Komutativní okruhy

Vítězslav Kala

6. května 2020

Obsah

Úvod

Toto je pracovní verze skript k přednášce Komutativní okruhy, určitě obsahuje netriviální množství překlepů a nedokonalostí – budu rád za jakékoli připomínky a komentáře.

Jejich cílem je být poměrně minimalistickým shrnutím probrané látky (v rozsahu mé výuky z let 2017 – 2019), jež blízce kopíruje průběh přednášek a nezahrnuje téměř žádné rozšiřující informace.
Materiál v těchto skriptech a jeho prezentace není vůbec původní: 1. a 2. kapitola jsou založené na skriptech Aleše Drápala [Dr] a částečně Davida Stanovského [St], 3. kapitola na knížce Williama Fultona [Fu] a 4. kapitola na textu Keitha Conrada [Co].
Závěrečná 5. kapitola skript shrnuje průběh přednášky, cvičení a domácích úkolů v roce 2019/2020. Tyto přednášky byly nahrávané a jsou k dispozici tady:
https://is.mff.cuni.cz/prednasky/prednaska/NMAG301/

Za sepsání skript děkuju Jakubu Novákovi; za upozorňování na chyby a překlepy děkuju studentům, kteří přednášku absolvovali v zimním semestru 2019/2020. I přes naši snahu v současné verzi nepochybně obsahují řadu chyb, překlepů a nejasností, takže uvítám jakékoli komentáře a návrhy na zlepšení. Časem do nich snad přibude aspoň trocha vysvětlujících a motivujících komentářů.

[Co] Keith Conrad, *Factoring in quadratic fields*
http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/quadraticgrad.pdf

[Dr] Aleš Drápal, *Komutativní okruhy*
http://www.karlin.mff.cuni.cz/~zemlicka/11-12/komalg.pdf

[Fu] William Fulton, *Algebraic curves*
http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf

[St] David Stanovský, *Základy algebry*, kapitola o Galoisově teorii
http://www.karlin.mff.cuni.cz/~stanovsk/vyuka/alg_galois.pdf

1. Základy

1.1 Úvod

Značení:
Ve skriptech používáme následující značení, které je na MFF spíše neobvyklé.

- $A \subset B$ značí neostrou inkluzi, tedy může být i $A = B$. Ostrou inkluzi značíme $A \subsetneq B$
- Invertibilní prvky v okruhu značíme $R^\times$ místo R^*
- Nepoužíváme značení $\mathbb{Z}_n$, místo toho $\mathbb{Z}/n = \mathbb{Z}/(n)$ (což si lze představovat jako množinu $\{0, 1, \ldots, n-1\}$ s operacemi uvažovanými modulo n)
- $\left(\mathbb{Z}/(n)\right)^\times$ = čísla nesoudělná s n modulo n
- velikost množiny M značíme $\#M$
- $A \twoheadrightarrow B$ značí surjekci (a často surjektivní homorfismus)
- $A \hookrightarrow B$ značí vnoření (a často injektivní homorfismus)

1.2 Ideály a faktorokruhy

Okruhem rozumíme $R(+, -, 0, \cdot)$, přičemž $+$ i $\cdot$ jsou komutativní.
S výjimkou této sekce vždy předpokládáme, že okruhy vždy mají 1.

Mějme okruh R. Ideál I je neprázdná podmnožina R taková, že:

- $a, b \in I \Rightarrow a + b, a - b \in I$
- $a \in I, r \in R \Rightarrow ra \in I$

Ideály značíme $I < R$.
Obvykle se v definici také zahrnuje podmínka, že $0 \in I$: ta ale vyplývá z ostatních dvou.
Podobně pokud $1 \in R$, pak také $-1 \in R$ a tedy $-b \in I$ (2. podmínka), takže $a - b \in I$ vyplývá z 1. podmínky.

Definice. Definujme relaci $a \sim b \Leftrightarrow a - b \in I$ (někdy se značí $a \equiv b \mod I$). Jde o ekvivalenci.
Třídy značíme $[a] = a + I := \{a + i \mid i \in I\}$
Pokud totiž $b \in [a]$, pak $b - a \in I$ (z def.), tedy $b \in a + I = \{a + i \mid i \in I\}$.

Definice. Množina tříd ekvivalence podle ideálu I je *faktorokruh* a značí se R/I.
Na třídách definujeme $+, \cdot$
$(a+I)+(b+I) := (a+b)+I$
$(a+I)\cdot(b+I) := (a\cdot b)+I$
$0_{R/I} = 0+I, 1_{R/I} = 1+I, -(a+I) = (-a)+I$

Příklad. $R = \mathbb{Z}, I = 6\mathbb{Z} = \{\dots, -6, 0, 6, 12, \dots\}$
$a \sim b \Leftrightarrow a-b \in 6\mathbb{Z} \Leftrightarrow a \equiv b \pmod 6$
Třídy:
$0+6\mathbb{Z}, 1+6\mathbb{Z}, \dots, 5+6\mathbb{Z}$
$R/I = \mathbb{Z}/6\mathbb{Z}$ má 6 prvků: je to obvyklé $\mathbb{Z}/6$

Příklad. R okruh, I, J ideály v R takové, že $J \subset I$

a) Pak J je ideál v I. (I je okruh, typicky bez 1)
Ověřujme: Uzavřenost J na sčítání a odčítání: OK (protože je to ideál v R).
Uzavřenost J na násobení prvky I: OK (protože $I \subset R$ a J je ideál v R)

b) I/J je ideál v R/J.
Ověřujme:
$R/J = \{a+J \mid a \in R\}$
$I/J = \{i+J \mid i \in I\} \subset R/J$

I/J uzavřené na $+$:
Ať $a+J, b+J \in I/J$.
Pak $a \in I, b \in I$, a tedy $a+b \in I$.
Tedy $(a+J)+(b+J) = (a+b)+J \in I/J$.
(Odčítání zcela analogicky.)

I/J uzavřené na $\cdot$ prvky R/J čili:
Pokud $a+J \in I/J, r+J \in R/J$, pak chci $(a+J)(r+J) = ar+J \in I/J$ (CVIČENÍ)

$\varphi\colon R \to S$ homomorfismus okruhů.
$R > \operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\}$
$\operatorname{Im}\varphi = \{\varphi(r) \mid r \in R\} \subset S$

Věta 1.1 (O homomorfismu)**.** *Buď $\varphi\colon R \to S$ homomorfismus okruhů, $I < R$ ideál takový, že $I \subset \operatorname{Ker}\varphi$. Pak*

$$\psi\colon R/I \to S$$
$$a+I \mapsto \varphi(a)$$

je dobře definovaný homomorfismus okruhů. Navíc $\operatorname{Ker}\psi = \operatorname{Ker}\varphi/I$ a $\operatorname{Im}\psi = \operatorname{Im}\varphi$.

Důkaz. 1) Dobře definované: Ať $a+I = b+I$, čili $b = a+i, i \in I$. Pak $\psi(b+I) = \varphi(b) = \varphi(a)+\varphi(i) \overset{i\in\operatorname{Ker}\varphi}{=} \varphi(a)+0 = \varphi(a) = \psi(a+I)$.

2) Homomorfismus: Potřebujeme ověřit, že zachovává $+, \cdot$ (a $-$ v případě okruhu bez 1):

Mějme $(a+I)(b+I) = ab+I$. Pak $\psi((a+I)(b+I)) = \psi(ab+I) = \varphi(ab) \overset{\varphi\text{hom.}}{=} \varphi(a)\varphi(b) = \psi(a+I)\psi(b+I)$.
$+, -$ se ověří podobně.

3)Im jasný.
I ideál v $\operatorname{Ker}\varphi, \psi(a+I) = 0 \Leftrightarrow \varphi(a) = 0$. Tedy
${}^{\operatorname{Ker}\varphi}/_{I} = \{a+I \mid a \in \operatorname{Ker}\varphi\} = \operatorname{Ker}\psi$. □

Věta 1.2 (1. věta o izomorfismu). *Buď $\varphi\colon R \to S$ (okruhový) homomorfismus. Pak ${}^{R}/_{\operatorname{Ker}\varphi} \simeq \operatorname{Im}\varphi$.*

Důkaz. Zvolme $I = \operatorname{Ker}\varphi$ ve větě o homorfismu 1.1. Máme homomorfismus $\psi\colon {}^{R}/_{\operatorname{Ker}\varphi} \to S$.
Jeho obraz $\operatorname{Im}\psi = \operatorname{Im}\varphi$, a tedy $\psi\colon {}^{R}/_{\operatorname{Ker}\varphi} \twoheadrightarrow \operatorname{Im}\varphi$.
Je ψ prosté? Homomorfismus je prostý, pokud $\psi(\alpha) = 0 \Leftrightarrow \alpha = 0$. Mějme tedy $\alpha = a + \operatorname{Ker}\varphi$. $0 = \psi(a+\operatorname{Ker}\varphi) = \varphi(a) \Rightarrow a \in \operatorname{Ker}\varphi \Rightarrow a + \operatorname{Ker}\varphi = \operatorname{Ker}\varphi = [0]$. □

Věta 1.3 (2. věta o izomorfismu). *R okruh, I, J ideály takové, že $J \subset I$. Pak $J < I, {}^{I}/_{J} < {}^{R}/_{J}$ a $\left({}^{R}/_{J}\right)/\left({}^{I}/_{J}\right) \simeq {}^{R}/_{I}$.*

Důkaz. Uvažujme projekci

$$\begin{aligned}\varphi\colon R &\twoheadrightarrow {}^{R}/_{I},\\ a &\mapsto a + I.\end{aligned}$$

Zřejmě je surjektivní a $\operatorname{Ker}\varphi = I$.
Podle věty o homorfismu 1.1 pro φ a $J \subset R$ (již můžeme použít, protože $J < \operatorname{Ker}\varphi = I$), máme $\exists\, \psi\colon {}^{R}/_{J} \to {}^{R}/_{I}$. Navíc $\operatorname{Im}\psi = \operatorname{Im}\ \varphi = {}^{R}/_{I}, \operatorname{Ker}\psi = {}^{\operatorname{Ker}\varphi}/_{J} = {}^{I}/_{J}$. Tedy podle věty 1.2 máme $\left({}^{R}/_{J}\right)/_{\operatorname{Ker}\psi} \simeq \operatorname{Im}\psi$. □

Důsledek 1.4. *Buď R okruh a J ideál. Všechny ideály v ${}^{R}/_{J}$ jsou právě ${}^{I}/_{J}$, kde I je ideál v R takový, že $J \subset I$.*

Důkaz. Víme, že ${}^{I}/_{J} < {}^{R}/_{J}$ díky příkladu výše.
Naopak, buď I_0 ideál v ${}^{R}/_{J}$. Chceme dokázat, že $I_0 = {}^{I}/_{J}$ pro nějaké I. Prvky I_0 jsou tvaru $a + J$, takže dává smysl definovat $I := \{a \in R \mid a + J \in I_0\}$, zřejmě $J \subset I$.
Chceme:
1) I je ideál v R:
Ať $a, b \in I$, $r \in R$. Pak $a + J, b + J \in I_0$, tedy $a + b + J \in I_0$, čili $a + b \in I$. Stejně pro $ra \in I$.
2) ${}^{I}/_{J} \simeq I_0$:
Stačí uvažovat zobrazení $I \to I_0, a \mapsto a + J$ a použít 1. větu o izomorfismu 1.2. □

Věta 1.5 (3. věta o izomorfismu). *R okruh, $I < R$ ideál, $S \subset R$ podokruh. Pak $S + I = \{s + a \mid s \in S, a \in I\}$ je podokruh v R a ${}^{(S+I)}/_{I} \simeq {}^{S}/_{(S\cap I)}$*

Důkaz. CVIČENÍ. (Projekce $\pi\colon R \twoheadrightarrow {}^{R}/_{I}$ a její zúžení na $\varphi\colon S \to {}^{R}/_{I}$. 1. věta o izomorfismu pro φ.) □

1.3 Prvoideály a maximální ideály

Definice. R okruh. $I < R$ je vlastní ideál, pokud $I \neq R$.
Vlastní ideál I je maximální, pokud neexistuje vlastní ideál $J < R$ takový, že $I \subsetneq J$.
Pro ideály I, J definujeme $IJ = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J, n \in \mathbb{N} \right\}$.
Vlastní ideál P je prvoideál, pokud pro všechny ideály $I, J < R$ platí $IJ \subset P \Rightarrow I \subset P$ nebo $J \subset P$.
Ideál I je hlavní, pokud $\exists a \in R$ takový, že $I = (a) = aR$.

Příklad. $R = \mathbb{Z}$. Všechny ideály v $\mathbb{Z}$ jsou tvaru $I = (n) = n\mathbb{Z} = \{\dots, -n, 0, n, 2n, \dots\}$, kde $n = 0, 1, 2, \dots$
Zřejmě $(n) = (-n)$.
Dělitelnost čísel $2 \mid 6$ odpovídá obrácené inkluzi ideálů $(2) \supset (6)$.

Pokud tedy $I = (a), J = (b)$ a $P = (p)$, pak máme:
$IJ = (ab)$
$(p) \supset (ab) \Leftrightarrow p \mid ab$
$(p) \supset (a) \Leftrightarrow p \mid a$
$(p) \supset (b) \Leftrightarrow p \mid b$
Tedy $P = (p)$ prvoideál $\Leftrightarrow |p|$ prvočíslo.
$5\mathbb{Z}$ je prvoideál, ale $10\mathbb{Z}$ ne, protože $(2) \cdot (5) \subset (10)$, ale $(2) \not\subset (10)$ a $(5) \not\subset (10)$.

Lemma 1.6. *Vlastní ideál I v okruhu R je prvoideál, právě když pro každé dva prvky $a, b \in R$ platí $ab \in I \Rightarrow a \in I$ nebo $b \in I$.*

Důkaz. „$\Rightarrow$“ Ať je I prvoideál a ať $ab \in I$. Pak $(aR)(bR) = (abR) \subset I$. Podle definice tedy máme $aR \subset I$ nebo $bR \subset I$, a tedy $a \in I$ nebo $b \in I$.

„$\Leftarrow$“ Ať J_1, J_2 jsou ideály takové, že $J_1 J_2 \subset I$. Předpokládejme, že $J_2 \not\subset I$, tedy že existuje $b \in J_2 \setminus I$. Pro každé $a \in J_1$ máme $ab \in J_1 J_2 \subset I$, a tedy $a \in I$ nebo $b \in I$. Ovšem $b \notin I$, a tedy $a \in I$ pro každé $a \in J_1$. Z toho vyplývá $J_1 \subset I$, jak jsme chtěli. □

Definice. S je obor (integrity), pokud $\forall a, b \in S$ platí $ab = 0 \Rightarrow a = 0$ nebo $b = 0$.

Pozorování. Okruh R je těleso $\Leftrightarrow (0)$ je jediný vlastní ideál.
Prvek a je invertibilní $\Leftrightarrow (a) = aR = R$.

Důsledek 1.7. *Ať I je vlastní ideál v R. Pak:*
a) I je maximální $\Leftrightarrow R/I$ je těleso
b) I je prvoideál $\Leftrightarrow R/I$ je obor.

Důkaz. a)
„$\Rightarrow$“ I maximální $\Rightarrow$ jediný vlastní ideál okruhu R, který je mezi R a I je samo I.
Důsledek 1.4 $\Rightarrow$ ideály R/I jsou právě J/I, kde $J \supset I$. Tedy může být jenom $J = I$ a $J = R$. Ale $R/I < R/I$ je nevlastní ideál a $R/R (= 0_{R/I}) < R/I$
Pozorování $\Rightarrow R/I$ je těleso.
„$\Leftarrow$“ Stejně R/I těleso $\Rightarrow (0_{R/I})$ jediný vlastní ideál v R/I.
Důsledek 1.4 $\Rightarrow$ jediné vlastní ideály v R, které obsahují I, jsou I a $R \Rightarrow I$ maximální.

b)
„$\Rightarrow$“ I prvoideál. Ať $a+I, b+I \in {}^{R}/_{I}$ jsou takové, že $ab+I = (a+I)(b+I) = 0_{R/I} = I$. Tedy $ab \in I$. Podle lemmatu 1.6 pak máme $a \in I \Rightarrow a+I = I = 0_{R/I}$ nebo $b \in I \Rightarrow b+I = 0_{R/I}$, čili jsme ověřili definici oboru.
„$\Leftarrow$“ Ať je ${}^{R}/_{I}$ obor a $ab \in I$. Chceme (podle lemmatu 1.6), že $a \in I$ nebo $b \in I$.
$ab \in I \Rightarrow I = ab + I = (a+I)(b+I) \overset{R/I \text{ obor}}{\Rightarrow} a+I = I$ nebo $b+I = I \Rightarrow a \in I$ nebo $b \in I$. □

1.4 Hlavní ideály a dělitelnost

Definice. Buď R okruh.
$a \mid b \Leftrightarrow \exists c : b = ac$
$a \parallel b \Leftrightarrow a \mid b$ a $b \mid a$

Pozorování. $a \mid b \Leftrightarrow (a) \supset (b), a \parallel b \Leftrightarrow (a) = (b)$

Definice. Obor R je gaussovký, pokud $\forall a \in R, a \neq 0$, má jednoznačný rozklad na součin ireducibilních prvků, čili $a \parallel p_1^{k_1} \cdots p_n^{k_n}$, kde $n \geq 0, k_i \geq 1$ a p_i jsou ireducibilní prvky takové, že $p_i \nparallel p_j$.

Poznámka. Buď R obor. Pak R gaussovký právě tehdy, když:

1. existuje NSD všech dvojic prvků a
2. neexistuje posloupnost prvků $a_1, a_2, .. \in R$ takových, že $a_{i+1} \mid a_i$ a $a_{i+1} \nparallel a_i$.

Příklad. $\mathbb{Z}, \mathbb{Z}[x], \mathbb{Q}[x], \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$ jsou gaussovské.
$\mathbb{Z}[\sqrt{D}]$ pro $D < 0$ skoro nikdy není: je gaussovský, právě když $D = -1, -2$.
$\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ pro $D < 0$ je gaussovský, právě když $D = -3, -7, -11, -19, -43, -67, -163$.
Jestli $\mathbb{Z}[\sqrt{D}]$ pro $D > 0$ je gaussovský pro nekonečně mnoho D je slavný otevřený problém, očekává se, že ano.

Definice. Obor R je obor hlavních ideálů (OHI), pokud je každý ideál hlavní, čili $\forall I < R, \exists a \in R : I = (a)$.

Definice. $I + J = \{a + b \mid a \in I, b \in J\}$

Tvrzení 1.8. *Buď R OHI. Potom R je gaussovský a platí Bezoutova rovnost $\forall a, b \in R\ \exists r, s \in R : \mathrm{NSD}(a, b) = ar + bs$.*

Důkaz. Ověříme dvě podmínky z poznámky uvedené výše:
1) Existence NSD: Pro $a, b \in R$ uvažujme ideál $(a)+(b)$. Jsme v OHI $\Rightarrow \exists c : (a)+(b) = (c)$. Máme $(a) \subset (c) \Rightarrow c \mid a$ a $(b) \subset (c) \Rightarrow c \mid b$.
Je-li d společný dělitel a, b, pak $(a) \subset (d), (b) \subset (d) \Rightarrow (c) = (a)+(b) \subset (d) \Rightarrow d \mid c$. Tedy c je *největší* společný dělitel. Bezoutova rovnost plyne z $(a) + (b) = (c)$.
2) Sporem, ať máme $\ldots a_{i+1} \mid a_i \mid a_{i-1} \mid \cdots \mid a_1$. Tedy $(a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq (a_i) \subsetneq \ldots$ je řetězec hlavních ideálů. Uvažme $I = \bigcup_{i=1}^{\infty} (a_i)$, což je ideál (cvičení).
OHI $\Rightarrow \exists a \in R : I = (a)$.
$a \in \bigcup_{i=1}^{\infty} (a_i) \Rightarrow \exists i : a \in (a_i)$. Tedy $a \in (a_j)\ \forall j \geq i$ a $(a) \subset (a_i) \subsetneq (a_j) \subset \bigcup_{i=1}^{\infty} (a_i) = (a)$. Spor. □

1.5 Noetherovskost

Definice. Okruh R je noetherovský, pokud neobsahuje nekonečný rostoucí řetězec ideálů $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$.

Například těleso je vždy noetherovské (protože obsahuje jen dva ideály).
Definice připomíná $\dots \mid a_3 \mid a_2 \mid a_1 \Rightarrow (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$

Tvrzení 1.9. *Obory hlavních ideálů jsou noetherovské.*

Důkaz. Buď R OHI. Ať není noetherovský. Tedy existuje $I_1 \subsetneq I_2 \subsetneq \dots$. Uvažujme $I := \bigcup_{j=1}^{\infty} I_j$, což je ideál (cvičení). OHI $\Rightarrow I$ je hlavní, $I = (a)$.
$a \in I = \bigcup I_j \Rightarrow \exists j : a \in I_j$. Máme $I_j \subset I_{j+1} \Rightarrow a \in I_{j+1} \Rightarrow (a) \subset I_j \subset I_{j+1} \subset I = (a) \Rightarrow$
$\Rightarrow$ všude rovnosti $\Rightarrow I_j = I_{j+1}$. Spor. □

$$\text{Euklidovský} \Rightarrow \begin{cases} \text{OHI} \Rightarrow \text{ gaussovský} \\ \text{noetherovský} \end{cases}$$

$\mathbb{Z}[\sqrt{-2019}]$ noetherovský, ale není gaussovský.
$R = K[X, Y]$ gaussovský, noetherovský, ne OHI.
$R = K[X_1, X_2, X_3, \dots]$ Gaussovský, ale *není* noetherovský.

Definice. Buď R okruh. R-modul M je abelovská grupa $M(+, -, 0)$ spolu se skalárním násobením $r \cdot m \in M$ pro $r \in R, m \in M$ takovým, že $\forall r, s \in R, \forall m, n \in M$:

- $r(m + n) = rm + rn$
- $r(sm) = (rs)m$
- $(r + s)m = rm + sm$
- $1m = m$

Jedná se o podobný pojem jako vektorový prostor, ale nad okruhem.
Pokud je R těleso, pak je R-modul totéž, co R-vektorový prostor.

Příklad.

- Každá abelovská grupa G je $\mathbb{Z}$-modul.
  $im = m + m + \dots + m, i \in \mathbb{N}, m \in G$
  $(-i) \cdot m = -(im)$
- R je R-modul
- $I < R \Rightarrow I$ je R-modul

Definice. R-modul M je noetherovský, pokud neexistuje nekonečná posloupnost $M_1 \subsetneq M_2 \subsetneq \dots$ R-podmodulů v M.

Pozorování. Okruh R je noetherovský okruh $\Leftrightarrow R$ je noetherovský R-modul.

Definice. Buď M R-modul a $X \subset M$ jeho podmnožina. Množina všech konečných sum $\sum_{i=1}^{k} r_i x_i$, pro $r_i \in R, x_i \in X$ je nejmenší R-podmodul v M, který obsahuje X. Nazývá se podmodul generovaný X.
Pokud existuje *konečná* množina X, která generuje M, pak M je konečně generovaný R-modul.

Definice. Mějme prvky $r_1, \dots, r_k$ v okruhu R. Ideál jimi generovaný značíme $(r_1, \dots, r_k) = r_1R + \dots + r_kR$ (zároveň jde o nejmenší ideál, který obsahuje dané prvky).

Tvrzení 1.10. *R-modul M je noetherovský $\Leftrightarrow$ každý R-podmodul $N \subset M$ je konečně generovaný.*

Důkaz.
„$\Leftarrow$" Sporem: Mějme posloupnost $M_1 \subsetneq M_2 \subsetneq \dots$
Pak $N = \bigcup\limits_{i=1}^{\infty} M_i$ je R-modul $\Rightarrow$ N je konečně generovaný nějakými prvky $n_1, n_2, \dots, n_k$.
$N = \bigcup M_i \Rightarrow \exists j$ takové, že $n_1, \dots, n_k \in M_j$
$\Rightarrow$ R-modul generovaný $n_1, \dots, n_k$ je podmnožina $M_j \Rightarrow N \subset M_j$.
Máme tedy $N \subset M_j \subsetneq M_{j+1} \subset N$. Spor.
„$\Rightarrow$" Sporem: Ať $N \subset M$ je R-podmodul, který není konečně generovaný.
Buď $M_0 = \{0\}$. Postupně volme $m_i \in N \setminus M_i$ a definujme $M_{i+1} := M_i + R \cdot m_i$, což jde, protože M_i je konečně generovaný a N není konečně generovaný, tedy $M_i \subsetneq N$. (Striktně vzato k zajištění existence této posloupnosti potřebujeme axiom výběru.)
Vyrobili jsme nekonečnou posloupnost $M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots$, což je spor. $\square$

Věta 1.11 (Hilbertova věta o bázi)**.** *Okruh R je noetherovský, právě když je $R[x]$ noetherovský.*

Důkaz. „$\Leftarrow$" cvičení.
„$\Rightarrow$" Ať R je noetherovský a $R[x]$ není. Podle tvrzení 1.10 pak existuje $R[x]$-podmodul v $R[x]$, který není konečně generovaný, neboli existuje ideál $I < R[x]$, který není konečně generovaný.
Buď $f_0 \in I$ nenulový polynom nejmenšího stupně a f_{i+1} nějaký polynom nejmenšího stupně v $I \setminus (f_0, f_1, \dots, f_i)$. Zřejmě $\deg f_0 \leq \deg f_1 \leq \dots$.
Buď a_i vedoucí koeficient polynomu f_i a $J_i =$ ideál v R generovaný prvky $a_0, \dots, a_i$.
$J_0 \subset J_1 \subset J_2 \dots$ je řetězec v noetherovském okruhu $R \Rightarrow \exists k$: $J_k = J_{k+1} = J_{k+2} = \dots$
Speciálně $\exists r_0, \dots, r_k \in R : a_{k+1} = r_0a_0 + \dots + r_ka_k$.

Buď $d = \deg f_{k+1}$, polynomy $f_0, f_1, \dots f_k$ můžeme vynásobit vhodnými $x^{\text{něco}}$, aby vznikly polynomy $\tilde{f}_0, \dots \tilde{f}_k$, všechny stupně d. Uvažme $g := f_{k+1} - r_0\tilde{f}_0 - \dots - r_k\tilde{f}_k$. Pak máme $\deg g \leq d$, ale koeficient u x^d je $a_{k+1} - r_0a_0 - \dots - r_ka_k = 0 \Rightarrow \deg g < d = \deg f_{k+1}$.
Ale $g \in I \setminus (f_0, \dots, f_k)$, což je spor s volbou f_{k+1} nejmenšího stupně. $\square$

Důsledek 1.12. *Je-li R noetherovský, pak je také $R[x_1, \dots, x_k]$ noetherovský.*

1.6 Ireducibilní polynomy

V celé sekci: R je gaussovský obor a T jeho podílové těleso.

Pro $a \in R$ buď $a \parallel p_1^{k_1} \cdots p_n^{k_n}$ jeho rozklad na prvočinitele, $p_i \nparallel p_j$, pro $i \neq j, k_i \geq 1, n \geq 0$.
Pak $(a) = (p_1)^{k_1} \cdots (p_n)^{k_n}$, protože $(b) \cdot (c) = (bc)$ (cvičení).

Cvičení: p prvočinitel $\Leftrightarrow$ (p) prvoideál.

Definice. Buď p prvočinitel. Pak *p-valuace* prvku $a \in R$ je

- $v_p(a) = \begin{cases} k_i \text{ pokud } \exists i : p \parallel p_i (\Leftrightarrow (p) = (p_i)) \\ 0 \text{ jinak.} \end{cases}$

- $v_p(0) = \infty$.

Pro $t = \frac{a}{b} \in T$ definujeme $v_p(t) := v_p(a) - v_p(b)$.

Zřejmě máme $v_p(uv) = v_p(u) + v_p(v)$, a tedy $v_p(t)$ je dobře definované, protože $v_p(\frac{ca}{cb}) = v_p(ca) - v_p(cb) = v_p(a) - v_p(b) = v_p(\frac{a}{b})$.

Definice. Buď $f(x) = \sum_{i=0}^{d} a_i x^i \in T[x]$ a $p \in R$ prvočinitel.
p-obsah polynomu f je $c_p(f) = \min\{v_p(a_i), 0 \leq i \leq d\}$.
Pro polynom $f \in R[x]$ řekneme, že je primitivní, pokud $\mathrm{NSD}(a_0, \ldots, a_d) = 1$, čili $c_p(f) = 0$ pro všechny ireducibilní prvky $p \in R$.

Lemma 1.13.
a) Ať $u \in T^\times = T \setminus \{0\}$, p je prvočinitel v R a $f \in T[x] \setminus \{0\}$. Pak $c_p(u \cdot f) = c_p(f) + v_p(u)$.
b) Buď $a \in T$. Pak $a \in R$, právě když $v_p(a) \geq 0$ pro všechny ireducibilní prvky $p \in R$.
c) Ať $f \in T[x]$. Pak $f \in R[x]$, právě když $c_p(f) \geq 0$ pro všechny ireducibilní prvky $p \in R$.

Důkaz. a) Platí $v_p(ua_i) = v_p(u) + v_p(a_i)$.
b), c) cvičení. □

Pozorování. $\varphi\colon R \to S$ homomorfismus okruhů. Pak $\exists! \varphi_x\colon R[x] \to S[x]$, který rozšiřuje φ a $\varphi_x(x) = x$.
Speciálně: pro gaussovský obor R a prvočinitel p máme
$\pi\colon R \twoheadrightarrow R/(p)$
$\pi_x\colon R[x] \twoheadrightarrow \left(R/(p)\right)[x]$

Lemma 1.14 (Gaussovo)**.** *Buď R gaussovský obor. Jsou-li primitivní polynomy $f, g \in R[x]$, pak je primitivní i $f \cdot g$.*

Důkaz. Použijeme: h primitivní $\Leftrightarrow c_p(h) = 0, \forall p$.
Buď p prvočinitel. Víme, že $c_p(f) = c_p(g) = 0$ a chceme $c_p(fg) = 0$.
$R/(p)$ obor $\overset{\text{cvičení}}{\Rightarrow} \left(R/(p)\right)[x]$ obor.
Zřejmě platí $c_p(h) = 0 \Leftrightarrow \pi_x(h) \neq 0$.
Tedy $c_p(f) = c_p(g) = 0 \Rightarrow \pi_x(f) \neq 0, \pi_x(g) \neq 0$. Tedy $\pi_x(fg) \overset{\text{hom}}{=} \pi_x(f) \cdot \pi_x(g) \overset{\text{obor}}{\neq} 0$. □

Důsledek 1.15. *Pro $f, g \in T[x] \setminus \{0\}$ a prvočinitele $p \in R$ platí $c_p(fg) = c_p(f) + c_p(g)$.*

Důkaz. Buď $u := \prod p^{-c_p(f)}$ a $v := \prod p^{-c_p(g)}$, kde násobíme po 2 neasociované prvočinitele, a $f_1 := uf, g_1 := vg$.
Máme $c_p(f_1) = 0 = c_p(g_1) \Rightarrow f_1, g_1$ primitivní. Podle lemmatu 1.14 tedy $f_1 g_1$ je primitivní $\Rightarrow c_p(f_1 g_1) = 0$. Ale $f_1 g_1 = uvfg$, takže

$$0 = c_p(f_1 g_1) = v_p(uv) + c_p(fg) = v_p(u) + v_p(v) + c_p(fg) = -c_p(f) - c_p(g) + c_p(fg).$$ □

Tvrzení 1.16. *Buď R gaussovský obor a T jeho podílové těleso. Ireducibilní prvky v $R[x]$ jsou právě*

- *prvočinitele $p \in R$ a*
- *primitivní nekonstantní polynomy $f \in R[x]$, které jsou ireducibilní jako prvky $T[x]$.*

Pro každý ireducibilní polynom $g \in T[x]$ existuje $u \in T$ takové, že ug je ireducibilní prvek okruhu $R[x]$.

Důkaz. Chceme popsat ireducibilní prvky $R[x]$; rozlišme konstantní a nekonstantní polynomy v $R[x]$.

a) $f \in R$ (je konstantní polynom)
Pokud $g \in R[x]$ splňuje $g \mid f$, pak $g \in R$ musí být taky konstantní. Tedy $f \in R$ ireducibilní v okruhu $R[x] \Leftrightarrow f$ je ireducibilní v $R \Leftrightarrow f$ je prvočinitel v R.

b) $f \in R[x]$, $\deg f \geq 1$.

Pozorování: Ať $f \in R[x], \deg f \geq 1$ a f primitivní. Pak f ireducibilní v $R[x] \Leftrightarrow f$ ireducibilní v $T[x]$.

Důkaz pozorování
„$\Leftarrow$“ Lehké cvičení
„$\Rightarrow$“ Ať f není ireducibilní v $T[x]$, čili $f = f_1 f_2$, kde $f_1, f_2 \in T[x]$ nekonstantní.
Podobně jako v důkazu důsledku 1.15 pro $u_1 = \prod p^{-c_p(f_1)}, u_2 = \prod p^{-c_p(f_2)}$ máme: $g_1 := u_1 f_1$ a $g_2 := u_2 f_2$ jsou primitivní polynomy v $R[x]$. Navíc f primitivní $\Rightarrow 0 = c_p(f) = c_p(f_1 f_2) \overset{1.15}{=} c_p(f_1) + c_p(f_2)$.
Tedy $u_1 \cdot u_2 = \prod p^{-(c_p(f_1)+c_p(f_2))} = \prod p^0 = 1$. Tedy $f = f_1 f_2 = (u_1 u_2)^{-1} g_1 g_2 = g_1 g_2 \Rightarrow f$ není ireducibilní v $R[x]$. □

Tedy primitivní polynomy $f \in R[x]$, které jsou ireducibilní v $T[x]$, jsou ireducibilní v $R[x]$.
Naopak buď (nekonstantní) $f \in R[x]$ ireducibilní v $R[x]$. Pak $f = uf_1$, kde $f_1 \in R[x]$ primitivní a $u = \prod p^{c_p(f)} \in R$.
Ale f ireducibilní $\Rightarrow u \parallel 1 \Rightarrow c_p(f) = 0, \forall p \Rightarrow f$ primitivní. Pozorování $\Rightarrow f$ ireducibilní v $T[x]$.

2. část tvrzení: Buď $g \in T[x]$ ireducibilní a definujme $v = \prod p^{-c_p(g)} \Rightarrow vg$ je primitivní prvek $R[x]$ a $vg \parallel g$ v $T[x] \Rightarrow vg$ je ireducibilní v $T[x]$. Pozorování $\Rightarrow vg$ je ireducibilní v $R[x]$. □

Věta 1.17. *Je-li R gaussovský obor, pak je i $R[x]$ gaussovský.*

Důkaz. Použijeme: R gaussovský $\Leftrightarrow$ 1. neexistují nekonečné řetězce vlastních dělitelů a 2. každý ireducibilní prvek je prvočinitel. (cvičení)

1. Ať $\dots f_i \mid f_{i-1} \mid \dots \mid f_2 \mid f_1, f_i \in R[x]$. Pak $\deg f_1 \geq \deg f_2 \geq \dots \geq 0$, a tedy $\exists k : \deg f_k = \deg f_{k+1} = \dots$.
Buď a_i vedoucí koeficient $f_i \Rightarrow \dots \mid a_i \mid a_{i-1} \dots \mid a_2 \mid a_1$. Toto je posloupnost dělitelů v gaussovském $R \Rightarrow \exists l : a_l \parallel a_{l+1} \parallel \dots$
Pro $i, j \geq \max\{k, l\}$ tedy $\deg f_i = \deg f_j$ a $a_i \parallel a_j \Rightarrow f_i \parallel f_j$.

2.Chceme dokázat, že pokud $f \mid gh$ (v $R[x]$), pak $f \mid g$ nebo $f \mid h$ (v $R[x]$). Mějme ireducibilní prvek f v $R[x]$ a použijme tvrzení 1.16, podle nějž máme dvě možnosti:
a) $f = p \in R$. Pak $1 \leq c_p(gh) = c_p(g) + c_p(h)$, a tedy $c_p(g) \geq 1$ nebo $c_p(h) \geq 1$. To implikuje, že $p \mid g$ nebo $p \mid h$.
b) $\deg f \geq 1$ a f je primitivní, ireducibilní v $T[x]$. $T[x]$ je euklidovské, tedy gaussovské, a tedy f je prvočinitel v $T[x]$. Zároveň $f \mid gh$ v $T[x]$.

BÚNO ať $f \mid g$ v $T[x]$, čili $g = qf, q \in T[x]$. f je primitivní, takže $c_p(g) = c_p(q)$ pro všechny p. Ale $g \in R[x]$, tedy $c_p(g) \geq 0$. Tudíž $c_p(q) \geq 0$ a $q \in R[x]$. Tedy jsme dokázali, že $f \mid g$ v $R[x]$. $\square$

1.7 Čínská zbytková věta

Definovali jsme už 3 operace na ideálech $I+J, IJ, I\cap J$, přičemž platí: $I(J+K) = IJ+IK$ a $IJ \subset I \cap J$. (Cvičení)

Definice. Ideály I, J v okruhu R jsou komaximální, pokud $I + J = R$.

Motivace:
1. Pokud je M maximální, tak $M + (a) = R$ pro všechny $a \notin M$. Tedy M, J jsou komaximální $\forall J \not\subset M$.
2. $R = \mathbb{Z}, I = (m), J = (n)$. Pak $(m) + (n) = (\mathrm{NSD}(m, n))$. Tedy $(m), (n)$ jsou komaximální, právě když m, n jsou nesoudělné. Jde tedy o variantu nesoudělnosti a oslabení maximality (která odpovídá prvočíslům, jež jsou nesoudělná se vším).

Lemma 1.18. *I, J komaximální $\Rightarrow I \cap J = IJ$.*

Důkaz. $I \cap J \overset{\text{komaximální}}{=} (I \cap J)(I + J) = (I \cap J)I + (I \cap J)J \subset JI + IJ = IJ.$ $\square$

Definice. Ideály $I_1, \dots, I_n < R$ jsou po dvou komaximální, pokud I_j, I_k jsou komaximální pro všechna $1 \leq j < k \leq n$.

Tvrzení 1.19. *Ať $I_1, \dots, I_n$ jsou po dvou komaximální ideály v okruhu R a $n \geq 2$. Pak $I_1 \cap \dots \cap I_n = I_1 \cdots I_n$ a dvojice $I_1 \cap \dots \cap I_{n-1}, I_n$ je komaximální.*

Důkaz. $I_1 \cdots I_{n-1}$ a I_n jsou komaximální:
Uvažujme

$$\begin{aligned} R =&(I_1 + I_n)(I_2 + I_n) \cdots (I_{n-1} + I_n) \\ =&I_1 I_2 \cdots I_{n-1} + \text{další členy, jež všechny obsahují } I_n \\ \subset&I_1 I_2 \cdots I_{n-1} + I_n \subset R. \end{aligned}$$

tedy $I_1 \cdots I_{n-1} + I_n = R$.

$I_1 \cap \dots \cap I_n = I_1 \cdots I_n$ dokážeme indukcí. Pro $n = 2$ jde o lemma 1.18.
Ať $n > 2$. Indukční předpoklad: $I_1 \cap \dots \cap I_{n-1} = I_1 \cdots I_{n-1}$.
Z 1. části důkazu: $I_1 \cdots I_{n-1}, I_n$ jsou komaximální. Pak

$$(I_1 \cdots I_{n-1}) \cdot I_n \overset{1.18}{=} (I_1 \cdots I_{n-1}) \cap I_n \overset{\text{indukční předpoklad}}{=} (I_1 \cap \dots \cap I_{n-1}) \cap I_n. \quad \square$$

Tvrzení 1.20. *Ať $I_1, \dots, I_n$ jsou ideály v okruhu R. Uvažujme homomorfismus*

$$\begin{aligned} \varphi \colon R &\to R/I_1 \times \dots \times R/I_n \\ r &\mapsto (r + I_1, \dots, r + I_n). \end{aligned}$$

Pak
a) $\operatorname{Ker} \varphi = I_1 \cap \dots \cap I_n$,
b) φ je surjektivní $\Leftrightarrow I_1, \dots, I_n$ jsou po dvou komaximální.

Důkaz. a) je jasné.
b) „⇒“ Ať φ je na a $i \neq j$. Máme

$$R \overset{\varphi}{\twoheadrightarrow} R/I_1 \times \cdots \times R/I_n \twoheadrightarrow R/I_i \times R/I_j \twoheadrightarrow (R/I_i)/(I_i + I_j/I_i) \times \Big(R/I_j\Big)/\Big(I_i + I_j/I_j\Big)$$
$$\overset{1.3}{\simeq} R/I_i + I_j \times R/I_i + I_j.$$

Tedy toto složení je surjektivní, ovšem jde o zobrazení $r \mapsto (r + I_i + I_j, r + I_i + I_j)$, čili v obou složkách obrazu máme stejnou hodnotu. Takovéto zobrazení je surjektivní jen, pokud $R/I_i + I_j$ má jen 1 prvek.
Tedy $I_i + I_j = R$ a I_i, I_j jsou komaximální.

„⇐“ Předpokládejme, že $I_1, \ldots, I_n$ jsou po dvou komaximální. Indukcí:
$n = 2$: Potřebujeme, že každé $(r_1 + I_1, r_2 + I_2)$ leží v $\operatorname{Im}\varphi$, čili že existuje $r \in R$ takové, že $r \equiv r_i \pmod{I_i}$ pro $i = 1, 2$.
Z komaximality vyplývá, že $\exists a_1 \in I_1, a_2 \in I_2$ taková, že $1 = a_1 + a_2$. Zvolme nyní $r := r_1a_2 + r_2a_1$. Pak $r - r_1 = (r_1a_2 + r_2a_1) - r_1(a_1 + a_2) = a_1(r_2 - r_1) \in I_1$. Stejně dostaneme $r - r_2 \in I_2$.

Ať $n \geq 3$. Uvažujme $I := I_1 \cdots I_{n-1} \overset{1.19}{=} I_1 \cap \cdots \cap I_{n-1}$. Z tvrzení 1.19 také vyplývá, že I, I_n jsou komaximální.
Indukční předpoklad pro 2 ideály: máme surjekci

$$\begin{aligned}\psi_1 \colon R &\twoheadrightarrow R/I \times R/I_n,\\ r &\mapsto (r + I, r + I_n).\end{aligned}$$

Pro $n - 1$ máme dále

$$\begin{aligned}\psi_2 : R &\twoheadrightarrow R/I_1 \times \cdots \times R/I_{n-1},\\ r &\mapsto (r + I_1, \ldots, r + I_{n-1}).\end{aligned}$$

s $\operatorname{Ker}\psi_2 = I_1 \cap \cdots \cap I_{n-1} = I$.
1. věta o izomorfismu pro ψ_2 pak dává

$$\begin{aligned}\psi \colon R/I &\simeq R/I_1 \times \cdots \times R/I_{n-1},\\ r + I &\mapsto (r + I_1, \ldots, r + I_{n-1}).\end{aligned}$$

Konečně složením máme

$$\varphi = (\psi \times \mathrm{id}) \circ \psi_1 \colon R \overset{\psi_1}{\twoheadrightarrow} R/I \times R/I_n \overset{\psi\times\mathrm{id}}{\twoheadrightarrow} \big(R/I_1 \times \cdots \times R/I_{n-1}\big) \times R/I_n.$$

□

Důsledek 1.21 (Čínská zbytková věta)**.** *Ať $I_1, \ldots, I_n$ jsou po dvou komaximální ideály v R takové že $I_1 \cap \cdots \cap I_n = \{0\}$. Pak $\forall r_1, \ldots, r_n \in R$ $\exists! r \in R$ takové, že $r \equiv r_i \pmod{I_i}$ pro všechna i.*

Poznámka. Mějme $n_1, \ldots, n_k \in \mathbb{Z}$ po 2 nesoudělná a buď $R = \mathbb{Z}/(n_1 \cdots n_k)$. Pak

$$\mathbb{Z}/(n_1 \cdots n_k) \simeq \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k,$$

což dává obvyklou čínskou zbytkovou větu pro celá čísla.

1.8 Zornovo lemma

Ať je $\mathcal{A}$ množina částečně uspořádané relací $\leq$, čili je

- reflexivní: $x \leq x$,
- (slabě) antisymetrická: $x \leq y$ a $y \leq x \Rightarrow x = y$,
- tranzitivní: $x \leq y \wedge y \leq z \Rightarrow x \leq z$

pro všechna $x, y, z \in \mathcal{A}$.

Řetězec $\mathcal{B}$ v $\mathcal{A}$ je podmnožina, která je lineárně uspořádaná, čili splňuje $\forall x, y \in \mathcal{B} : x \leq y$ nebo $y \leq x$.
Horní mez podmnožiny $\mathcal{C} \subset \mathcal{A}$ je prvek $a \in \mathcal{A}$ takový, že $a \geq c$ pro všechna $c \in \mathcal{C}$.
Prvek $a \in \mathcal{A}$ je maximální, pokud $a \leq b$ implikuje $a = b$ pro všechna $b \in \mathcal{A}$.

Lemma 1.22 (Zornovo lemma)**.** *Buď $\mathcal{A}$ neprázdná množina částečně uspořádaná relací $\leq$ taková, že pro každý řetězec $\mathcal{B}$ v $\mathcal{A}$ existuje horní mez. Pak $\forall a \in \mathcal{A} \exists b \in \mathcal{A}$ takové, že b je maximální v $\mathcal{A}$ a $a \leq b$.*

Toto lemma je ekvivalentní axiomu výběru, který je jedním z klíčových axiomů teorie množin, byť historicky byl poměrně problematický (řada matematiků nepovažovala jeho platnost za samozřejmou). My se ale zajímáme o okruhy a ne o teorii množin, takže budeme s Zornovým lemmatem běžně pracovat (jak je ostatně dnes běžné).

Příklad. Každý vektorový prostor V má bázi.
$\mathcal{A} :=$ {lineárně nezávislé podmnožiny ve V}, $\leq$ je uspořádání inkluzí, čili pro $X, Y \in \mathcal{A}$ definujeme $X \leq Y$, pokud $X \subset Y$.

Teď musíme ověřit předpoklad Zornova lemmatu.
Buď $\mathcal{B} \subset \mathcal{A}$ řetězec. Chceme jeho horní mez:
Volme $b \subset V$ jako $b = \bigcup$ řetězce $\mathcal{B}$, čili $b = \{v \in V \mid \exists a \in \mathcal{B}, v \in a\}$. Potřebujeme:
1. $b \in \mathcal{A}$. (Neboli b je lineárně nezávislé.)
2. $\forall a \in \mathcal{B} : a \leq b$.
Obojí není těžké ověřit.

Tedy podle Zornova lemmatu existuje maximální prvek $a \in \mathcal{A}$, čili lineárně nezávislá množina, ke které už nejde nic přidat tak, aby výsledek byl stále lineárně nezávislý.
Pro spor ať a není báze, tedy $\exists v \in V \setminus \mathrm{Span}(a)$. Pak ale $a \cup \{v\}$ by byla větší lineárně nezávislá množina, což by ale byl spor s maximalitou a. □

Teď si ukážeme několik užitečných aplikací Zornova lemmatu v teorii okruhů.

Lemma 1.23. *Buď A neprázdná podmnožina okruhu R a $I < R$. Pokud $I \cap A = \emptyset$, pak existuje ideál $J < R$ takový, že*

- $J \supset I$,
- $J \cap A = \emptyset$,
- $J' \cap A \neq \emptyset$ *pro každý ideál* $J' < R$ *takový, že* $J' \supsetneq J$.

Důkaz. Volme množinu $\mathcal{A} = \{J < R \mid J \supset I, J \cap A = \emptyset\}$ uspořádanou inkluzí $\subset$.
$\mathcal{A} \neq \emptyset$, protože $I \in \mathcal{A}$.
Dále pro řetězec $\mathcal{B} \subset \mathcal{A}$ je jeho horní mezí $\bigcup_{J \in \mathcal{B}} J \in \mathcal{A}$.
Předpoklady jsou splněny, tedy podle Zornova lemmatu 1.22 množina $\mathcal{A}$ má maximální prvek J. O tom snadno ověříme, že má všechny požadované vlastnosti. □

Důsledek 1.24. *Buď $I < R$* vlastní ideál*. Pak existuje maximální ideál M v R, který obsahuje I.*

Důkaz. V lemmatu 1.23 zvolme $A = \{1\}$. □

Pozor! Tento důsledek nemusí platit, pokud R je okruh bez 1! Dokonce existují okruhy (bez 1), které neobsahují žádné maximální ideály.
Cvičení: Rozmysli si, jaký ideál J dostaneme z důkazu lemmatu 1.23, pokud zvolíme $A = \emptyset$.

Definice. *Multiplikativní množina* S v okruhu R je neprázdná podmnožina R taková, že

- $0 \notin S$ a
- S je uzavřená na násobení, čili $a, b \in S \Rightarrow a \cdot b \in S$.

Tvrzení 1.25. *Buď $S \subset R$ multiplikativní množina a $I < R$ ideál takový, že $I \cap S = \emptyset$. Potom existuje prvoideál $P \supset I$ takový, že $P \cap S = \emptyset$.*

Důkaz. V lemmatu 1.23 zvolme $A = S$. Je pak potřeba ověřit, že ideál J, který existuje podle tohoto lemmatu, je prvoideál: cvičení. □

Důsledek 1.26. *Pro každou multiplikativní množinu S existuje prvoideál P takový, že $P \cap S = \emptyset$.*

Důkaz. Zvolme $I = \{0\}$ v tvrzení 1.25. □

2. Galoisova teorie

2.1 Opakování

Připomeňme si některé základní pojmy z teorie (komutativních) těles. Níže jsou T, U, V vždy tělesa taková, že $U \supset T$.

$U \supset T$ implikuje, že U je vektorový prostor nad T. Stupeň rozšíření těles $d = [U : T]=$ dimenze U jako vektorového prostoru nad T. Tedy existuje báze $\alpha_1, \alpha_2, \dots, \alpha_d \in U$, čili $\forall \alpha \in U\ \exists! t_i \in T$ taková, že $\alpha = \sum t_i \alpha_i$.
Pokud $V \supset U \supset T$, pak $[V : T] = [V : U] \cdot [U : T]$.

$\alpha \in U$ je algebraické nad T, pokud je kořenem nějakého $0 \neq f(x) \in T[x]$. Má-li f minimální stupeň, jde o minimální polynom pro α.

Pro $\alpha \in U$ definujeme $T[\alpha]$ jako nejmenší okruh, který obsahuje T a α, a $T(\alpha)$ jako nejmenší těleso, které obsahuje T a α.

Je-li α algebraické (nad T), pak $T[\alpha] = T(\alpha)$. Platí $d = [T(\alpha) : T] =$ deg minimálního polynomu pro α. Jako bázi $T(\alpha)$ můžeme volit $1, \alpha, \dots, \alpha^{d-1}$.

Pokud α není algebraické (nad T), pak $T[\alpha] \simeq T[x]$ a $T(\alpha) \simeq T(x)$ (což je okruh polynomů, resp. těleso racionálních funkcí).
Tedy α je algebraické nad $T \Leftrightarrow [T(\alpha) : T] < \infty$.

Rozšíření $U \supset T$ je algebraické, pokud každý prvek $\alpha \in U$ je algebraický nad T.
Je-li prvek α algebraický, pak je $T(\alpha) \supset T$ algebraické rozšíření.
$U \supset T$ rozšíření konečného stupně $\Rightarrow U \supset T$ algebraické rozšíření.

T má charakteristiku p (což je nutně prvočíslo), pokud $\underbrace{1 + \cdots + 1}_{p\text{-krát}} = 0$. Pokud takové p neexistuje, je charakteristika 0.

2.2 Úvod

Ať $U \supset T, V \supset T$ jsou tělesa. Homomorfismus $\varphi\colon U \to V$ je T-homomorfismus, pokud $\varphi(t) = t$ pro všechna $t \in T$.

$\mathrm{Gal}\left({}^{U}/_{T}\right) = \{\varphi\colon U \to U \mid \varphi \text{ je } T\text{-automorfismus}\}$ je Galoisova grupa rozšíření $U \supset T$.
Jde o grupu, protože automorfismy můžeme skládat a invertovat; identita id je 1 v grupě.
Například $\mathrm{Gal}\left({}^{\mathbb{Q}(i)}/_{\mathbb{Q}}\right) = \{\mathrm{id}, \varphi\}$, kde $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}, \varphi(a + bi) = a - bi$.

Příklad. Buď $D \in \mathbb{Z}$ takové, že D není čtverec. Uvažujme rozšíření $\mathbb{Q}(\sqrt{D}) \supset \mathbb{Q}$. Minimální polynom pro $\sqrt{D}$ je $x^2 - D$.

Buď $\varphi \in \mathrm{Gal}\left(\mathbb{Q}(\sqrt{D})/\mathbb{Q}\right)$. Pak

$$0 = \varphi(0) = \varphi\left((\sqrt{D})^2 - D\right) = \varphi(\sqrt{D})^2 - \varphi(D) = \varphi(\sqrt{D})^2 - D,$$

a tedy $\varphi(\sqrt{D}) = \pm\sqrt{D}$.
Naopak hodnota $\psi(\sqrt{D})$ jednoznačně určuje $\psi \in \mathrm{Gal}$: pro $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ máme $\psi(a + b\sqrt{D}) = a + b\psi(\sqrt{D})$.

Tedy $\mathrm{Gal}\left(\mathbb{Q}(\sqrt{D})/\mathbb{Q}\right) = \{\mathrm{id}, \varphi\}$, kde $\varphi(\sqrt{D}) = -\sqrt{D}$.

Obzvlášť je-li $U \supset T$ rozšíření konečného stupně, dává $\mathrm{Gal}\left(U/T\right)$ hodně informace o struktuře tohoto rozšíření (a prvku α takového, že $U = T(\alpha)$). V Algebře jste například viděli využití na konstrukce pravítkem a kružítkem a na neřešitelnost rovnice 5. stupně.

2.3 Celistvé prvky

Definice. Ať je R podokruh S. Prvek $v \in S$ je *celistvý* nad R, pokud je kořenem nějakého *monického* polynomu v $R[x]$, čili $\exists f \in R[x], f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ a $f(v) = 0$.

Poznámka. Pokud R, S jsou tělesa, pak $v \in S$ je algebraický nad $R \Leftrightarrow v \in S$ je celistvý nad R.

Poznámka. Ať $S = \mathbb{Q}, R = \mathbb{Z}$. Pak $v \in \mathbb{Q}$ je celistvý nad $\mathbb{Z} \Leftrightarrow v \in \mathbb{Z}$.

Tvrzení 2.1. *Ať je R podokruh* oboru *S a $v \in S$. Následující tvrzení jsou ekvivalentní:*
1) v je celistvý nad R.
2) $R[v]$ je konečně generovaný R-modul.
3) Existuje okruh $R', R[v] \subset R' \subset S$, takový, že R' je konečně generovaný R-modul.

Důkaz.
2) $\Rightarrow$ 3): Volíme $R' = R[v]$.

1) $\Rightarrow$ 2): Víme, že $v^n + a_{n-1}v^{n-1} + \cdots + a_0 = 0$ pro nějaká $a_i \in R$.
Dokážeme, že $R[v] = R \cdot 1 + R \cdot v + \cdots + R \cdot v^{n-1} =: \heartsuit$.

„$\supset$“ Ok
„$\subset$“ $R[v] = \{\sum r_j v^j\}$. Stačí tedy dokázat, že $v^j \in \heartsuit$ pro každé j.
Pro $j = 0$ máme $v^0 = 1$. Z definice pro $0 \leq j \leq n-1$ vidíme, že v^j už je v $\heartsuit$. Co v^n?
$v^n = \underbrace{-a_{n-1}v^{n-1}}_{\in R\cdot v_{n-1}} - \cdots - \underbrace{a_0}_{\in R\cdot 1} \in \heartsuit$.

Pokračujme indukcí pro $j \geq n+1$. Poslední rovnost přenásobíme v^{j-n} a máme

$$v^j = -a_{n-1}\underbrace{v^{j-1}}_{\in\heartsuit} - \cdots - a_0\underbrace{v^{j-n}}_{\in\heartsuit} \in \heartsuit.$$

3) $\Rightarrow$ 1) Ať $R' = \sum\limits_{j=1}^{n} Rw_j$. Tedy pro každé $v \in R'$ máme

$$v \cdot w_i = \sum_{j=1}^{n} a_{ij} w_j$$

pro nějaká $a_{ij} \in R$.

Podívejme se na tyto rovnice pro $i = 1, \dots, n$ jako na soustavu homogenních lineárních rovnic s proměnnými $w_1, \dots, w_n$ a s koeficienty z podílového tělesa oboru S.
$w_j \neq 0 \Rightarrow$ soustava má netriviální řešení $\Rightarrow$ determinant $= 0$.
Matice soustavy je

$$\begin{pmatrix} v - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a_{21} & v - a_{22} & \dots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \dots & v - a_{nn} \end{pmatrix},$$

takže její determinant je polynom v proměnné v s koeficienty v R a vedoucím členem $1 \cdot v^n$. Dává tedy hledaný monický polynom pro v. □

Poznámka. Tvrzení 2.1 platí, i pokud S není obor (s víceméně stejným důkazem).

Důsledek 2.2. *Množina prvků oboru S, jež jsou celistvé nad $R \subset S$, tvoří podokruh v S (obsahující R).*

Důkaz. Ať $a, b \in S$ jsou celistvé nad R. Pak $R[a]$ je konečně generovaný R-modul.
b je také celistvý nad $R[a]$, a tedy $R[a][b] = R[a, b]$ je konečně generovaný $R[a]$-modul.
Cvičení $\Rightarrow R[a, b]$ je konečně generovaný R-modul.
Pro $v = a \pm b, a \cdot b$ máme $R[v] \subset R[a, b]$, a tedy v je celistvé podle tvrzení 2.1. □

2.4 Kořenová a rozkladová nadtělesa

Definice. Buď $S \supset T$ rozšíření těles, $f(x) \in T[x]$. S je kořenové nadtěleso polynomu f, pokud f má kořen $\alpha \in S$ a $S = T(\alpha)$.
S je rozkladové nadtěleso polynomu f, pokud se f v $S[x]$ rokládá na lineární činitele $f(x) = c \cdot (x - \alpha_1) \cdots (x - \alpha_n)$, kde $c, \alpha_i \in S$ a $S = T(\alpha_1, \dots, \alpha_n)$.

Tvrzení 2.3. *Buď T těleso a $f \in T[x]$ polynom stupně ≥ 1. Pak*

(a) existuje kořenové nadtěleso pro f nad T a

(b) existuje rozkladové nadtěleso pro f nad T.

Důkaz. a) Ať $g \mid f$ je ireducibilní a uvažujme ideál $(g) = gT[x] < T[x]$.
g je ireducibilní $\Rightarrow$ (g) je maximální $\overset{1.7}{\Rightarrow}$ $S := {}^{T[x]}/_{(g)}$ je těleso. Dokážeme, že jde o hledané kořenové nadtěleso.
Máme projekci

$$\begin{aligned} \pi\colon T[x] &\twoheadrightarrow S \\ h &\mapsto h + (g) \end{aligned}$$

Dále uvažujme zúžení homomorfismu π na $T \subset T[x]$, čili $\pi \restriction T : T \to S$. Toto zúžení je prosté, protože kdyby $0 + (g) = (\pi \restriction T)(t) = \pi(t) = t + (g)$, tak $t \in (g)$, což jde jen pro $t = 0$, protože stupeň všech nenulových polynomů v $(g) \geq \deg g \geq 1$.
Můžeme tedy T ztotožnit s jeho obrazem $\mathrm{Im}(\pi \restriction T) \subset S$ a předpokládat, že $T \subset S$. Navíc si uvědomme, že pak π fixuje prvky T, čili je to T-homomorfismus. Protože $\pi\colon T[x] \twoheadrightarrow S$ je surjektivní T-homomorfismus, máme $S = T[\pi(x)]$.

Uvažujme nyní okruh polynomů $S[X]$ v proměnné X nad S. Máme $g(X) \in T[X] \subset S[X]$. Máme $\pi(x) \in S$, a tedy můžeme tuto hodnotu dosadit do $g(X)$:

$$g(\pi(x)) = \sum_i a_i \pi(x)^i = \pi\left(\sum_i a_i x^i\right) = \pi(g) = 0.$$

Tedy polynom $g \mid f$ má kořen $\pi(x) \in S$. Už jsme viděli, že $S = T[\pi(x)]$.

b) Indukcí podle stupně $\deg f$.
Pro $\deg f = 1$ je rozkladové nadtěleso $S = T$.
Pro $\deg f > 1$ buď $T(\alpha)$ kořenové nadtěleso f nad T. Pak $f(x) = g(x) \cdot (x - \alpha)$. Polynom $g(x)$ nad $T(\alpha)$ má stupeň $\deg f - 1$, proto pro něj existuje rozkladové nadtěleso nad $T(\alpha)$

$$S = T(\alpha)(\alpha_1, \ldots, \alpha_m) = T(\alpha, \alpha_1, \ldots, \alpha_m).$$

To je hledaným rozkladovým nadtělesem pro f nad T. $\square$

Teď si dokážeme jednoznačnost kořenových a rozkladových nadtěles až na T-izomorfismus.

Lemma 2.4. *Buď T těleso, $f \in T[x]$* ireducibilní *(nekonstantní) polynom. Jsou-li S_1, S_2 kořenová nadtělesa pro f nad T, pak existuje T-izomorfismus $\varphi\colon S_1 \to S_2$.*

Příklad. Toto lemma obecně neplatí, pokud je f reducibilní. Volme například $f(x) = x(x^2+1)$ a $T = \mathbb{Q}$. Polynom f má kořeny $0, \pm i$.
Tedy $S_1 = \mathbb{Q}$ a $S_2 = \mathbb{Q}(i)$ jsou jeho kořenová nadtělesa, ale $\mathbb{Q} \not\simeq \mathbb{Q}(i)$.

Důkaz. Ať $S_1 = T(\alpha), S_2 = T(\beta)$.
Víme, že $T(\alpha) = T[\alpha] = \{g(\alpha) \mid g \in T[x]\}$ a podobně pro $T(\beta)$.
Uvažujme

$$\begin{aligned} \varphi\colon T(\alpha) &\to T(\beta) \\ g(\alpha) &\mapsto g(\beta) \end{aligned}$$

Je to dobře definované? Všimneme si, že f je minimální polynom pro α i β, tedy $g(\alpha) = h(\alpha) \Leftrightarrow (g-h)(\alpha) = 0 \underset{f \text{ min. pol. pro } \alpha}{\Leftrightarrow} f \mid g-h \underset{f \text{ min. pol. pro } \beta}{\Leftrightarrow} (g-h)(\beta) = 0 \Leftrightarrow g(\beta) = h(\beta)$.
Tedy φ je dobře definované i prosté. *Na* je jasné z definice.
Zřejmě jde o T-homomorfismus, tedy máme T-izomorfismus. $\square$

Tvrzení 2.5. *Mějme rozšíření těles $T_1, T_2 \supset T$ a T-izomorfismus $\varphi\colon T_1 \to T_2$. Pro $f(x) = \sum a_i x^i \in T_1[x]$ definujeme $\varphi(f)(x) := \sum \varphi(a_i) x^i \in T_2[x]$.*

Ať $\deg f \geq 1$ a S_1 = rozkladové nadtěleso f nad T_1, S_2 = rozkladové nadtěleso $\varphi(f)$ nad T_2.
Pak existuje T-izomorfismus $\psi\colon S_1 \to S_2$ takový, že $\psi \restriction T_1 = \varphi$.

$$\begin{tikzcd}
S_1 \arrow[rr, dashed, "\psi"] \arrow[d, dash] & & S_2 \arrow[d, dash] \\
T_1 \arrow[rr, "\varphi"] \arrow[dr, dash] & & T_2 \arrow[dl, dash] \\
& T &
\end{tikzcd}$$

Volbou $T = T_1 = T_2$ a $\varphi = \mathrm{id}$ v tvrzení 2.5 dostaneme:

Věta 2.6. *Buď T těleso a $f \in T[x]$ nekonstantní polynom. Rozkladové nadtěleso f nad T je jednoznačně určené až na T-izomorfismus.*

Důkaz tvrzení 2.5. Indukcí podle $\deg f$:
$\deg f = 1$: Máme $S_1 = T_1, S_2 = T_2, \psi = \varphi$.

$\deg f > 1$: Buď $g \mid f$ ireducibilní polynom v $T[x]$ a $\alpha \in S_1$ kořen g. Pak $\varphi(g) \mid \varphi(f)$ a buď $\beta \in S_2$ kořen $\varphi(g)$. Podobně jako v lemmatu 2.4 máme T-isomorfismus

$$\begin{aligned} \sigma\colon T_1(\alpha) &\to T_2(\beta) \\ h(\alpha) &\mapsto \varphi(h)(\beta) \end{aligned}$$

(použije se: g je minimální polynom pro α nad T_1 a $\varphi(g)$ je minimální polynom pro β.)
Navíc $\sigma \restriction T_1 = \varphi$.
Buď $h \in T_1(\alpha)[x]$ takový, že $f(x) = (x-\alpha)h(x)$, pak $\sigma(f)(x) = (x-\beta)\sigma(h)(x)$, protože z definice máme $\beta = \sigma(\alpha)$.
Vidíme, že S_1, S_2 jsou rozkladová nadtělesa pro h, $\sigma(h)$ nad $T_1(\alpha)$, $T_2(\beta)$.
$\deg h < \deg f \Rightarrow$ podle IP máme T-izomorfismus $\psi\colon S_1 \to S_2$ takový, že $\psi \restriction T_1(\alpha) = \sigma$, a tedy $\psi \restriction T_1 = \sigma \restriction T_1 = \varphi$.

$$\begin{tikzcd}
S_1 \arrow[rr, dashed, "\psi"] \arrow[d, dash] & & S_2 \arrow[d, dash] \\
T_1(\alpha) \arrow[rr, dashed, "\sigma"] \arrow[d, dash] & & T_2(\beta) \arrow[d, dash] \\
T_1 \arrow[rr, "\varphi"] \arrow[dr, dash] & & T_2 \arrow[dl, dash] \\
& T &
\end{tikzcd}$$

□

2.5 Algebraický uzávěr

Definice. Těleso T je algebraicky uzavřené, pokud v T má každý nekonstantní polynom z $T[x]$ kořen.
Ekvivalentně: Každý polynom z $T[x]$ se rozkládá na lineární činitele.

Příklad. $\mathbb{C}$ je algebraicky uzavřené.
Žádné konečné těleso *není* algebraicky uzavřené (cvičení).

Definice. Buď T těleso. Jeho *algebraický uzávěr* je algebraicky uzavřené těleso $S \supset T$, které je algebraickým rozšířením T.
Algebraický uzávěr tělesa T často značíme $\overline{T}$.

Příklad. $\pi, e \in \mathbb{C}$ transcendentní nad $\mathbb{Q} \Rightarrow \mathbb{C}$ není algebraický uzávěr $\mathbb{Q}$.
$\mathbb{C} = \mathbb{R}(i)$ je algebraický uzávěr $\mathbb{R}$.

Postupně dokážeme, že algebraický uzávěr každého tělesa existuje a je jednoznačný (až na T-izomorfismus).

Tvrzení 2.7. *Mějme tělesa $S \supset T$ a buď $U = \{\alpha \in S \mid \alpha$ je algebraické nad $T\}$, což je těleso $T \subset U \subset S$. Je-li S algebraicky uzavřené, pak je U algebraický uzávěr T.*

Důkaz. Z Algebry víme, že U je těleso. Zřejmě $U \supset T$ je algebraické rozšíření. Je U algebraicky uzavřené?
Buď $f \in U[x]$. S algebraicky uzavřené $\Rightarrow f$ má kořen $\beta \in S$. Chceme $\beta \in U$.
Ať $f(x) = \sum \alpha_i x^i, \alpha_i \in U$. Tedy $f \in T(\alpha_0, \dots, \alpha_n)[x]$, takže β je algebraické nad $T(\alpha_0, \dots, \alpha_n)$, čili $[T(\alpha_0, \dots, \alpha_n, \beta) : T(\alpha_0, \dots, \alpha_n)] < \infty$.
Každé α_i je algebraické nad $T \Rightarrow [T(\alpha_0, \dots, \alpha_n) : T] < \infty$. Tedy $[T(\alpha_0, \dots, \alpha_n, \beta) : T] < \infty \Rightarrow \beta$ algebraické nad $T \Rightarrow \beta \in U$. □

Příklad. Algebraický uzávěr $\mathbb{Q}$ existuje a je spočetný (ale $\mathbb{C}$ je nespočetné).

Lemma 2.8. *Ke každému tělesu T existuje algebraické rozšíření $S \supset T$ takové, že každý nekonstantní polynom z $T[x]$ má kořen v S.*

Důkaz. Dokazuje se podobně jako existence kořenového nadtělesa v lemmatu 2.3, ale potřebujeme přidat kořeny všech polynomů zároveň.
Pro každý nekonstantní ireducibilní polynom $f \in T[x]$ zvolme proměnnou x_f a buď $X = \{x_f \mid f \in T[x]$ nekonstantní ireducibilní$\}$. Uvažujme $T[X] :=$ polynomy v proměnných X (každý polynom v sobě ale obsahuje jen konečně mnoho z nich).

Chceme faktorokruh, kde $x_f \mapsto$ kořen polynomu f:
Buď $I = (f(x_f) \mid f \in T[x]$ nekonstantní ireducibilní$) < T[X]$ ideál generovaný všemi $f(x_f)$.

Cvičení: $1 \notin I$.

Důkaz. Ať pro spor $1 \in I$. To znamená, že $1 = \sum f(x_f) g_f$ pro nějaké polynomy $g_f \in T[X]$. Na pravé straně máme konečnou sumu, takže se v ní vyskytuje jen konečně mnoho proměnných x_h. Uvažujme kořenové nadtěleso U všech polynomů h takových, že proměnná x_h se v rovnosti vyskytuje.
V tělese U má tedy každý takovýto polynom kořen α_h. Dosazením $x_h \mapsto \alpha_h$ v rovnosti dostaneme $1 = \sum f(\alpha_f) g_f = \sum 0 \cdot g_f = 0$, což je spor. □

Podle Zornova lemmatu existuje maximální ideál $M < T[X]$ takový, že $I \subset M$ (lemma 1.24). Pak je faktorokruh $S := {}^{T[X]}/_{M}$ těleso a máme $T \hookrightarrow S$ (jako v lemmatu 2.3). Každý polynom $f \in T[x]$ má v S kořen, a to $x_f + M$.
Navíc S vznikne přidáním všech těchto algebraických prvků $x_f + M$ k T (protože máme surjektivní T-homomorfismus $T[X] \twoheadrightarrow S$), a proto jde o algebraické rozšíření. □

Věta 2.9. *Pro každé těleso T existuje jeho algebraický uzávěr. Každé dva algebraické uzávěry tělesa T jsou T-izomorfní.*

Důkaz.
Existence: Buď $T = S_0 \subset S_1 \subset \cdots$ řetězec těles, kde S_{i+1} vznikne z S_i použitím lemmatu 2.8. Buď $S = \bigcup S_i$. Zřejmě: S je těleso, jež je algebraickým rozšířením T, protože každý prvek $\alpha \in S$ leží v nějakém S_i, což je algebraické rozšíření T.

S je algebraicky uzavřené, protože pro každé $f \in S[x]$ existuje i takové, že $f \in S_i[x]$, a tedy f má kořen v $S_{i+1} \subset S$.
S je tedy algebraický uzávěr T.

Jednoznačnost: Ať S_1, S_2 jsou algebraické uzávěry tělesa T.

Pozorování: Pokud $S_1 \subset S_2$, pak $S_1 = S_2$.

Důkaz pozorování. Ať $\alpha \in S_2 \Rightarrow \alpha$ je kořen nějakého $f \in T[x]$.
S_1 algebraicky uzavřené $\Rightarrow f(x) = c\prod(x - \alpha_i)$, kde $\alpha_i, c \in S_1 \Rightarrow \exists i : \alpha = \alpha_i \in S_1$.
Tedy $S_1 = S_2$. □

Obecně uvažujme množinu

$$\mathcal{M} := \{\varphi : U_1^\varphi \to U_2^\varphi \ T\text{-izomorfismus} \mid T \subset U_1^\varphi \subset S_1, T \subset U_2^\varphi = \varphi(U_1^\varphi) \subset S_2\}$$

(značení U_1^φ, U_2^φ používáme na zdůraznění, že tato tělesa přísluší k φ: formálně správně bychom měli $\mathcal{M}$ definovat jako množinu uspořádaných trojic $(\varphi, U_1^\varphi, U_2^\varphi)$).
Množinu $\mathcal{M}$ uspořádáme tak, že definujeme

$$\varphi \leq \psi, \text{ pokud } U_1^\psi \supset U_1^\varphi, U_2^\psi \supset U_2^\varphi \text{ a } \psi \restriction U_1^\varphi = \varphi.$$

Ověříme nyní předpoklady Zornova lemmatu 1.22:
$\mathcal{M} \neq \emptyset$, protože obsahuje $\mathrm{id} : T \to T$.
„Horní mez řetězce“ $\mathcal{B}$ je zase prvek $\mathcal{M}$: cvičení, vol $U_i = \bigcup_{\varphi \in \mathcal{B}} U_i^\varphi$ a definuj nové $\psi : U_1 \to U_2$ po prvku.

Podle Zornova lemmatu tedy existuje maximální prvek φ: $U_1 \to U_2$ v $\mathcal{M}$.
Chci: φ je T-izomorfismus $S_1 \to S_2$.
Ať $U_1 \neq S_1 \Rightarrow U_1 \subsetneq S_1 \Rightarrow U_1$ není algebraicky uzavřené (podle pozorování výše) $\Rightarrow$ $\exists f(x) = \sum a_i x^i \in U_1[x]$, který nemá kořen v U_1. Buď V_1 rozkladové nadtěleso pro f nad U_1 a V_2 rozkladové nadtěleso pro $\varphi(f) := \sum \varphi(a_i)x^i$ nad U_2.
Podle tvrzení 2.5 existuje T-izomorfismus ψ: $V_1 \to V_2$ takový, že $\psi \restriction U_1 = \varphi$, což je ale spor s maximalitou φ, a tedy $U_1 = S_1$.
φ: $U_1 \to U_2$ je T-izomorfismus a $U_1 = S_1$ algebraický uzávěr. Tedy $U_2 \subset S_2$ jsou dva algebraické uzávěry. Pozorování $\Rightarrow U_2 = S_2$. □

Podobně se dokáže

Důsledek 2.10.
a) Mějme tělesa $T \subset U \subset K, T \subset V \subset K$, kde $K = \overline{T}$ je algebraický uzávěr T. Potom pro každý T-homomorfismus φ: $U \to V$ existuje T-automorfismus $\psi : K \to K$, který rozšiřuje φ, čili $\psi \restriction U = \varphi$.
b) Ať $T \subset U \subset W \subset K$, kde $K = \overline{T}$ je algebraický uzávěr T. Pro každý T-homomorfismus φ: $U \to K$ existuje T-homomorfismus σ: $W \to K$ takový, že $\sigma \restriction U = \varphi$

Důkaz. Důkaz jenom naznačíme.
$a) \Rightarrow b)$ je snadné, stačí totiž vzít $V = K$ a $\sigma = \psi \restriction W$.
$a)$ stačí dokázat pro φ je T-izomorfismus, neboť

Cvičení. Buď φ: $U \to V$ T-homomorfismus. Pak je φ prosté, a tedy dává T-izomorfismus $U \to \mathrm{Im}(\varphi)$.

K důkazu je teď potřeba rozšířit $\varphi : U \to V$ na maximální T-izomorfismus použitím Zornova lemmatu podobně jako v předchozím důkaze. □

Často se taky hodí tento výsledek:

Cvičení. Buď $T \subset U$ algebraické rozšíření a $U \subset K$. Pak K je algebraický uzávěr $T \Leftrightarrow K$ je algebraický uzávěr U.

2.6 Galoisova grupa

Připomeňme, že pro rozšíření těles $U \supset T$ je Galoisova grupa $\mathrm{Gal}\left({}^{U}/_{T}\right) = \{T$-automorfismy $\varphi : U \to U\}$.

Tvrzení 2.11. *Mějme tělesa $U, V \supset T$ a nenulový polynom $f \in T[x]$.*
a) Každý T-homomorfismus $\varphi : U \to V$ zobrazí každý kořen f v U na kořen f ve V.
b) Buď M množina všech kořenů f v tělese U. Pokud je $\varphi : U \to U$ prostý T-homomorfismus, pak $\varphi \restriction M$ je permutace množiny M.

Speciálně část b) platí pro každé $\varphi \in \mathrm{Gal}\left({}^{U}/_{T}\right)$.

Důkaz. a) Ať $f(x) = \sum a_i x^i \in T[x]$ a $u \in U$ je jeho kořen. Pak $\varphi(u)$ je taky kořen f, protože

$$f(\varphi(u)) = \sum a_i(\varphi(u))^i \overset{T\text{-hom}}{=} \varphi(\sum a_i u^i) = \varphi(f(u)) = \varphi(0) = 0.$$

b) Podle části a) pro $V = U$ máme $\varphi \restriction M \colon M \to M$.
φ prosté $\Rightarrow \varphi \restriction M$ prosté.
M konečné $\Rightarrow \varphi \restriction M$ permutace. □

Tvrzení 2.12. *Buď U rozkladové nadtěleso polynomu $f \in T[x]$ a $\deg f = n \geq 1$.*
a) Galoisova grupa se vnořuje do symetrické grupy S_n, neboli máme

$$\begin{aligned} \mathrm{Gal}\left({}^{U}/_{T}\right) &\hookrightarrow S_n \\ \varphi &\mapsto \varphi \restriction M \end{aligned}$$

b) Je-li f ireducibilní nad T, pak pro každé dva kořeny $\alpha, \beta \in U$ existuje $\varphi \in \mathrm{Gal}\left({}^{U}/_{T}\right)$ takový, že $\varphi(\alpha) = \beta$.

Důkaz. a) Buď $M = \{\alpha_1, \dots, \alpha_k\}$ množina kořenů f. Podle tvrzení 2.11b) je $\varphi \restriction M$ permutace na k-prvkové množině M pro každé $\varphi \in \mathrm{Gal}\left({}^{U}/_{T}\right)$, tedy dává prvek S_k. Tuto permutaci rozšíříme na permutaci z S_n tak, že ji dodefinujeme jako identitu pro $i = k+1, \dots, n$. Dostáváme tedy zobrazení

$$\begin{aligned} \mathrm{Gal}\left({}^{U}/_{T}\right) &\to S_n \\ \varphi &\mapsto \varphi \restriction M \end{aligned}$$

Snadno se ověří, že jde o homomorfismus (cvičení).
Z definice rozkladového nadtělesa máme $U = T(\alpha_1, \dots, \alpha_k)$, a tedy je φ jednoznačně určené svými hodnotami $\varphi(\alpha_1), \dots, \varphi(\alpha_k)$, neboli právě zúžením $\varphi \restriction M$. Zobrazení $\varphi \mapsto \varphi \restriction M$ je tudíž prosté.

b) f ireducibilní $\Rightarrow$ kořenová nadtělesa $T(\alpha), T(\beta)$ jsou T-izomorfní podle lemmatu 2.4. Máme tedy T-izomorfismus $\varphi\colon T(\alpha) \to T(\beta)$ takový, že $\varphi(\alpha) = \beta$. Podle tvrzení 2.5 pak můžeme φ rozšířit na T-izomorfismus $\psi\colon U \to U$ (volíme $T_1 = T(\alpha), T_2 = T(\beta), S_1 = S_2 = U$).
Tedy $\psi \in \mathrm{Gal}\left({}^{U}\!/_{T}\right)$ a $\psi(\alpha) = \beta$. □

2.7 Separabilní rozšíření

Buď $f \in \mathbb{Q}[x]$ a $T = \mathbb{Q}(\alpha)$ jeho kořenové nadtěleso. Uvažujme $\mathbb{Q}$-homomorfismus do algebraického uzávěru $\varphi\colon \mathbb{Q}(\alpha) \to \overline{\mathbb{Q}}$.
φ je jednoznačně určené hodnotou $\varphi(\alpha)$, což musí být kořen f v $\overline{\mathbb{Q}}$ podle tvrzení 2.11a).
Polynom f má maximálně $\deg f$ kořenů, a tedy existuje nejvýše $\deg f$ různých $\mathbb{Q}$-homomorfismů $\varphi\colon \mathbb{Q}(\alpha) \to \overline{\mathbb{Q}}$.
Pokud je f ireducibilní nad $\mathbb{Q}$, pak je počet φ roven $\deg f$.

Obecně může být počet $\varphi < \deg f$ i pro ireducibilní polynom f, pokud má T konečnou charakteristiku.
Například volme $T = \mathbb{F}_p(y)$ a $f(x) = x^p - y \in T[x]$. Tento polynom je ireducibilní nad T podle Eisensteinova kritéria, ale $f(x) = (x - \sqrt[p]{y})^p$ nad jeho kořenovým nadtělesem $T(\sqrt[p]{y})$ (a tedy i nad algebraickým uzávěrem). Tedy jediné $\varphi : T(\sqrt[p]{y}) \to \overline{T}$ je identita a počet $\varphi = 1$.

Definice. Ať jsou $T \subset U \subset \overline{T}$ tělesa, kde $\overline{T}$= algebraický uzávěr T. Mohutnost množiny $\{\varphi\colon U \to \overline{T} \mid T\text{-homomorfismus}\}$ se nazývá *stupeň separability* rozšíření $U \supset T$ a značí se $[U : T]_s$.

Tvrzení 2.13. *Mějme* algebraická *rozšíření* $T \subset U \subset V$. *Pak*

$$[V : T]_s = [V : U]_s \cdot [U : T]_s.$$

Důkaz. Stačí dokázat toto pozorování:
Pozorování: Buď $\overline{T}$ algebraický uzávěr T a definujme

$$\Phi = \{\varphi\colon U \to \overline{T} \mid T\text{-homomorfismus}\}, \Psi = \{\psi\colon V \to \overline{T} \mid U\text{-homomorfismus}\}.$$

Pro $\varphi \in \Phi$ zvolme $\overline{\varphi}\colon \overline{T} \to \overline{T}$ nějaký T-automorfismus rozšiřující φ (podle důsledku 2.10a).
Pak $\{\overline{\varphi} \circ \psi \mid \varphi \in \Phi, \psi \in \Psi\}$ je množina všech T-homomorfismů $V \to \overline{T}$.
Navíc $\overline{\varphi_1} \circ \psi_1 = \overline{\varphi_2} \circ \psi_2$ implikuje $\varphi_1 = \varphi_2$ a $\psi_1 = \psi_2$.

Důkaz pozorování. Buď $\rho\colon V \to \overline{T}$ T-homomorfismus. Pak můžeme zvolit $\varphi := \rho \restriction U \in \Phi$ a $\psi := \overline{\varphi}^{-1} \circ \rho \in \Psi$ (cvičení: proč je ψ U-homomorfismus?), abychom dostali $\rho = \overline{\varphi} \circ \psi$.

Pokud $\overline{\varphi_1} \circ \psi_1 = \overline{\varphi_2} \circ \psi_2$, pak $\varphi_1(u) = \overline{\varphi_1}(u) = \overline{\varphi_1} \circ \psi_1(u) = \overline{\varphi_2} \circ \psi_2(u) = \varphi_2(u)$ pro každé $u \in U$. Tedy $\varphi_1 = \varphi_2$, takže $\overline{\varphi_1} = \overline{\varphi_2}$, a konečně $\psi_1 = \psi_2$ (protože $\overline{\varphi_1} = \overline{\varphi_2}$ je bijekce). □

□

Lemma 2.14. *Buď $U \supset T$ rozšíření těles konečného stupně.*
a) Pak $[U : T]_s \leq [U : T]$.
b) Je-li $\alpha \in U$ prvek takový, že stupeň minimálního polynomu m pro α nad T je n a polynom m má v algebraickém uzávěru právě k kořenů, pak

$$[U : T]_s \leq \frac{k}{n}[U : T].$$

Důkaz. a) Je-li $U = T(\beta)$, pak $[T(\beta) : T]_s \leq [T(\beta) : T]$ (protože $\varphi(\beta)$ je kořen minimálního polynomu pro β). Obecně máme $U = T(\beta_1, \dots, \beta_l)$ a můžeme použít indukci pomocí tvrzení 2.13.

b) Máme $T \subset T(\alpha) \subset U$, a tedy

$$[U : T] = [U : T(\alpha)] \cdot [T(\alpha) : T] = [U : T(\alpha)] \cdot n.$$

Pak

$$[U : T]_s \overset{2.13}{=} [U : T(\alpha)]_s \cdot [T(\alpha) : T]_s = [U : T(\alpha)]_s \cdot k \overset{\text{část } a)}{\leq} [U : T(\alpha)] \cdot k = \frac{[U : T]}{n} \cdot k. \quad \square$$

Definice. Buď T těleso. Polynom $f \in T[x]$ je *separabilní polynom*, pokud nemá násobné kořeny v algebraickém uzávěru $\overline{T}$.
Je-li $T \subset U$ a $\alpha \in U$, potom α je *separabilní prvek*, pokud je jeho minimální polynom separabilní.
Rozšíření $U \supset T$ je *separabilní rozšíření*, pokud všechny prvky $\alpha \in U$ jsou separabilní.

Tvrzení 2.15. *Buď $U \supset T$ rozšíření těles konečného stupně. Následující tvrzení jsou ekvivalentní:*

1. *$U = T(\alpha_1, \dots, \alpha_k)$ pro α_i separabilní,*
2. *$[U : T] = [U : T]_s$,*
3. *$U \supset T$ je separabilní rozšíření.*

Důkaz.
3) $\Rightarrow$ 1) $U \supset T$ je rozšíření konečného stupně, a tedy $U = T(\alpha_1, \dots, \alpha_k)$ pro nějaké prvky $\alpha_i \in U$. Tyto prvky jsou separabilní, protože $U \supset T$ je separabilní rozšíření.

1) $\Rightarrow$ 2) Pokud $k = 1$ a $U = T(\alpha)$, pak $[U : T]_s = \#$ kořenů (v algebraickém uzávěru) minimálního polynomu pro α = deg minimálního polynomu = $[U : T]$.
Pro $k > 1$ indukcí pomocí tvrzení 2.13.

2) $\Rightarrow$ 3) Kdyby existovalo $\alpha \in U$, které není separabilní nad T, podle lemmatu 2.14b) bychom měli $[U : T]_s < [U : T]$, neboť $k < n$. $\square$

Cvičení: Prvek je separabilní $\Leftrightarrow$ je kořenem nějakého separabilního polynomu.
Cvičení: Mějme rozšíření těles $U \supset T$. Všechny prvky $\alpha \in U$, jež jsou separabilní nad T, tvoří podtěleso U, tzv. separabilní uzávěr T v U.

Tvrzení 2.16. *Je-li U separabilní rozšíření tělesa T a V separabilní rozšíření tělesa U, pak je V separabilní rozšíření tělesa T.*

Důkaz. Nemůžeme hned použít tvrzení 2.15, protože nemáme nutně rozšíření konečného stupně. Proto důkaz provedeme po prvcích (podobně, jako se analogická vlastnost dokazovala pro algebraická rozšíření!).

Ať $\alpha \in V$ a $m(x) = \sum_{i=0}^{n} a_i x^i$ je minimální polynom pro α nad U. Buď $U_1 = T(a_0, \ldots, a_n)$ a $V_1 = U_1(\alpha)$. Vidíme, že $U_1 \supset T$ a $V_1 \supset U_1$ jsou konečného stupně.
Podmínka 1) z tvrzení 2.15 je splněno pro $U_1 \supset T$, takže platí podmínka 2) $[U_1 : T]_s = [U_1 : T]$. Stejně tak máme $[V_1 : U_1]_s = [V_1 : U_1]$.
Jejich vynásobením dostaneme $[V_1 : T]_s = [V_1 : T]$, a tedy opět podle tvrzení 2.15 je $V_1 \supset T$ separabilní rozšíření. Konečně tedy $\alpha \in V_1$ je separabilní prvek nad T. □

Ireducibilní neseparabilní polynomy jsou poměrně neobvyklé, pojďme si tedy dokázat docela silné nutné podmínky pro jejich existenci.

Tvrzení 2.17. *Buď T těleso a $f(x) = \sum a_i x^i$ (nekonstantní) ireducibilní* neseparabilní *polynom. Pak*
a) T má charakteristiku $p > 0$,
b) $\exists i : a_i \neq b^p$ pro všechna $b \in T$ a
c) $\exists g \in T[x] : f(x) = g(x^p)$, neboli $a_i = 0$ pokud $p \nmid i$.

K důkazu potřebujeme použít formální derivaci polynomu.

Pozorování. Pro polynom $f(x) = \sum a_i x^i$ definujeme jeho formální derivaci jako $f'(x) = \sum i a_i x^{i-1}$. Ta se mimo jiné hodí k detekci násobných kořenů:
Pokud $f(x) = (x-\alpha)^k \cdot g(x)$, pak

$$f'(x) = [(x-\alpha)^k \cdot g(x)]' = k(x-\alpha)^{k-1} g(x) + (x-\alpha)^k g'(x) = (x-\alpha)^{k-1}(\text{něco}).$$

Tedy $(x-\alpha)^{k-1}$ je společný dělitel f a f'.

Důkaz tvrzení 2.17. a) Protože f je neseparabilní, má násobný kořen $\alpha \in \overline{T}$. Tedy příslušné $(x-\alpha)^{k-1}$ je společný dělitel f a f', a tedy $\mathrm{NSD}(f, f') \not\parallel 1$.
Zároveň ale $\mathrm{NSD}(f, f') \mid f$ a f je ireducibilní, tedy $\mathrm{NSD}(f, f') \parallel f$.
Máme $f \parallel \mathrm{NSD}(f, f') \mid f'$. Ale $\deg f' < \deg f$, a tedy $f' = 0$, neboli $i a_i = 0 \forall i$. Ovšem některý koeficient a_i je nenulový, a tedy charakteristika tělesa T není 0, takže se rovná nějakému prvočíslu p.

c) Pokud $p \nmid i$, pak $i a_i = 0$ implikuje $a_i = 0$, a tedy $f(x) = g(x^p)$ pro $g(x) = \sum a_{pi} x^i$.

b) Sporem. Pokud $a_i = b_i^p$ pro každé i, pak

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots = b_0^p + b_p^p x^p + b_{2p}^p x^{2p} + \cdots = (b_0 + b_p x + b_{2p} x^2 + \cdots)^p,$$

což je spor s ireducibilitou f. □

Definice. Těleso T je perfektní, pokud má charakteristiku 0, nebo má charakteristiku p a „Frobeniovo zobrazení“ $x \mapsto x^p$ je automorfismus.

Tedy nad perfektním tělesem neexistují ireducibilní neseparabilní polynomy. Například $\mathbb{F}_p$ je perfektní, protože $x = x^p$ (a podobně každé konečné těleso je perfektní).
Každé algebraicky uzavřené těleso je taky perfektní.

Důsledek 2.18. *Každé algebraické rozšíření perfektního tělesa je separabilní.*

2.8 Jednoduchá rozšíření

Definice. Rozšíření $U \supset T$ je jednoduché, pokud $U = T(\alpha)$ pro nějaký prvek $\alpha \in U$, který je algebraický nad T.

Věta 2.19. *Každé* separabilní *rozšíření těles* konečného stupně *je jednoduché.*

Důkaz. Buď $U \supset T$ konečné separabilní rozšíření. Rozlišíme dva případy:

1. T je konečného těleso $\Rightarrow$ U je také konečné $\Rightarrow$ $U^\times = U \setminus \{0\}$ je cyklická (multiplikativní) grupa (z Algebry známe tvrzení, že *každá konečná multiplikativní podgrupa tělesa je cyklická*). Je-li α její generátor, pak $U = T(\alpha)$.

2. T je nekonečné. Buď $\alpha \in U$ takové, že $[T(\alpha) : T]$ je největší možný (maximum existuje, protože $[T(\alpha) : T] \leq [U : T] < \infty$). Chceme dokázat, že $T(\alpha) = U$. Pro spor ať to neplatí.

Buď $\beta \in U \setminus T(\alpha)$ a $V = T(\alpha, \beta)$. Stačí dokázat, že $V = T(\gamma)$ pro nějaké γ, protože potom $[T(\gamma) : T] > [T(\alpha) : T]$.
$U \supset T$ je separabilní, takže $V \supset T$ je separabilní rozšíření konečného stupně. Uvažujme všechny T-homomorfismy $f_1, \ldots, f_n \colon V \to \overline{T}$, kde $\overline{T} = \overline{V}$ je algebraický uzávěr. Jde o separabilní rozšíření, takže $n = [V : T]_s = [V : T]$.

Hledejme γ ve tvaru $\gamma = \alpha + t\beta$ pro nějaké $t \in T$. Pokud budeme vědět, že $f_i(\alpha + t\beta) \neq f_j(\alpha + t\beta)$ pro všechna $i \neq j$, pak

$$n = [V : T] \geq [T(\gamma) : T] = [T(\gamma) : T]_s \underset{f_1,\ldots,f_n \text{ jsou různé}}{\geq} n.$$

Máme tedy všude rovnosti, takže platí $V = T(\gamma)$.

Jak zvolit t? Chceme, aby

$$\prod_{i<j} [f_j(\alpha + t\beta) - f_i(\alpha + t\beta)] = \prod_{i<j} [f_j(\alpha) - f_i(\alpha) + t(f_j(\beta) - f_i(\beta))] \neq 0.$$

K tomu stačí, že máme různé uspořádané dvojice $(f_i(\alpha), f_i(\beta)) \neq (f_j(\alpha), f_j(\beta))$ pro všechna $i \neq j$, neboť pak jde o nenulový polynom a ten má konečně kořenů, a tedy existuje $t \in T$, které není jeho kořenem. Ale $f_i : T(\alpha, \beta) \to \overline{T}$ je jednoznačně určené hodnotami $f_i(\alpha), f_i(\beta)$, a tedy uspořádané dvojice těchto hodnot pro $i \neq j$ vskutku jsou různé. □

Definice. Buď $U \supset T$ algebraické rozšíření.

$$\mathrm{Aut}(U) := \{\varphi \colon U \to U \text{ automorfismus}\}.$$

Je-li G podgrupa $\mathrm{Aut}(U)$, definujeme

$$\mathrm{Fix}(U, G) = U^G := \{u \in U \mid g(u) = u, \forall g \in G\}.$$

Poznámka. $\mathrm{Fix}(U, G)$ je těleso a $\mathrm{Gal}\left({}^{U}/_{T}\right)$ je podgrupa grupy $\mathrm{Aut}(U)$.

Následující věta bude zcela zásadní pro důkaz vztahu mezi Gal a Fix v Galoisově korespondenci (věty 2.25, 2.26).

Věta 2.20. *Mějme těleso U a podgrupu $G \subset \mathrm{Aut}(U)$ konečného řádu n. Buď $T = \mathrm{Fix}(U, G)$. Pak*
a) $U \supset T$ je separabilní rozšíření,
b) $[U : T] = n$,
c) $\mathrm{Gal}\left({}^{U}/_{T}\right) = G$.

Důkaz. a) Buď $\alpha \in U$. Chceme dokázat, že α je kořen nějakého separabilního polynomu z $T[x]$.
Uvažujme $G\alpha := \{g\alpha \mid g \in G\}$ (což je orbita prvku α v působení G na U). Poznamenejme, že máme $g \in G \subset \mathrm{Aut}(U)$, tedy g je automorfismus na U a $g\alpha = g(\alpha)$ je obraz prvku $\alpha \in U$ v tomto automorfismu (ve značení $g\alpha$ tedy nepíšeme závorky kolem prvku α).

Protože $\mathrm{id} \in G$, máme $\alpha \in G\alpha$. Buď

$$f_\alpha(x) = \prod_{\beta \in G\alpha} (x - \beta).$$

Vidíme, že α je kořen f_α, polynom f_α je separabilní a $\deg f_\alpha \leq n = \#G$.

Chceme dokázat, že $f_\alpha \in T[x]$.
Připomeňme, že pro $h \in \mathrm{Aut}(U)$ a $f \in U[x]$ definujeme $h_x(f(x)) := \sum h(a_i)x^i$, kde $f(x) = \sum a_i x^i$.
Buď $h \in G$. Všimněme si $h(G\alpha) := \{h\beta \mid \beta \in G\alpha\} = \{(hg)\alpha \mid g \in G\} = G\alpha$, neboli h dává permutaci množiny $G\alpha$.
Tedy

$$h_x(f_\alpha(x)) = \prod_{\beta \in G\alpha} (x - h\beta) = \prod_{\gamma \in G\alpha = h(G\alpha)} (x - \gamma) = f_\alpha(x).$$

Vidíme, že h fixuje všechny koeficienty polynomu f_α. Toto platí pro všechna h, takže $f_\alpha \in T[x]$, což jsme chtěli dokázat. Navíc stupeň α jako algebraického prvku nad $T \leq n$.

b), c) Napřed dokážeme, že $[U : T] \leq n$. Ať pro spor $[U : T] > n$ (tento stupeň by mohl být konečný i nekonečný). Pak existuje $U \supset V \supset T$ takové, že $[V : T] = k > n$.
Ale $U \supset T$ separabilní $\Rightarrow$ $V \supset T$ separabilní.
Podle věty 2.19 pak existuje $\gamma \in V \subset U$ takové, že $V = T(\gamma)$. Pak ovšem $n < k = [V : T] =$ stupeň γ nad $T \leq n$ podle první části důkazu, což je spor.

Víme tedy, že $[U : T] \leq n$. Pro $\varphi \in \mathrm{Gal}\left({}^{U}/_{T}\right)$ máme, že $\varphi\colon U \to U$ je T-automorfismus. Tedy φ dává T-homomorfismus $\varphi\colon U \to \overline{T}$ a máme

$$n = \#G \overset{G \subset \mathrm{Gal}\left({}^{U}/_{T}\right)}{\leq} \#\,\mathrm{Gal}\left({}^{U}/_{T}\right) \leq [U : T]_s \overset{2.15}{=} [U : T] \leq n.$$

Všude tedy musí být rovnosti, takže máme $G = \mathrm{Gal}\left({}^{U}/_{T}\right)$ a $[U : T] = n$. □

2.9 Normální rozšíření

Definice. Mějme tělesa $T \subset U \subset \overline{T} =$ algebraický uzávěr T. Řekneme, že U je *normální rozšíření* T, pokud je to algebraické rozšíření takové, že pro každý T-homomorfismus $\varphi\colon U \to \overline{T}$ platí $\varphi(U) \subset U$, neboli φ dává T-homomorfismus $U \to U$.

Připomeňme, že zde pracujeme s algebraickými rozšířeními, takže platí $\overline{T} = \overline{U}$. Mezi těmito algebraickými uzávěry tedy nebudeme dále rozlišovat.

Definice. *Galoisovo rozšíření* je normální, separabilní rozšíření konečného stupně.

Následující tvrzení dává důležitou intuici pro normální rozšíření: odpovídají totiž rozkladovým nadtělesům.

Tvrzení 2.21.
a) Rozkladové nadtěleso polynomu f nad T je normální rozšíření.
b) Rozkladové nadtěleso separabilního *polynomu f nad T je* Galoisovo *rozšíření T.*
c) Každé Galoisovo rozšíření $U \supset T$ je rozkladové nadtěleso nějakého ireducibilního separabilního polynomu.

Důkaz. a) Buď $U \subset \overline{T}$ rozkladové nadtěleso f nad T. Ať $\alpha_1, \dots, \alpha_n$ jsou kořeny f v U a buď $\varphi\colon U \to \overline{T}$ T-homomorfismus $\Rightarrow \varphi$ permutuje $\{\alpha_1, \dots, \alpha_n\}$ podle tvrzení 2.11.
Jde o rozkladové nadtěleso, takže $U = T(\alpha_1, \dots, \alpha_n)$, a tedy φ je jednoznačně určené hodnotami $\varphi(\alpha_1), \dots, \varphi(\alpha_n)$, a ty jsou všechny v U. Tudíž φ každý prvek z $U = T(\alpha_1, \dots, \alpha_n)$ zobrazí do U.
Zřejmě máme, že $U \supset T$ je algebraické, jde tedy vskutku o normální rozšíření.

b) f separabilní polynom $\Rightarrow \alpha_1, \dots, \alpha_n$ separabilní prvky $\Rightarrow U = T(\alpha_1, \dots, \alpha_n)$ je separabilní rozšíření podle 2.15. Konečný stupeň je jasný a normalitu víme z části a).

c) Podle věty 2.19 je U jednoduché, čili $U = T(\gamma)$ pro nějaké γ.
Buď f minimální polynom pro γ nad T a buď $\beta \in \overline{T}$ kořen f. Chceme dokázat, že $\beta \in U$. Podle lemmatu 2.4 máme T-homomorfismus

$$\begin{aligned} \varphi\colon T(\gamma) &\to T(\beta) \subset \overline{T} \\ \gamma &\mapsto \beta \end{aligned}$$

$U \supset T$ je normální, takže $T(\beta) = \varphi(U) \subset U$, a tedy $\beta \in U$.
Vidíme, že f se v U rozkládá na lineární činitele a $U = T(\gamma)$, takže U je rozkladové nadtěleso f.

f minimální polynom pro $\gamma \Rightarrow f$ ireducibilní.
$U \supset T$ separabilní rozšíření $\Rightarrow \gamma$ separabilní prvek $\Rightarrow f$ separabilní polynom. □

Podobně jako v části c) se ukáže následující užitečné lemma.

Lemma 2.22. *Buď $U \supset T$ normální rozšíření a $f \in T[x]$ ireducibilní. Má-li f v U jeden kořen, pak už tam má všechny kořeny.*

Důkaz. Buď $\alpha \in U$ kořen f a buď $\beta \in \overline{T}$ kořen f. Podle lemmatu 2.4 máme T-homomorfismus

$$\begin{aligned} \varphi\colon T(\alpha) &\to T(\beta) \subset \overline{T} \\ \alpha &\mapsto \beta \end{aligned}$$

Pomocí důsledku 2.10b) rozšíříme φ na T-homomorfismus $\sigma\colon U \to \overline{T}$ takový, že $\sigma \restriction T(\alpha) = \varphi$.
$U \supset T$ normální, takže $\sigma(U) \subset U$. To znamená, že $\beta \in \varphi(U) \subset \sigma(U) \subset U$, jak jsme chtěli dokázat. □

Normální rozšíření jde dokonce charakterizovat jako rozkladová nadtělesa, jde ale o rozkladová nadtělesa množin polynomů podle následující definice.

Definice. $U \supset T$ je *rozkladové nadtěleso množiny polynomů* $\mathcal{M} \subset T[x]$, pokud se každý polynom $f \in \mathcal{M}$ rozkládá v U na lineární činitele a $U = T[M]$, kde M je množina všech kořenů všech polynomů $f \in \mathcal{M}$.

Tvrzení 2.23. *Rozšíření $U \supset T$ je normální, právě když existuje $\mathcal{M} \subset T[x]$ takové, že U je rozkladové nadtěleso $\mathcal{M}$ nad T.*

Důkaz. Důkaz jen naznačíme (pro detaily viz [Drápal, Tvrzení II.3.5]).
„$\Rightarrow$“ Definuj $\mathcal{M} := \{$minimální polynom nějakého $\alpha \in U\}$ a použij lemma 2.22.
„$\Leftarrow$“ Cvičení (podobně jako v tvrzení 2.21a). $\square$

Tvrzení 2.24.
Buď $U \supset T$ rozšíření a $V := \left\{ \alpha \in U \;\middle|\; \begin{array}{l} \alpha \text{ algebraické nad } T \text{ a minimální polynom} \\ \text{pro } \alpha \text{ se v } U \text{ rozkládá na lineární činitele} \end{array} \right\}$.
Pak V je těleso, které je největším normálním rozšířením T obsaženým v U.
V se nazývá „normální uzávěr T v U“.

Důkaz. Cvičení (pro důkaz viz [Drápal, Tvrzení II.3.6]). $\square$

2.10 Galoisova korespondence

Dostáváme se konečně ke vzájemně inverznímu vztahu mezi zobrazeními Fix a Gal. Několikrát se nám přitom bude hodit toto cvičení:

Cvičení (DÚ 2.2). Mějme algebraické rozšíření těles $U \supset T$ a T-homomorfismus $\varphi : U \to U$. Dokaž, že pak je φ dokonce T-automorfismus.

Důkaz. Potřebujeme dokázat, že φ je prosté a na.

Prosté: $\operatorname{Ker}(\varphi)$ je ideál v tělese U, a tedy $\operatorname{Ker}(\varphi) = 0, U$. Protože je φ T-homomorfismus, máme $T \not\subset \operatorname{Ker}(\varphi)$, a tedy $\operatorname{Ker}(\varphi) \neq U$. Tudíž $\operatorname{Ker}(\varphi) = 0$.

Na: Buď $\alpha \in U$. Protože jsme v algebraickém rozšíření, existuje minimální polynom $f(x) \in T[x]$ pro α. Podle tvrzení 2.11b) pak dává φ permutaci na množině kořenů tohoto polynomu v U, existuje tedy kořen β polynomu f takový, že $\varphi(\beta) = \alpha$. $\square$

Tvrzení 2.25. *Buď $U \supset T$ rozšíření těles. Pak:*
a) $\operatorname{Fix}\left(U, \operatorname{Gal}\left({}^{U}/_{T}\right)\right) \supset T$.
b) Pro $G < \operatorname{Aut}(U)$ je $\operatorname{Gal}\left({}^{U}/_{\operatorname{Fix}(U,G)}\right) \supset G$.
c) Je-li $U \supset T$ Galoisovo rozšíření, pak

$$[U : T] = \#\operatorname{Gal}\left({}^{U}/_{T}\right) \ \ a \ \ \operatorname{Fix}\left(U, \operatorname{Gal}\left({}^{U}/_{T}\right)\right) = T.$$

Důkaz. a) Buď $t \in T$. Pak $\varphi(t) = t$ pro každé $\varphi \in \operatorname{Gal}\left({}^{U}/_{T}\right)$, protože φ je T-homomorfismus. To ale implikuje, že $t \in \operatorname{Fix}\left(U, \operatorname{Gal}\left({}^{U}/_{T}\right)\right)$.
b) Podobně se rozepíše z definic.
c) Buď $S := \operatorname{Fix}(U, \operatorname{Gal}\left({}^{U}/_{T}\right))$. Podle a) máme $S \supset T$. Stačí tedy dokázat $[U : S] = [U : T]$ (protože pak $S = T$).

Podle věty 2.20 použité pro U a $G = \mathrm{Gal}\left({}^{U}/_{T}\right)$ máme pro $S = \mathrm{Fix}(U, G)$, že platí $[U : S] = \#G$ a $\mathrm{Gal}\left({}^{U}/_{S}\right) = G$. Tedy $[U : S] = \#\,\mathrm{Gal}\left({}^{U}/_{T}\right)$.

Rozšíření $U \supset T$ je normální, takže

$$\begin{aligned}[U : T]_s &= \#\{\varphi\colon U \to \overline{T} \mid T\text{-hom}\} \overset{\text{normální}}{=} \#\{\varphi\colon U \to U \mid T\text{-hom}\} \\ &\overset{\text{DÚ 2.2}}{=} \#\{\varphi\colon U \to U \mid T\text{-automorfismus}\} = \#\,\mathrm{Gal}\left({}^{U}/_{T}\right).\end{aligned}$$

Rozšíření $U \supset T$ je separabilní, takže $[U : T]_s = [U : T]$.
Dohromady máme $[U : T] = [U : S]$, jak jsme chtěli.

Poznamenejme, že předpoklad věty 2.20 o tom, že grupa $\mathrm{Gal}\left({}^{U}/_{T}\right)$ musí být konečná, je jasný z toho, že jsme výše dokázali, že $\#\,\mathrm{Gal}\left({}^{U}/_{T}\right) = [U : T]_s = [U : T]$. $\square$

Definice. Mějme (částečně) uspořádané množiny $(A, \leq)$ a $(B, \leq)$ a zobrazení $\alpha : A \to B$, $\beta : B \to A$ taková, že:
$a_1 \leq a_2 \Rightarrow \alpha(a_1) \geq \alpha(a_2)$,
$b_1 \leq b_2 \Rightarrow \beta(b_1) \geq \beta(b_2)$,
$a \leq \beta(\alpha(a)), b \leq \alpha(\beta(b))$.
Pak se (α, β) nazývá *(abstraktní) Galoisova korespondence mezi A a B.*

Příklad. Buď $U \supset T$ rozšíření těles a uvažujme inkluzí uspořádané množiny

$$A := \{\text{tělesa } V \mid T \subset V \subset U\} \text{ a } B := \{\text{podgrupy } G < \mathrm{Gal}\left({}^{U}/_{T}\right)\}.$$

Jako zobrazení z definice pak můžeme vzít

$$\alpha(V) = \mathrm{Gal}\left({}^{U}/_{V}\right) \text{ a } \beta(G) = \mathrm{Fix}(U, G).$$

Podle tvrzení 2.25a,b jde o Galoisovu korespondenci.

Další příklad Galoisovy korespondence uvidíme v další kapitole o algebraické geometrii.

Tvrzení 2.26. *Nechť (α, β) jsou abstraktní Galoisova korespondence.*
a) Pak α, β poskytují vzájemně inverzní bijekce mezi $\mathrm{Im}\,\alpha$ a $\mathrm{Im}\,\beta$.
b) Jsou-li α, β surjektivní, pak jsou bijektivní a dávají vzájemně inverzní antiizomorfismy uspořádaných množin $(A, \leq)$ a $(B, \leq)$.

Podobně v případě b) jsou-li navíc $(A, \leq)$ a $(B, \leq)$ *svazy*, pak α, β dávají vzájemně inverzní antiizomorfismy těchto svazů.

Důkaz. a) Pro $a \in A$ máme $\beta\alpha a \geq a$, a tedy $\alpha(\beta\alpha a) \leq \alpha a$.
Zároveň $\alpha\beta(\alpha a) \geq \alpha a$, dohromady tedy máme $\alpha\beta\alpha a = \alpha a$.

Tedy složení $\alpha\beta\colon \mathrm{Im}\,\alpha \to \mathrm{Im}\,\alpha$ je identita.
Toto složení je $\mathrm{Im}\,\alpha \xrightarrow{\beta} \mathrm{Im}\,\beta \xrightarrow{\alpha} \mathrm{Im}\,\alpha$, a tedy nutně $\alpha\colon \mathrm{Im}\,\beta \to \mathrm{Im}\,\alpha$ je na a $\beta\colon \mathrm{Im}\,\alpha \to \mathrm{Im}\,\beta$ je prosté.
Symetricky: $\alpha\colon \mathrm{Im}\,\beta \to \mathrm{Im}\,\alpha$ je prosté a $\beta\colon \mathrm{Im}\,\alpha \to \mathrm{Im}\,\beta$ je na. Tedy α, β jsou bijekce na obrazech $\mathrm{Im}\,\alpha, \mathrm{Im}\,\beta$.
b) je jasné, protože α, β z definice převracejí uspořádání. $\square$

Věta 2.27 (Základní věta Galoisovy teorie)**.** *Nechť $U \supset T$ je Galoisovo rozšíření. Potom máme antiizomorfismus uspořádaných množin*

$$\begin{aligned} \{\textit{těleso } V \mid T \subset V \subset U\} &\longleftrightarrow \{\textit{podgrupy } H < \operatorname{Gal}\left({}^{U}/_{T}\right)\} \\ V &\longmapsto \operatorname{Gal}\left({}^{U}/_{V}\right) \\ \operatorname{Fix}(U, H) &\longleftarrow\!\shortmid H \end{aligned}$$

Normální rozšíření tělesa T odpovídají normálním podgrupám $\operatorname{Gal}\left({}^{U}/_{T}\right)$*.*

Důkaz. Podle tvrzení 2.25 jde o Galoisovu korespondenci. Věta 2.20 implikuje, že zobrazení $V \mapsto \operatorname{Gal}\left({}^{U}/_{V}\right)$ je surjektivní.
Buď $T \subset V \subset U$. Pak je taky $U \supset V$ Galoisovo rozšíření (cvičení!), takže můžeme použít tvrzení 2.25c). Podle něj je $V = \operatorname{Fix}\left(U, \operatorname{Gal}\left({}^{U}/_{V}\right)\right)$, a tedy $H \mapsto \operatorname{Fix}(U, H)$ je na. Tvrzení 2.26b) pak dává antiizomorfismus.

Zbývá dokázat část o normálních rozšířeních, k čemuž dokážeme dvě implikace.
1. Ať je $V \supset T$ normální. Uvažujme $\varphi \in \operatorname{Gal}\left({}^{U}/_{T}\right)$, neboli T-automorfismus $\varphi \colon U \to U$. Jeho zúžením na V dostaneme T-homomorfismus $\varphi \restriction V : V \to U \subset \overline{T}$. Ovšem $V \supset T$ je normální, takže obraz tohoto zúžení leží ve V, neboli $\varphi \restriction V : V \to V$. Podle DÚ 2.2 pak jde o automorfismus, neboli $\varphi(V) = V$.

Buď $\psi \in \operatorname{Gal}\left({}^{U}/_{V}\right)$, k důkazu normality této podgrupy chceme dokázat, že $\varphi\psi\varphi^{-1} \in \operatorname{Gal}\left({}^{U}/_{V}\right) < \operatorname{Gal}\left({}^{U}/_{T}\right)$, tedy chceme, že $\varphi\psi\varphi^{-1}(v) = v$ pro každé $v \in V$.
Protože $\varphi(V) = V$, máme $\varphi^{-1}(v) \in V$. Tedy $\psi\varphi^{-1}(v) = \varphi^{-1}(v)$ a

$$\varphi\psi\varphi^{-1}(v) = \varphi\varphi^{-1}(v) = v.$$

Tedy $\operatorname{Gal}\left({}^{U}/_{V}\right)$ normální podgrupa v $\operatorname{Gal}\left({}^{U}/_{T}\right)$.

2. Ať je $H \lhd \operatorname{Gal}\left({}^{U}/_{T}\right)$ normální podgrupa.

Cvičení (DÚ 2.4). Buď U těleso a $G < \operatorname{Aut}(U)$ podgrupa. Dokaž, že pak pro všechna $\varphi \in \operatorname{Aut}(U)$ platí $\operatorname{Fix}(U, \varphi G \varphi^{-1}) = \varphi(\operatorname{Fix}(U, G))$.
Poznamenejme, že $\varphi G \varphi^{-1} = \{\varphi g \varphi^{-1} \mid g \in G\}$.

Pro $\varphi \in \operatorname{Gal}\left({}^{U}/_{T}\right)$ máme tedy $\operatorname{Fix}(U, \varphi H \varphi^{-1}) = \varphi(\operatorname{Fix}(U, H))$. Zároveň z normality $\varphi H \varphi^{-1} = H$, takže $\operatorname{Fix}(U, H) = \operatorname{Fix}(U, \varphi H \varphi^{-1}) = \varphi(\operatorname{Fix}(U, H))$.
Tedy každé $\varphi \in \operatorname{Gal}\left({}^{U}/_{T}\right)$ zobrazí $V = \operatorname{Fix}(U, H)$ na sebe. $\circledast$

Dokažme nyní, že $V \supset T$ je normální rozšíření. Buď $\varphi \colon V \to \overline{T}(= \overline{U} = \overline{V})$ T-homomorfismus. Podle důsledku 2.10b) jde φ rozšířit na T-homomorfismus $\psi \colon U \to \overline{T}$.
Rozšíření $U \supset T$ je normální, takže $\psi(U) \subset U$. Podle DÚ 2.2 je pak $\psi \in \operatorname{Gal}\left({}^{U}/_{T}\right)$.
Zároveň $\varphi = \psi \restriction V$. Podle $\circledast$ máme $\psi(V) = V$, a tedy $\varphi(V) = V$.
Tedy $V \supset T$ je normální rozšíření. □

2.11 Výpočty Galoisových grup

Příklad. $\operatorname{Gal}\left({}^{\mathbb{Q}(\sqrt{2})}/_{\mathbb{Q}}\right) \simeq {}^{\mathbb{Z}}/_{(2)}$

Věta 2.28. *Buď $n \in \mathbb{N}, a_1, \dots, a_n \in \mathbb{Q}$ takové, že pro každou neprázdnou podmnožinu $I \subset \{1, \dots, n\}$ máme $\prod\limits_{i \in I} \sqrt{a_i} \notin \mathbb{Q}$. Potom:*

- $\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n}) \supset \mathbb{Q}$ *je Galoisovo rozšíření*
- $[\mathbb{Q}(\sqrt{a_1}, \dots \sqrt{a_n}) : \mathbb{Q}] = 2^n$.
- $\operatorname{Gal}\left(\mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/2\right)^n$

Poznámka. Místo $\mathbb{Q}$ můžeme vzít libovolné T charakteristiky $\neq 2$.

Důkaz. Buď $K := \mathbb{Q}(\sqrt{a_1}, \dots, \sqrt{a_n})$. Klíčem k důkazu je dokázat, že $[K : \mathbb{Q}] = 2^n$. Pro důkaz tohoto faktu viz text Honzy Šarocha *Lineární nezávislost druhých odmocnin*, http://karlin.mff.cuni.cz/~kala/1819%20ko/odm.pdf.

Zde jenom naznačíme, jak z toho už snadno plyne zbytek důkazu.
Předpokládejme tedy, že $[K : \mathbb{Q}] = 2^n$. Rozšíření $K \supset \mathbb{Q}$ je konečného stupně, separabilní a normální (je totiž rozkladovým nadtělesem polynomu $(x^2 - a_1) \cdots (x^2 - a_n)$), a tedy $\# \operatorname{Gal}\left(K/\mathbb{Q}\right) = [K : \mathbb{Q}] = 2^n$.
Každý automorfismus $\varphi \in \operatorname{Gal}\left(K/\mathbb{Q}\right)$ je určený svými hodnotami na $\sqrt{a_1}, \dots, \sqrt{a_n}$ a $\varphi(\sqrt{a_i}) = \pm\sqrt{a_i}$. Takovýchto φ je tedy nejvýše 2^n.
Zároveň ale $\# \operatorname{Gal}\left(K/\mathbb{Q}\right) = 2^n$, takže každá z kombinací znamének opravdu dává prvek $\operatorname{Gal}\left(K/\mathbb{Q}\right)$. Každá volba znaménka pro $\sqrt{a_i}$ odpovídá jedné složce $\mathbb{Z}/(2)$, takže $\operatorname{Gal}\left(K/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/(2)\right)^n$. □

Podobně při určování jiných Galoisových grup je často nejtěžším krokem určení stupně daného rozšíření. Například pro cyklotomická tělesa $\mathbb{Q}(e^{2\pi i/n}) \supset \mathbb{Q}$ je stupeň rozšíření daný Eulerovou funkcí $\varphi(n)$. Důkaz tohoto faktu se opírá o důkaz ireducibility cyklotomických polynomů, který je poměrně netriviální (viz druháckou přednášku z Teorie čísel a má vznikající skripta k ní). Z toho pak už jde snadno dokázat (podobně jako v částečném důkazu tvrzení 2.28 výše), že

$$\operatorname{Gal}\left(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/n\right)^\times,$$

přičemž prvku $a \in \left(\mathbb{Z}/n\right)^\times$ odpovídá automorfismus $e^{2\pi i/n} \mapsto e^{2\pi i a/n}$.

3. Algebraická geometrie

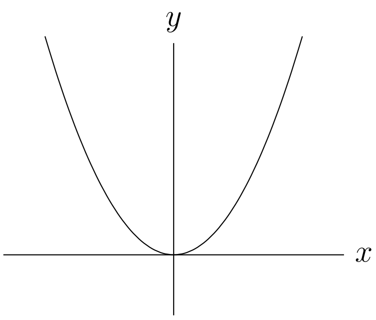
3.1 Algebraické množiny a ideály

- $K =$ těleso (časem algebraicky uzavřené)
- $R = K[x_1, \dots, x_n]$

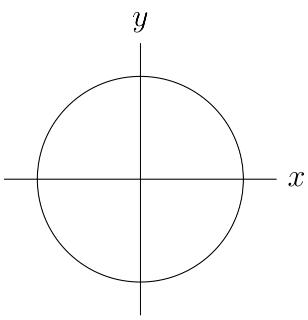
Definice. Ať $p = (a_1, \dots, a_n) \in K^n$ a $f \in K[x_1, \dots, x_n]$. Bod p je *nula* polynomu f, pokud $f(p) = 0$.
Množina všech nul polynomu f se značí $V(f)$. Pokud f není konstantní polynom, pak se $V(f)$ nazývá *nadplocha*.

Příklad.

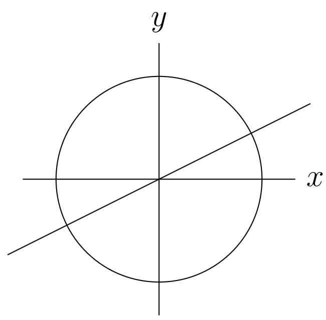
- $n = 2$:



$V(y - x^2)$

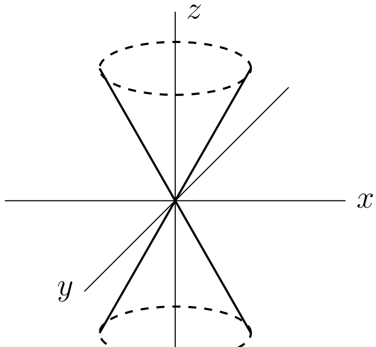


$V(x^2 + y^2 - 1)$



$V((x^2 + y^2 - 1)(x - 2y))$

- $n = 3$: kužel



$V(z^2 - y^2 - x^2)$

- $y = e^x$ není nadplocha

Definice. Pro množinu polynomů $S \subset K[x_1, \dots, x_n]$ definujeme

$$V(S) = \{p \in K^n \mid f(p) = 0 \, \forall f \in S\}.$$

Množina $X \subset K^n$ je *algebraická množina*, pokud $X = V(S)$ pro nějaké $S \subset K[x_1, \dots, x_n]$.

Zřejmě platí $S \subset S' \Rightarrow V(S) \supset V(S')$ (ale opačná implikace platit nemusí!).
Máme následující základní vlastnosti zobrazení V (připomeňme, že $R = K[x_1, \dots, x_n]$):

Lemma 3.1. *Buď $I = (S)$ ideál generovaný množinou $S \subset R$ v okruhu R. Pak $V(I) = V(S)$.*

Důkaz. „$\subseteq$“: Jasné
„$\supseteq$“: Stačí si rozepsat, jak funguje generování: $I = \{\sum r_i f_i \mid r_i \in R, f_i \in S\}$. Tedy pokud $f(p) = 0$ pro všechna $f \in S$, pak také $(\sum r_i f_i)(p) = 0$. □

Tedy každá algebraická množina je tvaru $V(I)$ pro nějaký ideál $I < R$.

Lemma 3.2. *a) Je-li $\mathcal{J}$ množina ideálů v R, pak*

$$V(\bigcup_{I \in \mathcal{J}} I) = \bigcap_{I \in \mathcal{J}} V(I).$$

Průnik libovolně mnoha algebraických množin je algebraická množina.

b) Ať $f, g \in R$ a $I, J < R$. Pak $V(fg) = V(f) \cup V(g)$ a

$$V(I) \cup V(J) = V(\{fg \mid f \in I, g \in J\}) = V(IJ).$$

Sjednocení konečně mnoha algebraických množin je algebraická množina.

c) $V(0) = K^n, V(1) = \emptyset$
$V((x_1 - a_1, \dots, x_n - a_n)) = \{(a_1, \dots, a_n)\} \; \forall (a_1, \dots, a_n) \in K^n$.
Každá konečná podmnožina K^n je algebraická.

Důkaz. Snadné cvičení. □

Spousta běžných množin jsou algebraické; cílem *algebraické geometrie* je porozumět jejich struktuře. Například máme tuto překvapivou vlastnost:

Tvrzení 3.3. *Každá algebraická množina $X \subsetneq K^n$ je průnikem konečně mnoha nadploch.*

Důkaz. Buď $X = V(I)$ pro ideál $I < R$. Protože $X \neq K^n$, máme $I \neq 0$.
Protože K je těleso, je to také noetherovský okruh. Podle důsledku 1.12 Hilbertovy věty o bázi je i $R = K[x_1, \dots, x_n]$ noetherovský. Podle tvrzení 1.10 je pak ideál I konečně generovaný, čili $I = (f_1, \dots, f_k)$ pro nějaké polynomy $f_i \neq 0$.
Tedy $X = V(I) = V(\{f_1, \dots, f_k\}) = \bigcap V(f_i)$.

Potřebujeme, že f_i jsou nekonstantní, aby $X = \bigcap$ nadplochy $V(f_i)$.
Kdyby $f_i = c, c \neq 0$, pro nějaké i, potom nutně $1 \in I$ (protože R obsahuje c^{-1}). Pak $I = R$, z čehož plyne $X = V(I) = V(R) = \emptyset$. Ale pro $X = \emptyset$ stačí zvolit například $f(x_1, \dots, x_n) = x_1, g(x_1, \dots, x_n) = x_1 + 1$ a dostaneme $V(f) \cap V(g) = \emptyset = X$. □

Definice. Pro množinu $X \subset K^n$ definujeme *ideál množiny* X jako

$$I(X) = \{f \in R \mid f(p) = 0 \ \forall p \in X\}.$$

(Zřejmě jde o ideál.)

Zřejmě máme, že $X \subset Y \Rightarrow I(X) \supset I(Y)$.

Tvrzení 3.4. *a)* $I(\emptyset) = R$.
b) $I(K^n) = 0$, *pokud je* K *nekonečné těleso.*
c) $I(\{(a_1, \dots, a_n)\}) = (x_1 - a_1, \dots, x_n - a_n)$.

Kupodivu není úplně triviální dokázat části b) a c); b) nemusí platit nad konečným tělesem:

Příklad. Buď $K = \mathbb{F}_p = \mathbb{Z}/p$.
Podle malé Fermatovy věty máme pro každé $a \in$K, že $a^p = a$, a tedy všechny tyto prvky jsou kořeny $x^p - x \in I(K)$.
(Dokonce platí $I(K) = (x^p - x)$.)

Důkaz. a) je jasné.

b) Chceme dokázat, že pokud $f(a_1, \dots, a_n) = 0$ pro všechna $a_1, \dots, a_n \in K$, potom $f = 0$.
Indukcí podle n:
$n = 1$: $f(x_1)$ má jen konečně mnoho kořenů, zatímco K je nekonečné.
$n \geq 2$: Ať

$$0 \neq f(x_1, \dots, x_n) = \sum_{i=0}^{k} f_i(x_1, \dots, x_{n-1}) x_n^i \text{ pro } f_i \in K[x_1, \dots, x_{n-1}].$$

Volme $a_1, \dots, a_{n-1} \in K$ a uvažujme $f(a_1, \dots, a_{n-1}, x_n)$. Máme 2 možnosti:
1) Je to nulový polynom (v proměnné x_n). Pak $(a_1, \dots, a_{n-1})$ je nulou všech f_i, ale $f(x_1, \dots, x_n) \neq 0$, a tedy nějaké $f_i(x_1, \dots, x_{n-1}) \neq 0$. Tento polynom pak podle IP nemá všechny $(a_1, \dots, a_{n-1}) \in K^{n-1}$ jako nuly, a tedy existuje $(a_1, \dots, a_{n-1}) \in K^{n-1}$ pro které nastane případ 2):
2) $f(a_1, \dots, a_{n-1}, x_n)$ je nenulový polynom. Ten pak má konečně mnoho kořenů, a tedy je jen konečně mnoho a_n takových, že $f(a_1, \dots, a_{n-1}, a_n) = 0$. Tedy $f \notin I(K^n)$.

c) Vyjádřeme polynom f „Taylorovým rozvojem kolem bodu $(a_1, \dots, a_n)$“, čili

$$f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n} \lambda_{i_1, \dots, i_n} (x_1 - a_1)^{i_1} \cdots (x_n - a_n)^{i_n} \text{ pro } \lambda_{i_1, \dots, i_n} \in K$$

(kde je jen konečně mnoho koeficientů $\lambda_{i_1, \dots, i_n} \neq 0$).
Proč to jde? Uvažujme polynom

$$f(y_1 + a_1, \dots, y_n + a_n) = g(y_1, \dots, y_n) = \sum \lambda_{i_1, \dots, i_n} y_1^{i_1} \cdots y_n^{i_n}.$$

Pak máme $f(x_1, \dots, x_n) = g(x_1 - a_1, \dots, x_n - a_n)$, odkud dostáváme hledané vyjádření.

Pokud $f \in I(\{(a_1, \dots, a_n)\})$, pak $\lambda_{0, \dots, 0} = f(a_1, \dots, a_n) = 0$, a tedy $f \in (x_1 - a_1, \dots, x_n - a_n)$. Opačná inkluze je jasná. $\square$

Tvrzení 3.5. *Ať $S \subset R$ a $X \subset K^n$. Pak:*
a)

$$I(V(S)) \supset S, V(I(X)) \supset X$$

Zobrazení I, V tedy dávají abstraktní Galoisovu korespondenci.
b)

$$V(I(V(S))) = V(S), I(V(I(X))) = I(X)$$

Důkaz. a) se snadno ověří rozepsáním definic.
b) pak vyplývá z tvrzení 2.26. □

Jaké jsou obrazy V a I? Obraz V jsou z definice algebraické množiny, obraz I jsou radikálové ideály (aspoň pokud je K algebraicky uzavřené), jak časem dokážeme.

3.2 Radikály

V této sekci buď R obecný okruh.

Definice. Buď $I < R$ ideál. Potom definujeme jeho *radikál*

$$\sqrt{I} = \{a \in R \mid \exists k \geq 1 : a^k \in I\}.$$

Pozorování. $\sqrt{I}$ je ideál.

Důkaz. Ať $a, b \in \sqrt{I}$. Chceme ověřit, že $a + b \in \sqrt{I}$ ($ra \in \sqrt{I}$ pro $r \in R$ je snadné).
Z definice máme $a^k, b^l \in I$ a spočteme

$$(a+b)^{k+l-1} = a^{k+l-1} + \binom{k+l-1}{1} a^{k+l-2} b + \cdots + b^{k+l-1}.$$

Prvních l sčítanců je násobkem $a^k \in I$ a zbývajících k je násobkem $b^l \in I$, celý součet tedy leží v I a $a + b \in \sqrt{I}$. □

Lemma 3.6. *Buď $X \subset K^n$. Pak $I(X)$ je* radikálový ideál*, čili $I(X) = \sqrt{I(X)}$*

Důkaz. Inkluze „$\subset$“ je jasná. Pro opačnou inkluzi „$\supset$“ mějme $f \in \sqrt{I(X)}$. Pak $f^k \in I(X)$ pro nějaké k, což znamená, že $f^k(p) = 0$ pro všechna $p \in X$. To ale implikuje $f(p) = 0$, a tedy $f \in I(X)$. □

Definice. Buď I ideál. Množina všech prvoideálů P v R, které obsahují I, se nazývá varieta I a značí se $\operatorname{Var} I$.

Cvičení. Je-li I vlastní ideál, pak je $\operatorname{Var} I$ neprázdná.

Připomeňme si, že prvoideál je z definice vlastním ideálem.

Tvrzení 3.7. *Buď $I < R$ vlastní ideál a $P \in \operatorname{Var} I$. Pak $\operatorname{Var} I$ obsahuje alespoň jeden* minimální prvek *Q takový, že $Q \subset P$. Tedy pokud $Q' \in \operatorname{Var} I$ a $Q' \subset Q$, pak $Q' = Q$.*

Důkaz. Použijeme Zornovo lemma 1.22 na množině $\operatorname{Var} I$ uspořádané *opačnou inkluzí*, čili $Q_1 \leq Q_2 \Leftrightarrow Q_1 \supset Q_2$.

Mějme řetězec $\mathcal{B}$ v $\operatorname{Var} I$. Má horní mez? Zkusme $\bigcap\limits_{Q \in \mathcal{B}} Q$.

Máme $Q \supset I$ pro všechna $Q \in \operatorname{Var} I$, a tedy $\bigcap Q \supset I$.
Je $\bigcap\limits_{Q \in \mathcal{B}} Q =: J$ prvoideál? Ať $ab \in J, a \notin J$, chceme dokázat $b \in J$.
$a \notin J$, takže existuje $Q_0 \in \mathcal{B}$ takové, že $a \notin Q\ \forall Q \subset Q_0$. Ale $ab \in J$, a tedy $ab \in Q\ \forall Q$.
Q je prvoideál, a proto $b \in Q\ \forall Q \subset Q_0$.
Jde ale o řetězec, takže $b \in Q\ \forall Q \in \mathcal{B}$, což už implikuje $b \in J$.

Předpoklady Zornova lemmatu jsou splněny, takže existuje maximální prvek Q vůči $\leq$, který je větší než P. Tento prvek Q je tedy minimální prvek vůči $\subset$ a $Q \subset P$. □

Tvrzení 3.8. *Buď I vlastní ideál v R. Pak* $\sqrt{I} = \bigcap\limits_{P \in \operatorname{Var} I} P$.

Důkaz. „$\subset$“: Ať $a \in \sqrt{I}, P \in \operatorname{Var} I$. Chceme $a \in P$.
Máme $a^k \in I \subset P$, a tedy $a^k = a^{k-1}a \in P$. Pak máme $a \in P$, jak jsme chtěli, nebo $a^{k-1} = a^{k-2}a \in P$, odkud zase $a \in P$ nebo $a^{k-2} \in P$ atd., až dostaneme ve všech případech $a \in P$.

„$\supset$“: Ať $b \in P\ \forall P \in \operatorname{Var} I$. Chceme $b \in \sqrt{I}$. Pro spor ať $b \notin \sqrt{I}$ a buď $S = \{b^k \mid k \geq 1\}$.

Připomeňme, že podle tvrzení 1.25 pro každou multiplikativní množinu S a ideál $I < R, I \cap S = \emptyset$, existuje $P \in \operatorname{Var} I$ takové, že $P \cap S = \emptyset$.

S je uzavřená na násobení, navíc $0 \notin S$, protože kdyby ano, tak $\exists k : b^k = 0 \in I$, a tedy $b \in \sqrt{I}$.
Tedy S je multiplikativní množina a můžeme použít tvrzení 1.25: $b \notin \sqrt{I}$, takže $I \cap S = \emptyset$, a tedy existuje $P \in \operatorname{Var} I$ takové, že $P \cap S = \emptyset$. Pak ale $b \notin P$, což je spor. □

Definice. Nilradikál R je ideál $\sqrt{0}$.
Máme $\sqrt{0} = \bigcap\limits_{P \text{ prvoideál}} P$.

Definice. Jacobsonův radikál $\mathcal{J}(R) = \bigcap\limits_{M \text{ maximální}} M$.

Tvrzení 3.9. *$a \in R$ leží v $\mathcal{J}(R)$, právě když $\forall r \in R$ je $1 - ra \in R^\times$.*

Důkaz. Cvičení. □

3.3 Konečně generovaná tělesa

K důkazu vztahu mezi zobrazeními I, V a popisu obrazu zobrazení I budeme potřebovat řadu tvrzení o konečné generovanosti těles jako okruh a modul.
Připomeňme tvrzení 2.1, podle nějž pro obory $R \subset S$ a $v \in S$ jsou následující tvrzení ekvivalentní:

1. v je celistvý nad R,
2. $R[v]$ je konečně generovaný R-modul ($\exists a_1, \ldots, a_k : R[v] = Ra_1 + \cdots + Ra_k$),
3. $\exists R'$ obor, $R[v] \subset R' \subset S$ a R' je konečně generovaný R-modul.

Důsledek 3.10. *Buďte $K \subset L$ tělesa, K algebraicky uzavřené. Pokud je L konečně generovaný K-modul, pak $L = K$.*

Důkaz. Mějme $\alpha \in L$. Pak $K \subset K[\alpha] \subset L$ a L je konečně generovaný K-modul, takže α je celistvý prvek. Podle tvrzení 2.1 nad K je α kořenem nějakého polynomu, čili $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ pro nějaká $a_i \in K$.
Ale K je algebraicky uzavřené, takže $\alpha \in K$. □

Lemma 3.11. *Buď K těleso a $n \geq 1$. Pak $K(x_1, \ldots, x_n)$ není konečně generovaný okruh nad K (čili neexistují $f_1, \ldots, f_m \in K(x_1, \ldots, x_n)$ takové, že $K(x_1, \ldots, x_n) = K[f_1, \ldots, f_m]$).*

Důkaz. Ať pro spor existují a buď $f_i = \frac{p_i}{q_i}$, kde $p_i, q_i \in K[x_1, \ldots, x_n]$. Zřejmě aspoň jeden $f_i \notin K[x_1, \ldots, x_n]$, čili $\deg q_i \geq 1$.
Uvažujme prvek $\frac{1}{q_1 \cdots q_m + 1} \in K[f_1, \ldots, f_m]$, tedy tento prvek jde vyjádřit jako polynom v $f_1, \ldots, f_m$. V tomto vyjádření se zbavíme jmenovatelů vynásobením $(q_1 \cdots q_m + 1) q_1^{r_1} \ldots q_m^{r_m}$, kde exponenty r_i jsou dostatečně velké. Tím dostaneme rovnost tvaru

$$q_1^{r_1} \cdots q_m^{r_m} = (q_1 \cdots q_m + 1) \cdot a \text{ pro nějaké } a \in K[x_1, \ldots, x_n].$$

Jsme v gaussovském okruhu $K[x_1, \ldots, x_n]$, takže můžeme vzít prvočinitele $f \mid q_1 \cdots q_m + 1$ s $\deg f \geq 1$. Pak $f \mid q_i$ pro nějaké i, a tedy $f \mid 1$, což je spor. □

Cvičení: R gaussovský obor a K jeho podílové těleso. Je-li $u \in K$ celistvý nad R, pak $u \in R$.

Důsledek 3.12. *Buď K těleso a $L = K(x)$. Pak neexistuje $f \in K(x)$ takové, že $\forall z \in L\, \exists n \geq 1 : f^n z$ je celistvý nad $K[x]$.*

Důkaz. Sporem. V předchozím cvičení zvolme $R = K[x]$, jehož podílové těleso je L.
$f^n z \in K(x)$ je celistvé nad R, takže $f^n z \in K[x] = R$, a tedy $z \in K[x, f^{-1}]$. Tohle ale platí pro všechna $z \in L$, takže $L = K(x) = K[x, f^{-1}]$, což je spor s lemmatem 3.11. □

Tvrzení 3.13. *Mějme tělesa $K \subset L$. Předpokládejme, že L je konečně generovaný okruh nad K, čili $L = K[v_1, \ldots, v_n]$ pro nějaká $v_1, \ldots, v_n \in L$. Pak L je konečně generovaný K-modul.*

Důkaz. Postupujme indukcí podle n.

$\underline{n = 1}$: $L = K[v]$. Máme 2 případy:
a) v je algebraický nad K, takže v je celistvé a podle tvrzení 2.1 je $L = K[v]$ konečně generovaný K-modul.

b) v není algebraické nad K, takže $L = K[v] = K[x]$. Ale L je těleso, takže zároveň $L = K(x)$, což je spor s lemmatem 3.11.

$\underline{n \geq 2}$: Buď $K_1 = K(v_1)$, takže $L = K_1[v_2, \ldots, v_n]$. IP implikuje, že L je konečně generovaný K_1-modul. Opět rozlišíme dva případy:

a) v_1 je algebraické nad K. Pak $K_1 = K[v_1]$ je konečně generovaný K-modul a podle DÚ 2.1 je L konečně generovaný K-modul.

b) $v_1 = x$ je transcendentní nad K. L je konečně generovaný K_1-modul, takže podle 2.1 jsou $v_2, \dots, v_n$ celistvé nad K_1.
Máme tedy rovnosti $v_i^{n_i} + a_{i,n_i-1}v_i^{n_i-1} + \dots + a_{i,0} = 0$ pro $a_{ij} \in K_1$.
Ty vynásobíme α^{n_i}, kde $\alpha \in K[x]$ je společný násobek jmenovatelů všech a_{ij}. Tím dostaneme

$$(\alpha v_i)^{n_i} + \alpha a_{i,n_i-1}(\alpha v_i)^{n_i-1} + \dots + \alpha^{n_i} a_{i,0} = 0,$$

takže prvky αv_i jsou celistvé nad $K[x]$.
$L = K[x][v_2, \dots, v_n]$, takže pro každé $z \in L$ existuje n takové, že $\alpha^n z$ je polynom v $\alpha v_2, \dots, \alpha v_n$ s koeficienty v $K[x]$. To jsou celistvé prvky a celistvé prvky tvoří okruh, takže $\alpha^n z$ je celistvý nad $K[x]$. Speciálně to platí pro $z \in K(x) \subset L$, což je ale spor s důsledkem 3.12 (všimněme si, že $\alpha \in K[x] \subset K(x)$). Tedy b) nemůže nastat, může nastat pouze případ a), v němž jsme tvrzení už dokázali. □

Důsledek 3.14. *Nechť $K \subset L$ jsou tělesa a K je algebraicky uzavřené. Pokud je L konečně generovaný okruh nad K, potom $L = K$.*

Důkaz. Tvrzení 3.13 + důsledek 3.10. □

3.4 Hilbertova věta o nulách

Věta 3.15 (Slabá Hilbertova věta o nulách)**.**
Buď K těleso a $R = K[x_1, \dots, x_n]$. Pak:

a) Ideál $I = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$ je maximální v R pro každá $\alpha_1, \dots, \alpha_n \in K$. Navíc polynom $f \in R$ leží v tomto ideálu, právě když $f(\alpha_1, \dots, \alpha_n) = 0$.

b) Pokud je K algebraicky uzavřené, potom všechny maximální ideály v R jsou tvaru $(x_1 - \alpha_1, \dots, x_n - \alpha_n)$ pro nějaká $\alpha_1, \dots, \alpha_n \in K$.

Důkaz.
a) Polynom $f \in R$ uvažujme jako polynom v proměnné x_n nad $K[x_1, \dots, x_{n-1}]$. Můžeme jej napsat jako $f = a_n(x_n - \alpha_n) + b_{n-1}$, kde $a_n \in R$ a $b_{n-1} \in K[x_1, \dots, x_{n-1}]$. Podobně $b_{n-1} = a_{n-1}(x_{n-1} - \alpha_{n-1}) + b_{n-2}$, až postupně dostaneme

$$f = \sum_{i=1}^{n} a_i(x_i - \alpha_i) + b_0, \text{ pro } a_i \in R, b_0 \in K.$$

Vidíme, že $\sum a_i(x_i - \alpha_i) \in I = (x_1 - \alpha_1, \dots, x_n - \alpha_n)$. Tedy platí:
„Navíc“: $f \in I \Leftrightarrow f - \sum_{i=1}^{n} a_i(x_i - \alpha_i) \in I \Leftrightarrow b_0 \in I \Leftrightarrow b_0 = f(\alpha_1, \dots, \alpha_n) = 0$.
„Maximalita“: Nechť $f \notin I$, neboli $b_0 \neq 0$. Uvažujme ideál $I + (f)$. Ten obsahuje $b_0 \in K^\times$, a tedy $1 = b_0 b_0^{-1} \in I + (f)$ a $I + (f) = R$. Tedy I je maximální ideál.

b) Nechť M je maximální ideál v R. Potom $L = R/M$ je těleso a navíc K můžeme brát jako podtěleso L, protože máme projekci $\pi\colon R \twoheadrightarrow R/M$, jejíž zúžení $\pi \restriction K\colon K \to R/M$ je prosté (protože $\operatorname{Ker}(\pi \restriction K) < K$)).
Ale L je nad K generované prvky $x_1 + M, \dots, x_n + M$ jako okruh. Důsledek 3.14 $\Rightarrow L = K$.
Tedy

$$\pi \restriction K\colon K \to L = R/M$$
$$a \mapsto a + M$$

je izomorfismus, tedy je speciálně surjektivní.
Tudíž pro každé i existuje α_i tak, že $x_i + M = \alpha_i + M$. Tedy $x_i - \alpha_i \in M$, takže $(x_1 - \alpha_1, \ldots, x_n - \alpha_n) \subset M$. Ale ideál $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ je maximální podle a), a tedy se rovná M. □

Speciálně vidíme, že $V(I) \neq \emptyset$ pro každý vlastní ideál $I < R$ (pokud je K algebraicky uzavřené). Máme totiž, že $I \subset M$ pro nějaký maximální ideál M, a pak $V(I) \supset V(M) = \{(\alpha_1, \ldots, \alpha_n)\}$.

Věta 3.16 (Hilbertova věta o nulách)**.** *Ať je K algebraicky uzavřené těleso a I ideál v $R = K[x_1, \ldots, x_n]$. Potom $I(V(I)) = \sqrt{I}$.*

Důkaz. „$\supset$“: cvičení
„$\subset$“: Buď $g \in I(V(I))$, chceme $g \in \sqrt{I}$.
Každý ideál v noetherovském okruhu R je konečně generovaný podle tvrzení 1.10. Tedy $I = (f_1, \ldots, f_r)$ pro nějaké polynomy $f_1, \ldots, f_r \in R$.

Uvažujme ideál $J = (f_1, \ldots, f_r, x_{n+1}g - 1) < K[x_1, \ldots, x_{n+1}]$. Potom $V(J) = \emptyset$, protože: Pokud $f_1(\alpha) = \cdots = f_r(\alpha) = 0$ pro nějaké $\alpha \in K^n$, potom taky $g(\alpha) = 0$. Tedy pokud $(\alpha, \alpha_{n+1}) \in K^{n+1}$, potom $g(\alpha, \alpha_{n+1}) = g(\alpha) = 0$, a tedy $\alpha_{n+1}g(\alpha, \alpha_{n+1}) - 1 = -1 \neq 0$, takže $(\alpha, \alpha_{n+1}) \notin V(J)$.

Tedy J není vlastní ideál díky slabé Hilbertově větě o nulách 3.15. Máme tedy $J = K[x_1, \ldots, x_{n+1}] \ni 1$, takže $\exists a_i, b \in K[x_1, \ldots, x_{n+1}]$ takové, že $1 = \sum a_i f_i + b(x_{n+1}g - 1)$. Označme $y = \frac{1}{x_{n+1}}$, neboli $x_{n+1} = \frac{1}{y}$. Po dosazení do vyjádření pro 1 dostaneme nějaké mocniny y ve jmenovatelích, takže vynásobme rovnost y^N tak, abychom se jich zbavili. Tím dostaneme $\sum c_i f_i + d(g - y) = y^N$, kde $c_i, d \in K[x_1, \ldots, x_n, y]$. Sem konečně dosadíme $y = g$ a máme $I \ni \sum c_i f_i + 0 = g^N$, tedy $g \in \sqrt{I}$. □

Tímto jsme popsali obraz zobrazení I, takže z abstraktní Galoisovy korespondence 2.26 dostáváme:

Důsledek 3.17. *Buď K algebraicky uzavřené těleso. Pokud je I radikálový ideál v $R = K[x_1, \ldots, x_n]$ (tedy $I = \sqrt{I}$), potom $I(V(I)) = \sqrt{I}$.*
Tedy máme bijekci (respektive antiizomorfismus uspořádaných množin)

$$\{\textit{radikálové ideály v } R\} \leftrightarrow \{\textit{algebraické množiny v } K^n\}$$
$$I \mapsto V(I)$$
$$I(X) \leftarrow\!\shortmid X$$

Maximální ideály odpovídají bodům v K^n.

3.5 Ireducibilní algebraické množiny

Čemu odpovídají prvoideály v této korespondenci?

Definice. Buď K těleso. Algebraická množina $V \subset K^n$ je *reducibilní*, pokud $V = V_1 \cup V_2$ pro nějaké algebraické množiny $V_1, V_2 \subset K^n$, $V_1 \neq V \neq V_2$. Jinak je V *ireducibilní*.

Tvrzení 3.18. *Neprázdná algebraická množina V je ireducibilní, právě když $I(V)$ je prvoideál.*

Důkaz. DÚ 3.4 □

Lemma 3.19. *a) Buď $\mathcal{S}$ neprázdná množina ideálů v noetherovském okruhu R. Potom $\mathcal{S}$ má maximální prvek, tedy existuje $I \in \mathcal{S}$ takový, že pro každé $J \in \mathcal{S}$ máme $I \subset J \Rightarrow I = J$.*
b) Každá neprázdná množina algebraických množin $\mathcal{T}$ v K^n má minimální prvek.

Důkaz. a) Sporem: Ať to neplatí, tedy pro každé $I \in \mathcal{S}$ existuje $J \in \mathcal{S}$ takové, že $I \subsetneq J$. Zvolme libovolné $I_1 \in \mathcal{S}$; pak ať $I_2 \in \mathcal{S}$ splňuje $I_1 \subsetneq I_2$. Podobně volme $I_2 \subsetneq I_3$, atd. (zde potřebujeme použít axiom výběru), čímž dostaneme nekonečný rostoucí řetězec ideálů v noetherovském okruhu, což je spor.
b) Uvažujeme $\mathcal{S} := \{I(V) \mid V \in \mathcal{T}\}$. Je-li $I(V)$ její maximální prvek, pak je V minimální prvek $\mathcal{T}$. □

Věta 3.20. *Buď $V \subset K^n$ algebraická množina. Potom existují jednoznačně určené algebraické množiny $V_1, \ldots, V_m$ takové, že V_i je ireducibilní, $V = V_1 \cup \cdots \cup V_m$ a $V_i \not\subset V_j$ pro $i \neq j$. V_i jsou ireducibilní komponenty množiny V.*

Důkaz. Buď $\mathcal{T} = \left\{ \text{algebraická množiny } V \subset K^n \,\middle|\, \begin{array}{l} V \text{ není sjednocení konečně mnoha} \\ \text{ireducibilních algebraických množin} \end{array} \right\}$.
Pro spor nechť $\mathcal{T} \neq \emptyset$. Podle lemmatu 3.19 pak existuje její minimální prvek V. V není ireducibilní, takže $V = V_1 \cup V_2$ pro algebraické množiny $V_1, V_2 \subsetneq V$. Z minimality V máme $V_1, V_2 \notin \mathcal{T}$, a tedy V_1, V_2 se dají rozložit, takže jde rozložit i V, což je spor.

Každé V tedy jde napsat jako $V = V_1 \cup \cdots \cup V_m$ pro ireducibilní V_i. Zahodíme všechny V_i takové, že $\exists j\, V_i \subset V_j$.

Jednoznačnost: Nechť $V = V_1 \cup \cdots \cup V_m = W_1 \cup \cdots \cup W_n$. Potom $V_i = (V_i \cap W_1) \cup \cdots \cup (V_i \cap W_n)$. Jde o ireducibilní množinu, takže existuje $j = \sigma(i)$ takové, že $V_i = V_i \cap W_{\sigma(i)}$, čili $V_i \subset W_{\sigma(i)}$.
Podobně existuje k takové, že $W_{\sigma(i)} \subset V_k$. Tedy $V_i \subset V_k$, takže $i = k$ a $V_i = W_{\sigma(i)}$. Symetricky $\forall j\, \exists \rho(j) : W_j = V_{\rho(j)}$. □

Důsledek 3.21. *Ať je K algebraicky uzavřené těleso. Je-li I prvoideál, pak je $V(I)$ ireducibilní.*
Máme bijekci

$$\{\textit{prvoideály v } K[x_1, \ldots, x_n]\} \leftrightarrow \{\textit{ireducibilní algebraické množiny v } K^n\}.$$

Důkaz. Pokud I je prvoideál, pak $I = \sqrt{I} = I(V(I))$ podle Hilbertovy věty o nulách 3.16. Podle tvrzení 3.18 pak to, že $I(V(I))$ je prvoideál, implikuje, že $V(I)$ ireducibilní.
Zbytek důsledku je jasný. □

Důsledek 3.22. *Buď K algebraicky uzavřené těleso a $f = f_1^{n_1} \cdots f_r^{n_r} \in K[x_1, \ldots, x_n]$ ireducibilní rozklad nekonstantního polynomu f.*
Pak $V(f) = V(f_1) \cup \cdots \cup V(f_r)$ je ireducibilní rozklad $V(f)$ a $I(V(f)) = (f_1 \cdots f_r)$.
Máme bijekci $\left\{ \begin{array}{l} \textit{ireducibilní nekonstantní monické} \\ \textit{polynomy v } K[x_1, \ldots, x_n] \end{array} \right\} \leftrightarrow \{\textit{ireducibilní nadplochy v } K^n\}$.

Důkaz. Cvičení. □

4. Algebraická teorie čísel

4.1 Rozklady diofantických rovnic

Algebraická teorie čísel se zabývá vlastnostmi *číselných těles*, tedy rozšíření $K \supset \mathbb{Q}$ konečného stupně. Motivací pro její rozvoj byla snaha o řešení diofantických rovnic, jak zde stručně nastíníme. Pro výrazně víc informací a řešených příkladů doporučuji diplomku Maroše Hrnčiara http://karlin.mff.cuni.cz/~kala/theses/hrnciar.pdf.

4.1.1 $x^2 + 1 = y^3$

Příklad. Najdi všechna celá čísla x, y taková, že $x^2 + 1 = y^3$.

Řešení. Rovnici rozložíme jako $(x + i)(x - 1) = y^3$ v $\mathbb{Z}[i]$.
Jen stručně nastíníme princip. Postupně se dokáže:

1. $\mathrm{NSD}(x + i, x - i) = 1$
2. $x + i \parallel (a + bi)^3$ pro $a, b \in \mathbb{Z}$.
3. $x + i = \varepsilon(a + bi)^3$, kde $\varepsilon \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Jsou tedy potřeba rozlišit tyto 4 případy, ilustrujme zbytek řešení jen pro $\varepsilon = 1$.
4. $x + i = 1 \cdot (a + b)^3 = a^3 + 3a^2bi - 3ab^2 - b^3i$
5. $1 = \mathrm{Im}(x + i) = 3a^2b - b^3 = b(3a^2 - b^2)$
6. $a = 0, b = -1$
7. $x = \mathrm{Re}(x + i) = a^3 - 3ab^3$
8. $x = 0 \Rightarrow y = 1$
9. Ostatní tři případy dopadnou stejně (ve skutečnosti totiž nebylo potřeba je rozlišovat, protože každá jednotka je třetí mocninou), takže rovnice má jedno řešení $(0, 1)$.

Jaké vlastnosti $\mathbb{Z}[i]$ jsme použili?

- konjugace $\overline{a + bi} = a - bi$ je netriviální prvek $\mathrm{Gal}\left(\mathbb{Q}(i)/\mathbb{Q}\right)$
- $\alpha \mid \beta \Rightarrow \overline{\alpha} \mid \overline{\beta}$
- Norma $N(\alpha) = \alpha\overline{\alpha} = a^2 + b^2$
- $\alpha \mid \beta \Rightarrow N\alpha \mid N\beta$
- Jednotky $\mathbb{Z}[i]^\times$:
  $\alpha \in \mathbb{Z}[i]^\times \Leftrightarrow N\alpha = \pm 1$. Tedy $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
- Gaussovskost (v kroku 1. $\Rightarrow$ 2.).

4.1.2 $x^2 + 5 = y^3$

Příklad. Najdi všechna celá čísla x, y taková, že $x^2 + 5 = y^3$.

Řešení. Opět rozložíme jako $(x + \sqrt{-5})(x - \sqrt{-5}) = y^3$ v $\mathbb{Z}[\sqrt{-5}]$.
Vlastnosti $\mathbb{Z}[\sqrt{-5}]$:

- $(a + b\sqrt{-5})' = a - b\sqrt{-5}$
- $N\alpha = \alpha\alpha' = a^2 + 5b^2 \geq 0$
- $\alpha \in \mathbb{Z}[\sqrt{-5}]^\times \Leftrightarrow N\alpha = \pm 1 \Leftrightarrow \alpha = \pm 1.$
- Gaussovskost? Ne!

Například $2\cdot 3 = 6 = (1-\sqrt{-5})(1+\sqrt{-5})$, ale $2, 3, 1\pm\sqrt{-5}$ jsou (neasociované) ireducibilní prvky. Ukážeme to na příkladu 2:

Ať $\alpha \mid 2, \alpha \nparallel 1, \alpha \nparallel 2$.
Tedy $N\alpha \mid N2 = 4 \Rightarrow N\alpha = 1, 2, 4$. Protože α není invertibilní, $N\alpha \neq 1$.
Pokud $N\alpha = 4$, potom $N(\frac{2}{\alpha}) = 1$, tedy $\frac{2}{\alpha}$ je jednotka a $\alpha \parallel 2$.
$2 = N\alpha = a^2 + 5b^2$ není možné, protože taková celá čísla a, b neexistují.

Aby se vyřešil problém s nejednoznačnými rozklady, zavedla se „ideální čísla“:
$A = (2, 1 + \sqrt{-5})$, kde si značení představujeme jako NSD
$A' = (2, 1 - \sqrt{-5})$
$B = (3, 1 + \sqrt{-5})$
$B' = (3, 1 - \sqrt{-5})$

Pak dává smysl uvažovat, že $2 = AA', 1 + \sqrt{5} = AB, 1 - \sqrt{5} = A'B', 3 = BB'$, takže máme jednoznačný rozklad $6 = AA'BB'$.
Vzpomeňme si, že v $\mathbb{Z}$ NSD odpovídá sčítání ideálů $(\mathrm{NSD}(m, n)) = (m) + (n))$.
Uvažujme tedy $A = (2, 1 + \sqrt{-5}) = 2 \cdot \mathbb{Z}[\sqrt{-5}] + (1 - \sqrt{-5})\mathbb{Z}[\sqrt{5}]$ jako ideál.
Násobení ideálů pak vyjde $A \cdot A' = (2), A \cdot A' \cdot B \cdot B' = (6)$.
Prvoideály odpovídají prvočinitelům a skutečně platí:

Věta. *Každý nenulový ideál v $\mathbb{Z}[\sqrt{-5}]$ jde jednoznačně rozložit na součin prvoideálů.*

Důkaz. Časem jako speciální případ věty 4.17. □

Ideály generují grupu $\mathcal{I} = \{AB^{-1} \mid A, B \text{ nenulové ideály}\}$. Definujeme $(AC) \cdot (BC)^{-1} = AB^{-1}$.
Pro $\alpha \in \mathbb{Z}[\sqrt{-5}]$ máme hlavní ideál (α).
$\mathcal{P} = \{(\alpha) \cdot (\beta)^{-1} \mid \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]\}$ je podgrupa v $\mathcal{I}$.

Platí: OHI $\Leftrightarrow \mathcal{I} = \mathcal{P} \Leftrightarrow \mathcal{I}/\mathcal{P} = \{1\}$.
Také OHI $\Rightarrow$ Gaussovskost.

Definuje se tedy *třídová grupa* jako $\mathcal{C}\ell := \mathcal{I}/\mathcal{P}$.
Obecně: $\mathcal{C}\ell$ je vždy *konečná.* (Její velikost měří, „jak špatná je nejednoznačnost rozkladů“).

Pro $\mathbb{Z}[\sqrt{-5}]$ máme $\mathcal{C}\ell \simeq \mathbb{Z}/(2)$ a konečně můžeme naznačit řešení naší rovnice $(x + \sqrt{-5})(x - \sqrt{-5}) = y^3$.

1. Počítáním s ideály zjistíme, že neexistuje žádný prvoideál P, který by dělil $x + \sqrt{-5}$ i $x - \sqrt{-5}$, tyto dva prvky (resp. jejich hlavní ideály) jsou tedy nesoudělné.

2. Uvažujme teď rozklad na součin prvoideálů v rovnici $(x+\sqrt{-5})(x-\sqrt{-5}) = (y)^3$:
$P_1^{k_1}\cdots P_r^{k_r} Q_1^{l_1}\cdots Q_s^{l_s} = R_1^{3m_1}\cdots R_t^{3m_t}$.
Z nesoudělnosti v bodu 1. máme $P_i \neq Q_j$.
Tedy jednoznačnost rozkladů implikuje $3 \mid k_i, 3 \mid l_j$ pro všechna i, j.

3. Existuje tedy ideál $A < \mathbb{Z}[\sqrt{-5}]$ takový, že $(x+\sqrt{-5}) = A^3$.

4. Tento ideál je hlavní, čili $A \in \mathcal{P}$, protože:
Víme, že $A^3 \in \mathcal{P}$. $\#\mathcal{C}\ell = 2$, a tedy pro libovolný ideál platí $I^2 \in \mathcal{P}$. Pro náš ideál to ale implikuje $A = A^3 \cdot (A^2)^{-1} \in \mathcal{P}$.

5. Ať $A = (a + b\sqrt{-5})$. Tedy $x + \sqrt{-5} = \pm(a+b\sqrt{-5})^3$. Toto už snadno dořešíme roznásobením a porovnáním racionálních a iracionálních částí; vyjde, že daná rovnice nemá žádné řešení v $\mathbb{Z}$.

Podobně se matematici snažili dokázat velkou Fermatovu větu o rovnici $x^p - y^p = z^p$:
$(x-y)(x-\zeta_p y)\cdots(x-\zeta_p^{p-1}y)$, kde $\zeta_p = e^{\frac{2\pi i}{p}} \rightsquigarrow \mathbb{Z}[\zeta_p]$.

4.2 Celistvé prvky

Definice. Těleso K je *číselné těleso*, pokud je to rozšíření $\mathbb{Q}$ konečného stupně.

Příklad. $\mathbb{Q}(\sqrt{D}), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\zeta_p), \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, kde $\zeta_p = e^{\frac{2\pi i}{p}}$.
Vhodnou analogií celých čísel v K jsou celistvé prvky (viz sekci 2.3).

Definice. Okruh všech prvků tělesa K, jež jsou celistvé nad $\mathbb{Z}$, se značí $\mathcal{O}_K$.

Zřejmě: $\mathcal{O}_{\overline{\mathbb{Q}}} \cap K = \mathcal{O}_K$.

Lemma 4.1. *Buď K číselné těleso. Pro $\alpha \in K$ buď $m_\alpha(x) \in \mathbb{Q}[x]$ jeho minimální monický polynom. Pak $\alpha \in \mathcal{O}_K$, právě když $m_\alpha \in \mathbb{Z}[x]$.*

Důkaz. „$\Leftarrow$“: Jasné
„$\Rightarrow$“: Ať $f \in \mathbb{Z}[x]$ je monický takový, že $f(\alpha) = 0$. Pak $m_\alpha \mid f$ v okruhu $\mathbb{Q}[x]$, čili $f = m_\alpha \cdot g$ pro nějaké $g \in \mathbb{Q}[x]$. g je tedy také monický.
Buď p prvočíslo. Vedoucí koeficient g je 1 a $v_p(1) = 0$, tedy obsah $c_p(g) \leq 0$. Stejně tak $c_p(m_\alpha) \leq 0$.
Zároveň víme, že $c_p(m_\alpha) + c_p(g) = c_p(f) = 0$, a tedy $c_p(g) = 0 = c_p(m_\alpha)$. Toto platí pro všechna prvočísla p, takže $m_\alpha \in \mathbb{Z}[x]$. □

Důsledek 4.2.
a) $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$
b) Každý prvek $\alpha \in K$ jde napsat jako $\frac{\beta}{n}$, kde $\beta \in \mathcal{O}_K, n \in \mathbb{N}$.

Důkaz.
a) $\alpha \in \mathcal{O}_K \cap \mathbb{Q} \Leftrightarrow m_\alpha(x) = (x-\alpha) \in \mathbb{Z}[x] \Leftrightarrow \alpha \in \mathbb{Z}$.

b) Vynásobíme $m_\alpha(x)$ nejmenším společným násobkem n jmenovatelů koeficientů m_α, čili $n \cdot m_\alpha \in \mathbb{Z}[x]$ a $c_p(n \cdot m_\alpha) = 0$ pro všechna prvočísla p.
Snadno se ověří, že $n\alpha \in \mathcal{O}_K$ (porovnej $n \cdot m_\alpha$ a $m_{n\alpha}$).
Pak $\alpha = \frac{\beta}{n}$ pro $\beta = n\alpha \in \mathcal{O}_K$. □

Příklad. Uvažujme kvadratické těleso $K = \mathbb{Q}(\sqrt{D})$ pro bezčtvercové $D \neq 0, 1$.
Pak m_α má stupeň ≤ 2 pro všechna $\alpha \in K$.

Pro $\alpha = a + b\sqrt{D}$ (s $b \neq 0$) je

$$m_\alpha(x) = (x - \alpha)(x - \alpha') = x^2 - (\alpha + \alpha')x + \alpha \cdot \alpha' = x^2 - 2ax + (a^2 - Db^2),$$

kde $\alpha' = a - b\sqrt{D}$.
Proč je to minimální polynom pro α?
$\alpha \notin \mathbb{Q}$, a tedy m_α má stupeň přesně 2. Polynom $(x - \alpha)(x - \alpha') \in \mathbb{Q}[x]$ má α za kořen a stupeň 2, je to tedy vskutku minimální polynom m_α.
Tvaru tohoto polynomu jde výhodně využít k určování okruhu celistvých prvků, jak uvidíme v další sekci.

4.3 Norma a stopa

Po celý zbytek kapitoly buď $K = \mathbb{Q}(\sqrt{D}), D \neq 0, 1$ bezčtvercové.

Definice. Normu definujeme jako zobrazení

$$\begin{aligned} N = N_{K/\mathbb{Q}} \colon K &\to \mathbb{Q} \\ \alpha = a + b\sqrt{D} &\mapsto \alpha \cdot \alpha' = a^2 - b^2 D \end{aligned}$$

kde $\alpha' = a - b\sqrt{D}$.

Definice. Stopu definujeme jako zobrazení

$$\begin{aligned} \mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}} \colon K &\to \mathbb{Q} \\ \alpha = a + b\sqrt{D} &\mapsto \alpha + \alpha' = 2a \end{aligned}$$

Pozorování.

- $\alpha \in \mathcal{O}_K \Leftrightarrow \mathrm{Tr}(\alpha), N\alpha \in \mathbb{Z}$.
  Pro $\alpha \in K \setminus \mathbb{Q}$ jsme to dokázali v příkladu výše; pro $\alpha \in \mathbb{Q}$ jde o jednoduché cvičení.
- $(\alpha\beta)' = \alpha'\beta'$, $(\alpha + \beta)' = \alpha' + \beta'$
- $N(\alpha\beta) = N\alpha \cdot N\beta$, neboť to můžeme rozepsat jako $(\alpha\beta)(\alpha\beta)' = (\alpha\alpha')(\beta\beta')$.
  $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$ podobně.

Věta 4.3. *Buď $D \neq 0, 1$ bezčtvercové a $K = \mathbb{Q}(\sqrt{D})$. Pak*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \textit{pro } D \equiv 2, 3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \textit{pro } D \equiv 1 \pmod 4 \end{cases}$$

Důkaz. Dokážeme inkluzi „$\subset$“, opačnou inkluzi necháme jako lehké cvičení.
Ať $\alpha \in \mathcal{O}_K, \alpha = a + b\sqrt{D}$. Pak stopa $\mathrm{Tr}(\alpha) = 2a$ je celé číslo, a tedy $a = c/2$ pro $c \in \mathbb{Z}$.
Norma je také celočíselná, čili

$$N\alpha = a^2 - b^2 D = \frac{c^2 - 4b^2 D}{4} \in \mathbb{Z}.$$

Speciálně máme $4b^2D = (2b)^2D \in \mathbb{Z}$.
Jmenovatel racionálního čísla $(2b)^2$ je čtverec, který musí dělit D, aby $(2b)^2D \in \mathbb{Z}$. Ovšem D je bezčtvercové, a tedy tento jmenovatel je 1, čili $(2b)^2$ i $(2b)$ jsou v $\mathbb{Z}$.
Buď $b = \frac{d}{2}$ pro $d \in \mathbb{Z}$. Pak $N\alpha = \frac{c^2-d^2D}{4} \in \mathbb{Z}$ implikuje $c^2 \equiv d^2D \pmod 4$.

Všimněme si, že protože $4 \nmid D$, čísla c a d mají stejnou paritu. Rozlišme tedy dva případy:
1) c, d sudá. Pak $a = \frac{c}{2}, b = \frac{d}{2} \in \mathbb{Z}$.
2) c, d lichá. Pak $1 \equiv c^2 \equiv d^2 \equiv D \pmod 4$, čili nutně $D \equiv 1 \pmod 4$.

Tedy pro $D \equiv 2, 3 \pmod 4$ musí nastat případ 1), a tedy $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$.
Pokud $D \equiv 1 \pmod 4$, může se taky stát, že c, d jsou obě lichá.
Pak ale $\alpha = a + b\sqrt{D} = \left(\frac{c-1}{2} + \frac{d-1}{2}\sqrt{D}\right) + \frac{1+\sqrt{D}}{2}$. Protože první sčítanec leží v $\mathbb{Z}[\sqrt{D}] \subset \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, dostáváme $\alpha \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. □

Tvrzení 4.4. $\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K \mid N\alpha = \pm 1\}$

Důkaz. „$\subset$“: $\alpha \in \mathcal{O}_K^\times \Rightarrow \exists \beta : \alpha\beta = 1 \Rightarrow N(\alpha) \cdot N(\beta) = N(1) = 1$.
$N\alpha, N\beta \in \mathbb{Z} \Rightarrow N\alpha = \pm 1$
„$\supset$“: $N\alpha = \pm 1 \Rightarrow \alpha \cdot \alpha' = \pm 1 \Rightarrow \pm\alpha'$ je inverzní prvek k α. □

Příklad. $K = \mathbb{Q}(\sqrt{D})$

- $D < 0 \Rightarrow a^2 + b^2(-D) = \pm 1 \Rightarrow$ konečně mnoho jednotek, typicky jenom $\mathcal{O}_K^\times = \{\pm 1\}$. Více jednotek máme jen ve dvou případech, a sice
  $\mathcal{O}_{\mathbb{Q}(i)}^\times = \{\pm 1, \pm i\}$.
  $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}^\times = \{e^{\frac{k\pi i}{3}} \mid k \in \{0, 1, 2, 3, 4, 5\}\}$

- $D > 0, D \equiv 2, 3 \pmod 4$. Jde o řešení Pellovy rovnice $x^2 - Dy^2 = \pm 1$, jež má nekonečně mnoho řešení.
  Například pro $D = 2$ máme $\mathcal{O}_K^\times = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$.
  (Pro $0 < D \equiv 1 \pmod 4$ je třeba uvažovat Pellovu rovnici $x^2 - Dy^2 = \pm 4$.)

4.4 Ideály

Nemáme jednoznačné rozklady na součin ireducibilních prvků. Například v $\mathbb{Z}[\sqrt{-14}]$ platí

$$3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14}) \text{ a } 3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14}),$$

což jsou vše ireducibilní prvky.
Místo toho budeme rozkládat na součin prvoideálů, jak jsem už naznačili v sekci 4.1. K tomu si napřed dokážeme některé základní vlastnosti ideálů.
Stejně jako v celé kapitole buď $K = \mathbb{Q}(\sqrt{D})$ pro bezčtvercové $D \neq 0, 1$.

Tvrzení 4.5. *Každý ideál v $\mathcal{O}_K$ je konečně generovaný, a to nejvýše dvěma generátory.*

Důkaz. Ideál I v $\mathcal{O}_K$ je podgrupa $I(+)$ v $\mathcal{O}_K(+) \simeq \mathbb{Z}^2(+)$ podle věty 4.3. Ale každá podgrupa v $\mathbb{Z}^2$ je izomorfní $\mathbb{Z}^n$ pro nějaké $0 \leq n \leq 2$ (cvičení). Tedy $I(+) \simeq \mathbb{Z}^n(+)$, a tedy I má $n \leq 2$ generátorů jako abelovská grupa. □

Příklad. Jak vypadá izomorfismus $\mathcal{O}_K(+) \simeq \mathbb{Z}^2(+)$?
a) $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$. Pak $a + b\sqrt{D} \mapsto (a,b) \in \mathbb{Z}^2$.
b) $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$. Pak $a + b\frac{1+\sqrt{D}}{2} \mapsto (a,b) \in \mathbb{Z}^2$.

Důsledek 4.6. *$\mathcal{O}_K$ je noetherovský obor.*

Důkaz. Tvrzení 1.10 + tvrzení 4.5. □

Lemma 4.7. *Buď $I < \mathcal{O}_K$ ideál takový, že $I = (a_1, \dots, a_m)$ pro $a_1, \dots, a_m \in \mathbb{Z}$. Pak $I = (a)$ je hlavní (pro nějaké $a \in \mathbb{Z}$).*

Důkaz. Buď $a = \mathrm{NSD}(a_1, \dots, a_m)$ v $\mathbb{Z}$. Pak $a \mid a_i$ v $\mathbb{Z}$, takže $a \mid a_i$ v $\mathcal{O}_K$, a tedy $a_i \in (a)$. Toto ale platí pro všechna i, a tedy $I \subset (a)$.
Na druhou stranu z Bézoutovy rovnosti v $\mathbb{Z}$ plyne existence prvků $b_i \in \mathbb{Z}$ takových, že $a = a_1b_1 + \cdots + a_mb_m \in I$, a tedy $(a) \subset I$. □

Tvrzení 4.8. *Nechť $I = (\alpha_1, \dots, \alpha_m), J = (\beta_1, \dots, \beta_l), \alpha_i, \beta_i \in \mathcal{O}_K$. Potom:*

- $I + J = (\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_l)$
- $I \cdot J = (\alpha_1\beta_1, \alpha_1\beta_2, \dots, \alpha_i\beta_j, \dots, \alpha_m\beta_l)$
- $I \subset J \Leftrightarrow$ *každé* α_i *je* $\mathcal{O}_K$*-lineární kombinace* β_j
- $I \cdot J = 0 \Leftrightarrow I = 0$ *nebo* $J = 0$

Důkaz. První 3 body jsou jasné z definic. Ten poslední také není těžký:
„$\Leftarrow$“ Jasné.
„$\Rightarrow$“ Sporem. Nechť $0 \neq \alpha \in I, 0 \neq \beta \in J$. Pak ale $\alpha \cdot \beta \in I \cdot J = 0$. To je spor s tím, že $\mathcal{O}_K$ je obor (což platí, protože jde o podmnožinu tělesa $\mathcal{O}_K \subset K$). □

Definice. Buďte I, J ideály v $\mathcal{O}_K$. Řekneme, že I *dělí* J, což značíme $I \mid J$, pokud existuje ideál H takový, že $J = I \cdot H$.

Pozorování. Pro $\alpha, \beta \in \mathcal{O}_K$ máme $\alpha \mid \beta \Leftrightarrow (\alpha) \mid (\beta)$.

Důkaz.
„$\Rightarrow$“: $\exists \gamma \in \mathcal{O}_K$ takové, že $\beta = \alpha\gamma \Rightarrow (\beta) = (\alpha\gamma) = (\alpha)(\gamma) \Rightarrow (\alpha) \mid (\gamma)$
„$\Leftarrow$“: $\beta \in (\beta) = (\alpha) \cdot H = \{\alpha i \mid i \in H\}$. Tedy $\exists i \in H : \beta = \alpha \cdot i \Rightarrow \alpha \mid \beta$. □

Tvrzení 4.9. *Buď $\alpha \in \mathcal{O}_K, I = (\beta_1, \dots, \beta_m) < \mathcal{O}_K$. Následující tvrzení jsou ekvivalentní:*
a) $(\alpha) \mid I$
b) $\alpha \mid \beta_j$ *pro všechna* j
c) $(\alpha) \supset I$

Důkaz. „$a \Rightarrow b$“ Nechť $I = (\alpha)J = \{\alpha i \mid i \in J\}$ pro nějaký ideál J. Tedy α dělí všechny prvky I, speciálně i generátory, čili $\alpha \mid \beta_j \ \forall j$.
„$b \Leftrightarrow c$“ $\alpha \mid \beta_j$ pro všechna $j \Leftrightarrow \alpha$ dělí všechny prvky $I \Leftrightarrow I \subset (\alpha)$.
„$b \Rightarrow a$“ Nechť $\beta_j = \alpha\gamma_j$ pro nějaké prvky $\gamma_j \in \mathcal{O}_K$. Potom

$$I = (\beta_1, \dots, \beta_m) = (\alpha\gamma_1, \dots, \alpha\gamma_m) = (\alpha) \cdot (\gamma_1, \dots, \gamma_m),$$

a tedy $(\alpha) \mid I$. □

Věta 4.10. *Pro nenulové ideály $I, J < \mathcal{O}_K$ máme $I \mid J \Leftrightarrow I \supset J$.*

Důkaz. Zatím jen „$\Rightarrow$“, druhou implikaci dokážeme v příští sekci.
Nechť $J = I \cdot H$. Protože $H \subset \mathcal{O}_K$, tak $J = I \cdot H \subset I \cdot \mathcal{O}_K = I$. □

4.5 Krácení ideálů

Stále buď $K = \mathbb{Q}(\sqrt{D})$ pro bezčtvercové $D \neq 0, 1$.

Definice. Buď $I < \mathcal{O}_K$ ideál. Jeho *konjugovaný ideál* je $I' = \{\alpha' \mid \alpha \in I\}$.

Pozorování. Zřejmě máme:

- $(\alpha_1, \dots, \alpha_m)' = (\alpha_1', \dots, \alpha_m')$
- $(IJ)' = I'J'$
- $I'' = I$

Tvrzení 4.11. *Nechť $I = (\alpha, \beta) < \mathcal{O}_K$. Potom $II' = (N\alpha, \mathrm{Tr}(\alpha\beta'), N\beta)$, a tedy II' je hlavní ideál.*

Důkaz. Pokud $\alpha = 0$ nebo $\beta = 0$, tak tvrzení platí.
Ať $\alpha \neq 0 \neq \beta$. Máme

$$II' = (\alpha, \beta)(\alpha', \beta') = (\alpha\alpha', \alpha\beta', \alpha'\beta, \beta\beta') = (N\alpha, \alpha\beta', \alpha'\beta, N\beta).$$

Všimněme si, že $\mathrm{Tr}(\alpha\beta') = \alpha\beta' + \alpha'\beta$, a tedy $(N\alpha, \mathrm{Tr}(\alpha\beta'), N\beta) \subset II'$.

Zbývá dokázat opačnou inkluzi, k níž potřebujeme $\alpha\beta' \in (N\alpha, \mathrm{Tr}(\alpha\beta'), N\beta)$.
Buď $g = \mathrm{NSD}_{\mathbb{Z}}(N\alpha, \mathrm{Tr}(\alpha\beta'), N\beta)$, čili $(g) = (N\alpha, \mathrm{Tr}(\alpha\beta'), N\beta)$ (viz důkaz lemmatu 4.7).
Tedy chceme dokázat, že $\alpha\beta' \in (g)$, neboli $\frac{\alpha\beta'}{g} \in \mathcal{O}_K$. K tomu stačí, že norma a stopa tohoto prvku $\in \mathbb{Z}$. Máme:
$\mathrm{Tr}(\frac{\alpha\beta'}{g}) = \frac{\alpha\beta'}{g} + \frac{\alpha'\beta}{g} = \frac{\alpha\beta' + \alpha'\beta}{g} = \frac{\mathrm{Tr}(\alpha\beta')}{g} \in \mathbb{Z}$, protože $g = \mathrm{NSD}(N(\alpha), \mathrm{Tr}(\alpha\beta'), N\beta)$.
$N\left(\frac{\alpha\beta'}{g}\right) = \frac{\alpha\beta'}{g} \cdot \frac{\alpha'\beta}{g} = \frac{\alpha\alpha'}{g} \cdot \frac{\beta\beta'}{g} = \frac{N\alpha}{g} \cdot \frac{N\beta}{g} \in \mathbb{Z}$.
Tím jsme dokázali, že $\alpha\beta' \in (g) = (N\alpha, \mathrm{Tr}(\alpha\beta'), N\beta)$.

Symetricky $\alpha'\beta \in (N\alpha, \mathrm{Tr}(\alpha\beta'), N\beta)$, a tedy $II' \subset (N\alpha, \mathrm{Tr}(\alpha\beta'), N\beta)$.

To, že II' je hlavní ideál, pak vyplývá z lemmatu 4.7. □

Důsledek 4.12. *Je-li $I = (\alpha_1, \dots, \alpha_m) < \mathcal{O}_K$, pak II' je ideál generovaný prvky $N\alpha_1, \dots, N\alpha_m$ a všemi prvky $\mathrm{Tr}(\alpha_i\alpha_j')$ pro $1 \leq i < j \leq m$.*

Důkaz. Opakovaně použijeme tvrzení 4.11. □

Nyní můžeme dokázat, že nenulovými ideály jde krátit.

Tvrzení 4.13. *Buďte $H, I, J < \mathcal{O}_K$ ideály takové, že $H \neq 0$ a $HI = HJ$. Pak $I = J$.*

Důkaz. Rozlišíme dva případy:
a) H je hlavní, čili $H = (\alpha), \alpha \neq 0$. Máme $HI = (\alpha)I = \{\alpha i \mid i \in I\}$ a také $HJ = (\alpha)J = \{\alpha j \mid j \in J\}$.
$\mathcal{O}_K$ je obor, a tedy $\alpha i = \alpha j$ implikuje $i = j$. Tedy $I = J$.

b) H je obecný ideál. Podle tvrzení 4.11 máme $HH' = (g)$ pro nějaké g. Tedy

$$HI = HJ \Rightarrow HH'I = HH'J \Rightarrow (g)I = (g)J \overset{\text{část a)}}{\Rightarrow} I = J. \quad \square$$

Teď se už můžeme vrátit k důkazu těžší implikace ve větě 4.10.

Důkaz věty 4.10. „$\Leftarrow$“: Ať $I \supset J$. Pak $II' \supset JI'$. Podle tvrzení 4.11 existuje g takové, že $II' = (g)$.
Máme tedy $(g) \supset JI'$. Podle tvrzení 4.9 pak $(g) \mid JI'$, tedy existuje ideál H takový, že $JI' = (g)H = II'H$. Podle tvrzení 4.13 můžeme zkrátit I', čímž dostaneme $J = IH$, čili $I \mid J$. □

Poznamenejme, že zatímco věta 4.10 platí obecně (a je klíčem k důkazu jednoznačné faktorizace na prvoideály ve větě 4.17), tvrzení 4.11 je specifické jen pro kvadratická tělesa. Obecně se k důkazu věty 4.10 pracuje s „lomenými ideály“ a „anihilátory“.

Důsledek 4.14. *Mějme prvoideál $P < \mathcal{O}_K$ a ideály $I, J < \mathcal{O}_K$. Pokud $P \mid IJ$, pak $P \mid I$ nebo $P \mid J$.*

Důkaz. $P \mid IJ \overset{4.10}{\Rightarrow} P \supset IJ \overset{\text{def.}}{\Rightarrow} P \supset I$ nebo $P \supset J \overset{4.10}{\Rightarrow} P \mid I$ nebo $P \mid J$. □

4.6 Norma ideálu

Stále buď $K = \mathbb{Q}(\sqrt{D})$ pro bezčtvercové $D \neq 0, 1$.

Definice. Buď I ideál v $\mathcal{O}_K$. *Norma ideálu I* je celé číslo $NI \geq 0$ takové, že $II' = (NI)$.

Toto celé číslo existuje podle tvrzení 4.11, a tedy definice dává smysl.

Pozorování.

- $N(0) = 0$
- $I = \mathcal{O}_K \Leftrightarrow NI = 1$
  Důkaz. „$\Leftarrow$“ $(1) = II' \subset I\mathcal{O}_K = I \Rightarrow I = \mathcal{O}_K$.
- $N(IJ) = NI \cdot NJ$
- $I \mid J \Rightarrow NI \mid NJ$
- Pokud $I \mid J$ a $J \neq 0, J \neq I$, pak $NI < NJ$.
- Pokud $I = (\alpha)$ je hlavní, pak $NI = |N\alpha|$.
  Důkaz. $(NI) = II' = (\alpha)(\alpha') = (\alpha\alpha') = (N\alpha)$

Příklad. Ať $K = \mathbb{Q}(\sqrt{-14})$.
Pro $I = (3, 1 + \sqrt{-14})$ máme

$$NI = \mathrm{NSD}(N3, \mathrm{Tr}(3 \cdot (1 - \sqrt{-14})), N(1 + \sqrt{-14})) = \mathrm{NSD}(9, 6, 15) = 3.$$

Pro $J = (1 + \sqrt{-14}, 1 - \sqrt{-14})$ máme

$$NJ = \mathrm{NSD}(15, \mathrm{Tr}\left((1 + \sqrt{-14})^2\right), 15) = \mathrm{NSD}(15, -26) = 1.$$

Tedy $J = \mathcal{O}_K$.

Lemma 4.15. *Je-li $I < \mathcal{O}_K$ nenulový ideál, pak faktorokruh ${}^{\mathcal{O}_K}/_{I}$ je konečný.*

Důkaz. Buď $n = NI$. Máme surjekci

$$\begin{aligned} {}^{\mathcal{O}_K}/_{(n)} = {}^{\mathcal{O}_K}/_{II'} &\twoheadrightarrow {}^{\mathcal{O}_K}/_{I} \\ \alpha + II' &\mapsto \alpha + I \end{aligned}$$

Toto zobrazení je dobře definované, protože $II' \subset I$.
Stačí tedy dokázat, že ${}^{\mathcal{O}_K}/_{(n)}$ je konečné.
Uvažujme to jako aditivní grupu. $\mathcal{O}_K(+) \simeq \mathbb{Z}^2(+)$ podle věty 4.3. Pak (n) odpovídá $(n\mathbb{Z})^2$, a tedy máme izomorfismy aditivních grup ${}^{\mathcal{O}_K}/_{(n)} \simeq {}^{\mathbb{Z}^2}/_{(n\mathbb{Z})^2} = \left({}^{\mathbb{Z}}/_{n\mathbb{Z}}\right)^2$, jež má n^2 prvků. □

4.7 Prvoideály a faktorizace

Buď $K = \mathbb{Q}(\sqrt{D}), D \neq 0, 1$ bezčtvercové.

Tvrzení 4.16. *Buď $P < \mathcal{O}_K$ ideál. Následující tvrzení jsou ekvivalentní:*
a) P je nenulový prvoideál,
b) P je maximální ideál,
c) P je vlastní ideál a platí: Pokud $P = IJ$ pro nějaké ideály $I, J < \mathcal{O}_K$, pak $I = \mathcal{O}_K$ nebo $J = \mathcal{O}_K$.

Důkaz. b) $\Rightarrow$ a) je jasné.

c) $\Rightarrow$ b): Ať $P \subset I$. K důkazu maximality chceme dokázat, že $I = P$ nebo $I = \mathcal{O}_K$.
Věta 4.10 implikuje $I \mid P$, čili $P = IJ$ pro nějaké J. Podle c) pak máme $I = \mathcal{O}_K$ nebo $J = \mathcal{O}_K$. Pokud $J = \mathcal{O}_K$, pak $P = IJ = I$.

a) $\Rightarrow$ c): Ať $P = IJ$. Pak $P \supset IJ$, a tedy $P \supset I$ nebo $P \supset J$ z definice prvoideálu, búno $P \supset I$. Podle věty 4.10 pak máme $P \mid I$.
Zároveň ale $I \mid P$, protože $P = IJ$. Dohromady tedy máme $P = I$, a tedy $P\mathcal{O}_K = P = PJ$, což podle tvrzení 4.13 implikuje $J = \mathcal{O}_K$.

Tím je tvrzení dokázané, ale pro zajímavost si ukažme ještě jednu implikaci.
a) $\Rightarrow$ b): P prvoideál implikuje, že ${}^{\mathcal{O}_K}/_P$ je obor. Chceme, že ${}^{\mathcal{O}_K}/_P$ je těleso, protože pak je P maximální ideál. Podle lemmatu 4.15 víme, že ${}^{\mathcal{O}_K}/_P$ je konečné.

Lemmátko. Každý konečný obor je těleso.
Důkaz. Buď R konečný obor a $\alpha \in R, \alpha \neq 0$.
Uvažujme hlavní ideál $(\alpha) = \{\alpha r \mid r \in R\} \subset R$.
Platí, že $\alpha r = \alpha r' \Leftrightarrow r = r'$, protože R je obor ($\alpha(r - r') = 0 \Rightarrow r - r' = 0$).
Tedy $\#(\alpha) = \#R$. Ale protože $(\alpha) \subset R$, máme $(\alpha) = R \ni 1$, a tedy $\exists \beta : \alpha\beta = 1$, čili α je invertibilní. □

Poznámka. Dokázali jsme, že $\mathcal{O}_K$ (pro $K = \mathbb{Q}(\sqrt{D})$) je *Dedekindův obor*, kde obor R je Dedekindův, pokud:

- R je noetherovský.
- R je celistvě uzavřený: Buď T podílové těleso R. R je *celistvě uzavřený*, pokud $\forall \alpha \in T$ platí: α je celistvý nad $R \Rightarrow \alpha \in R$.
- Každý nenulový prvoideál je maximální.

Poznámka. Okruh celistvých prvků $\mathcal{O}_K$ libovolného číselného tělesa K je Dedekindův.
Jednoznačná faktorizace na prvoideály platí i v obecném Dedekindově oboru.

Věta 4.17. *Buď $K = \mathbb{Q}(\sqrt{D}), D \neq 0, 1$ bezčtvercové. Každý nenulový ideál $I < \mathcal{O}_K$ jde rozložit na součin prvoideálů*

$$I = P_1^{k_1} \cdots P_r^{k_r}, r \geq 0, k_1, \ldots, k_r \in \mathbb{N},$$

kde $P_1, \ldots, P_r$ jsou po dvou různé prvoideály. Tento rozklad je jednoznačný až na pořadí.

Důkaz.
Existence. Indukcí podle $N(I)$:

- $N(I) = 1$. Pak $I = \mathcal{O}_K$ a zvolíme $r = 0$.
- $N(I) > 1$. Rozlišíme dva případy:
  - I je prvoideál. Pak máme rozklad $I = I^1$.
  - I není prvoideál, potom z tvrzení 4.16 máme, že $I = HJ$ pro nějaké ideály $H \neq \mathcal{O}_K, J \neq \mathcal{O}_K$.

    Norma je multiplikativní, takže máme $NH, NJ < NI$, a tedy H, J mají rozklad podle indukčního předpokladu.

  (Poznamenejme, že přestože jsme udělali důkaz indukcí podle normy $NI \in \mathbb{N}$, typicky neexistují ideály všech možných norem.)

Jednoznačnost. Ať $P_1^{k_1} \cdots P_r^{k_r} = Q_1^{\ell_1} \cdots Q_s^{\ell_s}$.
Pak $P_1 \mid Q_1^{\ell_1} \cdots Q_s^{\ell_s}$, a tedy podle důsledku 4.14 $P_1 \mid Q_j$ pro nějaké j. Podle věty 4.10 pak máme $P_1 \supset Q_j$. Ovšem podle tvrzení 4.16 jsou P_1, Q_j maximální, takže $P_1 = Q_j$.
Z tvrzení 4.13 pak dostaneme $P_1^{k_1-1} \cdots P_r^{k_r} = Q_1^{\ell_1} \cdots Q_j^{\ell_j-1} \cdots Q_s^{\ell_s}$ a můžeme pokračovat indukcí. □

V tvrzení 1.8 jsme dokázali, že OHI implikuje gaussovskost, pro OHI tedy máme jednoznačné rozklady na součin prvků, jež jsou silnější, než rozklady na součin prvoideálů. Obecně existují gaussovské obory, které nejsou OHI, ne však v případě $\mathcal{O}_K$:

Věta 4.18. *$\mathcal{O}_K$ je OHI, právě když je gaussovský.*

Důkaz. „$\Rightarrow$“: Tvrzení 1.8
„$\Leftarrow$“: Postupně dokážeme:

(1) Pokud je π prvočinitel v $\mathcal{O}_K$, potom je (π) prvoideál.
Podle lemmatu 1.6 stačí dokázat, že $\alpha\beta \in (\pi)$ implikuje $\alpha \in (\pi)$ nebo $\beta \in (\pi)$.
Nechť $\alpha\beta \in (\pi)$. Pak $\pi \mid \alpha\beta$, a protože je π prvočinitel, máme $\pi \mid \alpha$ nebo $\pi \mid \beta$. To ale znamená, že $\alpha \in (\pi)$ nebo $\beta \in (\pi)$.

(2) Každý prvoideál $P < \mathcal{O}_K$ je hlavní.
$P = (0)$ zřejmě je hlavní, nechť $P \neq (0)$.
Potom P dělí (n) pro nějaké $n \in \mathbb{Z}$ (například můžeme vzít $n = NP$). Uvažujme rozklad čísla n na prvočinitele v $\mathcal{O}_K$: $n = \pi_1^{k_1} \cdots \pi_r^{k_r}$.
Máme $P \mid (n) = (\pi_1)^{k_1} \cdots (\pi_r)^{k_r}$, a tedy $P \mid (\pi_j)$ pro nějaké j, protože P je prvoideál.
Podle (1) máme, že (π_j) je prvoideál, a tedy $P = (\pi_j)$ je hlavní ideál

(3) Každý ideál je hlavní.
$I \overset{4.17}{=} P_1^{k_1} \cdots P_r^{k_r} \overset{(2)}{=} (\pi_1)^{k_1} \cdots (\pi_r)^{k_r} = (\pi_1^{k_1} \cdots \pi_r^{k_r}).$ □

4.8 Popis prvoideálů

Buď $K = \mathbb{Q}(\sqrt{D}), D \neq 0, 1$ bezčtvercové. Chceme explicitně popsat, jak vypadají prvoideály v $\mathcal{O}_K$. Například víme, že:

Příklad. V $\mathbb{Z}[i]$ je každý ideál hlavní a jsou tři typy prvoideálů, které dostaneme rozkladem prvočísel $p \in \mathbb{N}$:

- $(2) = (1+i)^2$, kde $(1+i)$ je prvoideál,
- pro prvočíslo $p \equiv 3 \pmod 4$ je (p) prvoideál,
- pro prvočíslo $p \equiv 1 \pmod 4$ existuje jednoznačné vyjádření $p = a^2 + b^2$ s $a, b \in \mathbb{N}$ a odpovídající rozklad $(p) = (a+bi)(a-bi)$, kde $(a+bi), (a-bi)$ jsou různé prvoideály.

Například $(5) = (2+i)(2-i), (13) = (3+2i)(3-2i)$.

Podobné tři možnosti nastanou obecně, jak za chvíli dokážeme.

Lemma 4.19. *Buď P nenulový prvoideál v $\mathcal{O}_K$. Pak*
a) $\exists!$ prvočíslo $p \in \mathbb{N} : P \mid (p)$.
b) $N(P) = p$ nebo p^2.
c) Je-li I ideál v $\mathcal{O}_K$ takový, že $N(I) = p$ je prvočíslo, pak je I prvoideál.

Důkaz.
a) Ať $n = N(P)$ a uvažujme prvočíselný rozklad $n = p_1^{k_1} \cdots p_r^{k_r}$ v $\mathbb{Z}$.
Pak $P \mid PP' = (N(P)) = (p_1)^{k_1} \cdots (p_r)^{k_r}$, a tedy $P \mid (p_j)$ pro nějaké j. Zbývá dokázat jednoznačnost.
Ať $P \mid (p), (q)$, kde $p \neq q$ jsou prvočísla v $\mathbb{Z}$. Podle Bézoutovy rovnosti existují $a, b \in \mathbb{Z}$ taková, že $ap + bq = 1$. Pak ale $P \mid (ap + bq) = (1) = \mathcal{O}_K$, což je spor s tím, že P je prvoideál.

b) $P \mid (p) \Rightarrow N(P) \mid N((p)) = p^2$. Tedy $N(P)$ může být $1, p$ nebo p^2, ale $N(P) = 1$ nejde, protože $P \neq \mathcal{O}_K$.

c) Ať I není prvoideál, čili podle tvrzení 4.16 máme $I = AB$ pro vlastní ideály A, B. Pak ale $p = NI = NA \cdot NB$, a tedy NA nebo NB se rovná 1, což implikuje $A = \mathcal{O}_K$ nebo $B = \mathcal{O}_K$. $\square$

Věta 4.20. *Ať $\mathcal{O}_K = \mathbb{Z}[\omega]$, kde*

$$\omega = \begin{cases} \sqrt{D} \\ \frac{1+\sqrt{D}}{2} \end{cases} \quad \textit{má minimální polynom } f(x) = \begin{cases} x^2 - D & \textit{pro } D \equiv 2, 3 \pmod 4 \\ x^2 - x + \frac{1-D}{4} & \textit{pro } D \equiv 1 \pmod 4 \end{cases}$$

Pokud je $p \in \mathbb{Z}$ prvočíslo, potom rozklad (p) na prvoideály v $\mathcal{O}_K$ odpovídá rozkladu polynomu $(f(x) \mod p) \in \mathbb{F}_p[x]$ na součin ireducibilních polynomů.
Můžou nastat tři případy:

a) $f(x) \mod p$ je ireducibilní. Potom (p) je prvoideál s normou p^2.

b) $f(x) \equiv (x-c)(x-d) \mod p$ pro nějaká $c \not\equiv d \mod p$. Potom $(p) = PP'$ pro prvoideály $P \neq P', N(P) = N(P') = p$.

c) $f(x) \equiv (x-c)^2 \mod p$ pro nějaké c. Potom $(p) = P^2$ pro prvoideál P takový, že $N(P) = p$.

Důkaz. Máme

$$\begin{aligned} \mathcal{O}_K = \mathbb{Z}[\omega] &\simeq \mathbb{Z}[x]/(f(x)) \\ a + b\omega &\mapsto a + bx \end{aligned}$$

a

$$\begin{array}{ccc} \mathcal{O}_K/(p) \simeq \mathbb{Z}[x]/(p, f(x)) & \simeq & \mathbb{F}_p[x]/(f(x)) \\ (a + b\omega) \mod p & \longmapsto & (a \mod p) + (b \mod p)x \end{array}$$

Rozlišme, jak vypadá $\mathbb{F}_p[x]/(f(x))$ v našich třech případech:

a) $f(x) \mod p$ je ireducibilní. Pak $\mathbb{F}_p[x]/(f(x))$ je těleso.

b) $f(x) \equiv (x-c)(x-d) \mod p$ pro $c \not\equiv d \mod p$. Podle čínské zbytkové věty pak máme

$$\mathbb{F}_p[x]/(f(x)) \simeq \mathbb{F}_p[x]/(x-c) \times \mathbb{F}_p[x]/(x-d) \simeq \mathbb{F}_p \times \mathbb{F}_p.$$

Není to tedy těleso a neobsahuje žádný *nilpotent*, což je prvek $u \neq 0$ takový, že $u^k = 0$ pro nějaké k.

c) $f(x) \equiv (x-c)^2 \mod p$. Potom $\mathbb{F}_p[x]/(x-c)^2$ není těleso a obsahuje nilpotent $(x-c)$, protože $(x-c)^2 \equiv 0 \mod (x-c)^2$.

Podobně uvažujme, jak vypadá $\mathcal{O}_K/(p)$. Díky izomorfismu $\mathcal{O}_K/(p) \simeq \mathbb{F}_p[x]/(f(x))$ musí odpovídat případům výše:

a) $\mathcal{O}_K/(p)$ je těleso. Pak (p) je maximální ideál, a tedy podle tvrzení 4.16 je (p) prvoideál.

b,c) $\mathcal{O}_K/(p)$ není těleso, a tedy (p) není prvoideál.
Pak $(p) = PI$ pro vlastní ideály $P, I < \mathcal{O}_K$. Máme $N(p) = p^2 = N(P) \cdot N(I)$, a tedy $N(P) = N(I) = p$. Podle lemmatu 4.19c) jsou pak P, I prvoideály.
Zároveň z definice normy máme $(p) = (N(P)) = PP'$, tudíž $P' = I$ díky jednoznačné faktorizaci 4.17.

Zbývá rozlišit dva případy:
- Pokud $P = P'$, potom $\mathcal{O}_K/(p) = \mathcal{O}_K/P^2$ obsahuje nenulový nilpotent, a to obraz libovolného prvku $\alpha \in P \setminus P^2$ (máme totiž $\alpha \notin P^2$ a $\alpha^2 \in P^2$). Jedná se tedy o případ c).
- Pokud $P \neq P'$, potom $\mathcal{O}_K/(p) = \mathcal{O}_K/PP' \overset{\text{ČZV}}{\simeq} \mathcal{O}_K/P \times \mathcal{O}_K/P'$, kde $\mathcal{O}_K/P, \mathcal{O}_K/P'$ jsou tělesa, protože P, P' jsou maximální ideály. Tedy $\mathcal{O}_K/(p)$ neobsahuje nilpotenty. Jedná se tedy o případ b).

Ověření norem je triviální. $\square$

Tímto způsobem můžeme i explicitně určit, jak rozklad na prvoideály vypadá:

Důsledek 4.21. *Buď $p \in \mathbb{N}$ prvočíslo takové, že (p) není prvoideál v $\mathcal{O}_K$. Potom $f(x) \equiv (x-c)(x-d) \mod p$ (přičemž může být $c \equiv d \mod p$) a platí $(p) = (p, \omega - c)(p, \omega - d)$.*

Důkaz. Podle věty 4.20 máme $(p) = PP'$ a $f(x) \equiv (x-c)(x-d) \mod p$.
Buď $I = (p, \omega - c)$. Potom $I = (p, \omega - c) \supset (p)$, a tedy $I \mid (p) = PP'$. Platí $\omega - c \notin (p)$ (cvičení), a tedy $I \neq (p)$. Tedy $I = P$ nebo $I = P'$ nebo $I = \mathcal{O}_K$; chceme dokázat, že $I \neq \mathcal{O}_K$, čili že $N(I) \neq 1$.
Podle tvrzení 4.11 máme $N(I) = \text{NSD}(N(p), \text{Tr}(p(\omega - c)), N(\omega - c))$. Spočtěme tyto hodnoty:

- $N(p) = p^2$
- $\mathrm{Tr}(p(\omega - c)) = p\,\mathrm{Tr}(\omega - c)$
- $N(\omega - c) = (\omega - c)(\omega - c)' = (c - \omega)(c - \omega') = f(c) \equiv 0 \mod p$.

Z toho plyne, že všechna tato čísla jsou dělitelná p, a tedy $p \mid N(I) \neq 1$. Tudíž $I \neq \mathcal{O}_K$, a tedy $I = P$ nebo P' je prvoideál.

Podobně máme, že $(p, \omega - d) = P$ nebo P' je prvoideál.
Zároveň máme $P = P' \Leftrightarrow c \equiv d \mod p \Leftrightarrow (p, \omega - c) = (p, \omega - d)$. V každém případě dostaneme $(p) = PP' = (p, \omega - c)(p, \omega - d)$. □

Věty 4.20 a 4.21 nám umožňují najít rozklad libovolného ideálu I v $\mathcal{O}_K$ na prvoideály, například takto:
1. Rozlož $N(I)$ na součin prvočísel $N(I) = p_1^{k_1} \cdots p_r^{k_r}$ v $\mathbb{Z}$.
2. Každé (p_i) rozlož na součin prvoideálů v $\mathcal{O}_K$.
3. Tím dostaneme rozklad ideálu $(N(I)) = P_1^{\ell_1} \cdots P_s^{\ell_s}$ na součin prvoideálů v $\mathcal{O}_K$.
4. Zároveň máme $I \mid II' = (N(I))$, a tedy $I = P_1^{m_1} \cdots P_s^{m_s}$ pro nějaká $0 \leq m_i \leq \ell_i$.
5. Najdi správné hodnoty m_i: přinejhorším jde vyzkoušet všechny možné kombinace, ale uvažování norem ideálů hodně pomůže; v zásadě jde o to vždy správně vybrat mezi P_i a P_i'.

4.9 Příklady v $K = \mathbb{Q}(\sqrt{-14})$

V této sekci buď $K = \mathbb{Q}(\sqrt{-14})$, takže $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$.

Příklad. Jak hledat prvoideály?

- Zajímá nás $x^2 + 14 \mod p$, tedy $x^2 \equiv -14 \mod p$
- $f(x) \mod p$ reducibilní $\Leftrightarrow -14$ je kvadratický zbytek modulo p.
- $p = 2, x^2 \equiv -14 \pmod 2 \Rightarrow x \equiv 0 \pmod 2$ (0 je dvojnásobný kořen)
  $(2) = P_2^2$ pro $P_2 = (2, \sqrt{-14})$
- $p = 3, x^2 \equiv -14 \equiv 1 \pmod 3 \Rightarrow x = \pm 1$
  $(3) = P_3 \cdot P_3{}'$ pro $P_3 = (3, \sqrt{-14} + 1)$
- $p = 5, x^2 \equiv -14 \equiv 1 \pmod 5 \Rightarrow x = \pm 1$
  $(5) = P_5 \cdot P_5{}'$ pro $P_5 = (5, \sqrt{-14} + 1)$
- $p = 7, (7) = P_7^2$ pro $P_7 = (7, \sqrt{-14})$
- $p = 11, x^2 \equiv -14 \equiv 8 \pmod{11}$, 8 není kvadratický zbytek modulo 11 $\Rightarrow (11)$ je prvoideál
- $p = 13, x^2 \equiv -14 \equiv -1 \pmod{13} \Rightarrow x = \pm 5$
  $(13) = P_{13} \cdot P_{13}'$ pro $P_{13} = (13, \sqrt{-14} + 5)$

Příklad. Rozložte $(1 + \sqrt{-14})$ na součin prvoideálů
$N(1 + \sqrt{-14}) = 1 + 14 = 15 = 3 \cdot 5$
Platí: $1 + \sqrt{-14} \in P_3$? Ano
Také $1 + \sqrt{-14} \in P_5$. Tedy $(1 + \sqrt{-14}) = P_3 \cdot P_5$

Příklad. Rozložte $(2 + 3\sqrt{-14})$
$N(2 + 3\sqrt{-14}) = 4 + 9 \cdot 14 = 130 = 2 \cdot 5 \cdot 13$
$2 + \sqrt{-14} \in P_2$

$2+\sqrt{-14} \in P_5$? $2+3\sqrt{-14} - 3(\underbrace{\sqrt{-14}+1}_{\in P_5}) = -1 \notin P_5 \Rightarrow 2+3\sqrt{-14} \notin P_5$
$2+3\sqrt{-14} - 3(\sqrt{-14}+5) = -13 \in P_{13}$, tedy $2+3\sqrt{-14} \in P_{13}$
$(2+3\sqrt{-14}) = P_2 \cdot P_5{}' \cdot P_{13}$

Příklad. Rozložte $(5+2\sqrt{-14})$.
$N(5+2\sqrt{-14}) = 25 + 4 \cdot 14 = 25 + 56 = 81 = 3^4$.
Kdyby $P_3, P_3{}' \mid (5+2\sqrt{-14})$, potom by $(3) \mid (5+2\sqrt{-14})$, to by znamenalo $3 \mid 5+2\sqrt{-14}$ v $\mathcal{O}_K$, ale to není pravda.
Tedy jen jedno z P_3, P_3' dělí $(5+2\sqrt{-14})$
$5+2\sqrt{-14} - 2(\sqrt{-14}+1) = 3 \in P_3$, tedy $P_3 \mid (5+2\sqrt{-14})$ a z toho $(5+2\sqrt{-14}) = R_3^4$

Příklad. Rozložte $(1+\sqrt{-14}, 5+2\sqrt{-14})$
$(1+\sqrt{-14}) = P_3 \cdot P_5$, $(5+2\sqrt{-14}) = P_3^4$
Tedy $(1+\sqrt{-14}, 5+2\sqrt{-14}) = P_3$

5. Příklady

Skripta jsem dokončoval zároveň s přednáškou v roce 2019/2020. Uvedu zde tedy i časový průběh přednášky v tomto roce (kdy měl semestr jen 13 týdnů místo obvyklých 14) a příklady ze cvičení a domácích úkolů.
Přednášky byly nahrávané a jsou k dispozici tady:
https://is.mff.cuni.cz/prednasky/prednaska/NMAG301/

5.1 Harmonogram semestru 2019/2020

1. 10. **1. Základy.** úvod, faktorokruhy, věty o izomorfismu (do věty 1.2)
7. 10. věty o izomorfismu, prvoideály a maximální ideály, opakování gaussovských okruhů, obory hlavních ideálů (před tvrzení 1.8)
8. 10. 1. cvičení
14. 10. noetherovské okruhy a moduly, Hilbertova věta o bázi (do důsledku 1.12)
15. 10. p-valuace a p-obsah, Gaussovo lemma, ireducibilní prvky a gaussovskost $R[x]$, začátek čínské zbytkové věty (před lemma 1.18)
21. 10. čínská zbytková věta, Zornovo lemma (do konce 1. kapitoly)
22. 10. 2. cvičení
29. 10. **2. Galoisova teorie.** opakování, celistvé prvky, rozkladové nadtěleso (do tvrzení 2.3)
4. 11. kořenová a rozkladová nadtělesa, algebraický uzávěr (do konce sekce 2.5; přečtěte si i důsledek 2.10)
5. 11. 3. cvičení
11. 11. Galoisova grupa, separabilní rozšíření (do tvrzení 2.16 – přečtěte si jeho důkaz)
18. 11. dokončení separabilních rozšíření, jednoduchá rozšíření (do konce sekce 2.8)
19. 11. normální rozšíření, Galoisova korespondence (zbývá dodělat druhá půlka důkazu věty 2.27)
25. 11. dokončení Galoisovy korespondence, **3. Algebraická geometrie.** algebraické množiny a ideály (do konce sekce 3.1, zbývá dodělat důkaz tvrzení 3.4c)
26. 11. 4. cvičení
2. 12. radikály, rozšíření konečně generovaná jako okruh a jako modul (po důsledek 3.12 včetně)
3. 12. 5. cvičení
9. 12. Hilbertova věta o nulách, ireducibilní algebraické množiny (po větu 3.20 včetně)

10. 12. dokončení ireducibilních množin, **4. Algebraická teorie čísel.** řešení diofantických rovnic pomocí rozkladem: $x^2 + 5 = y^3$, motivace třídové grupy, začátek celistvých prvků (po lemma 4.1 včetně)

16. 12. celistvé prvky v číselných tělesech, norma a stopa, generátory ideálů, dělitelnost ideálů (do konce sekce 4.4)

17. 12. 6. cvičení

6. 1. norma ideálu, jednoznačný rozklad na prvoideály (po větu 4.17 včetně)

7. 1. popis prvoideálů kvadratických číselných těles (po první příklad v sekci 4.9 včetně)

5.2 Zkouška

Zkoušky v roce 2019/2020 probíhaly takto:

U zkoušky si každý vylosuje dvojici lehčí a těžší otázky (přičemž jsem se snažil o to, aby jednotlivé dvojice byly obtížností vyvážené). Ke zdárnému složení zkoušky je třeba pro každou z otázek písemně zformulovat definice a tvrzení a nastínit příslušný důkaz. Samozřejmě je vhodné si na začátku (a potom průběžně) ujasnit, co přesně chci slyšet, případně se mě průběžně ptát na hinty. Po cca 1 hodině se na sepsané podívám a případně si nechám ještě něco dovysvětlit nebo dopřipravit. Dýl než 2 hodiny bych jednoho člověka zkoušel opravdu nerad.
U všech otázek si představuju znalosti zhruba v rozsahu skript (+ schopnost dokázat lehčí tvrzení nechaná jako cvičení, včetně těch, jež byla za DÚ nebo na cvičeních).
Pokud se nebude dařit teorie, můžu to zkusit zachránit dotazem na příklady.

Hrubý nástin známkování:
1: umí všechno, případně s několika málo drobnými chybkami nebo hinty v důkaze
2: umí definice a formulace tvrzení a lehký nebo těžký důkaz, v látce se orientuje
3: umí definice a formulace tvrzení a orientuje se v nich, i když toho moc neumí dokázat
4: umí toho míň

5.2.1 Lehčí otázky

Věty o homomorfismu a izomorfismu
Charakterizace maximálních ideálů a prvoideálů
OHI a gaussovskost
Charakterizace noetherovských modulů
Obsah polynomu a Gaussovo lemma
Zornovo lemma a aplikace na existenci ideálů
Charakterizace celistvých prvků
Existence kořenového nadtělesa
Stupeň separability: multiplikativita a porovnání se stupněm rozšíření
Charakterizace separabilních rozšíření, separabilita v $V \supset U \supset T$
Normální a Galoisova rozšíření ve vztahu k rozkladovým nadtělesům
Abstraktní Galoisova korespondence
Základní vlastnosti Fix a Gal
Galoisova grupa pro $\mathbb{Q}(\sqrt{a}_1, \ldots, \sqrt{a}_n) \supset \mathbb{Q}$
Charakterizace radikálu

Základní vlastnosti $V(S), I(X)$
Algebraické množiny jako průnik nadploch
Charakterizace ireducibilních algebraických množin
Celistvé prvky v $\mathbb{Q}(\sqrt{D})$
Norma, stopa a invertibilní prvky v kvadratických tělesech
Ideály v kvadratických tělesech a dělitelnost
Norma ideálu

5.2.2 Těžší otázky

Hilbertova věta o bázi
Ireducibilní prvky v $R[x]$ a gaussovskost $R[x]$
Čínská zbytková věta
Rozšiřování homomorfismů mezi rozkladovými nadtělesy
Existence a jednoznačnost algebraického uzávěru
Separabilní konečná rozšíření jsou jednoduchá
$T = \mathrm{Fix}(U, G)$. Vlastnosti $U \supset T$
Základní věta Galoisovy teorie
Tělesa konečně generovaná jako modul a okruh
Slabá Hilbertova věta o nulách
Hilbertova věta o nulách
Rozklad algebraické množiny na ireducibilní komponenty
Krácení ideálů v kvadratických tělesech
Prvoideály a faktorizace v kvadratických tělesech
Popis prvoideálů v kvadratických tělesech

5.3 Cvičení

5.3.1 Cvičení 1

8. října 2019

1. Dokaž, že sjednocení řetězce (libovolně mnoha) ideálů $I_1 \subset I_2 \subset I_3 \subset \dots$ je ideál.
2. Pro ideály I, J definujme $I + J := \{a + b | a \in I, b \in J\}$. Dokaž, že $I + J$ je nejmenší ideál v R, který obsahuje I a J.
3. Buď R okruh a M ideál v R. Dokaž:

   a) M je maximální, právě když pro všechna $a \in R \backslash M$ platí $R = M + aR$.

   b) Pokud M je maximální a $a \in R \backslash M$, pak existují $m \in M$ a $r \in R$ taková, že $1 = m + ar$.
4. Urči $\mathbb{Q}[x]/(x + 2), \mathbb{Q}[x]/(x^2 - 2), \mathbb{Q}[x]/(x^2 - 1), \mathbb{R}[x]/(x^2 - 2), \mathbb{Z}[x]/(x^2 - 2)$.
5. Mějme ideály I, J, K okruhu R. Dokaž, že $IJ \subset I \cap J$ a $I(J + K) = IJ + IK$. Najdi příklad, kdy $IJ \neq I \cap J$.

Další příklady:

6. Dokaž, že operace na faktorokruhu jsou definované korektně a že jde o okruh (a dokaž ostatní věci z přednášky, které jsme nechali jako cvičení).

7. Dokaž 3. větu o izomorfismu (větu 1.5).
8. Pro podmnožiny A, B okruhu R definujme $A \odot B := \{ab | a \in A, b \in B\}$ (pozor, toto neodpovídá násobení ideálů). Buď I ideál v R. Dokaž, že $(a+I) \odot (b+I) \subset ab+I$. Platí opačná inkluze?
9. Uvažujme okruh $\mathbb{Z}$ a uvažujme v něm ideály $I = (168)$ a $J = (288)$.
   a) Jak vypadají všechny maximální ideály a prvoideály v $\mathbb{Z}$?
   b) Urči $I + J, IJ, I \cap J, I^2 + J$.
   c) Najdi všechny prvoideály, které obsahují ideál I, J, IJ, $I \cap J$, resp. J^2.
10. Buď R obor hlavních ideálů a $a, b \in R$.
    a) Urči $(a)(b), (a) + (b), (a) \cap (b)$.
    b) Jak vypadají všechny maximální ideály a prvoideály v R?
    c) Dokaž, že faktor R podle nenulového prvoideálu je těleso.
11. Uvažujme obor hlavních ideálů $\mathbb{Q}[x]$ a ideály $I = (x^3 + x^2 + 2x + 2)$ a $J = (x^3 - 2x^2 + 2x - 4)$.
    a) Urči $I + J, IJ, I \cap J, I^2 + J^3$.
    b) Které faktory modulo hlavní ideál z bodu a) jsou obory?
    c) Najdi všechny prvoideály, které obsahují ideál I, J, IJ, $I \cap J$, resp. J^2.

Hinty:
Obecně: když nevíš, zkus to sporem!
4. 1. věta o izomorfismu.
7. Projekce $\pi\colon R \twoheadrightarrow R/I$ a její zúžení na $\varphi\colon S \to R/I$. 1. věta o izomorfismu pro φ.
8. Neplatí. Zvol $R = \mathbb{Z}$ a prvočíslo v $ab + I$.

5.3.2 Cvičení 2

22. října 2019

1. Popiš všechny ideály v okruhu $\mathbb{Z}/(150)$ a charakterizuj, které dvojice z nich jsou komaximální.
2. Najdi příklad uspořádané množiny $\mathcal{A}$, která obsahuje nespočetný řetězec $\mathcal{B}$ (speciálně tedy takový, který nejde indexovat přirozenými čísly).
3. Použij důkaz tvrzení 1.20 (zejména krok, kdy $1 = a_1 + a_2$) ke konstrukci explicitního izomorfismu
$$\mathbb{Z}/(n) \times \mathbb{Z}/(m) \simeq \mathbb{Z}/(mn)$$
   pro $n = 16, m = 35$. Jaké známé větě krok ze závorky odpovídá?
4. Buď R okruh. Pomocí Zornova lemmatu dokaž, že každý vlastní ideál je obsažený v nějakém maximálním ideálu.
5. Ať je R okruh a $I_1, \ldots, I_n$ po dvou komaximální ideály v R. Dokaž, že pak máme izomorfismus multiplikativních grup
$$(R/(I_1 \cdots I_n))^\times \simeq (R/I_1)^\times \times \cdots \times (R/I_n)^\times .$$
6. Pomocí Zornova lemmatu dokaž, že každá lineárně nezávislá podmnožina vektorového prostoru jde rozšířit na bázi.

7. Buď $(M, \leq)$ částečně uspořádaná množina. Dokaž pomocí Zornova lemmatu, že uspořádání $\leq$ jde rozšířit na lineární uspořádání, čili že existuje uspořádání $\preceq$ na M, které je lineární a splňuje: $x \leq y \Rightarrow x \preceq y$ pro všechna $x, y \in M$.

Další příklady:

8. Buď R okruh. R je obor, právě když $R[x]$ je obor.
9. Buď K těleso. Pak $K[x, y]$ i $K[x_1, x_2, \ldots]$ (nekonečně mnoho proměnných) jsou gaussovské, ale $K[x, y]$ není obor hlavních ideálů (ale je noetherovský) a $K[x_1, x_2, \ldots]$ není noetherovský ani obor hlavních ideálů.
10. a) Buď M noetherovský modul a N jeho podmodul. Dokaž, že pak je faktormodul M/N noetherovský.

    b) * Buď M modul a N jeho podmodul. Pokud jsou N a M/N oba noetherovské, pak je noetherovský také M (použij tvrzení 1.10).
11. Buď R gaussovský obor a T jeho podílové těleso. Mějme nekonstantní primitivní polynom $f \in R[x]$. Pak f je ireducibilní v $T[x]$, právě když je ireducibilní v $R[x]$.
12. * Pomocí Zornova lemmatu dokaž, že pokud v okruhu R existuje vlastní ideál, který není konečně generovaný, pak v něm také existuje prvoideál, který není konečně generovaný.

Úlohy s * jsou trochu těžší.

5.3.3 Cvičení 3

5. listopadu 2019

1. Pro těleso T a polynom $f(x)$ urči: všechna možná kořenová nadtělesa pro f nad T, rozkladové nadtěleso pro f nad T, stupně rozšíření všech těchto těles a také jejich Galoisovy grupy nad T.

   a) $f(x) = x^2 + 3$, $T = \mathbb{R}$

   b) $f(x) = x^2 - 1$, $T = \mathbb{Q}$

   c) $f(x) = x^3 - 1$, $T = \mathbb{Q}$
2. Ať je prvek α algebraický nad tělesem T a $f \in T[x]$ je jeho minimální polynom. Pak $[T(\alpha) : T] = \deg f$.
3. Buď R gaussovský obor a T jeho podílové těleso. Je-li $u \in T$ celistvé nad R, pak $u \in R$.
4. Buďte T, U tělesa charakteristiky 0. Pak $\mathbb{Q} \subset T, U$ a každý homomorfismus $\varphi : T \to U$ je $\mathbb{Q}$-homomorfismem.
5. Mějme tělesa $T \subset U \subset V$. Je-li V algebraické nad U a U algebraické nad T, pak je také V algebraické nad T.
6. Buď $T \subset U$ algebraické rozšíření těles a $U \subset K$ (ne nutně algebraické). Pak K je algebraický uzávěr U, právě když K je algebraický uzávěr T.
7. Urči okruh celistvých prvků v tělese a) $\mathbb{Q}(i)$, b) $\mathbb{Q}(\sqrt{2})$, c) * $\mathbb{Q}(\sqrt{-3})$. (Použij cvičení 12.)

Další příklady:

8. Pro těleso T a polynom $f(x)$ urči: všechna možná kořenová nadtělesa pro f nad T, rozkladové nadtěleso pro f nad T, stupně rozšíření všech těchto těles a (případně)

také jejich Galoisovy grupy nad T.

a) $f(x) = x^2 + 1$, $T = \mathbb{Q}$

b) $f(x) = x^4 - 1$, $T = \mathbb{Q}$

c) $f(x) = x^3 - 2$, $T = \mathbb{Q}$

*d) $f(x) = x^n - 1$, $T = \mathbb{Q}$ $(n \in \mathbb{N})$

9. Prvek α je algebraický nad tělesem T, právě když $T(\alpha) = T[\alpha]$.
10. Rozšíření těles konečného stupně je nutně algebraické.
11. Mějme rozšíření těles $V \supset U \supset T$. Pak $[V : T] = [V : U] \cdot [U : T]$.
12. Je-li R gaussovský obor, $R \subset S$ a $\alpha \in S$ celistvý prvek nad R, pak minimální polynom α nad R jde zvolit jako monický.

    Pozn.: Minimálním polynomem nad oborem zde myslíme toto: Buď T podílové těleso R a $m(x)$ minimální monický polynom α nad T. Minimální polynom α nad R pak definujeme jako $n \cdot m(x)$, kde n je nejmenší společný násobek jmenovatelů všech koeficientů polynomu $m(x)$ (neboli $n \cdot m(x)$ je primitivní).
13. Žádné konečné těleso není algebraicky uzavřené.
14. * Algebraický uzávěr nekonečného tělesa T má stejnou mohutnost jako T.
15. Ať je obor S konečně generovaný okruh nad R. Pak S je konečně generovaný R-modul, právě když S je celistvý nad R (neboli každý prvek $s \in S$ je celistvý nad R).
16. Pro která $m, n \in \mathbb{Z}$ jsou tělesa $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$ $\mathbb{Q}$-izomorfní?

Úlohy s * jsou trochu těžší.

5.3.4 Cvičení 4

26. listopadu 2019

1. Buď U těleso a $G < \mathrm{Aut}(U)$ podgrupa. Pak $\mathrm{Gal}(U/\mathrm{Fix}(U, G)) \supset G$.
2. Buď $V \supset U \supset T$ rozšíření těles.

   a) Ať $V \supset T$ je normální. Pak $V \supset U$ je normální. Musí být $U \supset T$ normální?

   b) Ať $V \supset T$ je Galoisovo. Pak $V \supset U$ je Galoisovo. (Může se hodit použít cvičení 6.)
3. Pro rozšíření těles $U \supset T$ urči $[U : T], [U : T]_s, \mathrm{Gal}(U/T)$, pokud $T = \mathbb{R}, U = \mathbb{C}$.
4. Buď $V \supset T$ Galoisovo rozšíření a $V \supset U \supset T$. Dokaž, že
   $$[U : T] = \frac{\#\mathrm{Gal}(V/T)}{\#\mathrm{Gal}(V/U)}.$$
5. Buď $U \supset T$ konečné rozšíření. Toto rozšíření je Galoisovo, právě když $[U : T] = \#\mathrm{Gal}(U/T)$.
6. Prvek $\alpha \in U$ je separabilní nad tělesem T, pokud je kořenem nějakého separabilního polynomu v $T[x]$.

Další příklady:

7. Buď $f(x) \in T[x]$ polynom, jehož ireducibilní rozklad nad T je $f(x) = f_1(x) \cdots f_k(x)$. Uvažujme Galoisovu grupu rozkladového nadtělesa polynomu f jako grupu permu-

tací na množině jeho kořenů. Dokaž, že každá z těchto permutací obsahuje aspoň k cyklů (pevný bod zde považujeme za cyklus délky 1).

8. Pro rozšíření těles $U \supset T$ urči $[U : T], [U : T]_s, \mathrm{Gal}(U/T)$, pokud $T = \mathbb{F}_p(y), U = T(\sqrt[p]{y})$ (k ověření ireducibility použij Eisensteinovo kritérium).
9. Buď $U \supset T$ rozšíření těles. Všechny prvky $\alpha \in U$, jež jsou separabilní nad T, tvoří podtěleso U (tzv. separabilní uzávěr T v U).
10. Rozšíření $U \supset T$ je normální, právě když existuje množina $\mathcal{M} \subset T[x]$ taková, že U je rozkladové nadtěleso množiny $\mathcal{M}$ nad T.
11. Dokaž tvrzení 2.24 ze skript (o existenci normálního uzávěru).
12. Buď U těleso charakteristiky různé od 2 a $a, b \in U$ prvky takové, že $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin U$. Pak $[U(\sqrt{a}, \sqrt{b}) : U] = 4$.

5.3.5 Cvičení 5

3. prosince 2019

1. Buď U rozkladové, resp. kořenové nadtěleso polynomu $f(x)$ nad tělesem T. Urči $U, [U : T], \mathrm{Gal}(U/T)$, bázi U jako vektorového prostoru nad tělesem T.

   Rozhodni, zda jde o Galoisovo rozšíření, a pokud ano, tak popiš všechna tělesa $U \supset V \supset T$, jestliže

   a) $f(x) = x^2 - 5, T = \mathbb{Q}$
   b) $f(x) = x^3 - 2, T = \mathbb{Q}$
   c) $f(x) = x^3 - 2, T = \mathbb{Q}(e^{2\pi i/3})$
   d) $f(x) = (x^2 - 3)(x^2 - 5), T = \mathbb{Q}$
   e) $f(x) = x^{12} - 1, T = \mathbb{Q}$
   f) $f(x) = x^{20} - 1, T = \mathbb{Q}(i)$
   h) $f(x) = x^n - 1,\ T = \mathbb{Q}\ (n \in \mathbb{N})$
2. Pro rozšíření těles $U \supset T$ urči $[U : T], \mathrm{Gal}(U/T)$, bázi U jako vektorového prostoru nad tělesem T.

   Rozhodni, zda jde o Galoisovo rozšíření, a pokud ano, tak popiš všechna tělesa $U \supset V \supset T$, jestliže

   a) $U = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}), T = \mathbb{Q}$
   b) $U = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i), T = \mathbb{Q}$
   c) atd. :)

Další příklady:

3. Mějme tělesa $V \supset U \supset T$ taková, že $V \supset T$ a $U \supset T$ jsou normální rozšíření. Pak $\mathrm{Gal}(V/U) \triangleleft \mathrm{Gal}(V/T)$ a $\mathrm{Gal}(V/T)/\mathrm{Gal}(V/U) \simeq \mathrm{Gal}(U/T)$.
4. Dokaž větu 2.28 (o rozšíření $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n}) \supset \mathbb{Q}$).

Příklady 1b) a 2b) jsem na začátku cvičení vyřešil na tabuli.

5.3.6 Cvičení 6

17. prosince 2019

1. Urči v oboru celých čísel $\mathbb{Z}(+,-,0,\cdot,1)$
   a) $\sqrt{(0)}$, $J(\mathbb{Z})$,
   b) $\sqrt{(25)}$, $\sqrt{(125)}$, $\sqrt{(50)}$, $\sqrt{(100)}$, $\sqrt{(\prod_i p_i^{r_i})}$ pro po dvou různá prvočísla p_i.
   Dále urči
   c) $J(\mathbb{Z}/(100))$,
   d) * kdy je $(\mathbb{Z}/(n))/J(\mathbb{Z}/(n))$ těleso.
2. Rozhodni, které z následujících množin jsou algebraické:
   a) $\{(t,t^2,t^3) \in K^3 | t \in K\}$,
   b) $\{(\cos t, \sin t) \in \mathbb{R}^2 | t \in \mathbb{R}\}$,
   c) * $\{(t, \sin t) \in \mathbb{R}^2 | t \in \mathbb{R}\}$.
3. Buď K těleso.
   a) Pro $S \subset K[x_1,\dots,x_n]$ dokaž $V(I(V(S))) = V(S)$.
   b) Pro $X \subset K^n$ dokaž $I(V(I(X))) = I(X)$.
   c) Pro ideál $I < K[x_1,\dots,x_n]$ dokaž $I(V(I)) \supset \sqrt{I}$.
4. Buď R gaussovský obor a T jeho podílové těleso. Je-li $u \in T$ celistvé nad R, pak $u \in R$.

Další příklady:

5. V oboru polynomů nad komplexními čísly $\mathbb{C}[x](+,-,\cdot,0,1)$
   a) spočítej $\sqrt{(0)}$, $J(\mathbb{C}[x])$, $\sqrt{(x-3)^5(x-1)^4(x^3+2)}$, $\sqrt{(x^6-x^4-x^2+1)}$,
   b) dokaž, že $\sqrt{(p)} = (\frac{p}{NSD(p,p')})$, kde $p \in \mathbb{C}[x]$.
6. Je-li K konečné těleso, pak je každá podmnožina v K^n algebraická.
7. Buď K nekonečné těleso a $V = \{(t,t^2,t^3,\dots,t^n) | t \in K\} \subset K^n$.
   a) Najdi $I(V)$ (a dokaž svou odpověď).
   b) Dokaž, že V je ireducibilní.
8. Pracujme nad $K = \mathbb{C}$.
   a) Dokaž, že $I(V(x^2-y)) = (x^2-y)$ a že algebraická množina $V(x^2-y) \subset \mathbb{C}^2$ je ireducibilní.
   b) Urči množinu $V(y^4-x^2, y^4-x^2y^2+xy^2-x^3) \subset \mathbb{C}^2$ a rozlož ji na ireducibilní komponenty.
   c) * Rozlož $V(x^2+y^2-1, x^2-z^2-1) \subset \mathbb{C}^3$ na ireducibilní komponenty.
9. Dokaž, že $f(x,y) = y^2 + x^2(x-1)^2 \in \mathbb{R}[x,y]$ je ireducibilní polynom, ale množina $V(f) \subset \mathbb{R}^2$ je reducibilní.
10. Pokud K není algebraicky uzavřené, pak Hilbertova věta o nulách neplatí (tedy věty 3.15b), 3.16).

Úlohy s * jsou trochu těžší.

5.3.7 Cvičení 7

Kvůli kratšímu semestru na toto cvičení v roce 2019/2020 nedošlo.

1. Najdi všechny jednotky v $\mathbb{Q}(\sqrt{D})$ pro $D = -2, -3, -7$, *2, *5.
2. Buď $K = \mathbb{Q}(\sqrt{D})$ a $\omega = \sqrt{D}$, resp. $\frac{1+\sqrt{D}}{2}$ pro $D \equiv 2, 3$, resp. $1 \pmod 4$. Pro $m \in \mathbb{Z}$ a $\alpha = a + b\omega \in \mathcal{O}_K$ dokaž, že $m|\alpha$ v $\mathcal{O}_K$, právě když $m|a, b$ v $\mathbb{Z}$. Dokaž, že to nemusí platit pro $m|a + b\sqrt{D}, a, b \in \mathbb{Z}$.
3. Ireducibilní prvky:

   a) Pokud má prvek $\alpha \in \mathcal{O}_K$ normu p, což je prvočíslo v $\mathbb{Z}$, pak je α ireducibilní v $\mathcal{O}_K$.

   b) Najdi nějaký ireducibilní prvek v $\mathbb{Z}[\sqrt{-14}]$ s prvočíselnou normou.

   c) Dokaž, že 3 a $1 + \sqrt{-14}$ jsou ireducibilní.

   d) Dokaž, že $3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14})(5 - 2\sqrt{-14})$ jsou dva různé ireducibilní rozklady.
4. Hlavní ideály:

   a) Dokaž, že $(17 + 2\sqrt{-14}, 20 + \sqrt{-14}) = (3 - \sqrt{-14})$ je hlavní ideál v $\mathbb{Z}[\sqrt{-14}]$.

   b) $(2, \sqrt{-14})$ není hlavní ideál v $\mathbb{Z}[\sqrt{-14}]$.

   c) Pomocí faktorokruhů modulo daný ideál dokaž, že $(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) = (3, 1 - \sqrt{-14})$ a že jde o vlastní ideál (protože norma všech prvků je dělitelná 3).
5. Násobení ideálů:

   a) $(5 + \sqrt{-14}, 2 + \sqrt{-14})(4 + \sqrt{-14}, 2 - \sqrt{-14}) = (6, 3\sqrt{-14})$.

   b) Buď $I = (3, 1 + \sqrt{-14})$. Pak $II' = (3)$, I není hlavní a $I \neq I'$.

   c) Buď $J = (5, 1+\sqrt{-14})$. Pak $(15) = IJI'J'$. Využij toho k nalezení dvou různých ireducibilních rozkladů 15.

   *d) I, J jsou prvoideály.

Další příklady:

6. Dokaž, že $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} \supset \mathbb{Z}[\sqrt{D}]$, resp. $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ pro $D \equiv 2, 3$, resp. $1 \pmod 4$.
7. Dokonči důkaz důsledku 4.2 z přednášky, že každý prvek K jde vyjádřit jako α/n pro $\alpha \in \mathcal{O}_K$ a $n \in \mathbb{N}$.
8. Buď G podgrupa aditivní grupy $\mathbb{Z}^n$, kde $n \in \mathbb{N}$. Dokaž, že $G \simeq \mathbb{Z}^m$ pro nějaké m, $0 \leq m \leq n$.
9. Vyřeš diofantické rovnice $x^2 + 1 = y^5$, $x^2 + 3 = y^3$ a $x^2 + 4 = y^3$.

Úlohy s * jsou trochu těžší.

5.4 Domácí úkoly

K získání zápočtu bylo potřeba získat 60 bodů ze 75 možných.

5.4.1 Domácí úkol 1

Termín odevzdání: 4. listopadu 2019 do 12:20

1. a) Dokaž lemma 1.6: Vlastní ideál I v okruhu R je prvoideál, právě když pro všechna $a, b \in R$ platí: $ab \in I \Rightarrow a \in I$ nebo $b \in I$.

   b) Použij lemma 1.6 k přímému důkazu, že pokud je ideál M maximální, pak je M prvoideál.
2. Buď R okruh. Dokaž, že je-li $R[x]$ noetherovský okruh, pak je také R noetherovský okruh. Hint: Je-li I ideál v R, uvažuj $I[x] \subset R[x]$.
3. Buď R gaussovský obor. Dokaž, že je-li $f \in R[x]$ ireducibilní, pak je to prvočinitel v $R[x]$ (bez použití věty 1.17 z přednášky, jde totiž o část jejího důkazu).
4. Buď R okruh a I, J komaximální ideály v R. Dokaž, že pro libovolná přirozená čísla m, n jsou také ideály I^m, J^n komaximální.
5. Buď R okruh. Multiplikativní množina S v R je neprázdná podmnožina $S \subset R$, která je uzavřená na násobení a neobsahuje 0. Pomocí Zornova lemmatu 1.22 (tedy bez použití lemmatu 1.23) dokaž:

   Buď S multiplikativní množina v okruhu R a I ideál v R takový, že $I \cap S = \emptyset$. Pak existuje prvoideál $P < R$ takový, že $P \supset I$ a $P \cap S = \emptyset$.

Každá úloha je za 5 bodů.

5.4.2 Domácí úkol 2

Termín odevzdání: 2. prosince 2019 do 12:20

1. (7 bodů) Mějme obory $R \subset S \subset T$. Dokaž:

   a) Je-li T konečně generovaný S-modul a S konečně generovaný R-modul, pak je také T konečně generovaný R-modul.

   b) Ať $\alpha, \beta \in S$. Je-li α celistvý prvek nad R a β celistvý prvek nad $R[\alpha]$, pak je β celistvý prvek nad R.

   c) $\sqrt[3]{\sqrt{3} + \sqrt[5]{5}}$ je celistvý prvek nad $\mathbb{Z}$.
2. (6 bodů) Mějme algebraické rozšíření těles $U \supset T$ a T-homomorfismus $\varphi : U \to U$. Dokaž, že pak je φ dokonce T-automorfismus.
3. (6 bodů) Najdi prvek $\alpha \in \mathbb{C}$ takový, že $\mathbb{Q}(\sqrt{2}, \sqrt{7}) = \mathbb{Q}(\alpha)$.
4. (6 bodů) Buď U těleso a $G < \mathrm{Aut}(U)$ podgrupa. Dokaž, že pak pro všechna $\varphi \in \mathrm{Aut}(U)$ platí $\mathrm{Fix}(U, \varphi G \varphi^{-1}) = \varphi(\mathrm{Fix}(U, G))$.

5.4.3 Domácí úkol 3

Termín odevzdání: 16. prosince 2019 do 12:20

1. (8 bodů) Buď U rozkladové nadtěleso polynomu $f(x) = x^4 - 2$ nad tělesem $\mathbb{Q}$. Rozhodni, zda jde o Galoisovo rozšíření a urči $U, [U : \mathbb{Q}]$, bázi U jako vektorového prostoru nad tělesem $\mathbb{Q}$ a $\mathrm{Gal}(U/\mathbb{Q})$.
2. (7 bodů) Buď V rozkladové nadtěleso polynomu $(x^2 + 3)(x^2 - 2)$ nad tělesem $\mathbb{Q}$. Popiš $\mathrm{Gal}(V/\mathbb{Q})$ a všechna tělesa $V \supset U \supset \mathbb{Q}$. (Bez použití věty 2.28, kterou jsme úplně nedokázali.)
3. (5 bodů) Buď P prvoideál v okruhu R a I, J vlastní ideály v R. Dokaž:

   a) $\sqrt{I} \subset P$, právě když $I \subset P$.

b) $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

4. (5 bodů) Buď K těleso a $V \subset K^n$ neprázdná algebraická množina. Dokaž, že V je ireducibilní, právě když je $I(V)$ prvoideál.