# ALGEBRA II (NMAG202) – TEST, 21. ZÁŘÍ 2017

**Tvrzení a definice pečlivě formulujte včetně všech předpokladů. Odpovědi na otázky zdůvodněte. Pokud používáte nějaké netriviální tvrzení z přednášky, uveďte explicitně odkaz (často budete vyzváni, abyste všechna použitá tvrzení zformulovali). Časový limit je 90 minut.**

(1) Kolik prvků má faktor algebry $(\mathbb{Z}, +)$ podle nejmenší možné kongruence takové, že $3 \sim 4$? Kolik prvků má faktor algebry $(\mathbb{N}, +)$ podle nejmenší kongruence takové, že $3 \sim 4$? V obou případech popište bloky kongruence.

(10 bodů)

(2) Rozhodněte, které z následujících dvojic grup jsou isomorfní:
(a) $\mathbb{Z}_{12}^*$ a $\mathbb{Z}_2 \times \mathbb{Z}_2$,
(b) $\mathbb{Z}_{31}^*$ a $\mathbb{Z}_5 \times \mathbb{Z}_6$,
(c) $\mathbb{Z}_9$ a $\mathbb{Z}_3 \times \mathbb{Z}_3$.
Je-li dvojice grup isomorfní, popište konkrétní isomorfismus. V opačném případě neisomorfnost stručně zdůvodněte.

(10 bodů)

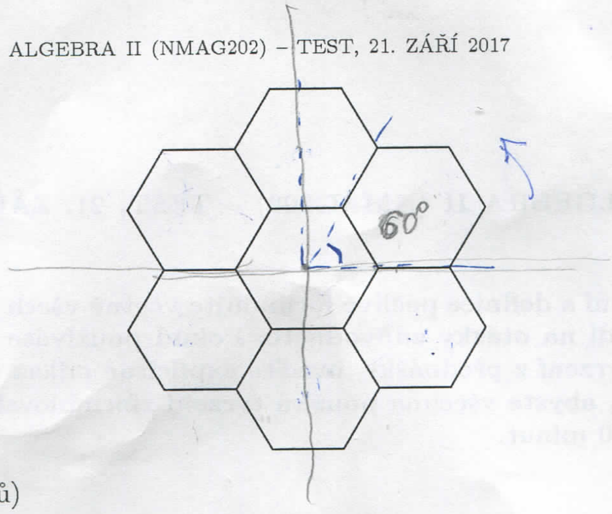
(3) Uvažujte polynom $f = x^2 + 1 \in \mathbb{Z}_3[x]$. Je faktorokruh $R = \mathbb{Z}_3[x]/(f)$ tělesem? Proč? Ukažte, že grupa invertibilních prvků $(R^*, \cdot, ^{-1}, 1)$ je cyklická a najděte nějaký její generátor.

(15 bodů)

(4) Buď $T$ těleso a $f \in T[x]$ polynom. Definujte pojem rozkladového nadtělesa polynomu $f$ a formulujte větu o jeho existenci.
Spočítejte stupeň rozšíření rozkladového nadtělesa polynomu $f = x^3 - 2$ v konkrétních případech, kdy a) $T = \mathbb{Q}$ a b) $T = \mathbb{R}$. Použitá tvrzení z přednášky přesně formulujte.

(15 bodů)

(5) Přesně formulujte Burnsideovu větu. Kolika způsoby lze políčka plástve níže obarvit třemi barvami? Dvě obarvení považujeme za stejná, pokud se liší jen o otočení.




(15 bodů)

(6) Přesně formulujte a dokažte Lagrangeovu větu o řádu podgrupy konečné grupy.
(20 bodů)

sousední musí mít stejnou barvu

• uprostřed

$2 \cdot 9$ ot. o $\pm 60°$

$2 \cdot 3 \cdot 3 \cdot 3$ ot. o $\pm 120°$

$3^4$ ot. o $180°$

$3^7$ ot o $360° = id$

$$\frac{2 \cdot 9 + 2 \cdot 3 \cdot 3 \cdot 3 + 3^4 + 3^7}{6}$$

(1.) Kolik prvků má faktor algebry $(\mathbb{Z},+)$ podle nejmenší možné kongruence takové, že $3 \sim 4$ ?

Kolik prvků má faktor algebry $(\mathbb{N},+)$ ?

Popište bloky kongruence.

---

1) $(\mathbb{Z},+)$ $\quad 3\sim 4 \iff 0 \sim 1$, neboť v algebře $(\mathbb{Z},+)$ lze přičítat libovolné celé číslo

proto $\forall k \in \mathbb{Z} : k \sim k+1$

kongruence je relace ekvivalence, proto z tranzitivity plyne, že $0\sim 1$ a $1 \sim 2 \Rightarrow 0 \sim 2$, atd. ...

$\sim \subseteq \mathbb{Z}\times\mathbb{Z}$, $\forall n \geq 1 : a_0 \simeq a_n$

tedy $(a_0, a_n)$ bude v tranzitivním uzávěru $\sim$

Vezmeme-li fixní $a \in \mathbb{Z}$, např. $a=0$, pak $[a]_\sim = \mathbb{Z}$

- právě jeden blok ekvivalence - celé $\mathbb{Z}$

$\Rightarrow \mathbb{Z}/\sim$ má právě jeden prvek

---

2) $(\mathbb{N},+)$, $3\sim 4 \iff 4\sim 5, 5\sim 6, 6 \sim 7, \ldots$ atd.

$1\sim 1$ } relace $\sim$ musí být reflexivní

$2 \sim 2$

$a \sim b \ \forall a,b \geq 3$ neboť:
- $a=b$ - reflexivita $\sim$
- $a<b$ - $a \sim a+1 \ \forall a \geq 3$ + indukce
- $a>b$ - symetrie $\sim$

$[1]_\sim = \{1\}$
$[2]_\sim = \{2\}$
$[3]_\sim = \{b \mid b \geq 3\}$
} bloky relace kongruence $\sim$

(2.) Rozhodněte, zda jsou grupy izomorfní; pokud ano, popište izomorfismus.

a) $\mathbb{Z}_{12}^*$ a $\mathbb{Z}_2 \times \mathbb{Z}_2$

$\mathbb{Z}_{12}^* = \{1; 5; 7; 11\}$ --> 4-prvková grupa, proto je nutně izomorfní buď $\mathbb{Z}_4$ nebo $\mathbb{Z}_2 \times \mathbb{Z}_2$ !

V $\mathbb{Z}_4$ je jeden prvek řádu 4, $\underset{\mathbb{Z}_4}{ord}(1) = 4$ $(1+1+1+1 = 4)$

řády prvků v grupě $\mathbb{Z}_{12}^*$ :
$ord(1) = 1$
$ord(5) = 2$
$ord(7) = 2$
$ord(11) = 2$

V $\mathbb{Z}_{12}^*$ neexistuje prvek řádu 4, proto nutně

$$\boxed{\mathbb{Z}_{12}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2}$$

$1 \overset{\varphi}{\longmapsto} (0,0)$ --> řád 1

$\left.\begin{array}{l} 5 \longmapsto (1,0) \\ 7 \longmapsto (0,1) \\ 11 \longmapsto (1,1) \end{array}\right\}$ řády 2

b) $\mathbb{Z}_{31}^*$ a $\mathbb{Z}_5 \times \mathbb{Z}_6$

$\mathbb{Z}_{31}^* \simeq \mathbb{Z}_{30}$ neboť $\mathbb{Z}_{31}$ je těleso a multiplikativní grupa tělesa je cyklická

a $\langle 3 \rangle = \mathbb{Z}_{31}^*$ neboť $3^{30} = 1$ a $\forall k \in \mathbb{N}, k \mid 30 : 3^k \neq 1$

Izomorfismus $\varphi : \mathbb{Z}_{30} \to \mathbb{Z}_{31}^*$ je $k \xmapsto{\varphi} 3^k$

⌈ neboť $\varphi(0) = 1$
$\varphi(1) = 3$ a $\varphi(k) = \varphi(\underbrace{1 + \dots + 1}_{k\text{-krát}}) = \underbrace{\varphi(1) \cdot \dots \cdot \varphi(1)}_{k\text{-krát}} = 3^k$ ⌋

a $\boxed{\mathbb{Z}_{30} \simeq \mathbb{Z}_5 \times \mathbb{Z}_6}$ neboť $\boxed{NSD(5,6) = 1}$

c) $\mathbb{Z}_9$ a $\mathbb{Z}_3 \times \mathbb{Z}_3$ $\boxed{\mathbb{Z}_9 \not\simeq \mathbb{Z}_3 \times \mathbb{Z}_3}$

neboť $\boxed{\mathbb{Z}_{m \cdot n} \simeq \mathbb{Z}_m \times \mathbb{Z}_n \iff NSD(m,n) = 1}$

(3.) $f = x^2 + 1 \in \mathbb{Z}_3[x]$

Je $R = \mathbb{Z}_3[x]\big|_{(f)}$ tělesem? Proč?

Ukažte, že grupa $(R^*, \cdot, {}^{-1}, 1)$ je cyklická a najděte nějaký její generátor.

---

$\mathbb{Z}_3[x]\big|_{(f)} = \{ax + b ; a, b \in \mathbb{Z}_3\}$ má 9 prvků: 0, 1, 2, $x$, $x+1$, $x+2$, $2x$, $2x+1$, $2x+2$

$R^*$ má 8 prvků

(neboť už víme, že $R$ je těleso)

$\Rightarrow R^*$ je cyklická grupa

ve faktorokruhu $\mathbb{Z}_3[x]\big|_{(x^2+1)}$ se počítá tak, že $x^2 + 1 = 0$ tj. $x^2 = -1$

$\mathrm{ord}(1) = 1$

$\mathrm{ord}(2) = 2$

$\mathrm{ord}(x) = 4$, neboť $x \cdot x \cdot x \cdot x = x^2 \cdot x^2 = (-1)\cdot(-1) = 1$

Víme: Je-li $G$ cyklická grupa, $|G| = n$, pak $\forall k \in \mathbb{N}$ takové, že $k \mid n$ $\exists!\ \varphi(k)$ prvků řádu $k$ $\neq 1$

$R^*$ má 8 prvků, dělitelé 8 jsou pouze 1, 2, 4, 8

EULEROVA FUNKCE: $\varphi(p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}) = p_1^{k_1 - 1} \cdot (p_1 - 1) \cdot \ldots$

$\varphi(2) = 1 \Rightarrow \exists!\ 1$ prvek řádu 2

$\varphi(4) = 2 \Rightarrow \exists!\ 2$ prvky řádu 4

$\varphi(8) = \varphi(2^3) = 2^2 \cdot 1 = 4 \Rightarrow \exists!\ 4$ prvky řádu 8

$\mathrm{ord}_{R^*}(x+1) = ?$

| $n$ | 0 | 1 | 2 | 3 | 4 | 8 |
|---|---|---|---|---|---|---|
| $(x+1)^n$ | 1 | $x+1$ | $2x$ | $2x-1$ | $-1$ | 1 |

- $(x+1)^2 = x^2+2x+1 = \underline{\underline{2x}}$

$\downarrow$ $x^2 = -1$ v $\mathbb{Z}_3[x] / (x^2+1)$

- $(x+1)^3 = 2x(x+1) = 2x^2+2x = \underline{\underline{2x-1}}$
- $(x+1)^4 = 2x \cdot 2x = 4x^2 = -4 = \underline{\underline{-1}}$
- $(x+1)^8 = (-1)\cdot(-1) = \underline{\underline{1}}$

$\Rightarrow \mathrm{ord}_{R^*}(x+1) = 8$

$x+1 \in R^*$ NEMÁ ŘÁD 1, 2, 4
$\Rightarrow x+1$ MÁ ŘÁD 8

proto prvek $x+1$ je generátor grupy $R^*$ – je tedy <u>cyklická</u>

$\Rightarrow$ našli jsme generátor $R^*$ $\Rightarrow$ grupa $R^*$ je cyklická

$\Rightarrow R$ je <u>těleso</u>

nebo: (i) Je-li $f$ <u>ireducibilní</u> polynom v $R$, <u>$R$ OIHI</u>,
potom $R/(f)$ je <u>těleso</u>

(ii) $R/I$ je <u>těleso</u> $\Longleftrightarrow$ $I$ je <u>maximální ideál</u> oboru $R$
(tj. $\forall J \subset R$, $I \subsetneq J \subseteq R$, pak $J = R$)

$R/I$ je <u>obor integrity</u> $\Longleftrightarrow$ $I$ je <u>prvoideál</u> (je-li $ab \in I$ pak $a \in I \vee b \in I$)

4.) Buď $T$ těleso, $f \in T[x]$ polynom.

Definujte pojem rozkladového nadtělesa polynomu $f$ a formulujte větu o jeho existenci

Def. Nechť $T \leq S$ je rozšíření těles, $f \in T[x]$

$S$ je rozkladové nadtěleso polynomu $f$, pokud:

- $S = T(a_1, \dots, a_n)$, kde $a_1, \dots, a_n$ jsou kořeny $f$

a • $f \,||\, (x - a_1) \cdot \ldots \cdot (x - a_n)$

---

$$f(x) = x^3 - 2$$

Určete stupeň rozšíření rozkladového nadtělesa polynomu $f \in T[x]$

pro: a) $T = Q$

kořeny: $\sqrt[3]{2} \cdot e^{\frac{2\pi i}{3} \cdot k}$, $k = 0, 1, 2$

tedy: $\sqrt[3]{2}, \sqrt[3]{2} e^{\frac{2\pi i}{3}}, \sqrt[3]{2} e^{\frac{4\pi i}{3}}$

$\Rightarrow$ rozkladové rozšíření: $Q(\underbrace{\underbrace{\sqrt[3]{2}}_{a_1}, \underbrace{\sqrt[3]{2} e^{\frac{2\pi i}{3}}}_{a_2}, \underbrace{\sqrt[3]{2} e^{\frac{4\pi i}{3}}}_{a_3}})$

toto je těleso, proto jsou-li $a_1, a_2 \in S$, pak i $\frac{a_2}{a_1} \in S$

a zároveň $a_3 = a_1 \cdot \left(\frac{a_2}{a_1}\right)$

proto $Q(\sqrt[3]{2}, \sqrt[3]{2} e^{\frac{2\pi i}{3}}, \sqrt[3]{2} e^{\frac{4\pi i}{3}}) = Q(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$

$$\left[Q(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}) : Q\right] = \underbrace{\left[Q(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}) : Q(\sqrt[3]{2})\right]}_{\deg m_{e^{\frac{2\pi i}{3}}, Q(\sqrt[3]{2})}} \cdot \underbrace{\left[Q(\sqrt[3]{2}) : Q\right]}_{\deg m_{\sqrt[3]{2}, Q}}$$

$$\left.\begin{aligned} m_{\sqrt[3]{2},\mathbb{Q}} &= x^3 - 2 \\ m_{e^{\frac{2\pi i}{3}},\mathbb{Q}(\sqrt[3]{2})} &= x^2 + x + 1 \end{aligned}\right\} \Rightarrow \left[\mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right) : \mathbb{Q}\right] = 2 \cdot 3 = 6$$

$\downarrow$

prvok $e^{\frac{2\pi i}{3}}$ je koreňom polynómu $x^3 - 1$,

ale $x^3 - 1 = (x-1)(x^2+x+1)$

EISENSTAINOVO KRITÉRIUM $\oplus$ GAUSSOVO LEMMA:

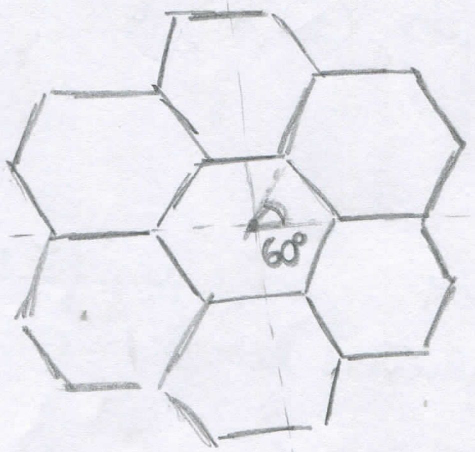
polynóm $x^2 + x + 1 \in \mathbb{Q}[x]$ je ireducibilný

f) $T = \mathbb{R}$

$$\left[\mathbb{R}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right) : \mathbb{R}\right] = \underbrace{\left[\mathbb{R}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right) : \mathbb{R}(\sqrt[3]{2})\right]}_{\deg_{\mathbb{R}(\sqrt[3]{2})}(x^2+x+1)} \cdot \underbrace{\left[\mathbb{R}(\sqrt[3]{2}) : \mathbb{R}\right]}_{\deg_{\mathbb{R}}(x - \sqrt[3]{2})}$$

$$= 2 \cdot 1 = \underline{\underline{2}}$$

5.) Kolika způsoby lze políčka obarvit 3 barvami?




BURNSIDEOVA VĚTA

KONEČNÁ GRUPA $G$ PŮSOBÍ NA MNOŽINU $X$

$$\left| X|_{\sim} \right| = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|$$

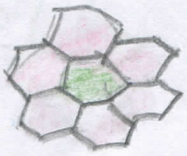
KDE $X_g = \{x \in X \mid g(x) = x\}$ PRO PEVNÉ $g \in G$, MNOŽINA PEVNÝCH BODŮ

A $X|_{\sim} = \{[x]_{\sim} \mid x \in X\}$ POČET ORBIT

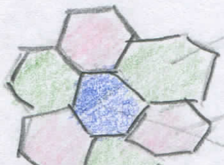
Grupa působící na množinu všech obarvení sestává ze 6 zobrazení: otočení o ±60°, o ±120°, o 180°, id

| ZOBRAZENÍ | POČTY MOŽNÝCH OBARVENÍ |
|---|---|
| otočení o ±60° | $2 \cdot 9$ |

± sousední políčka musí mít stejnou barvu a uprostřed může být jakákoliv barva



otočení o ±120° $\quad 2 \cdot 3 \cdot 3 \cdot 3$

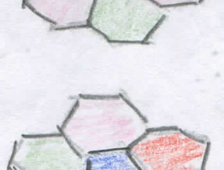


3 možnosti volby

3 možnosti

3 možnosti

otočení o 180° $\quad 3^4$



otočení o 360° - identita $\quad 3^7$

počet obarvení je: $\dfrac{2 \cdot 9 + 2 \cdot 3 \cdot 3 \cdot 3 + 3^4 + 3^7}{6}$

## ALGEBRA II (NMAG202) – TEST, 19. ČERVNA 2017

**Tvrzení a definice pečlivě formulujte včetně všech předpokladů. Odpovědi na otázky zdůvodněte. Pokud používáte nějaké netriviální tvrzení z přednášky, uveďte explicitně odkaz (často budete vyzváni, abyste všechna použitá tvrzení zformulovali). Časový limit je 90 minut.**

(1) Definujte pojem cyklické grupy. Rozhodněte, které z následujících grup jsou cyklické: a) $\mathbb{Z}_{10}^*$, b) $\mathbb{Z}_{11}^*$ c) $\mathbb{Z}_{12}^*$? U cyklických grup najděte generátor. U necyklických stručně zdůvodněte, proč nejsou cyklické.

(10 bodů)

(2) Obsahuje
  (a) grupa $S_5$ podgrupu isomorfní $\mathbb{Z}_8^*$ a
  (b) grupa $D_{14}$ podgrupu isomorfní $\mathbb{Z}_7^*$?

V obou případech buď popište konkrétní isomorfismus, nebo stručně zdůvodněte jeho neexistenci.

(10 bodů)

(3) Definujte pojem kongruence na grupě a bez důkazu vysvětlete vztah k normálním podgrupám. Popište nejmenší kongruenci
  (a) na grupě $S_4$ takovou, že $(1\ 2) \sim (2\ 3)$, a
  (b) na grupě $D_8$ takovou, že otočení o $+90°$ a $-90°$ jsou kongruentní.

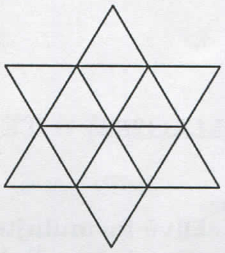
Kolik prvků má v každém z případů faktorgrupa?

(15 bodů)

(4) Formulujte první větu o isomorfismu pro okruhy. Ukažte, že faktor okruhu polynomů $\mathbb{R}[x, y]$ podle ideálu generovaného prvky $x$ a $y$ je isomorfní tělesu $\mathbb{R}$.

(15 bodů)

(5) Přesně formulujte Burnsideovu větu. Kolika způsoby lze z šesti bílých a šesti modrých trojúhelníkových destiček sestavit pravidelnou šesticípou hvězdu jako na obrázku níže? Dvě sestavy považujeme za totožné, dostaneme-li jednu z druhé otočením.



(15 bodů)

(6) Definujte pojem rozkladového nadtělesa polynomu. Přesně formulujte a dokažte větu o jeho existenci.

(20 bodů)

1. Které grupy jsou cyklické?

Najděte generátor nebo zdůvodněte proč není.

a) $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$

ord(1) = 1

ord(3) = 4 - generátor

ANO

$3 \cdot 3 \cdot 3 \cdot 3 = 9 \cdot 9 = 81 = 1$

f) $\mathbb{Z}_{11}^*$ ano, 11 je prvočíslo

$\mathbb{Z}_{11}^* = \{1, \dots, 10\}$ - každý prvek 2, 3, ..., 10 je generátor

e) $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

ord(1) = 1

ord(5) = 2

ord(7) = 2

ord(11) = 2

⟹ NENÍ CYKLICKÁ!

3. KONGRUENCE NA GRUPĚ

nechť $G = (G, *, ', e)$ je grupa,

$\sim$ relace ekvivalence na $G$,

$\sim$ je kongruence, pokud $\forall a_1, b_1, a_2, b_2 \in G$,

$$\begin{matrix} a_1 \sim b_1 \\ a_2 \sim b_2 \end{matrix} \implies a_1 * a_2 \sim b_1 * b_2$$

(3b) Popište nejmenší kongruenci na grupě $D_8$ takovou, že otočení o $90°$ a otočení o $-90°$ jsou kongruentní

$\exists$ bijekce mezi $N \trianglelefteq D_8 \longrightarrow$ kongruence na $D_8$

$\downarrow$

normální podgrupa

že $N \longmapsto \sim_N$ taková, že $a \sim_N b \overset{def}{\iff} ab^{-1} \in N$

$N_\sim := [id]_\sim \longleftarrow\!\!| \sim$

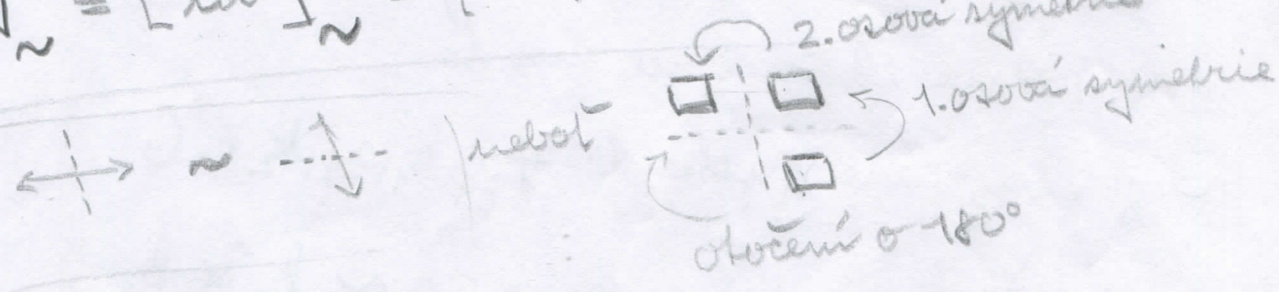
$\to$ bijekce zachovávající inkluze tj. kdykoliv $N \subseteq N' (\subseteq D_8)$, $\iff \sim_N \subseteq \sim_{N'} (\subseteq D_8 \times D_8)$

otočení o $90°$ $\sim$ otočení o $-90°$

$\iff$ identita $\sim$ ot. o $180°$

$N_\sim = [id]_\sim = \{id, \text{ot. o } 180°\}$

neboť




je-li $A \in D_8$, pak $A \circ \underline{\text{otočení o } 180°} \circ A^{-1} = \text{ot. o } 180°$

$A \circ \underline{\text{identita}} \circ A^{-1} = \text{identita}$

$\forall A \in D_8$, proto $N \trianglelefteq D_8$,

tj. $N_\sim = \{id, \circlearrowleft 180°\}$ je normální podgrupa $D_8$

Popište nejmenší kongruenci na $S_4$ takovou, že $(1\ 2) \sim (2\ 3)$

---

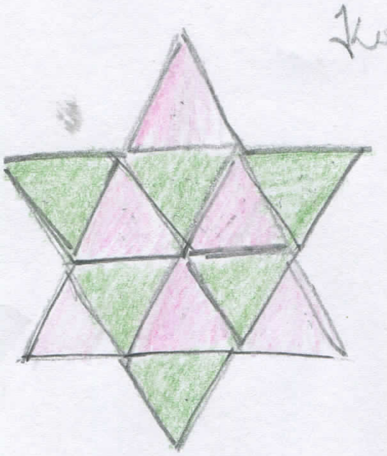
$(1\ 2) \sim (2\ 3)$

$\underbrace{(1\ 2)(2\ 3)}_{(2\ 3\ 1)} \sim \underbrace{(2\ 3)(2\ 3)}_{id}$

tedy $\boxed{N_\sim = [id]_\sim = \{id, (1\ 2\ 3)\}}$

$|S_4/_\sim| = |S_4/A_4|$

Kolika způsoby lze obarvit objekt z 6 bílých a 6 černých $\triangle$?



BURNSIDEOVA VĚTA

$$\left| X|_\sim \right| = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|$$

kde $X|_\sim = \{ [x]_\sim , x \in X \}$

$x \sim y \iff \exists g \in G : y = g(x)$

$X_g = \{ x \in X, g(x) = x \}$

| PRVKY GRUPY $G$ | $\lvert X_g \rvert$ |
|---|---|
| OTOČENÍ O $\pm 60°$ | $2 \cdot 2$ |
| OTOČENÍ O $\pm 120°$ | $2 \cdot 4$ |
| OTOČENÍ O $180°$ | $\binom{6}{3}$ |
| IDENTITA | $\binom{12}{6} = \frac{12!}{6! \cdot 6!}$ |

$$\left| X|_\sim \right| = \frac{1}{6} \cdot \left( 4 + 8 + \frac{6!}{3! \cdot 3!} + \frac{12!}{6!\, 6!} \right)$$

$$= \frac{1}{6}\left( 12 + 20 + \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7}{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2} \right) = \frac{32 + 924}{6} = \frac{956}{6}$$

Obsahuje grupa $S_5$ podgrupu izomorfní $\mathbb{Z}_8^*$ ?

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ , $ord(1) = 1$

$ord(3) = ord(5) = ord(7) = 2$

prvky grupy $S_5$ řádu 2 musí být nutně jen dvojcykly

např. $H := \{ id ; (1\,2) ; (3\;4) ; (1\,2)(3\;4) \} \leq S_5$

$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$

$1 \quad 3 \quad 5 \quad 7$

tj. $H \simeq \mathbb{Z}_8^*$ a $H$ je skutečně podgrupa ($\forall \pi, \rho \in H : \pi \circ \rho \in H$)

Obsahuje grupa $D_{14}$ podgrupu izomorfní $\mathbb{Z}_7^*$ ?

$|\mathbb{Z}_7^*| = 6$ , $|D_{14}| = 14$

Lagrangeova věta : $\boxed{\text{Je-li } H \leq G \text{, pak } |H| \mid |G|}$

Neexistuje $H \leq D_{14}$ taková, že $H \simeq \mathbb{Z}_7^*$

neboť $6 \nmid 14$

(3.) Ukažte, že grupy $\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_8^*$, $S_3$, $D_8$ jsou po dvou neizomorfní.

$$|\mathbb{Z}_2 \times \mathbb{Z}_3| = 6$$
$$|\mathbb{Z}_2 \times \mathbb{Z}_4| = 8$$
$$|\mathbb{Z}_4| = 4$$
$$|\mathbb{Z}_8| = 8$$
$$|\mathbb{Z}_8^*| = 4$$
$$|S_3| = 6$$
$$|D_8| = 8$$

1) $\mathbb{Z}_2 \times \mathbb{Z}_4 \not\cong \mathbb{Z}_8$ neboť $\boxed{\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \iff NSD(m,n) = 1}$

2) $\mathbb{Z}_4 \not\cong \mathbb{Z}_8^*$, $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

$\mathbb{Z}_8^* \rightarrow$ nemá prvek řádu 4

ord(1) = 1
ord(3) = 2
ord(5) = 2
ord(7) = 2

$\mathbb{Z}_4 \downarrow$ cyklická grupa

$\exists$ prvek řádu 4, ord(1) = 4

3) $\mathbb{Z}_8 \not\cong D_8$

grupa $\mathbb{Z}_8$ je cyklická a počet jejích generátorů je $\varphi(8) = \varphi(2^3) = 4$ a to jsou takové prvky $a$, že $NSD(a, 8) = 1$, tedy 1, 3, 5, 7

$D_8 = \{ id, \circlearrowright \circ 90°, \circlearrowright \circ 180°, \circlearrowright \circ 270°, \ldots \}$

řády: 1, 4, 2, 4, 2, 2, 2, 2

4) $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ neboť $NSD(2,3) = 1$

$\mathbb{Z}_6 \rightarrow$ cyklická

$S_3 \cong D_6 = \{ id, \circlearrowright \circ 120°, \circlearrowright \circ 240°, \ldots \}$

řády: 1, 3, 3, 2, 2, 2

$\downarrow$ není cyklická $\Rightarrow S_3 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_3$

Najděte nějaký izomorfismus $(\mathbb{Z}_7^*, \cdot, ^{-1}, 1)$ do $(\mathbb{Z}_6, +, -, 0)$

$\mathbb{Z}_6 \xrightarrow{\varphi} \mathbb{Z}_7^*$

$\varphi(0) = 1$

$\varphi(1) = a \in \mathbb{Z}_7^*$

$\varphi(k) = \varphi(\underbrace{1 + \dots + 1}_{k\text{-krát}}) = \varphi(1) \cdot \ldots \cdot \varphi(1) = (\varphi(1))^k = a^k$

$\forall k, l: \quad \varphi(k+l) = a^{k+l} = a^k \cdot a^l$

generátor $\mathbb{Z}_7^*$ : $\quad \mathrm{ord}(2) = 4$

$\mathrm{ord}(3) = 6$ - generátor

tedy $\varphi(1) = 3$

$\boxed{\varphi(k) = 3^k \quad \forall k = 0,1,2,3,4,5}$

$\varphi(6) = \varphi(2 \cdot 3) = 2$

generátory $\mathbb{Z}_6$ : $1, 5$

$\varphi^{-1} : \mathbb{Z}_7^* \to \mathbb{Z}_6$ : $\boxed{\varphi^{-1}(k) = \log_3 k}$

Určete všechny homomorfismy grupy $(\mathbb{Z}_3, +, -, 0)$ do grupy $(S_5, \circ, ^{-1}, id)$.

---

$\mathbb{Z}_3 = \{0,1,2\}$, $\operatorname{ord}(0) = 1$

$\operatorname{ord}(1) = \operatorname{ord}(2) = 3$

prvky řádu 3 v grupě $S_5$ jsou pouze trojcykly

neboť pro $\pi \in S_n$ je $\operatorname{ord}(\pi) = \mathrm{NSN}$(délek cyklů)

(o rozkladu na nezávislé cykly)

proto homomorfismy budou vypadat takto:

$$\left.\begin{aligned} 1 &\longmapsto id \\ 2 &\longmapsto (a_1\ a_2\ a_3) \\ 3 &\longmapsto (a_1\ a_2\ a_3)^{-1} \end{aligned}\right\}$$

tohle tvoří vždy podgrupu grupy $S_5$

je jich celkem $\binom{5}{3} \cdot 2$

---

ověření: nechť $(a_1\ a_2\ a_3) = (2\ 1\ 3)$

inverze $\begin{pmatrix} 1 & 2 & 3 \\ \uparrow & \uparrow & \uparrow \\ 3 & 1 & 2 \end{pmatrix}$ je: $(3\ 1\ 2)$

$$(2\ 1\ 3) \circ (2\ 1\ 3) = (2\ 3\ 1) = (2\ 1\ 3)^{-1}$$

$\downarrow$ uzavřenost na skládání