Характеристика на поле. Основни свойства на полетата с ненулева характеристика.

Нека F е поле. Както доказахме при групите, в адитивната група на това поле е вярно равенството:

$(mn)\,a = m\,(na)$ (1)

за всяко $a \in F$ и всеки $m, n \in \mathbb{Q}$ равенството е доказано в мултипликативен вариант.

Твърдение 1: *Нека F е поле и* ***e*** *е единичният елемент на това поле. Тогава*

$na = (ne)a$ *, за всяко* $a \in F$ *и всяко* $n \in \mathbb{Z}$ (2)
$m.ne = (me)(ne)$ (3)

Доказателство:
Доказателство на (2)
Ако $n = 0$, равенството (2) е очевидно. Нека $n \neq 0$. Разглеждаме два случая:
сл.1) $n > 0$

$$na = \underbrace{a + a + ... + a}_{n-пъти} = \underbrace{ea + ea + ... + ea}_{n-пъти} = (\underbrace{e + e + ... + e}_{n-пъти})a = (ne)a$$

сл.2) $n < 0$. Нека $n' = -n$. Тогава

$$na = \underbrace{(-a) + (-a) + ... + (-a)}_{n'-пъти}, \qquad (*)$$

да забележим, че

$$a + (-e)a = ea + (-e)a = (e + (-e))a = 0.a = 0$$

следователно $-a = (-e)a$. Поради това от (*) получаваме

$$na = \underbrace{(-ea) + (-ea) + ... + (-ea)}_{n'-пъти} = \left(\underbrace{(-e) + (-e) + ... + (-e)}_{n'-пъти}\right)a = (ne)a,$$

тъй като по дефиниция $\underbrace{(-e) + (-e) + ... + (-e)}_{n'-пъти} = ne$

Доказателство на равенството (3)
От (1) имаме: $(mn)e = m(ne)$. Нека $ne = a$. Тогава $m(ne) = ma$. От (2) получаваме:
$ma = (me)a = (me)(ne)$.

Определение: *Нека F е поле и* $e \in F$ *е единичният елемент на това поле. Казваме, че полето F има характеристика нула, ако никое от кратните* $e, 2e, 3e, \ldots, ne, \ldots$ *на единичния елемент не е равно на нула, т.е., когато единичният елемент* e *има в адитивната група на полето безкраен ред. Казваме, че полето F иам крайна характеристика, ако за някое естествено число* n *имаме* $ne = 0$*. Най-малкото естествено число* n*, за което* $ne = 0$ *се нарича характеристика на полето F и се бележи с* $char(F)$*, т.е., ако F има крайна характеристика, тогава числото char(F) е реда на единичния елемент в адитивната група.*

Твърдение 2: *Ако F има крайна характеристика, тогава тя е просто число.*

Доакзателство:
Нека $char(F) = p$. Ако допуснем, че p е съставно, т.е. $p = p_1 p_2$, където $1 < p_1 < p$, $1 < p_2 < p$. Тогава имаме $0 = pe = (p_1 p_2)e$. Поради това от (3) получаваме $(p_1 e)(p_2 e) = 0$. От дефиницията на характеристиката следва $p_1 e \neq 0$ и $p_2 e \neq 0$. Получихме, че в полето има делител на нулата, което е противоречие.□

Примери:

1) В числовите полета (подполетата на **C**) характеристиката е равна на нула, защото кратните на единицата са различни от нула.
2) Разглеждаме факторпръстена $\boldsymbol{Z}_p = \boldsymbol{Z} / p\boldsymbol{Z}$. За този пръстен ще докажем:

Твърдение 3: *Ако* p *е просто число, тогава* $\boldsymbol{Z}_p$ *е поле, чиято характеристика е равна на* p.

Доказателство:
Ясно е, че $\boldsymbol{Z}_p$ е комутативен пръстен и този пръстен има единица (единицата е съседният клас $1+p\boldsymbol{Z}$). Поради това трябва да проверим, че всеки ненулев съседен клас, т.е всеки съседен клас, който е различен от идеала $p\boldsymbol{Z}$ е обратим. Нека $n + p\boldsymbol{Z} \neq p\,\boldsymbol{Z}$. Това означава, че n не се дели на p. Понеже p е просто $\Rightarrow (p, n) = 1$. Поради това $\exists u, v \in \boldsymbol{Z}$, такива, че $1 = un + vp$. От последното равенство следва

$$1 + p\boldsymbol{Z} = un + vp + p\boldsymbol{Z} = un + \underbrace{(vp + p\boldsymbol{Z})}_{p\boldsymbol{Z}} = un + p\boldsymbol{Z} = (u+p\boldsymbol{Z})(n+p\boldsymbol{Z}).$$

Следователно

$$1 + p\boldsymbol{Z} = (u + p\boldsymbol{Z})(n + p\boldsymbol{Z}).$$

От последното равенство става ясно, че съседният клас $n + p\boldsymbol{Z}$ е обратим. С това доказахме, че ако p е просто число $\boldsymbol{Z}_p$ е поле. В това поле имаме

$$\underbrace{(1 + p\boldsymbol{Z}) + (1 + p\boldsymbol{Z}) + \ldots + (1 + p\boldsymbol{Z})}_{p-\text{пъти}} = p(1+p\boldsymbol{Z}) = p + p\boldsymbol{Z} = p\boldsymbol{Z}$$ (нулевият елемент на $\boldsymbol{Z}_p$).

Следователно $char(\boldsymbol{Z}_p) \leq p$. Ако $k \in \boldsymbol{N}$ и $1 \leq k < p$, тогава $k(1+p\boldsymbol{Z}) = k + p\boldsymbol{Z}$. Понеже $k < p \Rightarrow k$ не се дели на p. Това означава, че $k + p\boldsymbol{Z} \neq p\boldsymbol{Z}$. С това изяснихме, че $char(\boldsymbol{Z}_p) = p$. □

Твърдение 3: *Нека F е поле и* $char(F) = p$. *Тогава* $pa = 0$ *за всяко* $a \in F$.

Доказателство:
Съгалсно равенството (2) имаме $pa = (pe)a$. Понеже $pe = 0$ следва $pa = 0$.

Твърдение 4: *Нека F е поле и char(**F**)=**p**. Ако **a** ≠ **0** имаме*
ma = 0 ⇔ *когато **p** дели **m**.*

Доказателство:

I) Нека $m = pm_1$, тогава $ma = (m_1 p)a = m_1(pa) = 0$, защото $pa = 0$.

II) Нека $ma = 0$. Нека $m = pq + r$, където $0 \le r < p$. Трябва да докажем, че $r = 0$. Да допуснем, че $r \neq 0$, тогава $ma = (pq + r)a = (pq)a + ra$. Понеже $ma = 0$ и $pa = 0$, следва, че $ra = 0$. Тъй като $r \neq 0$ и $r < p$ това противоречи на дефиницията на характеристиката на полето F.□

Твърдение 5: *Нека F е поле и char(F)=p. Тогава*

$$(a+b)^{p^k} = a^{p^k} + b^{p^k}, \text{ за } \forall a, b \in F \text{ и } k \in \mathbf{N}.$$

Доказателство:

Доказателството ще направим по индукция относно k.
База: k=1. Имаме

$$(a+b)^p = a^p + \underbrace{\binom{p}{1} a^{p-1}b + \ldots + \binom{p}{p-1} ab^{p-1}}_{\text{A}} + b^p$$

$\binom{p}{k}$ се дели на p, ако $1 \le k < p$. Следователно всеки от коефициентите в А се дели на p. Съгласно Твърдение 4 всяко от събираемите в А е равно на нула и следователно е вярно $(a+b)^p = a^p + b^p$. С това базата на индукцията е доказана.
Нека $k \ge 2$. Тогава

$$(a+b)^{p^k} = \left((a+b)^{p^{k-1}}\right)^p$$

Съгласно индуктивната хипотеза имаме

$$(a+b)^{p^{k-1}} = a^{p^{k-1}} + b^{p^{k-1}}$$

Следователно

$$(a+b)^{p^k} = \left(a^{p^{k-1}} + b^{p^{k-1}}\right)^p.$$

Като приложим към последното равенство базата на индукцията

$$(a+b)^{p^k} = \left(a^{p^{k-1}}\right)^p + \left(b^{p^{k-1}}\right)^p = a^{p^k} + b^{p^k}.\square$$

С последователно прилагане на Твърдение 5 получаваме:

Следствие: $(a_1 + a_2 + ... + a_s)^{p^k} = a_1^{p^k} + ... + a_s^{p^k}$

Ще докажем следната:

Теорема: *Нека F е поле и char(F)=p и* $\boldsymbol{e} \in F$ *е единичният елемент. Тогава цикличната подгрупа на адитивната група на F, породена от* $\boldsymbol{e}$ *е подполе на F, което е изоморфно на полето* $\boldsymbol{Z}_p$.

Доказателство:
Както знаем от лекцията за цикличните подгрупи, цикличната подгрупа породена от $\boldsymbol{e}$ е

$$F' = \{0, e, 2e, ..., (p-1)e\}$$

Също там изяснихме (в мултипликативен вариант), че

$$me \in F' \text{ за } \forall m \in \boldsymbol{Z} \qquad (*)$$

Знаем, че F' е подгрупа на адитивната група на полето F. Тъй като $\boldsymbol{e} \in F'$, то F' съдържа ненулев елемент. Поради това остава да проверим, че F' удовлетворява останалите две аксиоми за подполе. Нека $ke, se \in F'$, тогава съгласно равенството (3) имаме

$$(ke)(se) = (ks)(e)$$

От това равенство и (*) следва $(ks)(se) \in F'$, с което доказахме, че произведението на два елемента от F' също е елемент от F'. Остава да проверим, че обратният елемент на всеки ненулев елемент от F' също принадлежи на F'.

Нека $ke \in F'$ и $k \neq 0$, т.е. $1 \leq k \leq p-1$. Понеже характеристиката е просто число $\Rightarrow (p, k) = 1$ Поради това $\exists u, v \in \boldsymbol{Z}$ такива, че $1 = uk + pv$. С помощта на последното равенство и равенството (3) получаваме

$$e = 1e = (uk + pv)e = (uk)e + (pv)e = (uk)e = (ue)(ke)$$

И така

$$e = (ue)(ke).$$

Следователно (ke) е обратим и $(ke)^{-1} = ue$. Съгласно (*) $ue \in F' \Rightarrow (ke)^{-1} \in F'$, с което доказахме , че F' удовлетворява и последното изискване за поле.

Разглеждаме изображението

$$m \xrightarrow{\varphi} m\boldsymbol{e}, \ \forall m \in \boldsymbol{Z}$$

, където $\boldsymbol{e}$ е единичният елемент на F. Ясно е, че

$$\boldsymbol{Z} \xrightarrow{\varphi} F.$$

Имаме

$$a+b \xrightarrow{\varphi} (a+b)e = ae + be$$

и

$$ab \xrightarrow{\varphi} (ab)e = (ae)(be) \text{ (от (3))}$$

Следователно φ е хомоморфизъм на $\boldsymbol{Z}$ в полето F. От (*) става ясно, че $Im(\varphi)=F'$. Последното равенство означава, че φ е епиморфизм на $\boldsymbol{Z}$ върху F'. Съгласно Теоремата за епоморфизмите на пръстени имаме, че $\boldsymbol{Z/Ker(\varphi)}$ е изоморфен на F'. Ясно е, че

$$m \in Ker(\varphi) \Leftrightarrow me = 0$$

Поради това от Твърдение 4 следва, че $Ker(\varphi)=\boldsymbol{pZ}$, с което доказахме, че $\boldsymbol{Z/Z}_p$ е изоморфно на полето F'. Понеже $\boldsymbol{Z}_p = \boldsymbol{Z/Z}_p$ теоремата е доказана.□

С тази теорема изяснихме, че всяко поле, чиято характеристика е простото число $\boldsymbol{p}$, съдържа в себе си полето $\boldsymbol{Z}_p$ като подполе (в смисъл на този изоморфизъм). Поради това всяко поле с характеристика $\boldsymbol{p}$ може да се разглежда като разширение на полето $\boldsymbol{Z}_p$.