frac{k}{m}\right) = (k1)(m1)^{-1}$

- $\varphi\left(\frac{k}{m} + \frac{s}{e}\right) = \varphi\left(\frac{ke+sm}{me}\right) = (ke+sm)1 \cdot ((me)1)^{-1} =$

$= [(k1)(e1)) + (s1)(m1)](m1)^{-1}(e1)^{-1} = (k1)\underbrace{(e1)(m1)^{-1}(e1)^{-1}}_{1} + (s1)\underbrace{(m1)(m1)^{-1}}_{=1}(e1)^{-1} =$

$= (k1)(m1)^{-1} + (s1)(e1)^{-1} = \varphi\left(\frac{k}{m}\right) + \varphi\left(\frac{s}{e}\right)$

- аналогично $\varphi\left(\frac{k}{m}\cdot\frac{s}{e}\right) = \varphi\left(\frac{k}{m}\right)\cdot\varphi\left(\frac{s}{e}\right)$

Изоморф: $\frac{k}{m} \neq \frac{s}{e} \Leftrightarrow ke \neq sm \Leftrightarrow (k1)(e1) \neq (s1)(m1) \Leftrightarrow$

$\Leftrightarrow (k1)(m1)^{-1} \neq (s1)(e1)^{-1} \Leftrightarrow \varphi\left(\frac{k}{m}\right) \neq \varphi\left(\frac{s}{e}\right)$

сторекция: $F_1 = \varphi(\mathbb{Q}) = \{(k1)(s1)^{-1} \mid k \in \mathbb{Z}, s \in \mathbb{Z}, s \neq 0\}$

F_1 - поле $\Rightarrow F_1$ подполе на F - (просто)

$\Rightarrow F_1 = F \Rightarrow$ сторекция $\Rightarrow F \cong \mathbb{Q}$

Следствие: Ако F е поле тогава:

а) ако $\operatorname{char} F = p \Rightarrow \mathbb{Z}_p \cong F_1 \subset F$ (F - разширение на $\mathbb{Z}_p$)

б) ако $\operatorname{char} F = 0 \Rightarrow \mathbb{Q} \cong F_1 \subset F$ (F разширение на полето $\mathbb{Q}$)