ZMB
ВАД

Класната 10.04

22.04 понеделник, 13 - 16 контролно Т 604 ХФ
консултация ~~ПТ~~ 04 13 60 1 ХФ
На 18 изпращат домашните site - ресурси, които контрол самостоятелност рой

## Симетрична група

Пермутациите $\tau, \gamma \in S_n$ са спрегнати, т.е. $\exists \xi \in S_n$ с $\gamma = \xi \tau \xi^{-1} \Leftrightarrow$ $\tau$ и $\gamma$ имат еднаков цикличен строеж. Оттук $\Rightarrow$ че ПГ $H$ на $S_n$ е нормална $\Leftrightarrow$ за $\forall \tau \in H$ групата $H$ съдържа $\forall$-ви $\gamma \in S_n$ които имат еднаков цикличен строеж с $\tau$

Пр
Множеството $K_4 := \{\varepsilon, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ е нормална ПГ на $S_4$ наречена група на Клайн

$(i,j)(k,l)$ $i,j,k,l$ са различни $\Rightarrow$
$\{i,j,k,l\} = \{1,\dots,4\}$
$(1,i)(j,k) \Rightarrow i \in \{2,3,4\}$ $\{2,3,4\} \setminus \{i\} = \{j,k\}$

Зада проверим че $K_4$ е ПГ на $S_4$ забелязваме че за $\forall \tau \in K_4 \setminus \{\varepsilon\}$ имаме $\varepsilon\tau = \tau \in K_4$,
$\tau^2 = (1,i)(j,k)(1,i)(j,k) = (1,i)^2(j,k)^2 = \varepsilon\varepsilon = \varepsilon \in K_4$
Ако $\forall \tau, \gamma \in K_4 \setminus \{\varepsilon\}$ и $\tau \neq \gamma$ то $\exists$ пермутация $i,j,k$ на $2,3,4$ т.е. $\tau = (1,i)(j,k) = (1,i)(k,j)$
Поради $\tau \neq \gamma$ имаме образът на единицата $\gamma(1) \in \{2,3,4\} \setminus \{i\} = \{j,k\}$ и можем да считаме че $\gamma(1) = j$. Тогава $\gamma = (1,j)(i,k)$ и
$\gamma\tau = (1,j)(i,k)(1,i)(j,k) =$

$= (1,k)(i,j) \in K_4$ Това установява затвореност на $K_4$ спрямо умнож.

От $\varepsilon^{-1} = \varepsilon$ и $\gamma^{-1} = [(1,i)(j,k)]^{-1} = (j,k)^{-1}(1,i)^{-1} =$

$= (j,k)(1,i) = \gamma \in K_4$

т.к $a^{-1} = a \iff a^2 = \varepsilon$ в група $G$.

Следователно $K_4$ е затворено и относно обръщане така че $K_4 \leq S_4$ е ПГ

Заедно с $\forall \gamma = (1,i)(j,k) \in K_4$ групата $K_4$ съдържа $\forall \sigma \in S_4$

като има еднакво цикличен строеж с $\gamma$ и $K_4 \trianglelefteq S_4$ е нормална ПГ

Деф

Цикъльт $(i,j)$ $i \neq j$ с дължина 2 се нарича транспозиция

Деф

Числата $\gamma(p)$ и $\gamma(q)$ от редицата $\gamma(1) \dots \gamma(p) \dots \gamma(q) \dots \gamma(n)$ на образите на $1, \dots n$ под действие на пермутацията $\forall \in S_n$ образуват инверсия ако $p < q$ и $\gamma(p) > \gamma(q)$.

Деф

Пермутацията $\gamma \in S_n$ е четна (нечетна) ако в редицата $\gamma(1) \dots \gamma(n)$ на образите $1 \dots n$ под действие на $\gamma$ има четен (нечетен) брой инверсии

Лема

Произведението $(i,j)\gamma$ на четна (нечетна) пермутация $\gamma \in S_n$ с транспозиция $(i,j)$ $i \neq j$ е нечетна (четна) пермутация

Док

1 сл) Ако транспозицията $(i,j) = (\sigma(p))(\sigma(p+1))$ за някое $1 \le p \le n-1$ разменя съседни числа в $\sigma(1) \dots \sigma(p-1), \sigma(p), \sigma(p+1) \dots \sigma(n)$ то взаимното положение на $\sigma(k)$ и $\sigma(p)$ на $\sigma(k)$ и $\sigma(p+1)$ както и на $\sigma(k)$ и $\sigma(\ell)$ за различни $k, \ell \in \{1, \dots n\} \setminus \{p, p+1\}$ не се променя при прилагане $(\sigma(p), \sigma(p+1))$. Ако $\sigma(p) < \sigma(p+1)$ то след прилагане на транспозицията $(\sigma(p), \sigma(p+1))$ се появява точно 1 нова инверсия м/у $\sigma(p)$ и $\sigma(p+1)$. Ако $\sigma(p) > \sigma(p+1)$ то прилагането на транспозицията на $(\sigma(p), \sigma(p+1))$ премахва инверсията м/у $\sigma(p)$ и $\sigma(p+1)$

2 сл) Общия случай $(i,j) = (j,i) = (\sigma(p), \sigma(q))$ $1 \le p < q \le n$ прилагането на транспозицията $(\sigma(p), \sigma(q))$ върху $\sigma(1), \dots \sigma(p), \dots \sigma(q) \dots \sigma(n)$ се разпада в произведение на транспозиции на съседни числа по следния начин

$$(\sigma(p), \sigma(q)) = (\sigma(q)\sigma(p+1))\underbrace{(\sigma(q),\sigma(q-1))(\sigma(p),\sigma(q))}_{q-p-1 \text{ на брой}} \dots (\sigma(p),\sigma(p+2))$$

Понеже $(\sigma(p)\sigma(q))$ е произведение на $q-p$ на брой нечетен брой, $2(q-p)-1$ транспозиции на съседни числа и приложено на транспозиция на съседни числа променя четността на броя на инверсиите и прилагането на $(\sigma(p)\sigma(q))$ променя четността на броя на инверсиите

ТЛМЧ

ZTA

(Из ИЛ 25 ~~Недостатъчно~~ 96) Да не се

Т6: (i)

Всяка перестановка $\tau \in S_n$ се разлага в произведение на (необходимо независими) транспозиции

(ii)

Броят на множителите в D-ко разлагане на $\tau$ в произведение на транспозиции има една и съща четност съвпадаща със четността на $\tau$

Док:

Ако перестановка $\tau \in S_n$ се разлага в произведение на независими цикли достатъчно е да разложим произволен цикъл $(i_1, i_k)$ в произведение на транспозиции за да докажем условие 1

$(i_1 \dots i_k) \quad i_1 \; i_2 \; \dots \; i_{k-1}, i_k \; )(i_1, i_2)$

$i_2, i_1, i_3 \dots i_k \longrightarrow (i_1, i_3) \to i_2(3, i_1 \dots i_k$

$i_2, i_3 \dots i_k, i_1$

Следователно $(i_1 \dots i_k) = (i_1$

(Т1) Нека $\tau = \tau_{om} \dots \tau_1 = \tau'_k \dots \tau'_1$ са две разлагания на $\tau \in S_n$ в произведение на транспозиции $\tau_i \dots \tau'_j$. Тогава четността на броя на инверсиите в $\tau(1) \dots \tau(n)$ съвпада с четността на m и четността на k защото прилагането на транспозиция променя четността на броя на инверсиите $\square$

Лагранж $|S_n| = |A_n|[S_n : A_n] = n! = |A_n| \cdot 2$

$|A_n| = \frac{n!}{2}$ броят на елементите

Отук и ги имат една и съща четност. Пр

$(2,3)(1,2)(2,3)^{-1} = ((2,3)(1), (2)(2,3)) = (1,3)$

броят на транспозициите в двете разлагания може да е различен

Тв:

Множеството $A_n$ на четните перумтации $\sigma \in S_n$ е нормална подгрупа на $S_n$ с индекс $[S_n : A_n] = 2$, която се нарича алтернативна група

Док

От предишното тв част 2 следва че $\sigma \in S_n$ е четна перумтация $\Leftrightarrow \sigma$ се разлага в произведение на четен брой транспозиции. Затова за $\forall \sigma, \tau \in A_n$ нека $\sigma = \tau_{2m} \dots \tau_1$ и $\tau = \tau_{2k} \dots \tau_1$ за транспозиции $\tau_i, \tau_j$. сега $\sigma\tau = \tau_{2k} \dots \tau_1 \tau_{2m} \dots \tau_1 \in A_n$ като произведение на четен брой $= 2k + 2m$ транспозиции и $\sigma^{-1} = (\tau_{2m} \dots \tau_1)^{-1} = \tau_1 \dots \tau_{2m} \in A_n$ т.е $A_n$ е ПГ на $S_n$. За $\forall (i,j) \in S_n$ при $n \geq 2$ ще докажем че $S_n \setminus A_n = (i,j) A_n$. Отук $\Rightarrow$ че $S_n$ е непресичащо се обединение т.е. $S_n = A_n \cup (S_n \setminus A_n) = A_n \cup (i,j) A_n$ е непресичащо се обединение на два леви съседни класа по модул $A_n$, т.е $[S_n : A_n] = 2$

За $S_n \setminus A_n = (i,j) A_n$

$\tau_i^2 = \varepsilon \Rightarrow \tau_i = \tau_i^{-1}$

Забелязваме че за $\forall \gamma \in S_n / A_n$ имаме
$(i\ j)\gamma = \tau \in A_n$. Сега
$\gamma = \varepsilon\gamma = ((i\ j)(i\ j))\gamma = (i\ j)\tau \in (i\ j)A_n$

Обратно за $\forall \tau = (i\ j)\tilde{\gamma}$ с $\tilde{\gamma} \in A_n$ знаем че $\tau$ четна перпутация т.е. левият съседен клас $(i,j)A_n \leq S_n / A_n$ и $(i,j)A_n = S_n / A_n$ От $[S_n : A_n] = 2$ следва че $A_n \trianglelefteq S_n$ □

## Пръстен и подпръстен - определение примери основни св-ва

**Определение**
Непразното мн-во $R$ е пръстен, ако в него са определени две бинарни операции - събиране $R \times R \to R$, $(a,b) \mapsto a+b$ и умножение $R \times R \to R$ $(a,b) \mapsto ab$ т.е

(i) $R$ е абелева група относно събирането
(ii) Умножението е асоциативно т.е. $(ab)c = a(bc)$ за $\forall a,b,c \in R$
(iii) В сила са дистрибутивните закони за събиране и умножение
$(a+b)c = ac+bc$ и $a(b+c) = ab+ac$ за $\forall a,b,c \in R$

Пр
1) $\mathbb{Z}$ е пръстен
2) $\forall$ числово поле $F \subseteq \mathbb{C}$ е пръстен

(по определение числово поле $F$ е подмножество на $\mathbb{C}$ с поне 2 елемента което е затворено относно събиране, изваждане, умножение и деление с ненулев елемент)

$0 \in (F, +)$ За $x \in F \Rightarrow -x = 0 - x \in F$

3) За произволно числово поле $F$ и произволно $n \in \mathbb{N}$ множеството $M_{nxn}(F)$ на $nxn$ матриците с елементи от $F$ е пръстен относно обичайните операции събиране и умножение на матрици

$0_{nxn} \in (M_{nxn}(F), +)$

Деф

Ако $R$ е пръстен то абелевата група $(R, +)$ образувана от $R$ относно събирането се нарича адитивна група на $R$.

Неутралният елемент на $(R, +)$ се нарича нула на $R$ и се бележи с $0$ или $0_R$

За $\forall \varepsilon \in R$, елементът $-\varepsilon \in R$ с условието $\varepsilon + (-\varepsilon) = 0_R$ се нарича противоположен на $\varepsilon$

Деф

Елементът $1 \in R$ или $1_R$ от пръстен $R$ е единица ако $1_R \cdot \varepsilon = \varepsilon 1_R = \varepsilon$ за $\forall \varepsilon \in R$

Ако $R$ е пръстен с единица то м-во $R^*$ на обратимите относно умножението елементи на $R$ е група относно умножението което се нарича мултипликативна група на $R$

Например

$\mathbb{Z}^* = \{\pm 1\}$. Ако $a \in \mathbb{Z}$ $\exists\, b \in \mathbb{Z}$ с

$ab = 1 \Rightarrow a = b = \pm 1$

Ако $F$ е числово поле то $F^* = F \setminus \{0\}$

т.к. за $\forall\, x \in F \setminus \{0\}$ знаем че $\frac{1}{x} = x^{-1} \in F$

$Mat_n(F)^* = \{A \in Mat_n(F) \mid \det A \neq 0\} = GL(n, F)$

Т-т нрбстени без 1-ца. Например

$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ за $n \in \mathbb{N}$ при $n \geq 2$ е

нрстен без единица. Ако $\exists$ 1-ца на $n\mathbb{Z}$

то $\exists\, nz = nz_0$ за $z_0 \in \mathbb{Z}$ и за $\forall\, z \in \mathbb{Z}$ е в

сила $(nz_0)(nz) = nz$ т. е. $(nz_0)(nz) = (nz)$

или $n^2 z_0 z = nz$. За $z \neq 0$ получаваме

делене с $nz$ даващо $z_0 = 1$ което е

невъзможно за $n \geq 2$, $n \in \mathbb{N}$