Формула за класовете еквивалентност или орбитите

$|C_x| = \frac{|G|}{|G_G(x)|}$ ↳ $|G| = \sum_{i=1}^{k} |C_{x_i}| = \sum \frac{|G|}{|G_G(x)|}$

9

Определение Нека $M \neq \emptyset$ дефинираме 2 бинарни операции „+" и „·" т.е $\forall a, b \in M$: $a+b \in M$, $a \cdot b \in M$ и M е пръстен ако са изпълнени следните свойства:

1) $(M, +)$ е Абелева група $\begin{cases} a+b = b+a \\ (a+b)+c = a+(b+c) \\ \exists 0: a+0 = a, \forall a \\ \forall a, \exists b_{(a)}: a+b_{(a)} = 0 \end{cases}$

2) Асоциативност за умножението
$(ab)c = a(bc) \quad \forall a, b, c \in M$

3) Са изпълнени двата дистрибутивни закона: т.е.
$a(b+c) = ab+ac \quad \forall a, b, c \in M$
$(b+c)a = ba+ca$

- Ако M изпълнява и $ab = ba \Rightarrow M$ - комутативен пръстен

Опр за Подпръстен: Нека M - пръстен и $K \neq \emptyset$ $K \subset M$, K - подпръстен на M ако е пръстен относно същите операции в M. Записваме $K < M$.

Примери за пръстени:
- Комутативни пръстени: ① $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
  ② Множеството на четните цели числа
  ③ Множ. на цели числа кратни на фиксирано $k \in \mathbb{R}$
- Некомутативни пръстени: Матриците $M = M_{n \times n}(\mathbb{R})$
- Крайни комутативни пръстени: • $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ - класовете ост. по $(\mathrm{mod}\, n)$
  $\bar{a} + \bar{b} = \bar{c}$ където $\bar{c} \equiv a+b \,(\mathrm{mod}\, n)$
  $\bar{a} \cdot \bar{b} = \bar{r}_1$ където $\bar{r}_1 \equiv ab \,(\mathrm{mod}\, n)$
- Крайни некомутативни пръстени: $M_{n \times n}(\mathbb{Z}_2)$, [illegible]

$\mathbb{Z}_6$ - класове остатъци по (mod 6)

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

обратични → $\bar{1}$, $\bar{5}$; $\bar{1}\cdot\bar{1}=\bar{1}$, $\bar{5}\cdot\bar{5}=\bar{1}$

Опр. Казваме че М е пръстен с единица ако $\exists e: ea=a\cdot e=a\ \forall a\in M$

Опр Обратим ел: Ако М е пръстен с единица елемента a се нарича обратим ако $\exists b\in M: ab=ba=e$

- $M^* = \{x\in M \mid x\text{-обратим}\}$ - обратимо множество пр: $\mathbb{Z}_6^* = \{\bar{1}, \bar{5}\}$ (обратими)

Тв Множ. обратими: $M^*_{n\times n}(\mathbb{R}) = \{A \mid \det A \neq 0\} = GL(n,\mathbb{R})$ (общата линейна група)

пр: за пръстен без единица// множ. $2\mathbb{Z} < \mathbb{Z}$ - $2\mathbb{Z}$ пръстен на $\mathbb{Z}$

$2\mathbb{Z} = \{2k \mid k\in\mathbb{Z}\}$

$2k+2s = 2(k+s)\in 2\mathbb{Z}$

$2k\cdot 2s = 2(2ks)\in 2\mathbb{Z}$

$0 = 2\cdot 0 \in 2\mathbb{Z}$

Тв Ако М е пръстен с единица то M^* (множ. от н обратими ел. от М) е група относно умножението

Док// $A, B, C \in M^*$

$(AB)C = A(BC) \Rightarrow$ (от 2) св. от пр за пръстени)

$e\in M^*: ee=e$

Ако $A, B\in M^*$ (обратими) $\Rightarrow \exists A^{-1}, B^{-1}\in M$ т.е

$AA^{-1} = A^{-1}A = e \Rightarrow A^{-1}\in M^*$ (A^{-1}, B^{-1} - обратими ел. $\in M^*$)

$BB^{-1} = B^{-1}B = e \Rightarrow B^{-1}\in M^*$

$(AB)(B^{-1}A^{-1}) = e$

$(B^{-1}A^{-1})(AB) = e$ } по деф за обратим ел $\Rightarrow AB\in M^*$ и $(AB)^{-1} = B^{-1}A^{-1}$

Опр M^* е мултипликативна група на пръстена М.

$\Rightarrow$ мултипликативни са и $\mathbb{C}^* = \mathbb{C}\setminus\{0\} - \mathbb{C}$, $\mathbb{R}^* = \mathbb{R}\setminus\{0\} - \mathbb{R}$, $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\} - \mathbb{Q}$, $\mathbb{Z}^* = \mathbb{Z}\setminus\{0\} - \mathbb{Z}$.

Опр За делители на 0: М - пръстен ел $a, b: a\neq 0, b\neq 0$ и $a\cdot b = 0$ се нарича делители на 0. (Елементи които като се умножат помежду себе си дават 0 са делители на 0)

пр. двоч матрици $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1&0\\-1&0\end{pmatrix} = \begin{pmatrix}0&0\\0&0\end{pmatrix}$

Тв: Делителите на 0 нямат за техни обратими елементи.

Док: // Нека a - делител на 0 $\Rightarrow \exists b \neq 0 : ab = 0$

Допускаме, че $\exists a^{-1} : aa^{-1} = a^{-1}a = e$ тогава

$a^{-1}|ab = 0 \Rightarrow a^{-1}(ab) = a^{-1}0 = 0 \Rightarrow (a^{-1}a)b = 0 \Rightarrow b = 0$ ↯

Свойства: 1) Ако $a \in M$: $a0 = 0a = 0$

2) Нулевия ел е единствен в M

3) Противоположния ел. $(-a)$ е единствен в M

4) Ако $\exists$ единичен елемент то той е единствен.

Опр. за Поле (Комутативен бул пръстен)

F е Поле ако F е комутативен пръстен с единица (1) в който всеки ненулев елемент е обратим

Th: В пръстена $\mathbb{Z}_n$, $\bar{a} \in \mathbb{Z}_n$, $\bar{a} \neq \bar{0}$

1) $\bar{a}$ - обратим ел $\Leftrightarrow (a,n) = 1$ (a и n взаимно прости)

2) $\bar{a}$ - делител на 0 $\Leftrightarrow$ НОД $(a,n) = d > 1$

Док: //

① Нека $(a,n) = 1$ [от Теза Безу] $\Rightarrow \exists u, v \in \mathbb{Z} : au + nv = 1$

$au \equiv 1 \pmod n$

$\bar{a} \cdot \bar{u} = \bar{1}$ в $\mathbb{Z}_n \Rightarrow \bar{u} = \bar{a}^{-1}$

② $(a,n) = d > 1$

$a = da_1$, $a_1 = \frac{a}{d}$

$n = dn_1$, $n_1 = \frac{n}{d}$ $\quad 1 < n_1 < n \Rightarrow \bar{n}_1 \neq \bar{0}$

$\bar{a}\,\bar{n}_1 = \bar{a}_1 \bar{d}\,\bar{n}_1 = \bar{a}_1 \cdot \bar{0} = \bar{0} \Rightarrow \bar{a}$ - делител на $\bar{0}$ в $\mathbb{Z}_n$

Следствия:

1) $|\mathbb{Z}_n^*| = \varphi(n)$ - функция на Ойлер

2) $\mathbb{Z}_n$ - поле $\Leftrightarrow n$ - просто число $\rightarrow$ (всички ненулеви елем. са обратими)

3) $|\mathbb{Z}_n^*| = \varphi(n)$ $\quad \bar{a} \in \mathbb{Z}_n^* \Rightarrow (a,n) = 1$

Разглеждане $\mathbb{Z}_n^*$ и прилагане следствието от Th на Лагранж

$\Rightarrow |\bar{a}| \mid |\mathbb{Z}_n^*| \Rightarrow |\bar{a}| \mid \varphi(n) \Rightarrow \bar{a}^{\varphi(n)} = \bar{1} \Rightarrow$

4) когато $(a,n) = 1$ то $\boxed{a^{\varphi(n)} \equiv 1 \pmod n}$ → Th на Ойлер-Ферма

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

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

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

- Единствените елементи от ред 2 са -1

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

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

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

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

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

Th: Нека $K \subseteq M$ и M - пръстен

$$K < M \Leftrightarrow \begin{cases} \text{(1)} & a - b \in K, \forall a, b \in K \\ \text{(2)} & ab \in K, \forall a, b \in K \end{cases}$$

Док: //

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

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

10.

Опр: Характеристика на поле: Нека F - поле. Казваме, че F има характеристика $k \neq 0$ (записваме $\text{char } F = k$) 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 $\text{char } F = 0$, 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.

Th: (Характеристика на всяко поле е просто число или 0) $\equiv$ F - поле $\Rightarrow \text{char } F$ е или 0 или просто число.