Aritmetika a algebra II

Osnova předmětu

1. Lineární rovnice, řešení v tělesech $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$, počet řešení v okruhu $\mathbb{Z}_n$, $n \in \mathbb{N} \setminus \mathbb{P}$.

2. Kvadratická rovnice. Didaktický postup, řešení speciálních případů, odvození Viétových vzorců. Odvození vzorce pro kořeny: klasické doplnění na čtverec, mezopotámské řešení na základě Viétových vzorců, řešení soustavy z Vietových vět. Geometrické znázornění reálných a komplexních kořenů rovnice s reálnými koeficienty.

3. Kubická rovnice. Substituce pro odstranění členu obsahujícího x^2, Cardanův postup řešení (substituce $y = u + v$), kvadratická resolventa, diskriminant kubické rovnice, význam výrazu $D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$. Získání všech kořenů pomocí $\varepsilon = \cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3}$. Vlastnosti u, v. Vietovy vzorce. Casus irreducibilis – řešení pomocí goniometrické substituce.

4. Rovnice binomické, trinomické, bikvadratické.

5. Reciproká rovnice 1. druhu ($a_k = a_{n-k}$, stupně $n = 2k + 1$ a $n = 2k$) a 2. druhu ($a_k = -a_{n-k}$), vlastnosti, kořeny, řešení.

6. Základní věta algebry a její důsledky.

7. Konstrukce oboru celých a racionálních čísel, abstraktní podstata obou konstrukcí: rozšíření komutativního monoidu na grupu. Podílové pole oboru integrity celých čísel.

8. Iracionální čísla. Důkaz iracionality odmocnin přirozených čísel, která nejsou čtverci. Čísla algebraická a transcendentní. Mohutnost množiny všech algebraických čísel. Liouvilleovo číslo, mohutnost množiny všech transcendentních čísel. Bez důkazu: věta Gelfandova–Schneiderova. Důkaz iracionality čísla e. Pro zajímavost: důkaz iracionality čísla π (nezkouší se). Konstrukce druhých odmocnin.

9. Pole reálných čísel – zavedení: 1) desetinné rozvoje, 2) Dedekindovy řezy, 3) axiomatické zavedení reálných čísel, 4) základní myšlenka zúplnění $\mathbb{Q}$, cauchyovské posloupnosti.

10. Pole komplexních čísel: zavedení (problémy se zavedením), vlastnosti, geometrie v komplexní souřadnici.

11. Hyperkomplexní čísla: neúspěšné snahy o aritmetizaci bodů (třírozměrného) prostoru, tj. rozšíření $\mathbb{C}$ o jednu další imaginární jednotku; kvaterniony (základní myšlenka).

12. Řetězové zlomky: konečné, nekonečné, periodické; výpočet článků řetězového zlomku čísel racionálních, iracionálních, druhých odmocnin. Aproximace racionálních a iracionálních čísel řetězovými zlomky, přesnost aproximace, chování posloupnosti konvergentů (věta „o cikcaku“). Řešení lineární diofantické rovnice a Pellovy rovnice pomocí řetězových zlomků.

13. Průměry: harmonický, geometrický, aritmetický, kvadratický. Geometrické znázornění, úloha o pohybu a harmonický průměr.

14. Grupy, homomorfismy grup, faktorizace. Relace kongruence, normální podgrupa, jádro homomorfismu je normální podgrupou. Lagrangeova věta. Cyklické grupy.

15. Dělitelnost, prvočinitel, ireducibilní prvek, nsn, NSD, eukleidovské obory integrity.

Literatura k předmětu:

[BeDla] Bečvář J., Dlab V.: *Od aritmetiky k abstraktní algebře.* Serifa, Praha, 2016.

Podmínky udělení zápočtu:

- portfolio: je třeba jej přinést ke zkoušce (praktická část), ověřuje se samostatné vypracovávání domácích úkolů (úlohy označené hvězdičkou) v průběhu semestru
- úspěšné napsání testíku s úlohami (tzv. praktická část) na kterémkoli vypsaném termínu zkoušky (je možno používat samostatný kalkulátor; ne v mobilu, ne grafický)

Požadavky ke zkoušce:

zkouškový testík (tzv. teoretická část) cca 90 min., ověřuje se dobrá znalost teorie (definice, věty, důkazy) v rozsahu probíraném na seminářích (včetně úloh zadávaných k samostatnému rozmyšlení)

Materiály k jednotlivým tématům

- lineární a kvadratická rovnice: zde
- kubická rovnice: zde
- casus irreducibilis, binomické a trinomické rovnice: zde
- odmocniny a reciproké rovnice: zde
- tzv. základní věta algebry: zde

- text o konstrukci $(\mathbb{Z}, +)$ na základě $(\mathbb{N}, +)$, rozšíření komutativního monoidu na grupu a o zavedení $\mathbb{Q}$: zde
- tabule ke konstrukci podílového pole: zde
- tabule k iracionálním číslům (a také algebraickým a transcendentním): zde
- tabule k důkazu iracionality e a π: zde (důkaz iracionality π se nezkouší)
- reálná čísla: v příslušné kapitole
- komplexní a hyperkomplexní čísla: zde
- pro zájemce: hyperkomplexní čísla – scan z knihy: zde

- řetězové zlomky, lineární diofantická rovnice a Pellova rovnice: zde (kromě poslední strany věnované souvislosti ŘZ s řadami)
- průměry: zde
- faktorizace grup (základní idea) a Lagrangeova věta: zde

1 Kvadratická rovnice

1. * Najděte všechna řešení rovnice v $\mathbb{Z}_3$ (tj. v poli):
   a) $x^2 + 2 = 0$ b) $x^2 + x + 1 = 0$ c) $x^2 + x + 2 = 0$ d) $x^3 + 2x = 0$

   A pro zajímavost – kořenů může být více, než je stupeň rovnice
   a) $x^3 + 5x$ v $\mathbb{Z}_6$ b) $x^3 + 5x + 1$ v $\mathbb{Z}_6$

2. * Vyřešte mezopotámským způsobem kvadratickou rovnici

$$x^2 + 2 = 3x\,.$$

3. * Najděte souřadnice vrcholu V paraboly $y = ax^2 + bx + c$.

4. Pomocí prostředků matematické analýzy objevte diskriminant: najděte extrém funkce $f : y = ax^2 + bx + c$ a rozeberte následující případy:

   - f má dva různé průsečíky s osou x (f je konvexní a hodnota extrému je záporná, f je konkávní a hodnota extrému je kladná),
   - f se dotýká osy x (hodnota extrému je nulová),
   - f nemá průsečíky s osou x (f je konvexní a hodnota extrému je kladná, f je konkávní a hodnota extrému je záporná).

5. Pro nadšence: Pokuste se odvodit, jak by bylo možno znázornit kořeny kvadratické rovnice s reálnými koeficienty, které jsou komplexní.

1.1 Komplexní kořeny kvadratické rovnice

Uvažujme kvadratickou rovnici $ax^2 + bx + c = 0$, kde $a, b, c \in \mathbb{R}$, $a \neq 0$. Má-li tato rovnice

- 2 různé reálné kořeny, jsou rovny x-ovým souřadnicím průsečíků paraboly

$$y = ax^2 + bx + c \tag{1}$$

  s osou x,

- 1 dvojnásobný kořen, je roven x-ové souřadnici společného bodu paraboly (1) s osou x,
- 2 různé komplexní kořeny (tj. komplexně sdružené), jak je lze znázornit?

Návod:
Uvažujme parabolu

$$y = (x - \alpha)^2 + \beta^2 \,,$$

kde $\alpha, \beta \in \mathbb{R}$, $\beta > 0$. Souřadnice vrcholu V této paraboly jsou: $V = [\alpha, \beta^2]$.
Hledejme nulové body; dostaneme rovnici

$$(x - \alpha)^2 = -\beta^2 \,,$$

jejímiž kořeny jsou

$$\boxed{z_{1,2} = \alpha \pm \mathrm{i}\beta \,.}$$

Porovnejte tento výsledek se znázorněním kořenů rovnice, která má kořeny reálné:

$$y = (x - \alpha)^2 - \beta^2 \,,$$

kde $\alpha, \beta \in \mathbb{R}$, $\beta > 0$. Souřadnice vrcholu V této paraboly jsou: $V = [\alpha, -\beta^2]$.
Hledejme kořeny; dostaneme rovnici

$$(x - \alpha)^2 = \beta^2 \,,$$

jejímiž kořeny jsou

$$\boxed{z_{1,2} = \alpha \pm \beta \,.}$$

Závěr

- Reálné kořeny leží na ose x *ve vzdálenosti* β *od* x*-ové souřadnice* α *vrcholu* V.
- Pokud bychom se na rovinu xy dočasně dívali jako na Gaussovu rovinu, tak komplexně sdružené kořeny kvadratické rovnice s reálnými koeficienty leží na kolmici k reálné ose (ose x) *ve vzdálenosti* β *od reálné části* α *(*x*-ové souřadnice vrcholu* V*).*

Důkladnější výpočet
Určeme reálnou a imaginární část nulových bodů funkce komplexní proměnné $x \in \mathbb{C}$:

$$y(x) = (x - \alpha)^2 + \beta^2 = (x_1 + \mathrm{i}x_2 - \alpha)^2 + \beta^2 = [(x_1 - \alpha) + \mathrm{i}x_2]^2 + \beta^2$$

$$= (x_1 - \alpha)^2 - x_2^2 + \beta^2 \quad + \quad 2\mathrm{i}x_2\,(x_1 - \alpha)\,.$$

Nulové body lze tedy najít snadno: $y(x) = 0 \quad \Longleftrightarrow \quad \Re\, y(x) = 0$ a $\Im\, y(x) = 0$. Imaginární část se rovná nule právě tehdy, když $x_1 - \alpha = 0$ ($x_2 \neq 0$, neboť by pak rovnice měla jen reálné kořeny). Reálná část x_1 obou kořenů je tedy $x_1 = \alpha$.

Reálná část funkce $y(x)$ se rovná nule právě tehdy, když $(x_1-\alpha)^2+\beta^2 = x_2^2$, tj. $\beta^2 = x_2^2$. Imaginární část x_2 obou kořenů je proto $x_2 = \pm\beta$. Celkově má tedy funkce $y(x)$ nulové body $x_1 + \mathrm{i}x_2 = \alpha \pm \mathrm{i}\beta$.

Otázka pro zájemce. Existuje podobná souvislost komplexních kořenů s vrcholy také u kubické rovnice?

2 Kubická rovnice – Cardanův postup

stačí vypracovávat pouze úlohy označené hvězdičkou

1. Najděte jeden kořen následující kubické rovnice Cardanovým postupem.

$$x^3 + 6x - 20 = 0$$

   Ostatní kořeny najděte tak, že levou stranu vydělíte známým kořenovým činitelem a vyřešíte vzniklou kvadratickou rovnici.

2. * Najděte jeden kořen následující kubické rovnice Cardanovým postupem.

$$x^3 - 6x^2 + 10x - 8 = 0$$

   Následně najděte i ostatní kořeny této rovnice.
   (pro kontrolu: $y^3 - 2y - 4 = 0$, kvadratická resolventa je $t^2 - 4t + \frac{8}{27} = 0$)

3. Vyřešte binomickou rovnici (v $\mathbb{C}$): $z^3 = 1$. Řešení zapište v goniometrickém i algebraickém tvaru.

4. * Ukažte, že všechny komplexní kořeny binomické rovnice $z^3 = a$, $a \in \mathbb{R}$, lze zapsat ve tvaru:

$$x_1 = \sqrt[3]{a}\,, \qquad x_2 = \varepsilon \cdot \sqrt[3]{a}\,, \qquad x_3 = \varepsilon^2 \cdot \sqrt[3]{a}\,.$$

   Je předpoklad $a \in \mathbb{R}$ nutný?

5. Všimněte si, že právě v tomto tvaru

$$\sqrt[3]{t_1} = \{u\,, \quad \varepsilon \cdot u\,, \quad \varepsilon^2 \cdot u\}\,, \qquad \sqrt[3]{t_2} = \{v\,, \quad \varepsilon \cdot v\,, \quad \varepsilon^2 \cdot v\}\,,$$

   jsou komponenty kořenů

$$x_1 = u + v\,,$$
$$x_2 = \varepsilon u + \varepsilon^2 v\,,$$
$$x_3 = \varepsilon^2 u + \varepsilon v\,.$$

   kubické rovnice

$$x^3 + px + q = 0\,.$$

6. Dle Vietových vět platí: $x_1+x_2+x_3 = 0$; pozorujme, že koeficienty ε a ε^2 jsou skutečně umístěny tak, že $x_1 + x_2 + x_3 = 0$:

$$x_1 + x_2 + x_3 \quad = \quad u + \varepsilon u + \varepsilon^2 u \quad + \quad v + \varepsilon^2 v + \varepsilon v$$

$$= (1 + \varepsilon + \varepsilon^2) \cdot u + (1 + \varepsilon + \varepsilon^2) \cdot v \;=\; 0 \cdot u + 0 \cdot v = 0\,.$$

7. * Označme jednu z třetích odmocnin z jedné řeckým písmenem ε:
$$\varepsilon = \cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}\,.$$
Ukažte, že
$$1 + \varepsilon + \varepsilon^2 = 0\,.$$
8. * Ukažte, že předchozí tvrzení lze snadno zobecnit: označíme-li
$$\omega = \cos\frac{2\pi}{n} + \mathrm{i}\sin\frac{2\pi}{n}\,,$$
tak platí:
$$1 + \omega + \omega^2 + \cdots + \omega^{n-1} = 0\,.$$
9. * a) Ukažte, že platí následující tvrzení: jsou-li komplexní čísla $u = r\cdot(\cos\varphi + \mathrm{i}\sin\varphi)$ a $v = r\cdot(\cos\varphi - \mathrm{i}\sin\varphi)$ komplexně sdružená, jsou komplexně sdruženými také jejich třetí mocniny.
b) Platí analogické tvrzení pro druhé mocniny?

3 Kubická rovnice – diskriminant

1. * U kvadratické rovnice jsme objevili diskriminant prostředky matematické analýzy. Pokuste se provést totéž u kubické rovnice (uvažujte funkci $y = x^3 + px + q$).
2. * Najděte všechny kořeny rovnice $x^3 - 3x - 2 = 0$ standardním Cardanovým postupem. Vyšetřete průběh funkce $y = x^3 - 3x - 2$ (najděte extrémy, inflexní body, intervaly, kde je tato funkce rostoucí, klesající, konvexní, konkávní) a načrtněte její graf.
3. Zopakujte si: diskriminantem kubické rovnice $x^3 + px + q = 0$ rozumíme výraz:
$$D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\,.$$
Pokud jsou $p, q \in \mathbb{R}$, má tato kubická rovnice v případě, že:
   - $D < 0$, všechny tři kořeny reálné (tzv. *casus irreducibilis*),
   - $D > 0$, jeden reálný a dva komplexně sdružené kořeny,
   - $D = 0$, násobné kořeny.
4. *Zajímavost.* Pro rozhodování, zda nastává casus irreducibilis, používáme výraz
$$D = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\,,$$
což je modifikovaný diskriminant kvadratické resolventy. Přesně tento výraz se vyskytuje v Cardanových vzorcích pod druhou odmocninou. Pozor: ani diskriminant kvadratické resolventy, ani uvedený výraz D přísně vzato *není* diskriminantem kubické rovnice. Diskriminant D_n polynomiální rovnice stupně n je pojem, který bude důkladně zaveden v 5. ročníku. U kubické rovnice pak odvodíme, že jejím diskriminantem je výraz
$$\boxed{D_3 = -27\cdot 4\cdot\left(\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\right),}$$
který se od námi používaného D liší nejen faktorem $27\cdot 4$, ale i znaménkem (což je celkem nepříjemnost).

4 Kubická rovnice – casus irreducibilis

1. * Pokuste se najít jeden kořen následující kubické rovnice Cardanovým postupem.

$$x^3 - 13x + 12 = 0$$

Alespoň jeden kořen dopočítejte až „do konce“. (Tato rovnice má tři reálné kořeny, všechny jsou celými čísly. Aspoň jeden kořen vyjádřený pomocí třetích odmocnin komplexních čísel z Cardanových vzorců tedy dopočítejte až do podoby celého čísla. Třetí odmocniny komplexních čísel můžete hledat např. pomocí goniometrického tvaru a Moiverovy věty.)

2. * U následujících rovnic ověřte (pomocí diskriminantu), že nastává casus irreducibilis, následně najděte všechny jejich kořeny pomocí goniometrických substitucí.
a) $x^3 - 13x + 12 = 0$ b) $x^3 + 3x^2 - 4x - 12 = 0$

5 Rovnice binomická, trinomická a bikvadratická

1. * Najděte v komplexním oboru všechny třetí odmocniny z čísla -8:
a) řešte v $\mathbb{C}$ binomickou rovnici $z^3 = -8$;
b) pokuste se získaná řešení zapsat pomocí $\varepsilon = \cos\frac{2\pi}{3} + \mathrm{i}\sin\frac{2\pi}{3}$.

2. * Napište čtvrtou odmocninu čísla 16 v $\mathbb{R}$ a v $\mathbb{C}$.

3. * Řešte v $\mathbb{C}$ binomickou rovnici

$$z^4 = -1 + \mathrm{i}\sqrt{3}\,.$$

4. * Řešte v $\mathbb{C}$ bikvadratickou rovnici

$$x^4 + x^2 - 20 = 0\,.$$

5. * Řešte v $\mathbb{C}$ rovnici

$$x^3 \cdot (x^3 - 7) = 12 \cdot (18 + x^3)\,.$$

6. * Najděte v $\mathbb{C}$ všechny kořeny následujících trinomických rovnic.
a) $x^6 - 9x^3 + 8 = 0$
b) $x^6 - 19x^3 - 216 = 0$ $[3, -\frac{3}{2}(1 \pm \mathrm{i}\sqrt{3}), -2, 1 \pm \mathrm{i}\sqrt{3}]$

Reciproká rovnice

* **Pozorování**, která jsou zásadní (viz též přednáška):

1. Rovnici

$$a_0x^5 + a_1x^4 + a_2x^3 + a_2x^2 + a_1x + a_0 = 0$$

vydělte kořenovým činitelem $x + 1$.

2. Rovnici

$$a_0x^5 + a_1x^4 + a_2x^3 - a_2x^2 - a_1x - a_0 = 0$$

vydělte kořenovým činitelem $x - 1$.

6 Reciproké rovnice – teorie

Nechť je dána rovnice ve tvaru

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2 x^2 + a_1 x + a_0 = 0\,,$$

kde $a_n \neq 0$.

Reciproká rovnice 1. druhu: $a_i = a_{n-i}$ pro všechna $i = 0, 1, \ldots, n$

- lichého stupně: má kořen $x_1 = -1$
  po vydělení kořenovým činitelem $x + 1$ zbude reciproká rovnice 1. druhu sudého stupně
- sudého stupně: „prostřední“ koeficient $a_{\frac{n}{2}}$ může být libovolný
  řešíme pomocí substituce $z = x + \frac{1}{x}$

Reciproká rovnice 2. druhu: $a_i = -a_{n-i}$ pro všechna $i = 0, 1, \ldots, n$
- má vždy kořen $x_1 = 1$ (nezávisí na paritě stupně)
- po vydělení kořenovým činitelem $x - 1$ zbude reciproká rovnice 1. druhu (snadno se ověří vydělením $x - 1$)

Pozorování: Reciproká rovnice 2. druhu sudého stupně má jediný „prostřední“ koeficient $a_{\frac{n}{2}}$. Jak vypadá? Jelikož musí platit $a_i = -a_{n-i}$, tak musí být nulový: $a_{\frac{n}{2}} = 0$.

Proč se takové rovnice nazývají reciproké? Pro reciproké rovnice 1. i 2. druhu platí: je-li α kořenem této rovnice, pak je jejím kořenem také $\frac{1}{\alpha}$. A převrácená hodnota se také nazývá *reciproká hodnota*.
Jak tvrzení dokázat: Stačí předpokládat, že reciproká rovnice má kořen α, pak do ní dosadit $\frac{1}{\alpha}$ a ihned bude zřejmé, že je také kořenem.

Reciprokosti lze využít při hledání kořenů: Máme-li zadánu reciprokou rovnici 1. či 2. druhu s celočíselnými koeficienty, můžeme se pokusit hledat její kořeny pomocí Vietových vět. Je-li absolutní člen roven přirozenému číslu, můžeme zkusit všechny jeho dělitele. Výhodou je, že najdeme-li jeden kořen x_0, máme automaticky i další kořen, který je jeho převrácenou hodnotou: $\frac{1}{x_0}$.

Jaké reciproké rovnice lze vyřešit v radikálech? Reciproké rovnice jsou ve speciálním tvaru; díky symetričnosti (či antisymetričnosti) koeficientů stačí znát jen polovinu koeficientů. Podobné je to i s kořeny: také stačí znát jen polovinu kořenů, zbylé totiž jsou jejich převrácenými hodnotami. Díky tomuto speciálnímu tvaru tedy můžeme vždy řešit v radikálech (tj. „vzorečkem“ pro kořeny obsahujícím pouze $+, -, \cdot, :$ a k-té odmocniny) rovnice nejen stupně nižšího než pátého, ale až do stupně „dvojnásobného“, tj. do stupně devátého včetně.

1. Příklad reciproké rovnice, která je řešitelná i po redukci na rovnici polovičního stupně, přestože je to rovnice pátého stupně:

   $$x^{10} + 5\,x^8 + 10\,x^6 + x^5 + 10\,x^4 + 5\,x^2 + 1 = 0\,.$$

   Určete všechny její kořeny v $\mathbb{C}$. Platí i pro její komplexní kořeny, že je-li jejím kořenem $\alpha \in \mathbb{C}$, je také jejím kořenem $\frac{1}{\alpha} \in \mathbb{C}$?

2. Příklad reciproké rovnice, která po redukci na rovnici polovičního stupně není řešitelná:

$$x^{10} + 5\,x^8 + 11\,x^6 + x^5 + 11\,x^4 + 5\,x^2 + 1 = 0\,.$$

Proveďte redukci na rovnici polovičního stupně. Platí přesto pro každý z jejích deseti kořenů, že je-li jejím kořenem $\alpha \in \mathbb{C}$, je také jejím kořenem $\frac{1}{\alpha} \in \mathbb{C}$?

Dokažte následující tvrzení (viz též přednáška).

1. Jestliže je n liché a $a_k = a_{n-k}$ pro každé $k = 0, 1, \ldots, n$, pak má tato rovnice kořen $x_1 = -1$.
2. Jestliže $a_k = -a_{n-k}$ pro každé $k = 0, 1, \ldots, n$, pak má tato rovnice kořen $x_1 = 1$.
3. V obou předchozích případech platí: je-li α kořenem této rovnice, pak má také kořen $\frac{1}{\alpha}$.

Pozorování, která jsou zásadní (viz též přednáška):

1. Rovnici
$$a_0x^5 + a_1x^4 + a_2x^3 + a_2x^2 + a_1x + a_0 = 0$$
vydělte kořenovým činitelem $x + 1$.
2. Rovnici
$$a_0x^5 + a_1x^4 + a_2x^3 - a_2x^2 - a_1x - a_0 = 0$$
vydělte kořenovým činitelem $x - 1$.

6.1 Reciproké rovnice – ukázkový příklad

Řešte v $\mathbb{R}$ následující rovnici.

$$6x^5 + 11x^4 - 33x^3 - 33x^2 + 11x + 6 = 0$$

Řešení:

- Jedná se o reciprokou rovnici 1. druhu. Je lichého stupně, tj. jeden kořen je $x_0 = -1$. Vydělíme tedy kořenovým činitelem $x + 1$, dostaneme:
$$6x^4 + 5x^3 - 38x^2 + 5x + 6 = 0.$$
- Máme tedy reciprokou rovnici (opět 1. druhu, na tom se nic nemění) sudého stupně. Je-li stupeň $2n$, vydělíme rovnici x^n. Toto je klíčový trik vedoucí k řešení. Dostaneme:
$$6x^2 + \frac{6}{x^2} \quad + 5x + \frac{5}{x} \quad - 38 = 0.$$
- Zavedeme substituci $z = x + \frac{1}{x}$. Uvědomíme si, že $z^2 = x^2 + 2 + \frac{1}{x^2}$, tj. $x^2 + \frac{1}{x^2} = z^2 - 2$. Podobně příznivá situace nastane i v případě vyšších mocnin z (což bychom potřebovali, pokud bychom řešili reciprokou rovnici vyššího stupně).
- Rovnice přejde po substituci na tvar:
$$6(z^2 - 2) \quad + 5z \quad - 38 = 0.$$

- Tuto kvadratickou rovnici ($6z^2 + 5z - 50 = 0$) snadno vyřešíme: $z_1 = -\frac{10}{3}$, $z_2 = \frac{5}{2}$.
- Vrátíme se k původní neznámé x (pomocí substitučního vztahu $z = x + \frac{1}{x}$). První dva kořeny reciproké rovnice tedy získáme řešením rovnice $-\frac{10}{3} = x + \frac{1}{x}$, druhé dva kořeny z rovnice $\frac{5}{2} = x + \frac{1}{x}$. Jsou to vlastně kvadratické rovnice (po vynásobení $x \neq 0$).
- Rovnice $-\frac{10}{3} = x + \frac{1}{x}$, tj. $3x^2 + 10x + 3 = 0$ má kořeny $x_1 = -3$, $x_2 = -\frac{1}{3}$,
  rovnice $\frac{5}{2} = x + \frac{1}{x}$, tj. $2x^2 - 5x + 2 = 0$ má kořeny $x_3 = 2$, $x_4 = \frac{1}{2}$.
- Všechny kořeny zadané reciproké rovnice tedy jsou:

$$-1,\ -3,\ -\frac{1}{3},\ 2,\ \frac{1}{2}\,.$$

6.2 Reciproké rovnice – praxe

1. * Určete typ následujících reciprokých rovnic a najděte všechny jejich kořeny v $\mathbb{R}$.

   a) $6x^5 - 41x^4 + 97x^3 - 97x^2 + 41x - 6 = 0$ $[1, 2, \frac{1}{2}, 3, \frac{1}{3}]$

   b) $10x^4 - 77x^3 + 150x^2 - 77x + 10 = 0$ $[2, \frac{1}{2}, 5, \frac{1}{5}]$

   c) $8x^5 - 6x^4 - 83x^3 - 83x^2 - 6x + 8 = 0$ $[-1, -2, -\frac{1}{2}, 4, \frac{1}{4}]$

   d) $6\,x^5 + 11\,x^4 - 33\,x^3 - 33\,x^2 + 11\,x + 6 = 0$

7 Tzv. Základní věta algebry

Pozor: tzv. základní věta algebry sice na první pohled vypadá, že se týká hlavně polynomů, ale v podstatě jde spíše o vlastnost pole komplexních čísel: *je algebraicky uzavřené*.

Počet kořenů polynomu

Jeden z důsledků ZVA je, že polynom stupně $n \geq 1$ nad $\mathbb{C}$ má v $\mathbb{C}$ právě n kořenů (počítáno včetně násobnosti). Tohle však nad jinými poli neplatí. Na začátku semestru jsme na to měli příklady. Pro připomenutí:

Následující rovnice lze řešit zkusmo – dosazením všech hodnot z konečné množiny $\mathbb{Z}_n$.

1. * Najděte v poli $\mathbb{Z}_3$ všechna řešení rovnice $x^2 + x + 2 = 0$.
2. * Najděte v okruhu $\mathbb{Z}_6$ všechna řešení rovnice $x^3 + 5x = 0$.

8 Racionální čísla

1. * Dokažte, že násobení racionálních čísel je asociativní.

2. * Dokažte, že zobrazení $f\colon (\mathbb{Z},+,\cdot) \to (\mathbb{Q},+,\cdot)$ přiřazující celým číslům třídy ekvivalence dle následujícího předpisu je homomorfismus. Pro každé $n \in \mathbb{Z}$ definujeme

   $$f(n) = T([n,1])\,.$$

   Je tedy třeba dokázat, že pro každé $k, n \in \mathbb{Z}$ platí:

   $$f(n+k) = f(n) + f(k) \qquad \text{a} \qquad f(n\cdot k) = f(n)\cdot f(k)\,.$$

   Tento homomorfismus realizuje *vnoření* $\mathbb{Z}$ do $\mathbb{Q}$, $\mathbb{Q}$ je tedy rozšířením $\mathbb{Z}$.

3. Připomeňte si, jaké struktury tvoří následující množiny s binárními operacemi:

   $$(\mathbb{N},+) \quad \text{a} \quad (\mathbb{Z},+)$$

   $$(\mathbb{Z}\setminus\{0\},\cdot) \quad \text{a} \quad (\mathbb{Q}\setminus\{0\},\cdot)$$

4. Zkuste si rozmyslet, jak byste na úrovni druhého stupně ZŠ vyložili sčítání zlomků.

5. * Převeďte desetinné číslo $0,12$ na zlomek.

6. * Převeďte zlomek $\frac{23}{30}$ na desetinné číslo.

9 Iracionální čísla

1. Zopakujte si důkazy tvrzení:
   - mohutnost množiny racionálních čísel je spočetná,
   - mohutnost množiny reálných čísel je nespočetná.

2. * Uměli byste dokázat, že $\log_5 2$ je iracionálním číslem?

3. * Zkonstruujte dvěma různými způsoby úsečku délky $\sqrt{3}$ cm (Eukleidova věta o výšce a „šnek“).

4. V Platónově dialogu Theaitétos (147d) se píše: *Tuhle Theodóros nám znázorňoval obrazci cosi o mocninách, o čtverci obsahujícím tři čtverečné stopy a o čtverci obsahujícím pět čtverečných stop, že svou stranou nejsou souměřitelné se čtvercem o jedné stopě, a tak probíral jednu mocninu po druhé až po čtverec o sedmnácti čtverečných stopách; při tomto se nevím proč zastavil.*
   Proč se Theodóros zastavil právě u odmocniny čísla 17?

5. * Která z následujících čísel jsou transcendentní? Užijte Gelfandovu–Schneiderovu větu, ověřte splnění jejích předpokladů.

   $$\sqrt{5} \quad 2^{\frac{1}{3}} \quad 2^{\sqrt{2}} \quad (\sqrt{2})^{\sqrt{2}} \quad 1^{\pi} \quad e^{\pi} \quad \pi^{e}$$

10 Reálná čísla

Opakování:

1. Připomeňte si zavedení reálných čísel pomocí desetinných rozvojů.
2. Připomeňte si větu o supremu a Cantorův princip uzavřených do sebe vložených intervalů. (Matematická analýza I)

10.1 Různé způsoby zavedení $\mathbb{R}$

Reálná čísla je možno zavést různými způsoby, např.:

1. pomocí desetinných rozvojů (je nutno vyloučit periodu 9 a ošetřit periodu 0),
2. zúplněním $\mathbb{Q}$ (pomocí cauchyovských posloupností).
3. axiomaticky: zde v pdf (pouze pasáže označené svislým červeným pruhem),
4. pomocí Dedekindových řezů: zde v pdf,
   studovat pouze: Def. 1.7, V 1.10, Pozn. 1.11, V 1.12, Úml. 1.13, Def. 1.14, Def. 1.15, V 1.18 + Důsl., Def. 1.21, V 1.22 a 1.23,

Pro zájemce: Vývoj představ o reálných číslech

11 Komplexní čísla

1. * V čem je problém?
$$-1 = \mathrm{i} \cdot \mathrm{i} = \sqrt{-1} \cdot \sqrt{-1} = \sqrt{(-1) \cdot (-1)} = \sqrt{1} = 1$$
2. * Zdůvodněte, proč nestačí při zavádění komplexních čísel specifikovat, že se jedná o množinu všech uspořádaných dvojic reálných čísel. Co je třeba ještě dodat?
3. Připomeňme si: je třeba rozlišovat:
   - komplexní číslo
   - algebraický, goniometrický, exponenciální tvar komplexního čísla
   - obraz komplexního čísla v Gaussově rovině (komplexní číslo $[a, b]$ interpretujeme geometricky jako bod v rovině o souřadnicích $[a, b]$)
4. * Pomocí součtových vzorců odvoďte vztah pro součin dvou komplexních jednotek:
$$(\cos\alpha + \mathrm{i}\sin\alpha) \cdot (\cos\beta + \mathrm{i}\sin\beta) = \cos(\alpha+\beta) + \mathrm{i}\sin(\alpha+\beta)$$
5. * Ze vztahu pro násobení komplexních jednotek v goniometrickém tvaru odvoďte součtové vzorce pro funkce sinus a kosinus.
6. * Dokažte Moivreovu větu tak, jak ji budete dokazovat svým studentům. Zvažte různé možnosti.
   V: Pro každé $n \in \mathbb{N}$ a pro každé $\varphi \in \mathbb{R}$ platí:
$$(\cos\varphi + \mathrm{i}\sin\varphi)^n = \cos n\varphi + \mathrm{i}\sin n\varphi\,.$$

11.1 Geometrie komplexních čísel

Pomocí komplexních čísel lze snadno charakterizovat různé geometrické útvary.

1. kružnice: $|z - z_0| = r$
2. kruh: $|z - z_0| \leq r$
3. elipsa: $|z - f_1| + |z - f_2| = 2a$
4. oblast ohraničená elipsou: $|z - f_1| + |z - f_2| < 2a$
5. Analytickou geometrii v rovině lze přeformulovat na geometrii v komplexní souřadnici: bod $[x, y]$ lze reprezentovat komplexním číslem $z = x + \mathrm{i}y$. Potom $\bar{z} = x - \mathrm{i}y$, odkud sečtením, resp. odečtením těchto vztahů dostaneme:

   $$x = \frac{z + \bar{z}}{2} \qquad y = \frac{z - \bar{z}}{2\mathrm{i}}\,.$$

   Například **obecnou rovnici přímky**

   $$ax + by + c = 0$$

   pak můžeme přepsat ve tvaru $a\frac{z+\bar{z}}{2} + b\frac{z-\bar{z}}{2\mathrm{i}} + c = 0$, což po úpravě přejde na tvar:

   $$\bar{\alpha}z + \alpha\bar{z} + c = 0\,,$$

   kde $\alpha = \frac{1}{2}(a + b\mathrm{i})$.
6. * přímka procházející body, které jsou obrazy komplexních čísel $a, b \in \mathbb{C}$:

   $$\det \begin{pmatrix} z & \bar{z} & 1 \\ a & \bar{a} & 1 \\ b & \bar{b} & 1 \end{pmatrix} = 0$$

   Ukažte, že se skutečně jedná o specifikovanou přímku.
7. * kružnice procházející body, které jsou obrazy komplexních čísel $a, b, c \in \mathbb{C}$:

   $$\det \begin{pmatrix} z\bar{z} & \bar{z} & z & 1 \\ a\bar{a} & \bar{a} & a & 1 \\ b\bar{b} & \bar{b} & b & 1 \\ c\bar{c} & \bar{c} & c & 1 \end{pmatrix} = 0$$

   Ukažte, že se skutečně jedná o specifikovanou kružnici.
8. * Načrtněte v Gaussově rovině množinu obrazů všech komplexních čísel $z \in \mathbb{C}$, která splňují následující podmínku.

   a) $|z - \mathrm{i}| = 4$, b) $|z - \mathrm{i}| \leq 4$, c) $1 \leq |z - \mathrm{i}| \leq 4$, d) $|z - \mathrm{i}| = |z + \mathrm{i}|$, e) $|z - \mathrm{i}| + |z + \mathrm{i}| = 4$.
9. Pozorujme klíčový vztah ($a = a_1 + a_2\mathrm{i}$, $b = b_1 + b_2\mathrm{i}$):

   $$\boxed{a \cdot \bar{b} = (a_1 b_1 + a_2 b_2) + \mathrm{i}\,(a_1 b_2 - a_2 b_1).}$$

   Pokud bychom uvažovali vektory $\vec{a} = (a_1, a_2)$, $\vec{b} = (b_1, b_2)$, tak by

   $$\mathrm{Re}(a \cdot \bar{b}) = \vec{a} \cdot \vec{b}\,, \qquad \mathrm{Im}(a \cdot \bar{b}) = \det(\vec{a}, \vec{b}).$$

10. Některé partie **geometrie trojúhelníku** lze budovat pomocí tří navzájem různých komplexních čísel

$$\omega_1 = \cos\varphi_1 + \mathrm{i}\sin\varphi_1,$$
$$\omega_2 = \cos\varphi_2 + \mathrm{i}\sin\varphi_2,$$
$$\omega_3 = \cos\varphi_3 + \mathrm{i}\sin\varphi_3,$$

jejichž obrazy jsou vrcholy zadaného trojúhelníku. Všimněme si, že jeho opsaná kružnice je kružnicí jednotkovou.

Definujme dále užitečné výrazy

$$s_1 = \omega_1 + \omega_2 + \omega_3\,, \quad s_2 = \omega_1\,\omega_2 + \omega_2\,\omega_3 + \omega_3\,\omega_1\,, \quad s_3 = \omega_1\,\omega_2\,\omega_3.$$

11. * Dokažte, že trojúhelník s vrcholy reprezentovanými komplexními čísly $\omega_1, \omega_2, \omega_3$ je rovnostranný právě tehdy, když

$$s_1 = 0.$$

12. * Dokažte, že trojúhelník s vrcholy reprezentovanými komplexními čísly $\omega_1, \omega_2, \omega_3$ je pravoúhlý právě tehdy, když

$$s_1\,s_2 = s_3\,.$$

[Z Thalétovy věty plyne, že některé dva vrcholy leží na průměru jednotkové kružnice, tj. BÚNO: $\omega_1 = -\omega_2$.]

12 Hamiltonovy kvaterniony

Hamilton ukázal, že násobení kvaternionů založené na vztazích

$$\boxed{\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1}$$

vede k rozšíření komplexních čísel na (nekomutativní) těleso.

Pokuste se odvodit následující vztahy (za předpokladu asociativity násobení a distributivity, nepředpokládejte však asociativitu násobení).

1. * Hezké je násobení dvou imaginárních jednotek:

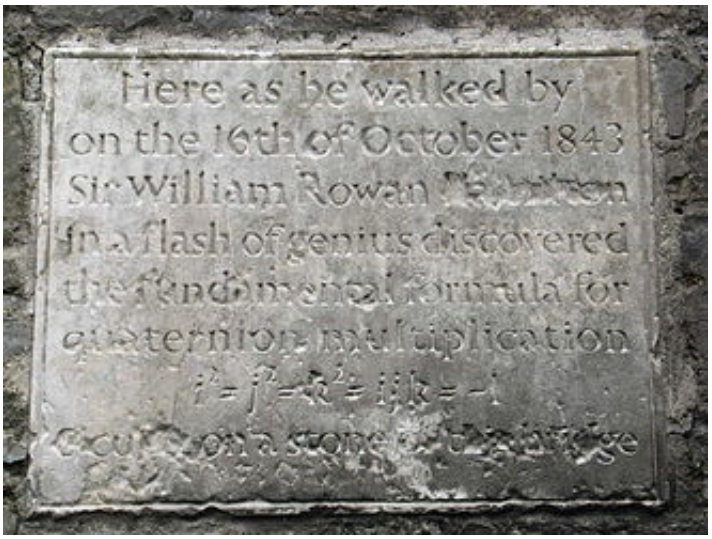
$$\mathrm{ij} = \mathrm{k} \qquad \mathrm{jk} = \mathrm{i} \qquad \mathrm{ki} = \mathrm{j}\,.$$

2. * Při násobení imaginárních jednotek se však objevuje zdroj nekomutativity násobení kvaternionů:

$$\mathrm{ij} = -\mathrm{ji} \qquad \mathrm{jk} = -\mathrm{kj} \qquad \mathrm{ki} = -\mathrm{ik}\,.$$

(Stačí odvodit jeden z těchto vztahů.) Z těchto rovností ihned plyne, že těleso kvaternionů není komutativní.

3. * Pokuste se najít inverzní prvek k prvku:
a) i, b) j, c) k, d) ij.



Nápis na mostě v Dublinu.

12.1 Pohádka o neexistenci hyperkomplexních čísel s právě dvěma imaginárními jednotkami

Komplexní čísla: $\mathbb{C} = \{[a,b];\, a,b \in \mathbb{R}\}$, sčítání probíhá po složkách (je tak kompatibilní se sčítáním reálných čísel, neboť $\mathbb{R} = \{[a,0];\, a \in \mathbb{R}\}$) a násobení je definováno tak, aby bylo distributivní vůči sčítání, asociativní a komutativní, navíc požadujeme, aby $[0,1]\cdot[0,1] = [-1,0]$, což odpovídá známému $\mathrm{i}^2 = -1$.

Pozor: při definici komplexních čísel se nelze omezit jen na množinu, pouhé $\mathbb{R}^2$ ještě nespecifikuje, že se jedná o komplexní čísla. Komplexní čísla se z $\mathbb{R}^2$ stanou až tehdy, když na $\mathbb{R}^2$ definujeme operace $+$ a $\cdot$ následujícím způsobem:

$$\begin{aligned} &\forall a,b,c,d \in \mathbb{R}\colon \quad [a,b] + [c,d] = [a+c, b+d]\,, \\ &\forall a,b,c,d \in \mathbb{R}\colon \quad [a,b] \cdot [c,d] = [ac-bd, ad+bc]\,. \end{aligned}$$

Komplexní čísla a lineární algebra: Běžně zapisujeme uspořádanou dvojici $[1,0] \in \mathbb{C}$ jako 1, uspořádanou dvojici $[0,1] \in \mathbb{C}$ jako i. Všimněme si, že tyto dva prvky, uvažujeme-li o nich jako o vektorech z $\mathbb{R}^2$ tvoří v $\mathbb{R}^2$ bázi: $\vec{e}_1 = (1,0)$, $\vec{e}_2 = (0,1)$. Vektor (a,b) reprezentující komplexní číslo $[a,b]$ tedy můžeme psát jako lineární kombinaci prvků báze, tj. $(a,b) = a\vec{e}_1 + b\vec{e}_2$. Odtud plyne algebraický tvar $a + b\mathrm{i}$ komplexního čísla $[a,b]$.

Komplexní čísla a geometrie: Jelikož lze komplexní čísla popsat pomocí uspořádaných dvojic reálných čísel a jejich součin (přesněji $\bar{a}\cdot b$) obsahuje v první složce skalární součin vektorů $\vec{a} = (a_1, a_2)$ a $\vec{b} = (b_1, b_2)$ (a ve druhé složce determinant, tj. „orientovaný“ obsah):

$$\bar{a}\cdot b = [a_1b_1 + a_2b_2,\ a_1b_2 - a_2b_1] = \left[\vec{a}\cdot\vec{b},\ \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}\right],$$

lze je pohodlně použít k popisu geometrie v rovině i k vyjádření metrických vztahů.

Nabízí se tak myšlenka, zda by nebylo možné analogicky definovat hyperkomplexní čísla, která by byla popsána uspořádanými trojicemi, a ta by se pak použila k popisu geometrie v trojrozměrném prostoru.

Co bychom si tedy přáli:

- Mělo by se jednat o *rozšíření* pole komplexních čísel $\mathbb{C} = \{[a,b];\, a,b \in \mathbb{R}\}$ na pole (či aspoň *na těleso*) s nosičem $\{[a,b,c];\, a,b,c \in \mathbb{R}\}$. Bázové vektory označíme $1 = [1,0,0]$, $\mathrm{i} = [0,1,0]$, $\mathrm{j} = [0,0,1]$. Místo uspořádaných trojic reálných čísel tak budeme moci hledaná hyperkomplexní čísla psát jako lineární kombinaci bázových vektorů, tj.
$$[a,b,c] = a \cdot 1 + b \cdot \mathrm{i} + c \cdot \mathrm{j}\,.$$
- *Sčítání* by tedy opět probíhalo *po složkách*.
- *Násobení* musí být distributivní vůči sčítání, mělo by být asociativní, navíc požadujeme, aby $[0,1,0] \cdot [0,1,0] = [-1,0,0]$, což odpovídá známému $\mathrm{i}^2 = -1$, a $[0,0,1] \cdot [0,0,1] = [-1,0,0]$, což odpovídá $\mathrm{j}^2 = -1$.

  Navíc předpokládáme, že $\mathrm{ij} \neq \mathrm{ji}$, abychom nevytvořili opět jen $\mathbb{C}$ (z podmínky $\mathrm{ij} \neq \mathrm{ji}$ už plyne, že $\mathrm{ji} = -\mathrm{ij}$). Nelze tedy očekávat, že násobení trojic bude komutativní. Abychom nevytvořili pouze $\mathbb{C}$, nestačí předpokládat, že $\mathrm{i} \neq \mathrm{j}$, neboť této podmínce by vyhovovala volba $\mathrm{j} = -\mathrm{i}$.
- Najdeme-li násobení, tak budeme pozorovat, zda obsahuje v některých svých složkách výrazy důležité pro třírozměrnou geometrii.

Hledejme tedy předpis pro násobení třísložkových hyperkomplexních čísel:

(viz přednáška, kde se ukazuje, že takové násobení neexistuje)

Pole komplexních čísel tedy nelze rozšířit pouze o jednu další imaginární jednotku tak, abychom opět dostali těleso (tj. násobení by bylo nekomutativní). Hledání součinu ij totiž vede ke sporu.

Jak Hamilton objevil kvaterniony? Hledal právě hodnotu součinu ij. Nakonec ji položil rovnu nějakému k:
$$\mathrm{ij} = \mathrm{k}\,,$$
o němž ukázal, že $\mathrm{k}^2 = -1$; uvědomil si tedy, že násobení uspořádaných trojic reálných čísel sice korektně definovat nelze, potíže však zmizí, přidáme-li ještě jednu imaginární jednotku k. Tak došlo k objevu kvaternionů.

Hamilton tak ukázal, že pole komplexních čísel lze rozšířit o další dvě imaginární jednotky, čímž dostaneme nekomutativní těleso *kvaternionů*. To tedy obsahuje celkem tři navzájem různé imaginární jednotky, takže jeho prvky jsou reprezentovány uspořádanými čtveřicemi reálných čísel (odtud název kvaterniony). Násobení kvaternionů už bohužel není komutativní ($\mathrm{ji} = -\mathrm{ij}$, ...).

12.2 Definice kvaternionů

Nekomutativní těleso kvaternionů budeme značit $\mathbb{H}$ (podle Hamiltona). Formálně jeho prvky můžeme považovat za prvky vektorového prostoru $\mathbb{R}^4$ s bází $\{\vec{e}_0, \vec{e}_1, \vec{e}_2, \vec{e}_3\}$, přičemž
$$\vec{e}_0 = (1,0,0,0), \quad \vec{e}_1 = (0,1,0,0), \quad \vec{e}_2 = (0,0,1,0), \quad \vec{e}_3 = (0,0,0,1)\,.$$
Místo $\vec{e}_0, \vec{e}_1, \vec{e}_2, \vec{e}_3$ však budeme psát obvyklé $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$.

Sčítání prvků vektorového prostoru $\mathbb{R}^4$ provádíme po složkách. Násobení definujeme pouze na prvcích báze, na celou množinu $\mathbb{H}$ jej rozšíříme pomocí distributivity. Definiční vztahy pro násobení jsou následující:

- $\vec{e}_0\,\vec{e}_n = \vec{e}_n\,\vec{e}_0 = \vec{e}_n$ pro $n = 0,1,2,3$ ($\vec{e}_0$ je jednotkovým prvkem),
- $\vec{e}_1{}^2 = \vec{e}_2{}^2 = \vec{e}_3{}^2 = -\vec{e}_0$ (imaginární jednotky),
- $\vec{e}_1\,\vec{e}_2 = -\vec{e}_2\,\vec{e}_1 = \vec{e}_3$, $\quad \vec{e}_2\,\vec{e}_3 = -\vec{e}_3\,\vec{e}_2 = \vec{e}_1$, $\quad \vec{e}_3\,\vec{e}_1 = -\vec{e}_1\,\vec{e}_3 = \vec{e}_2$ (násobení imag. jednotek).

12.3 Oktoniony, hexadekaniony

Z následujícího přehledu hyperkomplexních čísel je patrné, že se zvyšujícím se počtem imaginárních jednotek (je jich $2^n - 1$, $n = 0, 1, 2, 3, 4$) se postupně ztrácejí důležité vlastnosti. Násobení oktonionů není asociativní, hexadekaniony dokonce obsahují netriviální dělitele nuly.

reálná čísla	uspořádání; násobení: K, A; neex. netriv. dělitelé nuly
komplexní čísla	násobení: K, A; neex. netriv. dělitelé nuly
kvaterniony	násobení: A; neex. netriv. dělitelé nuly
oktoniony	neex. netriv. dělitelé nuly
hexadekaniony	—

13 Řetězové zlomky

13.1 Řetězové zlomky – opakování

1. * Pomocí Eukleidova algoritmu najděte největší společný dělitel čísel 633 a 132.
2. * Rozviňte do řetězového zlomku číslo $\frac{633}{132}$.
3. * Najděte racionální číslo, jehož řetězový zlomek je $[1; 1, 1, 1]$.
4. Jednoduchý algoritmus výpočtu prvních 10 článků řetězového zlomku daného čísla x. (Implementace je v jazyce Python 3.)

```
# Výpočet řetězového zlomku q čísla x

import math
x = math.pi
q = [ ]

for k in range(10):
   q.append( int(x) )       # přidat celou část do seznamu q
   x = 1 / (x - int(x))     # výpočet dalšího článku: odečíst celou část, převrácená hodnota

print(q)       # tisk řetězového zlomku
```

5. * S použitím kalkulátoru vypočtěte prvních deset článků řetězového zlomku čísla $\log_2 \frac{3}{2}$ a příslušné konvergenty.
6. * Uvažujme racionální číslo q, jehož hodnota je rovna řetězovému zlomku $q = [3; 4, 5, 6]$. Čemu je roven řetězový zlomek čísla $\frac{1}{q}$?

Teoretické opakování

7. * Jak lze efektivně počítat konvergenty příslušné jednotlivým článkům řetězového zlomku? Odvoďte vztah pro výpočet čitatelů konvergentů.
8. * Ukažte, že posloupnost konvergentů $\frac{A_{2n}}{B_{2n}}$ tvoří klesající posloupnost.
9. * Vypočtěte obecně rozdíl n-tého a $(n+1)$-ního konvergentu. Všimněte si čitatele tohoto rozdílu a vysvětlete, proč je tak důležitý.

10. * Dodatek – zajímavé pozorování:

    a) Vypočtěte následující součin matic.

$$\begin{pmatrix}1 & q_1\\0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & q_2\end{pmatrix}\begin{pmatrix}0 & 1\\1 & q_3\end{pmatrix}\begin{pmatrix}0 & 1\\1 & q_4\end{pmatrix}$$

    b) Vypočtěte hodnotu řetězového zlomku $[1;2,3,4]$.

    c) Vypočtěte následující součin matic: $\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\1 & 2\end{pmatrix}\begin{pmatrix}0 & 1\\1 & 3\end{pmatrix}\begin{pmatrix}0 & 1\\1 & 4\end{pmatrix}$.

13.2 Lineární diofantické rovnice – věta o existenci

Na základě tří pozorování:

Bezoutova věta garantuje existenci celočíselných řešení x, y rovnice $ax + by = \mathrm{NSD}(a, b)$,

$$43x + 30y = 1 \quad \Longrightarrow \quad 43 \cdot 3x + 30 \cdot 3y = 3,$$

$$12x + 15y = 7 \text{ nemá řešení, protože } 3 \cdot (4x + 5y) \neq 7,$$

odvoďte základní větu o existenci řešení lineární diofantické rovnice:

Věta: Lineární diofantická rovnice $ax + by = c$, kde a, b, $c \in \mathbb{Z}$, má řešení právě tehdy, když

$$\mathrm{NSD}(a, b) \mid c\,.$$

Je-li jedno řešení této rovnice x_0, y_0, pak všechna řešení jsou ve tvaru $x = x_0 - bn, y = y_0 + an$, $a \in \mathbb{Z}$.

13.3 Lineární diofantické rovnice

1. * Najděte všechna řešení následujících lineárních diofantických rovnic.

$$89x + 144y = 1 \qquad 89x + 144y = 5 \qquad 21x + 12y = 1 \qquad 11x + 29y = 1 \qquad 12x + 17y = 1$$

$$9x + 24y = 1 \qquad 9x + 24y = 3 \qquad 9x + 24y = 15$$

2. Pozorování:
   Lineární diofantická rovnice $43x + 30y = 1$ má řešení $x = 7 + 30k$, $y = -10 - 43k$, kde $k \in \mathbb{Z}$.
   Zkouška:

$$43x + 30y = 43(7 + 30k) + 30(-10 - 43k) = 301 + 43 \cdot 30k - 300 - 43 \cdot 30k = 1\,.$$

   Jaké bude mít řešení diofantická rovnice $43x + 30y = 3$? Pravá strana má vyjít trojnásobná, takže i řešení bude trojnásobné: $x = 3 \cdot 7 + 30k$, $y = 3 \cdot (-10) - 43k$. Zkouška:

$$43x + 30y = 43(3 \cdot 7 + 30k) + 30(3 \cdot (-10) - 43k) = 3 \cdot 301 - 3 \cdot 300 + 43 \cdot 30k - 43 \cdot 30k =$$

$$3 \cdot (301 - 300) + 0k = 3\,.$$

   Stručně řečeno:

$$43x + 30y = 1 \quad \Longrightarrow \quad 43 \cdot 3x + 30 \cdot 3y = 3$$

3. Pozorování:
   Lineární diofantická rovnice $6x + 15y = 1$ nemá řešení v $\mathbb{Z}$. Proč?
   Stačí si uvědomit: $3 \cdot (2x + 5y) = 1$. Součin čísla 3 a jiného celého čísla nikdy nedá 1.

   Všimněme si: jsou-li a, b nesoudělná (tj. $\mathrm{NSD}(a, b) = 1$), má lineární diofantická rovnice $ax+by = 1$ vždy řešení. Je to vlastně také důsledek Bezoutovy věty.

4. * Najděte kořeny kvadratické rovnice $x^2 + x - 1 = 0$. Kladný kořen této rovnice je tzv. *zlaté číslo*, značíme jej $\varphi \approx 0,618...$ Tj.

$$\varphi^2 + \varphi = 1 \quad \Longrightarrow \quad \boxed{\varphi + 1 = \frac{1}{\varphi}} \quad \Longrightarrow \quad \varphi = \frac{1}{1 + \varphi}$$

   Rozviňte zlaté číslo φ do řetězového zlomku a najděte prvních pět konvergentů.

5. Provokativní příklad. Pozorujte následující diofantické rovnice a (jedno) jejich řešení.

$$\begin{array}{ll} 2x + 3y = 1 & [-1, 1] \\ 3x + 5y = 1 & [2, -1] \\ 5x + 8y = 1 & [-3, 2] \\ 8x + 13y = 1 & [5, -3] \\ 13x + 21y = 1 & [-8, 5] \\ 21x + 34y = 1 & [13, -8] \\ 34x + 55y = 1 & [-21, 13] \\ 55x + 89y = 1 & [34, -21] \end{array}$$

   Hezké: Fibonacciho čísla se objevují v koeficientech i v řešení.

13.4 Řetězové zlomky – opakování

Následující opakování je užitečné při řešení Pellovy rovnice.

1. * Jakou strukturu má řetězový zlomek čísla $\sqrt{n}$, kde $n \in \mathbb{N}$ není čtvercové číslo?

2. * Najděte hodnotu následujících ryze periodických řetězových zlomků.

   a) $[\overline{2, 2, 3}]$ b) $[\overline{1}]$

3. * Které řetězové zlomky jsou periodické? Které jsou konečné (a proč)? Které jsou nekonečné (a proč)?

13.5 Pellova rovnice

1. * Najděte základní řešení Pellovy rovnice $x^2 - 2023y^2 = 1$

   [2024, 45]

2. * Najděte základní řešení následujících Pellových rovnic (jsou zvoleny tak, že pokrývají různé případy).

   a) $x^2 - 7y^2 = 1$ b) $x^2 - 17y^2 = 1$ c) $x^2 - 13y^2 = 1$ c$_1$) $x^2 - 13y^2 = -1$
   d) $x^2 - 130y^2 = 1$ e) $x^2 - 23y^2 = 1$

3. Srovnejte náročnost hledání řešení následujících Pellových rovnic.

   a) $x^2 - 420y^2 = 1$ b) $x^2 - 421y^2 = 1$

   Pozor: druhá rovnice je určena milovníkům počítání s pomocí počítače či programovatelného kalkulátoru (ruční výpočet zde nedoporučuji). K řešení potřebujeme konvergent příslušný zlomku [20, 1, 1, 13, 5, 1, 3, 1, 2, 1, 1, 1, 2, 9, 1, 7, 3, 3, 2, 2, 3, 3, 7, 1, 9, 2, 1, 1, 1, 2, 1, 3, 1, 5, 13, 1, 1, 40, 1, 1, 13, 5, 1, 3, 1, 2, 1, 1, 1, 2, 9, 1, 7, 3, 3, 2, 2, 3, 3, 7, 1, 9, 2, 1, 1, 1, 2, 1, 3, 1, 5, 13, 1, 1], jeho čitatel má 34 cifer, jmenovatel 33 cifer:

   $$\frac{3879474045914926879468217167061449}{1890739959518390208804997807062 60}.$$

   Jak je tomu s první rovnicí?

14 Průměry

1. Motocykl jede z místa z jednoho místa do druhého průměrnou rychlostí 40 $\frac{\text{km}}{\text{h}}$, zpět jede průměrnou rychlostí 60 $\frac{\text{km}}{\text{h}}$.
   a) Jakou měl průměrnou rychlost za obě cesty dohromady? Chybí údaj o vzdálenosti obou míst?
   * b) Jakou by motocykl musel jet na zpáteční cestě průměrnou rychlostí, aby dosáhl celkové (za obě cesty dohromady) průměrné rychlosti 60 $\frac{\text{km}}{\text{h}}$, 80 $\frac{\text{km}}{\text{h}}$?

2. A–G nerovnost platí obecně: jsou-li $a_1, a_2, \ldots, a_n$ nezáporná reálná čísla, $n \in \mathbb{N}$, potom

   $$a_1 a_2 \cdots a_n \leq \left(\frac{a_1 + a_2 + \cdots + a_n}{n} \right)^n .$$

   Rovnost nastává právě tehdy, když jsou si všechna $a_1, a_2, \ldots, a_n$ rovna.

3. * Celestýn má z průběžných testíků známky 1, 1, 1, 5. Jaká by mu vyšla výsledná známka na vysvědčení, pokud by se pro její výpočet použil průměr geometrický, aritmetický, kvadratický?

15 Lagrangeova věta pro grupy

1. Vezmeme-li podgrupu H konečné grupy G, tak každá třída tvaru gH, $g \in G$ má stejný počet prvků jako H. Proto řád podgrupy H dělí řád grupy G, přesněji

$$|G| = |H| \cdot [G : H] .$$

2. Pozor, Lagrangeova věta obecně neplatí opačným směrem: podgrupa řádu, který je dělitelem řádu grupy G, nemusí existovat.

3. * Dokažte, že pro každé prvočíselné p má grupa $(\mathbb{Z}_p, +)$ pouze dvě podgrupy: $(\{0\}, +)$ a $(\mathbb{Z}_p, +)$.

4. * Najděte všechny podgrupy grupy $(\mathbb{Z}_6, +)$.
Pozor, Lagrangeovu větu zde použijeme pouze k inspiraci, které podgrupy grupy $(\mathbb{Z}_6, +)$ mohou přicházet v úvahu. Z druhé strany, situace u grupy $(\mathbb{Z}_6, +)$ je výborná v tom, že je cyklická, takže ke každému děliteli čísla 6 skutečně existuje podgrupa takového řádu.

5. * Najděte všechny podgrupy alternující grupy $\mathbb{A}_3$.

16 Faktorizace grupy podle normální podgrupy

- základní jednoduchý přehled teorie: zde (Lagrangeova věta, normální podgrupa, faktorizace podle normální podgrupy)
- úplný přehled teorie: zde (pouze pasáže označené svislým červeným pruhem)
obsahuje navíc také: podgrupy, Cayleyho větu, cyklické grupy, faktorizace podle kongruence a podle jádra homomorfismu, věta o homomorfismu grup

Na úvod:

- Faktorizovat podle nějaké podgrupy znamená odhlédnout od prvků této podgrupy. Například z celých čísel, odhlédneme-li od násobků dvou, zůstanou dvě třídy: čísla sudá a lichá.
- Jak najít faktorovou grupu G/H? Jeden její prvek je jasný: H. A další prvky jsou také zřejmé: gH, $g \in G$.
- Pro pohodlné seznámení s faktorizací je užitečné pozorovat příklady faktorových grup.

Příklady faktorových grup známe již ze základní školy (i když jsme je tak tehdy nejspíše nenazývali):

1. grupa obsahující jako prvky právě dvě třídy: kladná a záporná čísla,
2. grupa obsahující jako prvky právě dvě třídy: sudá a lichá čísla.

Dobře známé jsou i tyto příklady:

3. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ (operace sčítání)
4. $\mathbb{C}/\mathbb{R} \cong \mathbb{R}$ (operace sčítání)

5. * Najděte faktorovou grupu $(\mathbb{R} \setminus \{0\}, \cdot)/(\mathbb{R}^+, \cdot)$.

A něco trošku k dokázání:

6. * Uvažujme množinu celých čísel $\mathbb{Z}$ a její podmnožinu $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, 9, 12, \dots\}$. Definujme třídy
$$\bar{1} = 1 + 3\mathbb{Z} = \{\dots, -5, -2, 1, 4, 7, 10, 13, \dots\},$$
$$\bar{2} = 2 + 3\mathbb{Z} = \{\dots, -4, -1, 2, 5, 8, 11, 14, \dots\}.$$
Množinu těchto tříd pak budeme značit $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. Ukažte, že je korektní, definujeme-li binární operaci $\oplus$ na množině těchto tříd $\mathbb{Z}_3$ takto:
$$\forall a, b \in \mathbb{Z}: \quad (a + 3\mathbb{Z}) \oplus (b + 3\mathbb{Z}) = (a + b) + 3\mathbb{Z},$$
tj. že tato definice nezávisí na volbě reprezentantů a, b; tedy že platí:
$$a' \in (a + 3\mathbb{Z}),\ b' \in (b + 3\mathbb{Z}) \quad \Longrightarrow \quad (a' + 3\mathbb{Z}) \oplus (b' + 3\mathbb{Z}) = (a + 3\mathbb{Z}) \oplus (b + 3\mathbb{Z}).$$

7. * Ukažte, že operace $\oplus$ z předchozího bodu je komutativní. Ukažte, že nulovým prvkem je třída $\bar{0} = 3\mathbb{Z} = 0 + 3\mathbb{Z}$. Najděte ke každé třídě opačný prvek vzhledem k operaci $\oplus$. Ukažte, že $(\mathbb{Z}_3, \oplus)$ tvoří komutativní grupu.

8. * Proč je $(n\mathbb{Z}, +)$ *normální* podgrupou grupy $(\mathbb{Z}, +)$?

9. * Dokažte, že $\mathbb{A}_3$ je normální podgrupou grupy $\mathbb{S}_3$. (To už není triviální, protože $(\mathbb{S}_3, \cdot)$ není komutativní grupou.) Najděte $\mathbb{S}_3/\mathbb{A}_3$.

10. * Najděte neutrální prvek ve faktorové grupě G/H.

17 Cyklické grupy

1. * Ověřte, že množina $[i] = \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$ tvoří vzhledem k operaci násobení komplexních čísel grupu.

2. * Ověřte, že grupa z předchozího bodu je izomorfní s grupou $(\mathbb{Z}_4, +)$. Proveďte to tak, že napíšete kompletní tabulku násobení pro grupu $([i], \cdot)$ a tabulku sčítání pro grupu $(\mathbb{Z}_4, +)$.

3. * Dokažte, že cyklické grupy jsou vždy komutativní.

4. * Dokažte, že každá konečná cyklická grupa je izomorfní s některou grupou $(\mathbb{Z}_n, +)$, pro nějaké $n \in \mathbb{N} \setminus \{1\}$. Důsledek: Protože nezáleží na označení prvků ani na označení operace, můžeme každou konečnou cyklickou grupu řádu n stručně značit $C(n)$.

18 Dělitelnost

- základní přehled teorie v knižní podobě: zde (studovat pouze červeně označené pasáže)
- základní přehled teorie – tabule: zde (obory integrity, eukleidovské obory integrity, Gaussovy obory integrity)

18.1 Dělitelnost v oborech integrity

1. eukleidovské obory integrity (jsou automaticky gaussovské):
   Obor integrity $(I, +, \cdot)$ *se nazývá eukleidovský, pokud v něm existuje eukleidovská norma, tj. zobrazení* $\nu : I \to \mathbb{N}_0$ *takové, že*

   a) $\nu(0) = 0$,

   b) pokud pro $b \neq 0$ $a|b$, *pak* $\nu(a) \leq \nu(b)$,

   c) $\forall a, b \in I$, $b \neq 0$ *existují* $q, r \in I$ *taková, že* $a = qb + r$ a $\nu(r) < \nu(b)$.

   Například:

   - celá čísla $(\mathbb{Z}, +, \cdot)$; norma: $\nu(z) = |z|$
   - množiny zbytkových tříd $(\mathbb{Z}_p, +, \cdot)$ pro každé prvočíslo $p \in \mathbb{P}$, pro čísla složená to neplatí: například v $(\mathbb{Z}_6, +, \cdot)$ je $2 \cdot 3 = 0$, tedy součin dvou nenulových prvků je nula (2 i 3 jsou tedy netriviální dělitelé nuly)
   - samozřejmě každé pole $(F, +, \cdot)$, tedy např. $(\mathbb{Z}_p, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$
   - polynomy nad polem F: $(F[x], +, \cdot)$
     norma: $\nu(P_n) = \deg P_n + 1 = n + 1$
   - Gaussova celá čísla: $(\mathbb{Z}[i], +, \cdot)$, tj. komplexní čísla $a + b\mathrm{i}$, kde $a, b \in \mathbb{Z}$
     norma: $\nu(a + b\mathrm{i}) = a^2 + b^2$
   - $(\mathbb{Z}[\sqrt{2}], +, \cdot)$, $(\mathbb{Z}[\mathrm{i}\sqrt{2}], +, \cdot)$
     norma: $\nu : \mathbb{Z}[k] \to \mathbb{N}_0$, kde k je celé číslo, které není dělitelné druhou mocninou žádného prvočísla; definujeme: $\nu(a + b\sqrt{k}) = a^2 - kb^2$

2. gaussovské obory integrity – obory s jednoznačným rozkladem:
   Obor integrity $(I, +, \cdot)$ *se nazývá gaussovský, pokud v něm má každý neinvertibilní nenulový prvek jednoznačný (až na pořadí a asociovanost) rozklad na ireducibilní činitele.*
   Neinvertibilní prvek a *se nazývá ireducibilní, pokud nemá vlastní dělitele. Tj. pokud* $a = bc$, *pak* $b \parallel 1$ *nebo* $c \parallel 1$.

   Například:

   - všechny eukleidovské obory integrity
   - polynomy nad oborem integrity, který je aspoň gaussovský: například $(\mathbb{Z}[x], +, \cdot)$

3. negaussovské obory integrity

   Například:

   - $(\mathbb{Z}[\sqrt{5}], +, \cdot)$
   - $(\mathbb{Z}[\mathrm{i}\sqrt{3}], +, \cdot)$

   protože například v $\mathbb{Z}[\sqrt{5}]$: $4 = 2 \cdot 2$, ale také $4 = (\sqrt{5} + 1) \cdot (\sqrt{5} - 1)$