

ЛЕКЦИЯ 28

ХАРАКТЕРИСТИКА НА ПОЛЕ. ОСНОВНИ СВОЙСТВА НА ПОЛЕТАТА С НЕНУЛЕВА ХАРАКТЕРИСТИКА.

Нека F е поле. Съгласно Лекция 21, в адитивната група на това поле са верни равенствата:

$$(mn)a = m(na), \quad \forall m, n \in \mathbb{Z} \text{ и } \forall a \in F \quad (1)$$

$$(m+n)a = ma + na, \quad \forall m, n \in \mathbb{Z} \text{ и } \forall a \in F \quad (1')$$

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

$$na = (ne)a, \quad \text{за всяко } a \in F \text{ и всяко } n \in \mathbb{Z}; \quad (2)$$

$$(m \cdot n)e = (me)(ne), \quad \forall m, n \in \mathbb{Z}. \quad (3)$$

Доказателство:

Доказателство на (2).

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

Сл.1) $n > 0$

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

Сл.2) $n < 0$. Нека $n' = -n$. Тогава

$$na = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n' \text{ пъти}}, \quad (*)$$

да забележим, че

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

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

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

тъй като по дефиниция

$$\underbrace{(-e) + (-e) + \dots + (-e)}_{n' \text{ пъти}} = ne$$

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 $e, 2e, 3e, \dots, ne, \dots$ на единичния елемент не е равно на нула, т. е., когато единичният елемент е има в адитивната група на полето безкраен ред. Казваме, че полето F има 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 $\text{char}(F)$, т. е., ако F има крайна характеристика, тогава числото $\text{char}(F)$ е равно на реда на единичния елемент в адитивната група.

Твърдение 2. Ако характеристиката на полето F е крайна, тогава тя е просто число.

Доказателство:

Нека $\text{char}(F) = p$. 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 F има делители на нулата, което е противоречие.

Примери.

1) В числовите полета (подполетата на \mathbb{C}) характеристиката е равна на нула, защото кратните на единицата са различни от нула.

2) Разглеждаме факторпръстен $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. За този пръстен ще докажем:

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

Доказателство:

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

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

Следователно

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

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

$$\begin{aligned} p(1 + p\mathbb{Z}) &= \underbrace{(1 + p\mathbb{Z}) + (1 + p\mathbb{Z}) + \cdots + (1 + p\mathbb{Z})}_{p \text{ пъти}} = \\ &= p + p\mathbb{Z} = p\mathbb{Z} \quad (\text{нулевият елемент на } \mathbb{Z}_p). \end{aligned}$$

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

Забележка. Ако n е естествено съставно число, т. е. $n = n_1 n_2$, $1 < n_1, n_2 < n$, тогава \mathbb{Z}_n не е поле, защото $\bar{n}_1 \bar{n}_2 = \bar{0}$, т. е. в \mathbb{Z}_n има делители на нулата.

Твърдение 4. Нека F е поле и $\text{char}(F) = p$. Тогава $pa = 0$ за всяко $a \in F$.

Доказателство:

Съгласно равенството (2) имаме $pa = (pe)a$. Понеже $pe = 0$, следва $pa = 0$.

Твърдение 5. Нека F е поле, $\text{char}(F) = p$ и $m \in \mathbb{Z}$. Ако $a \in F$ и $a \neq 0$ тогава имаме, че

$$ma = 0 \text{ тогава и само тогава, когато } p \text{ дели } m.$$

Доказателство:

I) Нека $m = pm_1$, тогава $ma = (m_1p)a = m_1(pa) = 0$, защото съгласно Твърдение 4 $pa = 0$.

II) Нека $ma = 0$. Нека $m = pq + r$, където $0 \leq r < p$. 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 $ra = 0$. Съгласно (2), $(re)a = 0$ и понеже $a \neq 0$, следва че $re = 0$. Тъй като $r \neq 0$ и $r < p$, това противоречи на дефиницията на характеристиката на полето F .

Твърдение 6. Нека F е поле и $\text{char}(F) = p$. Тогава

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

Доказателство:

Доказателството ще направим по индукция относно k .

База: $k = 1$. Имаме

$$(a + b)^p = a^p + \underbrace{\binom{p}{1}a^{p-1}b + \dots + \binom{p}{p-1}ab^{p-1}}_A + b^p$$

Понеже p е просто число, $\binom{p}{k}$ се дели на p , ако $1 \leq k < p$. Следователно всеки от коефициентите в A се дели на p . Съгласно Твърдение 5 всяко от събираемите в A е равно на нула и следователно е вярно $(a + b)^p = a^p + b^p$. С това базата на индукцията е доказана.

Нека $k \geq 2$. 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

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

С последователно прилагане на Твърдение 6 получаваме:

Следствие.

$$(a_1 + a_2 + \cdots + a_s)^{p^k} = a_1^{p^k} + a_2^{p^k} + \cdots + a_s^{p^k}.$$

Ще докажем следната:

Теорема. Нека F е поле, $\text{char}(F) = p$ и $e \in F$ е единичният елемент. Да означим цикличната подгрупа на адитивната група на F , породена от $e \in F$ с F' . Тогава F' е подполе на F , което е изоморфно на полето \mathbb{Z}_p .

Доказателство:

Да си припомним, че $F' = \langle e \rangle = \{a \in F \mid a = ke \text{ за някое } k \in \mathbb{Z}\}$. Понеже редът на e в адитивната група на F е равен на p , съгласно Твърдение 5 от лекцията за циклични подгрупи

$$\langle e \rangle = F' = \{0, e, 2e, \dots, (p-1)e\} \quad (*)$$

Знаем, че F' е подгрупа на адитивната група на полето F . Тъй като $e \in F'$, 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 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 $a \in F'$ и $a \neq 0$. Съгласно (*) $a = ke$, където $1 \leq k \leq p-1$. Понеже характеристиката е просто число, то $(p, k) = 1$. Поради това съществуват $u, v \in \mathbb{Z}$, 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 $(ke)^{-1} = ue \in F'$, с което доказахме, че F' удовлетворява и последното изискване за подполе.

Разглеждаме изображението

$$m \xrightarrow{\varphi} me, \quad \forall m \in \mathbb{Z},$$

където e е единичният елемент на F .

Нека $a, b \in \mathbb{Z}$. Тогава $a \xrightarrow{\varphi} ae$, $b \xrightarrow{\varphi} be$ и

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

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

Следователно φ е хомоморфизъм на \mathbb{Z} в полето F . Ясно е, че $\text{Im}(\varphi) = F'$. Последното равенство означава, че φ е епиморфизм на \mathbb{Z} върху F' . Съгласно Теоремата за епиморфизмите на пръстени имаме, че $\mathbb{Z}/\text{Ker}(\varphi)$ е изоморфен на F' . По дефиниция

$$m \in \text{Ker}(\varphi) \Leftrightarrow me = 0.$$

Поради това от Твърдение 5 следва, че $\text{Ker}(\varphi) = p\mathbb{Z}$. С това доказахме, че факторпръстенът $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ е изоморфен на подполето F' .

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