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

$\bar{x}^2 = \bar{1} \Rightarrow \bar{x} \in \{\pm\bar{1}\} \equiv \{\bar{1}, \overline{n-1}\}$

$\Rightarrow$ единственият елемент от ред 2 е $\overline{-1}$.

$\Rightarrow (\overline{n-1})! = \bar{1}.\underbrace{\bar{2}.\ldots.\overline{n-1}}_{\text{редове} > 2} \equiv -1\,(n)$

Нито един от тях не съвпада с обратния си.

$\Rightarrow$ Можем да го разбием на двойки $(a, a^{-1}) \Rightarrow \bar{1}.\bar{3}.\ldots.\overline{(n-2)} = \bar{1}$

Т Теорема на Уилсън

За $\forall$ n - просто $\Rightarrow (n-1)! \equiv -1\,(n)$.

ТВ Нека $K \subset M$, M - пръстен.

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

Доказателство:

$\Leftarrow$) $a-b \in K \Rightarrow K$ е подгрупа на $(M,+)$.

$ab \in K \Rightarrow$ умножението е бинарна операция за K.

② и ③ са в сила за елементите на $M \Rightarrow$

$\Rightarrow$ и за елементите на K

$\Rightarrow K < M$.

$\Rightarrow$)

Поле. Характеристика на поле.

D Характеристика на поле F:

F има характеристика $k \neq 0$ ($\operatorname{char} F = k$), ако k е минималното естествено число, за което $k1 = \underbrace{1+\ldots+1}_{k\text{-пъти}} = 0$. $\operatorname{char} F = 0$, ако $\forall k \in \mathbb{N}$

$\Rightarrow k1 \neq 0$.

Забележка: $k = |1|$, $1 \in (F,+)$.

Т $\operatorname{char} F \in 0$ или просто число, за всяко поле F.

Доказателство:

Допускаме, че $\operatorname{char} F = m = ks$, $k>1$, $s>1 \Rightarrow 0 = m1 = ks1 =$

$= \underbrace{1+1+\ldots+1}_{k.s\text{ пъти}} = \underbrace{(1+\ldots+1)}_{s\text{ пъти}} + \ldots + \underbrace{(1+\ldots+1)}_{s\text{ пъти}} = \underbrace{s1+\ldots+s1}_{k\text{ пъти}} = (k1)(s1) = ab$

k пъти; a и b; $a,b \neq 0$

$k,s < m \Rightarrow ab = 0 \Rightarrow a,b$ - делители на 0

F - поле и $a,b \in F \Rightarrow$ обратими

↯

$\Rightarrow$ Имаме доказано, че в пръстен не може да е обратим и делител на 0, $\Rightarrow$ m- просто.

! За всяко просто число p има поне едно поле с char $=p$: $\mathbb{Z}_p$!

D Полето F се нарича просто, ако няма собствени подполета.

$\mathbb{Z}_p$ - взимаме 1 и събираме k пъти $\rightarrow$ можем да получим всички елементи на $\mathbb{Z}_p \Rightarrow \forall \mathbb{Z}_p$ за p-просто е просто поле.

Св-во Ако F поле и $\bigcap_{F_i<F} F_i = T$, то T е просто поле

Тв $K \subset F$, F - поле $\Rightarrow$ K - подполе $\Leftrightarrow$ 1) $a-b \in K$; 2) $ab \in K$; 3) $a^{-1} \in K$ $\Big\}$ $\forall a,b \in K$

С-я Всяко поле има единствено просто подполе.

D F_1 и F_2 - полета. $F_1 \cong F_2$ (изоморфни), когато $\exists \varphi: F_1 \to F_2$:

1) $\varphi(a+b) = \varphi(a) + \varphi(b)$;
2) $\varphi(ab) = \varphi(a)\varphi(b)$;
3) φ - биекция;

φ се нарича изоморфизъм.

T Ако F е просто поле, тогава:

А) ако char $F = p$, то $F \cong \mathbb{Z}_p$;

Б) ако char $F = 0$, то $F \cong \mathbb{Q}$;

Док-во:

А) char $F = p \Rightarrow 0, 1, 2.1, \ldots, (p-1).1$ - различни помежду си.

$\varphi: \mathbb{Z}_p \to F \to \varphi(\bar{a}) = a1 = \underbrace{1+\ldots+1}_{a}$

1) φ - инекция

2) $\varphi(\bar{a}+\bar{b}) = \varphi(\bar{r}) = \underbrace{1+\ldots+1}_{r} \overset{p1=0}{=} \underbrace{1+\ldots+1}_{r} + \underbrace{1+\ldots+1}_{sp} = (sp+r)1 = (a+b)1 =$

$\bar{r} \to r = a+b(p)$, $r = r+sp$

$= \underbrace{1+\ldots+1}_{a} + \underbrace{1+\ldots+1}_{b} = a1 + b1 = \varphi(\bar{a}) + \varphi(\bar{b})$

3) $\varphi(\bar{a}\bar{b}) = \varphi(\bar{r_1}) = \bar{r_1}.1 = \underbrace{1+\ldots+1}_{r_1} = \underbrace{1+\ldots+1}_{a} + \underbrace{1+\ldots+1}_{pk} = (r_1+pk)1 = (ab)1 =$

$\bar{r_1}$, $r_1 = ab(p)$, $ab = r_1 + pk$

$= (\underbrace{1+\ldots+1}_{a})(\underbrace{1+\ldots+1}_{b}) = \varphi(\bar{a}).\varphi(\bar{b})$

Нека $F_1 = \varphi(\mathbb{Z}_p) = \{0, 1, 2.1, \ldots (p-1).1\}$

$a1 + b1 = (a+b)1 = (r+ps)1 = r.1 + s(p1) = r1 \in F_1$

$a1.b1 = (ab)1 = (r_1+pk).1 = r_1.1 + k(p.1) = r_1 \in F_1$.

$0 < a < p$

$a1 + (p-a)1 = p.1 = 0 \in F_1$

$a1 \neq 0$ $(a,p) = 1 = ua + vp = u1a1 + v1p1 = u1a1 \Rightarrow u1 = (a1)^{-1}$

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

$\Rightarrow F \cong \mathbb{Z}_p$.

б) $\mathrm{char}\, F = 0$.

$0, 1, 2.1, \ldots n1 \ldots$
$-1, 2.(-1) \ldots$ } различни помежду си.

$(k1)(m1)^{-1} = (s1)(t1)^{-1} \Delta \Rightarrow k1 \cdot t1 = s1 \cdot m1$.

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

$\varphi(k/m) = k1 \cdot (m1)^{-1}$

$\varphi\left(\frac{k}{m} + \frac{s}{l}\right) = \varphi\left(\frac{kl+sm}{ml}\right) = (kl+sm)1 \cdot ((ml)1)^{-1} =$

$= (k1\, l1 + s1\, m1)(m1)^{-1}(l1)^{-1} = k1\, l1\, (m1)^{-1}(l1)^{-1} +$

$+ s1\, m1\, (m1)^{-1}(l1)^{-1} = k1(m1)^{-1} + s1(l1)^{-1} = \varphi(k/m) + \varphi(s/l)$

$\varphi\left(\frac{ks}{ml}\right)$ - аналогично доказателство

$\frac{k}{m} \neq \frac{s}{l} \Delta \Rightarrow kl \neq sm \Delta \Rightarrow k1\, l1 \neq s1\, m1 \Delta \Rightarrow k1(m1)^{-1} \neq s1(l1)^{-1}$

$\varphi(k/m) \neq \varphi(s/m)$ - инекция.

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

/аналогично/ $\to F_1 < F \Rightarrow F \equiv \varphi(\mathbb{Q}) \Rightarrow F \cong \mathbb{Q}$

С1 Ако F - поле, $\Rightarrow$ а) $\mathrm{char}\, F = p \Rightarrow \mathbb{Z}_p \cong F_1 < F$ // F е разширение на $\mathbb{Z}_p$

б) $\mathrm{char}\, F = 0 \Rightarrow \mathbb{Q} \cong F_1 < F$

Влагане на област на цялост в поле от частни

D Област на цялост - комутативен пръстен без делители на 0.

A - област на цялост

$A = \{0\}$

Зав.: $\frac{a}{b} = \frac{c}{d} \Delta \Rightarrow ad = bc$
в $\mathbb{Q}$

Разглеждаме множеството $B = \{(a,b) \mid a, b \in A, b \neq 0\}$

$(a,b) \sim (c,d) \Delta \Rightarrow ad = bc$

↳ релация - еквивалентност

1) $(a,b) \sim (c,d)$
2) $(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$ } от комутативност на A.
3) $(a,b) \sim (c,d)$ и $(c,d) \sim (k,m) \Rightarrow (a,b) \sim (k,m)$.

Док-во

$ad = bc \Rightarrow adm = bcm = bdk \Rightarrow adm - bdk = 0 \Rightarrow d(am - bk) = 0, d \neq 0$

$cm = dk$

$\Rightarrow am - bk = 0$, т.к. няма делители на нулата $\Rightarrow am = bk$.