Теоритично контролно №2, I, Информатика

Иван Йочев

11 май 2019 г.

1 Действие на група върху множество

1.1 Определение

Нека G - група и M - множество
$f : G \times M \to M$
G действа върху M, ако:
0) $\exists f : G \times M \to M$
1) $\forall g \in G \ \forall m \in M \ f(g, m) \in M$
2) $\forall g_1, g_2 \in G \ \forall m \in M \ f(g_1 g_2, m) = f(g_1, f(g_2, m))$
3) $\forall m \in M \ f(e_H, m) = m$

1.2 Стабилизатор на елемент

Нека G - група, M - множество и G действа върху M
$f : G \times M \to M$ е действие на група върху множество
Нека $x \in M$
$St_G(x) = \{g \in G | f(g, x) = x\} \subseteq G$

1.3 Орбита на елемент

Нека G - група и M - множество и G действа върху M
$f : G \times M \to M$ е действие на група върху множество
Нека $x \in M$
$O_G(x) = \{f(g, x) | g \in G\} \subseteq M$

1.4 Изразяване на дължина на орбита

Нека G - група и M - множество и G действа върху M
Нека $x \in M$
$|O_G(x)| = |G \ : \ St_G(x)|$

1.5 Действие на група върху себе си чрез спрягане

Нека G - група
$\forall g \in G$ дефинираме $\phi_g : G \to G$
$\phi_g(x) = gxg^{-1}$
Тогава gxg^{-1} наричаме спрегнат на x по g

1.6 Клас спрегнати елементи

Нега G е група
Тогава за $x \in G$
$C_x = O_G(x) = \{gxg^{-1} \mid g \in G\}$
наричаме клас спрегнати с x елементи

1.7 Централизатор

Нега G е група и G действа върху себе си, чрез спрягане
Тогава за $x \in G$
$C_G(x) = St_G(x) = \{g \in G \mid gxg^{-1} = x\}$
наричаме централизатор на x в G

1.8 Център на група

Нека G е група
Множеството $Z(G) = \{z \in G | \forall g \in G\ zg = gz\}$
наричаме център на групата G $Z(G) = G$, когато G е абелева

1.9 Формула за класовете

Нека G е група и G действа върху M - множество.
$|M| = n < \infty$
$M = \{x_1, x_2, ..., x_n\}$
$\forall i \in \mathbb{N}\ \forall j \in \mathbb{N}\ O(x_i) \cap O(x_j) = \emptyset$
$M = \bigcup\limits_{i=1}^{n} O(x_i)$
$Z(G) = \{x_{i_1}, ..., x_{i_t}\}, t \leq n$
$|M| = \sum\limits_{i=1}^{n} |O(x_i)| = \sum\limits_{i=1}^{n} |G : St_G(x_i)|$
Ако $G \equiv M$ и G действа върху себе си, чрез спрягане
$|M| = |Z(G)| + \sum\limits_{j=1}^{t} |C_{x_{i_j}}|$

1.10 Теорема на Кейли

Нека G - група $|G| = n < \infty$
$\Rightarrow\ \exists\ G' \leq S_n : G \cong G'$

2 Пръстени

2.1 Определение

$(R, +, \cdot)$ е пръстен, ако:
0) $(R, +)$ е абелева група

1) $(\forall a \in R\ \forall b \in R) ab \in R$
затвореност относно умножение

2) $(\forall a \in R\ \forall b \in R\ \forall c \in R)$
$a(bc) = (ab)c = abc$
асоциативност за умножение

3) $(\forall a \in R\ \forall b \in R\ \forall c \in R)$
$(a+b)c = ac + bc\ \wedge a(b+c) = ab + ac$
дистрибутивност за умножение

2.2 Пръстен с единица

$(R, +, \cdot)$ е пръстен с единица, ако:
0) $(R, +, \cdot)$ е пръстен
1) $\exists e \in R\ \forall a \in R\ ae = ea = a$

2.3 Комутативен пръстен

$(R, +, \cdot)$ е комутативен пръстен, ако:
0) $(R, +, \cdot)$ е пръстен
1) $\forall a \in R\ \forall b \in R : ab = ba$

2.4 Област на цялост(област)

Нека $(R, +, \cdot)$ - комутативен пръстен
R е област, ако
0) $R \neq \{0\}$
1) Нека $a \in R$, $0_R \neq b \in R$
$(ab = 0_R) \rightarrow (a = 0_R)$
(в R има единствен делител на нулата и това е 0_R)

2.5 Делител на нулата

Нека $(R, +, \cdot)$ - комутативен пръстен, и $a \in R$
a е делител на нулата, ако
$\exists b \in R, b \neq 0_R : ab = ba = 0_R$

2.6 Поле

Нека $(R, +, \cdot)$ е пръстен
R е поле ако:
1) R е комутативен
2) R е тяло

2.7 Тяло

$(R, +, \cdot)$ е тяло, ако:
0) $(R, +, \cdot)$ е пръстен
1) $\exists 0 \in R\ \wedge\ \exists 1 \in R\ \wedge\ 0_R \neq 1_R$
2) $\forall a \in R\ \exists a' \in R : aa' = a'a = 1_R$

2.8 Подпръстен

Нека $(R, +, \cdot)$ е пръстен и нека $S \subseteq R, S \neq \emptyset$
S е подпръстен, ако $(\forall a \in S \ \forall b \in S)$
$(a \pm b \in S) \wedge (ab \in S)$

2.9 Мултипликативна група на пръстен

Нека $(R, +, \cdot)$ е пръстен с единица
$R^* = \{a \in R \mid \exists a' \in R : aa' = a'a = 1_R\}$
R^* се нарича мултипликативна група на пръстен R

3 Полета

3.1 Характеристика на поле

Нека F е поле

Нека $m \in Fn \in F, m \neq n$
Ако $m.1_R \neq n.1_R$, то $charF = 0$
Ако $m.1_R = n.1_R$, то $charF = |m - n|$

Алтернативна дефиниция:
$charF = |1|_{F+}$

3.2 Общ вид на характеристика на поле

Нека F е поле
$charF = 0$ или $charF = p$ - просто

3.3 Подполе

Нека F е поле
Нека $K \subset q, F, |K| \geq 2$
K е подполе ($K \leq F$), ако:
1) $\forall a \in K \forall b \in K \ a \pm b \in K$
2) $\forall a \in K \forall b \in K \ ab \in K$
3) $\forall a \in K \ a^{-1} \in K$

3.4 Разширение на поле

Нека F е поле и $K \leq F$
F наричаме разширение на K

3.5 Просто поле

Нека F е поле
F е просто, ако
$(\forall K \leq F) \ K = F$

3.6 Възможни прости подполета

Нека F е поле
$P = \bigcap\limits_{K \leq F} K$
P е единствено просто подполе на F

4 Хомоморфизъм на пръстени

4.1 Определение

Нека R и R' са пръстени
Нека $\phi : R \to R'$
ϕ е хомоморфизъм, ако
1) $\forall a \in R \ \forall b \in R \ \phi(a+b) = \phi(a) + \phi(b)$
2) $\forall a \in R \ \forall b \in R \ \phi(ab) = \phi(a)\phi(b)$

4.2 Изоморфизъм

Нека R и R' са пръстени
Нека $\phi : R \to R'$
ϕ е изоморфизъм, ако
1) ϕ е хомоморфизъм
2) ϕ е биекция

4.3 Ядро на хомоморфизъм

Нека R и R' са пръстени
Нека $\phi : R \to R'$ - хомоморфизъм
$Ker\phi = \{a \in R \mid \phi(a) = 0_{R'}\}$

4.4 Образ на хомоморфизъм

Нека R и R' са пръстени
Нека $\phi : R \to R'$ - хомоморфизъм
$Im\phi = \{\phi(a) \in R' \mid a \in R\}$

5 Идеали

5.1 Определение за ляв(десен) идеал

Нека R - пръстен
$I \trianglelefteq R$, ако
0) $\emptyset \neq I \subseteq R$
1) $\forall a \in I \ \forall b \in I \ a - b \in I$
2) $\forall a \in I \ \forall r \in R$
$ra \in I$(ляв идеал)
$ar \in I$(десен идеал)

5.2 Определение за двустранен идеал

Нека R - пръстен
$I \trianglelefteq R$, ако
0) $\emptyset \neq I \subseteq R$
1) $\forall a \in I \ \forall b \in I \ a - b \in I$
2) $\forall a \in I \ \forall r \in R \ ra \in I \ \wedge \ ar \in I$

5.3 Сума на идеали

Нека R - пръстен
$I \trianglelefteq R, J \trianglelefteq R$
$I + J = \{i + j | i \in I, j \in J\} \trianglelefteq R$
I+J се нарича сума на идеали

5.4 Главен идеал, породен от елемент

Нека R е комутативен пръстен с единица
Нека $a \in R$
$(a) = \{ar | r \in R\}$
(a) се нарича главен идеал породен от елемента a

5.5 Идеали в пръстена $\mathbb{Z}$

Нека $I \trianglelefteq \mathbb{Z}$
$\Rightarrow I = (n) = n\mathbb{Z}, n \in \mathbb{N} \cup 0_Z$

5.6 Събиране в факторпръстен

Нека R - пръстен
$I \trianglelefteq R$
Нека $a \in R$ и $b \in R$
$\bar{a} = a + I$
$\bar{b} = b + I$
$\bar{a} + \bar{b} = (a + I) + (b + I)$
$= (a + b) + I = \overline{a + b}$

5.7 Умножение в факторпръстен

Нека R - пръстен
$I \trianglelefteq R$
Нека $a \in R$ и $b \in R$
$\bar{a} = a + I$
$\bar{b} = b + I$
$\bar{a} \cdot \bar{b} = (a + I)(b + I)$
$= (ab) + I = \overline{ab}$

5.8 Теорема за хомоморфизмите за пръстени

Нека R, R' - пръстени
Нека $\phi : R \to R'$ - хомоморфизъм на пръстени
Нека Ker$\phi = I$
$\Rightarrow I \trianglelefteq R$ и $R/I \cong Im\phi$

6 Доказателства

6.1 Поле няма нетривиални идеали

Нека R е поле
$\{0\} \neq I \trianglelefteq R$
$a \in I, a \leq 0$
$\Rightarrow 1 = a^{-1}a \in I$
$\Rightarrow 1 \in I$
$\Rightarrow R = (1) \subseteq I \ \wedge \ I \subseteq R$
$\Rightarrow I = R$

6.2 Ако комутативен пръстен с единица няма нетривиални идеали, той е поле

Нека R е пръстен и R няма нетривиални идеали
Нека $0 \neq a \in R$
$\Rightarrow (a) \neq \{0\}$
$\Rightarrow (a) = R = (1)$
$\Rightarrow \exists a' \in R : aa' = a'a = 1$
$\Rightarrow$ а е обратим и $a^{-1} = a'$
$\Rightarrow \forall a \in R$ е обратим
$\Rightarrow$ R е поле

6.3 Всяко поле съдържа едниствено просто подполе

Нека R е поле. Ще докажем, че единственото
просто подполе на R е $P = \bigcap\limits_{K \leq R} K$
Да допуснем, че $\exists X : X < P$ (P не е просто поле)
$\Rightarrow X < R$
$(P = \bigcap\limits_{K \leq R} K) \rightarrow X \supseteq P$, но по допускане $X < P$
$\Rightarrow X = P$
Следователно P е единствено просто подполе