Homomorfismy okruhů

Algebra 2

Mgr. Markéta Trnečková, Ph.D.

Palacký University, Olomouc

Homomorfismus

Definice

Nechť $\phi : R \to R'$ *je homomorfismus okruhů.*
Podokruh
$\phi^{-1}[0'] = \{r \in R | \phi(r) = 0'\}$
je **jádro** *homomorfismu* ϕ*, označované* $Ker(\phi)$.

Homomorfismus

Věta 63

Nechť $\phi : R \to R'$ je homomorfismus okruhů, $H = Ker(\phi)$ a $a \in R$. Pak $\phi^{-1}[\{\phi(a)\}] = a + H = H + a$, kde $a + H = H + a$ je třída rozkladu $\langle R, + \rangle$ dle H obsahující a.

Podívejte se na větu 32.

Důsledek 23

Homomorfismus okruhů $\phi : R \to R'$ je injektivní, právě když $Ker(\phi) = \{0\}$.

Podívejte se na důsledek 7.

Faktorové okruhy

Věta 64

Nechť $\phi : R \to R'$ je homomorfismus okruhů, $Ker(\phi) = H$. Pak aditivní třídy H tvoří okruh R/H, jehož binární operace jsou definovány výběrem reprezentantů.
$(a + H) + (b + H) = (a + b) + H$,
$(a + H)(b + H) = (ab) + H$.
Dále, zobrazení $\mu : R/H \to \phi[R]$ definované jako $\mu(a + H) = \phi(a)$ je isomorfismus.

Podívejte se na větu 33.

Důkaz

Aditivní část je dokázána ve větě 33, musíme ověřit jen multiplikativní část.
Musíme ukázat, že součin tříd výběrem reprezentantů je dobře definovaný.
Nechť $h_1, h_2 \in H$ a uvažujme reprezentanty $a + h_1 \in a + H$ a $b + h_2 \in b + H$.
Nechť $c = (a + h_1)(a + h_2) = ab + ah_2 + h_1b + h_1h_2$.
Musíme ukázat, že c leží ve třídě $ab + H$. Protože $ab + H = \phi^{-1}[\{\phi(ab)\}]$, potřebujeme jen ukázat, že $\phi(c) = \phi(ab)$.

Faktorové okruhy

Důkaz (Pokračování)

Musíme ukázat, že c leží ve třídě $ab + H$. Protože $ab + H = \phi^{-1}[\{\phi(ab)\}]$, potřebujeme jen ukázat, že $\phi(c) = \phi(ab)$.
Protože ϕ je homomorfismus $\phi(h) = 0'$ pro $h \in H$, dostaneme:
$\phi(c) = \phi(ab + ah_2 + h_1b + h_1h_2) = \phi(ab) + \phi(ah_2) + \phi(h_1b) + \phi(h_1h_2) =$
$\phi(ab) + \phi(a)0' + 0'\phi(b) + 0'0' = \phi(ab) + 0' + 0' + 0' = \phi(ab)$
Takže součin je dobře definovaný.

Zbývá ukázat asociativita pro součin a distributivní zákony
Obojí plyne z vlastností počítání v R.

V grupách (Základní věta o homomorfismu) jsme dokázali, že μ je dobře definované, injektivní, surjektivní (je to zobrazení na $\phi[R]$) a splňuje aditivní podmínku homomorfismu.
Pro součin platí
$\mu[(a + H)(b + H)] = \mu(ab + H) = \phi(ab) = \phi(a)\phi(b) = \mu(a + H)\mu(b + H)$.
Jedná se tedy o isomorfismus.

Faktorové okruhy

Příklad 113

Zobrazení $\phi : \mathbb{Z} \to \mathbb{Z}_n$ definované $\phi(m) = r$, kde r je zbytek čísla m po dělení číslem n je homomorfismus.
Protože $Ker(\phi) = n\mathbb{Z}$, předchozí věta ukazuje, že $\mathbb{Z}/n\mathbb{Z}$ je okruh, kde operace na zbytkových třídách můžeme počítat výběrem reprezentantů.
Také ta věta říká že tento okruh $\mathbb{Z}/n\mathbb{Z}$ je isomorfní s $\mathbb{Z}_n$.

Faktorové okruhy

Věta 65

Nechť H je podokruh okruhu R.
Součin aditivních tříd rozkladu R podle H je dobře definovaný předpisem
$(a+H)(b+H) = ab+H$,
právě když $ah \in H$ a $hb \in H$ pro všechna $a, b \in R$ a $h \in H$.

Analogie věty 34

Důkaz

$\Leftarrow$ *Předpokládejme, že $ah \in H$ a $hb \in H$ pro všechna $a, b \in R$ a všechna $h \in H$.*
Nechť $h_1, h_2 \in H$, takže $a+h_1$ a $b+h_2$ jsou také reprezentanti tříd $a+H$ a $b+H$.
Pak $(a+h_1)(b+h_2) = ab+ah_2+h_1b+h_1h_2$.
Protože $ah_2, h_1b, h_1h_2 \in H$ dle předpokladu vidíme, že $(a+h_1)(b+h_2) \in ab+H$.

Důkaz (Pokračování)

$\Rightarrow$ *Předpokládejme, že součin tříd přes reprezentanty je dobře definovaný.*
Nechť $a \in R$ *a uvažujme součin tříd* $(a+H)H$.
Výběrem reprezentantů $a \in (a+H)$ *a* $0 \in H$ *vidíme, že*
$(a+H)H = a0 + H = 0 + H = H$.
Protože můžeme také spočítat $(a+H)H$ *výběrem* $a \in (a+H)$ *a libovolným* $h \in H$,
vidíme, že $ah \in H$ *pro libovolné* $h \in H$.
Podobně pomocí součinu $H(b+H)$ *můžeme ukázat, že* $hb \in H$ *pro libovolné* $h \in H$.

Tato věta říká, že podokruhy (pro které platí, že $aH \subseteq H$ a $Hb \subseteq H$) jsou analogií normálních podgrup v teorii grup. Ty jsme potřebovali pro vytváření faktorových grup s dobře definovanými operacemi nad reprezentanty.

Ideály

Definice

Aditivní podgrupa N okruhu R splňující
$aN \subseteq N$ *a* $Nb \subseteq N$ *pro všechna* $a, b \in R$
se nazývá **ideál**.

Příklad 114

Zjevně $n\mathbb{Z}$ *je ideál v okruhu* $\mathbb{Z}$*, protože víme, že je to podokruh a*
$s(mn) = (mn)s = n(ms)$
pro všechna $s \in \mathbb{Z}$.

Ideály

Příklad 115

Nechť F je okruh všech funkcí $f : \mathbb{R} \to \mathbb{R}$ a C je podokruh F sestávající se z konstantních funkcí.
Je C ideál v F? Proč?

Ideály

Příklad

Nechť F je okruh všech funkcí $f : \mathbb{R} \to \mathbb{R}$ a C je podokruh F sestávající se z konstantních funkcí.
Je C ideál v F? Proč?

- Není.
- Aby platilo $aC \subseteq C$, musel by součin libovolné funkce s konstantní funkcí být konstantní funkce
- Neplatí to například pro $c(x) = 1$, $f(x) = x$
  $cf(x) = x$

Ideály

Příklad 116

Nechť F je okruh všech funkcí $f : \mathbb{R} \to \mathbb{R}$ a N je podokruh F sestávající se z funkcí, pro které platí $f(2) = 0$.
Je N ideál v F? Proč?

Ideály

Příklad

Nechť F je okruh všech funkcí $f : \mathbb{R} \to \mathbb{R}$ a N je podokruh F sestávající se z funkcí, pro které platí $f(2) = 0$.
Je N ideál v F? Proč?

- Ano.
- Mějme $f(x) \in N$, $g(x) \in F$
- $fg(2) = f(2)g(2) = 0g(2) = 0$, takže $fg \in N$
- Podobně zjistíme, že i $gf \in N$
- Takže N je ideál F

Faktorový okruh

Důsledek 24

Nechť N je ideál okruhu R. Pak aditivní třídy rozkladu dle N tvoří okruh R/N s operacemi definovanými
$(a+N)+(b+N)=(a+b)+N$
$(a+N)(b+N)=(ab)+N$

Analogie důsledku 9.

Definice

Okruh R/N z předchozího důsledku se nazývá **faktorový okruh** *R dle N.*

Základní věta o homomorfismech

Věta 66

Nechť N je ideál okruhu R. Pak $\gamma : R \to R/N$ dané předpisem $\gamma(x) = x + N$ je homomorfismus okruhů s jádrem N.

Analogie věty 35.

Důkaz

Aditivní část je dokázána ve větě 35. Multiplikativní část:
$\gamma(xy) = (xy) + N = (x + N)(y + N) = \gamma(x)\gamma(y)$

Základní věta o homomorfismech

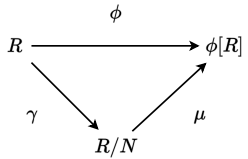
Věta 67

Nechť $\phi : R \to R'$ je homomorfismus okruhů s jádrem N.
Pak $\phi[R]$ je okruh a zobrazení $\mu : R/N \to \phi[R]$ dané předpisem $\mu(x + N) = \phi(x)$ je isomorfismus.
Pokud $\gamma : R \to R/N$ je homomorfismus daný $\mu(x) = x + N$, tak pro každé $x \in R$ platí $\phi(x) = \mu\gamma(x)$

Analogie základní věty o homomorfismech – věty 36.

Důkaz

Vyplývá z předchozích vět.



Základní věta o homomorfismech

Příklad 117

Ukázali jsme, že $n\mathbb{Z}$ je ideál okruhu $\mathbb{Z}$ (příklad 114).
Můžeme tedy zformovat faktorový okruh $\mathbb{Z}/n\mathbb{Z}$.

Ukázali jsme, že $\phi : \mathbb{Z} \to \mathbb{Z}_n$, kde $\phi(m)$ je zbytek po dělení čísla m číslem n, je homomorfismus. $Ker(\phi) = n\mathbb{Z}$.

Předchozí věta pak ukazuje, že zobrazení $\mu : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$, kde $\mu(m + n\mathbb{Z})$ je zbytek po dělení čísla m číslem n, je dobře definované zobrazení a je to isomorfismus.

Shrnutí:

- Každý homomorfismus okruhů s def. oborem R formuje faktorový okruh R/N.
- Každý faktorový okruh R/N vede k homomorfismu zobrazujícímu R do R/N.
- Ideál v teorii okruhů je analogický normální podgrupě v teorii grup.

Základní věta o homomorfismech

Věta 68 (Dodatek k větě 67)

Nechť $\phi : R \to R'$ je homomorfismus a nechť N je ideál R. Pak $\phi[N]$ je ideál $\phi[R]$, i když nemusí být ideálem R'.
Pokud N' je ideál $\phi[R]$ nebo R', pak $\phi^{-1}[N']$ je ideál R.

Základní věta o homomorfismech

Příklad 118

Okruh $\mathbb{Z}_p$ (p je prvočíslo), který je isomorfní s $\mathbb{Z}/p\mathbb{Z}$ je pole (komutativní těleso). Faktorový okruh oboru integrity může být pole.

Příklad 119

Okruh $\mathbb{Z} \times \mathbb{Z}$ není obor integrity. **Proč?**
Nechť $N = \{(0, n) | n \in \mathbb{Z}\}$. N je ideál okruhu $\mathbb{Z} \times \mathbb{Z}$ a $\mathbb{Z} \times \mathbb{Z}/N$ je isomorfní s $\mathbb{Z}$. **Jak by mohla vypadat bijekce?**
Takže faktorový okruh může být obor integrity, přestože původní nebyl.

Základní věta o homomorfismech

Příklad

Okruh $\mathbb{Z} \times \mathbb{Z}$ není obor integrity. **Proč?**
Nechť $N = \{(0, n) | n \in \mathbb{Z}\}$. N je ideál okruhu $\mathbb{Z} \times \mathbb{Z}$ a $\mathbb{Z} \times \mathbb{Z}/N$ je isomorfní s $\mathbb{Z}$. **Jak by mohla vypadat bijekce?**
Takže faktorový okruh může být obor integrity, přestože původní nebyl.

- **Proč?**
  Protože má dělitele nuly. Například $(0, 1)(1, 0)$
- **Jak by mohla vypadat bijekce?**
  $[(m, 0) + N] \to m$ pro $m \in \mathbb{Z}$

Základní věta o homomorfismech

Příklad 120

Podmnožina $N = \{0, 3\} \subseteq \mathbb{Z}_6$ *je zjevně ideál okruhu* $\mathbb{Z}_6$ *(***Je to zjevné?***) a* $\mathbb{Z}_6/N$ *má tři prvky:*
$0 + N$, $1 + N$, $2 + N$.
$\mathbb{Z}_6/N \simeq \mathbb{Z}_3$. *(***Jak vypadá bijekce?***).*
Vidíme, že R *nemusí být obor integrity a přesto* R/N *je pole.*

Příklad 121

$\mathbb{Z}$ *je obor integrity, ale* $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}_6$ *není.*

Ideály

Definice

Každý (nenulový) okruh R má alespoň dva ideály:
nevlastní ideál R,
triviální ideál $\{0\}$.

Tyto ideály formují nezajímavé faktorové okruhy – jednoprvkový R/R a $R/\{0\}$ isomorfní s R.

Faktorové okruhy

Věta 69

Pokud R je okruh s jedničkou a N je ideál okruhu R obsahující jednotku, tak $N = R$.

Důkaz

Nechť N je ideál okruhu R. Předpokládejme, že $u \in R$ implikuje, že pokud vezmeme $r = u^{-1}$ a $u \in N$, tak $1 = u^{-1}u \in N$.
Ale pak $rN \subseteq N$ pro všechna $r \in R$ implikuje, že $r1 = r \in N$ pro všechna $r \in R$, takže $N = R$.

Faktorové okruhy

Důsledek 25

Těleso nemá žádné vlastní netriviální ideály.

Důkaz

Protože každý prvek je jednotka, vyplývá to přímo z předchozí věty.

Nobody:

Fields:

Faktorové okruhy

Definice

Maximální ideál okruhu R *je ideál* $M \neq R$ *takový, že neexistuje žádný vlastní ideál* N*, takový, že* $M \subset N$*.*

Faktorové okruhy

Příklad 122

Nechť p je prvočíslo. Víme, že $\mathbb{Z}/p\mathbb{Z}$ je isomorfní s $\mathbb{Z}_p$.
$\mathbb{Z}_p$ a $\mathbb{Z}/p\mathbb{Z}$ jsou aditivní grupy.
$\mathbb{Z}_p$ je netriviální a nemá žádné netriviální normální podgrupy, $p\mathbb{Z}$ je maximální vlastní podgrupa $\mathbb{Z}$.
Protože je $\mathbb{Z}$ abelovská, každá podgrupa je normální. $p\mathbb{Z}$ je maximální normální podgrupa $\mathbb{Z}$.
Protože $p\mathbb{Z}$ je ideál okruhu $\mathbb{Z}$, vyplývá z toho, že $p\mathbb{Z}$ je maximální ideál okruhu $\mathbb{Z}$.
Víme, že $\mathbb{Z}/p\mathbb{Z}$ je isomorfní s okruhem $\mathbb{Z}_p$ a že je to pole.
Takže $\mathbb{Z}/p\mathbb{Z}$ je pole.

Faktorové okruhy

Věta 70

Nechť R je komutativní okruh s jedničkou.
Pak M je maximální ideál R, právě když R/M je pole.

Důkaz

Vynechán.

Příklad 123

Protože $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$, právě když n je prvočíslo, vidíme, že maximální ideály $\mathbb{Z}$ jsou právě ideály $p\mathbb{Z}$ pro prvočísla p.

Faktorové okruhy

Důsledek 26

Komutativní okruh s jedničkou je pole, právě když nemá žádné vlastní netriviální ideály.

Důkaz

Důsledek 25 ukazuje, že pole nemá žádné vlastní netriviální ideály.
Naopak, pokud komutativní okruh R s jedničkou nemá žádné vlastní netriviální ideály, pak $\{0\}$ je maximální ideál a $R/\{0\}$ je maximální ideál a $R/\{0\}$ ($\simeq R$) je pole dle Věty 70.

Prvoideál

Příklad 124

Všechny ideály okruhu $\mathbb{Z}$ jsou ve tvaru $n\mathbb{Z}$.

Pro $n = 0$ máme $n\mathbb{Z} = \{0\}$ a $\mathbb{Z}/\{0\} \simeq \mathbb{Z}$, což je obor integrity.

Pro $n > 0$ máme $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ je obor integrity, právě, když je n prvočíslo.
Samozřejmě je $\mathbb{Z}/p\mathbb{Z}$ i těleso, takže $p\mathbb{Z}$ je maximální ideál okruhu $\mathbb{Z}$.
Všimněme si, že aby byl součin rs v $p\mathbb{Z}$, musí být prvočíslo p dělitelem r nebo s.

Definice

Ideál $N \neq R$ v komutativním okruhu R je **prvoideál**, *pokud $ab \in N$ implikuje, že $a \in N$ nebo $b \in N$ pro všechna $a, b \in R$.*

Prvočísla v definici hrají velkou roli, odtud tedy prvoideál.

Prvoideál

Příklad 125

Jsou následující množiny prvoideály?

1. $\{0\}$ *v* $\mathbb{Z}$
2. $\{0\} \times \mathbb{Z}$ *v* $\mathbb{Z} \times \mathbb{Z}$

Prvoideál

Příklad

Jsou následující množiny prvoideály?

1. $\{0\}$ *v* $\mathbb{Z}$
2. $\{0\} \times \mathbb{Z}$ *v* $\mathbb{Z} \times \mathbb{Z}$

1. $\{0\}$ v $\mathbb{Z}$
   Ano, $\{0\}$ je prvoideál v každém oboru integrity.
2. $\{0\} \times \mathbb{Z}$ v $\mathbb{Z} \times \mathbb{Z}$
   Ano.
   Pokud $(a,b)(c,d) \in \{0\} \times \mathbb{Z}$, tak musí být $ac = 0$ v $\mathbb{Z}$.
   To je pokud $a = 0$ a pak $(a,b) \in \{0\} \times \mathbb{Z}$ nebo $c = 0$ a pak $(c,d) \in \{0\} \times \mathbb{Z}$
   $(\mathbb{Z} \times \mathbb{Z}/\{0\} \times \mathbb{Z}$ je isomorfní s $\mathbb{Z}$, což je obor integrity

Prvoideál

Věta 71

Nechť R je komutativní okruh s jedničkou a $N \neq R$ je ideál v R. Pak R/N je obor integrity, právě když N je prvoideál v R.

Důsledek 27

Každý maximální ideál v komutativním okruhu R s jedničkou je prvoideál.

Důkaz

Pokud je M maximální ideál v komutativním okruhu R, pak R/M je pole, takže i obor integrity, a tedy M je prvoideál dle předchozí věty.

Věta 72

Nechť R je libovolný okruh s jedničkou, pak zobrazení $\phi : \mathbb{Z} \to R$ dané $\phi(n) = n \cdot 1$ pro $n \in \mathbb{Z}$ je homomorfismus $\mathbb{Z}$ do R.

Důkaz

Všimněme si, že $\phi(n+m) = (n+m)\cdot 1 = (n\cdot 1) + (m \cdot 1) = \phi(n) + \phi(m)$.
Distributivní zákony v R ukazují, že

$$\underbrace{(1+\cdots+1)}_{n \text{ sčítanců}}\underbrace{(1+\cdots+1)}_{m \text{ sčítanců}} = \underbrace{(1+\cdots+1)}_{nm \text{ sčítanců}}$$

Takže $(n\cdot 1)(m\cdot 1) = (nm)\cdot 1$ *pro* $n, m > 0$.
Podobně dostaneme $(n\cdot 1)(m\cdot 1) = (nm)\cdot 1$ *i pro ostatní případy.*
Takže $\phi(nm) = (nm)\cdot 1 = (n\cdot 1)(m\cdot 1) = \phi(n)\phi(m)$

Důsledek 28

Každý okruh R s jedničkou a charakteristikou $n > 1$ má podokruh isomorfní s $\mathbb{Z}_n$.
Každý okruh R s jedničkou a charakteristikou 0 má podokruh isomorfní s $\mathbb{Z}$.

Důkaz

Zobrazení $\phi : \mathbb{Z} \to R$ dané $\phi(m) = (m \cdot 1)$ pro $m \in \mathbb{Z}$ je homomorfismus z věty 72. Jádro $Ker(\phi)$ je ideál v $\mathbb{Z}$.
Všechny ideály v $\mathbb{Z}$ jsou ve tvaru $s\mathbb{Z}$ pro nějaké $s \in \mathbb{Z}$.
Dle věty 45 vidíme, že pokud má R charakteristiku $n > 0$, tak jádro $Ker(\phi) = n\mathbb{Z}$. Pak obraz $\phi[\mathbb{Z}] \leq R$ je isomorfní s $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.
Pokud je charakteristika R 0, pak $m \cdot 1 \neq 0$, takže jádro ϕ je $\{0\}$. Takže obraz $\phi[\mathbb{Z}] \leq R$ je isomorfní s $\mathbb{Z}$.

Prvopole

Věta 73

Pole F je buďto prvočíselné charakteristiky p a obsahuje podpole isomorfní se $\mathbb{Z}_p$ nebo charakteristiky 0 a obsahuje podpole isomorfní s $\mathbb{Q}$.

Důkaz

Pokud F není charakteristiky 0, důsledek 27 říká, že F obsahuje podokruh isomorfní se $\mathbb{Z}_n$. Pak n musí být prvočíslo, jinak by F mělo dělitele nuly.

Pokud F není charakteristiky 0, tak F musí obsahovat podokruh isomorfní s $\mathbb{Z}$.
V tom případě důsledky 15 a 16 ukazují, že F musí obsahovat podílové těleso a to musí být isomorfní s $\mathbb{Q}$.

Takže každé pole obsahuje buďto podpole isomorfní s $\mathbb{Z}_p$ pro nějaké prvočíslo p nebo podpole isomorfní s $\mathbb{Q}$.

Definice

Pole $\mathbb{Z}_p$ a $\mathbb{Q}$ jsou **prvopole**.

Hlavní ideál

Definice

Pokud R je komutativní okruh s jedničkou a $a \in R$, tak ideál $\{ra | r \in R\}$ všech násobků a je **hlavní ideál generovaný** a *a značí se $\langle a \rangle$.*
Ideál N okruhu R je **hlavní ideál**, *pokud $N = \langle a \rangle$ pro nějaké $a \in R$.*

Příklad 126

Každý ideál okruhu $\mathbb{Z}$ je ve tvaru $n\mathbb{Z}$, který je generovaný n, takže každý ideál $\mathbb{Z}$ je hlavní ideál.

Příklad 127

Ideál $\langle x \rangle$ v $F[x]$ sestává ze všech polynomů v $F[x]$, které mají nulový konstantní term.

Hlavní ideál

Věta 74

Pokud F je pole, každý ideál v $F[x]$ je hlavní ideál.

Důkaz

Nechť N je ideál $F[x]$. Pokud $N = \{0\}$, pak $N = \langle 0 \rangle$.
Předpokládejme, že $N \neq \{0\}$ a $g(x) \in F$ je nenulový prvek N minimálního stupně.
Pak má $g(x)$ stupeň 0, tak $g(x) \in F$ a je to jednotka, takže $N = F[x] = \langle 1 \rangle$ dle věty 69, takže N je hlavní.
Pokud má $g(x)$ stupeň ≥ 1 a $f(x) \in N$, tak dle věty 57 $f(x) = g(x)q(x) + r(x)$, kde $r(x) = 0$ nebo má nižší stupeň než $g(x)$.
$f(x), g(x) \in N$ implikuje, že $f(x) - g(x)q(x) = r(x)$ je v N dle definice ideálu.
Protože $g(x)$ je nenulový prvek minimálního stupně v N, musí platit $r(x) = 0$
Takže $f(x) = g(x)q(x)$ a $N = \langle g(x) \rangle$.

Dělitelnost polynomů

Věta 75

Ideál $\langle p(x)\rangle \neq \{0\}$ okruhu $F[x]$ je maximální, právě když $p(x)$ je nedělitelný nad F.

Důkaz

Předpokládejme, že $\langle p(x)\rangle \neq \{0\}$ je maximální ideál okruhu $F[x]$.
Pak $\langle p(x)\rangle \neq F[x]$ a $p(x) \notin F$.
Nechť $p(x) = f(x)g(x)$ je faktorizace $p(x)$ v $F[x]$.
Protože $\langle p(x)\rangle$ je maximální ideál a tedy i prvoideál, $(f(x)g(x)) \in \langle p(x)\rangle$ implikuje, že $f(x) \in \langle p(x)\rangle$ nebo $g(x) \in \langle p(x)\rangle$.
Tj. $f(x)$ nebo $g(x)$ má $p(x)$ kalo faktor. Ale pak nemůžeme mít stupně $f(x)$ a $g(x)$ menší než stupeň $p(x)$.
To ukazuje, že $p(x)$ je nedělitelný nad F.

Dělitelnost polynomů

Důkaz (Pokračování)

Naopak, pokud $p(x)$ je nedělitelný nad F, předpokládejme, že N je ideál takový, že $\langle p(x)\rangle \subseteq N \subseteq F[x]$.

Dle věty 74 je N hlavní ideál, takže $N = \langle g(x)\rangle$ pro nějaké $g(x) \in N$. Pak $p(x) \in N$ implikuje, že $p(x) = g(x)q(x)$ pro nějaké $q(x) \in F[x]$. Ale $p(x)$ je nedělitelný, což implikuje, že $g(x)$ nebo $q(x)$ má stupeň 0.

Pokud $g(c)$ je stupně 0, tj. nenulová konstanta v F, tak $g(x)$ je jednotka v $F[x]$, takže $\langle g(x)\rangle = N = F[x]$.
Pokud $q(x)$ je stupně 0, tak $q(x) = c$, kde $c \in F$ a $g(x) = (1/c)p(x)$ je v $\langle p(x)\rangle$, takže $N = \langle p(x)\rangle$.

Takže případ $\langle p(x)\rangle \subset N \subset F[x]$ nemůže nastat, a tedy $\langle p(x)\rangle$ je maximální.

Dělitelnost polynomů

Následující větu jsme uvedli bez důkazu, nyní ji dokážeme.

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 $s(x)$.

Důkaz

Předpokládejme, že $p(x)$ dělí $r(x)s(x)$. Pak $r(x)s(x) \in \langle p(x) \rangle$, který je maximální dle věty 75.
Dle důsledku 27 je $\langle p(x) \rangle$ prvoideál.
Takže $r(x)s(x) \in \langle p(x) \rangle$ implikuje, že
$r(x) \in \langle p(x) \rangle$ a tedy $p(x)$ dělí $r(x)$
nebo
$s(x) \in \langle p(x) \rangle$ a tedy $p(x)$ dělí $s(x)$