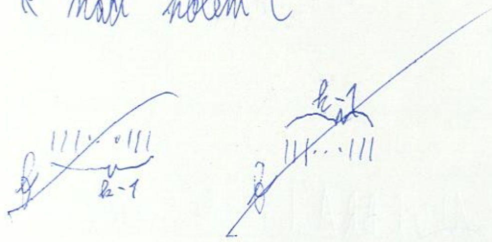
R $\quad s \in R \quad C_s = \{x \mid xs = sx\}$

$$C = \bigcap_{s \in R} C_s$$

R nad polem C_s

R nad polem C



nenírozkladný..? (?) základní věty algebry

1.CV.

1.1.) Rozhodněte, zda daný grupoid je pologrupa, zda obsahuje (levý, pravý) neutrální prvek, zda je to grupa a zda je operace komutativní

1) celá čísla s operací sčítání
2) reálná čísla s operací násobení
3) celá čísla s operací odečítání
4) přirozená čísla s operací největší společný dělitel

1) ~~pologrupa kom. grupa~~ | kom. grupa
2) ~~grupa kom.~~ monoid | není grupa
3) není pologrupa, není kom. | obsahuje ~~žádný~~ zleva pouze pravý neutrální prvek
4) je pologrupa, nemá neutrální prvky, není grupa, je kom.

$((a,b),c) = (a,(b,c))$ △ 0 by existovalo i neutrální prvky

$((a,b),c) \mid a$

$\forall d \quad ((a,b),c) \mid b,c$

$((a,b),c) \mid (b,c)$

$((a,b),c) \mid (a,(b,c))$

1.27.) Nechť G je pologrupa. Dokažte

$(ab)(cd) = a[(bc)d]$

$(ab)(cd) = a[b(cd)] = a[(bc)d]$

1.2.) Pro dané množiny matic typu 2×2 nad reálnými čísly rozhodněte zda je sčítání, resp. násobení matic operací na této množině. Pokud se jedná o operaci, zkuste zjistěte, zdaje operace asoc., kom., zda obsahuje neutrální prvek a zda se jedná o grupu.

1) $\mathbb{Z}$ ($Mat_2\mathbb{Z}$)
2) $\mathbb{Q}$
3) regulární mat $\mathbb{Q}$
4) $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$
5) regulární mat $\mathbb{Z}$

1) $(Mat_2\mathbb{Z}, +)$ je kom. grupa
$(Mat_2\mathbb{Z}, \cdot)$ je kom. monoid (není grupa)

2) stejně jak předtím

3) $(GL(2,\mathbb{Q}),+)$ není operace není grupoid

$(GL(2,\mathbb{Q}),\cdot)$ je to grupa

$A^{-1} = \frac{1}{|A|} \cdot (\tilde{A})^T$

$|A| \in \mathbb{Q}$, $(\tilde{A})^T \in \mathbb{Q}$

4) + není operace

$\{[\begin{pmatrix}0&1\\0&0\end{pmatrix}] + \begin{pmatrix}1&0\\0&1\end{pmatrix}, \cdot, \begin{pmatrix}1&0\\0&1\end{pmatrix}\}$ kom. pologrupa

5)

$\left(\begin{array}{cc|cc} 1&1&1&0\\0&2&0&1\end{array}\right) \sim \left(\begin{array}{cc|cc} 2&2&2&0\\0&2&0&1\end{array}\right) \sim \left(\begin{array}{cc|cc} 2&0&2&-1\\0&2&0&1\end{array}\right) \sim \left(\begin{array}{cc|cc} 1&0&1&-1/2\\0&1&0&1/2\end{array}\right)$

$\begin{pmatrix}2&0\\0&1\end{pmatrix}$ nemá inverzi (jinak jako 3)

1.30.) G je grupa, dokažte, že jediný prvek $g \in G$ $g^2 = g$ je 1.

$g \cdot g = g \cdot 1$

$g = 1$

1.35.) G je grupa, $\forall x \in G\ x^2 = 1 \Rightarrow$ G je abelovská

$(ab)^2 = 1$

$abab = 1$

$(a(ba))b = 1$

$a(ba) = b$

$ba = ab$

1.34) Nechť $G = GL(2,\mathbb{Q})$, $A = \begin{pmatrix}0&-1\\1&0\end{pmatrix}$, $B = \begin{pmatrix}0&1\\-1&1\end{pmatrix}$. Ukažte, že $A^4 = I = B^6$, ale $(AB)^n \neq I$ $\forall n > 0$. Odvoďte z toho, že AB může mít nekonečný řád i když A, B mají konečný řád.

$(AB)^n = \begin{pmatrix}1&-n\\0&1\end{pmatrix}$

1.7.)

∘	a	b	c
a	b	a	c
b	a	b	c
c	c	c	c

$ba = a(aa) = ab = a$

$bb = a(ab) = aa = b$

$bc = a(ac) = ac = c$

$c \cdot a = (cb)a$

$c \cdot b = (ca)a$

$cc = (ca)c$

$cb = (ca)a$

$cc = (ca)c = (cb)c$

i) $ca = a$
$cb = b$
$cc = c$

ii)
$c \cdot (ac) \cdot c = cca$
$c(bc)b = ccb$
$cac\,b = ccb$
$cbca = cca$
$cab = ca$
$cba = ca$

$ca, cb \in \{ab\} \Rightarrow ca = cb \wedge ca \neq cb$

SPORNÉ: $ca = c$

$(ca)(ca) = cca = ca$

$(cb)(cb) = (ca)(cb)$

$(ca)(ca) = (cb)(ca) = c$

$cacca = cca$

$cc = cca = b$

$a \Rightarrow cc = c$

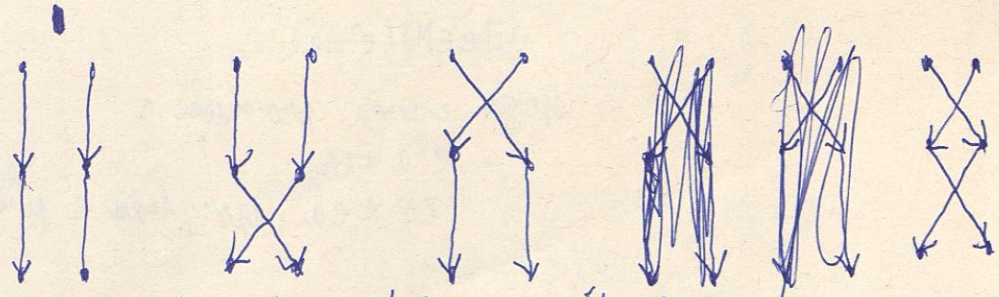
1. PŘ.

- zápočet – 3 V neúčasti
  - max neomluvené
  - 5 nanejvýš neomluvených nepřítomností (alespoň 5 bodů z 10)
  - odpovědníky – 4
    - 30 ze 40 bodů z 1 odpovědníku
    - 3 ze 4 odpovědníků
  - písemná zkouška – alespoň 35 z 70

věta 2.5.

$(i_1 i_2 i_3 \cdots i_k) = (i_1 i_2) \circ (i_2 i_3) \circ (i_3 i_4) \circ \cdots \circ (i_{k-1} i_k)$

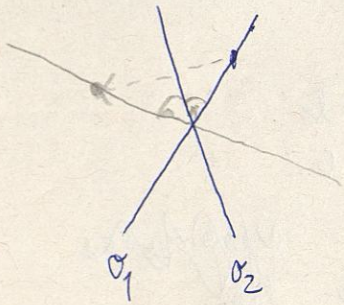
$\varepsilon(\beta\circ\gamma) = \varepsilon(\beta)\cdot\varepsilon(\gamma)$



počet inverzí složení se liší o sudé číslo od součtu počtu inverzí β a γ

$(-1)^{|\beta\circ\gamma|+2k} = (-1)^{|\beta|}\cdot(-1)^{|\gamma|}$

D_n



- $\sigma_2 \circ \sigma_1$ rotace o 2α

$\sigma_1 \circ \sigma_2$ rotace o -2α

2.CV.

2.2.1) V libovolné grupě platí zákony o krácení

$a = a(cc^{-1}) = (ac)c^{-1} = (bc)c^{-1} = b(cc^{-1}) = b$

$a = (cc^{-1})a = c^{-1}(ca) = c^{-1}(cb) = (c^{-1}c)b = b$

* Dokaž, že konečná pologrupa M se zákony o krácení je grupa

~~$e_a(x) = ax$ je bijekce~~

existuje spor $(\forall e \in M)(\exists a_e \in M)\ ea_e \neq a_e$

~~$e_a(x) = xa$ je bijekce~~

$ea = a$

$a, a^2, \dots, a^k, a^{k+1}$

$\mathrm{card}(M) = k$

$r = a^j$ $1 < j < k+1$ ... je nejmenší možné

$a^{j-1} = a$ a^{j-1}

$a^{j-1} = e$

$j - 1 = k + 1$ $(a^{j-1})^2 = a^{j-1} \cdot a^{j-1} = a^{j-2} = a \cdot a^{j-2} = a^{k+1}$

a^{j-1} je idempotent

$a^{j-1} \cdot a^{\ell} = a^{s}$ $s \geq 1$

$a^{\ell+1} = a^{s}$

$a^{j-1} = a^{s} \rightarrow j - 1 = s$ spor

a^{j-1} je idempotent

$(\exists e \in M)(e^2 = e)$

spor $ea \neq a$ pro nějaké a.

$e^2 a \neq ea$

$ea \neq ea$ | spor, tedy e je levý neutrální prvek, pravý je analogicky

$(\forall a)(\exists b)(ab=ba=e)$

$a \neq e$ $\quad a, a^2, a^3, \dots, a^k$

$a^k = e$

$a^{k-1} \neq a^{-1}$, existuje inverzní

$a^{k-1} \cdot a = a \cdot a^{k-1} = e$

$a^{k-1} = a^{-1}$ (jednoznačně určen délky krácení)

*

	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

doplňte nagrupu

$aa = b(ba) = bc = b$

$bb = b(ab) = b(b \cdot b) = ba = c$

* Dokažte, že grupy jsou právě ty pologrupy pro které platí $(\forall a, b)(\exists x, y)(ax = b \wedge ya = b)$

$\Rightarrow$ $\quad x = a^{-1}b$

$\Leftarrow$ $\quad a \cdot e_a = b$ $\quad b \neq a$

$e_a \cdot a = a$ $\quad ax = b$

$ya = b$

$ya e_a = ya$

$b e_a = b$

$e_a = e_b$ analogicky $e'_a = e'_b$

$e' = e'e = e$ máme neutrální prvek

$b = e$: máme inverzi

* Dokažte, že v každé konečné pologrupě existuje idempotent

$a, a^2, a^3, \dots, a^k$

$a^i = a^k$

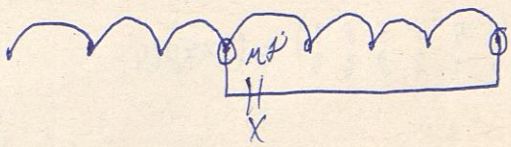
$x := a^i$

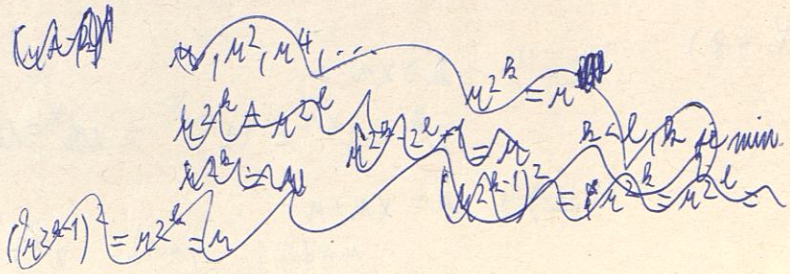
$x^1, x^2, \dots, x^{ka}$

$x^a = x^b$

$a^{i \cdot a} = a^{i \cdot b}$

$b - a = k - i$





$u, u^2, u^4, u^8, \ldots$

$u^{2^k} = u^{2^{k-1}}$

$u^{2^k} = (u^{2^{k-1}})^2 = u^{2^k} u^{2^k} =$

$u^{2^k} u^{2^k} \quad (u^{2^{k-1}})^2 = u^{2^k} = u^{2^k}$

$(x^{2^{k-1}})^2 = x^{2^k} x^{2^k}$

$u = u^{2^k}$

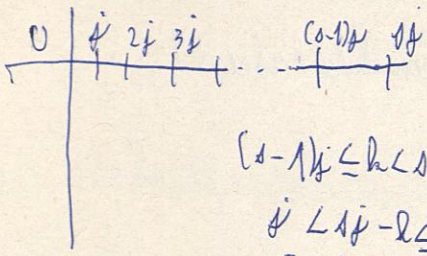
$u^{2^k} = u^{2^{k+1}}$

$(u^{2^k})^2 = u^{2^k} = u$

$(u^{2^k})^2 =$

$[u^{2^{k+1}}]^2 = u^{2^{k+2}}$

$(u^{2^k - 1})^2 =$



$(s-1)i \leq k < si$

$i < si - k \leq i$

$k = (s-1)i$

$k > (s-1)i$

$si - k < i$

$u^{si-k} \neq u^i$

$u^k = u^i$

$u^k \cdot u^{si-k} = u^i = u^{sk}$

$u^i \cdot u^{si-k} = u^{sk}$

$k = (s-1)i$

$k - i = (s-2)i$

$x^1 = x^k$

$x^k = x$

pokud $k \geq 3$

$x^k \cdot x^k = x^1 \cdot x^{2k-1}$

$(x^k)^k = x^k = x$

$(x^k)^s = x^k = x^s$

$x^k \cdot x^k \cdot x^k = x$

1) $s > k$ 2) $s = k$

$x^k = x$

$(x^{k-1})^2 = x^k \cdot x^{k-2} = x \cdot x^{k-2} = x^{k-1}$

2. PŘ.

* $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 7 & 2 & 1 & 9 & 8 & 6 & 5 \end{pmatrix} = (13789)$

*.3.8.) $\Leftarrow$ $k = xn$

$a^k = a^{xn} = (a^n)^x = id^x = id$

$\Rightarrow$ $k = xn + m$

$m \in \{0, 1, \ldots, n-1\}$ $a^k = a^{xn+m} = a^m = id \Rightarrow m = 0$

rozkladní část

$1 \to k+1$

$2 \to k+1 \to 2k+1$

$2k+1 \to 3k+1$

$\vdots$

$1 \xrightarrow{\frac{n}{d}} \frac{n}{d}k+1 = [n,k]+1 \equiv 1 \pmod n$

~~3.10.~~) $(k, k+1), (n, 1)$

$(k+1, k+2) \circ (k, k+1) \circ (k+1, k+2)$

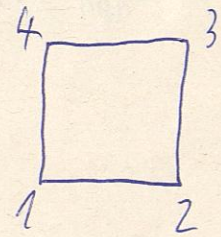
$(k, k+2)$

* 3.11.) Určete následující grupy symetrií. (Zdůvodněte.)

1) $D_3 = S_3$

2) D_4

1	2	3	4
1	2	3	4
4	1	2	3
3	4	1	2
2	3	4	1
2	1	4	3
1	4	3	2
3	2	1	4
4	3	2	1



~~(4 1 2 3) ∘ (3 2 4 1)~~

3) $n = 2k$ $\varphi = \frac{360^\circ}{n}$

n vrcholů → $\frac{n}{2}$ os jdoucích vrcholy → $\frac{n}{2}$ otočení

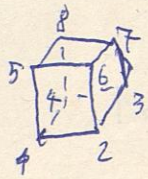
rotace ∘ rotace = ~~rotace~~

$|D_n| = 2n$ první vrchol n způsoby, druhý vrchol 2 způsoby

4)

C_4

5)



$8 \cdot 3 = 24$

3. PŘ.

1 ... nesudální prvek

– nedělitelné (ireducibilní)

4. CV.

* $[17]^{-1}_{181}$

$181 = 10 \cdot 17 + 11$

$17 = 1 \cdot 11 + 6$

$11 = 1 \cdot 6 + 5$

$6 = 1 \cdot 5 + 1$

$1 = 6 - 5 = 6 - (11 - 6) = 2 \cdot 6 - 11 = 2(17 - 11) - 11 = 2 \cdot 17 - 3 \cdot 11 = 2 \cdot 17 - 3(181 - 10 \cdot 17)$

$= 32 \cdot 17 - 3 \cdot 181$

$[17]^{-1}_{181} = 32$

* $[2^k - 1]^{-1}_{2^{2k}+1}$

$2^{2k} + 1 = 2^k(2^k - 1) + 2^k + 1$

$= (2^k + 1)(2^k - 1) + 2$

$2^k + 1 = 2^k(2^{k-1} - 1) \cdot 2 + 1$

$1 = 2^k - 1 - 2 \cdot (2^{k-1} - 1) = 2^k - 1 - (2^{2k} + 1 - (2^k + 1)(2^k - 1)) \cdot (2^{k-1} - 1)$

$= (2^{k-1} - 1)(2^{2k} + 1)$

$1 = 2^k + 1 - 2 \cdot 2^{k-1} = 2^k + 1 - 2^{k-1}(2^{2k} + 1 - (2^k - 1)(2^k + 1))$

$= 2^{k-1}(2^{2k} + 1) = (1 - 2^{k-1})(2^k - 1)$

$2^k - 1 = 2(2^{k-1} - 1) \cdot 2 + 1$

$1 = 2^k - 1 - 2(2^{k-1} - 1) \cdot 2 = 2^k - 1 - (2^{k-1} - 1) \cdot (2^{2k} + 1 - (2^k + 1)(2^k - 1))$

$1 + (2^{k-1} - 1)(2^{2k} + 1) = 2^{2k-1} - 2^k + 2^{k-1}$

$[2^k - 1]^{-1}_{2^{2k}+1} = [2^{2k-1} - 2^k + 2^{k-1}]_{2^{2k}+1}$

* Určete $n \in \mathbb{N}$ taková, že $\varphi(n) \mid n$

$$n \in \{2^{\alpha_1} \cdot 3^{\alpha_2} \mid \alpha_1, \alpha_2 \geq 1\} \cup \{2^{\alpha} \mid \alpha \geq 0\}$$

* $2^{50} + 3^{50} + 4^{50} \equiv 2^2 + 3^2 + 4^2 \equiv 4 + 9 + 1 \equiv 12 \pmod{17}$

* $13 \mid 2^{60} + 7^{30}$

$7^{30} \equiv 7^6 \equiv 49^3 \equiv 10^3 \equiv (-3)^3 \equiv -27 \equiv -1 \pmod{13}$

$2^{60} \equiv 1 \pmod{13}$

* $15^{15^{15}} \pm 1 \quad \varphi(100)$

$15^{15^{15}} \equiv -1 \pmod{4}$

$15^{15^{15}} = 0 \pmod{25}$

$15^{15^{15}} \equiv 75 \pmod{100}$

0, 25, 50, 75

* čínská

$1000 = 8 \cdot 125$

$15^{15^{15}} \equiv (-1)^{15^{15}} \equiv -1 \pmod{8}$

$15^{15^{15}} \equiv 0 \pmod{125}$

0, 125, 250, 375, 500, 625, 750, 875,

$15^{15^{15}} \equiv 375 \pmod{1000}$

* Dokažte, že pro libovolné $n \in \mathbb{N}$ je $2^{2^{2n+1}} + 3$ složené

$2^{2^{2n+1}} \equiv 2^2 \pmod{7}$

$2^{2n+1} \equiv 2^1 \pmod{3}$

$2n + 1 \equiv 1 \pmod{2}$ □

4. PŘ.

3. př.

1 ... neutrální prvek

– neexistuje (různí)

4. CV.

* $[17]^{-1}_{181}$

$181 = 10 \cdot 17 + 11$

$17 = 1 \cdot 11 + 6$

$11 = 1 \cdot 6 + 5$

$6 = 1 \cdot 5 + 1$

$1 = 6 - 5 = 6 - (11 - 6) = 2 \cdot 6 - 11 = 2(17 - 11) - 11 = 2 \cdot 17 - 3 \cdot 11 = 2 \cdot 17 - 3(181 - 10 \cdot 17)$

$= 32 \cdot 17 - 3 \cdot 181$

$[17]^{-1}_{181} = 32$

* $[2^k - 1]^{-1}_{2^{2k}+1}$

$2^{2k} + 1 = 2^k(2^k - 1) + 2^k + 1$

$= (2^k + 1)(2^k - 1) + 2$

$2^k + 1 = 2^k(2^k - 1) \cdot 2 + 1$

$1 = 2^k - 1 - 2 \cdot (2^{k-1} - 1) = 2^k - 1 - (2^{2k} + 1 - (2^k + 1)(2^k - 1)) \cdot (2^{k-1} - 1)$

$= (2^{k-1} - 1)(2^{2k} + 1)$

$1 = 2^k + 1 - 2 \cdot 2^{k-1} = 2^k + 1 - 2^{k-1}(2^{2k} + 1 - (2^k - 1)(2^k + 1))$

$= 2^{k-1}(2^{2k} + 1) = (1 - 2^{k-1})(2^k - 1)$

$2^k - 1 = 2(2^{k-1} - 1) \cdot 2 + 1$

$1 = 2^k - 1 - 2(2^{k-1} - 1) \cdot 2 = 2^k - 1 - (2^{k-1} - 1) \cdot (2^{2k} + 1 - (2^k + 1)(2^k - 1))$

$1 + (2^{k-1} - 1)(2^{2k} + 1) = 2^{2k-1} - 2^k + 2^{k-1}$

$[2^k - 1]^{-1}_{2^{2k}+1} = [2^{2k-1} - 2^k + 2^{k-1}]_{2^{2k}+1}$

* Určete $n \in \mathbb{N}$ taková, že $\varphi(n) \mid n$

$$n \in \{2^{\alpha_1} \cdot 3^{\alpha_2} \mid \alpha_1, \alpha_2 \geq 1\} \cup \{2^{\alpha} \mid \alpha \geq 0\}$$

* $2^{50} + 3^{50} + 4^{50} \equiv 2^2 + 3^2 + 4^2 \equiv 4 + 9 + 1 \equiv 12 \pmod{17}$

* $13 \mid 2^{60} + 7^{30}$

$7^{30} \equiv 7^6 \equiv 49^3 \equiv 10^3 \equiv (-3)^3 \equiv -27 \equiv -1 \pmod{13}$

$2^{60} \equiv 1 \pmod{13}$

* $15^{15^{15}} \pm$

$15^{15^{15}} \equiv -1 \pmod{4}$

$15^{15^{15}} \equiv 0 \pmod{25}$

$0, 25, 50, 75$

$15^{15^{15}} \equiv 75 \pmod{100}$

*

$1000 = 8 \cdot 125$

$15^{15^{15}} \equiv (-1)^{15^{15}} \equiv -1 \pmod{8}$

$15^{15^{15}} \equiv 0 \pmod{125}$

$0, 125, 250, 375, 500, 625, 750, 875,$

$15^{15^{15}} \equiv 375 \pmod{1000}$

* Dokažte, že pro libovolné $n \in \mathbb{N}$ je $2^{2^{2n+1}} + 3$ složené.

$2^{2^{2n+1}} \equiv 2^2 \pmod{7}$

$2^{2n+1} \equiv 2^1 \pmod{3}$

$2n + 1 \equiv 1 \pmod{2}$ □

4. PŘ.

5. CV.

* $(1245)\circ(378)\circ(69)$ má řád $\operatorname{lcm}[4,3,2]=12$

$(12453679)\circ(378)\circ(629) = (12)(39786 45)$ má řád $2\cdot 7=14$

5.3.) $3\cdot 5\cdot 7 = 105$

$3\cdot 4\cdot 7 = 84$

5.6.) řády prvků $[2]_{17}$ a $[13]_{17}$

řád $[2]_{17}$ 8

řád $[13]_{17}$ 4

* řády $\begin{pmatrix}1&0\\2&1\end{pmatrix}$ a $\begin{pmatrix}1&1\\1&2\end{pmatrix}$ v $\mathbb{Z}_3$. $\quad (3^2-1)\cdot(3^2-3) = 8\cdot 6 = 48$

$\begin{pmatrix}1&0\\2&1\end{pmatrix}^2 = \begin{pmatrix}1&0\\1&1\end{pmatrix}$

$\begin{pmatrix}1&0\\2&1\end{pmatrix}^3 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$ řád $\begin{pmatrix}1&0\\2&1\end{pmatrix}$ je 3.

$\begin{pmatrix}1&1\\1&2\end{pmatrix}^2 = \begin{pmatrix}2&0\\0&2\end{pmatrix} = 2\begin{pmatrix}1&0\\0&1\end{pmatrix}$ $\qquad \begin{pmatrix}1&1\\1&2\end{pmatrix}^4 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$

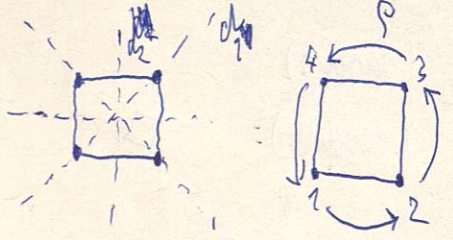
$= 2\begin{pmatrix}1&0\\0&1\end{pmatrix}\cdot\begin{pmatrix}1&1\\1&2\end{pmatrix} \neq \begin{pmatrix}1&0\\0&1\end{pmatrix}$

* najděte $GL(n,\mathbb{Z}_p)$

$|GL(n,\mathbb{Z}_p)| = (p^n-1)\cdot(p^n-p)\cdot(p^n-p^2)\cdots(p^n-p^{n-1})$

$= p^{\frac{(n-1)n}{2}}\cdot(p^n-1)(p^{n-1}-1)\cdots(p-1)$

* najděte podgrupy D_4.



$D_4 = \langle d_1, \rho\rangle$

$d_2 = \rho\circ d_1$

$\{id\}$, $\{id, d_1\}$, $\{id, \rho, \rho^2, \rho^3\}$, $\{id, \rho^2\}$, D_4, $\{id, \rho^2, d_1, d_3\}$, $\{id, \rho^2, \rho\circ d_2, d_4\}$

* dva $A_n \leq S_n$ různé

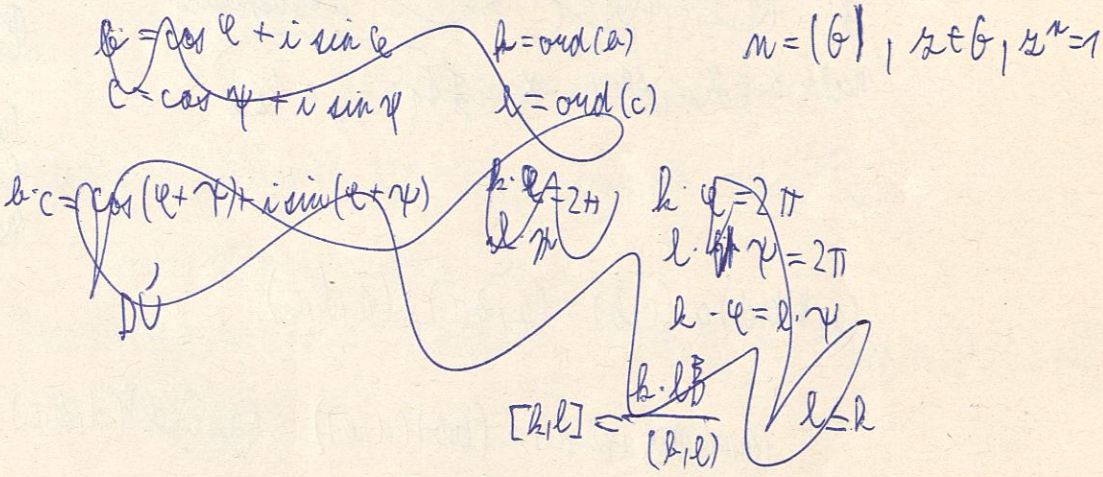
* 6.9.) $\langle (12)(12\dots n) \rangle = S_n$

* 6.CV.

* Určete všechny konečné podgrupy $\mathbb{C}$

$\mathbb{R}^*$: $\{1\}, \{-1,1\}$

$\mathbb{C}^*$: $\{1\}, \{-1,1\}, \dots, \langle e^{i\frac{\pi}{n}} \rangle, \langle \{a \mid a^n = 1\} \rangle$



... ... atd.

* homomorfismy $\mathbb{Z}_n \to \mathbb{Z}_k$

* $(P(X), \div)$ je grupa $X = \{1, \dots, n\}$

$(P(X), \div) \cong \mathbb{Z}_2^n$

je to obrovská operace

$A, B, C \in P(X)$

* vnitřní automorfismy

* libovolný automorfismus v S_n zachovává součin permutace / DÚ

$\beta : S_n \to S_n$

nechť a je transpozice $(a \circ a = id)$, tedy $\beta(a) \circ \beta(a) = id$

$\beta(a) \cdot \beta(a)$ je součin transpozice nebo identita, ale je to izomorfismus, tedy

$\beta(a)$ je součin transpozic

$\beta(a \circ \beta(a)) = \beta(a) \circ \beta(\beta(a))$

$\beta(\beta(a) \circ a) = \beta(a) \circ \beta(\beta(a))$

Komutátory generují A_n.

* $f: G \to G$ $f(x) = x^{-1}$ je automorfismus $\Leftrightarrow$ G je komutativní

$\Leftarrow$ $f(a \cdot b) = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = a \cdot b$

7.CV.

8.4.) $n \in \mathbb{N}$, $n > 4$, dokažte, že A_n nemá vlastní normální podgrupy a že je to jediná netriviální norm. podgrupa S_n

$\alpha \in A_n \setminus \{id\}$

[illegible] ukážeme, že cykly délky 3 generují A_n.

$(1,2,3,4,5) = (\quad)(\quad)$ transpozice

Nechť $\alpha \in A_n$, sudý $\alpha = t_1 \circ \dots \circ t_{2k}$

$(a,b)(a,b) = id$

$(a,b) \circ (b,c) = (a,b,c)$

$(a,b) \circ (c,d) = (a,b,c) \circ (a,d,c)$

$(a,b) \circ (a,d) \circ (c,b) = (a,b,c) \circ (a,d,c)$

$(a,b) \circ (b,c) \circ (a,b) \circ (d,b) = (a,c) \circ (d,b,c) \circ (a,b,d) = (a,c,d)$

$f: S_n \to \mathbb{Z}$ $x \in H$ x liché

$n = 2k+1$

$x = t_1 \circ \dots \circ t_m$

$(a,c,b) \circ (a,b) \circ (a,b,c) = (a,c)$

$t_m \cdots t_{k+2} t_k^{-1} \cdots t_1^{-1} \times t_m^{-1} \cdots t_{k+2}^{-1} t_k \cdots t_1$

8.9.) Dokažte, že $Inn(G)$ je normální podgrupa v $Aut(G)$

$\varphi_a : G \to G$ $\varphi_a(x) = a x a^{-1}$

$Inn(G) = \{\varphi_a \mid a \in G\}$

$\varphi \in Aut(G)$

$\varphi \circ \varphi_a \circ \varphi^{-1}$

$\varphi(\varphi_a(\varphi^{-1}(x))) = \varphi(a \cdot \varphi^{-1}(x) \cdot a^{-1}) = \varphi(a) \cdot x \cdot (\varphi(a))^{-1}$

tedy $\varphi \circ \varphi_a \circ \varphi^{-1} \in Inn(G)$

8.2.) Popište všechny normální podgrupy S_3 a A_4.

$S_3 = \{id, (12), (23), (13), (123), (132)\}$

normální podgrupy: $\{id\}, S_3, A_3$

normální podgrupy A_4: id, A_4, V_4

$A_4 = \{id, (123), (124), (132), (142), (234), (243), (134), (143), \underbrace{(12)(34)}_{\alpha_1}, \underbrace{(13)(24)}_{\alpha_2}, \underbrace{(14)(23)}_{\alpha_3}\}$

$V_4 = \{id, \alpha_1, \alpha_2, \alpha_3\}$ Kleinova grupa

$\alpha_1 \circ \alpha_2 = (14)(23) \ldots$

$(123)(12)(34)(132) = (14)(23) \ldots$

9.11.) S_4/V_4 existuje, protože V_4 není normální dělič S_4

$(13) \circ (12)(34) \circ (13) = (14)(23)$

$(1234) \circ (12)(34) \circ (1432) = (14)(23)$

$(1,2) \circ V_4 = \{(34), (1423), (1324)\}$

$S_4/V_4 = \{V_4, (1,2) \circ V_4, \ldots\}$ $\quad |S_4/V_4| = 6$

DÚ 9.12.) $|G| = 2p$ $\quad |Z(G)| \in \{1, 2, p, 2p\}$

Rokud je G cyklická, tak určitě

Cauchyova (Sylowa) věta, existují $a, b \in G$, $ord(a) = 2$, $ord(b) = p$

$|G/\langle b \rangle| \overset{\text{Lagrange}}{=} 2$, takže $\langle b \rangle$ je normální, tedy $aba = b^x$ $\quad (a = a^{-1})$

$\leftarrow 1 \cdot \langle b \rangle = \langle b \rangle \cdot 1$ $\qquad x \in \{0, 1, \ldots, p-1\}$

Díky dobrý rozkład, tedy bod se rovnají prvkům

tedy $\underbrace{(aba) \cdots (aba)}_{x} = ab^x a = b^{x^2}$, tedy $a^2 b a^2 = b^{x^2}$

$b = b^{x^2}$

$b^{x^2 - 1} = 1$

takže $p \mid (x-1)(x+1)$, tedy $p \mid x-1$ nebo $p \mid x+1$

$\rightarrow x = 1$ $\qquad \rightarrow x = p-1$

$(ab)^2 = abab = baab = b^2$

$(ab)^p = baabaab \cdots baabab = b^p \cdot a = a$

$ord(ab) = 2p$

$aba = b$

$ab = ba$

$b^{-1} a b = a^{-1}$

$aba = b^{p-1}$

$abab = 1 \Rightarrow D_p$

8. CV.

$A_4/V_4 = \{V_4, \{(123), (134), (243), (142)\}, (234)\circ V_4\}$

* $(GL_2(\mathbb{Q}), \circ)$

$N = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{Q}^*\right\}$

$GL_2(\mathbb{Q})/N \cong SL_2(\mathbb{Q})$

* D_n, $n/2n$ n-sylovské podgrupy

$|D_n| = 2n$: $2n = p^k \cdot m$

$D_n = \langle a, b \mid a^n = b^2 = (ba)^2 = 1\rangle$ $p \nmid m$ $p \neq 2$

p-sylow

$b \cdot a^x$

$(b\cdot a^x)^2 = b\cdot a^x \cdot b \cdot a^x = (ba)a^{x-1}(ba)a^{x-1} = a^{-1}\cdot b\cdot a^{x-1}\cdot(a^{-1}\cdot b)a^{x-1} = \dots = a^{2x}$

$b\cdot a^x = a^{2y}$

$b = a^{2y-x}$

$H \leq \langle a\rangle$

$a^{-y}\cdot a^x \cdot a^y = a^x \in H$

H

$(b\cdot a^y)^{-1}\cdot a^x \cdot b\cdot a^y = a^{-y}\cdot b\cdot a^x \cdot b a^y = \dots = (a^{-1})^x \in H$

H normální

$H = \langle a^{\frac{m}{2}}\rangle = \langle a^{\frac{n}{2^k}}\rangle$

* $2 \nmid n$ D_n $n/2n$

$n = 1$

$n \geq 3$

$n = 2$

$n \in 2\mathbb{Z}$ (viz. předchozí úloha)

$2n = p^k \cdot m$

$k = 1$, $n = m$

$N = \langle b\cdot a^n\rangle$

$b\cdot a^n \cdot b \cdot a^n = 1$

* n-sylovské podgrupy S_4

3-sylovské: $\{id, a, a^{-1}\}$ a 3-cykly

2-sylovské: $\langle(1234), (12)(34)\rangle$, $\langle(12)(34), (13)(24), (14)(23)\rangle$

6.10 9.PŘ

$a^{\lambda(n)} \equiv 1 \pmod{n}$

- Rozložte grupu $(\mathbb{Z}_{60}^{\times}, \cdot)$ na součin cyklických grup.

$\varphi(60) = 16$

$\mathbb{Z}_{60}^{\times} = \{[1]_{60}, [7]_{60}, [11]_{60}, [13]_{60}, \dots, [59]_{60}\}$

spočítáme řády všech prvků a najdeme prvek nejvyššího řádu, který je nesoucím prvočísla

$\text{ord}([1]_{60}) = 1$

$\text{ord}([7]_{60}) = 4$

$\langle [7]_{60} \rangle = \{[1]_{60}, [7]_{60}, [-17]_{60}, [-11]_{60}\}$

Hledáme prvek co nejvyššího řádu k, ale takový, aby $a, a^2, \dots, a^{k-1} \notin \langle [7] \rangle$

$[-1]_{60} \notin \langle [7]_{60} \rangle$ má řád 2

$\langle [7]_{60}, [-1]_{60} \rangle = \{[1], [-1], [7], [-7], [-17], [17], [-11], [11]\}$

$[19]^2 = [361] = [1]$

$\langle [7], [-1], [19] \rangle = \mathbb{Z}_{60}^{\times}$ $\qquad \mathbb{Z}_{60}^{\times} \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

~~10.CV.~~

9.CV.

* 11.3) $a^n = 1$ $\qquad \text{ord}(x) = m$

$ax \neq xax \neq ax$

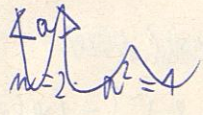
$x^{m-1} x a \neq x$

$(x^m) x a = 1$

$(xax^{-1})^n = x a^n \cdot x^{-1} = 1$

$xax^{-1} = a$

$xa = ax$



11.4) i) $[x,y]^{-1} = [y,x]$ $\qquad 1 = [1,1]$

$c \in G', g \in G$

$g^{-1} \cdot c \cdot g \cdot c^{-1} \in G'$

ať tedy $g^{-1} \cdot c \cdot g \cdot c^{-1} \cdot c = g^{-1} \cdot c \cdot g \in G'$

ii) $a, b \in G$

$a \cdot G' \cdot b \cdot G' = b \cdot G' \cdot a \cdot G'$

$a \cdot b \cdot a^{-1} \cdot b^{-1} \in G'$

$ab \cdot G' = b \cdot a G'$

iii)

$a, b \in G$ $\quad aba^{-1} \in H$

$b \in H$ $\quad abH = baH$

$G' \ni [a,b] = aba^{-1}b^{-1} \in H$ — generátory G'

$G' \subseteq H$

iv) ~~$G = \{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$~~

$M, N \in G$

$|[M,N]| = 1$

$[M,N] = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ (asi)

$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & -\frac{b}{ca} \\ 0 & \frac{1}{c} \end{pmatrix}$

$\begin{pmatrix} \frac{1}{a} & -\frac{b}{ca} \\ 0 & 1/c \end{pmatrix} \begin{pmatrix} \frac{1}{\bar{a}} & -\frac{\bar{b}}{c\bar{a}} \\ 0 & \frac{1}{\bar{c}} \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} \bar{a} & \bar{b} \\ 0 & \bar{c} \end{pmatrix}$

$\begin{pmatrix} \frac{1}{a\bar{a}} & -\frac{a\bar{b}+b\bar{c}}{a\bar{a}c\bar{c}} \\ 0 & \frac{1}{c\bar{c}} \end{pmatrix} \cdot \begin{pmatrix} a\bar{a} & a\bar{b}+b\bar{c} \\ 0 & c\bar{c} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

~~$G \setminus \{I_2\} \cong G$~~

*11.5.) i) $(1,1)$ ... neutrální prvek

~~Def~~ $(a,e)^{-1} = (e(b^{-1})(a^{-1}), b^{-1})$

+ asociativita

wreath product semidirect

ii) ~~$e = id$~~ $\quad e(b)(c) = c$

iii) $(1,1)$ ... neutrální prvek

~~$c = b^{-1}$~~

$e(b)(c) = bcb^{-1}$

*11.6.)

$\varepsilon_b(a) := a \cdot b$

$\chi_b(a) := \varepsilon_a^2(a) = a \cdot b^2$ je bijekce

DÚ

~~$b^2 \cdot a = c^2 \cdot b$~~

9. PŘ.

- def. homomorfismu!

ker $f = \{a \in R \mid f(a) = 0\}$

Isom. věta - kom.

Bacha! - $\{0\}$ není podokruh $\mathbb{Z}$, ale je to obrus

10. CV.

* Rozhodněte zda zobrazení $f: \mathbb{C} \to \mathbb{C}$ je homomorfismus okruhu $(\mathbb{C}, +, \cdot)$ do $(\mathbb{C}, +, \cdot)$

a) $f(a+bi) = a+b$

$f(0) = 0$

$f(1) = 1$

~~$f(a+bi+c+di)$~~ sčítání je zachování

$f((a+bi)(c+di)) = f(ac - bd + i(bc+ad)) = ac - bd + bc - ad$

$f(a+bi) \cdot f(c+di) = (a+b)(c+d) = ac + bd + ad + bc$

není homomorfismus

* $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$ podokruh $(\mathbb{R}, +, \cdot)$. Ukažte, že $(\mathbb{Q}(\sqrt{3}) \setminus \{0\}, \cdot)$ je těleso

stačí najít inverzi $\frac{1}{a+b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} = \frac{a}{a^2-3b^2} + \frac{-b}{a^2-3b^2}\sqrt{3}$ ✓

$\neq 0$, protože $\frac{a}{a^2-3b^2}$ je racionální

* dokažte, že libovolný homomorfismus $\alpha: \mathbb{Q}(\sqrt{3}) \to \mathbb{C}$ je identický na $\mathbb{Q}$, tj. $\alpha(r) = r$, $\forall r \in \mathbb{Q}$

~~$\alpha(a+b\sqrt{3}) = \alpha(a) + \sqrt{3}\alpha(b)$~~

~~$\alpha(a+b\sqrt{3}) = \alpha(a) + \alpha(\sqrt{3}b)$~~

$\alpha(1) = 1$

$\alpha(n) = n \quad n \in \mathbb{N}$

$\alpha\left(\frac{1}{n}\right) = \frac{1}{n} \quad \alpha\left(\frac{n}{q}\right) = \frac{n}{q}$

↑ těleso

* popište všechny homomorfismy $\alpha: \mathbb{Q}(\sqrt{3}) \to \mathbb{C}$

$\alpha(\sqrt{3}) \cdot \alpha(\sqrt{3}) = \alpha(3) = 3$

$\alpha(\sqrt{3}) = \pm\sqrt{3}$

$\alpha(a + b\sqrt{3}) = a \pm b\sqrt{3}$

$\alpha((a+b\sqrt{3})(c+d\sqrt{3})) = (\alpha(a)+\alpha(\sqrt{3}b))(\alpha(c)+\alpha(\sqrt{3}d))$

$= (a-b\sqrt{3})(c-\sqrt{3}d) = ac+3bd-\sqrt{3}(bc+ad)$

$\alpha(ac+3bd+\sqrt{3}(bc+ad)) = ac+3bd-\sqrt{3}(bc+ad)$ ✓ žádné nejsou izomorfismy

* $h(x) = x^4 - x^3 - 7x^2 + x + 6$

	1	−1	−7	1	6
1	1	0	−7	−6	0
−1	1	−1	−6	0	
2	1	1	−4		
−2	1	−3	0		

$h(x) = (x-1)(x^3-7x-6)$

$= (x-1)(x+1)(x^2-x-6)$

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

* $\dfrac{12x^4+3x^3-4x+3}{2x^2-1} = 6x^2 + \dfrac{3x^3+6x^2-4x+3}{2x^2-1} = 6x^2 + \dfrac{3}{2}x + \dfrac{6x^2 - \frac{5}{2}x + 3}{2x^2-1} =$

$= 6x^2 + \frac{3}{2}x + 3 + \dfrac{-\frac{5}{2}x+6}{2x^2-1}$

* $f(x) = x^6 - 6x^5 + 9x^4 + 8x^3 - 24x^2 + 16$

~~Řekněte, že 2 je 2-násobný kořen~~ rozhodněte kolika násobný je ten kořen

	1	−6	9	8	−24	0	16
2	1	−4	1	10	−4	−8	0
2	1	−2	−3	4	4	0	
2	1	0	−3	−2	0		
2	1	2	1	0			
2	1	4	9				

$h(x) = (x-2)^4(x+1)^2$

* $x^5 - ax^2 - ax + 1 \in \mathbb{Q}[x]$

najděte a tak aby byl dvojnásobný kořen $c=-1$

	1	0	0	−a	−a	1
−1	1	−1	1	−1−a	1	0
−1	1	−2	3	−4−a	5+a	

$\longrightarrow a = -5$

$x^5 + 5x^2 + 5x + 1$

* $b(x) = nx^{n+1} - (n+1)x^n + 1 \in \mathbb{Z}[x]$

dokažte, že pro všechna $n \in \mathbb{N}$ je $c=1$ dvojnásobný kořen

určitě $b(1)=0$

$n>1$: $f'(x) = n(n+1)x^{n+1} - (n+1)nx^{n-1} = 0$

$x^{n+1} - x^{n-1} = 0$

$x^{n-1}(x-1) = 0$ není kořen derivace

$$\frac{nx^{n+1} - (n+1)x^n + 1}{x-1} = nx^n + \frac{-x^n + 1}{x-1} = nx^n - x^{n-1} - x^{n-2} - \dots - x - 1$$

$n \cdot 1 - 1 - 1 - \dots - 1 = 0$

* Vyjádřete polynom $f(x) = x^4 + 2x^3 - 3x^2 - 4x + 1$ v mocninách $x+1$

$$f(x) = f(-1) + f'(-1)(x+1) + \frac{f''(-1)(x+1)^2}{2} + \frac{f'''(-1)(x+1)^3}{6} + \frac{f''''(-1)(x+1)^4}{24}$$

$f'(x) = 4x^3 + 6x^2 - 6x - 4$ $\quad f(-1) = 1$ $\quad f''''(-1) = 24$

$f''(x) = 12x^2 + 12x - 6$ $\quad f'(-1) = 4$

$f'''(x) = 24x + 12$ $\quad f''(-1) = -6$

$f'''(-1) = -12$

$f(x) = 1 + 4(x+1) - 3(x+1)^2 - 2(x+1)^3 + (x+1)^4$

* $f(x) = (x-2)^4 + 4(x-2)^3 + 6(x-2)^2 + 10(x-2) + 20$

$= ((x-2)+1)^4 + 6(x-2) + 19 = (x-1)^4 + 6x + 7 = x^4 - 4x^3 + 6x^2 + 2x + 8$

* $f(x) = 12x^6 + 8x^5 - 85x^4 + 15x^3 + 55x^2 + x - 6$

$f'(x) = 72x^5 + 40x^4 - 336x^3 + 45x^2 + 110x + 1$ zbytek

$12x^6 + 8x^5 - 84x^4 + 15x^3 - 5$

$\frac{f(x)}{f'(x)} = \frac{1}{6}x + \dots$ $\quad (72x^5 + 40x^4 - 336x^3 + 45x^2 + 110x + 1)$

$\frac{f(x)}{f'(x)} = \frac{1}{6}x + \dots$ $\quad f'(x)$

	12	8	-85	15	55	1	-6
1	12	20	-65	-50	5	6	0
2	12	44	23	-4	-3	0	
-3	12	8	-1	-1	0		
$-\frac{1}{2}$	12	2	-2	0			

$f(x) = (x-1)(x-2)(x+3)(x+\frac{1}{2})(12x^2 + 2x - 2)$

$6x^2 + x - 1 = \frac{(6x)^2 + (6x) - 6}{6} = \frac{(6x+3)(6x-2)}{6} = (2x+1)(3x-1)$

$f(x) = 12(x-1)(x-2)(x+3)(x+\frac{1}{2})^2(x-\frac{1}{3})$

11. CV.

* $2x^6 - x^5 - 11x^4 - x^3 + ax^2 + 2ax + 8$

určete a aby to mělo kořen 2 a pro to a určete všechny kořeny

	2	−1	−11	−1	a	2a	8
2	2	3	−5	−11	a−22	4a−44	8a−80
2	2	7	9	7	2	0	
2	2	11					
−2	2	3	3	1	0		
−1	2	1	2	−1			
$-\frac{1}{2}$	2	2	2	0			

$8a - 80 = 0 \rightarrow a = 10$

$x^2 + x + 1 = 0$ ... zatím nemá reš. kořeny

všechny reš. kořeny jsou $2, 2, -2, -\frac{1}{2}$

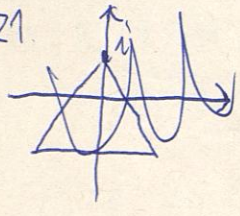
* $x^4 + 2x^3 - 3x^2 + ax - 4$

určete a všechna taková, že polynom má reš. kořen

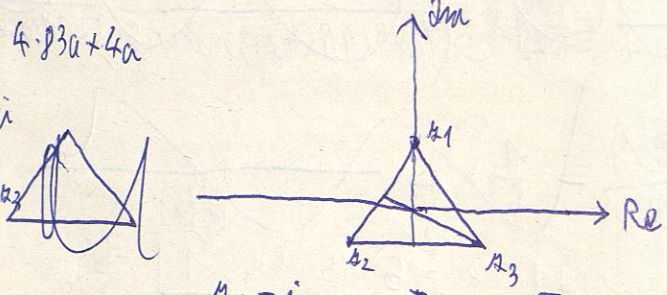
	1	2	−3	a	−4
1	1	3	0	+a	a−4
−1	1	1	−4	4+a	−8−a
2	1	4	5	10+a	2a+16
−2	1	0	−3	6+a	−16−2a
−4	1	−2	5	−20+a	76−4a
4	1	6	21	84+a	4·83a+4a

$a \in \{4, -8, 19, -83\}$

* [illegible]



najděte rovnicí jejich kořeny jsou z_1, z_2, z_3



$z_1 = i = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$

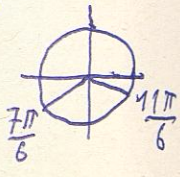
$z_2 = \cos\left(\frac{\pi}{2} + \frac{2\pi}{3}\right) + i\sin\left(\frac{\pi}{2} + \frac{2\pi}{3}\right)$

$= \cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}$

$z_3 = \cos\left(\frac{11\pi}{6}\right) + i\sin\left(\frac{11\pi}{6}\right)$

$z_2 = -\frac{\sqrt{3}}{2} - i\frac{1}{2}$

$z_3 = \frac{\sqrt{3}}{2} - i\frac{1}{2}$



$(x-i)\left(x+\frac{\sqrt{3}}{2}+i\frac{1}{2}\right)\left(x-\frac{\sqrt{3}}{2}+i\frac{1}{2}\right) = (x-i)\left(x^2+xi+1\right) = \underbrace{x^3+i=0}_{\text{hledaná rovnice}}$

* rozložte na ireducibilní polynomy nad $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

$$x^3-\frac{5}{6}x^2-\frac{1}{2}x+\frac{1}{3} = \frac{1}{6}(x-1)(6x^2+x-2) = (x-1)(x+\tfrac{2}{3})(x-\tfrac{1}{2})$$

$6x^3-5x^2-3x+2$

	6	−5	−3	2
1	6	1	−2	0

$x_2 = -\frac{2}{3}$

$x_3 = \frac{1}{2}$

* sc sami

$9x^6-21x^5-17x^4+15x^3-42x^2-34-6$

	9	−21	−17	15	−42	−34	−6
−1	9	−30	13	2	−44	10	16
2							
−2							
$\frac{1}{3}$	9	−18	−11	$\frac{34}{3}$	$-\frac{344}{9}$	$\frac{574}{27}$	
$\frac{2}{3}$	9	−15	−27	−3	−44		
$-\frac{2}{3}$	9	−17	1	$\frac{43}{3}$	$-\frac{212}{9}$		
3	9	6	1	18	12	2	0
$-\frac{1}{3}$	9	3	0	18	6	0	
$-\frac{1}{3}$	9	0	0	18			

$x^3+2=0$

$\mathbb{Q}$: $\boxed{9(x^3+2)(x-3)(x+\frac{1}{3})^2}$

$\mathbb{R}$: $\boxed{9(x+\sqrt[3]{2})(x^2-\sqrt[3]{2}x+\sqrt[3]{4})(x-3)(x+\frac{1}{3})}$

$\mathbb{C}$: $x_{1,2} = \frac{+\sqrt[3]{2} \pm \sqrt{\sqrt[3]{4}-4\sqrt[3]{4}}}{2} = \sqrt[3]{\frac{1}{4}}(1 \pm i\sqrt{3})$

$9(x+\sqrt[3]{2})\left(x-\sqrt[3]{\frac{1}{4}}(1+i\sqrt{3})\right)\left(x+\sqrt[3]{\frac{1}{4}}(1+i\sqrt{3})\right)(x-3)(x+\frac{1}{3})^2$

* $4x^5 - 4x^4 - 5x^3 - 7x^2 + x + 2$

	4	-4	-5	-7	1	2
1						
-1						
2	4	4	3	-1	-1	0
$\frac{1}{2}$	4	6	6	2	0	
$-\frac{1}{2}$	2	2	2	0		

$\mathbb{R}, \mathbb{Q}$: $4(x-2)(x-\frac{1}{2})(x+\frac{1}{2})(x^2+x+1)$

$x = -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$

$\mathbb{C}$: $4(x-2)(x-\frac{1}{2})(x+\frac{1}{2})(x+\frac{1}{2}+i\frac{\sqrt{3}}{2})(x+\frac{1}{2}-i\frac{\sqrt{3}}{2})$

* najděte normovaný polynom nejmenšího stupně nad $\mathbb{R}[x]$ s kořeny $-\frac{1}{3}, 3+2i, 3+2i$

$(x-3-2i)(x-3+2i) = x^2 - 6x + 13$

$\mathbb{C}$: $(x+\frac{1}{3})(x^2-6x+13)(x-3-2i)^a(x-3+2i)(x-3-2i)(x-3+2i)$

$\mathbb{R}, \mathbb{Q}$: $(x^2-6x+13)^2(x+\frac{1}{3})$

* $x^6 - x^5 - x^4 - x^3 - x^2 - x + 1 \in \mathbb{Z}_3[x]$

	1	-1	-1	-1	-1	-1	1
1	1	0	-1	1	0	-1	0
1	1	1	0	1	1	0	
-1	1	0	0	1	0		
-1	1	-1	1	0			
-1	1	1	0				
-1	1	0					

$(x-1)^2(x+1)^4$

* $\mathbb{Z}_7[x]$ $x^3 + x^2 + x + a$

3 d)

	1	1	1	a
0	1	1	1	a
1	1	2	3	3+a
2	1	3	0	a
3	1	4	6	a+6
4	1	5	0	a
5	1	6	3	a+1
6	1	0	1	a+6

$a \in \{2, 5\}$

(v posledním sloupci nesmí být 0.)

12. CV.

R těleso, $f \in R[x]$

A) f je ired. nad R
B) f nemá v R žádný kořen

st $f = 1$ A platí, B neplatí
st $f \geq 2$ A $\Rightarrow$ B
st $f \in \{2,3\}$ B $\Rightarrow$ A

* 39 a) ~~$(x+1)^5$~~ ~~$(x^2+x+1)(x^3+x+1)$~~ x^5+x^4+1

úplné ired. polynomy:

- $x, x+1$
- x^2+x+1
- x^3+x+1, x^3+x^2+1
- $x^4+x+1, x^4+x^3+1, x^4+x^3+x^2+x+1$

$$\frac{x^5+x^4+1}{x^2+x+1} = x^3+x+1$$

* 39 e) $(x-2)^2(x-4)(x^3+x^2+1)$

$1^3=1$ $1^2=1$
$2^3=3$ $2^2=-1$
$3^3=2$ $3^2=-1$
$4^3=4$ $4^2=1$

* Napište nejmenší podobor tělesa $\mathbb{C}$ obsahující číslo $\sqrt[5]{2}$

$$\mathbb{Z}[\sqrt[5]{2}] = \{a+b\sqrt[5]{2} \mid a, b \in \mathbb{Z}\}$$

$$= \{f(\sqrt[5]{2}) \mid f \in \mathbb{Z}[x]\} = \{a_0 + a_1\sqrt[5]{2} + a_2\sqrt[5]{4} + a_3\sqrt[5]{8} + a_4\sqrt[5]{16} \mid a_i \in \mathbb{Z}\}$$

$\alpha = e^{i\frac{2\pi}{7}}$

$$\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[x]\} = \{a_0 + a_1\alpha + \dots + a_6\alpha^6 \mid a_0, \dots, a_6 \in \mathbb{Z}\}$$

$$= \{a_0 + a_1\alpha + \dots + a_5\alpha^5 \mid a_0, \dots, a_5 \in \mathbb{Z}\}$$

$$x^6+x^5+\dots+x+1 = \frac{x^7-1}{x-1} = \frac{(y+1)^7-1}{y} = \sum_{i=1}^{7}\binom{7}{i}y^{7-i-1}$$ ... ired. dle Eisensteina

* Rozložte v $\mathbb{C}[x]$ na lineární činitele polynom f, nebo-li, že f má alespoň 1 vícenásobný kořen (tj. alespoň dvojnásobný) kořen:

$$f = x^4 + 2ix^3 + x^2 + 2ix + 1$$

$$f' = 2(2x^3 + 3ix^2 + x + i)$$

$$\frac{x^4 + 2ix^3 + x^2 + 2ix + 1}{2x^3 + 3ix^2 + x + i} = \frac{1}{2}x + \frac{1}{4}i + \frac{\frac{5}{4}x^2 + \frac{5}{4}ix + \frac{5}{4}}{2x^3 + 3ix^2 + x + i}$$

$$\frac{2x^3 + 3ix^2 + x + i}{x^2 + ix + 1} = 2x + i + \frac{0}{x^2 + ix + 1}$$

$x^2 + ix + 1 = 0$ $d = (f, f') = x^2 + ix + 1$

$$D = -5$$

$$\alpha_{1/2} = \frac{-i \pm i\sqrt{5}}{2} = i \cdot \frac{-1 \pm \sqrt{5}}{2}$$

(2 dvojnásobné kořeny f.)

$$f = (x - \alpha_1)^2 (x - \alpha_2)^2$$

α je k-násobný kořen f
α je $(k-1)$-násobný kořen f'
α je $(k-1)$-násobný kořen d
α je jednoduchý kořen $\frac{f}{d}$

* ~~12-stěn~~ 12-sten ~~grupa~~ grupa G rotací $G \cong A_5$

				řády	
1	id			1	id
24	~~osy protějších stěn~~ osa procházející středy protějších stěn	6 os	$\pm 72°, \pm 144°$	5	cyklus délky 5
20	osa procházející středy protějších hran	10 os	$\pm 120°$	3	cyklus délky 3
15	osa procházející středy protějších hran		$180°$	2	složení transpozic

grupa G' všech symetrií není isomorfní S_5

$$G' \cong \mathbb{Z}_2 \times G \cong \mathbb{Z}_2 \times A_5$$

T. Středová