

# Algebra – osnova předmětu

## Elementární úvod

### Kořeny polynomů nad $\mathbb{C}$

$\mathbb{C}[x]$ : Tzv. základní věta algebry a její důsledky.

Násobný kořen. *Derivace polynomu, souvislost derivace a násobnosti kořenů, eliminace násobnosti kořenů.*

*Hranice rozložení kořenů polynomů – věta o mezikružích.*

Hornerovo schéma. Lagrangeova interpolační formule.

### Elementární úvod ke Galoisově teorii

*Elementární úvod ke Galoisově teorii – řešení kvadratické a kubické rovnice Lagrangeovým postupem postupné symetrizace. Aplikace symetrických polynomů, faktorizace  $S_n$  a svazu jejích podgrup; význam cyklických grup. Normální řady, řešitelné grupy.*

## Polynomy

### Definice polynomu

Definice polynomu: algebraická, pomocí algebry cest, polynomiální funkce. Porovnání těchto definic v případě konečných a nekonečných polí.

### Vlastnosti polynomů

Algebraická uzavřenost pole  $F$ ,  $\mathbb{Z}_p$  není algebraicky uzavřené.

Polynomy nad polem a nad okruhem, ilustrace na počtech kořenů kvadratických rovnic nad  $\mathbb{Z}_n$ .

Nenulový polynom má nejvýše  $n$  různých kořenů

Analogie základní věty aritmetiky pro polynomy, důsledky, rozklad polynomu nad algebraicky uzavřeným polem.

$D$  je oborem integrity  $\Leftrightarrow D[x]$  je oborem integrity. Jednotky v oboru integrity  $D[x]$ . Pole racionálních lomených funkcí  $F(x)$  jako podílové pole oboru integrity  $F[x]$ .

### 4 Kongruence

Kongruentní polynomy (modulo  $I$  a modulo  $q$ ), kongruenční třídy, faktorový okruh  $F[x]/\langle q \rangle$  a jeho vlastnosti v případě  $q$  reducibilního/ireducibilního.

Kroneckerova věta, algebraické rozšíření pole, rozkladové pole, příklady.

Struktura konečných polí.

### 7 Symetrické polynomy

Symetrické polynomy, lexikografické uspořádání. Jednoduché symetrické polynomy, vedoucí člen.

Elementární symetrické polynomy  $E_k$ , hlavní věta o symetrických polynomech.

Vztah mezi  $E_k$  a  $S_k$ , Newtonův vzorec.

Diskriminant – obecná definice a jeho vyjádření pomocí determinantu, diskriminant redukované kubické rovnice.

## VIII. Grupy

Jednoduché abelovské grupy jsou cyklické grupy prvočíselného řádu.

$A_5$  je jednoduchá (s důk.).  $A_n$  jsou pro  $n \geq 5$  jednoduché (stačí bez důk.).

Cyklické grupy: každá cyklická grupa je komutativní, abelovské grupy lze psát jako direktní součin cyklických grup řádu rovnému mocninám prvočísel.

Počet (normálních) podgrup konečné cyklické grupy řádu  $n$ .

Podmínka, kdy  $G$  nemá vlastní podgrupy.

Jednoduché grupy, popis všech jednoduchých grup. Grupy prvočíselného řádu jsou cyklické.

Hölderův program, klasifikace konečných grup.

Věta Cauchyova a věty Sylowovy. (bez důkazu)

## IX. Okruhy a pole

Rozšíření pole  $F$ , stupeň rozšíření. Rozkladové pole polynomu.

Řešitelnost algebraické rovnice v radikálech, Abelova-Ruffiniova věta, základní věta Galoisovy teorie.

Eukleidovské konstrukce, konstruovatelné body a čísla.