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. Polynomy nad $\mathbb{Z}_n$.
   Je-li D obor integrity, pak také $D[x]$ tvoří obor integrity.

2. Základní věta algebry a její důsledky.
   Derivace polynomu, násobnost kořenů polynomu, eliminace násobnosti kořenů.

3. Hornerovo schéma, Lagrangeova interpolace.
   Vietovy věty. Hranice rozložení kořenů.

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

5. 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.

Grupy a pole

K SZZ vše, co je *kurzívou*.

6. 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.

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

8. Kořenové a rozkladové nadtěleso, stupeň rozšíření.

9. *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.*

10. *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

1 Seminář 27. 10. 2026

1.1 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)?

1.2 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

1.3 Eukleidův algoritmus – opakování

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

1.4 Hornerovo schéma – základní pozorování

1. **Pozorování:** Pokud polynom $p(x)$ napíšeme ve tvaru $p(x) = q(x) \cdot (x - c) + r$, tak hodnotu $p(c)$ najdeme snadno: je to přímo zbytek po dělení $p(c) = r$.

2. Je-li
$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \,,$$
pak porovnáním koeficientů můžeme získat koeficienty neznámého polynomu q:
$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \;=\; \left(b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1}\right) \cdot (x - c) \;+\; r \,.$$

3. Porovnejte koeficienty polynomů na levé a pravé straně ve formuli v předchozím bodě.
$$\begin{aligned} a_n &= b_{n-1} \\ a_{n-1} &= ... \\ &..... \\ a_0 &= r - c b_0 \end{aligned}$$

4. Pokud rovnosti z předchozího bodu zapíšeme do vhodného schématu, obdržíme tzv. *Hornerovo schéma.*

2 Seminář 3. 11. 2026

2.1 Hornerovo schéma, Lagrangeova interpolace

1. Pomocí Hornerova schématu najděte následující hodnoty polynomu
$$p(x) = -x^4 + 4x^3 - 2x^2 - 3x + 2.$$
   a) $p(2) =$ b) $p(-1) =$ c) $p(3) =$ d) $p(4) =$

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

2.2 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
$$\frac{p(x)}{\mathrm{NSD}(p(x), p'(x))} \,.$$

2.3 Kořeny rovnic a jejich vlastnosti

1. Čemu je rovna druhá odmocnina $\sqrt{1}$ v $\mathbb{R}$?
2. Čemu je rovna druhá odmocnina $\sqrt{1}$ v $\mathbb{C}$?
   Obojí pečlivě vypočtěte.

3. **Pozorování 1** (velmi důležité): najděte všechny třetí odmocniny z 1 v $\mathbb{C}$, tj. najděte všechny kořeny binomické rovnice $z^3 = 1$. Zapište je v goniometrickém i algebraickém tvaru.
4. **Pozorování 2:** všimněte si, že všechny třetí odmocniny z 1 lze napsat ve tvaru $1, \varepsilon, \varepsilon^2$. Kterou ze tří třetích odmocnin z 1 jsme označili jako ε?
5. **Pozorování 3:** všimněte si, že součet všech třetích odmocnin z 1 je roven nule:
$$1 + \varepsilon + \varepsilon^2 = 0\,.$$
6. **Dokažte:** analogické tvrzení platí obecně pro součty všech n-tých odmocnin z 1 ($n > 1$):
$$1 + \omega + \omega^2 + \omega^3 + \cdots + \omega^{n-1} = 0\,.$$

2.4 Numerické řešení rovnice – aplikace spojitosti a Bolzanových vět

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

2. Najděte „metodou zkusmo“ reálný kořen (s přesností na 3 desetinná místa) rovnice
$$x - \cos x = 0\,.$$

3 Semináře 10. 11. 2026 a 17. 11. 2026

Rektorské volno a státní svátek. Přednáška se sice nekoná, ale je třeba studovat.
Úkolem je vypracovat řešení následující úloh
a prostudovat vše, co je zde (až do konce souboru).

3.1 Vietovy věty

1. Odvoďme Vietovy věty pro kvadratický polynom

$$x^2 + px + q$$

porovnáním s výsledkem součinu kořenových činitelů:

$$(x - x_1) \cdot (x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2 \,.$$

Dostáváme tak Vietovy věty:

$$\begin{aligned} x_1 + x_2 &= -p \\ x_1x_2 &= q \end{aligned}$$

2. Odvoďte samostatně Vietovy věty pro kubický polynom

$$x^3 + ax^2 + bx + c$$

porovnáním s výsledkem součinu kořenových činitelů. Dostanete tak Vietovy věty:

$$\begin{aligned} x_1 + x_2 + x_3 &= -a \\ x_1x_2 + x_2x_3 + x_3x_1 &= b \\ x_1x_2x_3 &= -c \end{aligned}$$

Všimněme si indexů v jednotlivých součinech: postupně vytváříme všechny kombinace; všech příslušných kombinací v jednotlivých řádcích je:

$$\binom{3}{1} \qquad \binom{3}{2} \qquad \binom{3}{3} .$$

3. Odvoďte samostatně Vietovy věty pro polynom čtvrtého stupně

$$x^4 + ax^3 + bx^2 + cx + d \,.$$

Pro kontrolu: počet sčítanců v jednotlivých řádcích je:

$$\binom{4}{1} = 4 \qquad \binom{4}{2} = 6 \qquad \binom{4}{3} = 4 \qquad \binom{4}{4} = 1 \,.$$

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

5. O polynomu

$$2x^3 - x^2 - 7x + d$$

víme, že všechny jeho kořeny jsou reálné a součet dvou z nich je roven jedné. Najděte: hodnotu parametru d a všechny kořeny tohoto polynomu.

Prostudujte následující text.

4 Diskriminant

4.1 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.

4.2 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.*

4.3 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

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

4.4 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 tak je determinant známý jako *Vandermondův determinant*

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

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 dvojčlenem $x_3 - x_1$ 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.:

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