Charakteristika poľa

11. mája 2020

Charakteristika poľa

Grupová mocnina

$$a^n = \underbrace{a * a * \cdots * a}_{n\text{-krát}}$$

$$a^k * a^l = a^{k+l}$$

$$(a^m)^n = a^{mn}$$

Charakteristika poľa

$$n \times a = \underbrace{a + a + \cdots + a}_{n\text{-krát}}$$

- $0 \times a = 0$
- $(n+1) \times a = n \times a + a$
- Ak $n > 0$ tak definujeme $(-n) \times a = -(n \times a)$

$$k \times a + l \times a = (k + l) \times a$$
$$k \times (l \times a) = (kl) \times a$$
$$(k \times a)(l \times b) = (kl) \times (ab)$$

Charakteristika poľa

Definícia

Charakteristika poľa F je najmenšie prirodzené číslo $k > 0$ s vlastnosťou $k \times 1 = 0$. Označujeme ju $\mathrm{char}(F)$. Ak neexistuje k s uvedenou vlastnosťou, tak definujeme $\mathrm{char}(F) = \infty$.

$$\mathrm{char}\, F = \min\{k \in \mathbb{N}, k > 0; k \times 1 = 0\}$$

- $\mathrm{char}(\mathbb{Z}_p) = p$
- $\mathrm{char}(\mathbb{Q}) = \infty$

Charakteristika poľa

Lema

Každé konečné pole F má konečnú charakteristiku.

Tvrdenie

Charakteristika ľubovoľného poľa F je prvočíslo alebo ∞.

Najmenšie podpole

Tvrdenie

Nech F, F' sú polia a zobrazenie $\varphi\colon F \to F'$ je okruhový homomorfizmus. Potom buď $\varphi[F] = \{0\}$, alebo $\varphi[F]$ je podpole F', ktoré je izomorfné s F. (Inými slovami: zobrazenie φ je buď nulové alebo injektívne; čiže vnorenie – izomorfizmus na svoj obraz.)

Tvrdenie

Ak $\operatorname{char} F = \infty$, *tak existuje injektívny homomorfizmus z* $\mathbb{Q}$ *do* F.
Ak $\operatorname{char} F = p$ *pre nejaké prvočíslo* p, *tak existuje injektívny homomorfizmus zo* $\mathbb{Z}_p$ *do* F.

Nadpole ako vektorový priestor

Tvrdenie

Nech K, F sú polia a K je nadpole poľa F (t.j. $K \supseteq F$ a operácie na F sú zúženia operácií na K). Potom K je vektorový priestor nad poľom F (so sčitovaním a násobením skalárom rovnakým ako je sčitovanie a násobenie v K).

Dôsledok

Konečné pole charakteristiky p má p^n prvkov pre nejaké $n \in \mathbb{N}$.

Frobeniov homomorfizmus

Tvrdenie

Nech $\mathrm{char}(F) = p$ (p *je prvočíslo*). *Potom pre ľubovoľné* $a, b \in F$ *platí*

$$(a+b)^p = a^p + b^p$$
$$(ab)^p = a^p b^p$$

čiže zobrazenie $f : F \to F$, $f(x) = x^p$, *je homomorfizmus* (*endomorfizmus poľa* F).
Ďalej pre ľubovoľné $n \in \mathbb{N}$ *a* $q = p^n$ *máme*

$$(a+b)^q = a^q + b^q$$
$$(ab)^q = a^q b^q$$

Charakteristika poľa

Frobeniov homomorfizmus

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} \times a^k b^{p-k}.$$

$$\binom{p}{k} = \frac{p!}{k!(p-k!)}$$