Teoretická aritmetika

1 Přirozená čísla

Peanova aritmetika - axiomatický systém:
Peanovy axiomy:

(PA 1) $\exists! x \, \forall y : x \neq \sigma(y)$
... takové číslo značíme 0.

(PA 2) $\forall x \, \forall y : \sigma(x) = \sigma(y) \Rightarrow x = y$.

(PA 3) $\forall x : x + 0 = x$.

(PA 4) $\forall x \, \forall y : x + \sigma(y) = \sigma(x + y)$.

(PA 5) $\forall x : x \cdot 0 = 0$.

(PA 6) $\forall x \, \forall y : x \cdot \sigma(y) = x \cdot y + x$.

(PA 7) Je-li $U \subseteq \mathbf{N}$ taková, že platí:
$0 \in U$,
$\forall x : x \in U \Rightarrow \sigma(x) \in U$,
potom $U = \mathbf{N}$.

(PA 7*) (další možná formulace axiomu (PA 7),):
Nechť φ je libovolná formule Peanovy aritmetiky, přičemž x je její jedinou proměnnou, která v ní není kvantifikována.
Potom

$$[\, \varphi(0) \, \wedge \, \forall x : [\varphi(x) \Rightarrow \varphi(\sigma(x))] \,] \, \Rightarrow \, \forall x : \varphi(x) \, .$$

Vlastnosti operací sčítání a násobení na $\mathbf{N}$:

1) $\forall x, y, z \in \mathbf{N}$:
$(x + y) + z = x + (y + z)$

2) $\forall x, y \in \mathbf{N}$:
$x + y = y + x$

3) $\forall x, y, z \in \mathbf{N}$:
$x + z = y + z \Rightarrow x = y$

4) $\forall x, y \in \mathbf{N}$:
$x + y = 0 \Rightarrow (x = 0 \wedge y = 0)$

5) $\forall x \in \mathbf{N}$:
$x + 1 = 1 + x = \sigma(x)$

I) $\forall x, y, z \in \mathbf{N}$:
$(x.y).z = x.(y.z)$

II) $\forall x, y \in \mathbf{N}$:
$x.y = y.x$

III) $\forall x, y, z \in \mathbf{N}, z \neq 0$:
$x.z = y.z \Rightarrow x = y$

IV) $\forall x, y \in \mathbf{N}$:
$x.y = 1 \Rightarrow (x = 1 \wedge y = 1)$

V) $\forall x \in \mathbf{N}$:
$x.1 = 1.x = x$

VI) $\forall x, y \in \mathbf{N}$:
$x.y = 0 \Rightarrow (x = 0 \vee y = 0)$

7) $\forall x, y, z \in \mathbf{N}$:
$x.(y + z) = x.y + x.z$

Poznámka:
Struktura $(\mathbf{N}, +, .)$ je tzv. komutativní polookruh s nulovým a jednotkovým prvkem, s krácením nenulovými prvky a bez dělitelů nuly.

Uspořádání na $\mathbf{N}$:

$$\forall x, y \in \mathbf{N} : x < y \iff \exists z \in \mathbf{N}, z \neq 0 : x + z = y\,.$$

Příslušné neostré uspořádání přirozených čísel lze definovat takto:

$$\forall x, y \in \mathbf{N} : x \leq y \iff (x < y \vee x = y)\,.$$

Zřejmě platí:

$$\forall x, y \in \mathbf{N} : x \leq y \iff \exists z \in \mathbf{N} : x + z = y\,.$$

Vlastnosti uspořádání „<“ na $\mathbf{N}$:

1. Relace „<“ je ostré uspořádání na $\mathbf{N}$, které je úplné (tj. je to relace antireflexivní, tranzitivní a trichotomická).
2. $\forall x \in \mathbf{N}, x \neq 0 : 0 < x$.
3. $\forall x \in \mathbf{N} : x < \sigma(x)$.

4. $\forall x, y \in \mathbf{N} : x < y \Rightarrow (\sigma(x) < y \vee \sigma(x) = y)$.

5. $\forall x, y, z \in \mathbf{N} : x < y \Rightarrow x + z < y + z$.

6. $\forall x, y, z \in \mathbf{N} : (x < y \wedge z \neq 0) \Rightarrow x.z < y.z$.

7. $\forall x, y \in \mathbf{N}, y \neq 0 \ \exists z \in \mathbf{N} : x < y.z$.

Věta (o dělení se zbytkem v $\mathbf{N}$) :

$$\forall x, y \in \mathbf{N}, y \neq 0 \ \exists! u \in \mathbf{N}, \exists! r \in \mathbf{N} : x = y.u + r \wedge r < y \, .$$

Díky tvrzení věty o dělení se zbytkem jsou vlastně na přirozených číslech definovány další dvě (parciální) operace: jedna každé dvojici (x, y), kde $y \neq 0$, přiřazuje číslo u - této operaci se říká neúplný podíl, druhá číslo r, tzv. zbytek (po dělení čísla x číslem y).

2 Celá čísla

Metoda založená na myšlence německého matematika L.Kroneckera (1823-1891) spočívá v tom, že k množině $\mathbf{N}$ „připojíme“ všechny ty rozdíly dvou přirozených čísel, které nepatří do $\mathbf{N}$ a rozšíříme operace sčítání a násobení na celou takto vzniklou množinu.

Sestrojíme množinu

$$\mathbf{N} \times \mathbf{N} = \{(x, y);\, x, y \in \mathbf{N}\}$$

všech uspořádaných dvojic přirozených čísel. Na ní definujeme relaci

$$(x, y) \approx (x', y') \iff x + y' = x' + y \, .$$

Relace $\approx$ je ekvivalencí na množině $\mathbf{N} \times \mathbf{N}$, protože se jedná o relaci reflexivní, symetrickou a tranzitivní.

Ekvivalence $\approx$ indukuje rozklad množiny $\mathbf{N} \times \mathbf{N}$ na třídy ekvivalence, tento rozklad značíme $\mathbf{Z}$:

$$\mathbf{Z} = \mathbf{N} \times \mathbf{N} /_{\approx} = \{T(x, y);\, x, y \in \mathbf{N}\} \, .$$

Prvky množiny $\mathbf{Z}$ jsou podmnožiny v $\mathbf{N} \times \mathbf{N}$, které nazýváme třídy rozkladu $\mathbf{Z}$ a označujeme $T(x, y)$, přičemž pro každé $x, y \in \mathbf{N}$ je

$$T(x, y) = \{(u, v) \in \mathbf{N} \times \mathbf{N};\ \ (u, v) \approx (x, y)\} \, .$$

Dvojici (x, y) nazýváme reprezentantem třídy $T(x, y)$.

Uvědomme si, že táž třída rozkladu může mít různé uspořádané dvojice za své reprezentanty, přičemž platí

$$T(x, y) = T(x', y') \iff (x, y) \approx (x', y')$$

pro $\forall (x, y), (x', y') \in \mathbf{N} \times \mathbf{N}$.

Sčítání na $\mathbf{Z}$:

$$T(x,y)+T(u,v)=T(x+u,y+v)\,.$$

Věta:
Struktura $(\mathbf{Z},+)$ je komutativní grupa.

Věta:
V $(\mathbf{Z},+)$ existuje podstruktura $(\mathbf{Z}_0,+)$ izomorfní s $(\mathbf{N},+)$, píšeme

$$(\mathbf{N},+)\simeq(\mathbf{Z}_0,+)\,.$$

Označíme-li

$$\mathbf{Z}_0=\{T(z,0);\ z\in\mathbf{N}\}$$

množinu všech takových tříd ze $\mathbf{Z}$, do nichž patří dvojice tvaru $(z,0)$, je zřejmě $\mathbf{Z}_0\subseteq\mathbf{Z}$ a $(\mathbf{Z}_0,+)$ je podstrukturou grupy $(\mathbf{Z},+)$. Potom stačí uvažovat zobrazení

$$\begin{aligned}\varphi:\ &\mathbf{N}\to\mathbf{Z}_0\\ &x\mapsto\varphi(x)=T(x,0)\,,\end{aligned}$$

které je izomorfismem.

Existence izomorfismu φ umožňuje ztotožnit libovolné přirozené číslo $x\in\mathbf{N}$ a rozkladovou třídu $T(x,0)\in\mathbf{Z}_0$, která mu odpovídá v tomto zobrazení. Položíme-li

$$\forall x\in\mathbf{N}:\ x=T(x,0)\,,$$

potom $\mathbf{N}\subseteq\mathbf{Z}$.

Věta:
Pro každou třídu $T(x,y)\in\mathbf{Z}$ lze nalézt právě jedno přirozené číslo z tak, že buď $T(x,y)=T(z,0)$ nebo $T(x,y)=T(0,z)$, neboli

$$\forall T(x,y)\in\mathbf{Z}\ \exists!z\in\mathbf{N}:\ \ T(x,y)=T(z,0)\ \vee\ T(x,y)=T(0,z)\,.$$

Množinu $\mathbf{Z}$ nazýváme obvykle množinou (všech) celých čísel. Tuto množinu lze rozdělit do tří disjunktních podmnožin

$$\mathbf{Z}=\mathbf{Z}^+\cup\mathbf{Z}^-\cup\{0\}\,,$$

kde $\mathbf{Z}^+=\{z;\ z\in\mathbf{N},z\neq0\}=\{T(z,0);\ z\in\mathbf{N},z\neq0\}$ je množina kladných celých čísel, $\mathbf{Z}^-=\{-z;\ z\in\mathbf{N},z\neq0\}=\{T(0,z);\ z\in\mathbf{N},z\neq0\}$ je množina záporných celých čísel a $0=T(0,0)$ je jediné celé číslo, které není ani kladné ani záporné.

Opačný prvek k zápornému číslu (celému) je číslo kladné a opačný prvek ke kladnému číslu je číslo záporné:

$$\forall x\in\mathbf{Z}^-:-x\in\mathbf{Z}^+\ \ \wedge\ \ \forall x\in\mathbf{Z}^+:-x\in\mathbf{Z}^-\,.$$

Další důležité vlastnosti:

$$\forall x \in \mathbf{Z} : \ -(-x) = x \,,$$
$$\forall x, y \in \mathbf{Z} : \ -(x+y) = (-x) + (-y) \,,$$
$$\forall x, y \in \mathbf{Z}^+ : \ x + y \in \mathbf{Z}^+ \,,$$
$$\forall x, y \in \mathbf{Z}^- : \ x + y \in \mathbf{Z}^- \,.$$

Násobení na Z :

$$x \odot y = \begin{cases} x.y & \text{pro } x, y \in \mathbf{N}, \\ (-x).(-y) & \text{pro } x, y \in \mathbf{Z}^-, \\ -(x.(-y)) & \text{pro } x \in \mathbf{N}, y \in \mathbf{Z}^-, \\ -((-x).y) & \text{pro } x \in \mathbf{Z}^-, y \in \mathbf{N} \,. \end{cases}$$

Poznámka:
$x \odot y \in \mathbf{N} \iff$ obě čísla x, y patří do téže z množin $\mathbf{N}, \mathbf{Z}^-$,
$x \odot y \in \mathbf{Z}^- \iff$ obě čísla x, y nejsou prvky téže z množin $\mathbf{N}, \mathbf{Z}^-$.

Věta (Vlastnosti násobení na Z):
$(\mathbf{Z}, \odot)$ je komutativní pologrupa s jednotkovým prvkem, v níž lze krátit každým nenulovým prvkem, tj. platí:

1. $\forall x, y \in \mathbf{Z} : \ x \odot y = y \odot x \,,$
2. $\forall x, y, z \in \mathbf{Z} : \ (x \odot y) \odot z = x \odot (y \odot z) \,,$
3. $\exists e \in \mathbf{Z} \ \ \forall x \in \mathbf{Z} : \ x \odot e = e \odot x = x \,,$
4. $\forall x, y, z \in \mathbf{Z} : \ (x \odot y = x \odot z \ \wedge \ x \neq 0) \ \Rightarrow \ y = z \,.$

Shrňme nyní vlastnosti operací sčítání a násobení na množině celých čísel.
Věta:
Struktura $(\mathbf{Z}, +, \odot)$ je komutativní obor integrity, který není tělesem, operace sčítání a násobení na $\mathbf{Z}$ mají následující vlastnosti:

1. $\forall x, y \in \mathbf{Z} : \ x + y = y + x \,,$
2. $\forall x, y, z \in \mathbf{Z} : \ (x + y) + z = x + (y + z) \,,$
3. $\exists 0 \in \mathbf{Z} \ \ \forall x \in \mathbf{Z} : \ x + 0 = 0 + x = x \,,$
4. $\forall x \in \mathbf{Z} \ \ \exists (-x) \in \mathbf{Z} : \ x + (-x) = 0 \,,$
5. $\forall x, y \in \mathbf{Z} : \ x \odot y = y \odot x \,,$

6. $\forall x, y, z \in \mathbf{Z}: \ (x \odot y) \odot z = x \odot (y \odot z)$,

7. $\exists 1 \in \mathbf{Z} \ \ \forall x \in \mathbf{Z}: \ x \odot 1 = 1 \odot x = x$,

8. $\forall x, y \in \mathbf{Z}: \ x \odot y = 0 \ \Rightarrow \ (x = 0 \vee y = 0)$,

9. $\forall x, y, z \in \mathbf{Z}: \ x \odot (y + z) = x \odot y + x \odot z$,

10. $\forall x, y, z \in \mathbf{Z}: \ (y + z) \odot x = y \odot x + z \odot x$.

Uspořádání na $\mathbf{Z}$:

$$\forall x, y \in \mathbf{Z}: \ x \prec y \Longleftrightarrow y + (-x) \in \mathbf{Z}^{+}.$$

Relace $\prec$ je skutečně ostrým uspořádáním na množině celých čísel $\mathbf{Z}$, neboli je to relace antireflexivní a tranzitivní.

Věta:

Pro libovolnou dvojici celých čísel platí :

$$\forall x, y \in \mathbf{Z}: \ x \prec y \Longleftrightarrow$$

$$\Longleftrightarrow [\,(x, y \in \mathbf{N} \wedge x < y) \vee (x \in \mathbf{Z}^{-} \wedge y \in \mathbf{N}) \vee (x, y \in \mathbf{Z}^{-} \wedge -y < -x)\,].$$

Poznámka:
Tvrzení předchozí věty ukazuje, že uspořádání $<$ je zúžením (restrikcí) relace $\prec$ na množinu $\mathbf{N}$. Tato skutečnost umožňuje obě relace označovat týmž znakem $<$, čehož se také běžně využívá.

Vlastnosti uspořádání „$\prec$“ na $\mathbf{Z}$:

1. Uspořadání $\prec$ je relace trichotomická, tj.
   $\forall x, y \in \mathbf{Z}: \ x \prec y \vee y \prec x \vee x = y$.

2. $\forall x, y, z \in \mathbf{Z}: \ x \prec y \ \Rightarrow \ x + z \prec y + z$.

3. $\forall x, y \in \mathbf{Z}, z \in \mathbf{Z}^{+}: \ x \prec y \ \Rightarrow \ x \odot z \prec y \odot z$.

4. $\forall x \in \mathbf{Z} \ \forall y \in \mathbf{Z}^{+} \ \exists n \in \mathbf{N}: \ x \prec n.y$.

Poznámka:
Struktura $(\mathbf{Z}, +, \odot)$ s uvažovaným uspořádáním $\prec$ má vlastnosti archimedovsky uspořádaného oboru integrity.

Absolutní hodnota čísla z

je zobrazení množiny celých čísel $\mathbf{Z}$ na množinu přirozených čísel $\mathbf{N}$, definované pro libovolné $z \in \mathbf{Z}$ takto:

$$z \mapsto \begin{cases} |z| = z & \text{pro} \quad z \in \mathbf{N}, \\ |z| = -z & \text{pro} \quad z \in \mathbf{Z}^{-}. \end{cases}$$

Věta (Vlastnosti absolutní hodnoty):

1. $\forall z \in \mathbf{Z}: \ |z| \in \mathbf{N}\,,$
2. $\forall z \in \mathbf{Z}: \ |z| = 0 \Leftrightarrow z = 0\,,$
3. $\forall z \in \mathbf{Z}: \ |z| = |-z|\,,$
4. $\forall z \in \mathbf{Z}: \ -|z| \leq z \leq |z|\,,$
5. $\forall n \in \mathbf{N}\ \forall z \in \mathbf{Z}: \ -n \leq z \leq n \ \Rightarrow\ |z| \leq n\,,$
6. $\forall x, y \in \mathbf{Z}: \ |x + y| \leq |x| + |y|\,,$
7. $\forall x, y \in \mathbf{Z}: \ |x \odot y| = |x|.|y|\,.$

Věta (o dělení se zbytkem v $\mathbf{Z}$) :

$$\forall x, y \in \mathbf{Z}, y \neq 0 \ \exists! u \in \mathbf{Z}\ \exists! r \in \mathbf{Z}: \ (\, x = y \odot u + r \ \wedge\ 0 \leq r < |y|\,)\,.$$

Podobně jako v případě přirozených čísel nazýváme i v oboru integrity $(\mathbf{Z}, +, \odot)$ jednoznačně určené celé číslo u neúplným podílem a číslo r nejmenším nezáporným zbytkem (po dělení čísla x číslem y).

3 Okruhy a faktorokruhy

Definice:
Nechť M je neprázdná množina se dvěma operacemi $*, \circ$, pro něž platí:

1. $(M, *)$ je Abelova grupa, tj.

$$\forall a, b \in M: \ a * b = b * a\,,$$

$$\forall a, b, c \in M: \ a * (b * c) = (a * b) * c\,,$$

$$\exists e \in M \ \forall a \in M: \ a * e = a\,,$$

$$\forall a \in M \ \exists (-a) \in M: \ a * (-a) = e\,.$$

2. Distributivnost
$$\forall a,b,c \in M: \quad a \circ (b * c) = a \circ b * a \circ c\,, \\ (b * c) \circ a = b \circ a * c \circ a\,.$$

Potom struktura $(M, *, \circ)$ se nazývá okruh.

Poznámky:

1. V případě okruhu se dvěma operacemi se většinou používá značení $+$ pro operaci $*$ a $\cdot$ pro operaci $\circ$. O grupě $(M, +)$ se potom hovoří jako o aditivní grupě, pro neutrální prvek e užíváme symbol 0 a nazýváme jej nulový prvek okruhu a pro inverzní prvky užíváme název opačné prvky.

2. Struktura $(\mathbf{Z}, +, .)$ celých čísel je okruhem, ale struktura $(\mathbf{N}, +, .)$ okruhem není, protože $(\mathbf{N}, +)$ není grupou, neexistují zde opačné prvky ke všem přirozeným číslům.

Věta:
Nechť $(M, +, \cdot)$ je okruh, potom platí:

1. $\forall a \in M: \quad a.0 = 0 \wedge 0.a = 0\,,$

2. $\forall a,b \in M: \quad a.(-b) = (-a).b = -(a.b), \quad (-a).(-b) = a.b\,,$

3. $\forall a,b \in M \ \ \forall n \in \mathbf{N}: \quad (n.a).b = n.(a.b) = a.(n.b)\,.$

Má-li multiplikativní struktura $(M, .)$ některou další vlastnost, rozšiřujeme pojmenování okruhu o příslušnou vlastnost.

Definice:
Nechť $(M, +, \cdot)$ je okruh.
Okruh $(M, +, \cdot)$ je asociativní okruh, pokud operace násobení je asociativní, tj. platí-li:

$$\forall a,b,c \in M: \quad a.(b.c) = (a.b).c\,.$$

Okruh $(M, +, \cdot)$ se nazývá komutativní okruh, je-li operace násobení komutativní, tj. platí-li:

$$\forall a,b \in M: \quad a.b = b.a\,.$$

Okruh $(M, +, \cdot)$ je nazýván okruhem s jednotkovým prvkem, existuje-li prvek $e \in M$ takový, že platí:

$$\forall a \in M: \quad a.e = e.a = a\,.$$

Takový prvek pak obvykle značíme $e = \underline{1}$ a nazýváme jej jednotkovým prvkem.

Definice:
Nechť $(M, +, \cdot)$ je okruh a nechť S je neprázdná podmnožina M
($S \subseteq M, S \neq \emptyset$).
S je podokruh okruhu M právě tehdy, když $(S, +, \cdot)$ je okruh.

Věta:

1. S je podokruh okruhu $(M, +, \cdot)$

$$\iff \forall a, b \in S : \ (a - b \in S \ \wedge \ a.b \in S) \, .$$

2. $\forall i \in I = \{1, 2, \ldots\} : \ S_i$ je podokruh okruhu M

$$\implies \bigcap_{i \in I} S_i \text{ je podokruh okruhu } M \, .$$

3. $\forall i \in I = \{1, 2, \ldots\} : S_i$ je podokruh okruhu M, $S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots$

$$\implies \bigcup_{i \in I} S_i \text{ je podokruh okruhu } M \, .$$

4. Okruh $(M, +, \cdot)$ je asociativní (resp. komutativní), S je podokruh okruhu M. Potom také $(S, +, \cdot)$ je okruh asociativní (resp. komutativní).

Poznámka:
Jestliže M je okruh s jednotkovým prvkem $\underline{1}_M$ a S je podokruh okruhu M, potom S nemusí mít jednotkový prvek, S může mít jednotkový prvek $\underline{1}_S \neq \underline{1}_M$ nebo S může mít jednotkový prvek $\underline{1}_S = \underline{1}_M$.

Faktorizace okruhu.

Uvažujme okruh $(M, +, \cdot)$. Protože v okruhu je struktura $(M, +)$ Abelova grupa, je podgrupa $(S, +)$ této grupy rovněž Abelovou podgrupou. Potom lze udělat faktorovou grupu $(M/_S, +)$, která bude opět Abelovou grupou.

Prvky faktorové grupy označíme

$$a + S = \{a + s; \ s \in S\} \, .$$

Získáme tím rozklad množiny M podle podgrupy S, pro jehož prvky platí:

1. $\bigcup_{a \in M} (a + S) = M \, ,$
2. $(a + S) \cap (b + S) \neq \emptyset \implies a + S = b + S \, ,$
3. $a + S = b + S \iff -b + a \in S \, .$

Sčítání je pro prvky faktorové grupy definováno jako

$$(a + S) + (b + S) = (a + b) + S \, .$$

Definice:
Nechť $(M, +, \cdot)$ je okruh. Podgrupa I aditivní grupy $(M, +)$ okruhu M se nazývá:

- levý ideál, jestliže

$$\forall b \in I \ \forall x \in M : \ x.b \in I \, .$$

- pravý ideál, jestliže
$$\forall b \in I \ \ \forall x \in M : \ \ b.x \in I \, .$$
- ideál, pokud I je současně levý i pravý ideál.

Poznámka:
Shrňme podmínky, které musí splňovat ideál :
I je ideál okruhu $(M, +, \cdot)$, platí-li:

$$\forall a, b \in I : \ \ a - b \in I \, ,$$

$$\forall b \in I \ \ \forall x \in M : \ \ x.b \in I, \ \ b.x \in I \, .$$

Je-li I ideál okruhu $(M, +, \cdot)$, můžeme vytvořit tzv. faktorokruh

$$(M/_I, +, \cdot)$$

okruhu M podle ideálu I, kde operace sčítání a násobení jsou definovány takto:

$$(a + I) + (b + I) = (a + b) + I \, ,$$

$$(a + I) \cdot (b + I) = a \cdot b + I \, .$$

Takto získaná struktura má opět vlastnosti okruhu.

Faktorizací okruhu M podle ideálu I získáváme opět okruh - faktorový okruh $M/_I$ okruhu M podle ideálu I.

Definice:
Nechť $(M, +, \cdot)$ a $(S, +, \cdot)$ jsou dva okruhy. Zobrazení $\varphi : M \longrightarrow S$ je homomorfismem okruhů právě tehdy, když

$$\forall a, b \in M : \ \ \varphi(a + b) = \varphi(a) + \varphi(b) \, ,$$

$$\forall a, b \in M : \ \ \varphi(a.b) = \varphi(a) \cdot \varphi(b) \, .$$

Důležitým příkladem homomorfismu okruhů je zobrazení

$$\begin{aligned} \pi : \ \ & M \to M/_I \\ & a \mapsto a + I \, , \end{aligned}$$

které se nazývá přirozená projekce okruhu M na okruh $M/_I$.

I v případě homomorfismu okruhů $\varphi : M \longrightarrow S$ má smysl hovořit o jádru homomorfismu

$$Ker\, \varphi = \{x \in M;\, \varphi(x) = 0\}$$

a obrazu homomorfismu

$$Im\, \varphi = \{s \in S;\, \exists x \in M : \, \varphi(x) = s\} \, .$$

Poznámka:
Nechť $\varphi : M \longrightarrow S$ je homomorfismem okruhů.
Potom $Im\,\varphi \preceq S$ je podokruh okruhu S a $Ker\,\varphi \preceq M$ je podokruh okruhu M, který je dokonce ideálem okruhu M.

Věta o izomorfismu:
$\varphi : M \longrightarrow S$ je homomorfismus okruhu M do okruhu S.
Potom

$$M/_{Ker\,\varphi} \simeq Im\,\varphi, \;\; Im\,\varphi \preceq S\,.$$

Další známé matematické struktury se dvěma binárními operacemi jsou vlastně speciálními případy okruhů.

Definice:
Struktura $(T, +, \cdot)$ se nazývá těleso, pokud T je netriviální asociativní okruh a $(T \setminus \{0\}, \cdot)$ je grupa.

Poznámka:
Okruh $(T, +, \cdot)$ je těleso
$\iff$ $(T, +)$ je Abelova grupa, $(T \setminus \{0\}, \cdot)$ je grupa
$\iff$ $(T, +)$ je Abelova grupa, $(T \setminus \{0\}, \cdot)$ je asociativní, T má jednotkový prvek $\underline{1}$ a ke každému nenulovému prvku z T existuje prvek inverzní.

Lemma:
Je-li $(T, +, \cdot)$ těleso, potom platí:

$$\forall a, b \in T, a \neq 0, b \neq 0 \implies a.b \neq 0\,,$$

neboli těleso je bez dělitelů nuly.

Důkaz:
Je-li $a \in T, a \neq 0$, existuje k němu prvek inverzní $a^{-1} \in T : a.a^{-1} = a^{-1}.a = \underline{1}$. Kdyby potom měl být součin $a.b = 0$, muselo by platit $0 = a^{-1}.0 = a^{-1}.(a.b) = (a^{-1}.a).b = \underline{1}\,.b = b$, což je ve sporu s předpokladem nenulovosti b.

V lemmatu se vyskytla vlastnost, která charakterizuje tzv. okruhy bez dělitelů nuly.

Definice:
Řekneme, že okruh $(M, +, \cdot)$ je okruh bez dělitelů nuly, jestliže platí:

$$\forall a, b \in M, a \neq 0, b \neq 0 \implies a.b \neq 0\,.$$

Definice:
Obor je netriviální asociativní okruh bez dělitelů nuly a s jednotkovým prvkem.
Obor integrity je obor, který je navíc komutativní.

4 Podílové těleso oboru integrity

Nechť $(R, +, \cdot)$ je obor integrity, tj. komutativní a asociativní okruh s jednotkovým prvkem $\underline{1}$ a bez dělitelů nuly.

Označme $K = R \setminus \{0\}$ a uvažujme uspořádané dvojice

$$(a, b) \in R \times K \ \ldots \ a \in R,\, b \in K = R \setminus \{0\}\,.$$

Na množině $R \times K$ je relace $\sim$ definována takto:

$$(a, b) \sim (a', b') \iff ab' = a'b\,.$$

Tato relace je ekvivalencí na $R \times K$.

Ekvivalence $\sim$ indukuje rozklad množiny $R \times K$ na třídy ekvivalence. Jednotlivé rozkladové třídy podle ekvivalence $\sim$ označíme

$$a/b = \{(a', b') \in R \times K;\, (a', b') \sim (a, b)\}\,.$$

Množinu všech rozkladových tříd a/b označíme S.

Na množině S všech rozkladových tříd a/b definujeme operace sčítání

$$a/b + c/d = (ad + cb)/bd$$

a násobení

$$a/b \cdot c/d = ac/bd\,.$$

Obě operace jsou tímto korektně definovány, tj. nezáleží na volbě uspořádané dvojice reprezentující příslušnou rozkladovou třídu.

Struktura $(S, +, \cdot)$ je komutativní těleso s nulovým prvkem $0/\underline{1}$, opačnými prvky $-(a/b) = (-a)/b$ ke všem prvkům $a/b \in S$, jednotkovým prvkem $\underline{1}\,/\,\underline{1}$ a inverzními prvky $(a/b)^{-1} = b/a$, které existují ke všem nenulovým prvkům $a/b \in S \setminus \{0/\underline{1}\}$. Toto těleso nazýváme podílovým tělesem oboru integrity R.

Dále se nabízí otázka, zda existuje nějaká souvislost mezi prvky oboru integrity R a prvky jeho podílového tělesa S.

Uvažujme zobrazení

$$\begin{aligned} \omega :\ & R \to S \\ & a \mapsto \omega(a) = a/1\,. \end{aligned}$$

Toto zobrazení je homomorfismem okruhů, neboť pro libovolně zvolené prvky $a, b \in R$ je obraz součtu $\omega(a + b) = (a + b)/1$ roven součtu obrazů $\omega(a) + \omega(b) = a/1 + b/1 = (a.1 + b.1)/1.1 = (a + b)/1$ a také obraz součinu $\omega(a.b) = ab/1$ se shoduje se součinem obrazů $\omega(a) \cdot \omega(b) = a/1 \cdot b/1 = ab/1.1 = ab/1$.

Sporem se dokáže, že zobrazení ω je prosté. Zobrazení ω je monomorfismem.

Existence monomorfismu ω umožňuje ztotožnit prvky $a \in R$ s prvky $\omega(a) = a/1 \in S$. Po tomto ztotožnění je obor integrity R podokruhem jeho podílového tělesa S.

5 Racionální čísla

Celá čísla $(\mathbf{Z}, +, .)$ jsou konkrétním příkladem oboru integrity, tj. komutativního a asociativního okruhu s jednotkovým prvkem a bez dělitelů nuly. Vytvoříme-li podílové těleso oboru integrity S, dostaneme těleso $\mathbb{Q}$ racionálních čísel. Popišme tuto konstrukci podrobněji.

Nechť $R = \mathbf{Z}$, je to obor integrity. Označíme $K = R \setminus \{0\} = \mathbf{Z} \setminus \{0\} = \{z \in \mathbf{Z}; z \neq 0\}$.

Vytvoříme podílové těleso oboru integrity $\mathbf{Z}$, je jím množina

$$\mathbb{Q} = \{a/b;\ \ a \in \mathbf{Z},\, b \in \mathbf{Z}, b \neq 0\}$$

s operacemi sčítání

$$a/b + c/d = (ad + cb)/bd$$

a násobení

$$a/b \cdot c/d = ac/bd\,.$$

Samozřejmě i nyní symbolem a/b značíme rozkladovou třídu všech navzájem ekvivalentních prvků, tj. analogicky jako v obecném případě platí: $(a, b) \in a/b, (a', b') \in a/b \Leftrightarrow (a, b) \sim (a', b') \Leftrightarrow a.b' = a'.b\,.$

Struktura $(\mathbb{Q}, +, \cdot)$ je těleso. Množina $\mathbf{Z}$ všech celých čísel je podokruhem tělesa $\mathbb{Q}$, ztotožníme-li $z \in \mathbf{Z}$ se zlomkem $z/1 \in \mathbb{Q}$.

Dále můžeme předpokládat, že jednotlivé třídy rozkladu množiny $\mathbf{Z} \times \mathbf{Z} \setminus \{0\}$ jsou reprezentovány zlomky a/b, kde $b > 0$. Uvažujme $(a, b) \in \mathbf{Z} \times \mathbf{Z} \setminus \{0\}$, kde $b < 0$. Potom ale z rovnosti $(-a).b = -a.b = a.(-b)$ vyplývá ekvivalence dvojic $(-a, -b) \sim (a, b)$, proto $(-a)/(-b) = a/b$. Tedy každé racionální číslo $a/b \in \mathbb{Q}$ můžeme psát tak, že „jmenovatel“ b je kladný: $b > 0$, neboli

$$\forall a/b \in \mathbb{Q}\ \ \exists a_0/b_0 :\ a/b = a_0/b_0\ \wedge\ 0 < b_0\ .$$

Podobně jako u ostatních číselných oborů se pokusíme i pro racionální čísla definovat uspořádání podle jejich velikosti.

Uspořádání na $\mathbb{Q}$:

$$\forall a, b, c, d \in \mathbf{Z}, b > 0, d > 0 :\ \ a/b < c/d \iff ad < cb\,.$$

Další vlastnosti uspořádání racionálních čísel shrneme do následující věty.

Věta (Vlastnosti uspořádání $<$ na $\mathbb{Q}$) :

1. Uspořádání $<$ na $\mathbb{Q}$ je lineární.
2. Uspořádání na $\mathbf{Z}$ je zúžením tohoto uspořádání na $\mathbb{Q}$.
3. $\forall a/b, c/d, p/q \in \mathbb{Q} :\ \ a/b < c/d \Rightarrow a/b + p/q < c/d + p/q.$
4. $\forall a/b, c/d \in \mathbb{Q} :\ \ (a/b > 0\ \wedge\ c/d > 0) \Rightarrow a/b \cdot c/d > 0.$

5. $\forall a/b, c/d, p/q \in \mathbb{Q}: \ (a/b < c/d \wedge p/q > 0) \Rightarrow a/b \cdot p/q < c/d \cdot p/q.$

6. $\forall a/b \in \mathbb{Q}, \forall p/q \in \mathbb{Q}, p/q > 0 \ \exists n \in \mathbf{N}:$

$$a/b < n.(p/q) = \underbrace{p/q + p/q + \cdots + p/q}_{n} .$$

7. $\forall a/b, c/d \in \mathbb{Q}: \ a/b < c/d \ \Rightarrow \ \exists p/q \in \mathbb{Q}: \ a/b < p/q < c/d.$

Poznámka:
Vlastnost 7. z právě dokázané věty vlastně říká, že racionální čísla tvoří hustě uspořádanou množinu. Struktura $(\mathbb{Q}, +, ., <)$ tvoří tzv. archimédovsky a hustě uspořádané komutativní těleso.

6 Podílový okruh

Příklad:
Uvažujme strukturu tvořenou množinou $\mathbf{Z}_3 = \{0, 1, 2\}$ zbytkových tříd celých čísel modulo 3 s operacemi sčítání + a násobení . modulo 3. $(\mathbf{Z}_3, +, .)$ je nejenom okruh, je to i obor integrity, kde neexistují dělitelé nuly.

Můžeme proto zkonstruovat podílové těleso oboru integrity $\mathbf{Z}_3$, které označíme $\mathbb{Q}_3$. Množina

$$\mathbb{Q}_3 = \{p/q;\, p, q \in \mathbf{Z}_3, q \neq 0\}$$

je tvořena třemi prvky, neboť $0/1 = 0/2, 1/1 = 2/2, 2/1 = 1/2$.

Sčítání v podílovém tělese reprezentuje tabulka:

+	0/1	1/1	2/1
0/1	0/1	1/1	2/1
1/1	1/1	2/1	0/1
2/1	2/1	0/1	1/1

Násobení v podílovém tělese $\mathbb{Q}_3$ je reprezentováno tabulkou:

.	0/1	1/1	2/1
0/1	0/1	0/1	0/1
1/1	0/1	1/1	2/1
2/1	0/1	2/1	1/1

Tyto tabulky přesně odpovídají tabulkám sčítání a násobení v množině zbytkových tříd $\mathbf{Z}_3$. Je to proto, že $(\mathbf{Z}_3, +, .)$ není jenom obor integrity, tato struktura má totiž všechny vlastnosti tělesa. Obě uvažované struktury jsou tedy izomorfní:

$$\mathbb{Q}_3 \simeq \mathbf{Z}_3 .$$

Okruh $\mathbf{Z}_k$ zbytkových tříd modulo k s příslušnými operacemi počítanými modulo k je ale tělesem pouze pro k prvočísla. Není-li k prvočíslo, jedná se pouze o okruh, který není ani oborem integrity. Např. v $\mathbf{Z}_4$ je $2.2 = 0$, neboli existují zde dělitelé nuly. Nemůžeme potom konstruovat podílová tělesa. Přesto lze podobným způsobem dělat podílové okruhy, jen potřebujeme napřed definovat pojem multiplikativní množiny.

Poznámka:
Je-li $S = \{a/b;\, a, b \in R, b \neq 0\}$ podílové těleso oboru integrity R, je S nejmenší takové těleso, které obsahuje R jako podokruh.

Nechť $(R, +, \cdot)$ je komutativní, asociativní okruh s jednotkovým prvkem $\underline{1}$. (R nemusí být obor integrity, tedy může mít dělitele nuly.)

Podmnožina $S \subseteq R$ se nazývá multiplikativní množinou okruhu R právě tehdy, když:
1) $0 \notin S$,
2) $\underline{1} \in S$,
3) $\forall a, b \in S: \;\; a.b \in S$.

Je-li S multiplikativní množina okruhu R, potom na množině $R \times S$ uspořádaných dvojic $(a, s), a \in R, b \in S$ definujeme relaci

$$(a, s) \sim (b, r) \iff \exists s_1 \in S : (ar - bs).s_1 = 0\,.$$

Relace $\sim$ na množině $R \times S$ je reflexivní, symetrická a tranzitivní, je to tedy ekvivalence. Tato ekvivalence určuje rozklad množiny $R \times S$ na třídy navzájem ekvivalentních prvků. Označme

$$a/s = \{(b, r) \in R \times S;\, (b, r) \sim (a, s)\}$$

rozkladovou třídu spolu ekvivalentních prvků a

$$S^{-1}R = \{a/s;\, a \in R, s \in S\}$$

množinu všech takových rozkladových tříd. Na množině $S^{-1}R$ definujme operace sčítání

$$a/s + b/r = (ar + bs)/sr$$

a násobení

$$a/s \cdot b/r = ab/sr\,.$$

$(S^{-1}R, +, \cdot)$ je komutativní a asociativní okruh s jednotkovým prvkem $\underline{1}\,/\,\underline{1}$, který nazýváme podílovým okruhem okruhu R (podle multiplikativní množiny S).

Podobně jako při konstrukci podílového tělesa oboru integrity si můžeme i nyní položit otázku, zda existuje nějaký vztah mezi prvky původního okruhu R a prvky jeho podílového okruhu $S^{-1}R$.

Přirozeným homomorfismem okruhů R a $S^{-1}R$ je zobrazení

$$\begin{aligned} \omega: \;\; & R \to S^{-1}R \\ & a \mapsto \omega(a) = a/\,\underline{1} = as/s,\; s \in S\,. \end{aligned}$$

Věta:
Nechť $(S^{-1}R, +, \cdot)$ je podílový okruh okruhu R (podle multiplikativní množiny S). Potom pro přirozený homomorfismus $\omega : R \to S^{-1}R$ platí:

$$\omega \text{ prosté} \quad \Leftrightarrow \quad S \text{ neobsahuje dělitele } 0\,.$$

Důsledkem právě dokázané věty je následující fakt pro podílový okruh okruhu R: Jestliže multiplikativní množina S neobsahuje dělitele nuly, je přirozený homomorfismus těchto okruhů $\omega : R \to S^{-1}R$ prostým zobrazením. Můžeme proto ztotožnit prvky $a \in R$ a $\omega(a) = a/\underline{1}$. Po tomto ztotožnění lze R chápat jako podokruh okruhu $S^{-1}R$.

V podílovém okruhu $S^{-1}R$ není zaručena existence inverzních prvků (vzhledem k násobení) ke každému prvku $a/s \in S^{-1}R$. Přesto můžeme najít příklady prvků, ke kterým inverzní prvky existují. Zavádí se proto následující pojem:

Definice:
Nechť $(S^{-1}R, +, \cdot)$ je podílový okruh okruhu R (podle multiplikativní množiny S). Prvek v $S^{-1}R$ se nazývá invertibilní, pokud má inverzní prvek v $S^{-1}R$.

Je-li $a/s \in S^{-1}R$, kde je navíc $a \in S$, platí $s/a \cdot a/s = s.a/a.s = \underline{1}\,/\,\underline{1}$. To znamená, že každý prvek $a/s \in S^{-1}R$, kde $a \in S$, je invertibilní.

Příklady:

1. Nechť $R = \mathbf{Z}_4 = \{0, 1, 2, 3\}$ je okruh zbytkových tříd při dělení modulo 4 s operacemi sčítání a násobení mod 4. Pro multiplikativní množinu $S = \{1, 3\}$ má podílový okruh $S^{-1}R$ čtyři prvky: $S^{-1}R = \{0/1 = 0/3, 1/1 = 3/3, 2/1 = 2/3, 3/1 = 1/3\}$. V tomto okruhu jsou invertibilní pouze prvky $1/1, 3/1$.

2. Je-li $R = \mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ okruh zbytkových tříd při dělení modulo 6 s příslušnými operacemi sčítání a násobení mod 6 a multiplikativní množina $S = \{1, 5\}$, má podílový okruh $S^{-1}R$ šest prvků: $S^{-1}R = \{0/1 = 0/5, 1/1 = 5/5, 2/1 = 4/5, 3/1 = 3/5, 4/1 = 2/5, 5/1 = 1/5\}$. V tomto okruhu jsou invertibilní prvky $1/1, 5/1$.

3. V okruhu $R = \mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ s příslušnými operacemi sčítání a násobení mod 6 uvažujme multiplikativní množinu $S = \{1, 2, 4, 5\}$. Potom má podílový okruh $S^{-1}R$ tři prvky: $S^{-1}R = \{0/1, 1/1, 2/1\}$. V tomto okruhu jsou invertibilní oba nenulové prvky $1/1, 2/1$. Přirozený homomorfismus ω v tomto případě není prosté zobrazení, je totiž $\omega(3) = 3/1 = 0/1 = \omega(0), \omega(4) = 4/1 = 1/1 = \omega(1), \omega(5) = 5/1 = 2/1 = \omega(2)$.

4. Pokud v okruhu $R = \mathbf{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ zbytkových tříd při dělení modulo 8 (s příslušnými operacemi sčítání a násobení mod 8) uvažujeme multiplikativní množinu $S = \{1, 3\}$, má podílový okruh $S^{-1}R$ osm prvků: $S^{-1}R = \{0/1 = 0/3, 1/1 = 3/3, 2/1 = 6/3, 3/1 = 1/3, 4/1 = 4/3, 5/1 = 7/3, 6/1 = 2/3, 7/1 = 5/3\}$. Invertibilními prvky v tomto okruhu jsou prvky $1/1, 3/1, 5/1, 7/1$.

7 Reálná čísla

$\mathbb{Q}$ je množina všech racionálních čísel.

Řez $\alpha = (A/B)$ je dvojice množin $A, B \subseteq \mathbb{Q}$, která splňuje následující tři podmínky:

1. $A \neq \emptyset, \;\; B \neq \emptyset$
2. Každé číslo $q \in \mathbb{Q}$ leží v jedné a jen v jedné z množin A, B :

$$A \cup B = \mathbb{Q},\; A \cap B = \emptyset$$

3. $\forall a \in A \;\; \forall b \in B : \;\; a < b$

Tři druhy řezů:

1.druh .. A obsahuje největší číslo, B neobsahuje nejmenší číslo
2.druh .. A neobsahuje největší číslo, B obsahuje nejmenší číslo
3.druh .. A neobsahuje největší číslo, B neobsahuje nejmenší číslo

Řezy 1. druhu vzájemně jednoznačně odpovídají racionálním číslům:

$$a \in \mathbb{Q} \;\; \longleftrightarrow \;\; a^* = (A, B), A = \{x \in \mathbb{Q};\, x \leq a\}, B = \mathbb{Q} \setminus A\,,$$

a podobně též platí pro řezy 2. druhu:

$$a \in \mathbb{Q} \;\; \longleftrightarrow \;\; a^{**} = (A, B), B = \{x \in \mathbb{Q};\, a \leq x\}, A = \mathbb{Q} \setminus B\,.$$

Racionálnímu číslu $a \in \mathbb{Q}$ tedy odpovídají dva řezy, řez 1. druhu a^* a řez 2. druhu a^{**}.Tato duplicita umožňuje omezit se nadále pouze na řezy 1. a 3. druhu.

Uspořádání řezů :

Nechť $\alpha = (A/B), \alpha' = (A', B')$ jsou řezy 1. nebo 3. druhu:

$$\alpha \prec \alpha' \;\; \Longleftrightarrow \;\; A' \cap B \neq \emptyset\,.$$

Věta :

Relace $\prec$ je ostré, nelineární uspořádání na množině řezů 1. a 3. druhu, tj. je to relace antireflexivní, tranzitivní a trichotomická.

Vlastnosti uspořádání :

1. Je-li α řez 1. nebo 3. druhu, potom $\exists n \in \mathbf{N}$ tak, že $a \prec n^*$.
2. Jsou-li $a, b \in \mathbb{Q}$, potom platí:

$$a = b \Rightarrow a^* = b^*\,,$$
$$a < b \Rightarrow a^* \prec b^*\,.$$

Věta :
Nechť $\alpha = (A/B), \alpha' = (A', B')$ jsou řezy 1. nebo 3. druhu.
Označme $D = \{b + b';\ b \in B, b' \in B'\}, C = \mathbb{Q} \setminus D$.
Potom $\gamma = (C, D)$ je řez 1. nebo 3. druhu.

Řez γ je součet řezů α, α', píšeme:

$$\gamma = \alpha + \alpha' .$$

Vlastnosti sčítání :

1. $\forall \alpha, \alpha'$ řezy 1. nebo 3. druhu : $\alpha + \alpha' = \alpha' + \alpha$
2. $\forall \alpha, \alpha', \alpha''$ řezy 1. nebo 3. druhu : $(\alpha + \alpha') + \alpha'' = \alpha + (\alpha' + \alpha'')$
3. $\forall \alpha$ řez 1. nebo 3. druhu : $\alpha + 0^* = \alpha$
4. $\forall \alpha, \alpha'$ řezy 1. nebo 3. druhu $\exists!$ řez ξ 1. nebo 3. druhu tak, že :

   $$\alpha' + \xi = \alpha ,$$

   tedy $\forall \alpha\, \exists - \alpha$ tak, že $\alpha + (-\alpha) = 0^*$
5. $\forall \alpha, \alpha', \alpha''$ řezy 1. nebo 3. druhu :

   $$\alpha \prec \alpha' \ \Rightarrow \ \alpha + \alpha'' \prec \alpha' + \alpha''$$

6. $\forall a, b \in \mathbb{Q}$: $a^* + b^* = (a + b)^*$

Dále platí:

$$\alpha \prec 0^* \iff -\alpha \succ 0^* .$$

Věta :
Nechť $\alpha = (A/B) \succ 0^*, \alpha' = (A', B') \succ 0^*$ jsou řezy 1. nebo 3. druhu.
Označme $D = \{b.b';\ b \in B, b' \in B'\}, C = \mathbb{Q} \setminus D$.
Potom (C, D) je řez 1. nebo 3. druhu, $(C/D) \succ 0^*$.

Tento řez (C/D) je součin řezů α, α', značíme jej:

$$\alpha.\alpha' = (C/D).$$

(! pouze pro řezy $\alpha \succ 0^*, \alpha \succ 0^*$!)

Definice :
Nechť α, α' jsou řezy 1. nebo 3. druhu, potom definujeme součin řezů:

$$\alpha.\alpha' = (C/D), \text{ kde } D = \{b.b'; b \in B, b' \in B'\} \text{ pro } \alpha = (A/B) \succ 0^*, \alpha' = (A', B') \succ 0^*$$

$$\alpha.0^* = 0^*$$

$$0^*.\alpha = 0^*$$

$$\alpha.\alpha' = -((-\alpha).\alpha') \text{ pro } \alpha \prec 0^*, \alpha' \succ 0^*$$

$$\alpha.\alpha' = -(\alpha.(-\alpha')) \text{ pro } \alpha \succ 0^*, \alpha' \prec 0^*$$

$$\alpha.\alpha' = (-\alpha).(-\alpha') \text{ pro } \alpha \prec 0^*, \alpha' \prec 0^*$$

Vlastnosti násobení :

1. $\forall \alpha, \alpha'$ řezy 1. nebo 3. druhu : $\alpha.\alpha' = \alpha'.\alpha$
2. $\forall \alpha, \alpha', \alpha''$ řezy 1. nebo 3. druhu : $(\alpha.\alpha').\alpha'' = \alpha.(\alpha'.\alpha'')$
3. $\forall \alpha$ řez 1. nebo 3. druhu : $\alpha.1^* = \alpha$
4. $\forall \alpha, \alpha', \alpha''$ řezy 1. nebo 3. druhu : $(\alpha + \alpha').\alpha'' = \alpha.\alpha'' + \alpha'.\alpha''$, $\alpha''.(\alpha + \alpha') = \alpha''.\alpha + \alpha''.\alpha'$
5. $\forall \alpha, \alpha', \alpha''$ řezy 1. nebo 3. druhu :

$$(\alpha \prec \alpha' \wedge \alpha'' \succ 0^*) \Rightarrow \alpha.\alpha'' \prec \alpha'.\alpha''$$

6. $\forall \alpha, \alpha'$ řezy 1. nebo 3. druhu, $\alpha' \neq 0^*$ $\exists!$ řez ξ 1. nebo 3. druhu tak, že : $\alpha'.\xi = \alpha$.

Důsledek:
$\forall \alpha'$ řez 1. nebo 3. druhu, $\alpha' \neq 0^*$ $\exists!$ řez ξ 1. nebo 3. druhu tak, že :
$\alpha'.\xi = 1^*$,
tedy každý nenulový řez má řez inverzní.

Poznámka:
Násobení řezů je rozšířením násobení na $\mathbb{Q}$, tj.

$$\forall a, b \in \mathbb{Q} : \ a^*.b^* = (a.b)^* \, , \ -a^* = -a^* \, .$$

8 Komplexní čísla

$$\mathbf{C} = \{(a, b);\ a, b \in \mathbf{R}\} = \mathbf{R} \times \mathbf{R}$$

... Gaussova rovina komplexních čísel

Operace sčítání a násobení:

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b).(c, d) = (ac - bd, ad + bc)$$

Struktura $(\mathbf{C}, +, \cdot)$ je komutativní těleso s nulovým prvkem $(0,0)$, opačnými prvky $-(a,b) = (-a,-b)$, jednotkovým prvkem $(1,0)$ a převrácenými prvky
$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right)$.

Protože existuje homomorfismus

$$\begin{aligned} \varphi: \quad & \mathbf{R} \to \mathbf{C} \\ & r \mapsto \varphi(r) = (r,0) \end{aligned} \quad ,$$

který je prostým zobrazením tělesa $\mathbf{R}$ všech reálných čísel do tělesa $\mathbf{C}$ všech komplexních čísel, můžeme ztotožnit

$$r = \varphi(r) = (r,0)\,.$$

$(\mathbf{R}, +, \cdot)$ je tedy podtěleso tělesa $(\mathbf{C}, +, \cdot)$.

Dvojici $(0,1)$ označíme symbolem $i = (0,1)$ a nazýváme ji imaginární jednotkou. Platí pro ni

$$i^2 = (0,1).(0,1) = -1\,.$$

Komplexní čísla pak vyjadřujeme v tzv. algebraickém tvaru

$$(a,b) = a + b.i\,.$$

Absolutní hodnotou komplexního čísla $a + b.i$ rozumíme číslo

$$|a+b.i| = |(a,b)| = \sqrt{a^2+b^2} = \sqrt{(a+bi).(a-bi)}\,.$$

Vlastnosti absolutní hodnoty komplexních čísel:

1. $\forall a+bi \in \mathbf{C}: \quad |a+bi| \in \mathbf{R}, \quad |a+bi| \geq 0,$

$$|a+bi| = 0 \Leftrightarrow a+bi = 0$$

2. $\forall a+bi \in \mathbf{C}\ \forall c+di \in \mathbf{C}:$

$$|(a+bi).(c+di)| = |a+bi|.|c+di|$$

3. $\forall a+bi \in \mathbf{C}\ \forall c+di \in \mathbf{C}:$

$$|(a+bi)+(c+di)| \leq |a+bi| + |c+di|$$

9 Polynomy

Definice 9.1 *Nechť S je asociativní, komutativní okruh s 1, nechť R je podokruh okruhu S takový, že $1 \in R$. Zvolme prvek $x \in S$ a označme*
$R[x] = \{p(x) = p_0 + p_1x + \cdots + p_nx^n \ : \ n \in \mathbf{N}, p_0, p_1, ..., p_n \in R\}$.
Každý prvek z množiny $R[x]$ se nazývá polynom nad okruhem R.

Poznámka 9.1
1. Zřejmě $R[x] \subseteq S$, $R \subseteq R[x]$.
2. Zřejmě $p(x) = p_0+p_1x+\cdots+p_nx^n \longleftrightarrow (p_0, p_1, ..., p_n, 0, 0, ...)$, kde je jen konečně mnoho nenulových prvků.
3. $\mathrm{st}(p) = n = \max\{i : p_i \neq 0\}$, $\mathrm{st}(0) = \max \emptyset = -\infty$.

Operace s polynomy

Sčítání: $p(x) = p_0+p_1x+\cdots+p_nx^n$, $\mathrm{st}(p) = n$, $q(x) = q_0+q_1x+\cdots+q_mx^m$, $\mathrm{st}(q) = m$,
$p(x) + q(x) = (p_0 + q_0) + (p_1 + q_1)x + \cdots$,
$\mathrm{st}(p + q) \leq \max\{\mathrm{st}(p), \mathrm{st}(q)\}$.

Vlastnosti: $(R[x], +)$ je Abelova grupa.

Důkaz Protože R je podokruh okruhu S, který je asociativní, komutativní, je také sčítání v $R[x]$ asociativní a komutativní:
$p(x) + q(x) = (p_0 + q_0) + (p_1 + q_1)x + \cdots = (q_0 + p_0) + (q_1 + p_1)x + \cdots = q(x) + p(x)$,
$(p(x) + q(x)) + r(x) = ((p_0 + q_0) + r_0) + ((p_1 + q_1) + r_1)x + \cdots =$
$(p_0 + (q_0 + r_0)) + (p_1 + (q_1 + r_1))x + \cdots = (p(x) + (q(x) + r(x))$.
Pro každý polynom $p(x)$ je $p(x) + 0(x) = (p_0 + 0) + (p_1 + 0)x + \cdots = p_0 + p_1x + \cdots = p(x)$, proto $0(x)$ je nulový prvek v $R[x]$.
Pro každý prvek $p(x) = p_0 + p_1x + \cdots + p_nx^n$ jsou prvky $p_0, p_1, ..., p_n$ z okruhu R, proto pro každé $i = 0, 1, ..., n$ existuje prvek $-p_i \in R$ tak, že $p_i + (-p_i) = 0$. Potom pro polynom $-p(x) = (-p_0) + (-p_1)x + \cdots + (-p_n)x^n$ získáme
$p(x) + (-p(x)) = (p_0 + (-p_0)) + \cdots + (p_n + (-p_n))x^n = 0 + \cdots + 0x^n = 0(x)$.

■

Násobení: $p(x) = p_0+p_1x+\cdots p_nx^n$, $\mathrm{st}(p) = n$, $q(x) = q_0+q_1x+\cdots+q_mx^m$, $\mathrm{st}(q) = m$,
$p(x)q(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$, kde $c_k = \sum_{i=0}^{k} p_iq_{k-i} = \sum_{i+j=k} p_iq_j$,
$\mathrm{st}(pq) \leq \mathrm{st}(p) + \mathrm{st}(q)$.

Vlastnosti: pro každé $p(x), q(x), z(x) \in R[x]$ platí:
$p(x)q(x) = q(x)p(x)$ - komutativita
$(p(x)q(x))r(x) = p(x)(q(x)r(x))$ - asociativita,
$p(x)(q(x) + r(x)) = p(x)q(x) + p(x)r(x)$, - distributivita,
$(q(x) + r(x))p(x) = q(x)p(x) + r(x)p(x)$, - distributivita,
$p(x) \cdot 1 = p(x)$.

Důkaz Označme
$p(x) = p_0 + p_1x + \cdots + p_nx^n$,
$q(x) = q_0 + q_1x + \cdots + q_mx^m$,
$r(x) = r_0 + r_1x + \cdots + r_kx^k$.

Pro každé $i = 0, 1, ..., n$ a pro každé $j = 0, 1, ..., m$ je $(p_ix^i)(q_jx^j) = p_i(x^iq_j)x^j = p_i(q_jx^i)x^j = (p_iq_j)x^ix^j = (p_iq_j)x^{i+j}$, neboť okruh S je asociativní a komutativní. Tím je jasná korektnost definice násobení polynomů.

Komutativita: označme $p(x)q(x) = a(x) = a_0 + a_1x + \cdots + a_{n+m}x^{n+m}$, $q(x)p(x) = b(x) = b_0 + b_1x + \cdots + b_{m+n}x^{m+n}$, kde pro každé $u = 0, 1, ..., m+n$ je $a_u = \sum_{i+j=u} p_iq_j$, $b_u = \sum_{j+i=u} q_jp_i$. Potom $a_u = \sum_{i+j=u} p_iq_j = \sum_{j+i=u} q_jp_i = b_u$ pro každé $u = 0, 1, ..., m+n$.

Asociativita: označme
$p(x)q(x) = a_0 + a_1x + \cdots + a_{n+m}x^{n+m}$, kde $a_j = \sum_{i+l=j} p_iq_l$ pro každé $j = 0, 1, ..., n+m$,
$(p(x)q(x))r(x) = b_0 + b_1x + \cdots + b_{n+m+k}x^{n+m+k}$, kde $b_u = \sum_{j+v=u} a_jr_v$ pro každé
$u = 0, 1, ..., n+m+k$,
$q(x)r(x) = c_0 + c_1x + \cdots + c_{m+k}x^{m+k}$, kde $c_y = \sum_{l+v=y} q_lr_v$ pro každé $y = 0, 1, ..., m+k$,
$p(x)(q(x)r(x)) = d_0 + d_1x + \cdots + d_{n+m+k}x^{n+m+k}$, kde $d_u = \sum_{i+y=u} p_ic_y$ pro každé
$u = 0, 1, ..., n+m+k$.
Potom užijeme distributivnosti a asociativnosti okruhu R pro každé $u = 0, 1, ..., n+m+k$:
$b_u = \sum_{j+v=u} a_jr_v = \sum_{j+v=u} (\sum_{i+l=j} p_iq_l)r_v = \sum_{i+l+v=u} (p_iq_l)r_v = \sum_{i+l+v=u} p_i(q_lr_v) = \sum_{i+y=u} p_i(\sum_{l+v=y} q_lr_v)$
$= \sum_{i+y=u} p_ic_y = d_u$.

Distributivita: označme $t = \max\{m, k\}$, potom $q(x) = q_0 + q_1x + \cdots + q_tx^t$, kde $q_l = 0$ pro každé $l = m+1, ..., t$, $r(x) = r_0 + r_1x + \cdots + r_tx^t$, kde $r_e = 0$ pro každé $e = k+1, ..., t$. Potom $p(x)(q(x) + r(x)) = a_0 + a_1x + \cdots + a_{n+t}x^{n+t}$, kde pro každé $u = 0, 1, ..., n+t$ je $a_u = \sum_{i+j=u} p_i(q_j + r_j) = \sum_{i+j=u} p_iq_j + \sum_{i+j=u} p_ir_j$, proto $p(x)(q(x)+r(x)) = p(x)q(x)+p(x)r(x)$.

Z komutativity $R[x]$ pak plyne: $(q(x) + r(x))p(x) = p(x)(q(x) + r(x)) = p(x)q(x) + p(x)r(x) = q(x)p(x) + r(x)p(x)$.

Protože $1 = 1 + 0x + 0x^2 + \cdots$, je $p(x) \cdot 1 = a_0 + a_1x + \cdots + a_nx^n$, kde pro každé $u = 0, 1, ..., n$ je $a_u = p_u1 + p_{u-1}0 + \cdots + p_00 = p_u$.

■

Tím jsme dokázali větu.

Věta 9.1 *Množina $R[x]$ je komutativní, asociativní okruh s jednotkou.*

Definice 9.2 *Okruh $R[x]$ se nazývá okruh polynomů jedné neurčité nad okruhem R v S.*

Věta 9.2 *$R[x]$ je obor integrity právě tehdy, když R je obor integrity.*

Důkaz Nechť $R[x]$ je obor integrity. Jsou-li $a, b \in R$ libovolné prvky, $a \neq 0$, $b \neq 0$, potom položme $p(x) = a + 0x + 0x^2 + \cdots$, $q(x) = b + 0x + 0x^2 + \cdots$. Protože $R[x]$ je obor integrity, je $ab = p(x)q(x) \neq 0$. Tím R je obor integrity.
Nechť R je obor integrity. Jsou-li $p(x), q(x) \in R[x]$ libovolné prvky, $p(x) \neq 0$, $q(x) \neq 0$, potom označme $p(x) = p_0 + p_1x + \cdots + p_nx^n$, kde $n \geq 0$, $p_n \neq 0$, $q(x) = q_0 + q_1x + \cdots + q_mx^m$, kde $m \geq 0$, $q_m \neq 0$. Pak $p(x)q(x) = a_0 + a_1x + \cdots + a_{n+m}x^{n+m}$, kde $a_{n+m} = p_nq_m \neq 0$, neboť R je obor integrity. Tím $R[x]$ je obor integrity.

■

Definice 9.3 *Nechť S je asociativní, komutativní okruh s 1, nechť R je podokruh okruhu S takový, že $1 \in R$, nechť $a \in S$. Budeme říkat, že prvek $a \in S$ je algebraický nad R, jestliže existuje nenulový polynom $p(x) \in R[x]$ takový, že $p(a) = 0$, t.j. a je kořenem nějakého polynomu nad R.*
Budeme říkat, že prvek $a \in S$ je transcendentní nad R, jestliže takový polynom neexistuje, t.j. pro každý nenulový polynom $p(x)$ nad R je $p(a) \neq 0$.

Věta 9.3 *Nechť R_1 je podokruh komutativního, asociativního okruhu S_1 s jednotkou, která leží v R_1. Nechť R_2 je podokruh komutativního, asociativního okruhu S_2 s jednotkou, která leží v R_2. Nechť $\varphi: R_1 \longrightarrow R_2$ je homomorfismus okruhů, nechť $x \in S_1$, $u \in S_2$. Potom existuje jednoznačně určené zobrazení $\psi: R_1[x] \longrightarrow R_2[u]$ takové, že pro každé $r \in R_1$ je $\psi(r) = \varphi(r)$ a $\psi(x) = u$.*
Navíc: Jestliže φ je izomorfismus, potom $R_1[x]/\mathrm{Ker}\,\psi \cong R_2[u]$, $\mathrm{Ker}\,\psi \cap R_1 = \{0\}$.
Jestliže φ je izomorfismus, jestliže u je prvek transcendentní nad R_2, potom $R_1[x] \cong R_2[u]$.

Důkaz Zobrazení ψ definujeme přirozeným způsobem.
Pro libovolný prvek $p(x) = p_0 + p_1x + \cdots + p_nx^n$ položme:
$\psi(p(x)) = \varphi(p_0) + \varphi(p_1)u + \cdots + \varphi(p_n)u^n$
Ukážeme, že takto definované zobrazení je homomorfismus z $R_1[x]$ do $R_2[u]$.
Jsou-li $p(x) = p_0 + p_1x + \cdots + p_nx^n$, $q(x) = q_0 + q_1x + \cdots + q_mx^m$ libovolné prvky z $R_1[x]$, potom položme $k = \max\{n, m\}$ a polynomy doplníme nulovými koeficienty. Tím $p(x) = p_0 + p_1x + \cdots + p_kx^k$, $q(x) = q_0 + q_1x + \cdots + q_kx^k$. Potom
$\psi(p(x) + q(x)) = \psi((p_0 + q_0) + (p_1 + q_1)x + \cdots + (p_k + q_k)x^k) =$
$\varphi(p_0 + q_0) + \varphi(p_1 + q_1)u + \cdots + \varphi(p_k + q_k)u^k =$
$(\varphi(p_0) + \varphi(q_0)) + (\varphi(p_1) + \varphi(q_1))u + \cdots + (\varphi(p_k) + \varphi(q_k))u^k =$
$(\varphi(p_0) + \varphi(p_1)u + \cdots + \varphi(p_k)u^k) + (\varphi(q_0) + \varphi(q_1)u + \cdots + \varphi(q_k)u^k) = \psi(p(x)) + \psi(q(x))$.
Jestliže označíme $p(x)q(x) = a_0 + a_1x + \cdots + a_{n+m}x^{n+m}$, kde $a_l = \sum_{i+j=l} p_iq_j$ pro každé $l = 0, 1, ..., n + m$, potom
$\psi(p(x)q(x)) = \psi(a_0 + a_1x + \cdots + a_{n+m}x^{n+m}) = \varphi(a_0) + \varphi(a_1)u + \cdots + \varphi(a_{n+m})u^{n+m}$.
Protože φ je homomorfismus okruhu R_1 do okruhu R_2, je
$\varphi(a_l) = \varphi(\sum_{i+j=l} p_iq_j) = \sum_{i+j=l} \varphi(p_i)\varphi(q_j)$ pro každé $l = 0, 1, ..., n + m$. Tím
$\psi(p(x)q(x)) = \varphi(a_0) + \varphi(a_1)u + \cdots + \varphi(a_{n+m})u^{n+m} = (\varphi(p_0) + \varphi(p_1)u + \cdots + \varphi(p_n)u^n) \cdot$
$(\varphi(q_0) + \varphi(q_1)u + \cdots + \varphi(q_m)u^m) = \psi(p(x)) \cdot \psi(q(x))$.

Pro každé $r \in R_1$ je polynom $r(x) = r$ prvek z $R_1[x]$, proto $\psi(r) = \psi(r(x)) = \varphi(r)$.
Pro polynom $p(x) = x$ je $\psi(p(x)) = \psi(x) = \psi(1 \cdot x) = \varphi(1)u = 1 \cdot u = u$.
Pro ověření jednoznačnosti zobrazení předpokládejme, že existují dvě takováto zobrazení, tedy: $\psi_1 \colon R_1[x] \longrightarrow R_2[u]$, $\psi_2 \colon R_1[x] \longrightarrow R_2[u]$, ψ_1, ψ_2 jsou homomorfismy okruhů,
$\psi_1(r) = \varphi(r)$, $\psi_2(r) = \varphi(r)$ pro každé $r \in R_1$, $\psi_1(x) = u$, $\psi_2(x) = u$.
Potom pro libovolný prvek $p(x) = p_0 + p_1x + \cdots + p_nx^n \in R_1[x]$ máme
$\psi_1(p(x)) = \psi_1(p_0) + \psi_1(p_1)\psi_1(x) + \cdots + \psi_1(p_n)\psi_1(x)^n = \varphi(p_0) + \varphi(p_1)u + \cdots + \varphi(p_n)u^n = \psi_2(p_0) + \psi_2(p_1)\psi_2(x) + \cdots + \psi_2(p_n)\psi_2(x)^n = \psi_2(p(x))$.

Je-li φ izomorfismus, pro libovolný prvek $p(u) \in R_2[u]$ je $p(u) = p_0 + p_1u + \cdots + p_nu^n$, kde pro každé $i = 0, 1, ..., n$ je $p_i \in R_2$. Protože φ je izomorfismus, existují prvky $r_i \in R_1$ tak, že $\varphi(r_i) = p_i$ pro každé $i = 0, 1, ..., n$. Potom $r(x) = r_0 + r_1x + \cdots + r_nx^n \in R_1[x]$ a platí $\psi(r(x)) = \varphi(r_0) + \varphi(r_1)u + \cdots + \varphi(r_n)u^n = p_0 + p_1u + \cdots + p_nu^n = p(u)$. Tím ψ je epimorfismus a platí: $R_1[x]/\mathrm{Ker}\,\psi \cong R_2[u]$.
Pro libovolný prvek $r \in \mathrm{Ker}\,\psi \cap R_1$ je $0 = \psi(r) = \varphi(r)$. Tím $r = 0$, protože φ je izomorfismus.

Je-li φ izomorfismus a je-li u transcendentní prvek nad R_2, potom pro libovolný prvek $p(x) = p_0 + p_1x + \cdots + p_nx^n \in \mathrm{Ker}\,\psi$ je $0 = \psi(p(x)) = \varphi(p_0) + \varphi(p_1)u + \cdots + \varphi(p_n)u^n$. Protože u je transcendentní nad R_2, je tento polynom nulový, proto $\varphi(p_i) = 0$ pro každé $i = 0, 1, ..., n$. Protože φ je izomorfismus, je $p_i = 0$ pro každé $i = 0, 1, ..., n$, a tedy $p(x)$ je nulový polynom. Tím $\mathrm{Ker}\,\psi = 0$ a ψ je izomorfismus.

■

Věta 9.4 *Nechť R je asociativní, komutativní okruh s jednotkou. Označme $B = \{(r_n) \ : \ (r_n) = (r_0, r_1, ...)$ je nekonečná posloupnost prvků z R, kde je jen konečně mnoho nenulových prvků $\}$.*
Definujme operace sčítání a násobení takto:
$(r_n) + (q_n) = (r_n + q_n)$,
$(r_n) \cdot (q_n) = (c_n)$, *kde* $c_n = \sum_{i+j=n} r_iq_j$.
Potom $(B, +, \cdot)$ je asociativní, komutativní okruh s jednotkou.
Je-li navíc R obor integrity, potom B je také obor integrity.

Důkaz Podle poznámky 9.1 si výrazy $p_0+p_1x+\cdots+p_nx^n$ a $(p_0, p_1, ...)$, kde je jen konečně mnoho nenulových prvků vzájemně jednoznačně odpovídají. Proto ověření, že množina B spolu se zavedenými operacemi tvoří asociativní, komutativní okruh s jednotkou, je zcela analogické důkazu věty 9.1.

■

Věta 9.5 *Ke každému asociativnímu, komutativnímu okruhu R s jednotkou existuje okruh polynomů $R[x]$, kde prvek x je transcendentní nad R, který je určen jednoznačně až na izomorfismus.*

Důkaz Ukážeme, že okruh B z předchozí věty 9.4 je okruh polynomů $R[x]$.
Pro každé $r \in R$ položme $\overline{r} = (r, 0, 0, ...)$. Označíme-li $\overline{R} = \{\overline{r} \ : \ r \in R\}$, potom $\overline{R}$ je

podokruh okruhu B. Zobrazení $\alpha: R \longrightarrow \overline{R}$ definované předpisem $\alpha(r) = \overline{r}$ pro každé $r \in R$ je izomorfismus, proto $R \cong \overline{R}$.
Položme $x = (x_0, x_1, x_2, ...)$, kde $x_1 = 1$ a $x_i = 0$ pro každé $i \neq 1$, tedy $x = (0, 1, 0, 0, ...)$.
Potom $x^2 = x \cdot x = (c_n)$, kde
$c_0 = 0 \cdot 0 = 0$,
$c_1 = 0 \cdot 1 + 1 \cdot 0 = 0$,
$c_2 = 0 \cdot 0 + 1 \cdot 1 + 0 \cdot 0 = 1$,
$c_3 = 0 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 + 0 \cdot 0 = 0$,
$c_i = 0$ pro každé $i \geq 3$,
proto $x^2 = (0, 0, 1, 0, 0, ...)$.
Matematickou indukcí lze ukázat, že $x^k = (d_n)$, kde $d_k = 1$, $d_i = 0$ pro každé $i \neq k$.
Pro každé $\overline{r} \in \overline{R}$ a pro každé k je $\overline{r}x^k = (r_n) \cdot (d_n) = (f_n)$,
kde $r_0 = r$, $r_i = 0$ pro každé $i \geq 1$, $d_k = 1$, $d_j = 0$ pro každé $j \neq k$. Potom
$f_k = \sum_{i+j=k} r_i d_j = r_0 d_k + r_1 f_{k-1} + \cdots + r_{k-1} f_1 + r_k f_0 = r \cdot 1 + 0 + \cdots + 0 = r$
a pro každé $l \neq k$ je $f_l = 0$.
Proto $\overline{r}x^k = (0, 0, ..., 0, r, 0, 0, ..)$, kde prvek r je na místě k.
Tím pro každé $p(x) \in \overline{R}[x]$ máme
$p(x) = \overline{r}_0 + \overline{r}_1 x + \cdots + \overline{r}_n x^n = (r_0, 0, ...) + (0, r_1, 0, ..) + (0, 0, r_2, 0, ...) + \cdots + (0, ..., 0, r_n, 0, ...) = (r_0, r_1, r_2, ..., r_n, 0, 0, ...)$, a tedy $p(x) \in B$. Proto $\overline{R}[x] \subseteq B$.
Je-li naopak $(b_n) \in B$, potom posloupnost (b_n) má jen konečně mnoho nenulový prvků, proto existuje m tak, že $b_m \neq 0$ a $b_n = 0$ pro každé $n > m$. Tím $(b_n) = (b_0, b_1, ..., b_m, 0, 0, ...)$.
Označme $\overline{b}_i = (b_i, 0, 0, 0, ...)$. Protože pro každé i je $b_i \in R$, je $\overline{b}_i \in \overline{R}$. Potom
$\overline{b}_0 + \overline{b}_1 x + \cdots + \overline{b}_m x^m = (b_0, b_1, ..., b_m, 0, 0, ...) = (b_n)$, tedy $(b_n) \in \overline{R}[x]$. Tím $B \subseteq \overline{R}[x]$.
Proto $B = \overline{R}[x]$, tedy B je okruh polynomů nad okruhem $\overline{R}$.
Je-li $p(x) \in \overline{R}[x]$ takový polynom, že $p(x) = 0$, potom $p(x) = (r_0, r_1, ..., r_m, 0, 0, ...) = (0, 0, ..., 0, 0, 0, ...)$, a tedy $r_i = 0$ pro každé i, polynom $p(x)$ je nulový, proto prvek x je transcendentní nad $\overline{R}$.
Ztotožníme-li okruh R s okruhem $\overline{R}$, pak B je okruh polynomů nad okruhem R.

Jednoznačnost. Jsou-li $R[x]$ a $R[u]$ okruhy polynomů nad okruhem R takové, že x je transcendentní nad R, u je transcendentní nad R, potom identiské zobrazení $\varphi: R \longrightarrow R$ definované předpisem $\varphi(r) = r$ pro každé $r \in R$ je izomorfismus. Podle věty 9.3 existuje izomorfismus $\psi: R[x] \longrightarrow R[u]$ takový, že $\psi(r) = \varphi(r) = r$ pro každé $r \in R$, $\psi(x) = u$. Tím $R[x] \cong R[u]$.

■

Věta 9.6 *(O dělení polynomů se zbytkem)*
Nechť T je komutativní těleso, nechť $T[x]$ jsou polynomy jedné neurčité nad tělesem T. Jsou-li $f(x), g(x) \in T[x]$, $g(x) \neq 0$ libovolné polynomy, potom existují jednoznačně určené polynomy $q(x), r(x) \in T[x]$ takové, že $f(x) = g(x)q(x) + r(x)$, kde $\mathrm{st}(r) < \mathrm{st}(g)$.

Důkaz Označme $f(x) = f_0 + f_1 x + \cdots + f_n x^n$,
$g(x) = g_0 + g_1 x + \cdots + g_m x^m$, $g_m \neq 0$, $\mathrm{st}(g) = m$, $m \geq 0$.

1. Je-li $\mathrm{st}(f) < \mathrm{st}(g)$, potom položme $q(x) = 0$, $r(x) = f(x)$.

2. Je-li $\mathrm{st}(f) \geq \mathrm{st}(g)$, potom $f(x)$ je nenulový polynom, označme $\mathrm{st}(f) = n$, tedy $n \geq m$. Důkaz povedeme matematickou indukcí podle $n = \mathrm{st}(f)$.

   (i) Nechť $n = 0$. Pak $f(x) = f_0 \neq 0$, tím $m = 0$, a tedy $g(x) = g_0 \neq 0$. V tělese T existuje prvek $g_0^{-1} \in T$. Položme $q(x) = g_0^{-1} f_0$, $r(x) = 0$. Potom $f(x) = f_0 = g_0(g_0^{-1} f_0) + 0 = g(x)q(x) + r(x)$, $\mathrm{st}(r) = -\infty < 0 = \mathrm{st}(g)$.

   (ii) Nechť $n > 0$ a nechť tvrzení platí pro všechna $k < n$.
   Položme $f'(x) = f(x) - g(x) f_n g_m^{-1} x^{n-m}$, neboť prvek g_m^{-1} v tělese T existuje. Potom $\mathrm{st}(f') < n$, proto podle indukčního předpokladu existují polynomy $q'(x)$, $r'(x)$ takové, že $f'(x) = g(x)q'(x) + r'(x)$, kde $\mathrm{st}(r') < \mathrm{st}(g)$. Potom $f(x) = f'(x) + g(x) f_n g_m^{-1} x^{n-m} = g(x)q'(x) + r'(x) + g(x) f_n g_m^{-1} x^{n-m} = g(x)(q'(x) + f_n g_m^{-1} x^{n-m}) + r'(x)$.
   Položme tedy $q(x) = q'(x) + f_n g_m^{-1} x^{n-m}$, $r(x) = r'(x)$.

Jednoznačnost.
Nechť $f(x) = g(x)q(x) + r(x)$, $\mathrm{st}(r) < \mathrm{st}(g)$, $f(x) = g(x)\overline{q}(x) + \overline{r}(x)$, $\mathrm{st}(\overline{r}) < \mathrm{st}(g)$. Potom $g(x)(q(x) - \overline{q}(x)) = \overline{r}(x) - r(x)$.
Kdyby $\overline{r}(x) - r(x) \neq 0$, potom $\mathrm{st}(\overline{r}(x) - r(x)) \geq 0$, a také $\mathrm{st}(q - \overline{q}) \geq 0$. Tím získáváme $\mathrm{st}(g) \leq \mathrm{st}(g) + \mathrm{st}(q - \overline{q}) = \mathrm{st}(\overline{r} - r) \leq \max\{\mathrm{st}(\overline{r}), \mathrm{st}(r)\} < \mathrm{st}(g)$ - spor. Proto $r(x) = \overline{r}(x)$. Pak $g(x)(q(x) - \overline{q}(x)) = 0$, a protože $T[x]$ je obor integrity, a $g(x) \neq 0$, je $q(x) = \overline{q}(x)$.

■

Důsledek 1 Nechť T je těleso, nechť $T[x]$ jsou polynomy jedné neurčité nad tělesem T. Nechť $f(x) \in T[x]$, $c \in T$. Potom existuje jednoznačně určený polynom $q(x) \in T[x]$ takový, že $f(x) = (x - c)q(x) + f(c)$.

10 Dělitelnost v oborech integrity

Definice 10.1 *Nechť S je obor integrity, t.j. asociativní, komutativní okruh s 1, bez dělitelů nuly ($\forall a, b \in S,\ a \neq 0,\ b \neq 0$ je $ab \neq 0$). Nechť $a, b \in S$.*

Budeme říkat, že b dělí a, jestliže existuje $c \in S$ tak, že $bc = a$. Píšeme $b|a$.

Budeme říkat, že prvky $a, b \in S$ jsou asociované, jestliže $a|b$ a současně $b|a$. Píšeme $a \sim b$.

Prvky asociované s jednotkovým prvkem 1 se nazývají dělitelé jednotky. Množinu všech dělitelů jednotky značíme $U(S)$.

Věta 10.1 *Nechť S je obor integrity. Potom platí:*

1. *$a|0$, $1|a$, $a|a$ pro každé $a \in S$.*
2. *Jestliže $a|b$, $b|c$, potom $a|c$.*
3. *Jestliže $a|b$, $c|d$, potom $ac|bd$.*
4. *$0|a$ právě tehdy, když $a = 0$.*
5. *Jestliže $ac|bc$, $c \neq 0$, potom $a|b$.*
6. *Jestliže $a|a_i$ pro každé $i = 1, ..., n$, potom $a|(r_1a_1 + r_2a_2 + \cdots + r_na_n)$ pro každé $r_1, ..., r_n \in S$.*

Důkaz

1. $a \cdot 0 = 0$, $1 \cdot a = a$, $a \cdot 1 = a$ pro každé $a \in S$.
2. Existují-li prvky $d, e \in S$ tak, že $ad = b$, $be = c$, potom $a(de) = (ad)e = be = c$.
3. Existují-li prvky $e, f \in S$ tak, že $ae = b$, $cf = d$, potom $(ac)(ef) = a(ce)f = a(ec)f = (ae)(cf) = bd$.
4. Jestliže $0|a$, potom existuje $b \in S$ tak, že $0 \cdot b = a$. Tím $a = 0 \cdot b = 0$. Jestliže $a = 0$, potom např. $0 \cdot 1 = 0 = a$, tedy $0|a$.
5. Existuje-li $e \in S$ tak, že $(ac)e = bc$, potom $bc = (ac)e = a(ce) = a(ec) = (ae)c$, tím $(b - ae)c = 0$. Protože $c \neq 0$ a S je obor integrity, je $b - ae = 0$, a tedy $b = ae$.
6. Existují-li prvky $e_i \in S$ takové, že $ae_i = a_i$ pro každé $i = 1, ..., n$, potom $a(r_1e_1 + \cdots + r_ne_n) = a(r_1e_1) + \cdots + a(r_ne_n) = (ar_1)e_1 + \cdots + (ar_n)e_n = (r_1a)e_1 + \cdots + (r_na)e_n = r_1(ae_1) + \cdots + r_n(ae_n) = r_1a_1 + \cdots + r_na_n$.

■

Věta 10.2 *Nechť S je obor integrity. Potom platí:*

1. *$U(S)$ tvoří grupu s operací násobení.*
2. *$a \sim b$ v S právě tehdy, když $\exists u \in U(S)$ tak, že $au = b$.*

Důkaz

1. Jsou-li $u, v \in U(S)$ libovolné prvky, potom $u|1$, $v|1$, tím $uv|1 \cdot 1 = 1$. Protože $1|uv$, je $uv \in U(S)$.
   Protože $1|1$, je $1 \in U(S)$.
   Je-li $u \in U(S)$ libovolný prvek, potom $u|1$, a tedy existuje $v \in S$ tak, že $uv = 1$. Tím $v|1$, a tedy $v \in U(S)$. Protože $uv = 1$, je $v = u^{-1}$.

2. Je-li $a \sim b$, potom existují prvky $c, d \in S$ tak, že $ac = b$, $bd = a$. Tím $a = bd = (ac)d = a(cd)$, a proto $a(1 - cd) = 0$.
Pro $a \neq 0$ je $1 = cd$, a tedy $c, d \in U(S)$. Pro $a = 0$ je $b = 0$, a potom pro $1 \in U(S)$ máme $a \cdot 1 = b$.
Jestliže existuje $u \in U(S)$ tak, že $au = b$, potom $a|b$. Protože $u \in U(S)$, existuje $v \in S$ tak, že $uv = 1$. Potom $a = a \cdot 1 = a(uv) = (au)v = bv$, tím $b|a$, a tedy $a \sim b$.

■

Definice 10.2 *Nechť S je obor integrity, nechť $a, b \in S$. Říkáme, že a je triviální dělitel prvku b, jestliže $a \sim 1$ nebo $a \sim b$.*

Prvek $p \in S \setminus U(S)$, $p \neq 0$ se nazývá ireducibilní, jestliže má pouze triviální dělitele, t.j. jestliže $a|p$, potom $a \sim 1$ nebo $a \sim p$.

Definice 10.3 *Obor integrity S se nazývá Gaussův obor integrity (obor integrity s jednoznačným rozkladem), jestliže pro každé $a \in S \setminus U(S)$, $a \neq 0$ existuje $u \in U(S)$ a existují ireducibilní prvky $p_1, ..., p_k \in S$ takové, že $a = up_1p_2 \cdots p_k$, přičemž tento zápis je jednoznačný, t.j. jestliže $a = vq_1q_2 \cdots q_r$, kde $v \in U(S)$, $q_1, ..., q_r$ jsou ireducibilní prvky S, potom $r = k$ a existuje bijekce $\varphi\colon \{1, ..., k\} \longrightarrow \{1, ..., r\}$ taková, že pro každé $i = 1, ..., k$ je $p_i \sim q_{\varphi(i)}$.*

Tento jednoznačný rozklad prvku a se nazývá kanonický rozklad prvku a.

Poznámka 10.1 Kanonický rozklad $a = up_1p_2 \cdots p_k$ můžeme přepsat do tvaru $a = up_1^{m_1}p_2^{m_2} \cdots p_l^{m_l}$, kde $u \in U(S)$, $p_1, ..., p_l$ jsou ireducibilní prvky, $m_i \in \mathbf{N}$ pro každé $i = 1, ..., l$ a $p_i \not\sim p_j$ pro každé $i \neq j$.

Lemma 10.1 *Nechť S je Gaussův obor integrity, nechť $a = up_1p_2 \cdots p_k$, $b = vq_1q_2 \cdots q_r$ jsou kanonické rozklady nenulových prvků $a, b \in S$. Potom $a|b$ právě tehdy, když existuje prosté zobrazení $\varphi\colon \{1, ..., k\} \longrightarrow \{1, ..., r\}$ takové, že $p_i \sim q_{\varphi(i)}$ pro každé $i = 1, ..., k$.*

Důkaz Jestliže $a|b$, potom existuje $c \in S$ tak, že $ca = b$. Tím $cup_1p_2 \cdots p_k = vq_1q_2 \cdots q_r$. Je-li $c \in U(S)$, je $cu \in U(S)$, a tím $cup_1p_2 \cdots p_k$ je také kanonický rozklad prvku b. Z jednoznačnosti kanonického rozkladu víme, že existuje bijekce, tedy zobrazení prosté, $\varphi\colon \{1, ..., k\} \longrightarrow \{1, ..., r\}$ takové, že $p_i \sim q_{\varphi(i)}$ pro každé $i = 1, ..., k$.
Je-li $c \in S \setminus U(S)$, ($c \neq 0$, neboť $b \neq 0$), potom napišme jeho kanonický rozklad, t.j. $c = wt_1t_2 \cdots t_s$, kde $w \in U(S)$ a $t_1, ..., t_s$ jsou ireducibilní. Protože $b = ca$, je $vq_1q_2 \cdots q_r = wt_1t_2 \cdots t_sup_1p_2 \cdots p_k = (wu)t_1t_2 \cdots t_sp_1p_2 \cdots p_k$. Z jednoznačnosti kanonického rozkladu existuje bijekce $\varphi\colon \{1, ..., s, 1, ..., k\} \longrightarrow \{1, ..., r\}$ tak, že $t_i \sim q_{\varphi(i)}$ pro každé $i = 1, ..., s$, $p_j \sim q_{\varphi(j)}$ pro každé $j = 1, ..., k$. Zúžením zobrazení φ na množinu $\{1, ..., k\}$ získáme hledané prosté zobrazení.

Naopak, existuje-li prosté zobrazení $\varphi\colon \{1, ..., k\} \longrightarrow \{1, ..., r\}$ takové, že $p_i \sim q_{\varphi(i)}$ pro každé $i = 1, ..., k$, potom $b = vq_1q_2 \cdots q_r = v(q_{\varphi(1)} \cdots q_{\varphi(k)})(q_{i_1} \cdots q_{i_s})$, kde $\{i_1, ..., i_s\} = \{1, ..., r\} \setminus \{\varphi(1), ..., \varphi(k)\}$. Označme $c = q_{i_1} \cdots q_{i_s}$. Protože $a \sim (q_{\varphi_1}) \cdots q_{\varphi(k)})$, existuje $z \in U(S)$ tak, že $(q_{\varphi_1}) \cdots q_{\varphi(k)}) = za$. Potom $b = v(za)c = (vzc)a$, a tedy $a|b$.

■

Definice 10.4 *Nechť S je obor integrity. Nenulový prvek $p \in S \setminus U(S)$ se nazývá prvočinitel (prvotní), jestliže pro každé dva prvky $a, b \in S$ platí: když $p|ab$, potom $p|a$ nebo $p|b$.*

Lemma 10.2 *Nechť S je obor integrity. Je-li prvek $p \in S$ prvočinitel, potom p je prvek ireducibilní.*

Důkaz Je-li p prvočinitel, potom $p \in S \setminus U(S)$, $p \neq 0$. Nechť $a|p$, kde $a \in S$. Potom existuje $b \in S$ tak, že $p = ab$. Protože $p|p$, pak $p|ab$, a tedy $p|a$ nebo $p|b$. Jestliže $p|a$, potom $a \sim p$. Jestliže $p|b$, potom $b \sim p$, a tím existuje $u \in U(S)$ tak, že $b = up$. Potom $p = ab = aup$, a tedy $(1 - au)p = 0$. Protože $p \neq 0$, je v oboru integrity $au = 1$, a tím $a \sim 1$.

■

Lemma 10.3 *Nechť S je Gaussův obor integrity. Potom nenulový prvek $p \in S \setminus U(S)$ je prvočinitel právě tehdy, když p je ireducibilní.*

Důkaz Je-li p prvočinitel, potom p je ireducibilní podle předchozího lemmatu 10.2.
Naopak, nechť p je ireducibilní, nechť $p|ab$, kde $a, b \in S$.
Jestliže $a \neq 0$, $b \neq 0$ a $a \not\sim 1$ nebo $b \not\sim 1$, potom $a = up_1 \cdots p_k$ nebo $b = vq_1 \cdots q_r$, kde $u, v \in U(S)$ a prvky $p_1, ..., p_k, q_1, ..., q_r$ jsou ireducibilní, protože S je Gaussův obor integrity. Tím $ab = uvp_1 \cdots p_k q_1 \cdots q_r$, kde $k \geq 0$, $r \geq 0$ a alespoň jeden index je větší nebo roven 1. Protože $p|ab$, existuje podle lemmatu 10.1 prosté zobrazení $\varphi\colon \{1\} \longrightarrow \{1, ..., k, 1, ..., r\}$ takové, že $p \sim p_{\varphi(1)}$ nebo $p \sim q_{\varphi(1)}$. Tím $p|a$ nebo $p|b$.
Jestliže $a \neq 0$, $b \neq 0$, $a \sim 1$, $b \sim 1$, potom $a, b \in U(S)$, tedy $ab \in U(S)$. Protože $p|ab$, $ab|1$, pak $p|1$, což nemůže nastat.
Jestliže $a = 0$ nebo $b = 0$, potom $p \cdot 0 = 0 = a$ nebo $p \cdot 0 = 0 = b$, tedy $p|a$ nebo $p|b$.

■

Lemma 10.4 *Nechť S je obor integrity, nechť v S platí podmínka*
(KŘD) Jestliže $a_1, a_2, ..., a_n, ...$ je posloupnost prvků z S taková, že $a_{n+1}|a_n$ pro každé $n \in \mathbf{N}$, potom existuje $k \in \mathbf{N}$ tak, že pro každé $r \in \mathbf{N}$ je $a_{k+r} \sim a_k$.
Potom pro každý nenulový prvek $a \in S \setminus U(S)$ existuje ireducibilní prvek $p \in S$ takový, že $p|a$.

Důkaz Nechť $a \in S \setminus U(S)$, $a \neq 0$.
Jestliže a je ireducibilní, potom existuje $p = a$.
Jestliže a není ireducibilní, potom existuje $a_1 \in S$ tak, že $a_1|a$, $a_1 \not\sim a$, $a_1 \not\sim 1$.
Opakujeme totéž pro a_1. Jestliže a_1 je ireducibilní, potom $p = a_1$.
Jestliže a_1 není ireducibilní, potom existuje $a_2 \in S$ tak, že $a_2|a_1$, $a_2 \not\sim a_1$, $a_2 \not\sim 1$.
Opakujeme totéž pro $a_2 \ldots$.
Tím získáme posloupnost $a, a_1, a_2, ..., a_n, ...$, kde $a_1|a$, $a_{n+1}|a_n$ pro každé $n \in \mathbf{N}$.
Podle (KŘD) existuje $k \in \mathbf{N}$ tak, že $a_{k+r} \sim a_k$ pro každé $r \in \mathbf{N}$. Tím prvek a_k nemá vlastní dělitele, a tedy prvek a_k je ireducibilní. Položíme proto $p = a_k$.

■

Věta 10.3 *Nechť S je obor integrity. Potom S je Gaussův obor integrity právě tehdy, když platí podmínky:*

(P) Každý ireducibilní prvek je prvočinitel.

(KŘD) Jestliže $a_1, a_2, ..., a_n, ...$ je posloupnost prvků z S taková, že $a_{n+1}|a_n$ pro každé $n \in \mathbf{N}$, potom existuje $k \in \mathbf{N}$ tak, že pro každé $r \in \mathbf{N}$ je $a_{k+r} \sim a_k$.

Důkaz Nechť S je Gaussův obor integrity. Podle lemmatu 10.3 je splněna podmínka (P). Ověříme (KŘD). Nechť $a_1, a_2, ..., a_n, ... \in S$, $a_{n+1}|a_n$ pro každé $n \in \mathbf{N}$.
Jestliže existuje $n \in \mathbf{N}$ tak, že $a_n \in U(S)$, potom $a_n|1$, tím $a_{n+1}|a_n$, $a_n|1$, tedy $a_{n+1}|1$. Potom pro každé $r \in \mathbf{N}$ $a_{n+r}|1$, tedy $a_{n+r} \in U(S)$, a proto $a_{n+r} \sim a_n$ pro každé $r \in \mathbf{N}$.
Jestliže existuje $n \in \mathbf{N}$ tak, že $a_n = 0$, potom $0|a_{n-1}$, tedy $a_{n-1} = 0$, potom $0|a_{n-2}$, tedy $a_{n-2} = 0$ atd. Proto $a_k = 0$ pro každé $k = 1, ..., n$.
Nechť tedy $a_1 \neq 0$, nechť $a_n \in S \setminus U(S)$ pro každé $n \in \mathbf{N}$. V Gaussově oboru integrity existuje kanonický rozklad každého prvku a_n. Označme:
$a_1 = u_1 p_{11} \cdots p_{1r_1}$,
$a_2 = u_2 p_{21} \cdots p_{2r_2}$,
$\vdots$
$a_i = u_i p_{i1} \cdots p_{ir_i}$,
$a_{i+1} = u_{i+1} p_{i+1,1} \cdots p_{i+1,r_{i+1}}$,
$\vdots$
kde $u_i \in U(S)$, p_{ij} jsou ireducibilní pro každé $i \in \mathbf{N}$ a pro každé $j = 1, ..., r_i$.
Protože $a_{i+1}|a_i$ pro každé i, existuje podle lemmatu 10.1 prosté zobrazení
$\varphi\colon \{1, ..., r_{i+1}\} \longrightarrow \{1, ..., r_i\}$ takové, že $p_{i+1,j} \sim p_{i\varphi(j)}$ pro každé $j = 1, ..., r_{i+1}$.
Tím $r_{i+1} \leq r_i$ pro každé $i \in \mathbf{N}$.
Tedy $r_1 \geq r_2 \geq ... \geq r_i \geq r_{i+1} \geq ...$
Nerostoucí posloupnost přirozených čísel se musí zastavit, proto existuje $k \in \mathbf{N}$ tak, že $r_k = r_m$ pro každé $m \geq k$. Potom ovšem existuje bijekce $\varphi\colon \{1, ..., r_m\} \longrightarrow \{1, ..., r_k\}$ taková, že $p_{k,j} \sim p_{k\varphi(j)}$ pro každé $j = 1, ..., r_m$. Z existence inverzního zobrazení φ^{-1} plyne $a_k|a_m$, a potom $a_k \sim a_m$ pro každé $m \geq k$.

Naopak, nechť v oboru integrity S platí podmínky (P), (KŘD), nechť $a \in S \setminus U(S)$, $a \neq 0$. Podle lemmatu 10.4 existuje ireducibilní prvek $p_1 \in S$ takový, že $p_1|a$. Tím existuje $a_1 \in S$ tak, že $a = p_1 a_1$.
Pokud $a_1 \in U(S)$, pak $a = a_1 p_1$ je kanonický rozklad prvku a.
Pokud $a_1 \in S \setminus U(S)$, potom opět podle lemmatu 10.4 existuje ireducibilní prvek $p_2 \in S$ takový, že $p_2|a_1$. Tím existuje $a_2 \in S$ tak, že $a_1 = p_2 a_2$.
Pokud $a_2 \in U(S)$, pak $a = a_2 p_2 p_1$ je kanonický rozklad prvku a.
Pokud $a_2 \in S \setminus U(S)$, potom opět podle lemmatu 10.4 existuje ireducibilní prvek $p_3 \in S$ takový, že $p_3|a_2$. Tím existuje $a_3 \in S$ tak, že $a_3 = p_3 a_3$.
A tak dále.
Kdyby $a_r \in S \setminus U(S)$ pro každé r, potom získáme posloupnost $a, a_1, a_2, ..., a_r, a_{r+1}, ...$ prvků z S, kde $a_1|a$, $a_{r+1}|a_r$ pro každé r, a podle podmínky (KŘD) existuje $k \in \mathbf{N}$ takové, že

$a_k \sim a_m$ pro každé $m \geq k$. Tedy $a_k \sim a_{k+1}$. Existuje prvek $z \in S$ tak, že $a_{k+1} = a_k z$, $a_k = p_{k+1} a_{k+1}$. Potom $a_k(1 - p_{k+1}z) = 0$, a proto $p_{k+1} \in U(S)$, neboť $a_k \neq 0$. To je ovšem spor, proto existuje $r \in \mathbf{N}$ tak, že $a_r \in U(S)$. Tím $a = p_1 a_1 = p_1 p_2 a_2 = \cdots = p_1 p_2 \cdots p_r a_r$, kde $p_1, ..., p_r$ jsou ireducibilní a $a_r \in U(S)$, tedy existuje kanonický rozklad prvku a.
Jednoznačnost.
Mějme dva ireducibilní rozklady $a = up_1 \cdots p_k = vq_1 \cdots q_r$, kde $u, v \in U(S)$ a prvky $p_1, ..., p_k, q_1, ..., q_r$ jsou ireducibilní. Předpokládejme, že např. $k \leq r$. Budeme postupovat matematickou indukcí podle k.
Pro $k = 1$ je $a = up_1 = vq_1 \cdots q_r$. Podle podmínky (P) je p_1 prvočinitel, a tedy existuje $j \in \{1, ..., r\}$ tak, že $p_1 | q_j$. Protože p_1, q_j jsou ireducibilní, je $p_1 \sim q_j$, tedy existuje $w \in U(S)$ tak, že $q_j = wp_1$. Kdyby $r > 1$, pak $a = up_1 = vq_1 \cdots q_{j-1} q_j q_{j+1} \cdots q_r = vq_1 \cdots q_{j-1}(p_1 w) q_{j+1} \cdots q_r = vw(q_1 \cdots q_{j-1} q_{j+1} \cdots q_r) p_1$. Protože $p_1 \neq 0$ a S je obor integrity, je $u = vw(q_1 \cdots q_{j-1} q_{j+1} \cdots q_r)$. To je ovšem spor, neboť $u \in U(S)$ a $q_i \notin U(S)$ pro každé $i = 1, ..., r$, $i \neq j$. Proto $r = 1$, a tedy $a = up_1 = vq_j$, $p_1 \sim q_j$.
Nechť tvrzení platí pro všechny kanonické rozklady, kde je méně než k ireducibilních prvků, nechť $a = up_1 \cdots p_k = vq_1 \cdots q_r$. Ireducibilní prvek p_k je prvočinitel, proto $p_k | vq_1 \cdots q_r$, a tedy existuje $j \in \{1, ..., r\}$ tak, že $p_k | q_j$, tím $p_k \sim q_j$. Proto $q_j = wp_k$, kde $w \in U(S)$. Pak $a = (up_1 \cdots p_{k-1}) p_k = vw(q_1 \cdots q_{j-1} q_{j+1} \cdots q_r) p_k$. V oboru integrity je $up_1 \cdots p_{k-1} = vw(q_1 \cdots q_{j-1} q_{j+1} \cdots q_r)$, což jsou dva kanonické rozklady. Podle indukčního předpokladu $k - 1 = r - 1$ a existuje bijekce $\varphi' \colon \{1, ..., k-1\} \longrightarrow \{1, ..., j-1, j+1, ..., r\}$ tak, že $p_i \sim q_{\varphi'(i)}$ pro každé $i = 1, ..., k-1$. Definujeme-li zobrazení $\varphi \colon \{1, ..., k\} \longrightarrow \{1, ..., r\}$ předpisem $\varphi(i) = \varphi'(i)$ pro každé $i = 1, ..., k-1$ a $\varphi(k) = j$, potom toto zabrazení φ je také bijekce a platí $p_i \sim q_{\varphi(i)}$ pro každé $i = 1, ..., k$.

■

Definice 10.5 *Nechť S je obor integrity, nechť $a, b, d \in S$. Říkáme, že d je největší společný dělitel prvků a, b, jestliže platí:*
(*i*) *$d|a$, $d|b$;*
(*ii*) *jestliže prvek $g \in S$ je takový, že $g|a$, $g|b$, potom $g|d$.*
Píšeme $d = (a, b)$.

Poznámka 10.2 Je-li $d_1 = (a, b)$, $d_2 = (a, b)$, potom $d_1 \sim d_2$.

Věta 10.4 *Nechť S je obor integrity, nechť $a, b, c \in S$. Potom platí:*
1. $(a, (b, c)) \sim ((a, b), c)$;
2. $c(a, b) \sim (ca, cb)$;
3. $(a, c) \sim 1$, $(a, b) \sim 1$ *právě tehdy, když* $(a, cb) \sim 1$.

Důkaz 1. Označme $d = (b, c)$, $e = (a, b)$, $f = (a, (b, c)) \sim (a, d)$, $g = ((a, b), c) \sim (e, c)$. Potom $f|a$, $f|d$, $d|b$, $d|c$, tím $f|a$, $f|b$, $f|c$, a tedy $f|e$, $f|c$, proto $f|g$. Stejně lze ukázat, že $g|f$, proto $f \sim g$.
2. Označme $d = (a, b)$, $e = (ca, cb)$. Nechť $c \neq 0$. Potom $d|a$, $d|b$, tím $cd|ca$, $cd|cb$, a proto $cd|e$. Protože $c|ca$, $c|cb$, máme $c|e$, tím existuje $f \in S$ tak, že $cf = e$. Protože $e|ca$, $e|cb$,

máme $cf|ca$, $cf|cb$ a podle věty 10.1 pro $c \neq 0$ získáváme $f|a$, $f|b$. Tím $f|d$, a proto existuje $f_1 \in S$ tak, že $ff_1 = d$, tím $cd = cff_1 = ef_1$, a tedy $e|cd$. Proto pro $c \neq 0$ je $cd \sim e$.
Je-li $c = 0$, je $(ca, cb) = (0, 0) \sim 0 = 0 \cdot (a, b)$.
3. Je-li $(a, b) \sim 1$, $(a, c) \sim 1$, potom podle právě dokázaného 2. tvrzení je $(ca, cb) \sim c \cdot 1 = c$, $(a, ca) \sim a(1, c) \sim a \cdot 1 = a$. Potom užitím právě dokázaného 1. tvrzení získáváme
$(a, cb) \sim ((a, ca), cb) \sim (a, (ca, cb)) \sim (a, c) \sim 1$.
Je-li $(a, cb) \sim 1$, potom označme $e = (a, b)$. Protože $e|b$, existuje $b_1 \in S$ tak, že $eb_1 = b$, potom $eb_1c = bc = cb$, a tedy $e|cb$. Protože $e|a$, získáme $e|1$, a proto $(a, b) = e \sim 1$. Stejně se ukáže, že $(a, c) \sim 1$.

■

Věta 10.5 *Nechť S je Gaussův obor integrity. Potom existuje největší společný dělitel libovolných dvou prvků z S, t.j. pro každé $a, b \in S$ existuje $d \in S$ tak, že $d \sim (a, b)$.*

Důkaz Je-li $a \in U(S)$ nebo $b \in U(S)$, potom $1 \sim (a, b)$.
Je-li $a = 0$, potom $b \sim (a, b)$. Je-li $b = 0$, potom $a \sim (a, b)$.
Nechť tedy $a, b \in S \setminus U(S)$, $a \neq 0$, $b \neq 0$. V Gaussově oboru integrity napišme kanonické rozklady těchto prvků.
$a = uf_1 \cdots f_h$, $b = vq_1 \cdots q_{h'}$, kde $u, v \in U(S)$, $f_1, ..., f_h, q_1, ..., q_{h'}$ jsou ireducibilní.
Označme $\{p_1, ..., p_r\}$ množinu ireducibilních prvků z S takovou, že $\{f_1, ..., f_h\} \subseteq \{p_1, ..., p_r\}$, $\{q_1, ..., q_{h'}\} \subseteq \{p_1, ..., p_r\}$ a pro každé $i, j \in \{p_1, ..., p_r\}$, $i \neq j$ máme $p_i \not\sim p_j$. Potom můžeme psát
$a = up_1^{k_1} \cdots p_r^{k_r}$, kde $k_i \geq 0$ pro každé $i = 1, ..., r$,
$b = vp_1^{m_1} \cdots p_r^{m_r}$, kde $m_i \geq 0$ pro každé $i = 1, ..., r$.
Označme $s_i = \min\{k_i, m_i\}$ pro každé $i = 1, ..., r$. Ukážeme, že prvek $d = p_1^{s_1} \cdots p_r^{s_r} \sim (a, b)$. Pro každé $i = 1, ..., r$ máme $p_i^{s_i}|p_i^{k_i}$, $p_i^{s_i}|p_i^{m_i}$, proto $d|a$, $d|b$. Nechť $g \in S$ je takový prvek, že $g|a$, $g|b$. Jestliže $g \in U(S)$, potom $g|1$, $1|d$, proto $g|d$. Jestliže $g \in S \setminus U(S)$, $g \neq 0$ (protože $a \neq 0$), potom napišme kanonický rozklad tohoto prvku $g = wq_1^{t_1} \cdots q_z^{t_z}$, kde $w \in U(S)$, $q_1, ..., q_z$ jsou ireducibilní, $q_i \not\sim q_j$ pro každé $i, j \in \{1, ..., z\}$, $i \neq j$, $t_i > 0$ pro každé $i \in \{1, ..., z\}$. Protože $g|a$ a $g|b$, existuje prosté zobrazení $\varphi\colon \{1, ..., z\} \longrightarrow \{1, ..., r\}$ takové, že $q_i \sim p_{\varphi(i)}$, $t_i \leq k_{\varphi(i)}$, $t_i \leq m_{\varphi(i)}$ pro každé $i = 1, ..., z$. Potom existuje $\overline{w} \in U(S)$ tak, že $g = \overline{w}p_i^{v_1} \cdots p_r^{v_r}$, kde $v_i \geq 0$ pro každé $i = 1, ..., r$, $t_i = v_{\varphi(i)}$ pro každé $i = 1, ..., z$. Tím $v_{\varphi(i)} = t_i \leq k_{\varphi(i)}$, $v_{\varphi(i)} = t_i \leq m_{\varphi(i)}$, proto $v_{\varphi(i)} = t_i \leq \min\{k_{\varphi(i)}, m_{\varphi(i)}\} = s_{\varphi(i)}$, a tedy $g|d$.

■

Věta 10.6 *Nechť S je obor integrity. Potom S je Gaussův obor integrity právě tehdy, když platí podmínky:*

(KŘD) Jestliže $a_1, a_2, ..., a_n, ...$ je posloupnost prvků z S taková, že $a_{n+1}|a_n$ pro každé $n \in \mathbf{N}$, potom existuje $k \in \mathbf{N}$ tak, že pro každé $r \in \mathbf{N}$ je $a_{k+r} \sim a_k$.

(NSD) V oboru integrity S existuje největší společný dělitel libovolných dvou prvků z S.

Důkaz Je-li S Gaussův obor integrity, potom je podle věty 10.5 splněna podmínka (NSD) a podle věty 10.3 je splněna podmínka (KŘD).
Naopak, nechť v oboru integrity S jsou spněny podmínky (NSD) a (KŘD). Ukážeme, že v S je splněna podmínka (P). Tvrzení věty pak plyne podle věty 10.3. Nechť $p \in S$ je ireducibilní prvek, nechť $p|ab$, $a, b \in S$. Z podmínky (NSD) existuje $d \in S$ tak, že $d \sim (p, ab)$. Potom $(p, ab) \sim d \sim p$. Předpokládejme sporem, že $p \not| a$, $p \not| b$.
Protože p je ireducibilní, je $(p, a) \sim 1$ a $(p, b) \sim 1$. Podle věty 10.4 je $(p, ab) \sim 1$. Ovšem $p|p$, $p|ab$, proto $p|1$, což je spor. Proto $p|a$ nebo $p|b$, a tím je prvek p prvočinitel.

■

Definice 10.6 *Obor integrity S se nazývá euklidovský, jestliže existuje zobrazení $\sigma: S \setminus \{0\} \longrightarrow \mathbf{Z}$ takové, že platí:*

(*i*) *$\sigma(a) \geq 0$ pro každé $a \in S$,*

(*ii*) *pro každé $a, b \in S$, $b \neq 0$ existují $q, r \in S$ tak, že $a = bq + r$, kde $r = 0$ nebo $\sigma(r) < \sigma(b)$.*

Zobrazení σ se nazývá ohodnocení.

Lemma 10.5 *Nechť S je obor integrity, nechť $a = bq + r$ pro $a, b, q, r \in S$. Potom existuje největší společný dělitel prvků a, b právě tehdy, když existuje největší společný dělitel prvků b, r. Platí $(a, b) \sim (b, r)$.*

Důkaz Je-li $d = (a, b)$, potom $d|a$, $d|b$, a z rovnosti $a = bq + r$ plyne, že $d|r$. Jestliže $g \in S$ je takový prvek, že $g|b$, $g|r$, potom z rovnosti $a = bq + r$ plyne, že $g|a$, a tedy $g|(a, b) = d$. Tím $d \sim (b, r)$, a tedy $(a, b) \sim (b, r)$.
Je-li $f = (b, r)$, potom $f|b$, $f|r$, a z rovnosti $a = bq + r$ plyne, že $f|a$. Jestliže $g \in S$ je takový prvek, že $g|a$, $g|b$, potom z rovnosti $a = bq + r$ plyne, že $g|r$, a tedy $g|(b, r) = f$. Tím $f \sim (a, b)$, a tedy $(b, r) \sim (a, b)$.

■

Věta 10.7 (Euklidův algoritmus).
Nechť S je euklidovský obor integrity. Potom v S existuje největší společný dělitel libovolných dvou prvků z S.

Důkaz Nechť $a, b \in S$. Je-li $a = 0$, potom $b \sim (a, b)$. Je-li $b = 0$, potom $a \sim (a, b)$. Jestliže $a \neq 0$, $b \neq 0$, $a \in U(S)$, potom $1 \sim (a, b)$. Jestliže $a \neq 0$, $b \neq 0$, $b \in U(S)$, potom $1 \sim (a, b)$. Nechť tedy $a \neq 0$, $b \neq 0$, $a, b \in S \setminus U(S)$.
Protože S je euklidovský obor integrity, $a, b \in S$, $b \neq 0$, potom existují $q_0, r_0 \in S$ tak, že $a = bq_0 + r_0$, kde $r_0 = 0$ nebo $\sigma(r_0) < \sigma(b)$. Je-li $r_0 = 0$, potom $(a, b) \sim b$.
Je-li $r_0 \neq 0$, potom existují $q_1, r_1 \in S$ tak, že $b = r_0 q_1 + r_1$, kde $r_1 = 0$ nebo $\sigma(r_1) < \sigma(r_0)$.
Je-li $r_1 \neq 0$, potom existují $q_2, r_2 \in S$ tak, že $r_0 = r_1 q_2 + r_2$, kde $r_2 = 0$ nebo $\sigma(r_2) < \sigma(r_1)$.
A tak dále.
Je-li $r_k \neq 0$, potom existují $q_{k+1}, r_{k+1} \in S$ tak, že $r_{k-1} = r_k q_{k+1} + r_{k+1}$, kde $r_{k+1} = 0$ nebo $\sigma(r_{k+1}) < \sigma(r_k)$.

Je-li $r_{k+1} \neq 0$, potom existují $q_{k+2}, r_{k+2} \in S$ tak, že $r_k = r_{k+1}q_{k+2} + r_{k+2}$, kde $r_{k+2} = 0$ nebo $\sigma(r_{k+2}) < \sigma(r_{k+1})$.
Je-li $r_{k+2} \neq 0$, potom existují $q_{k+3}, r_{k+3} \in S$ tak, že $r_{k+1} = r_{k+2}q_{k+3} + r_{k+3}$, kde $r_{k+3} = 0$ nebo $\sigma(r_{k+3}) < \sigma(r_{k+2})$.
Protože $\sigma(b) > \sigma(r_0) > \sigma(r_1) > \sigma(r_2) > \cdots > \sigma(r_{k+1}) > \sigma(r_{k+2}) > \cdots$, musí existovat k tak, že $r_{k+3} = 0$. Potom:
$a = bq_0 + r_0$,
$b = r_0q_1 + r_1$,
$r_0 = r_1q_2 + r_2$,
$\vdots$
$r_k = r_{k+1}q_{k+2} + r_{k+2}$,
$r_{k+1} = r_{k+2}q_{k+3}$.
$\sigma(b) > \sigma(r_0) > \sigma(r_1) > \sigma(r_2) > \cdots > \sigma(r_{k+1}) > \sigma(r_{k+2}) > 0$.
Potom $r_{k+2} \sim (r_{k+1}, r_{k+2})$. Podle lemmatu 10.5 je $r_{k+2} \sim (r_{k+1}, r_{k+2}) \sim (r_k, r_{k+1}) \sim (r_{k-1}, r_k) \sim \cdots \sim (r_1, r_2) \sim (r_0, r_1) \sim (b, r_0) \sim (a, b)$.
Tento postup hledání největšího společného dělitele se nazývá Euklidův algoritmus.

■

Důsledek 2 Nechť S je euklidovský obor integrity, nechť $a, b \in S$. Potom existují prvky $u, v \in S$ takové, že $(a, b) \sim ua + vb$.

Důkaz Je-li $a = 0$, potom $(a, b) \sim b = 0 \cdot a + 1 \cdot b$.
Je-li $b = 0$, potom $(a, b) \sim a = 1 \cdot a + 0 \cdot b$.
Je-li $a \neq 0$, $b \neq 0$, $a \in U(S)$, potom existuje $u \in S$ tak, že $ua = 1$, tím $(a, b) \sim 1 = ua + 0 \cdot b$.
Je-li $a \neq 0$, $b \neq 0$, $b \in U(S)$, potom existuje $v \in S$ tak, že $vb = 1$, tím $(a, b) \sim 1 = 0 \cdot a + vb$.
Je-li $a \neq 0$, $b \neq 0$, $a, b \in S \setminus U(S)$, potom podle důkazu věty 10.7 je $(a, b) \sim r_{k+2}$, kde
$a = bq_0 + r_0 \Rightarrow r_0 = a - q_0b = u_0a + v_0b$, kde $u_0 = 1$, $v_0 = -q_0$,
$b = r_0q_1 + r_1 \Rightarrow r_1 = b - q_1r_0 = u_1a + v_1b$, kde $u_1 = -u_0q_1$, $v_1 = 1 - v_0q_1$,
$r_0 = r_1q_2 + r_2 \Rightarrow r_2 = r_0 - q_2r_1 = u_2a + v_2b$, kde $u_2 = u_0 - u_1q_2$, $v_2 = v_0 - v_1q_2$,
$\vdots$
$r_k = r_{k+1}q_{k+2} + r_{k+2} \Rightarrow r_{k+2} = r_k - q_{k+2}r_{k+1} = u_{k+2}a + v_{k+2}b$, kde $u_{k+2} = u_k - u_{k+1}q_{k+2}$, $v_{k+2} = v_k - v_{k+1}q_{k+2}$, $r_{k+2} \sim (a, b)$ podle věty 10.7.

■

Věta 10.8 *Nechť S je komutativní, asociativní okruh s 1, nechť $a \in S$. Potom množina $aS = \{as : s \in S\}$ je ideál okruhu S.*

Důkaz Pro libovolné $as_1, as_2 \in aS$ je $as_1 - as_2 = a(s_1 - s_2) \in aS$.
Pro libovolné $as_1 \in aS$ a pro libovolné $s \in S$ je
$(as_1)s = a(s_1s) \in aS$, $s(as_1) = (as_1)s = a(s_1s) \in aS$.

■

Poznámka 10.3 $0S = \{0s : s \in S\} = \{0\}$, $1S = \{1s : s \in S\} = S$.

Definice 10.7 *Nechť S je komutativní, asociativní okruh s 1. Jestliže I je ideál okruhu S takový, že $I = aS$, kde $a \in S$, potom I se nazývá hlavní ideál.*

Komutativní, asociativní okruh s 1 se nazývá okruh hlavních ideálů, jestliže každý ideál okruhu S je hlavní.

Obor integrity S se nazývá obor integrity hlavních ideálů, jestliže každý ideál oboru integrity S je hlavní.

Věta 10.9 *Je-li S euklidovský obor integrity, potom S je okruh hlavních ideálů.*

Důkaz Nechť I je ideál euklidovského oboru integrity S.
Je-li $I = 0$, potom $I = 0 \cdot I$.
Je-li $I \neq 0$, potom existuje $a \in I$, $a \neq 0$.
Označme $K = \{\sigma(b) \ : \ b \in I, b \neq 0\}$. Množina $K \neq \emptyset$, protože $a \in K$. Neprázdná podmnožina nezáporných celých čísel má nejmenší prvek. Buď $\sigma(b_0) \in K$ nejmenší prvek, $b_0 \in I$, $b_0 \neq 0$. Potom $b_0 S \subseteq I$. Je-li naopak $c \in I$ libovolný prvek, potom v euklidovském oboru integrity existují prvky $q, r \in S$ tak, že $c = b_0 q + r$, kde $r = 0$ nebo $\sigma(r) < \sigma(b_0)$. Protože $r = c - b_0 q \in I$, a protože $\sigma(b_0)$ je nejmenší v K, musí být $r = 0$. Tím $c = b_0 q \in b_0 S$. Proto $I = b_0 S$, a tedy I je hlavní ideál.

■

Lemma 10.6 *Nechť S je okruh hlavních ideálů, nechť $a, b \in S$. Potom platí:*

1. *$a|b$ právě tehdy, když $bS \subseteq aS$.*
2. *$a \sim b$ právě tehdy, když $aS = bS$.*

Důkaz 1. Jestliže $a|b$, potom existuje $s \in S$ tak, že $as = b$. Pro každý prvek $s_1 \in S$ je $bs_1 = (as)s_1 = a(ss_1) \in aS$, tím $bS \subseteq aS$.
Jestliže $bS \subseteq aS$, pak $b = b \cdot 1 \in bS \subseteq aS$, tedy existuje $s_1 \in S$ tak, že $b = as_1$. Tím $a|b$.
2. $a \sim b \Leftrightarrow a|b \wedge b|a \Leftrightarrow bS \subseteq aS \wedge aS \subseteq bS \Leftrightarrow aS = bS$.

■

Lemma 10.7 *Nechť S je okruh hlavních ideálů, nechť $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ jsou ideály okruhu S. Potom existuje $k \in \mathbf{N}$ tak, že $I_k = I_{k+1} = \cdots$, t.j. pro každé $j \in \mathbf{N}$ je $I_{k+j} = I_k$.*

Důkaz Označme $I = \bigcup_{n \in \mathbf{N}} I_n$. Množina I je opět ideál okruhu hlavních ideálů S, proto existuje $c \in I$ tak, že $I = cS$. Protože $I = \bigcup_{n \in \mathbf{N}} I_n$, existuje $k \in \mathbf{N}$ tak, že $c \in I_k$. Tím $I = cS \subseteq I_k$, a proto $I = I_k$. Tím pro každé $j \in \mathbf{N}$ je $I_{k+j} = I = I_k$.

■

Lemma 10.8 *Nechť S je okruh hlavních ideálů, nechť $a, b \in S$ jsou libovolné prvky. Potom množina $aS + bS = \{as_1 + bs_2 : s_1, s_2 \in S\}$ je ideál okruhu S, a tedy existuje $d \in S$ tak, že $dS = aS + bS$. Potom $d \sim (a, b)$.*

Důkaz Pro libovolné prvky $s, s_1, s_2, s_1', s_2' \in S$ je
$(as_1 + bs_2) - (as_1' + bs_2') = a(s_1 - s_1') + b(s_2 - s_2') \in aS + bS$,
$s(as_1 + bs_2) = a(ss_1) + b(ss_2) \in aS + bS$,
$(as_1 + bs_2)s = a(s_1 s) + b(s_2 s) \in aS + bS$,
tedy $aS + bS$ je ideál okruhu hlavních ideálů S. Tím existuje $d \in S$ tak, že $aS + bS = dS$. Protože $aS \subseteq dS$, pak $d|a$ podle lemmatu 10.6. Stejně $d|b$, protože $bS \subseteq dS$. Je-li $g \in S$ takové, že $g|a$, $g|b$, potom opět podle lemmatu 10.6 je $aS \subseteq gS$, $bS \subseteq gS$. Tím máme $dS = aS + bS \subseteq gS$, a proto $g|d$. Tím jsme ukázali $d \sim (a, b)$.

■

Věta 10.10 *Nechť S je obor integrity hlavních ideálů. Potom S je Gaussův obor integrity.*

Důkaz Podle lemmatu 10.8 existuje největší společný dělitel libovolných dvou prvků, tím je v oboru integrity S splněna podmínka (NSD).
Nechť $a_1, a_2, ..., a_n, a_{n+1}, ...$ je posloupnost prvků z S taková, že $a_{n+1}|a_n$ pro každé n. Podle lemmatu 10.6 máme posloupnost ideálů $a_1S \subseteq a_2S \subseteq \cdots \subseteq a_nS \subseteq a_{n+1}S \subseteq \cdots$, kde podle lemmatu 10.7 existuje $k \in \mathbf{N}$ tak, že $a_{k+j}S = a_kS$ pro každé $j \in \mathbf{N}$. Pak opět podle lemmatu 10.6 je $a_{k+j} \sim a_k$ pro každé $j \in \mathbf{N}$. Tím jsme ukázali, že je splněna podmínka (KŘD). S je Gaussův obor integrity podle věty 10.6.

■

Důsledek 3 Každý euklidovský obor integrity je Gaussův obor integrity.

Důkaz Euklidovský obor integrity je podle věty 10.9 obor integrity hlavních ideálů, a ten je Gaussův podle věty 10.10.

■

11 Gaussovy obory integrity polynomů

Věta 11.1 *Nechť S je komutativní, asociativní okruh s 1. Jestliže $S[x]$ okruh polynomů nad S je Gaussův obor integrity, potom S je také Gaussův obor integrity.*
Navíc platí: $u \in U(S)$ právě tehdy, když $u \in U(S[x])$.

Důkaz Podle věty 9.2 je $S[x]$ obor integrity právě tehdy, když S je obor integrity.
Je-li $u \in U(S)$, potom existuje $s \in S$ tak, že $us = 1$. Pro polynomy $p_1(x) = u$, $p_2(x) = s$ platí $p_1(x)p_2(x) = us = 1$, tedy $u \in U(S[x])$.
Je-li $u(x) \in U(S[x])$, potom existuje polynom $p(x) \in S[x]$ tak, že $u(x)p(x) = 1$, tím $0 = \mathrm{st}(1) = \mathrm{st}(u) + \mathrm{st}(p)$. Proto $\mathrm{st}(u) = 0$, $\mathrm{st}(p) = 0$, a tedy $u(x) = u \in S$, $p(x) = p \in S$. Tím $u \in U(S)$.
Nechť $a \in S \setminus U(S)$, $a \neq 0$. Polynom $a(x) = a \in S[x] \setminus U(S[x])$, $a(x) \neq 0$. Protože $S[x]$ je Gaussův obor integrity, existuje kanonický rozklad prvku $a(x)$, tedy $a = a(x) = up_1(x)p_2(x)\cdots p_k(x)$, kde $u \in U(S[x])$ a prvky $p_1(x), ..., p_k(x)$ jsou ireducibilní v $S[x]$. Pak $u \in U(S), \mathrm{st}(u) = 0$. Protože $\mathrm{st}(a) = 0 = \mathrm{st}(u)+\mathrm{st}(p_1)+\cdots+\mathrm{st}(p_k) = 0+\mathrm{st}(p_1)+\cdots+\mathrm{st}(p_k)$, je $p_i(x) = p_i \in S$ pro každé $i = 1, ..., k$. Kdyby $p_i(x) = p_i$ nebyl ireducibilní v S, pak by existovaly prvky $c, d \in S$ tak, že $cd = p_i$, $c \not\sim 1$, $d \not\sim 1$, $c \not\sim p_i$, $d \not\sim p_i$ v S. Protože však $u \in U(S) \Leftrightarrow u \in U(S[x])$, máme $c \not\sim 1$, $d \not\sim 1$, $c \not\sim p_i$, $d \not\sim p_i$ v $S[x]$. Což je spor, neboť prvky p_i byly ireducibilní v $S[x]$. Tím $a = up_1p_2\cdots p_k$ je kanonický rozklad v S.
Jednoznačnost rozkladu: nechť $a = up_1p_2\cdots p_k$, $a = vq_1q_2\cdots q_l$ jsou dva kanonické rozklady prvku a v S. Potom jsou to také kanonické rozklady prvku $a = a(x)$ v $S[x]$, a tedy existuje bijekce $\varphi\colon \{1, ..., k\} \longrightarrow \{1, ..., l\}$ tak, že $p_i \sim q_{\varphi(i)}$ v $S[x]$. Tím existuje $w_i \in U(S[x])$ tak, že $p_i = w_i q_{\varphi(i)}$. Protože $w_i \in U(S)$ a $p_i, q_{\varphi(i)} \in S$, je $p_i \sim q_{\varphi(i)}$ v S.

■

Důsledek 4 Jestliže S není Gaussův obor integrity, potom $S[x]$ také není Gaussův obor integrity.

Definice 11.1 *Nechť S je Gaussův obor integrity, nechť polynom $f(x) \in S[x]$ je tvaru $f(x) = f_0 + f_1x + \cdots + f_nx^n$. Polynom $f(x)$ nazýváme primitivní, jestliže $(f_0, f_1, ..., f_n) \sim 1$.*

Lemma 11.1 *Nechť S je Gaussův obor integrity, nechť $f(x), g(x) \in S[x]$ jsou nenulové polynomy nad S. Nechť $f(x) = a\overline{f}(x)$, $g(x) = c\overline{g}(x)$, kde $\overline{f}(x)$, $\overline{g}(x)$ jsou primitivní polynomy, $a, c \in S$, $a \neq 0$, $c \neq 0$. Potom platí: jestliže $f(x) = g(x)$, potom $a \sim c$.*

Důkaz Označme $f(x) = f_0 + f_1x + \cdots + f_nx^n$, $\overline{f}(x) = \overline{f}_0 + \overline{f}_1x + \cdots + \overline{f}_nx^n$,
$g(x) = g_0 + g_1x + \cdots + g_mx^m$, $\overline{g}(x) = \overline{g}_0 + \overline{g}_1x + \cdots + \overline{g}_mx^m$. Z rovnosti $f(x) = g(x)$ plyne $n = \mathrm{st}(f) = \mathrm{st}(g) = m$, $f_0 = g_0$, $f_1 = g_1$, ..., $f_n = g_n$. Potom $a \sim a\cdot 1 \sim a\cdot(\overline{f}_0, \overline{f}_1, ..., \overline{f}_n) \sim (a\overline{f}_0, a\overline{f}_1, ..., a\overline{f}_n) \sim (f_0, f_1, ..., f_n) \sim (g_0, g_1, ..., g_n) \sim (c\overline{g}_0, c\overline{g}_1, ..., c\overline{g}_n) \sim c\cdot(\overline{g}_0, \overline{g}_1, ..., \overline{g}_n) \sim c \cdot 1 = c$.

■

Lemma 11.2 *Nechť S je Gaussův obor integrity, nechť T je podílové těleso nad okruhem S, nechť $f(x) \in T[x]$, $f(x) \neq 0$. Potom existuje prvek $a/b \in T$ a existuje primitivní polynom $\overline{f}(x) \in S[x]$ takový, že $f(x) = a/b \cdot \overline{f}(x)$.*
Tento zápis je jednoznačný až na asociovanost, t.j. jestliže $f(x) = c/d \cdot \overline{g}(x)$, kde $\overline{g}(x) \in S[x]$ je primitivní polynom, prvek $c/d \in T$, potom existuje prvek $u \in U(S)$ takový, že $u \cdot a/b = c/d$, $\overline{f}(x) = u \cdot \overline{g}(x)$.

Důkaz Protože $f(x) \in T[x]$, $f(x) \neq 0$, označme $f(x) = a_0/b_0 + a_1/b_1 x + \cdots + a_n/b_n x^n$, kde $a_i/b_i \in T$ pro každé $i = 0, 1, ..., n$.
Položme $b = b_0 b_1 \cdots b_n$. Potom pro každé $i = 0, 1, ..., n$ máme
$a_i/b_i = a_i(b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n)/b_i(b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n) = a_i b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n / b$.
Tím $f(x) = (a_0 b_1 \cdots b_n/b) + (a_1 b_0 b_2 \cdots b_n/b)x + \cdots + (a_n b_0 b_1 \cdots b_{n-1}/b)x^n$.
Položme $a \sim (a_0 b_1 \cdots b_n, a_1 b_0 b_2 \cdots b_n, ..., a_n b_0 b_1 \cdots b_{n-1})$.
Pro každé $i = 0, 1, ..., n$ získáváme $a | a_i b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n$, proto existuje $\overline{a}_i \in S$ takové, že $a\overline{a}_i = a_i b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n$. Potom $a_i b_0 b_1 \cdots b_{i-1} b_{i+1} \cdots b_n / b = a\overline{a}_i / b = a/b \cdot \overline{a}_i/1 = a/b \cdot \overline{a}_i$. Tím $f(x) = (a/b \cdot \overline{a}_0) + (a/b \cdot \overline{a}_1)x + \cdots + (a/b \cdot \overline{a}_n)x^n = a/b(\overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_n x^n)$.
Položíme-li $\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \cdots + \overline{a}_n x^n$, potom $\overline{f}(x) \in S[x]$, $f(x) = a/b \cdot \overline{f}(x)$.
$a \sim (a_0 b_1 \cdots b_n, a_1 b_0 b_2 \cdots b_n, ..., a_n b_0 b_1 \cdots b_{n-1}) \sim (a\overline{a}_0, a\overline{a}_1, ..., a\overline{a}_n) \sim a(\overline{a}_0, \overline{a}_1, ..., \overline{a}_n)$
Protože $f(x) \neq 0$, je $a \neq 0$, a proto v oboru integrity je $(\overline{a}_0, \overline{a}_1, ..., \overline{a}_n) \sim 1$, tedy polynom $\overline{f}(x)$ je primitivní.
Jednoznačnost. Nechť $f(x) = a/b \cdot \overline{f}(x) = c/d \cdot \overline{g}(x)$, kde $\overline{f}(x), \overline{g}(x) \in S[x]$ jsou primitivní, $a/b, c/d \in T$. Potom $ad\overline{f}(x) = cb\overline{g}(x)$, a podle lemmatu 11.1 je $ad \sim cb$, tedy existuje $u \in U(S)$ tak, že $uad = cb$. Potom $ad\overline{f}(x) = uad\overline{g}(x)$, a tím $\overline{f}(x) = u\overline{g}(x)$, neboť pro $f(x) \neq 0$ je $ad \neq 0$. Potom $u \cdot a/b = u/1 \cdot a/b = ua/b = uad/bd = cb/bd = c/d$.

■

Lemma 11.3 (Gaussovo lemma)
Nechť S je Gaussův obor integrity, nechť $a(x), b(x) \in S[x]$. Potom polynom $a(x) \cdot b(x)$ je primitivní právě tehdy, když jsou primitivní oba polynomy $a(x)$ i $b(x)$.

Důkaz Jsou-li polynomy $a(x) = a_0 + a_1 x + \cdots + a_n x^n$, $b(x) = b_0 + b_1 x + \cdots + b_m x^m$ primitivní, potom $(a_0, a_1, ..., a_n) \sim 1$, $(b_0, b_1, ..., b_m) \sim 1$.
Označme $a(x)b(x) = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m}$, kde $c_k = \sum_{i+j=k} a_i b_j$ pro každé $k = 0, 1, ..., n+m$. Předpokládejme sporem, že $(c_0, c_1, ..., c_{n+m}) \sim d \not\sim 1$ v oboru integrity S. Podle lemmatu 10.4 existuje ireducibilní prvek $p \in S$ takový, že $p|d$. Tím $p|c_0 = a_0 b_0$. V Gaussově oboru integrity je každý ireducibilní prvek prvočinitel, proto $p|a_0$ nebo $p|b_0$.
Protože $(a_0, a_1, ..., a_n) \sim 1$, existuje $i \in \{0, 1, ..., n\}$ tak, že $p \not| a_i$.
Označme i_0 nejmenší index takový, že $p \not| a_i$.
Protože $(b_0, b_1, ..., b_m) \sim 1$, existuje $j \in \{0, 1, ..., m\}$ tak, že $p \not| b_j$.
Označme j_0 nejmenší index takový, že $p \not| b_j$.
Potom pro $k_0 = i_0 + j_0$ máme $c_{k_0} = \sum_{i+j=k_0} a_i b_j = a_0 b_{k_0} + \cdots + a_{i_0} b_{j_0} + \cdots + a_{k_0} b_0$. Tím $a_{i_0} b_{j_0} = c_{k_0} - (a_0 b_{k_0} + \cdots + a_{i_0-1} b_{j_0+1}) - (a_{i_0+1} b_{j_0-1} + \cdots + a_{k_0} b_0)$. Z volby i_0, j_0 plyne, že

$p|a_0$, ... ,$p|a_{i_0-1}$, $p|b_0$, ... ,$p|b_{j_0-1}$. Protože $p|c_{k_0}$, nutně $p|a_{i_0}b_{j_0}$, ovšem $p \not| a_{i_0}$, $p \not| b_{j_0}$, což je spor.
Nechť naopak plynom $a(x)b(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$ je primitivní. Potom máme $(c_0, c_1, ..., c_{n+m}) \sim 1$. Předpokládejme sporem, že např. polynom $a(x) = a_0+a_1x+\cdots+a_nx^n$ primitivní není. Potom $(a_0, a_1, ..., a_n) \sim d \not\sim 1$ v oboru integrity S. Pak $d|a_i$ pro každé $i = 0, 1, ..., n$, a tím $d|c_k$ pro každé $k = 0, 1, ..., n + m$, což je spor.

■

Věta 11.2 *Nechť S je Gaussův obor integrity, nechť $f(x) \in S[x]$, $f(x) \neq 0$, nechť T je podílové těleso oboru integrity S. Potom $f(x)$ je ireducibilní v $S[x]$ právě tehdy, když*

buď $\mathrm{st}(f) = 0$ *a* $f(x) = f$ *je ireducibilní v* S

nebo $\mathrm{st}(f) \geq 1$, $f(x)$ *je primitivní v* $S[x]$ *a* $f(x)$ *je ireducibilní v* $T[x]$.

Důkaz Nechť polynom $f(x)$ je ireducibilní v $S[x]$.
Je-li $\mathrm{st}(f) = 0$, potom $f(x) = f \in S$. Jestliže $g|f$ pro $g \in S$, potom polynom $g(x) = g|f = f(x)$ v $S[x]$, a tedy $g(x) \sim 1$ nebo $g(x) \sim f(x)$ v $S[x]$. Podle věty 11.1 máme $g \sim 1$ nebo $g \sim f$ v S, a tedy $f(x) = f$ je ireducibilní v S.
Je-li $\mathrm{st}(f) \geq 1$, potom označme $f(x) = a_0 + a_1x + \cdots + a_nx^n$, kde $a_0, a_1, ..., a_n \in S$, $\mathrm{st}(f) = n \geq 1$. Označme dále $d \sim (a_0, a_1, ..., a_n)$ v Gaussově oboru integrity S. Potom existují prvky $a'_i \in S$ takové, že $da'_i = a_i$ pro každé $i = 0, 1, ..., n$. Tím $d|f(x)$ v $S[x]$, a tedy $d \sim 1$ nebo $d \sim f(x)$ v $S[x]$. Protože však $d \in S$ a $\mathrm{st}(f) \geq 1$, je $d \not\sim f$, tím $d \sim 1$, a tedy polynom $f(x)$ je primitivní.
Nechť $g(x)|f(x)$ v $T[x]$. Potom existuje $h(x) \in T[x]$ tak, že $g(x)h(x) = f(x)$ v $T[x]$. Polynom $g(x) \neq 0$, proto podle lemmatu 11.2 existuje prvek $a/b \in T$ a primitivní polynom $\overline{g}(x) \in S[x]$ tak, že $g(x) = a/b \cdot \overline{g}(x)$. Stejně existuje prvek $c/e \in T$ a primitivní polynom $\overline{h}(x) \in S[x]$ tak, že $h(x) = c/e \cdot \overline{h}(x)$. Tím $f(x) = a/b \cdot c/e \cdot \overline{g}(x)\overline{h}(x)$, a potom získáváme $bef(x) = ac(\overline{g}(x)\overline{h}(x))$, kde polynom $f(x)$ je primitivní a polynom $\overline{g}(x)\overline{h}(x)$ je primitivní podle Gaussova lemmatu. Podle lemmatu 11.1 je $ac \sim be$, tedy existuje $u \in U(S)$ tak, že $ac = ube$. Potom $be(f(x) - u\overline{g}(x)\overline{h}(x)) = 0$, a tím jsme v oboru integrity $S[x]$ získali $f(x) = u\overline{g}(x)\overline{h}(x)$. Protože $f(x)$ je ireducibilní v $S[x]$, je $\overline{g}(x) \sim 1$ nebo $\overline{g}(x) \sim f(x)$ v $S[x]$.
Ukážeme, že $g(x) \sim 1$ nebo $g(x) \sim f(x)$ v $T[x]$, a tedy polynom $f(x)$ je ireducibilní v $T[x]$.
Je-li $\overline{g}(x) \sim 1$ v $S[x]$, potom existuje $v \in U(S[x])$, a tedy $v \in U(S)$ tak, že $\overline{g}(x) = v \cdot 1 = v$. Tím $\mathrm{st}(\overline{g}) = 0$. Protože $g(x) = a/b \cdot \overline{g}(x)$, je $\mathrm{st}(g) = 0$, proto $g(x) = g \in T$, $g \neq 0$, a tedy existuje $g^{-1} \in T$ tak, že $g \cdot g^{-1} = 1$. Tím $g(x) = g \sim 1$ v T, a tedy v $T[x]$.
Je-li $\overline{g}(x) \sim f(x)$ v $S[x]$, potom existuje $w \in U(S[x])$, a tedy $w \in U(S)$ tak, že $\overline{g}(x) = wf(x)$. Potom $w \in S \subseteq T$, $w \neq 0$, a tedy existuje $w^{-1} \in T$ tak, že $w \cdot w^{-1} = 1$, tím $w \in U(T)$, a tedy $w \in U(T[x])$. Proto $\overline{g}(x) \sim f(x)$ v $T[x]$. Protože $g(x) = a/b \cdot \overline{g}(x)$, $a/b \in T$, $a/b \neq 0$, je $a/b \in U(T)$, a tedy $a/b \in U(T[x])$. Tím $g(x) \sim \overline{g}(x)$ v $T[x]$. Potom $g(x) \sim \overline{g}(x) \sim f(x)$ v $T[x]$, a tedy $g(x) \sim f(x)$ v $T[x]$.

Nechť naopak jsou splněny podmínky věty, ukážeme, že polynom $f(x)$ je ireducibilní v $S[x]$. Nechť $g(x)|f(x)$ v $S[x]$. Potom existuje $h(x) \in S[x]$ tak, že $g(x)h(x) = f(x)$.
Jestliže $\mathrm{st}(f) = 0$, potom $f(x) = f \in S$, $f \neq 0$, a tím $\mathrm{st}(g) = 0$, $\mathrm{st}(h) = 0$, tedy

$g(x) = g \in S$, $h(x) = h \in S$, $g \neq 0$, $h \neq 0$. Protože podle předpokladu věty je $f(x) = f$ ireducibilní v S, je $g \sim 1$ nebo $g \sim f$ v S, potom $g \sim 1$ nebo $g \sim f$ v $S[x]$, a tedy $f(x) = f$ je ireducibilní v $S[x]$.
Jestliže $\mathrm{st}(f) \geq 1$, potom podle Gaussova lemmatu jsou polynomy $g(x)$, $h(x)$ primitivní v $S[x]$, protože $f(x) = g(x)h(x)$ a polynom $f(x)$ je primitivní v $S[x]$. Protože $S \subseteq T$, jsou $g(x), h(x) \in T[x]$, $f(x) = g(x)h(x)$, ale polynom $f(x)$ je ireducibilní v $T[x]$. Proto $g(x) \sim 1$ nebo $g(x) \sim f(x)$ v $T[x]$.
Je-li $g(x) \sim 1$ v $T[x]$, pak existuje $u \in U(T[x])$, a tedy $u \in U(T)$ tak, že $u \cdot g(x) = 1$. Potom $\mathrm{st}(g) = 0$, a tím $g(x) = g \in S$, $g \neq 0$. Protože $g(x) = g$ je primitivní v $S[x]$, je $(g) \sim 1$ v S, a tedy $g \sim 1$ v $S[x]$.
Jestliže $g(x) \sim f(x)$ v $T[x]$, potom existuje $v \in U(T[x])$, a tedy $v \in U(T)$ takové, že $g(x) = v \cdot f(x)$. Protože $U(T) = T \setminus \{0\}$, je $v = a/b$, kde $a, b \in S$, $a, b \neq 0$. Potom $g(x) = a/b \cdot f(x)$, tím $bg(x) = af(x)$. Protože polynomy $f(x)$, $g(x)$ jsou primitivní, podle lemmatu 11.1 je $b \sim a$ v S, tím existuje $w \in U(S)$, a tedy $w \in U(S[x])$ tak, že $b = wa$. Potom $a(wg(x) - f(x)) = 0$, a tím v oboru integrity $wg(x) = f(x)$. Proto $g(x) \sim f(x)$ v $S[x]$.
Tím jsme ukázali, že polynom $f(x)$ je ireducibilní v $S[x]$.

■

Věta 11.3 *Nechť S je Gaussův obor integrity. Potom $S[x]$ je také Gaussův obor integrity.*

Důkaz Nechť $f(x) \in S[x] \setminus U(S[x])$, $f(x) \neq 0$.
Označme T podílové těleso oboru integrity S. Potom $S \subseteq T$, a tedy $f(x) \in T[x]$. Obor integrity polynomů nad tělesem T je euklidovský obor integrity, a proto Gaussův obor integrity. Polynom $f(x)$ má tedy v $T[x]$ kanonický rozklad $f(x) = a/b \cdot p_1(x) \cdots p_r(x)$, kde $a/b \in T \setminus \{0\} = U(T)$, tedy $a/b \in U(T[x])$, polynomy $p_1(x), ..., p_r(x)$ jsou ireducibilní v $T[x]$.
Podle lemmatu 11.2 pro každé $i = 1, ..., r$ existuje $c_i/d_i \in T$, $c_i, d_i \neq 0$ a primitivní polynom $\overline{p}_i(x) \in S[x]$ tak, že $p_i(x) = c_i/d_i \cdot \overline{p}_i(x)$.
Potom $f(x) = a/b \cdot c_1/d_1 \cdots c_r/d_r \cdot \overline{p}_1(x) \cdots \overline{p}_r(x)$.
Označme $c/d = a/b \cdot c_1/d_1 \cdots c_r/d_r = ac_1 \cdots c_r/bd_1 \cdots d_r$.
Potom $f(x) = c/d \cdot \overline{p}_1(x) \cdots \overline{p}_r(x)$, a tedy $df(x) = c \cdot \overline{p}_1(x) \cdots \overline{p}_r(x)$ v $S[x]$, $c, d \neq 0$.
Jestliže $f(x) = a_0 + a_1x + \cdots + a_nx^n$, pak označme $t \sim (a_0, a_1, ..., a_n)$. Pro každé $i = 0, 1, ..., n$ existuje $\overline{a}_i \in S$ tak, že $t\overline{a}_i = a_i$. Tím $f(x) = a_0 + a_1x + \cdots + a_nx^n = t(\overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n)$.
Položme $\overline{f}(x) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n$. Potom $f(x) = t \cdot \overline{f}(x)$.
Protože $t \sim (a_0, a_1, ..., a_n) \sim t \cdot (\overline{a}_0, \overline{a}_1, ..., \overline{a}_n)$, je v oboru integrity $(\overline{a}_0, \overline{a}_1, ..., \overline{a}_n) \sim 1$, a tím polynom $\overline{f}(x)$ je primitivní v $S[x]$.
Potom $dt\overline{f}(x) = df(x) = c \cdot \overline{p}_1(x) \cdots \overline{p}_r(x)$ v $S[x]$.
Polynom $\overline{f}(x)$ je primitivní, polynom $\overline{p}_1(x) \cdots \overline{p}_r(x)$ je primitivní podle Gaussova lemmatu.
Podle lemmatu 11.1 existuje $u \in U(S)$ tak, že $u(dt) = c$, tedy $d|c$. Tím existuje prvek $\overline{c} \in S$ tak, že $d\overline{c} = c$. Potom $dt\overline{f}(x) = d\overline{c} \cdot \overline{p}_1(x) \cdots \overline{p}_r(x)$ v $S[x]$, a proto v oboru integrity $S[x]$ máme $f(x) = t\overline{f}(x) = \overline{c} \cdot \overline{p}_1(x) \cdots \overline{p}_r(x)$, neboť $d \neq 0$.
Prvek $\overline{c} \in S$, $\overline{c} \neq 0$ a S je Gaussův obor integrity, proto existuje kanonický rozklad prvku

$\overline{c}$ v S, tedy $\overline{c} = uq_1 \cdots q_s$, kde $u \in U(S)$, $q_1, ..., q_s$ jsou ireducibilní v S.
Potom $f(x) = uq_1 \cdots q_s \overline{p}_1(x) \cdots \overline{p}_r(x)$.
Podle věty 11.1 je $u \in U(S[x])$ a podle věty 11.2 jsou polynomy $q_1(x) = q_1, ..., q_s(x) = q_s$ ireducibilní v $S[x]$.
Pro každé $i = 1, ..., r$ je polynom $p_i(x)$ jsou ireducibilní v $T[x]$, $p_i(x) = c_i/d_i \cdot \overline{p}_i(x)$, proto $\overline{p}_i(x)$ je ireducibilní v $T[x]$. Polynom $\overline{p}_i(x)$ je primitivní v $S[x]$, proto podle věty 11.2 je polynom $\overline{p}_i(x)$ ireducibilní v $S[x]$ pro každé $i = 1, ..., r$. Tím $f(x) = uq_1 \cdots q_s \overline{p}_1(x) \cdots \overline{p}_r(x)$ je kanonický rozklad prvku $f(x)$ v $S[x]$.
Jednoznačnost. Mějme v $S[x]$ dva kanonické rozklady
$f(x) = up_1 \cdots p_s \overline{p}_1(x) \cdots \overline{p}_r(x) = vq_1 \cdots q_t \overline{q}_1(x) \cdots \overline{q}_m(x)$,
kde $u, v \in U(S[x]), p_1, ..., p_s, \overline{p}_1(x), ..., \overline{p}_r(x), q_1, ..., q_t, \overline{q}_1(x), ..., \overline{q}_m(x)$ jsou ireducibilní v $S[x]$, $\mathrm{st}(p_1) = 0, ..., \mathrm{st}(p_s) = 0$, $\mathrm{st}(\overline{p}_1) \geq 1, ..., \mathrm{st}(\overline{p}_r) \geq 1$, $\mathrm{st}(q_1) = 0, ..., \mathrm{st}(q_t) = 0$, $\mathrm{st}(\overline{q}_1) \geq 1$, $..., \mathrm{st}(\overline{q}_m) \geq 1$. Tím $p_1, ..., p_s, q_1, ..., q_t \in S$. Podle věty 11.2 jsou prvky $p_1, ..., p_s, q_1, ..., q_t$ ireducibilní v S, prvky $\overline{p}_1(x), ..., \overline{p}_r(x), \overline{q}_1(x), ..., \overline{q}_m(x)$ primitivní v $S[x]$ a ireducibilní v $T[x]$, kde T je podílové těleso oboru integrity S.
Protože $f(x) = (up_1 \cdots p_s)\overline{p}_1(x) \cdots \overline{p}_r(x) = (vq_1 \cdots q_t)\overline{q}_1(x) \cdots \overline{q}_m(x)$, a protože podle Gaussova lemmatu jsou polynomy $(\overline{p}_1(x) \cdots \overline{p}_r(x))$, $(\overline{q}_1(x) \cdots \overline{q}_m(x))$ primitivní, existuje podle lemmatu 11.1 prvek $w \in U(S)$ tak, že $up_1 \cdots p_s = wvq_1 \cdots q_t$. Tím máme dva kanonické rozklady prvku v Gaussově oboru integrity S, tedy existuje bijekce
$\varphi\colon \{1, ..., s\} \longrightarrow \{1, ..., t\}$ taková, že pro každé $i = 1, ..., s$ je $p_i \sim q_{\varphi(i)}$.
Proto existují $u_i \in U(S)$, tedy $u_i \in U(S[x])$ tak, že $p_i = u_i q_{\varphi(i)}$. Potom pro každé $i = 1, ..., s$ je $p_i \sim q_{\varphi(i)}$ v $S[x]$.
$f(x) = (vq_1 \cdots q_t)\overline{q}_1(x) \cdots \overline{q}_m(x) = (up_1 \cdots p_s)\overline{p}_1(x) \cdots \overline{p}_r(x) = (wvq_1 \cdots q_t)\overline{p}_1(x) \cdots \overline{p}_r(x)$
Tím v oboru integrity $S[x]$ máme $\overline{q}_1(x) \cdots \overline{q}_m(x) = w\overline{p}_1(x) \cdots \overline{p}_r(x)$, neboť $vq_1 \cdots q_t \neq 0$.
Protože $S[x] \subseteq T[x]$, a protože polynomy $\overline{p}_i(x)$, a $\overline{q}_j(x)$ jsou ireducibilní v $T[x]$ pro každé i, j, jsou to dva kanonické rozklady jediného prvku v Gaussově oboru integrity $T[x]$, existuje tedy bijekce $\psi\colon \{1, ..., r\} \longrightarrow \{1, ..., m\}$ taková, že pro každé $i = 1, ..., r$ máme $\overline{p}_i(x) \sim \overline{q}_{\psi(i)}(x)$ v $T[x]$. Tím existuje $z_i \in U(T[x])$ tak, že $\overline{p}_i(x) = z_i \overline{q}_{\psi(i)}(x)$. Protože tyto polynomy jsou primitivní v $S[x]$, existují podle lemmatu 11.1 prvky $y_i \in U(S)$ tak, že $1 \cdot y_i = z_i$ pro každé i. Tím $z_i \in U(S)$, a tedy $\overline{p}_i(x) \sim \overline{q}_{\psi(i)}(x)$ v $S[x]$.
Zobrazení $\alpha\colon \{1, ..., s, 1, ..., r\} \longrightarrow \{1, ..., t, 1, ..., m\}$ definované předpisem

$$\alpha(i) = \begin{cases} \varphi(i) & \text{pro } i = 1, ..., s \\ \psi(i) & \text{pro } i = 1, ..., r \end{cases}$$

zaručuje jednoznačnost kanonického rozkladu v $S[x]$.

■

Důsledek 5 Jestliže S je Gaussův obor integrity, potom $S[x_1, x_2, ..., x_n]$ je také Gaussův obor integrity.

Lemma 11.4 (Eisensteinovo lemma)
Nechť S je Gaussův obor integrity, nechť $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n$ je primitivní polynom v $S[x]$, $\mathrm{st}(a) = n \geq 1$, nechť $p \in S$ je prvek ireducibilní v S takový, že $p | a_i$ pro každé $i = 0, 1, ..., n-1$, $p^2 \nmid a_0$, $p \nmid a_n$. Potom $a(x)$ je ireducibilní v $S[x]$.

Důkaz Předpokládejme, že polynom $a(x)$ není ireducibilní, potom $a(x) = b(x)c(x)$, kde $b(x), c(x) \in S[x]$, $b(x) \not\sim 1$, $c(x) \not\sim 1$, $b(x) \not\sim a(x)$, $c(x) \not\sim a(x)$, $b(x) \neq 0$, $c(x) \neq 0$. Tím $\mathrm{st}(b) \geq 0$, $\mathrm{st}(c) \geq 0$.
Je-li $\mathrm{st}(b) = 0$, potom $b(x) = b_0$, tím $\mathrm{st}(c) = n$. Označíme-li $c(x) = c_0 + c_1x + \cdots + c_nx^n$, pak $a(x) = b_0c_0 + b_0c_1x + \cdots + b_0c_nx^n$. Protože však polynom $a(x)$ je primitivní, získáváme $1 \sim (a_0, a_1, ..., a_n) \sim (b_0c_0, b_0c_1, ..., b_0c_n) \sim b_0(c_0, c_1, ..., c_n)$. Tím $b(x) = b_0 \sim 1$, což je spor. Proto $\mathrm{st}(b) \geq 1$.
Stejně dojdeme ke sporu, je-li $\mathrm{st}(c) = 0$. Proto $\mathrm{st}(c) \geq 1$.
Nechť tedy $b(x) = b_0 + b_1x + \cdots + b_mx^m$, $c(x) = c_0 + c_1x + \cdots + c_kx^k$, kde $m \geq 1$, $k \geq 1$. Potom pro každé $r = 0, 1, ..., n$ je $a_r = \sum_{i+j=r} b_ic_j$. Pro $r = 0$ je $a_0 = b_0c_0$, a protože $p|a_0$ musí v Gaussově oboru integrity $p|b_0$ nebo $p|c_0$. Protože $p^2 \not| a_0$, pak buď $p|b_0$, $p \not| c_0$ nebo $p|c_0$, $p \not| b_0$.
Nechť tedy např. $p|b_0$, $p \not| c_0$.
Ukážeme matematickou indukcí, že potom $p|b_i$ pro každé $i = 0, 1, ..., m$.
Pro $i = 0$ máme $p|b_0$. Nechť $p|b_i$ pro každé $i = 0, ..., r-1$, potom pro
$a_r = \sum_{i+j=r} b_ic_j = (b_0c_r + b_1c_{r-1} + \cdots + b_{r-1}c_1) + b_rc_0$ máme $p|(b_0c_r + b_1c_{r-1} + \cdots + b_{r-1}c_1)$.
Protože $r \leq m < m + k = n$, neboť $k \geq 1$, pak podle předpokladu lemmatu $p|a_r$.
Tím $p|(b_rc_0)$, a protože $p \not| c_0$, nutně $p|b_r$.
Tím $p|b_i$ pro každé $i = 0, 1, ..., m$, a tedy existují prvky $b'_i \in S$ tak, že $pb'_i = b_i$. Potom $b(x) = p(b'_0 + b'_1x + \cdots + b'_mx^m)$, a tím $a_n = a_{m+k} = b_mc_k = pb'_mc_k$, což je spor, neboť $p \not| a_n$.
Stejným způsobem dojdeme ke sporu, jestliže $p|c_0$, $p \not| b_0$. Proto polynom $a(x)$ je ireducibilní v $S[x]$.

■