ALGEBRA

Početní část: na zkoušku je třeba přinést portfolio, tj. vyřešené úlohy z této osnovy předmětu; dále je potřeba úspěšně napsat test s početními příklady, který se zadává u zkoušky.

Teoretická část: u zkoušky jsou zadávány teoretické otázky (důkazy, odvození).

Polynomy a jejich kořeny

1. Definice polynomu a polynomiální funkce. Hornerovo schéma, Lagrangeova interpolace. Základní věta algebry a její důsledky; polynomy nad $\mathbb{Z}_n$. Hranice rozložení kořenů. Vietovy věty.

2. Derivace polynomu, násobnost kořenů polynomu, eliminace násobnosti kořenů.

3. Řešení polynomiálních rovnic v radikálech:

   Lagrangeova postupná symetrizace na příkladu kubické rovnice, normální řada pro obecnou kubickou a kvartickou rovnici, věta o řešitelnosti algebraické rovnice v radikálech. Důkaz, že $\mathbb{A}_5$ je jednoduchá.

4. Symetrické polynomy, jednoduché symetrické polynomy. Hlavní věta o symetrických polynomech, elementární symetrické polynomy. Diskriminant, vyjádření pomocí determinantů.

Grupy a pole

K SZZ vše, co je *kurzívou*.

5. Pouze informativně: Struktura konečných abelovských (neboli komutativních) grup, cyklické grupy (komutativita cyklických grup, normální podgrupy konečných cyklických grup, cykličnost grup prvočíselného řádu), věta Cauchyova, první věta Sylowova.

6. *Prvopole konečného i nekonečného pole, struktura konečných polí.*

7. Kořenové a rozkladové nadtěleso, stupeň rozšíření.

8. *Konstruovatelnost pravítkem a kružítkem: eukleidovsky konstruovatelné body a čísla; tři klasické úlohy starověku, zdvojení krychle, trisekce úhlu, kvadratura kruhu (a rektifikace kružnice). Konstruovatelnost pravidelných n-úhelníků.*

9. *Kroneckerova věta, aplikace při zavedení komplexních čísel.*

Polynomy

Co je to polynom

- **definice** polynomu

Polynom a jeho hodnoty

- **Hornerovo schéma:** dán polynom, vypočíst efektivně jeho hodnoty
- **Lagrangeova interpolace:** dány hodnoty, najít polynom nabývající těchto hodnot

Polynom a jeho kořeny

- **Základní věta algebry**, polynomy nad $\mathbb{Z}_n$
  - Má vůbec každý polynom nějaké kořeny? Kolik jich má?
  - Řešení podstatně závisí na oboru integrity či poli…
- **Hranice rozložení kořenů**
  - kde se tyto kořeny nacházejí – přibližná lokalizace
- **Vietovy věty**
  - vztah mezi kořeny a koeficienty polynomu
- **Násobné kořeny**
  jsou-li některé kořeny polynomu násobné, jak:
  - to poznat (**diskriminant**)
  - se jich „zbavit“, tj. získat polynom se stejnými kořeny, avšak všemi jednoduchými (**derivace polynomu**)
- **Hledání kořenů**
  - existence obecného „vzorce“ pro kořeny polynomu stupně n
  - odvození vzorce pro kořeny ve speciálních případech (rovnice kvadratická, kubická)
  - obecný postup nalezení vzorce pro rovnice libovolného stupně

Seminář 29. 10. 2024

Lagrangeova interpolace, Hornerovo schéma

1. Pomocí předpisu pro Lagrangeovu interpolaci napište polynom $p \in \mathbb{R}[x]$, pro nějž platí:
   a) $p(2) = -5$, $p(4) = 7$, $p(0) = 8$, b) $p(2) = 1$, $p(3) = 1$, $p(4) = 1$.
   Výsledný polynom není třeba převádět na tvar dle definice polynomu.
2. Pomocí Hornerova schématu najděte hodnoty $p(1), p(3), p(-2)$ polynomu
$$p(x) = 2x^4 - 3x^3 + x^2 - 5x + 1.$$

Eukleidův algoritmus – opakování

1. Pomocí Eukleidova algoritmu najděte největší společný dělitel čísel a a b.
   a) $a = 6\,487$, $b = 48\,403$, b) $a = 353\,623$, $b = 244\,571$.

Polynomy v $\mathbb{Z}_n$

Následující úlohy poskytují základ pro důležitá pozorování. Každá z nich má svůj význam pro teorii.

1. Následující rovnice lze řešit zkusmo – dosazením všech hodnot z konečné množiny $\mathbb{Z}_n$.
   a) Najděte v poli $\mathbb{Z}_7$ všechna řešení rovnice $x^2 + 3x + 2 = 0$.
   b) Najděte v okruhu $\mathbb{Z}_6$ všechna řešení rovnice $x^2 + 3x + 2 = 0$.
   c) Najděte v okruhu $\mathbb{Z}_6$ všechna řešení rovnice $x^3 + 5x = 0$.
   d) Najděte v poli $\mathbb{Z}_3$ všechna řešení rovnice $x^2 + x + 2 = 0$.
   e) Najděte v okruhu $\mathbb{Z}_9$ všechna řešení rovnice $6x + 1 = 0$.
2. Dosazením všech hodnot ze $\mathbb{Z}_3$ ověřte, že následující polynomy ze $\mathbb{Z}_3[x]$ nabývají pro každé $x \in \mathbb{Z}_3$ stejných hodnot:
$$2x + 2 \quad = \quad 2x^3 + 2 \quad = \quad 2x^4 + 2x^3 + x^2 + 2 \quad = \quad x^3 + x + 2 \qquad \forall x \in \mathbb{Z}_3\,.$$
   Takovýchto polynomů lze nalézt více, mezi polynomy stupně 4 jsou to také:
$$2x^4 + x^3 + x^2 + x + 2, \quad 2x^4 + x^2 + 2x + 2, \quad x^4 + 2x^2 + 2x + 2\,.$$
3. Uvažte, že uvedená tabulka skutečně obsahuje:
   a) *všechny* polynomiální funkce na $\mathbb{Z}_3$,
   b) *všechny* polynomy stupně nejvýše 2 (a nulový polynom) na $\mathbb{Z}_3$.
   Všechny polynomiální funkce na $\mathbb{Z}_3$ lze tedy popsat pomocí všech polynomů stupně nejvýše 2 (a nulového polynomu).
4. Pokuste se vlastním výpočtem (nikoli nahlédnutím do tabulky) najít polynom stupně nejvýše 2, který na $\mathbb{Z}_3$ nabývá hodnot
$$f(0) = 2\,, \quad f(1) = 2\,, \quad f(2) = 0\,.$$
   Můžete užít např. metodu neurčitých koeficientů.
5. Kolik je všech *polynomiálních funkcí* nad $\mathbb{Z}_n$? A kolik je úplně všech *funkcí* nad $\mathbb{Z}_n$?
6. Pokud bychom chtěli popsat všechny polynomiální funkce na $\mathbb{Z}_5$ pomocí polynomů co nejnižšího stupně n, kolik by bylo toto nejnižší možné n?
7. Pomocí konkrétních protipříkladů ukažte, že pole $\mathbb{Z}_3$ a $\mathbb{Z}_5$ nejsou algebraicky uzavřená, tj. najděte polynom stupně $n \geq 1$, který má méně než n kořenů. Konkrétně, najděte polynom stupně 2, který nemá v $\mathbb{Z}_3$, resp. v $\mathbb{Z}_5$, žádný kořen.
8. Najděte dva různé polynomy v $\mathbb{Z}_3$, jejichž polynomiální funkce jsou si rovny. Čím se tyto dva polynomy liší (jaký je jejich rozdíl)?

Polynomy $p(x) = ax^2 + bx + c$ se zadanými hodnotami v $\mathbb{Z}_3$

$p(0)$	$p(1)$	$p(2)$	polynom $p(x)$ v $\mathbb{Z}_3$
0	0	0	0
0	0	1	$2x^2 + x$
0	0	2	$x^2 + 2x$
0	1	0	$2x^2 + 2x$
0	1	1	x^2
0	1	2	x
0	2	0	$x^2 + x$
0	2	1	$2x$
0	2	2	$2x^2$
1	0	0	$2x^2 + 1$
1	0	1	$x^2 + x + 1$
1	0	2	$2x + 1$
1	1	0	$x^2 + 2x + 1$
1	1	1	1
1	1	2	$2x^2 + x + 1$
1	2	0	$x + 1$
1	2	1	$2x^2 + 2x + 1$
1	2	2	$x^2 + 1$
2	0	0	$x^2 + 2$
2	0	1	$x + 2$
2	0	2	$2x^2 + 2x + 2$
2	1	0	$2x + 2$
2	1	1	$2x^2 + 2$
2	1	2	$x^2 + x + 2$
2	2	0	$2x^2 + x + 2$
2	2	1	$x^2 + 2x + 2$
2	2	2	2

Seminář 12. 11. 2024

Vyřešte druhou úlohu z předchozího semináře (Hornerovo schéma).

Aplikace Eukleidova algoritmu a derivace polynomu

1. Najděte kořeny následujících polynomů.
   a) $p(x) = x^4 - 6\,x^3 + 13\,x^2 - 12\,x + 4$ b) $p(x) = x^5 - 7\,x^4 + 19\,x^3 - 25\,x^2 + 16\,x - 4$
   Postupujte tak, že se pokusíte snížit jejich stupeň odstraněním násobnosti kořenů.
   Využijte přitom:
   - větu o násobných kořenech polynomu a jeho derivace a
   - Eukleidova algoritmu pro nalezení $\mathrm{NSD}(p, p')$.
   Hledejte tedy kořeny polynomu

$$\frac{p(x)}{\mathrm{NSD}(p(x), p'(x))}\,.$$

Hranice rozložení kořenů polynomu

1. Najděte poloměr kruhu se středem v počátku (v Gaussově rovině), v němž se nacházejí všechny kořeny následujícího polynomu.

a) $x^3 - 3x^2 + x - 3 = 0$ b) $x^3 - 7x + 6 = 0$ c) $x^5 + 4x^4 - 6x^3 - 15x^2 + 26x - 10$

Vietovy věty

1. Uvažujme kubickou rovnici v redukovaném tvaru: $x^3 + px + q = 0$. Dokažte, že součet všech jejích kořenů je roven nule.

2. O polynomu
$$2x^3 - x^2 - 7x + d$$
víme, že všechny jeho kořeny jsou reálné a součet dvou z nich je roven jedné. Najděte d a všechny kořeny tohoto polynomu.

Kořeny rovnic a jejich vlastnosti

1. Čemu je rovna druhá odmocnina $\sqrt{1}$ v $\mathbb{R}$ a čemu je rovna $\sqrt{1}$ v $\mathbb{C}$? Vše pečlivě vypočtěte.

Numerické řešení rovnice – aplikace spojitosti a Bolzanových vět

1. Najděte „metodou zkusmo“ záporný kořen (s přesností na 3 desetinná místa) rovnice
$$x^2 = 2^x\,.$$
$$\begin{array}{rcl} x^2 & = & 2^x \\ (-1)^2 & > & 2^{-1} \\ 0^2 & < & 2^0 \\ (-0,7)^2 & < & 2^{-0,7} \\ (-0,8)^2 & > & 2^{-0,8} \end{array}$$
Vidíme, že záporný kořen rovnice $x^2 = 2^x$ leží mezi:
   - -1 a 0, je tedy roven $-0,...$
   - $-0,8$ a $-0,7$, je tedy roven $-0,7...$

2. Najděte „metodou zkusmo“ reálný kořen (s přesností na 3 desetinná místa) rovnice
$$x = \cos x\,.$$

Permutace a grupy – opakování

1. Zopakujte si vše o permutacích: J. Bečvář: *Lineární algebra*, str. 51–60.
   Připomeňte si pojmy: permutace, cyklus, rozklad na nezávislé cykly, znaménko permutace, počet inverzí, transpozice. Uvědomte si, že cyklus generuje cyklickou grupu. Uveďte konkrétní příklad.

2. Zopakujte si:
   a) Definujte cyklickou grupu.
   b) Je cyklická grupa vždy komutativní? Své tvrzení podložte.

3. Zopakujte si faktorizaci grupy podle normální podgrupy:
   a) Definujte normální podgrupu.
   b) Je podgrupa komutativní grupy vždy normální? Své tvrzení podložte.
   c) Lze vždy faktorizovat podle cyklické podgrupy? Své tvrzení podložte.

Příště budeme pracovat s textem obsahujícím formule ke kubické rovnici: zde v pdf

Z následujícího textu o diskriminantu prostudujte kap. 1.1 až 1.4.

1 Diskriminant

1.1 Diskriminant kvadratické rovnice

Diskriminant kvadratické rovnice $ax^2 + bx + c = 0$, $a, b, c \in \mathbb{R}$, $a \neq 0$ se ve školské matematice zavádí tak, že můžeme snadno nabýt dojmu, že je pouhým označením výrazu pod odmocninou ve vzorci pro kořeny:

$$D = b^2 - 4ac\,.$$

Toto označení se jeví jako užitečné, neboť diskriminant slouží při rozlišování (z latinského *discrimino*, odlišuji, odděluji) případů, které mohou nastat:

- $D > 0$, pak má rovnice 2 různé reálné kořeny,
- $D = 0$, pak má rovnice 1 dvojnásobný kořen,
- $D < 0$, pak má rovnice 2 komplexně sdružené kořeny.

1.2 Diskriminant libovolného polynomu stupně alespoň druhého

Je možné diskriminant definovat také pro rovnice vyšších stupňů? Jaký by mohl mít význam? Jelikož polynomy z $\mathbb{R}[x]$ vyšších stupňů mohou mít reálné i komplexní kořeny, není možné, aby znaménko jednoho čísla vypovídalo o počtu komplexních kořenů; pouhý údaj, že polynom má či nemá komplexní kořeny, není dostatečně zajímavý.

Vzpomeňme však na základní problém: *určit kořeny zadaného polynomu* $f \in \mathbb{C}[x]$. Než je začneme hledat, je výhodné ověřit, že polynom nemá násobné kořeny. Kdyby je měl, mohli bychom snížit jeho stupeň tím, že bychom vyšetřovali polynom $\bar{f}$ s týmiž kořeny jako f, avšak všechny by byly jednoduché. Takový polynom lze najít snadno:

$$\bar{f} = \frac{f}{\mathrm{NSD}\,(f, f')}\,.$$

Snížením stupně polynomu bychom si pak usnadnili výpočty spojené s hledáním kořenů. *Diskriminant by tedy mohl sloužit k rozhodování, zda má rovnice násobné kořeny.*

1.3 Obecná definice diskriminantu

Jak najít výraz, který by indikoval výskyt násobných kořenů? U kubické rovnice je to snadné; výraz

$$\tilde{D}_3 = (x_1 - x_2) \cdot (x_1 - x_3) \cdot (x_2 - x_3)$$

bude nulový právě tehdy, když si budou rovny alespoň dva z kořenů. Problém však je, že tento výraz můžeme napsat (a tedy i vyšetřovat) pouze tehdy, když známe všechny kořeny. Pak je však rozhodování o jejich násobnosti triviální. Výraz $\tilde{D}_3$ tedy budeme chtít vyjádřit pomocí koeficientů příslušného polynomu. To však bude možné pouze tehdy, pokud bude $\tilde{D}_3$ možno vyjádřit jako funkci symetrického polynomu s neurčitými x_1, x_2, x_3. Toho lze dosáhnout snadno, stačí místo $\tilde{D}_3$ vyšetřovat

$$\boxed{D_3 = (x_1 - x_2)^2 \cdot (x_1 - x_3)^2 \cdot (x_2 - x_3)^2\,.}$$

Tento výraz lze na základě hlavní věty o symetrických polynomech vyjádřit pomocí elementárních symetrických polynomů, tedy (na základě Vietových vzorců) pomocí koeficientů polynomu. Obecně *diskriminantem polynomu n-tého stupně* rozumíme výraz

$$D_n = \prod_{1 \leq i < k \leq n} (x_i - x_k)^2\,.$$

1.4 Vyjádření diskriminantu pomocí determinantu

Klíčové je uvědomit si, že výraz

$$\sqrt{D_3} = |(x_1 - x_2) \cdot (x_1 - x_3) \cdot (x_2 - x_3)|$$

je dělitelný každým dvojčlenem $x_i - x_j$, kde $i, j \in \{1, 2, 3\}$, $i \neq j$, stejně jako *Vandermondův determinant*

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix},$$

je dělitelný každým dvojčlenem $x_i - x_j$, kde $i, j \in \{1, 2, 3\}$, $i \neq j$; stačí odečíst j-tý sloupec od i-tého. Například dělitelnost $x_3 - x_1$ ověříme odečtením 1. sloupce od 3. sloupce, tj.

$$\begin{vmatrix} 1 & 1 & 0 \\ x_1 & x_2 & x_3 - x_1 \\ x_1^2 & x_2^2 & x_3^2 - x_1^2 \end{vmatrix}.$$

Vypočtěme nyní výše uvedený Vandermondův determinant. Začneme tím, že od 2. a 3. řádku odečteme x_1-násobek, resp. x_1^2-násobek 1. řádku (je-li x_1 nenulové):

$$\begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 0 & x_2 - x_1 & x_3 - x_1 \\ 0 & x_2^2 - x_1^2 & x_3^2 - x_1^2 \end{vmatrix}$$

Tento determinant rozvineme podle prvků 1. sloupce:

$$\begin{vmatrix} 1 & 1 & 1 \\ 0 & x_2 - x_1 & x_3 - x_1 \\ 0 & x_2^2 - x_1^2 & x_3^2 - x_1^2 \end{vmatrix} = 1 \cdot (-1)^{1+1} \cdot \begin{vmatrix} x_2 - x_1 & x_3 - x_1 \\ x_2^2 - x_1^2 & x_3^2 - x_1^2 \end{vmatrix} + 0 + 0$$

a z 1. sloupce vytkneme $x_2 - x_1$, z 2. sloupce vytkneme $x_3 - x_1$:

$$\begin{vmatrix} x_2 - x_1 & x_3 - x_1 \\ x_2^2 - x_1^2 & x_3^2 - x_1^2 \end{vmatrix} = (x_2 - x_1)(x_3 - x_1) \cdot \begin{vmatrix} 1 & 1 \\ x_2 - x_1 & x_3 - x_1 \end{vmatrix}$$

a zbylý determinant rozepíšeme pomocí Sarrusova pravidla:

$$(x_2 - x_1)(x_3 - x_1) \cdot \begin{vmatrix} 1 & 1 \\ x_2 - x_1 & x_3 - x_1 \end{vmatrix} = (x_2 - x_1)(x_3 - x_1) \cdot \Big[(x_3 - x_1) - (x_2 - x_1) \Big] =$$

$$(x_2 - x_1)(x_3 - x_1)(x_3 - x_2) = -\tilde{D}_3 \,.$$

Absolutní hodnota Vandermondova determinantu je tedy rovna $\sqrt{D_3}$. Hledáme však D_3, takže vypočtěme druhou mocninu tohoto determinantu. Jelikož je $\det A = \det A^T$ pro každou čtvercovou matici A, můžeme psát

$$D_3 = \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix} \cdot \begin{vmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{vmatrix} = \begin{vmatrix} 1+1+1 & x_1+x_2+x_3 & x_1^2+x_2^2+x_3^2 \\ x_1+x_2+x_3 & x_1^2+x_2^2+x_3^2 & x_1^3+x_2^3+x_3^3 \\ x_1^2+x_2^2+x_3^2 & x_1^3+x_2^3+x_3^3 & x_1^4+x_2^4+x_3^4 \end{vmatrix}.$$

Označíme-li součty k-tých mocnin

$$S_k = x_1^k + x_2^k + x_3^k \,, \quad k \in \{0, 1, 2, \dots\} \,,$$

můžeme psát

$$D_3 = \begin{vmatrix} S_0 & S_1 & S_2 \\ S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \end{vmatrix}.$$

Podobně D_n je možno zapsat pomocí analogicky sestaveného determinantu n-tého řádu, např.:

$$D_4 = \begin{vmatrix} S_0 & S_1 & S_2 & S_3 \\ S_1 & S_2 & S_3 & S_4 \\ S_2 & S_3 & S_4 & S_5 \\ S_3 & S_4 & S_5 & S_6 \end{vmatrix}.$$

1.5 Diskriminant kubické rovnice

Vypočtěme nyní diskriminant kubické rovnice v redukovaném tvaru

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

Z Vietových vět plyne, že $E_1 = 0$, $E_2 = p$, $E_3 = -q$. Vzhledem k tomu, že $E_1 = 0$, vyjádření S_k pomocí elementárních symetrických polynomů se podstatně zjednoduší. Pomocí postupu z důkazu hlavní věty o symetrických polynomech tak dostáváme:

$$S_0 = x_1^0 + x_2^0 + x_3^0 = 1 + 1 + 1 = 3$$

$$S_1 = x_1 + x_2 + x_3 = E_1 = 0$$

$$S_2 = x_1^2 + x_2^2 + x_3^2 = E_1^2 - 2E_2 = 0 - 2p = -2p$$

$$S_3 = x_1^3 + x_2^3 + x_3^3 = E_1^3 - 3E_1E_2 + 3E_3 = 0 - 3\cdot 0 + 3(-q) = -3q$$

Podobně

$$S_4 = x_1^4 + x_2^4 + x_3^4 = E_1^4 + 2E_2^2 + 4E_1E_3 - 4E_1^2E_2 = 2E_2^2 = 2p^2$$

Celkem tedy dostaneme:

$$S_0 = 3, \quad S_1 = E_1 = 0, \quad S_2 = -2E_2 = -2p, \quad S_3 = 3E_3 = -3q, \quad S_4 = 2E_2^2 = 2p^2\,.$$

$$D_3 = \begin{vmatrix} S_0 & S_1 & S_2 \\ S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \end{vmatrix} = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ p & -3q & 0 \end{vmatrix} =$$

$$3\cdot\begin{vmatrix} -2p & -3q \\ -3q & 0 \end{vmatrix} + (-2p)\cdot\begin{vmatrix} 0 & -2p \\ p & -3q \end{vmatrix} = 3\cdot(-9q^2) - 2p\cdot 2p^2 = -\left(27q^2 + 4p^3\right)$$

Dostáváme tak diskriminant, který známe z Cardanova postupu řešení kubické rovnice:

$$\boxed{D_3 = -27\cdot 4\cdot\left(\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\right).}$$

1.6 Rekurentní vzorce pro zájemce

Jelikož jsou S_k symetrické polynomy, lze je dle hlavní věty o symetrických polynomech zapsat pomocí elementárních symetrických polynomů (značme je E_d, tj. například $E_1 = \sum_{i=1}^r x_i$, $E_2 = \sum_{i=1}^r \sum_{j=i+1}^r x_ix_j$, $E_3 = \sum_{i=1}^r \sum_{j=i+1}^r \sum_{m=j+1}^r x_ix_jx_m$, …, přičemž pro $r > n$ klademe $E_r = 0$).

Při vyjadřování S_k pomocí E_d dle hlavní věty o symetrických polynomech ihned dojdeme k rekurentnímu vztahu, tzv. *Newtonovu vzorci*:

$$S_k = E_1S_{k-1} - E_2S_{k-2} + E_3S_{k-3} - E_4S_{k-4} + \cdots + (-1)^k E_{k-1}S_1 + (-1)^{k+1}kE_k\,.$$

Speciálně pro $n = 3$ tedy dostáváme:

$$S_0 = x_1^0 + x_2^0 + x_3^0 = 1 + 1 + 1 = 3$$

$$S_1 = x_1 + x_2 + x_3 = E_1$$

$$S_2 = x_1^2 + x_2^2 + x_3^2 = E_1S_1 - 2E_2 = E_1^2 - 2E_2$$

$$S_3 = x_1^3 + x_2^3 + x_3^3 = E_1S_2 - E_2S_1 + 3E_3 = E_1(E_1^2 - 2E_2) - E_2E_1 + 3E_3 =$$
$$= E_1^3 - 3E_1E_2 + 3E_3$$

$$S_4 = x_1^4 + x_2^4 + x_3^4 = E_1S_3 - E_2S_2 + E_3S_1 - 4E_4$$

Seminář 26. 11. 2024

formule ke kubické rovnici: zde v pdf

Opakování některých pojmů a výsledků

Normální řadou grupy $(G, \cdot)$ rozumíme konečný řetězec podgrup

$$N_1 = \{e\} \lhd N_2 \lhd N_3 \lhd N_4 \lhd \cdots \lhd N_{n-1} \lhd N_n \lhd G = N_{n+1},$$

kde pro každé $i = 1, 2, \ldots, n$ je N_i normální podgrupou grupy N_{i+1}. Číslo n nazýváme *délkou* normální řady, faktorové grupy N_{i+1}/N_i se nazývají *faktory* této normální řady.

Normální řada grupy G se nazývá *řešitelná*, je-li každý její faktor N_{i+1}/N_i cyklickou grupou.

Grupa G se nazývá *řešitelná*, má-li alespoň jednu řešitelnou normální řadu.

Věta: Obecná algebraická rovnice stupně $n \in \mathbb{N}$ je řešitelná v radikálech právě tehdy, když je grupa $\mathbb{S}_n$ řešitelná.

Věta Abelova–Ruffiniova: Pro $n \geq 5$ existují algebraické rovnice stupně n, které nejsou řešitelné v radikálech.

Neboli: grupy $\mathbb{S}_n$ nejsou pro $n \geq 5$ řešitelné.
(Důkaz pro grupu $\mathbb{S}_5$ provedeme na přednášce.)

Úlohy

1. Vyřešte následující soustavu (stačí najít t_1^3 a t_2^3) pro dané $q, D \in \mathbb{C}$.

$$t_1^3 + t_2^3 = -27q$$
$$(t_1^3 - t_2^3)^2 = (2 \cdot 27)^2 \cdot D$$

2. Vypište všechny permutace z grupy $\mathbb{S}_3$. Každou z těchto permutací rozložte na nezávislé cykly a určete její znaménko.

3. Dokažte, že $\mathbb{A}_3$ je cyklickou grupou.
. [zapíšeme všechny prvky $\mathbb{A}_3$ pomocí mocniny vhodného cyklu]

4. Dokažte, že každá grupa $\mathbb{S}_n$ má normální podgrupu $\mathbb{A}_n$ a faktorová grupa $\mathbb{S}_n/\mathbb{A}_n$ je cyklická. Najděte tuto faktorovou grupu.

5. Ukažte, že každá cyklická grupa je řešitelná. [$\{e\} \lhd C$]

6. Poznamenejme, že indukcí (přes řád grupy) by šlo dokázat, že každá konečná komutativní grupa je řešitelná. (důkaz není potřeba provádět)

7. Podrobně si zopakujte obecný postup řešení polynomiálních rovnic Lagrangeovou metodou postupné symetrizace, tj. pomocí symetrických polynomů a permutací, a to na příkladu kvadratické a kubické rovnice.

Kvartická rovnice

1. moc hezké shrnutí ke kvartické rovnici od pana Sedláka: zde v pdf

2. Všimněte si, jakého tvaru jsou všechny sudé permutace čtyř prvků, tj. permutace, jejichž znaménko je 1. Připomeňme si, že pro každou $P \in \mathbb{S}_4$ platí: $\operatorname{sgn} P = (-1)^{4-k}$, kde k je počet nezávislých cyklů, na něž se P rozkládá. Aby byla P sudá (tj. $\operatorname{sgn} P = 1$), musí být exponent $4 - k$ sudý. Takže sudé permutace čtyř prvků musí být pouze v jednom z následujících tvarů:

   - $k = 4$, tj. $\operatorname{sgn} P = (-1)^{4-4} = (-1)^0$, tj. $P = (1)(2)(3)(4) = \mathrm{id}$,
   - $k = 2$, tj. $\operatorname{sgn} P = (-1)^{4-2} = (-1)^2$, tj. $\quad P = (i,j)(k,l) \quad$ nebo $\quad P = (i,j,k)(l)$.

3. a) Vypište všechny permutace z alternující grupy $\mathbb{A}_4$ (tj. všechny sudé permutace čtyř prvků). Postupujte systematicky, využijte poznatků z předchozího bodu.

   b) Všimněte si, že všechny permutace, které jsou složením dvou cyklů délky 2 (tj. dvou transpozic) tvoří (společně s identitou) grupu řádu 4. Nazýváme ji Kleinovou čtyř-grupou, označujeme ji K_4 nebo V_4 (Viergruppe).

   c) Vypočtěte všechny prvky tříd $(2,3,4)K_4$ a $(2,3,4)^2K_4$. Všimněte si, že to jsou už všechny permutace z $\mathbb{A}_4$, které lze zapsat jako trojcyklus (tj. jsou složením cyklů délky 3 a 1).

4. Podaří se Vám na základě předchozího bodu najít následující normální řadu grupy $\mathbb{S}_4$?

$$\{\mathrm{id}\} \lhd C(2) \lhd K_4 \lhd \mathbb{A}_4 \lhd \mathbb{S}_4$$

   (K_4 – Kleinova čtyřgrupa, $C(2)$ – cyklická grupa řádu 2)

5. $\mathbb{A}_5$ je podgrupa sudých permutací v grupě $\mathbb{S}_5$. Na základě vztahu

$$\operatorname{sgn} P = (-1)^{\text{sudé číslo}} = (-1)^{5-k}$$

   zvažte, jaké permutace mohou být prvky $\mathbb{A}_5$. Vypište všechny typy kombinací zapsané pomocí rozkladů na nezávislé cykly (přesněji pomocí délek těchto cyklů podobně jako v bodě 2).

Zajímavosti (pro zájemce)

6. Problém z předchozího bodu souvisí s rozklady přirozených čísel na součty, o nichž se také hovoří ve filmu *Muž, který poznal nekonečno* (nazývané tam jako *parciace*, viz od 44. minuty):
   `https://www.youtube.com/watch?v=fAuDYnyvvw8`.

7. „Parciace“ dvou, tří, čtyř a pěti:

$$2 = 1 + 1$$

$$3 = 2 + 1 = 1 + 1 + 1$$

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$$

$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1$$

   Mimochodem, zde jsou počty $P(n)$ rozkladů na součty vybraných přirozených čísel n:

n	$P(n)$
1	1
2	2
3	3
4	5
5	7
6	11
7	15

n	$P(n)$
8	22
9	30
10	42
50	204 226
100	190 569 292
200	3 972 999 029 388

Symetrické polynomy

1. Zopakujte si pojmy: symetrický polynom, jednoduchý symetrický polynom, elementární symetrický polynom, výška, vedoucí člen.

2. Ověřte, že platí následující vztahy, postupujte při tom pomocí myšlenky z důkazu hlavní věty o symetrických polynomech.

$$S_0 = x_1^0 + x_2^0 + x_3^0 = 1 + 1 + 1 = 3$$

$$S_1 = x_1 + x_2 + x_3 = E_1$$
$$S_2 = x_1^2 + x_2^2 + x_3^2 = E_1^2 - 2E_2$$
$$S_3 = x_1^3 + x_2^3 + x_3^3 = E_1^3 - 3E_1E_2 + 3E_3$$

3. Z textu o diskriminantu prostudujte závěrečnou kapitolu 1.6.

4. Určete, jaký člen vyjádřený pomocí elementárních symetrických polynomů musíme od zadaného jednoduchého symetrického polynomu odečíst, abychom eliminovali člen s největší výškou.

   a) $\sum x_1^{10} x_2^5 x_3^2$ [musíme odečíst $E_1^5 E_2^3 E_3^2$]
   b) $\sum x_1^2 x_2 x_3$
   c) $\sum x_1^3 x_2^3 x_3$

Seminář 10. 12. 2024

Cyklické grupy, komutativní grupy

1. poznámky ke grupám zde v pdf

2. Vypište všechny podgrupy cyklické grupy $C(12)$. Jsou všechny tyto podgrupy normální?

3. Rozhodněte, zda je grupa řádu 7 cyklická.

4. O grupě G víme, že její řád je alespoň 14 a nejvýše 18, navíc víme, že nemá žádné vlastní podgrupy. Podaří se Vám přesně určit řád této grupy?

5. Určete počet (neizomorfních) komutativních grup řádu: a) 5, b) 32.

V následujícím svá rozhodnutí podložte příslušnou větou. Rozhodněte, zda grupa řádu

1. 12 má jako svou podgrupu: a) $C(2)$, b) $C(3)$.

2. 12 má podgrupu řádu 4.

3. 24 má podgrupu řádu: a) 8, b) 2, c) 3.

4. Rozhodněte, zda grupa $\mathbb{A}_4$ má podgrupu řádu: a) 2, b) 3, c) 4.

V případě existence tyto grupy stručně popište (název či stručná charakterizace).

Pole, prvopole, struktura konečných polí (opakování)

1. Struktura konečných polí: zde v pdf (text ze skripta D. Stanovského)
2. Prvopolem pole F rozumíme jeho nejmenší podpole.
3. Každé nekonečné pole obsahuje jako své podpole pole izomorfní s $\mathbb{Q}$.
4. $\mathbb{Q}$ je nejmenší nekonečné pole, je prvopolem (až na izomorfismus) každého nekonečného pole.
5. Zopakujte si konstrukci prvopole nekonečného i konečného pole. Vyjděte z axiomů pole (existence nulového a jednotkového prvku, existence opačných a inverzních prvků).
6. Každé konečné pole obsahuje jako své podpole pole izomorfní s $\mathbb{Z}_p$, kde p je nějaké prvočíslo. Každé konečné pole má právě p^k prvků, kde $p \in \mathbb{P}$ je nějaké prvočíslo a $k \in \mathbb{N}$ je nějaké přirozené číslo ($k \geq 1$). Konečná pole pak zpravidla zapisujeme $\mathbb{GF}(p^k)$ (podle *Galois field*).
7. Prvky konečného pole lze přehledně popsat: jsou to právě všechny kořeny polynomu $x^{p^k} - x$ nad $\mathbb{Z}_p$. Obecně však tyto kořeny nemusí ležet v $\mathbb{Z}_p$ (pro $k > 1$ je prvků pole $\mathbb{GF}(p^k)$ více než prvků pole $\mathbb{Z}_p$), $\mathbb{GF}(p^k)$ je tedy rozkladovým nadtělesem polynomu $x^{p^k} - x$ nad $\mathbb{Z}_p$. Samotné pole $\mathbb{Z}_p$ pak plní roli prvopole v $\mathbb{GF}(p^k)$.

Úlohy

8. Rozhodněte, zda mohou existovat konečná pole, která mají následující počty prvků.
   a) 1 b) 2 c) 4 d) 6 e) 8 f) 10 g) 11 h) 24 i) 25 j) 81

Kořenové a rozkladové nadtěleso, stupeň rozšíření

1. Ukažte, že rozkladové pole polynomu $p \in \mathbb{Q}[x]$, kde $p(x) = x^2 - 5$, je pole $\mathbb{Q}(\sqrt{5})$. Napište, jakého tvaru jsou všechny prvky z $\mathbb{Q}(\sqrt{5})$ (tj. k poli racionálních čísel je adjungován prvek $\sqrt{5}$).
2. Ukažte, že rozkladové pole polynomu $p \in \mathbb{Q}[x]$, kde $p(x) = (x^2 - 2) \cdot (x^2 - 5)$, je pole $\mathbb{Q}(\sqrt{2}, \sqrt{5})$.
3. Napište, jakého tvaru jsou všechny prvky z $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ (tj. k poli racionálních čísel jsou adjungovány prvky $\sqrt{2}, \sqrt{3}$).
4. Napište některé nadpole pole $\mathbb{Q}$, které je kořenovým nadpolem polynomu $p \in \mathbb{Q}[x]$, kde $p(x) = (x^2 - 2) \cdot (x^2 - 5)$.
   [$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$, ale také celé rozkladové nadpole, tj. $\mathbb{Q}(\sqrt{2}, \sqrt{5})$]

   Na příštím semináři probereme:

5. **Stupeň rozšíření:** Všechny prvky pole $\mathbb{Q}(\sqrt{3})$ jsou tvaru: $a \cdot 1 + b \cdot \sqrt{3}$, kde $a, b \in \mathbb{Q}$; tvoří tedy vektorový prostor s bází $\{1, \sqrt{3}\}$, **jeho dimenze je tedy 2**. Tuto dimenzi nazýváme stupněm rozšíření a značíme $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$, píšeme tedy:
$$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2\,.$$
6. Určete stupeň rozšíření $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$ a popište, jak vypadají všechny prvky vektorového prostoru $\mathbb{Q}(\sqrt{5})$ nad $\mathbb{Q}$.

7. **Pozor:** $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, neboť pole obsahující $\sqrt[3]{2}$ obsahuje také její mocniny: $\sqrt[3]{2}$, $(\sqrt[3]{2})^2$. Mocnina $(\sqrt[3]{2})^3$ už není novým prvkem, neboť $(\sqrt[3]{2})^3 = 2 \in \mathbb{Q}$.

   Všechny prvky z $\mathbb{Q}(\sqrt[3]{2})$ jsou tedy tvaru: $a \cdot 1 + b \cdot \sqrt[3]{2} + c \cdot (\sqrt[3]{2})^2$, kde $a, b, c \in \mathbb{Q}$; tvoří tedy vektorový prostor s bází $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$, **jeho dimenze je tedy 3**, proto:

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3\,.$$

8. Rozhodněte, zda je rozkladové pole polynomu $p \in \mathbb{Q}[x]$, kde $p(x) = (x^3 - 2) \cdot (x^2 - 5)$, rovno poli $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$. Určete stupeň rozšíření $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) : \mathbb{Q}]$ a napište, jakého tvaru jsou všechny prvky z $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5})$.

   Dále určete stupeň rozšíření $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) : \mathbb{Q}(\sqrt[3]{2})]$.

9. Ukažte (na jednom vhodně zvoleném konkrétním příkladě), že pro rozšíření $F \subset K \subset E$ platí:

$$[E : F] = [E : K] \cdot [K : F]\,.$$

Seminář 17. 12. 2024

Konstruovatelnost pravítkem a kružítkem

1. Materiály ke konstruovatelnosti pravítkem a kružítkem:
   scan z knihy [BeDla], str. 453–455 je (zde v pdf,
   výpisky doplněné o některá pozorování jsou zde v pdf)

2. Zopakujte si základní myšlenky důkazu tvrzení, že žádná se tří klasických úloh antické matematiky (zdvojení krychle, trisekce úhlu a kvadratura kruhu) není řešitelná pouze pomocí (eukleidovského) pravítka a kružítka.

3. Připomeňte si konstrukce součtu, rozdílu, součinu a podílu, což je základem důkazu tvrzení, že všechna racionální čísla jsou konstruovatelná.

4. Dokažte, že všechna pole $\mathbb{Q}(\sqrt{q})$, kde $q \in \mathbb{Q}^+$ obsahují pouze čísla, která jsou konstruovatelná. (Stačí dokázat, že druhá odmocnina každého kladného racionálního čísla je konstruovatelná – připomeňte si konstrukci pomocí Eukleidovy věty o výšce.)

Kroneckerova věta a zavedení komplexních čísel

1. Zopakujte si znění a ideu důkazu Kroneckerovy věty, viz též [BeDla] str. 311, věta číslo VII.77. Viz zde v pdf, výpisky doplněné o některá pozorování jsou zde v pdf.

2. Proč se v Kroneckerově větě předpokládá, že polynom p je nelineární? Uvažte například jednoduchý lineární polynom x a popište algebraické „rozšíření“ $\mathbb{R}[x]/\langle x\rangle$ pole $\mathbb{R}$, tj. popište, jak by vypadaly prvky $\mathbb{R}[x]/\langle x\rangle$.

3. Popište algebraické rozšíření $\mathbb{R}[x]/\langle x^2 + 1\rangle$ pole $\mathbb{R}$, tj. popište, jak by vypadaly prvky $\mathbb{R}[x]/\langle x^2 + 1\rangle$.

4. Na základě Kroneckerovy věty vysvětlete, proč jsou komplexní čísla reprezentovatelná lineárními polynomy s koeficienty z $\mathbb{R}$ (viz algebraický tvar komplexního čísla).

5. Proč jsou komplexní čísla reprezentovatelná právě lineárními polynomy s koeficienty z $\mathbb{R}$? Zvažte i tento argument: $\mathbb{C} = \mathbb{R}(\mathrm{i})$, tj. pole komplexních čísel vznikne z pole reálných čísel adjunkcí prvku i.

6. Srozumitelně vysvětlete, proč komplexní čísla nedefinujeme pomocí jejich algebraického tvaru ($a + b\,\mathrm{i}$, kde $\mathrm{i}^2 = -1$), ale definujeme je pomocí uspořádaných dvojic reálných čísel.

7. Pozor: při zavádění $\mathbb{C}$ nestačí uvažovat pouze množinu všech uspořádaných dvojic reálných čísel, k definici komplexních čísel to nestačí (tohle splňuje i vektorový prostor $\mathbb{R}^2$). Teprve zavedeme-li na těchto uspořádaných dvojicích operace sčítání a násobení:

$$\forall a, b, c, d \in \mathbb{R}\colon \quad [a, b] + [c, d] = [a + c, b + d]\,,$$

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

zavedli jsme komplexní čísla, tj. strukturu $(\mathbb{C}, +, \cdot)$.

Algebra

ukázkový zkouškový test

Jméno: Datum:

1. Pomocí konkrétního protipříkladu ukažte, že pole $\mathbb{Z}_5$ není algebraicky uzavřené.

2. Stručně naznačte ideu odvození vzorce pro odstranění násobnosti kořenů.

3. Najděte kořeny následujícího polynomu tak, že se pokusíte snížit jeho stupeň odstraněním násobných kořenů: $x^3 + 9x^2 + 27x + 27$. Využijte derivaci polynomu.

4. a) Definujte obecně diskriminant polynomu.
   b) Čím je tato definice motivována?
   c) Stručně odvoďte vyjádření diskriminantu kubického polynomu pomocí determinantu obsahujícího součty mocnin kořenů tohoto polynomu, využijte faktu, že $S_4 = 2p^2$.

5. a) Zformulujte základní výsledek o řešitelnosti rovnic v radikálech.
   b) Na příkladu kubické rovnice a chování t_1 a t_2 stručně vysvětlete, proč zde potřebujeme faktorové grupy a proč musejí být cyklické.
   c) Napište normální řadu grupy $\mathbb{S}_4$:
   d) Jak se projeví řád faktorové cyklické grupy (podgrup z normální řady) v Lagrangeově postupné symetrizaci? Uveďte reprezentativní konkrétní příklad u kvartické rovnice.

6. Symetrický polynom $x_1^3 + x_2^3 + x_3^3$ vyjádřete pomocí elementárních symetrických polynomů. Využijte postup z důkazu hlavní věty o symetrických polynomech.

7. Pomocí předpisu pro Lagrangeovu interpolaci napište polynom p, pro nějž platí:
   $p(2) = -5$, $p(1) = 3$, $p(0) = 8$.
   Výsledný polynom není třeba převádět na tvar dle definice polynomu.

8. Pomocí Hornerova schématu vypočtěte hodnotu polynomu $p(x) = -x^4 + 3x^2 + x + 6$ v bodě 2.

9. Uvažujme polynom $p(x) = (x^2 - 3)(x^2 - 2)$, $p \in \mathbb{Q}[x]$. Napište jeho rozkladové nadpole a nějaké jeho jeho kořenové nadpole (různé od rozkladového nadpole).

10. Názorně ukažte na konkrétním reprezentativním příkladě, že pro rozšíření $F \subset K \subset E$ platí:
$$[E : F] = [E : K] \cdot [K : F] .$$

11. Najděte stupeň rozšíření $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

12. Zdůvodněte, proč nelze klasickou úlohu zdvojení krychle řešit pouze pomocí eukleidovských konstrukcí.

13. Popište konstrukci úsečky délky: a) $a \cdot b$, b) $\sqrt{a}$, jsou-li dány úsečky délek a, b.

14. Odvoďte, jak vypadají prvopole konečných a nekonečných polí.

15. Zformulujte větu Cauchyovu a první Sylowovu pro grupy. Porovnejte je s klasickou větou Lagrangeovou.

16. Zformulujte Kroneckerovu větu a s její pomocí zdůvodněte, proč je jedním z vhodných zápisů komplexních čísel jejich algebraický tvar, tj. tvar lineárních polynomů.