# Okruhy polynomů

## Algebra 2

Mgr. Markéta Trnečková, Ph.D.

Palacký University, Olomouc

# Polynomy

- **Polynom s neurčitou** $x$ a s koeficienty z okruhu $R$. Množinu všech polynomů značíme $R[x]$.
  Např. okruh koeficientů je $\mathbb{Z}$. Množina polynomů $\mathbb{Z}[x]$. Konkrétní polynom $1x$ (nebo také jen $x$).
- $x$ nejsou prvky z okruhu $R$, nebudeme tedy psát $x = 1$
- Polynomy můžeme sčítat i násobit
- **Stupeň polynomu** – nejvyšší exponent neurčité $x$ s nenulovým koeficientem
- Množina $R[x]$ polynomů s koeficienty z $R$ tvoří spolu se sčítáním a násobením okruh
- $R$ je podokruh $R[x]$
- S polynomy budeme pracovat jinak než jak znáte ze střední školy.
- Nebudeme psát $2x - 4 = 0$, protože $2x - 4$ není nulový polynom.
- Místo řešení polynomické rovnice budeme hledat kořeny polynomu (nuly polynomu)

# Polynomy

## Definice

*Nechť $R$ je okruh.* **Polynom $f(x)$ s neurčitou $x$** *je nekonečná řada $\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots$, kde $a_i \in R$ a $a_i = 0$ pro téměř všechny hodnoty $i$. $a_i$ nazýváme* **koeficienty** *$f(x)$.*
*Pokud pro nějaké $i > 0$ platí, že $a_i = 0$, tak největší taková hodnota $i$ je* **stupeň** *$f(x)$.*
*Pokud jsou všechna $a_i = 0$, stupeň $f(x)$ je nedefinovaný.*

Pokud v $f(x)$ platí $a_i = 0$ pro $i > n$, pak $f(x)$ píšeme $a_0 + a_1 x + \dots + a_n x^n$. Také vynecháváme všechny termy, pro které je $a_i$ rovno $0$.

Pokud $R$ má jedničku $(1 \neq 0)$ zapisujeme $1x^k$ jako $x^k$.

Prvky $R$ se nazývají **konstantní polynomy**.

# Polynomy

## Definice

*Nechť* $R$ *je okruh.* $f(x) = a_0 + a_1x + \cdots + a_nx^n + \ldots$ *a* $g(x) = b_0 + b_1x + \cdots + b_nx^n + \ldots$ *jsou polynomy z* $R[x]$.

*Pak* **součet polynomů** *definujeme*

$f(x) + g(x) = c_0 + c_1x + \cdots + c_nx^n + \ldots$, *kde* $c_i = a_i + b_i$.

**Násobení polynomů** *definujeme*

$f(x)g(x) = d_0 + d_1x + \cdots + d_nx^n + \ldots$, *kde* $d_n = \sum_{j=0}^{n} a_j b_{n-j}$.

$\sum_{j=0}^{n} a_j b_{n-j}$ nemusí být rovno $\sum_{j=0}^{n} b_j a_{n-j}$, pokud $R$ není komutativní.

# Polynomy

**Věta 54**

*Množina $R[x]$ všech polynomů s neurčitou $x$ a s koeficienty v $R$ tvoří spolu s operacemi sčítání a násobení (z předchozí definice) okruh.*
*Pokud je $R$ komutativní, pak $R[x]$ je také komutativní.*
*Pokud má $R$ jedničku $1 \neq 0$, pak $1$ je také jednička pro $R[x]$.*

**Důkaz**

*Snadný. Jak bychom při důkazu postupovali?*

$\mathbb{Z}[x]$ je okruh polynomů s celočíselnými koeficienty.

$\mathbb{Q}[x]$ je okruh polynomů s racionálními koeficienty.

# Polynomy

## Příklad 100

*Vypočítejte součet a součin polynomů z* $\mathbb{Z}_2[x]$.
$f(x) = (x+1)$ *a* $g(x) = (x+1)$.

# Polynomy

**Příklad**

*Vypočítejte součet a součin polynomů z* $\mathbb{Z}_2[x]$.
$f(x) = (x+1)$ *a* $g(x) = (x+1)$.

- $(x+1) + (x+1) = (1+1)x + (1+1) = 0x + 0 = 0$
- $(x+1)(x+1) = x^2 + (1+1)x + 1 = x^2 + 1$

# Polynomy s více neurčitými

## Definice

*Nechť $R$ je okruh a $x$ a $y$ jsou dvě neurčité, můžeme vytvořit okruh $(R[x])[y]$, tj. okruh polynomů neurčité $y$ s koeficienty z okruhu polynomů neurčité $x$ s koeficienty z $R$.*

*Bez důkazu si uveďme, že $(R[x])[y] \simeq (R[y])[x]$.*

**Okruh polynomů dvou neurčitých $x$ a $y$ s koeficienty z $R$** *značíme $R[x, y]$.*

**Okruh polynomů $n$ neurčitých $x_i$ s koeficienty z $R$** *značíme $R[x_1, x_2, \ldots, x_n]$.*

# Polynomy s více neurčitými

- Pokud je $D$ obor integrity, pak $D[x]$ je také obor integrity.
- Pokud je $F$ těleso, $F[x]$ je obor integrity (ale ne těleso), protože $x$ není jednotka v $F[x]$.
  Neexistuje polynom $f(x) \in F[x]$ takový, že $xf(x) = 1$
- Můžeme však zkonstruovat podílové těleso $F(x)$ oboru integrity $F[x]$ (viz minulá přednáška).
- Každý prvek $F(x)$ může být reprezentován jako $\frac{f(x)}{g(x)}$ takový, že $g(x) \neq 0$.
- Analogicky definujeme $F(x_1, \ldots, x_n)$ jako podílové těleso $F[x_1, \ldots, x_n]$.

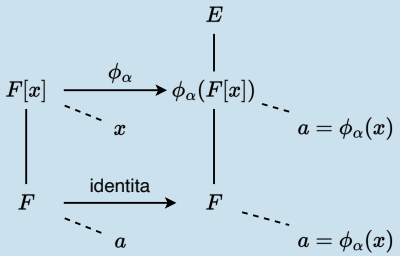
# Homomorfismus vyhodnocení

## Věta 55 (Homomorfismus vyhodnocení)

*Nechť $E$ a $F$ jsou tělesa taková, že $F \leq E$, $\alpha \in E$ a $x$ je neurčitá.*
*Zobrazení $\phi_\alpha : F[x] \to E$ definované předpisem*
$\phi_\alpha(a_0 + a_1x + \dots a_nx^n) = a_0 + a_1\alpha + \dots a_n\alpha^n$
*pro $(a_0 + a_1x + \dots a_nx^n) \in F[x]$ je homomorfismus $F[x] \to E$.*

## Důkaz

*Pokud* $f(x) = a_0 + a_1x + \dots + a_nx^n$,
$g(x) = b_0 + b_1x + \dots + b_mx^m$,
$h(x) = f(x) + g(x) = c_0 + c_1x + \dots + c_rx^r$
*Tak pro sčítání:*
$\phi_\alpha(f(x)+g(x)) = \phi_\alpha(h(x)) = c_0 + c_1\alpha + \dots c_r\alpha^r$,
$\phi_\alpha(f(x)) + \phi_\alpha(g(x)) =$
$(a_0 + a_1\alpha + \dots a_r\alpha^r) + (b_0 + b_1\alpha + \dots b_m\alpha^m)$
*Z definice sčítání polynomů je zřejmé, že*
$\phi_\alpha(f(x) + g(x)) = \phi_\alpha(f(x)) + \phi_\alpha(g(x))$.




*Čárkované čáry jsou prvky množiny.*

# Homomorfismus vyhodnocení

## Důkaz (Pokračování)

*Násobení:*

$f(x)g(x) = d_0 + d_1x + \cdots + d_sx^s$, *kde* $d_i = \sum_{j=0}^{i} a_j b_{i-j}$.

$\phi_\alpha(f(x)g(x)) = \phi_\alpha(h(x)) = d_0 + d_1\alpha + \ldots d_s\alpha^s$

$[\phi_\alpha(f(x))][\phi_\alpha(g(x))] = (a_0 + a_1\alpha + \ldots a_n\alpha^n)(b_0 + b_1\alpha + \ldots b_m\alpha^m)$

*Protože* $d_i = \sum_{j=0}^{i} a_j b_{i-j}$ *tak vidíme, že*

$\phi_\alpha(f(x)g(x)) = [\phi_\alpha(f(x))][\phi_\alpha(g(x))]$.

*Takže* $\phi_\alpha$ *je homomorfismus.*

## Příklad 101

*Nechť* $F$ *z předchozí věty je* $\mathbb{Q}$ *a* $E$ *je* $\mathbb{R}$. *Jak budou vypadat homomorfismy* $\phi_0 : \mathbb{Q}[x] \to \mathbb{R}$ *a* $\phi_2 : \mathbb{Q}[x] \to \mathbb{R}$*?*

# Homomorfismus vyhodnocení

## Příklad

*Nechť $F$ z předchozí věty je $\mathbb{Q}$ a $E$ je $\mathbb{R}$. Jak budou vypadat homomorfismy $\phi_0 : \mathbb{Q}[x] \to \mathbb{R}$ a $\phi_2 : \mathbb{Q}[x] \to \mathbb{R}$?*

- $\phi_0$
- $\phi_0(a_0 + \cdots + a_n x^n) = a_0 + a_1 0 + \cdots + a_n 0^n = a_0$
- Každý polynom je zobrazen na svůj konstantní člen

- $\phi_2$
- $\phi_2(a_0 + \cdots + a_n x^n) = a_2 + a_1 2 + \cdots + a_n 2^n$
- Např. $\phi_2(x^2 + x - 6) = 2^2 + 2 - 6 = 0$
  $x^2 + x - 6$ je v $Ker(\phi_2)$
- $x^2 + x - 6 = (x - 2)(x + 3)$
- Díky tomu, že $\phi_2(x - 2) = 2 - 2 = 0$ je $\phi_2(x^2 + x - 6) = 0$

# Homomorfismus vyhodnocení

**Příklad 102**

*Nechť $F$ z předchozí věty je $\mathbb{Q}$ a $E$ je $\mathbb{C}$. Jak bude vypadat homomorfismus $\phi_i : \mathbb{Q}[x] \to \mathbb{C}$?*

# Homomorfismus vyhodnocení

## Příklad

*Nechť $F$ z předchozí věty je $\mathbb{Q}$ a $E$ je $\mathbb{C}$. Jak bude vypadat homomorfismus $\phi_i : \mathbb{Q}[x] \to \mathbb{C}$?*

- $\phi_i(a_0 + \cdots + a_n x^n) = a_0 + a_1 i + \cdots + a_n i^n$
- $\phi_i(x) = i$
- $\phi_i(x^2 + 1) = i^2 + 1 = 0$
  $x^2 + 1$ je v $Ker(\phi_i)$

## Příklad 103

*Nechť $F$ je $\mathbb{Q}$ a $E$ je $\mathbb{R}$. Uvažujme homomorfismus $\phi_\pi : \mathbb{Q}[x] \to \mathbb{R}$?*
*Dá se dokázat, že $a_0 + a_1\pi + \cdots + a_n\pi^n = 0$ právě, když je $a_i = 0$ pro $i = 1, \ldots, n$.*
*$Ker(\phi_\pi) = \{0\}$ a $\phi_\pi$ je injektivní.*
*Všechny polynomy s neurčitou $\pi$ s racionálními koeficienty tvoří okruh isomorfní s $\mathbb{Q}$ přirozeným způsobem s $\phi_\pi(x) = \pi$.*

# Homomorfismus vyhodnocení

## Definice

*Nechť $F$ a $E$ jsou tělesa, $F \leq E$, $\alpha \in E$. $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$.*
*Homomorfismus vyhodnocení z předchozí věty $\phi_\alpha$. Označme $f(\alpha)$ hodnotu $\phi_\alpha(f(x)) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$.*
*Pokud $f(\alpha) = 0$, nazýváme $\alpha$* **kořenem** *polynomu $f(x)$.*

Problém hledání kořene polynomu $f(x)$ – nalezení všech $\alpha$, které splňují $\phi_\alpha(f(x)) = 0$

## Příklad 104

*Porovnejte zadání:*

1. *Vyřešte rovnici $r^2 + r - 6 = 0$.*
2. *Najděte kořeny polynomu $x^2 + x - 6$.*

# Homomorfismus vyhodnocení

**Příklad**

*Porovnejte zadání:*

1. *Vyřešte rovnici* $r^2 + r - 6 = 0$.
2. *Najděte kořeny polynomu* $x^2 + x - 6$.

1. $\{r \in \mathbb{R} | r^2 + r - 6 = 0\} = \{2, -3\}$
2. $\{\alpha \in \mathbb{R} | \phi_\alpha(x^2 + x - 6) = 0\} = \{2, -3\}$

# Homomorfismus vyhodnocení

**Věta 56**

*Polynom $x^2 - 2$ nemá kořeny v $\mathbb{Q}$. $\sqrt{2} \notin \mathbb{Q}$.*

**Proč je toto zajímavé zjištění?**
Podívejte se do skript.

**Důkaz**

*Předpokládejme, že pro $\frac{m}{n} \in \mathbb{Q}$ $(m, n \in \mathbb{Z})$. Platí $(\frac{m}{n})^2 = 2$ a že $gcd(m, n) = 1$.*
*Pak musí platit $m^2 = 2n^2$, kde $m, n \in \mathbb{Z}$.*
*Protože $2$ dělí $2n^2$, tak musí dělit $m^2$, takže musí dělit i $m$ a $2^2 = 4$ musí dělit $m^2$.*
*To ale znamená, že $n^2$ je dělitelné $2$. Jelikož je to druhá mocnina, pak $n$ musí být také dělitelné $2$.*
*Odtud ale máme, že $m$ i $n$ jsou dělitelné $2$ a tudíž $gcd(m, n)$ není $1$.*

# Faktorizace polynomů

## Věta 57

*Nechť* $f(x) = a_0 + a_1x + \cdots + a_nx^n$ *a* $g(x) = b_0 + b_1x + \cdots + b_mx^m$ *jsou dva prvky* $F[x]$*, kde* $a_n \neq 0$*,* $b_m \neq 0$ *a* $m > 0$*.*
*Pak existují unikátní polynomy* $q(x)$ *a* $r(x)$ *v* $F[x]$ *takové, že* $f(x) = g(x)q(x) + r(x)$*, kde buďto* $r(x) = 0$ *nebo* $r(x)$ *má menší stupeň než* $m$ *(tedy než je stupeň polynomu* $g(x)$*).*

Porovnejte tuto větu s větou o celočíselném dělení.

## Důkaz

*Uvažujme množinu* $S = \{f(x) - g(x)s(x) | s(x) \in F[x]\}$*.*
*Pokud* $0 \in S$*, pak existuje* $s(x)$ *takové, že* $f(x) - g(x)s(x) = 0$*, takže* $f(x) = g(x)s(x)$ *V takovém případě stačí vzít* $q(x) = s(x)$ *a* $r(x) = 0$*.*
*Jinak* $r(x)$ *je prvek minimálního stupně v* $S$*, pak* $f(x) = g(x)q(x) + r(x)$ *pro nějaké* $q(x) \in F[x]$*. Musíme ukázat, že* $r(x)$ *je stupně menšího než* $m$*.*

*Předpokládejme, že* $r(x) = c_0 + c_1x + \cdots + c_tx^t$ *takové, že* $c_t \neq 0$ *,* $c_i \in F$

# Faktorizace polynomů

## Důkaz (Pokračování)

*Předpokládejme, že* $r(x) = c_0 + c_1x + \cdots + c_tx^t$ *takové, že* $c_t \neq 0$ , $c_i \in F$
*Pokud* $t \geq m$, *pak*
$f(x) - q(x)g(x) - (c_t/b_m)x^{t-m}g(x) = r(x) - (c_t/b_m)x^{t-m}g(x)$
*a to je ve tvaru*
$r(x) - (c_tx^t +$ *termy nižšího stupně*$)$.
*To je polynom stupně nižšího než* $t$ *(stupně polynomu* $r(x)$*).*
*Ovšem polynom* $f(x) - q(x)g(x) - (c_t/b_m)x^{t-m}g(x)$ *můžeme zapsat*
$f(x) - g(x)[q(x) - (c_t/b_m)x^{t-m}]$, *takže je v* $S$, *což je v rozporu s faktem, že* $r(x)$ *bylo vybráno tak, aby mělo minimální stupeň v* $S$.

*Unikátnost: pokud*
$f(x) = g(x)q_1(x) + r_1(x)$ *a* $f(x) = g(x)q_2(x) + r_2(x)$ *tak odečtením dostaneme*
$g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x)$
*Buďto je* $r_2(x) - r_1(x) = 0$ *nebo je stupeň* $r_2(x) - r_1(x)$ *menší než stupeň* $g(x)$. *To může platit pouze pokud* $q_1(x) - q_2(x) = 0$, *takže* $q_1(x) = q_2(x)$. *Také tedy musí platit, že* $r_2(x) - r_1(x) = 0$ *tedy* $r_1(x) = r_2(x)$.

# Faktorizace polynomů

**Příklad 105**

*Nechť* $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ *a* $g(x) = x^2 - 2x + 3$ *jsou polynomy v* $\mathbb{Z}_5[x]$. *Najděte polynomy* $q(x)$ *a* $r(x)$ *tak, aby* $f(x) = q(x)g(x) + r(x)$. ($r(x)$ *má menší stupeň než* 2).

# Faktorizace polynomů

## Příklad

*Nechť* $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$ *a* $g(x) = x^2 - 2x + 3$ *jsou polynomy v* $\mathbb{Z}_5[x]$. *Najděte polynomy* $q(x)$ *a* $r(x)$ *tak, aby* $f(x) = q(x)g(x) + r(x)$. *(*$r(x)$ *má menší stupeň než* $2$*).*

- Vydělíme polynom $f(x)$ polynomem $g(x)$ znáte ze střední školy
- $(x^4 - 3x^3 + 2x^2 + 4x - 1) : (x^2 - 2x + 3) = x^2 + \dots$
  $x^2(x^2 - 2x + 3) = x^4 - 2x^3 + 3x^2$
  $(x^4 - 3x^3 + 2x^2 + 4x - 1) - (x^4 - 2x^3 + 3x^2) = (-x^3 - x^2 + 4x - 1)$
- $(-x^3 - x^2 + 4x - 1) : (x^2 - 2x + 3) = -x + \dots$
  $-x(x^2 - 2x + 3) = -x^3 + 2x^2 - 3x$
  $(-x^3 - x^2 + 4x - 1) - (-x^3 + 2x^2 - 3x) = (-3x^2 + 7x - 1)$ Pozor jsme v $\mathbb{Z}_5$
  $= (-3x^2 + 2x - 1)$
- $(-3x^2 + 2x - 1) : (x^2 - 2x + 3) = -3 + \dots$
  $-3(x^2 - 2x + 3) = -3x^2 - 6x - 9 = -3x^2 + x - 4$
  $(-3x^2 + 2x - 1) - (-3x^2 + x - 4) = x + 3$ Toto už je polynom nižšího stupně než $2$
- Řešení: $q(x) = x^2 - x - 3$, $r(x) = x + 3$

# Kořen polynomu

## Důsledek 17

*Prvek $a \in F$ je kořen $f(x) \in F[x]$, právě když $x - a$ je dělitel $f(x)$ v $F[x]$.*

## Důkaz

*Předpokládejme, že pro $a \in F$ máme $f(a) = 0$. Dle věty 57 existuji $q(x)$ a $r(x)$ takové, že $f(x) = (x - a)q(x) + r(x)$ $r(x)$ je stupně nižšího než $1$, tedy je to nějaká konstanta $c$*
*Aplikací homomorfismu vyhodnocení $\phi_a$ dostaneme*
$0 = f(a) = 0q(a) + c$
*Tedy $c$ musí být rovno $0$ a $f(x) = (x - a)q(x)$, což ale znamená, že $(x - a)$ je dělitel $f(x)$.*

*Naopak, pokud $(x - a)$ je faktor $f(x)$ v $F[x]$, kde $a \in F$, pak aplikací $\phi_a$ na $f(x) = (x - a)q(x)$ dostaneme $f(a) = 0q(a) = 0$.*

# Kořen polynomu

**Příklad 106**

*Nechť $f(x) = x^4 + 3x^3 + 2x + 4$ je polynom v $\mathbb{Z}_5[x]$. Určete, zda je $1$ kořen polynomu.*

Využijte předchozí důsledek.

# Kořen polynomu

**Příklad**

*Nechť $f(x) = x^4 + 3x^3 + 2x + 4$ je polynom v $\mathbb{Z}_5[x]$. Určete, zda je $1$ kořen polynomu.*

- Dle předchozího důsledku bychom měli být schopni vyjádřit $f(x) = (x-1)q(x)$.
- $(x^4 + 3x^3 + 2x + 4) : (x-1) = x^3 + 4x^2 + 4x + 1$
- Ano, $1$ je kořenem. $f(x) = (x-1)(x^3 + 4x^2 + 4x + 1)$

- I polynom $x^3 + 4x^2 + 4x + 1$ má kořen $1$
  $(x^3 + 4x^2 + 4x + 1) : (x-1) = x^2 + 4$
  $(x^3 + 4x^2 + 4x + 1) = (x-1)(x^2 + 4)$
- Polynom $x^2 + 4$ má také kořen $1$
  $(x^2 + 4) : (x-1) = x + 1$
- $\underline{f(x) = (x-1)^3(x+1)}$

# Kořen polynomu

## Důsledek 18

*Nenulový polynom $f(x) \in F[x]$ stupně $n$ může mít nejvýše $n$ kořenů v $F$.*

## Důkaz

*Z důsledku 17 víme, že pokud $a_1 \in F$ je kořen polynomu $f(x)$, pak $f(x) = (x - a_1)q_1(x)$, kde zjevně je stupeň $q(x)$ $n - 1$.*
*Dále pokud $a_2$ je kořen $q_1(x)$ pak $f(x) = (x - a_1)(x - a_2)q_2(x)$, kde $q_2(x)$ má stupeň $n - 2$ ...*
*$f(x) = (x - a_1)(x - a_2) \dots (x - a_r)q_r(x)$, kde $q_r(x)$ nemá další kořeny.*
*Protože stupeň $f(x)$ je $n$, nejvýše $n$ faktorů $(x - a_i)$ se může vyskytovat na pravé straně, takže $r \leq n$.*
*Pokud $b \neq a_i$ pro $i = 1, \dots, r$ a $b \in F$, tak*
*$f(b) = (b - a_1) \dots (b - a_r)q_r(b) \neq 0$, protože $F$ nemá dělitele nuly a žádný z $b - a_i$ ani $q_r(b)$ není nula.*
*Takže $a_i$, pro $i = 1, \dots r \leq n$ jsou všechny kořeny polynomu $f(x) \in F[x]$.*

# Kořen polynomu

## Důsledek 19

*Pokud $G$ je konečná podgrupa multiplikativní grupy $\langle F^*, \cdot \rangle$ komutativního tělesa $F$, pak $G$ je cyklická.*
*Multiplikativní grupa nenulových prvků konečného komutativního tělesa je konečná.*

## Důkaz

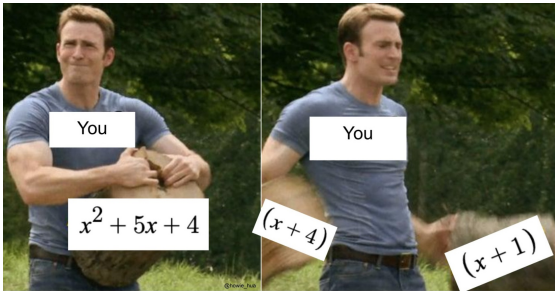
*$G$ je konečná abelovská grupa. Dle věty 26 (Základní věta konečně generovaných abelovských grup) je isomorfní s $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_r}$, kde každé $d_i$ je mocnina prvočísla.*
*Uvažujme každou $\mathbb{Z}_{d_i}$ jako cyklickou grupu řádu $d_i$ v multiplikativní notaci.*
*Nechť $m$ je nejmenší společný násobek všech $d_i$ pro $i = 1, \ldots, r$. $m \leq d_1 d_2 \ldots d_r$.*
*Pokud $a_i \in \mathbb{Z}_{d_i}$, tak $a_i^{d_i} = 1$, takže $a_i^m = 1$, protože $d_i$ dělí $m$.*
*Takže pro všechna $\alpha \in G$ máme $\alpha^m = 1$, takže každý prvek $G$ je kořen $(x^m - 1)$.*
*Ale $G$ má $d_1 d_2 \ldots d_r$ prvků, zatímco $(x^m - 1)$ může mít nejvýše $m$ kořenů v $G$ (dle předchozího důsledku). Takže $m \geq d_1 d_2 \ldots d_r$.*
*Dostáváme tedy, že $m = d_1 d_2 \ldots d_r$ a tedy prvočísla $d_1, d_2, \ldots, d_r$ jsou různé a $G$ je isomorfní s cyklickou grupou $\mathbb{Z}_m$.*

# Nedělitelné polynomy

## Definice

*Nekonstantní polynom $f(x) \in F[x]$ je* **nedělitelný nad** $F$ *(též* **ireducibilní nad** $F$*),*
*pokud nemůže být vyjádřen jako součin $g(x)h(x)$ dvou polynomů $g(x)$ a $h(x)$ v $F[x]$*
*tak, aby oba měly nižší stupeň než $f(x)$.*
*Jinak je* **dělitelný nad** $F$ *(též* **reducibilní nad** $F$*).*

Polynom může být ireducibilní nad tělesem $F$, ale nad jiným tělesem (které obsahuje $F$) může být dělitelný.



# Nedělitelné polynomy

**Příklad 107**

*Ukázali jsme, že $x^2 - 2$ v $\mathbb{Q}[x]$ nemá žádné kořeny v $\mathbb{Q}$, takže je nedělitelný nad $\mathbb{Q}$. Je dělitelný nad $\mathbb{R}$ ($x^2 - 2 \in \mathbb{R}[x]$)?*

# Nedělitelné polynomy

**Příklad**

*Ukázali jsme, že $x^2 - 2$ v $\mathbb{Q}[x]$ nemá žádné kořeny v $\mathbb{Q}$, takže je nedělitelný nad $\mathbb{Q}$. Je dělitelný nad $\mathbb{R}$ ($x^2 - 2 \in \mathbb{R}[x]$)?*

- Ano
  $(x^2 - 2) = (x - \sqrt{2})(x + \sqrt{2})$

**Příklad 108**

*Jak vypadají jednotky v $F[x]$?*

# Nedělitelné polynomy

**Příklad**

*Jak vypadají jednotky v $F[x]$?*

- **Jednotka** = prvek, který má multiplikativní inverzi
- Jednotky v $F[x]$ jsou právě všechny nenulové prvky $F$
- Polynom, který je nedělitelný nad $F$ můžeme tedy také definovat jak nekonstantní polynom $f(x) \in F[x]$ takový, že pro jakoukoli faktorizaci $f(x) = g(x)h(x)$ v $F[x]$ platí, že $g(x)$ nebo $h(x)$ je jednotka

**Příklad 109**

*Ukažte, že $f(x) = x^3 + 3x + 2$ v $\mathbb{Z}_5[x]$ je nedělitelný nad $\mathbb{Z}_5$.*

# Nedělitelné polynomy

**Příklad**

*Ukažte, že $f(x) = x^3 + 3x + 2$ v $\mathbb{Z}_5[x]$ je nedělitelný nad $\mathbb{Z}_5$.*

- Pokud by byl faktorizován v $\mathbb{Z}_5[x]$ na polynomy nižšího stupně, existoval by lineární faktor ve tvaru $x - a$ pro nějaké $a \in \mathbb{Z}_5$.
- Pak by $f(a) = 0$ dle důsledku 17
  $f(0) = 2,\ f(1) = 1,\ f(2) = 1,\ f(3) = f(-2) = -2 = 3,\ f(4) = f(-1) = -2 = 3$
- Což ukazuje, že f(x) nemá kořen v $\mathbb{Z}_5$, je tedy nedělitelná nad $\mathbb{Z}_5$
- Takto se dá testovat prakticky jen kvadratické a kubické polynomy nad konečnými tělesy s malým počtem prvků.

# Nedělitelné polynomy

**Věta 58**

*Nechť $f(x) \in F[x]$ je polynom stupně 2 nebo 3.*
*Pak je $f(x)$ dělitelný nad $F$, právě když má kořen v $F$.*

**Důkaz**

*Pokud $f(x)$ je dělitelný nad $F$, tak $f(x) = g(x)h(x)$, kde stupně $g(x)$ a $h(x)$ jsou oba stupně menší než $f(x)$.*
*Protože $f(x)$ je kvadratický, nebo kubický polynom, tak $g(x)$ nebo $h(x)$ musí být stupně $1$.*
*Řekněme, že je to $g(x)$ a ten je tedy ve tvaru $(x - a)$.*
*Pak $g(a) = 0$, což nám dává, že $f(a) = 0$, takže $f(x)$ má kořen v $F$.*
*Opačný směr vyplývá z důsledku 17.*

# Nedělitelné polynomy

## Věta 59

*Pokud $f(x) \in \mathbb{Z}[x]$, tak se $f(x)$ dá rozložit na polynomy nižších stupňů $r(x)$ a $s(x)$ v $\mathbb{Q}[x]$, právě když má takovou faktorizaci s polynomy stejných stupňů $r(x)$ a $s(x)$ v $\mathbb{Z}[x]$.*

## Důkaz

*Vynechán.*

## Důsledek 20

*Pokud $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ je v $\mathbb{Z}[x]$, $a_0 \neq 0$ a $f(x)$ má kořen v $\mathbb{Q}$, tak má kořen $m$ v $\mathbb{Z}$ a $m$ musí dělit $a_0$.*

## Důkaz

*Pokud $f(x)$ má kořen $a$ v $\mathbb{Q}$, pak $f(x)$ má lineární faktor $x - a$ v $\mathbb{Q}[x]$. Dle věty 58, $f(x)$ má faktorizaci s lineárním faktorem v $\mathbb{Z}[x]$, takže pro nějaké $m \in \mathbb{Z}$ musí platit $f(x) = (x - m)(x^{n-1} + \cdots + a_0/m)$. Takže $a_0/m$ je v $\mathbb{Z}$, takže $m$ dělí $a_0$.*

# Nedělitelné polynomy

## Příklad 110

*Předchozí důsledek nám dává další důkaz nedělitelnosti* $x^2 - 2$ *nad* $\mathbb{Q}$.
*Protože* $x^2 - 2$ *se netriviálně faktorizuje v* $\mathbb{Q}[x]$, *právě když má kořen v* $\mathbb{Q}$. *(věta 58)*
$x^2 - 2$ *má kořen v* $\mathbb{Q}$, *právě když má kořen v* $\mathbb{Z}$. *(důsledek 20)*
*Navíc jediné možnosti jsou* $\pm 1$ *a* $\pm 2$ *(dělitelé* $2$*)*
*Snadno ověříme, že ani jedno není kořen* $x^2 - 2$.

## Příklad 111

*Ukažte, že* $f(x) = x^4 - 2x^2 + 8x + 1$ *je v* $\mathbb{Q}[x]$ *nedělitelný nad* $\mathbb{Q}$.

# Nedělitelné polynomy

## Příklad

*Ukažte, že $f(x) = x^4 - 2x^2 + 8x + 1$ je v $\mathbb{Q}[x]$ nedělitelný nad $\mathbb{Q}$.*

- Pokud $f(x)$ má lineární faktor v $\mathbb{Q}$, pak má kořen v $\mathbb{Z}$ a dle důsledku 20 tento kořen musí být dělitel $1$ v $\mathbb{Z}$
- Jediná taková čísla jsou $1$ a $-1$
  $f(1) = 8$, $f(-1) = -8$
- Pokud se $f(x)$ dá rozložit na dva kvadratické faktory v $\mathbb{Q}[x]$, pak dle věty 59 má faktorizaci $(x^2 + ax + b)(x^2 + cx + d)$ v $\mathbb{Z}[x]$
- Porovnáním koeficientů mocnin $x$ zjistíme, že
  $bd = 1$, $ad + bc = 8$, $ac + b + d = -2$, $a + c = 0$ pro celá čísla $a, b, c, d \in \mathbb{Z}$
- Z $bd = 1$ vidíme, že buď $b = d = 1$ nebo $b = d = -1$
- Jelikož se $b = d$, pak $ad + bc = d(a + c) = 8$
- Ale to je nemožné, protože $a + c = 0$
- Takže faktorizace je nemožná, polynom je nedělitelný nad $\mathbb{Q}$

# Nedělitelné polynomy

## Věta 60 (Eisensteinovo kritérium)

*Nechť $p$ je prvočíslo. Předpokládejme, že $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ je v $\mathbb{Z}[x]$ a $a_n \not\equiv 0 \pmod{p}$, ale $a_i \equiv 0 \pmod{p}$ pro všechna $i < n$ a $a_0 \not\equiv 0 \pmod{p^2}$. Pak $f(x)$ je nedělitelný nad $\mathbb{Q}$.*

## Důkaz

*Dle věty 59 jen potřebujeme ukázat, že $f(x)$ se nedá faktorizovat na polynomy nižšího stupně v $\mathbb{Z}[x]$. Pokud*

$f(x) = (b_r x^r + \cdots + b_0)(c_s x^s + \cdots + c_0)$

*je faktorizace v $\mathbb{Z}[x]$, kde $b_r \neq 0$, $c_s \neq 0$ a $r, s < n$, tak $a_0 \not\equiv 0 \pmod{p^2}$ implikuje, že $b_0$ a $c_0$ nejsou oba kongruentní s $0$ modulo $p$.*

*Předpokládejme, že $b_0 \not\equiv 0 \pmod{p}$ a $c_0 \equiv 0 \pmod{p}$. Dále $a_n \not\equiv 0 \pmod{p}$ implikuje, že $b_r, c_s \not\equiv 0 \pmod{p}$, protože $a_n = b_r c_s$.*

*Nechť $m$ je nejmenší hodnota $k$ taková, že $c_k \not\equiv 0 \pmod{p}$, pak*

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + \begin{cases} b_m c_0 \text{ pokud } r \geq m \\ b_r c_{m-r} \text{ pokud } r < m \end{cases}$$

## Důkaz (Pokračování)

$$a_m = b_0 c_m + b_1 c_{m-1} + \cdots + \begin{cases} b_m c_0 \text{ pokud } r \geq m \\ b_r c_{m-r} \text{ pokud } r < m \end{cases}$$

*Fakt, že $b_0$ ani $c_m$ nejsou kongruentní s $0$ modulo $p$ a $c_{m-1}, \ldots, c_0$ jsou všechny kongruentní s $0$ modulo $p$, implikuje, že $a_m \not\equiv 0 \pmod{p}$, takže $n = m$.*
*V důsledku toho platí $s = n$, což je v rozporu s předpokladem $s < n$ (že faktorizace je netriviální).*

## Příklad 112

*Rozhodněte, zda je $25x^5 - 9x^4 - 3x^2 - 12$ dělitelný nad $\mathbb{Q}$.*

# Nedělitelné polynomy

**Příklad**

*Rozhodněte, zda je* $25x^5 - 9x^4 - 3x^2 - 12$ *dělitelný nad* $\mathbb{Q}$.

- Dle předchozí věty
- Vezměme $p = 3$
- $25 \equiv 1 \pmod 3$ $a_n \not\equiv 0 \pmod p$
- $-9, -3 - 12 \equiv 0 \pmod 3$ $a_i \equiv 0 \pmod p$ pro všechna $i < n$
- $-12 \not\equiv 0 \pmod 9$ $a_0 \not\equiv 0 \pmod{p^2}$
- Polynom je nedělitelný nad $\mathbb{Q}$

# Nedělitelné polynomy

## Důsledek 21

*Nechť $p$ je prvočíslo. Polynom*
$\Phi_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$ *$p$-tý cyklotomický polynom*
*je nedělitelný nad $\mathbb{Q}$.*

## Důkaz

*Dle věty 59 potřebujeme uvažovat pouze faktorizace v $\mathbb{Z}[x]$. Použijeme homomorfismus vyhodnocení $\phi_{x+1}(f(x))$ jako $f(x+1)$ pro $f(x) \in \mathbb{Q}[x]$.*
*Nechť* $g(x) = \Phi_p(x+1) = \frac{(x+1)^p-1}{(x+1)-1} = \frac{x^p+\binom{p}{1}x^{p-1}+\cdots+px}{x}$
*Koeficient u $x^{p-r}$ pro $0 < r < p$ je binomický koeficient $\binom{p}{r} = \frac{p!}{r!(p-r)!}$, který je dělitelný $p$, protože $p$ dělí $p!$, když $0 < r < p$. Takže*
$g(x) = x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + p$
*splňuje Eisensteinovo kritérium (Věta 60) pro prvočíslo $p$ a tedy je nedělitelný nad $\mathbb{Q}$.*
*Ale kdyby $\Phi_p(x) = h(x)r(x)$ byla netriviální faktorizace $\Phi_p(x)$ v $\mathbb{Z}[x]$, tak*
$\Phi_p(x+1) = g(x) = h(x+1)r(x+1)$
*by dala netriviální faktorizaci $g(x)$ v $\mathbb{Z}[x]$. Takže $\Phi_p(x)$ musí být také nedělitelný nad $\mathbb{Q}$.*

# Unikátnost faktorizace v $F[x]$

**Definice**

*Pro $f(x), g(x) \in F[x]$ říkáme, že $g(x)$* **dělí** *$f(x)$* **v** *$F[x]$ pokud existuje $q(x) \in F[x]$ takový, že $f(x) = g(x)q(x)$.*

**Věta 61**

*Nechť $p(x)$ je nedělitelný polynom v $F[x]$.*
*Pokud $p(x)$ dělí $r(x)s(x) \in F[x]$, tak $p(x)$ dělí $r(x)$ nebo $p(x)$ dělí $s(x)$.*

Pokud $r$ a $s$ jsou nesoudělná a pokud $r$ dělí $sm$, pak $r$ dělí $m$.

# Unikátnost faktorizace v $F[x]$

**Důsledek 22**

*Pokud $p(x)$ je nedělitelný polynom v $F[x]$ a $p(x)$ dělí součin $r_1(x) \dots r_n(x)$ pro $r_i \in F[x]$, pak $p(x)$ dělí $r_i(x)$ pro alespoň jedno $i$.*

**Důkaz**

*Indukcí dokážeme z předchozí věty.*

# Unikátnost faktorizace v $F[x]$

## Věta 62

*Pokud je $F$ komutativní těleso, tak každý nekonstantní polynom $f(x) \in F[x]$ může být faktorizován v $F[x]$ na součin nedělitelných polynomů – ten je unikátní až na jejich pořadí a jednotkové faktory v $F$ (nenulové konstanty).*

## Důkaz

*Nechť $f(x) \in F[x]$ je nekonstantní polynom. Pokud je dělitelný nad $F$, pak $f(x) = g(x)h(x)$, kde $g(x)$ a $h(x)$ mají nižší stupně než $f(x)$.*
*Pokud $g(x)$ a $h(x)$ jsou nedělitelné, skončíme.*
*Jinak se alespoň jeden faktorizuje na polynomy nižších stupňů. Pokračováním tohoto procesu dojdeme k faktorizaci*
$f(x) = p_1(x)p_2(x)\dots p_r(x)$, *kde $p_i(x)$ jsou nedělitelné pro $i = 1, 2, \dots, r$.*
*Potřebujeme ukázat unikátnost. Předpokládejme*
$f(x) = p_1(x)p_2(x)\dots p_r(x) = q_1(x)q_2(x)\dots q_s(x)$
*jsou dvě faktorizace $f(x)$ do nedělitelných polynomů.*

# Unikátnost faktorizace v $F[x]$

## Důkaz (Pokračování)

$f(x) = p_1(x)p_2(x)\dots p_r(x) = q_1(x)q_2(x)\dots q_s(x)$
*jsou dvě faktorizace* $f(x)$ *do nedělitelných polynomů.*
*Dle důsledku 22* $p_1(x)$ *dělí nějaký* $q_j(x)$ *Bez újmy na obecnosti* $q_1(x)$
*Protože* $q_1(x)$ *je nedělitelný,* $q_1(x) = u_1p_1(x)$*, kde* $u_1 \neq 0$*, ale je v* $F$ *(je to jednotka)*
*Pak nahrazením* $u_1p_1(x)$ *za* $q_1(x)$ *a zkrácením dostaneme*
$p_2(x)\dots p_r(x) = u_1q_2(x)\dots q_s(x)$
*Podobně* $q_2(x) = u_2p_2(x)$*, takže*
$p_3(x)\dots p_r(x) = u_1u_2q_3(x)\dots q_s(x)$
*Pokračováním dostaneme*
$1 = u_1u_2\dots u_rq_{r+1}(x)\dots q_s(x)$
*Toto je možné pouze pro* $s = r$*, takže ta rovnice je vlastně* $1 = u_1u_2\dots u_r$
*Takže nedělitelné faktory* $p_i(x)$ *a* $q_j(x)$ *jsou tytéž, až na pořadí a jednotkové faktory.*