Úvod do komutativní algebry

Vítězslav Kala

2. prosince 2024

Obsah

Úvod

Toto je pracovní verze skript k přednášce Úvod do komutativní algebry, snad už neobsahuje přespříliš překlepů a nedokonalostí – ale budu rád za jakékoli připomínky a komentáře.

Jejich cílem je být poměrně minimalistickým shrnutím probrané látky (v rozsahu výuky od roku 2017 dál), 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].
Kapitoly 5, 6 a 7 shrnují cvičení a domácí úkoly, částečně podle výuky z roku 2019/2020, později sepsané a zkompletované Matějem Doležálkem.
Přednášky v roce 2019/2020 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 potom v dalších letech). Za další opravy děkuju Davidovi Stanovskému. Cvičení a zejména jejich řešení v 6. kapitole sepsal Matěj Doležálek. 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 možná 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 homomorfismus)
- $A \hookrightarrow B$ značí vnoření (a často injektivní homomorfismus)

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. $R = \mathbb{Z}, I = 6\mathbb{Z} = \{\ldots, -6, 0, 6, 12, \ldots\}$
$a \sim b \Leftrightarrow a - b \in 6\mathbb{Z} \Leftrightarrow a \equiv b \pmod 6$

Třídy:
$0+6\mathbb{Z}, 1+6\mathbb{Z}, \ldots, 5+6\mathbb{Z}$
$R/I = \mathbb{Z}/6\mathbb{Z}$ 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*

$$\begin{aligned} \psi\colon R/I &\to S \\ a+I &\mapsto \varphi(a) \end{aligned}$$

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*

$$R/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi, \quad a + \operatorname{Ker}\varphi \mapsto \varphi(a).$$

Důkaz. Zvolme $I = \operatorname{Ker}\varphi$ ve větě o homomorfismu 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 homomorfismu 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) ${}^{I}/_{J} = I_0$:
Rozepsáním pomocí definice I máme

$${}^{I}/_{J} = \{i + J \mid i \in I\} = \{a + J \mid a \in R, a + J \in I_0\} = I_0. \quad \square$$

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

Připomeňme, že odteď až do konce skript všechny okruhy mají 1 (a jsou komutativní).

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 $\exists a \in R$ takové, že $I = (a) = aR$.

Příklad. $R = \mathbb{Z}$. Všechny ideály v $\mathbb{Z}$ jsou tvaru $I = (n) = n\mathbb{Z} = \{\ldots, -n, 0, n, 2n, \ldots\}$, kde $n = 0, 1, 2, \ldots$

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

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 $J = R$ a $J = I$. Ale tomu odpovídají nevlastní ideál ${}^{R}/_{I} < {}^{R}/_{I}$ a ${}^{I}/_{I} = (0_{R/I}) < {}^{R}/_{I}$.
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 gaussovský, 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 $p_i \nmid p_j$.

Poznámka (Věta z Algebry). Buď R obor. Pak R gaussovský 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 $a_{i+1} \nmid a_i$.

Příklad. $\mathbb{Z}, \mathbb{Q}[x], \mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$ jsou gaussovské, protože jsou euklidovské.
$\mathbb{Z}[x]$ je gaussovský, ale neeuklidovský.
$\mathbb{Z}[\sqrt{D}]$ 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
$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \ldots$.

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

Tvrzení 1.9. *Obory hlavních ideálů jsou noetherovské.*

Důkaz. Buď R OHI. Ať není noetherovský. Tedy existuje $I_1 \subsetneq I_2 \subsetneq \ldots$. 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. □

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

$\mathbb{Z}[\sqrt{-2019}]$ noetherovský, ale není gaussovský.
$R = K[X, Y]$ gaussovský, noetherovský, ne OHI.
$R = K[X_1, X_2, X_3, \ldots]$ 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.
  $im = m + m + \cdots + m, i \in \mathbb{N}, m \in G$
  $(-i) \cdot m = -(im)$
- R je R-modul
- $I < R \Rightarrow I$ je R-modul

Definice. R-modul M je noetherovský, pokud neexistuje nekonečná posloupnost $M_1 \subsetneq M_2 \subsetneq \ldots$ 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 $r_1, \ldots, r_k$ v okruhu R. Ideál jimi generovaný značíme $(r_1, \ldots, r_k) = r_1R + \cdots + r_kR$ (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 $M_1 \subsetneq M_2 \subsetneq \ldots$
Pak $N = \bigcup_{i=1}^{\infty} M_i$ je R-modul $\Rightarrow$ N je konečně generovaný nějakými prvky $n_1, n_2, \ldots, n_k$. $N = \bigcup M_i \Rightarrow$
$\exists j$ takové, že $n_1, \ldots, n_k \in M_j$
$\Rightarrow$ R-modul generovaný $n_1, \ldots, n_k$ 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. □

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 $I \setminus (f_0, f_1, \ldots, f_i)$. Zřejmě $\deg f_0 \leq \deg f_1 \leq \ldots$.

Buď a_i vedoucí koeficient polynomu f_i a $J_i =$ ideál v R generovaný prvky $a_0, \ldots, a_i$. $J_0 \subset J_1 \subset J_2 \ldots$ je řetězec v noetherovském okruhu $R \Rightarrow \exists k$: $J_k = J_{k+1} = J_{k+2} = \ldots$
Speciálně $\exists r_0, \ldots, r_k \in R : a_{k+1} = r_0 a_0 + \cdots + r_k a_k$.

Buď $d = \deg f_{k+1}$, polynomy $f_0, f_1, \ldots f_k$ můžeme vynásobit vhodnými $x^{\text{něco}}$, aby vznikly polynomy $\tilde{f}_0, \ldots \tilde{f}_k$, všechny stupně d. Uvažme $g := f_{k+1} - r_0\tilde{f}_0 - \ldots - r_k\tilde{f}_k$. Pak máme $\deg g \leq d$, ale koeficient u x^d je $a_{k+1} - r_0 a_0 - \cdots - r_k a_k = 0 \Rightarrow \deg g < d = \deg f_{k+1}$.
Ale $g \in I \setminus (f_0, \ldots, f_k)$, což je spor s volbou f_{k+1} nejmenšího stupně. □

Důsledek 1.12. *Je-li R noetherovský, pak je také $R[x_1, \ldots, x_k]$ 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 libovolného 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 dvou neasociované prvočinitele p, a $f_1 := uf, g_1 := vg$.
Pro každé p 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

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

Tvrzení 1.16. *Buď R gaussovský obor a T jeho podílové těleso.*
Ať $f, g \in R[x], \deg f \geq 1$ a f primitivní.
a) $f \mid g$ v $T[x] \Rightarrow f \mid g$ v $R[x]$.
b) f ireducibilní v $R[x] \Leftrightarrow f$ ireducibilní v $T[x]$.

Důkaz. a) Ať $g = qf, q \in T[x]$. 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 $R[x]$.
b)
„⇐“ Lehké cvičení
„⇒“ 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 $R[x]$. □

Tvrzení 1.17. *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) $f \in R[x]$, $\deg f \geq 1$.
Podle tvrzení 1.16b) 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. Tedy tvrzení 1.16b) $\Rightarrow f$ 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 $T[x]$. Tvrzení 1.16b) $\Rightarrow vg$ je ireducibilní v $R[x]$. □

Věta 1.18. *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 $\ldots f_i \mid f_{i-1} \mid \cdots \mid f_2 \mid f_1, f_i \in R[x]$. Pak $\deg f_1 \geq \deg f_2 \geq \cdots \geq 0$, a tedy $\exists k : \deg f_k = \deg f_{k+1} = \ldots.$
Buď a_i vedoucí koeficient $f_i \Rightarrow \cdots \mid a_i \mid a_{i-1} \cdots \mid a_2 \mid a_1$. Toto je posloupnost dělitelů v gaussovském $R \Rightarrow \exists l : a_l \parallel a_{l+1} \parallel \ldots$
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 1.17, 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 $T[x]$. Tvrzení 1.16a) pak implikuje $f \mid g$ v $R[x]$. □

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

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

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

Tvrzení 1.20. *Ať $I_1, \ldots, I_n$ jsou po dvou komaximální ideály v okruhu R a $n \geq 2$. Pak $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ a dvojice $I_1 \cap \cdots \cap I_{n-1}, I_n$ 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 $I_1 \cdots I_{n-1} + I_n = R$.

$I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ dokážeme indukcí. Pro $n = 2$ jde o lemma 1.19.
Ať $n > 2$. Indukční předpoklad: $I_1 \cap \cdots \cap I_{n-1} = I_1 \cdots I_{n-1}$.
Z 1. části důkazu: $I_1 \cdots I_{n-1}, I_n$ jsou komaximální. Pak

$$(I_1 \cdots I_{n-1}) \cdot I_n \overset{1.19}{=} (I_1 \cdots I_{n-1}) \cap I_n \overset{\text{indukční předpoklad}}{=} (I_1 \cap \cdots \cap I_{n-1}) \cap I_n. \quad \square$$

Tvrzení 1.21. *Ať $I_1, \dots, I_n$ jsou ideály v okruhu R. Uvažujme homomorfismus*

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

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

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

$$\begin{aligned}R \overset{\varphi}{\twoheadrightarrow} {}^{R}\!/_{I_1} \times \cdots \times {}^{R}\!/_{I_n} \twoheadrightarrow {}^{R}\!/_{I_i} \times {}^{R}\!/_{I_j} &\twoheadrightarrow \left({}^{R}\!/_{I_i}\right)\Big/\left({}^{I_i + I_j}\!/_{I_i}\right) \times \left({}^{R}\!/_{I_j}\right)\Big/\left({}^{I_i + I_j}\!/_{I_j}\right)\\ &\overset{1.3}{\simeq} {}^{R}\!/_{I_i + I_j} \times {}^{R}\!/_{I_i + I_j}.\end{aligned}$$

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.

„$\Leftarrow$“ Předpokládejme, že $I_1, \dots, I_n$ 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 $r := r_1 a_2 + r_2 a_1$. Pak $r - r_1 = (r_1 a_2 + r_2 a_1) - r_1(a_1 + a_2) = a_1(r_2 - r_1) \in I_1$. Stejně dostaneme $r - r_2 \in I_2$.

Ať $n \geq 3$. Uvažujme $I := I_1 \cdots I_{n-1} \overset{1.20}{=} I_1 \cap \cdots \cap I_{n-1}$. Z tvrzení 1.20 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

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

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

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

Konečně složením máme

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

□

Důsledek 1.22 (Čínská zbytková věta)**.** *Ať $I_1, \dots, I_n$ jsou po dvou komaximální ideály v R takové že $I_1 \cap \cdots \cap I_n = \{0\}$. Pak $\forall r_1, \dots, r_n \in R\ \exists! r \in R$ takové, že $r \equiv r_i \pmod{I_i}$ pro všechna i.*

Poznámka. Mějme $n_1, \dots, n_k \in \mathbb{Z}$ 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 1.23 (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.
$\mathcal{A} := \{\text{lineárně nezávislé podmnožiny ve } V\}, \leq$ 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 1.24. *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 1.23 množina $\mathcal{A}$ má maximální prvek J. O tom snadno ověříme, že má všechny požadované vlastnosti. □

Důsledek 1.25. *Buď $I < R$* vlastní ideál*. Pak existuje maximální ideál M v R, který obsahuje I.*

Důkaz. V lemmatu 1.24 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 1.24, 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 1.26. *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 1.24 zvolme $A = S$. Je pak potřeba ověřit, že ideál J, který existuje podle tohoto lemmatu, je prvoideál: cvičení. □

Důsledek 1.27. *Pro každou multiplikativní množinu S existuje prvoideál P takový, že $P \cap S = \emptyset$.*

Důkaz. Zvolme $I = \{0\}$ v tvrzení 1.26. □

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 $\alpha_1, \alpha_2, \ldots, \alpha_d \in U$, 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 podokruh U, který obsahuje T a α, a $T(\alpha)$ jako nejmenší podtěleso U, 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 $1, \alpha, \ldots, \alpha^{d-1}$.

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 $t \in T$.

Pozorování. Ať $U \supset T, V \supset T$ jsou tělesa. Každý T-homomorfismus $\varphi\colon U \to V$ je prostý.

Důkaz. Uvažujme jádro $\operatorname{Ker}\varphi$. To je ideál v U, ovšem těleso obsahuje jen ideály $\{0\}$ a U.
Buď $0 \neq t \in T$ nějaký prvek tělesa T (tady využíváme toho, že jednoprvkovou množinu nepovažujeme za těleso). Pak $\varphi(t) = t$, neboť jde o T-homomorfismus, a tedy $t \notin \operatorname{Ker}\varphi$, čili $\operatorname{Ker}\varphi \neq U$.
Pak $\operatorname{Ker}\varphi = \{0\}$ a φ je prostý, jak jsme chtěli. □

$\operatorname{Gal}\left(U/T\right) = \{\varphi\colon U \to U \mid \varphi \text{ je } T\text{-automorfismus}\}$ je Galoisova grupa rozšíření $U \supset T$.
Jde o grupu, protože automorfismy můžeme skládat a invertovat; identita id je 1 v grupě.
Například $\operatorname{Gal}\left(\mathbb{Q}(i)/\mathbb{Q}\right) = \{\mathrm{id}, \varphi\}$, 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?
$v^n = \underset{\in R \cdot v^{n-1}}{-a_{n-1}v^{n-1}} - \cdots - \underset{\in R \cdot 1}{a_0} \in \heartsuit$.

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

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

3) $\Rightarrow$ 1) Ať $R' = \sum_{j=1}^{n} Rw_j$. 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 $1 \cdot v^n$ – přesněji, determinant se rovná hodnotě $f(v)$ pro nějaký monický polynom $f \in R[x]$. Toto f je 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. □

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 $\mathbb{Q} \not\cong \mathbb{Q}(i)$.

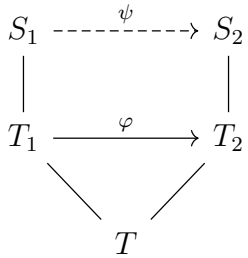
Důkaz. Ať $S_1 = T(\alpha), S_2 = T(\beta)$.
Víme, že $T(\alpha) = T[\alpha] = \{g(\alpha) \mid g \in T[x]\}$ a podobně pro $T(\beta)$.
Uvažujme

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

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. □

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 $\psi \restriction T_1 = \varphi$.



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

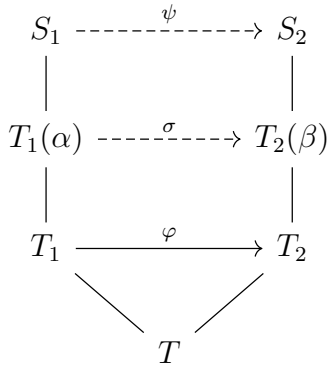
Věta 2.6. *Buď T těleso a $f \in T[x]$ nekonstantní polynom. Rozkladové nadtěleso f nad T je jednoznačně určené až na T-izomorfismus.*

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 $T_1[x]$ 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 $\psi \restriction T_1 = \sigma \restriction T_1 = \varphi$.



□

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).

Následující tvrzení v dalším textu nepotřebujeme, ale umožní nám například popsat, jak vypadá $\overline{\mathbb{Q}}$. Z Algebry totiž víme, že $\mathbb{C}$ je algebraicky uzavřené, a tedy tvrzení implikuje, že $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ je algebraické nad } \mathbb{Q}\}$.

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 $f \in T(\alpha_0, \ldots, \alpha_n)[x]$, takže β je algebraické nad $T(\alpha_0, \ldots, \alpha_n)$, čili $[T(\alpha_0, \ldots, \alpha_n, \beta) : T(\alpha_0, \ldots, \alpha_n)] < \infty$.
Každé α_i je algebraické nad $T \Rightarrow [T(\alpha_0, \ldots, \alpha_n) : T] < \infty$. Tedy $[T(\alpha_0, \ldots, \alpha_n, \beta) : T] < \infty \Rightarrow \beta$ 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 $X = \{x_f \mid f \in T[x] \text{ nekonstantní ireducibilní}\}$. 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 $I = (f(x_f) \mid f \in T[x] \text{ nekonstantní ireducibilní}) < T[X]$ 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 $H :=$ součin všech polynomů h takových, že proměnná x_h se v rovnosti vyskytuje, a buď U rozkladové nadtěleso polynomu H.
V tělese U má tedy každý takovýto polynom h 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 1.25). Pak je faktorokruh $S := {}^{T[X]}/_{M}$ těleso a máme $T \hookrightarrow S$ (jako v lemmatu 2.3). Každý nekonstantní ireducibilní polynom $f \in T[x]$ má v S kořen, a to $x_f + M$. Tedy mají kořeny i reducibilní polynomy. 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 1.23:
$\mathcal{M} \neq \emptyset$, 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 $\varphi\colon U_1 \to U_2$ 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 $\psi\colon V_1 \to V_2$ takový, že $\psi \restriction U_1 = \varphi$, což je ale spor s maximalitou φ, a tedy $U_1 = S_1$.
$\varphi\colon U_1 \to U_2$ 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 $\varphi\colon U \to V$ 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 $\varphi\colon U \to K$ existuje T-homomorfismus $\sigma\colon W \to K$ 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 T-izomorfismus φ, neboť

Cvičení. Buď $\varphi\colon U \to V$ 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 $\mathrm{Gal}\left(U/T\right) = \{T\text{-automorfismy } \varphi : U \to U\}$.

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 $\varphi : U \to U$ 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 $\varphi \restriction M \colon M \to M$.
Díky pozorování v sekci 2.2 je 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 $M = \{\alpha_1, \ldots, \alpha_k\}$ 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 $i = k+1, \ldots, n$. 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 $U = T(\alpha_1, \ldots, \alpha_k)$, a tedy je φ jednoznačně určené svými hodnotami $\varphi(\alpha_1), \ldots, \varphi(\alpha_k)$, 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 $\varphi \colon \mathbb{Q}(\alpha) \to \overline{\mathbb{Q}}$ (viz tvrzení 2.7 pro popis $\overline{\mathbb{Q}}$).
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 $\deg f$ (protože ireducibilní polynom nemá násobné kořeny v $\mathbb{C} \supset \overline{\mathbb{Q}}$ – viz například tvrzení 2.17 níže).

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 $U = T(\beta_1, \ldots, \beta_l)$ 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 α algebraický nad T a jeho minimální polynom je 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. *$U = T(\alpha_1, \ldots, \alpha_k)$ 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 $U = T(\alpha_1, \ldots, \alpha_k)$ 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 $k < n$. □

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 splněna 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 2.26, 2.27).

Věta 2.20 (klíčová věta pro důkaz Galoisovy korespondence)**.** *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 $\alpha_1, \ldots, \alpha_n$ jsou kořeny f v U a buď $\varphi\colon U \to \overline{T}$ T-homomorfismus $\Rightarrow \varphi$ permutuje $\{\alpha_1, \ldots, \alpha_n\}$ podle tvrzení 2.11.
Jde o rozkladové nadtěleso, takže $U = T(\alpha_1, \ldots, \alpha_n)$, a tedy φ je jednoznačně určené hodnotami $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$, a ty jsou všechny v U. Tudíž φ každý prvek z $U = T(\alpha_1, \ldots, \alpha_n)$ zobrazí do U.
Zřejmě máme, že $U \supset T$ je algebraické, jde tedy vskutku o normální rozšíření.

b) f separabilní polynom $\Rightarrow$ $\alpha_1, \ldots, \alpha_n$ separabilní prvky $\Rightarrow$ $U = T(\alpha_1, \ldots, \alpha_n)$ 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]).
„⇒“ Definuj $\mathcal{M} := \{\text{minimální polynom nějakého } \alpha \in U\}$ a použij lemma 2.22.
„⇐“ Cvičení (podobně jako v tvrzení 2.21a)). □

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]). □

2.10 Galoisova korespondence

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

Tvrzení 2.25. *Mějme algebraické rozšíření těles* $U \supset T$ *a* T*-homomorfismus* $\varphi : U \to U$. *Pak je* φ *dokonce* T*-automorfismus.*

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

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

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 $\varphi(\beta) = \alpha$. □

Tvrzení 2.26. *Buď* $U \supset T$ *rozšíření těles. Pak:*
a) $\mathrm{Fix}\left(U, \mathrm{Gal}\left(U/T\right)\right) \supset T$.
b) Pro $G < \mathrm{Aut}(U)$ *je* $\mathrm{Gal}\left(U/\mathrm{Fix}(U,G)\right) \supset G$.
c) Je-li $U \supset T$ *Galoisovo rozšíření, pak*

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

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

Rozšíření $U \supset T$ je normální, takže

$$\begin{aligned} [U : T]_s &= \#\{\varphi \colon U \to \overline{T} \mid T\text{-hom}\} \overset{\text{normální}}{=} \#\{\varphi \colon U \to U \mid T\text{-hom}\} \\ &\overset{2.25}{=} \#\{\varphi \colon U \to U \mid T\text{-automorfismus}\} = \#\,\mathrm{Gal}\left(U/T\right). \end{aligned}$$

Rozšíření $U \supset T$ je separabilní, takže $[U : T]_s = [U : T]$.

Grupa $\mathrm{Gal}\left(U/T\right)$ je konečná, protože jsme dokázali, že $\#\,\mathrm{Gal}\left(U/T\right) = [U : T]_s = [U : T]$. Tedy můžeme použít větu 2.20 pro U a $G = \mathrm{Gal}\left(U/T\right)$. Ta nám pro $S = \mathrm{Fix}(U, G)$ dává $[U : S] = \#G$ a $\mathrm{Gal}\left(U/S\right) = G$. Tedy $[U : S] = \#\,\mathrm{Gal}\left(U/T\right)$.
Dohromady máme $[U : T] = [U : S]$, jak jsme chtěli. □

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

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

Jako zobrazení z definice pak můžeme vzít

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

Podle tvrzení 2.26a), b) jde o Galoisovu korespondenci.

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

Tvrzení 2.27. *Nechť (α, β) jsou abstraktní Galoisova korespondence.*
a) Pak α, β poskytují vzájemně inverzní bijekce mezi $\operatorname{Im}\alpha$ a $\operatorname{Im}\beta$.
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 $\alpha\beta\colon \operatorname{Im}\alpha \to \operatorname{Im}\alpha$ je identita.
Toto složení je $\operatorname{Im}\alpha \xrightarrow{\beta} \operatorname{Im}\beta \xrightarrow{\alpha} \operatorname{Im}\alpha$, a tedy nutně $\alpha\colon \operatorname{Im}\beta \to \operatorname{Im}\alpha$ je na a $\beta\colon \operatorname{Im}\alpha \to \operatorname{Im}\beta$ je prosté.
Symetricky: $\alpha\colon \operatorname{Im}\beta \to \operatorname{Im}\alpha$ je prosté a $\beta\colon \operatorname{Im}\alpha \to \operatorname{Im}\beta$ je na. Tedy α, β jsou bijekce na obrazech $\operatorname{Im}\alpha, \operatorname{Im}\beta$.
b) je jasné, protože α, β z definice převracejí uspořádání. □

Věta 2.28 (Základní věta Galoisovy teorie)**.** *Nechť $U \supset T$ je Galoisovo rozšíření. Potom máme antiizomorfismus uspořádaných množin*

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

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

Důkaz. Podle tvrzení 2.26 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 2.26c). 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 2.27b) 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 $\varphi \restriction V\colon V \to U \subset \overline{T}$. Ovšem $V \supset T$ je normální, takže

obraz tohoto zúžení leží ve V, neboli $\varphi \restriction V : V \to V$. Podle tvrzení 2.25 pak jde o automorfismus, neboli $\varphi(V) = V$.

Buď $\psi \in \mathrm{Gal}\left(U/V\right)$, k důkazu normality této podgrupy chceme dokázat, že $\varphi\psi\varphi^{-1} \in \mathrm{Gal}\left(U/V\right) < \mathrm{Gal}\left(U/T\right)$, 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 $\mathrm{Gal}\left(U/V\right)$ je normální podgrupa v $\mathrm{Gal}\left(U/T\right)$.

2. Ať je $H \lhd \mathrm{Gal}\left(U/T\right)$ normální podgrupa. Bude se nám hodit následující pozorování:
Cvičení. Buď U těleso a $G < \mathrm{Aut}(U)$ podgrupa. Pak pro všechna $\varphi \in \mathrm{Aut}(U)$ platí $\mathrm{Fix}(U, \varphi G\varphi^{-1}) = \varphi(\mathrm{Fix}(U, G))$ (přičemž $\varphi G\varphi^{-1} = \{\varphi g\varphi^{-1} \mid g \in G\}$).

Podle tohoto cvičení tedy pro $\varphi \in \mathrm{Gal}\left(U/T\right)$ máme $\mathrm{Fix}(U, \varphi H\varphi^{-1}) = \varphi(\mathrm{Fix}(U, H))$. Zároveň z normality $\varphi H\varphi^{-1} = H$, takže $\mathrm{Fix}(U, H) = \mathrm{Fix}(U, \varphi H\varphi^{-1}) = \varphi(\mathrm{Fix}(U, H))$.
Tedy jsme dokázali:
$\circledast$ každé $\varphi \in \mathrm{Gal}\left(U/T\right)$ zobrazí $V = \mathrm{Fix}(U, H)$ na sebe.

Dokažme nyní konečně, že $V \supset T$ je normální rozšíření. Buď $\varphi : V \to \overline{T}(= \overline{U} = \overline{V})$ T-homomorfismus. Podle důsledku 2.10b) jde φ rozšířit na T-homomorfismus $\psi : U \to \overline{T}$.
Rozšíření $U \supset T$ je normální, takže $\psi(U) \subset U$. Podle tvrzení 2.25 je pak $\psi \in \mathrm{Gal}\left(U/T\right)$.
Zároveň $\varphi = \psi \restriction V$. Podle $\circledast$ máme $\psi(V) = V$, a tedy $\varphi(V) = V$.
Tedy $V \supset T$ je normální rozšíření. □

Důsledek 2.29. *Mějme tělesa $U \supset V \supset T$ taková, že $U \supset T$ a $V \supset T$ jsou Galoisova rozšíření. Pak*

$$\mathrm{Gal}\left(U/T\right)/\mathrm{Gal}\left(U/V\right) \simeq \mathrm{Gal}\left(V/T\right).$$

Důkaz. Uvažujme zobrazení

$$\Phi : \mathrm{Gal}\left(U/T\right) \to \mathrm{Gal}\left(V/T\right), \varphi \mapsto \varphi \restriction V.$$

Podle bodu 1. v předchozím důkazu víme, že Φ je dobře definované zobrazení; zřejmě jde o homomorfismus. Také vidíme, že $\mathrm{Ker}\,\Phi = \mathrm{Gal}\left(U/V\right)$, protože jádro sestává právě z těch automorfismů tělesa T, jejichž zúžení na V je identita. Podle důsledku 2.10b jde každý prvek $\mathrm{Gal}\left(V/T\right)$ rozšířit na prvek $\mathrm{Gal}\left(U/T\right)$, neboli Φ je surjektivní. 1. věta o izomorfismu pak dává kýžený izomorfismus (a také alternativní důkaz toho, že $\mathrm{Gal}\left(U/V\right) \lhd \mathrm{Gal}\left(U/T\right)$). □

2.11 Výpočty Galoisových grup

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

Věta 2.30. *Buď $n \in \mathbb{N}, a_1, \ldots, a_n \in \mathbb{Q}$ takové, že pro každou neprázdnou podmnožinu $I \subset \{1, \ldots, n\}$ máme $\prod_{i \in I} \sqrt{a_i} \notin \mathbb{Q}$. Potom:*

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

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

Důkaz. Buď $K := \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$. 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 $\sqrt{a_1}, \ldots, \sqrt{a_n}$ 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 $\operatorname{Gal}\left(K/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/2\right)^n$ (zde si člověk samozřejmě musí důkladně rozmyslet, že jde o izomorfismus grup – a jak přesně vlastně vypadá!). □

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 skripta k ní). Z toho pak už jde snadno dokázat (podobně jako v částečném důkazu věty 2.30 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

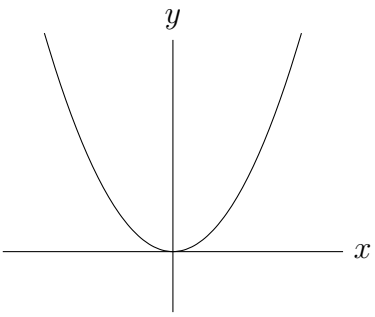
3.1 Algebraické množiny a ideály

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

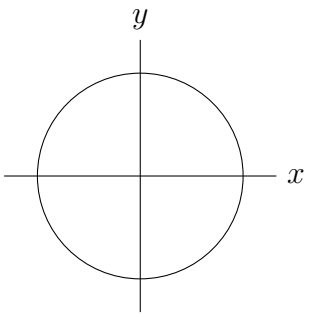
Definice. Ať $p = (a_1, \ldots, a_n) \in K^n$ a $f \in K[x_1, \ldots, x_n]$. Bod p je *nula* polynomu f, pokud $f(p) = 0$. Množina všech nul polynomu f se značí $V(f)$. Pokud f není konstantní polynom, pak se $V(f)$ nazývá *nadplocha*.

Příklad.

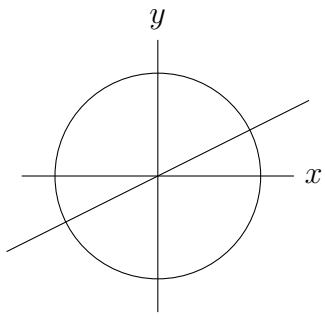
- $\underline{n = 2}$:



$V(y - x^2)$

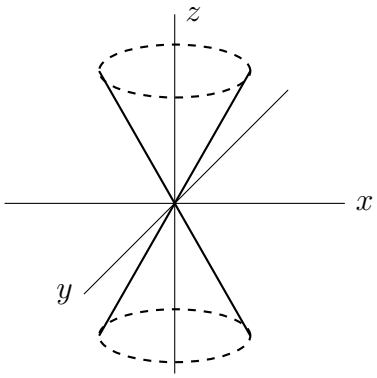


$V(x^2 + y^2 - 1)$



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

- $\underline{n = 3}$: kužel



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

- $y = e^x$ není nadplocha

Definice. Pro množinu polynomů $S \subset K[x_1, \ldots, x_n]$ 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 $f(a_1, \ldots, a_n) = 0$ pro všechna $a_1, \ldots, a_n \in K$, potom $f = 0$. Indukcí podle n:
$n = 1$: $f(x_1)$ má jen konečně mnoho kořenů, zatímco K je nekonečné.
$n \geq 2$: Ať

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

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

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

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

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

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

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

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

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 2.27. □

Jaké jsou obrazy V a I? Obraz V jsou z definice algebraické množiny. Pokud je K algebraicky uzavřené, tak obraz I jsou radikálové ideály (viz definice v příští sekci), 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 1.23 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 $\bigcap_{Q \in \mathcal{B}} Q$, což je zřejmě ideál.
Máme $Q \supset I$ pro všechna $Q \in \operatorname{Var} I$, a tedy $\bigcap Q \supset I$.
Je $\bigcap_{Q \in \mathcal{B}} Q =: J$ 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 $\sqrt{I} = \bigcap_{P \in \operatorname{Var} I} P$.*

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 1.26 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 1.26: $b \notin \sqrt{I}$, 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 $\sqrt{0} = \bigcap_{P \text{ prvoideál}} P$.

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

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.
K tomu budeme používat následující pojmy:

Definice. Buď $S \supset R$ rozšíření okruhů. Řekneme, že rozšíření je

1. *okruhově konečné*, pokud existuje $n \geq 1$ a prvky $a_1, \ldots, a_n \in S$ takové, že $S = R[a_1, \ldots, a_n]$;
2. *modulově konečné*, pokud S je konečně generované jako R-modul, tj. existuje $n \geq 1$ a prvky $a_1, \ldots, a_n \in S$ takové, že $S = Ra_1 + \cdots + Ra_n$.

V této terminologii 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. $R[v] \supset R$ je modulově konečné,
3. $\exists R'$ obor, $R[v] \subset R' \subset S$ a $R' \supset R$ je modulově konečné.

Důsledek 3.10. *Buďte $K \subset L$ tělesa, K algebraicky uzavřené. Pokud je $L \supset K$ je modulově konečné, 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 $a_i \in K$. *Tato část důkazu byla už v druhácké Algebře coby tvrzení, že každé rozšíření těles konečného stupně je algebraické.*
Ale K je algebraicky uzavřené, takže $\alpha \in K$. □

Lemma 3.11. *Buď K těleso a $n \geq 1$. Pak $K(x_1, \ldots, x_n) \supset K$ není okruhově konečné (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 $0 \neq f \in K(x)$ 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 $L \supset K$ je okruhově konečné rozšíření, čili $L = K[v_1, \ldots, v_n]$ pro nějaká $v_1, \ldots, v_n \in L$. Pak $L \supset K$ je modulově konečné rozšíření.*

Důkaz. Postupujme indukcí podle n.

$\underline{n = 1}$: $L = K[v]$. Máme 2 případy:
a) v je algebraické 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 $v_2, \ldots, v_n$ celistvé nad K_1.
Máme tedy rovnosti $v_i^{n_i} + a_{i,n_i-1} v_i^{n_i-1} + \cdots + a_{i,0} = 0$ 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

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

takže prvky αv_i jsou celistvé nad $K[x]$.
$L = K[x][v_2, \ldots, v_n]$, takže pro každé $z \in L$ existuje n takové, že $\alpha^n z$ je polynom v $\alpha v_2, \ldots, \alpha v_n$ 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 $L \supset K$ je okruhově konečné rozšíření, 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 $R = K[x_1, \ldots, x_n]$. Pak:

- *a) Ideál $I = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ je maximální v R pro každá $\alpha_1, \ldots, \alpha_n \in K$. Navíc polynom $f \in R$ leží v tomto ideálu, právě když $f(\alpha_1, \ldots, \alpha_n) = 0$.*
- *b) Pokud je K algebraicky uzavřené, potom všechny maximální ideály v R jsou tvaru $(x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ pro nějaká $\alpha_1, \ldots, \alpha_n \in K$.*

Důkaz.
a) Polynom $f \in R$ uvažujme jako polynom v proměnné x_n nad $K[x_1, \ldots, x_{n-1}]$. Můžeme jej napsat jako $f = a_n(x_n - \alpha_n) + b_{n-1}$, kde $a_n \in R$ a $b_{n-1} \in K[x_1, \ldots, x_{n-1}]$. 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 $\sum a_i(x_i - \alpha_i) \in I = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$. Tedy platí:
„Navíc“: $f \in I \Leftrightarrow f - \sum_{i=1}^{n} a_i(x_i - \alpha_i) \in I \Leftrightarrow b_0 \in I \Leftrightarrow b_0 = f(\alpha_1, \ldots, \alpha_n) = 0$.
„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 $\operatorname{Ker}(\pi \restriction K) = K \cap M = 0$).
Ale L je nad K generované prvky $x_1 + M, \ldots, x_n + M$ jako okruh. Důsledek 3.14 $\Rightarrow L = K$. Tedy

$$\begin{aligned} \pi \restriction K \colon K \to L &= {}^{R}/_{M} \\ a &\mapsto a + M \end{aligned}$$

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 $1 = \sum a_i f_i + b(x_{n+1}g - 1)$.

Pojďme nyní pracovat v $K[x_1, \ldots, x_n](x_{n+1})$. 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 2.27 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 $I(V(I)) = I$.*

Tedy máme bijekci (respektive antiizomorfismus uspořádaných množin)

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

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 $\mathcal{T} = \left\{ \text{algebraické množiny } V \subset K^n \;\middle|\; \begin{array}{l} V \text{ není sjednocení konečně mnoha} \\ \text{ireducibilních algebraických množin} \end{array} \right\}$.
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 $V = V_1 \cup \cdots \cup V_m = W_1 \cup \cdots \cup W_\ell$. Potom $V_i = (V_i \cap W_1) \cup \cdots \cup (V_i \cap W_\ell)$. 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 $\left\{ \begin{matrix} \text{ireducibilní nekonstantní monické} \\ \text{polynomy v } K[x_1, \ldots, x_n] \end{matrix} \right\} \leftrightarrow \{\text{ireducibilní nadplochy v } K^n\}$.

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 $(x + i)(x - i) = y^3$ 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 $\alpha \mid 2, \alpha \nmid 1, \alpha \nmid 2$.
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. □

Grupa ideálů

Množinu všech nenulových ideálů v $\mathbb{Z}[\sqrt{-5}]$ (ale i obecněji) s operací násobení můžeme rozšířit na grupu podobně jako se konstruuje podílové těleso: Uvažujeme formální podíly AB^{-1} pro nenulové ideály A, B, přičemž ztotožňujeme (formálně tak, že definujeme příslušnou ekvivalenci) AB^{-1} s CD^{-1}, právě když $AD = BC$.
Na výsledné množině $\mathcal{I} = \{AB^{-1} \mid A, B \text{ nenulové ideály}\}$ definujeme násobení tak, že $(AB^{-1}) \cdot (CD^{-1}) = (AB)(CD)^{-1}$, čímž dostáváme *grupu ideálů*.

Také pro $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ máme hlavní ideály $(\alpha), (\beta)$.
Definujeme pak $\mathcal{P} = \{(\alpha) \cdot (\beta)^{-1} \mid \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]\}$ coby podgrupu v $\mathcal{I}$.

Platí: OHI $\Leftrightarrow \mathcal{I} = \mathcal{P} \Leftrightarrow \mathcal{I}/\mathcal{P} = \{1\}$.
Také OHI $\Rightarrow$ Gaussovskost (což nás zajímá pro řešení diofantických rovnic).

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 $A^3 \in \mathcal{P}$ podle (3).
Zároveň $\#\mathcal{C}\ell = 2$, 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. „⇐“: Jasné
„⇒“: 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.
Není těžké ověřit, že $n\alpha \in \mathcal{O}_K$ (porovnej $n^k \cdot m_\alpha$ a $m_{n\alpha}$, kde k je stupeň minimálního polynomu α).
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. *Bud' $D \neq 0, 1$ bezčtvercové a $K = \mathbb{Q}(\sqrt{D})$. Pak*

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

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 $4b^2 D = (2b)^2 D \in \mathbb{Z}$.
Jmenovatel racionálního čísla $(2b)^2$ je čtverec, který musí dělit D, aby $(2b)^2 D \in \mathbb{Z}$. 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 $N\alpha = \frac{c^2 - d^2 D}{4} \in \mathbb{Z}$ implikuje $c^2 \equiv d^2 D \pmod 4$.

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 jsme 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 $a = a_1 b_1 + \dots + a_m b_m \in I$, 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:
„⇐“ Jasné.
„⇒“ 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.
„⇒“: $\exists \gamma \in \mathcal{O}_K$ takové, že $\beta = \alpha\gamma \Rightarrow (\beta) = (\alpha\gamma) = (\alpha)(\gamma) \Rightarrow (\alpha) \mid (\gamma)$
„⇐“: $\beta \in (\beta) = (\alpha) \cdot H = \{\alpha i \mid i \in H\}$. 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 ideály $I, J < \mathcal{O}_K$ máme $I \mid J \Leftrightarrow I \supset J$.*

Důkaz. Pokud je nějaký z ideálů I, J nulový, tak ekvivalence platí triviálně. Dál tedy uvažujme jen nenulové ideály. Pro ty zatím dokážeme jen „⇒“, druhá implikace pak bude 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:

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

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 $I = (\alpha_1, \ldots, \alpha_m) < \mathcal{O}_K$, pak II' je ideál generovaný prvky $N\alpha_1, \ldots, N\alpha_m$ 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. „⇐“: 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 v 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. „⇐“ $(1) = II' \subset I\mathcal{O}_K = I \Rightarrow I = \mathcal{O}_K$.
- $N(IJ) = NI \cdot NJ$
- $I \mid J \Rightarrow NI \mid NJ$
- 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. □

Poznamenejme, že faktorokruh $\mathcal{O}_K/I$ má ve skutečnosti přesně NI prvků (což v obecném číselném tělese slouží k definici normy ideálu).

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) ⇒ a) je jasné.

c) ⇒ 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) ⇒ 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) ⇒ 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. „⇒“: Tvrzení 1.8
„⇐“: 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 $B = \mathcal{O}_K$. □

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

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

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. □

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

Věta 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 $N(I) = \mathrm{NSD}(N(p), \mathrm{Tr}(p(\omega - c)), N(\omega - c))$. 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 $(2 + 3\sqrt{-14})$
$N(2 + 3\sqrt{-14}) = 4 + 9 \cdot 14 = 130 = 2 \cdot 5 \cdot 13$
$2 + 3\sqrt{-14} \in P_2$
$2 + 3\sqrt{-14} \in P_5$? $2 + 3\sqrt{-14} - 3(\underbrace{\sqrt{-14} + 1}_{\in P_5}) = -1 \notin P_5 \Rightarrow 2 + 3\sqrt{-14} \notin P_5$
$2 + 3\sqrt{-14} - 3(\sqrt{-14} + 5) = -13 \in P_{13}$, 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 $(5 + 2\sqrt{-14}) = P_3^4$

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. Zadání cvičení

Ve verzi ze zimního semestru 2023/2024 podle Matěje Doležálka. V další kapitole následují (částečná) řešení.

5.1 Cvičení 1

ideály, ideálové operace, prvoideály, maximální ideály

1. Dokaž, že sjednocení řetězce (libovolně mnoha) ideálů $I_1 \subset I_2 \subset I_3 \subset \cdots$ je ideál.

2. Pro ideály I, J definujme $I + J := \{a + b \mid a \in I, b \in J\}$. 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 $a \in R \setminus M$ platí $R = M + aR$.
b) Pokud M je maximální a $a \in R \setminus M$, pak existují $m \in M$ a $r \in R$ taková, že $1 = m + ar$.

4. Mějme ideály I, J, K okruhu R. Dokaž, že $IJ \subset I \cap J$ a $I(J + K) = IJ + IK$. Najdi příklad, kdy $IJ \neq I \cap J$.

5. Urči: $\mathbb{Q}[x]/(x+2)$, $\mathbb{Q}[x]/(x^2-2)$, $\mathbb{Q}[x]/(x^2-1)$, $\mathbb{R}[x]/(x^2-2)$, $\mathbb{Z}[x]/(x^2-2)$.

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: Je-li R okruh, $I < R$ ideál a $S \subset R$ podokruh, pak je $S + I$ podokruh v R a platí $(S + I)/I \simeq S/(S \cap I)$.

8. 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.

9. 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.

10. Pro podmnožiny A, B okruhu R definujme $A \odot B := \{ab \mid a \in A, b \in B\}$ (pozor, toto neodpovídá násobení ideálů). Buď I ideál v R. Dokaž, že $(a + I) \odot (b + I) \subset ab + I$. Platí opačná inkluze?

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.

12. Buď R noetherovský okruh a $I < R$ ideál. Dokaž, že R/I je také noetherovský.

13. Je dán okruh R, v němž pro každé $x \in R$ existuje celé číslo $n \geq 2$ tak, že $x^n = x$. Dokaž, že každý prvoideál v R je maximální.

Hinty

5. 1. věta o izomorfismu + někdy Čínská zbytková.
7. Projekce $\pi\colon R \twoheadrightarrow R/I$ a její zúžení na $\varphi\colon S \to R/I$. 1. věta o izomorfismu pro φ.
10. Neplatí. Zvol $R = \mathbb{Z}$ a prvočíslo v $ab + I$.
12. Ideály v R/I jsou přesně tvaru J/I pro $J < R$, $J \supset I$.
13. Najdi inverz ve faktorokruhu.

5.2 Cvičení 2

Gaussovo lemma, Čínská zbytková věta, využití Zornova lemmatu

1. Buď R gaussovský obor a T jeho podílové těleso. Pro každý ireducibilní polynom $f \in T[x]$ existuje $u \in T\backslash\{0\}$ takové, že uf je ireducibilní prvek $R[x]$.

2. Buď K těleso. Pak $K[x, y]$ i $K[x_1, x_2, \dots]$ (nekonečně mnoho proměnných) jsou gaussovské, ale $K[x, y]$ není obor hlavních ideálů (ale je noetherovský) a $K[x_1, x_2, \dots]$ není noetherovský ani obor hlavních ideálů.

3. Popiš všechny ideály v okruhu $\mathbb{Z}/(150)$ a charakterizuj, které dvojice z nich jsou komaximální.

4. Buď R okruh. Pomocí Zornova lemmatu dokaž, že každý vlastní ideál je obsažený v nějakém maximálním ideálu.

5. Použij důkaz Čínské zbytkové věty (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?

6. Uvědom si, že v uspořádané množině $\mathcal{A}$ může existovat i nespočetný řetězec $\mathcal{B}$, na jehož indexování nestačí přirozená čísla. Najdi pár příkladů takové situace. (Není v tom žádný chyták, jen by si člověk neměl utvořit představu, že v Zornovi stačí vyřešit řetězce indexované přirozenými čísly.)

7. Nahlédni, že je-li $\varphi : R \to S$ homomorfismus okruhů, pak vztahy $\psi(r) := \varphi(r)$ pro $r \in R$ a $\psi(x) := x$ splňuje právě jeden homomorfismus $\psi : R[x] \to S[x]$. Navíc je ψ injektivní/surjektivní, právě když φ je injektivní/surjektivní.

8. Ať je R okruh a $I_1, \dots, I_n$ po dvou komaximální ideály v R. Uvědom si, že z ČZV máme speciálně izomorfismus multiplikativních grup $(R/(I_1 \cdots I_n))^\times \simeq (R/I_1)^\times \times \cdots \times (R/I_n)^\times$. Jako aplikaci tohoto faktu si rozmysli, že pro lichá prvočísla $p \neq q$ nemůže být grupa $(\mathbb{Z}/(pq))^\times$ cyklická.

9. Dokaž Zornovým lemmatem: ve vektorovém prostoru lze libovolnou lineárně nezávislou množinu rozšířit na bázi.

10. 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 $x, y \in M$.

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. * Buď F konečné těleso. Nahlédni, že libovolné zobrazení $f : F \to F$ lze zapsat polynomem.

13. * (Eisensteinovo kritérium) Mějme primitivní polynom $f = a_n x^n + \cdots + a_1 x + a_0$ s celočíselnými koeficienty a prvočíslo p. Dokaž, že pokud $p \nmid a_n$, $p \mid a_i$ pro $i = 0, 1, \dots, n-1$ a $p^2 \nmid a_0$, pak je f ireducibilní nad $\mathbb{Z}$. Zkus se zamyslet nad zobecněním pro obecný obor integrity R namísto $\mathbb{Z}$.

14. * 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.

Hinty

12. Čínská zbytková věta v $F[x]$. Lineární polynomy dávají maximální ideály. (Alternativně Lagrangeova interpolace.)

13. Předpokládej pro spor $f = gh$, zobraz celou situaci projekcí $\mathbb{Z}[x] \twoheadrightarrow \mathbb{Z}_p[x]$ a využij jednoznačných rozkladů.

5.3 Cvičení 3

kořenová a rozkladová nadtělesa, algebraický uzávěr, Galoisova grupa, separabilita

1. Buď α algebraický prvek nad tělesem T. Pak $[T(\alpha) : T] = \deg m_{\alpha,T}$.

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

3. 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.

4. Buď $U \supset T$ rozšíření těles a $\alpha \in U$ kořen *nějakého* separabilního $f \in T[x]$. Potom už je α separabilní nad T.

5. Rozšíření těles konečného stupně je nutně algebraické.

6. Mějme rozšíření těles $V \supset U \supset T$. Pak $[V : T] = [V : U] \cdot [U : T]$.

7. 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.

8. Buď $\varphi : K \to R$ homomorfismus okruhů. Připomeň si, že když K je těleso, musí φ být prosté.

9. 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) $f(x) = x^2 + 1$, $T = \mathbb{Q}$, *c) $f(x) = x^2 + 1$, $T = \mathbb{Z}_7$,
b) $f(x) = x^4 - 1$, $T = \mathbb{Q}$, **d) $f(x) = x^n - 1$, $T = \mathbb{Q}$, $n \in \mathbb{N}$.

10. Buďte $S \supset T$ tělesa, S algebraicky uzavřené a $U = \{\alpha \in S \mid \alpha \text{ algebraické nad } T\}$. Pak je U algebraický uzávěr T. (tvrzení 2.7 ze skript)

11. Buďte T, U tělesa charakteristiky 0. Pak $\mathbb{Q} \subset T, U$ a každý homomorfismus $\varphi : T \to U$ je $\mathbb{Q}$-homomorfismem. (V charakteristice p má stejnou vlastnost těleso $\mathbb{Z}_p$.)

12. Prvek α je algebraický nad tělesem T, právě když $T(\alpha) = T[\alpha]$.

13. * Žádné konečné těleso není algebraicky uzavřené.

14. * Buď p prvočíslo, $T = \mathbb{Z}_p(y)$ a $U = T(\sqrt[p]{y})$. Urči $[U : T]$, $[U : T]_s$ a $\mathrm{Gal}(U/T)$.

15. * Algebraický uzávěr nekonečného tělesa T má stejnou mohutnost jako T.

Hinty

4. $m_{\alpha,T} \mid f$.

11. Homomorfismus musí nechávat na místě celé podtěleso generované jedničkou (tzv. *prvotěleso*).

12. Z minimálního polynomu vyrobíš inverz (a naopak).

13. Začni s polynomem, jehož kořeny jsou všechny prvky.

14. $x^p - y \in \mathbb{Z}_p[y][x]$ je ireducibilní z Eisensteina, ale má jen jeden p-násobný kořen.

15. Rozmysli si, že $\#T[x] = \#T$, takže když (v jednom kroku) přidáme kořeny všech polynomů, mohutnost se zachová.

5.4 Cvičení 4

rozšíření separabilní, normální, jednoduchá a Galoisova

1. Buď $U \supset T$ rozšíření konečného stupně. Dokaž, že je Galoisovo, právě když $[U : T] = \#\operatorname{Gal}(U/T)$.

2. (zachovávání a skládání význačných vlastností) Buďte $V \supset U \supset T$ rozšíření těles. Víš-li, že rozšíření $V \supset T$ má vlastnost X, rozhodni, zda nutně musí i $V \supset U$ či $U \supset T$ mít vlastnost X. Víš-li, že obě $V \supset U$, $U \supset T$ mají vlastnost X, rozhodni, zda ji nutně musí mít i $V \supset T$.

a) $X =$ konečného stupně,
b) $X =$ algebraické,
c) $X =$ separabilní,
d) $X =$ normální,
e) $X =$ Galoisovo.

3. Rozhodni o následujících rozšířeních, které z význačných vlastností z úlohy **2.** mají a které ne:
a) $\mathbb{C} \supset \mathbb{R}$, b) $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$, *c) $\mathbb{Z}_p(x) \supset \mathbb{Z}_p$, *d) $\overline{\mathbb{Q}} \supset \mathbb{Q}$.

4. Buď $V \supset T$ Galoisovo rozšíření a $V \supset U \supset T$. Dokaž, že $[U : T] = \frac{\#\operatorname{Gal}(V/T)}{\#\operatorname{Gal}(V/U)}$.

5. Buď $f \in T[x]$ polynom s rozkladem na navzájem neasociované ireducibilní polynomy $f = f_1 \cdots f_k$. Uvažujme Galoisovu grupu rozkladového nadtělesa f nad T jako grupu permutací na množině kořenů f. Nahlédni, že každá z těchto permutací musí mít alespoň k cyklů.

6. (opakování z přednášky) Buď U těleso, $G < \operatorname{Aut}(U)$ podgrupa a $T \subset U$ podtěleso. Potom platí $\operatorname{Gal}(U/\operatorname{Fix}(U, G)) \supset G$ a $\operatorname{Fix}(U, \operatorname{Gal}(U/T)) \supset T$.

7. Budiž $U \supset T$ separabilní rozšíření konečného stupně. Nahlédni, že existuje těleso V takové, že $U \subset V$, $[V : T] \leq ([U : T])!$ a rozšíření $V \supset T$ je Galoisovo.

8. Podle lemmatu 2.25, je-li $U \supset T$ algebraické rozšíření, pak už musí každý T-homomorfismus $\varphi : U \to U$ být dokonce T-automorfismus. Rozmysli si, že algebraičnost je nutná – pro $T = \mathbb{Z}_p$, $U = T(x)$ (těleso racionálních funkcí) najdi T-homomorfismus $\varphi : U \to U$, který není T-automorfismus.

9. Buď T těleso s $\operatorname{char} T \neq 2$ a $a, b \in T$ prvky s $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin T$. Pak $[T(\sqrt{a}, \sqrt{b}) : T] = 4$.
* Můžeš zkusit dokázat $\operatorname{Gal}(T(\sqrt{a}, \sqrt{b})/T) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

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. * (existence separabilního uzávěru) Buď $U \supset T$ rozšíření těles. Všechny prvky $\alpha \in U$, jež jsou separabilní nad T, tvoří podtěleso U.

12. * Buď p prvočíslo, $U = \mathbb{Z}_p(x, y)$, $T = \mathbb{Z}_p(x^p, y^p)$. Dokaž, že rozšíření $U \supset T$ není jednoduché.

Hinty

4. Stačí zkombinovat **2.**d) a **1.**.
7. Máš jednoduché rozšíření, rozlož minimální polynom.
11. Uvědom si, že libovolné dva separabilní prvky nagenerují separabilní rozšíření.
12. Pokud $U = T(r)$, nahlédni $r^p \in T$ a vyvoď spor pomocí stupňů.

5.5 Cvičení 5

počítání Galoisových grup, Galoisova korespondence

Na tomto cvičení pro nás *určit* Galoisovu grupu znamená najít nějakou „známou“ grupu, které je izomorfní, a rozmyslet si, jak jednotlivé automorfismy působí. Známe grupy jsou třeba $\mathbb{Z}_n$, D_{2n}, S_n nebo součiny známých grup.

1. Urči, zda je Galoisovu grupu $T \supset \mathbb{Q}$ a všechna tělesa U, $T \supset U \supset \mathbb{Q}$, jestliže

a) $T = \mathbb{Q}(i, \sqrt{2})$,

b) $T =$ rozkladové nadtěleso $x^3 - 2$ nad $\mathbb{Q}$.

2. Pro rozšíření těles $U \supset T$ urči $[U : T]$ spolu s bází U jako vektorového prostoru nad T, rozhodni, zda jde o Galoisovo rozšíření, a pokud ano, urči také všechna tělesa V, $U \supset V \supset T$, jestliže

a) $U = \mathbb{Q}(\sqrt{2}, e^{2\pi i/3})$, $T = \mathbb{Q}$,
b) $U = \mathbb{Q}(\sqrt[3]{3})$, $T = \mathbb{Q}$,
c) $U = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $T = \mathbb{Q}$,
d) $U = \mathbb{Q}\left(\sqrt{1 + \sqrt{2}}\right)$, $T = \mathbb{Q}$.

3. Buď U rozkladové nadtěleso polynomu f nad tělesem T. Urči U, $[U : T]$, bázi U nad T a $\mathrm{Gal}(U/T)$ (můžeš se taky zamyslet nad tělesy V, $U \supset V \supset T$, ale mnohdy vypadají dost ošklivě), jestliže

a) $f = x^2 - 5$, $T = \mathbb{Q}$,
b) $f = x^3 - 2$, $T = \mathbb{Q}(e^{2\pi i/3})$,
c) $f = (x^2 - 3)(x^2 - 5)$, $T = \mathbb{Q}(\sqrt{2})$,
*d) $f = (x^2 - 1)^2 - 2$, $T = \mathbb{Q}$.

4. Mějme tělesa $V \supset U \supset T$ taková, že jak $V \supset T$, tak $U \supset T$ jsou normální rozšíření. Pak $\mathrm{Gal}(V/U) \triangleleft \mathrm{Gal}(V/T)$ a $\mathrm{Gal}(V/T)/\mathrm{Gal}(V/U) \simeq \mathrm{Gal}(U/T)$.

5. Uvažujme cyklotomická tělesa.

a) Připomeň si, že $\mathrm{Gal}\left(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}\right) \simeq \mathbb{Z}_n^\times$. Předpokládej, že už víš $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$.
b) Buď U rozkladové nadtěleso $x^{20} - 1$ nad $\mathbb{Q}(i)$. Urči $\mathrm{Gal}(U/\mathbb{Q}(i))$ a všechna mezitělesa V, $U \supset V \supset \mathbb{Q}(i)$.
c) * Buď U kořenové nadtěleso $x^3 + x^2 - 2x - 1$ nad $\mathbb{Q}$. Urči $\mathrm{Gal}(U/\mathbb{Q})$.

6. Mějme rozšíření $U \supset \mathbb{Q}$ konečného stupně, které ale není normální. Zamysli se, jestli přesto nedovedeme *nějak* pomocí Galoisovy korespondence najít všechna tělesa V, $U \supset V \supset \mathbb{Q}$. Obecněji uvažuj totéž pro rozšíření $U \supset T$, jež je separabilní a konečného stupně, ale není normální.

7. * Buď U rozkladové nadtěleso polynomu f nad tělesem T. Urči U, $[U : T]$, bázi U nad T a $\mathrm{Gal}(U/T)$ a všechna tělesa V, $U \supset V \supset T$, jestliže

a) $f = x^3 - 5$, $T = \mathbb{Z}_7$,
b) $f = x^4 - 3$, $T = \mathbb{Z}_5$,
c) $f = x^{p^k} - x$, $T = \mathbb{Z}_p$.

8. ** Nahlédni, že pokud $\mathrm{Gal}(T/\mathbb{Q}) \simeq A_4$, pak neexistuje žádné těleso U, $T \supset U \supset \mathbb{Q}$ se stupněm $[U : \mathbb{Q}] = 2$. Pokud si věříš, zkus dokázat, že rozkladové nadtěleso $f = x^4 + 8x + 12$ nad $\mathbb{Q}$ je příkladem takového T. (Mně se to zatím nepovedlo dokázat, ale podle důvěryhodného zdroje by to měla být pravda.)

Hinty

5. b) Dívej se na $\mathrm{Gal}(U/\mathbb{Q}(i))$ uvnitř $\mathrm{Gal}(U/\mathbb{Q})$, její strukturu znáš. c) Dívej se v sedmém cyklotomickém tělese.

6. Nestačí se na všechno podívat uvnitř většího rozšíření, které je Galoisovo?

7. a), b) Jaké má $\mathbb{Z}_7/\mathbb{Z}_5$ třetí/čtvrté odmocniny z jedničky? c) Trik: množina kořenů je uzavřená na sčítání i násobení.

5.6 Cvičení 6

algebraické množiny, Hilbertova věta o nulách, radikály

1. Rozhodni, které z následujících množin jsou algebraické:

a) $\{(t, t^2, t^3) \in K^3 \mid t \in K\}$,
b) $\{(\cos t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$,
c) $\mathbb{Z}$ jako podmnožina $\mathbb{R}$,
d) * $\mathbb{Z}^2$ jako podmnožina $\mathbb{R}^2$,
e) * $\{(t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$.

2. (protipříklad Hilbertovy věty bez algebraické uzavřenosti) Najdi v $\mathbb{R}[x]$ maximální ideál, který neobsahuje žádný lineární polynom.

3. *Jacobsonův radikál* okruhu R definujeme jako $\mathcal{J}(R) := \bigcap_{M<R \text{ maximální}} M$. Nahlédni, že $a \in \mathcal{J}(R)$, právě když je $1 - ar$ jednotka pro každé $r \in R$.

4. Urči v oboru celých čísel $\mathbb{Z}$

a) $\sqrt{(0)}$, $\mathcal{J}(\mathbb{Z})$,
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) $\mathcal{J}(\mathbb{Z}/(100))$,
d) * kdy je ${}^{(\mathbb{Z}/(n))}/_{\mathcal{J}(\mathbb{Z}/(n)}$ těleso.

5. V oboru $\mathbb{C}[x]$ polynomů nad komplexními čísly

a) spočítej $\sqrt{(0)}$, $\mathcal{J}(\mathbb{C}[x])$, $\sqrt{(x-3)^5(x-1)^4(x^3+2)}$, $\sqrt{(x^6 - x^4 - x^2 + 1)}$,
b) dokaž, že $\sqrt{(p)} = (\frac{p}{\text{NSD}(p,p')})$, kde $p \in \mathbb{C}[x]$.

6. 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.

7. Je-li K konečné těleso, pak je každá podmnožina v K^n algebraická.

8. Nahlédni, že pro ideál $I < R$ je $\sqrt{I}$ roven $\pi^{-1}(\sqrt{0/I})$, kde $\pi : R \twoheadrightarrow R/I$ je přirozená projekce.

9. Buď K nekonečné těleso a $V = \{(t, t^2, t^3, \ldots, t^n) \mid t \in K\} \subset K^n$. Urči $I(V)$ (s důkazem!) a na základě úlohy z DÚ (V ireducibilní $\iff$ $I(V)$ prvoideál) vyvoď, že V je ireducibilní.

10. Rozmysli si následující charakterizace ideálů pomocí faktorokruhů: $I < R$ je

- maximální, právě když jsou všechny nenulové prvky R/I invertibilní,
- prvoideál, právě když je součin nenulových prvků v R/I vždy nenulový,
- radikálový, právě když je mocnina nenulového prvku v R/I vždy nenulová.

11. 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.

Hinty

7. Jednobodové množiny jsou vždy algebraické.
9. Převeď vše na jednu proměnnou.

5.7 Cvičení 7

Algebraická teorie čísel

1. Najdi všechny jednotky v $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ pro $D = -2, -3, -7$.
* Pokud už jsi někdy viděl(a) Pellovu rovnici, zkus i $D = 2, 5$.

2. Ireducibilní prvky pro $K = \mathbb{Q}(\sqrt{-14})$:
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.

3. Hlavní ideály pro $K = \mathbb{Q}(\sqrt{-14})$:
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) Dokaž, že $(2 + \sqrt{-14}, 7 + 2\sqrt{-14}) = (3, 1 - \sqrt{-14})$ a že jde o vlastní ideál, který není hlavní.

4. Násobení ideálů pro $K = \mathbb{Q}(\sqrt{-14})$:
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.

5. Buď G podgrupa aditivní grupy $\mathbb{Z}^n$, kde $n \in \mathbb{N}$. Dokaž, že $G \simeq \mathbb{Z}^m$ pro nějaké m, $0 \leq m \leq n$. Jako důsledek nahlédni, že libovolný ideál v $\mathcal{O}_K$ lze zapsat nanejvýš dvěma generátory.

6. 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 $m \mid \alpha$ v $\mathcal{O}_K$, právě když $m \mid a, b$ v $\mathbb{Z}$. Nahlédni, že pro $D \equiv 1 \pmod 4$ nemusí totéž platit pro $m \mid a + b\sqrt{D}, a, b \in \mathbb{Z}$.

7. Vyřeš diofantické rovnice $x^2 + 1 = y^5$, $x^2 + 3 = y^3$ a $x^2 + 4 = y^3$.

8. Dokaž, že $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\sqrt{D}]$, resp. $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ pro $D \equiv 2, 3$, resp. $1 \pmod 4$.

9. Buď $K = \mathbb{Q}(\sqrt{D})$. Je-li $P < \mathcal{O}_K$ nenulový prvoideál a $\alpha \in \mathcal{O}_K$, potom $\alpha^{NP} \equiv \alpha \pmod P$.

10. Buď R gaussovský obor a T jeho podílové těleso. Je-li $u \in T$ celistvé nad R, pak $u \in R$.

11. * Je dáno prvočíslo $p > 5$ a přirozené k takové, že $p \mid k^2 + 5$. Dokaž, že existují přirozená m, n splňující $p^2 = m^2 + 5n^2$. Předpokládej, že víš, že třídová grupa $\mathbb{Z}[\sqrt{-5}]$ je dvouprvková.

12. ** Zkus si rozmyslet, že když $D \equiv 1 \pmod 4$, pak $\mathbb{Z}[\sqrt{D}]$ nikdy nemůže být gaussovský obor.

Hinty

8. Dívej se, kdy má minimální polynom celočíselné koeficienty.
10. Věta o racionálním kořeni.
11. Najdi (prvo)ideál s normou p. Co potom třídová grupa říká o jeho druhé mocnině?
12. Úloha **10.** poukazuje na něco, co $\mathbb{Z}[\sqrt{D}]$ nemá.

6. Řešení cvičení

Ve verzi ze zimního semestru 2023/2024 podle Matěje Doležálka.

6.1 Cvičení 1

ideály, ideálové operace, prvoideály, maximální ideály

1. Dokaž, že sjednocení řetězce (libovolně mnoha) ideálů $I_1 \subset I_2 \subset I_3 \subset \cdots$ je ideál.

Řešení. Buď okruh R a zkoumané sjednocení I. Pro $a, b \in I$, $r \in R$ máme dokázat $a + b \in I$, $ra \in I$. Z definice sjednocení musí být pro nějaké indexy být $a \in I_k$, $b \in I_\ell$. Pro $m = \max\{k, \ell\}$ pak už $a, b \in I_m$, takže definicí ideálu $a + b$ i ra leží v $I_m \subset I$.

2. Pro ideály I, J definujme $I + J := \{a + b \mid a \in I, b \in J\}$. Dokaž, že $I + J$ je nejmenší ideál v R, který obsahuje I a J.

Řešení. $I + J$ je ideál: součet generických prvků z $I + J$ je

$$(a_1 + b_1) + (a_2 + b_2) = \underbrace{(a_1 + a_2)}_{\in I} + \underbrace{(b_1 + b_2)}_{\in J}.$$

Obdobně $r(a + b) = ra + rb \in I + J$. Dále $I + J$ triviálně obsahuje I i J. Naopak když nějaký ideál K obsahuje I i J, musí uzavřeností na sčítání obsahovat všechna $a + b$, tedy obsahovat $I + J$.

3. Buď R okruh a M ideál v R. Dokaž:
a) M je maximální, právě když pro všechna $a \in R \setminus M$ platí $R = M + aR$.
b) Pokud M je maximální a $a \in R \setminus M$, pak existují $m \in M$ a $r \in R$ taková, že $1 = m + ar$.

Řešení. a) $M + aR$ je ideál ostře větší než M (má navíc prvek a), z maximality už to tedy musí být celé R. Opačným směrem, když $M \subsetneq I \subset R$, volbou $a \in M \setminus I$ dostaneme $R = M + aR \subset I$, takže $I = R$, což dá maximalitu M.

b) Ideál na levé straně $R = M + aR$ obsahuje jedničku, takže i napravo ji lze tvarem $m + ar$ vyjádřit.

4. Mějme ideály I, J, K okruhu R. Dokaž, že $IJ \subset I \cap J$ a $I(J + K) = IJ + IK$. Najdi příklad, kdy $IJ \neq I \cap J$.

Řešení. Ideály jsou uzavřené na násobení, takže pro $a \in I$, $b \in J$ je speciálně $ab \in I$. Ideál IJ je tvořen součty takových součinů, takže $IJ \subset I$. Úplně analogicky $IJ \subset J$, takže $IJ \subset I \cap J$.

Pro $I(J + K) = IJ + IK$ dokažme obě inkluze, uvažujeme $a \in I$, $b \in J$, $c \in K$. Nalevo je součet součinů tvaru $a(b+c)$, napravo nějaký součet součinů ab plus součet součinů ac. Součiny tvaru $a(b+c)$ umíme roznásobit a interpretovat jako prvky ideálu napravo – to je inkluze „$\subset$“. Pro opačnou inkluzi můžeme každé ab přepsat na $a(b + 0)$ a každé ac na $a(0 + c)$, čímž vyrábíme tvary z levé strany – to je inkluze „$\supset$“.

5. Urči: $\mathbb{Q}[x]/(x + 2)$, $\mathbb{Q}[x]/(x^2 - 2)$, $\mathbb{Q}[x]/(x^2 - 1)$, $\mathbb{R}[x]/(x^2 - 2)$, $\mathbb{Z}[x]/(x^2 - 2)$.

Řešení. Vyjde po řadě $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}\times\mathbb{Q}$, $\mathbb{R}\times\mathbb{R}$ a $\mathbb{Z}[\sqrt{2}]$. Strategie: modulení ireducibilním polynomem = přidání kořene; součin různých ireducibilních polynomů rozlámeme Čínskou zbytkovou větou. Např. pro $\mathbb{Q}[x]/(x^2-2)$ pošleme homomorfismus

$$\begin{aligned}\mathbb{Q}[x] &\to \mathbb{Q}[\sqrt{2}],\\ f &\mapsto f(\sqrt{2}).\end{aligned}$$

Obraz je celé $\mathbb{Q}[\sqrt{2}]$ (předobrazem každého $a+b\sqrt{2}$ je třeba $bx+a$), jádro je (x^2-2) (minimální polynom $\sqrt{2}$). 1. věta o izomorfismu dá výsledek. Pro $\mathbb{Q}[x]/(x^2-1)$ musíme nejdřív rozložit na $\mathbb{Q}[x]/(x-1)\times\mathbb{Q}[x]/(x+1)$ (Čínská zbytková věta), oba činitelé jsou pak izomorfní $\mathbb{Q}$. (Alternativně rovnou pošleme homomorfismus $\mathbb{Q}[x]\to\mathbb{Q}\times\mathbb{Q}$, $f\mapsto(f(1),f(-1))$, ověříme, že je na, a zpozorujeme, že jádro bude (x^2-1).)

Speciálně u $\mathbb{Z}[x]/(x^2-2)$ může být technicky ošemetnější správně zformulovat, že jádro je přesně (x^2-2), kde oproti příkladu nad $\mathbb{Q}$ generujeme ideál ve smyslu okruhu $\mathbb{Z}[x]$. Pokud totiž máme vlastnosti minimálních polynomů zformulované a dokázané jen nad tělesy (jako třeba v druhácké Algebře), nemusí být hned jasné, zda je polynom $f\in\mathbb{Z}[x]$ nulující se v $\sqrt{2}$, který v důsledku toho musí být násobkem x^2-2 ve smyslu okruhu $\mathbb{Q}[x]$, také násobkem x^2-2 ve smyslu okruhu $\mathbb{Z}[x]$. Tuto obtíž lze odstranit více způsoby: např. se lze odkázat na Gaussovo lemma – *primitivní* celočíselný polynom dělí jiný celočíselný polynom ve smyslu $\mathbb{Q}[x]$, pak už je podíl nutně leží v $\mathbb{Z}[x]$. Druhou možností je ručně si rozmyslet, že když minimální polynom bereme monický a zároveň bude celočíselný, vše bude fungovat jak má: podíváme se na $f\in\mathbb{Z}[x]$ splňující $f(\sqrt{2})=0$ modulo x^2-2, postupně vždy x^k nahradíme za $2x^{k-2}$, až zbude lineární celočíselný polynom nulující se v $\sqrt{2}$, a takovým je jen 0.

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).

Řešení. R okruh, I ideál, $a,b\in R$. Chceme ověřit, že pro $x\in a+I$, $y\in b+I$ bude fungovat $x+y\in(a+b)+I$ a obdobně $xy\in ab+I$. K tomu vyjádříme $x=a+i_1$, $y=b+i_2$ a s pomocí uzavřenosti ideálu na sčítání a na násobení prvkem okruhu máme

$$\begin{aligned}x+y &= a+i_1+b+i_2 = (a+b)+\underbrace{(i_1+i_2)}_{\in I},\\ xy &= (a+i_1)(b+i_2) = ab+\underbrace{(ai_2+bi_1+i_1i_2)}_{\in I}.\end{aligned}$$

7. Dokaž 3. větu o izomorfismu: Je-li R okruh, $I<R$ ideál a $S\subset R$ podokruh, pak je $S+I$ podokruh v R a platí ${}^{(S+I)}\!/_I \simeq {}^{S}\!/_{(S\cap I)}$.

Řešení. Že $S+I$ je podokruh, se rutinně ověří (má jedničku, je uzavřený na sčítání i násobení). Dále směřujme k použití 1. věty o izomorfismu. Projekce $\pi\colon R\twoheadrightarrow R/I$, $r\mapsto r+I$ je surjektivní homomorfismus. Zužme ho na podokruh S a pojmenujme φ. Aby $\varphi(s)=s+I$ bylo 0, musí $s\in I$, takže $\operatorname{Ker}\varphi = S\cap I$. V obrazu se objeví přesně zbytkové třídy tvaru $s+I$, takže $\operatorname{Im}\varphi = {}^{(S+I)}\!/_I$ (jedna inkluze je zřejmá, pro tu druhou si uvědom, že cokoliv tvaru $s+i+I$ je jednoduše totéž jako $s+I$). 1. věta o izomorfismu pak dává výsledek.

8. 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.

Řešení. a) Hlavní ideály generované prvočísly.

b) Viz část a) v následujícím cvičení, vyjde $I + J = (24)$, $IJ = (48\,384)$, $I \cap J = (2016)$, $I^2 + J = (288)$.

c) Prvoideály obsahující (x) odpovídají prvočíslům dělícím x. Stačí tedy použít $168 = 2^3 \cdot 3 \cdot 7$, $288 = 2^5 \cdot 3^2$ a vždy vzít prvočísla z rozkladu.

9. 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.

Řešení. a) $(a)(b) = (ab)$, $(a) + (b) = (\mathrm{NSD}(a, b))$, $(a) \cap (b) = (\mathrm{nsn}(a, b))$.

b) Jsou to přesně hlavní ideály generované ireducibilními prvky/prvočiniteli (v OHI je ireducibilní = prvočinitel). V důsledku c) jsou prvoideály automaticky maximální.

c) Buď (p) prvoideál, pak je (p) ireducibilní. Chceme, aby libovolný nenulový prvek v $R/(p)$ měl inverz. Pro $a \notin (p)$ je ale $(a) + (p) = (\mathrm{NSD}(a, p)) = (1)$, takže $xa + yp = 1$ pro nějaká x, y. Pak ale $xy \equiv 1 \pmod{p}$.

10. Pro podmnožiny A, B okruhu R definujme $A \odot B := \{ab \mid a \in A, b \in B\}$ (pozor, toto neodpovídá násobení ideálů). Buď I ideál v R. Dokaž, že $(a + I) \odot (b + I) \subset ab + I$. Platí opačná inkluze?

Řešení. Dokazovaná inkluze je prostě to, že násobení prvků ve faktorokruhu modulo I funguje. Opačná inkluze neplatí: např. $2 \cdot 2 + 3\mathbb{Z}$ obsahuje jedničku, ale $(2 + 3\mathbb{Z}) \odot (2 + 3\mathbb{Z})$ nikoliv.

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.

Řešení. Faktorizujme polynomy:

$$x^3 + x^2 + 2x + 2 = (x + 1)(x^2 + 2), \qquad x^3 - 2x^2 + 2x - 4 = (x - 2)(x^2 + 2).$$

Snadno tedy v a) určíme potřebná NSD a nsn:

$$I + J = (x^2 + 2), \qquad IJ = \Big((x^3 + x^2 + 2x + 2) \cdot (x^3 - 2x^2 + 2x - 4)\Big),$$
$$I \cap J = \Big((x + 1)(x - 2)(x^2 + 2)\Big), \qquad I^2 + J^3 = \Big((x^2 + 2)^2\Big).$$

b) Faktor je obor, pokud modulíme prvoideálem, což zde odpovídá ireducibilnímu polynomu. Tedy pouze $I + J$, ostatní máme zapsány jako součiny více polynomů.

c) Opět vezmeme všechny hlavní ideály generované ireducibilními polynomy z rozkladu.

12. Buď R noetherovský okruh a $I < R$ ideál. Dokaž, že R/I je také noetherovský.

Řešení. Pro spor nebuď R/I noetherovský. Ideály v R/I jsou přesně tvaru J/I pro $J < R$, $J \supset I$, takže pro nenoetherovskost R/I musíme mít nekonečný rostoucí řetězec

$$J_1/I \subsetneq J_2/I \subsetneq J_3/I \subsetneq \cdots$$

Pak je ale i $J_1 \subsetneq J_2 \subsetneq J_3 \subsetneq \cdots$ nekonečný rostoucí řetězec ideálů v R – spor.

13. Je dán okruh R, v němž pro každé $x \in R$ existuje celé číslo $n \geq 2$ tak, že $x^n = x$. Dokaž, že každý prvoideál v R je maximální.

Řešení. Buď $P \leq R$ prvoideál a dívejme se na R/P. Chceme ukázat, že je to těleso, takže budiž $x + P \in R/P$ libovolné nenulové a najděme k němu inverz. Původní reprezentant $x \in R$ splňoval ze

zadání, že pro jisté $n \geq 2$ platí $x^n = x$. Toto zůstane v platnosti i v R/P a z předpokladu, že P je prvoideál, můžeme prvkem $x + P \neq 0 + P$ dělit, takže

$$(x+P)^n = x^n + P = x + P,$$
$$(x+P) \cdot (x+P)^{n-2} = 1 + P.$$

Každý nenulový prvek R/P tedy má inverz, tedy R/P je těleso, tedy P je maximální ideál.

6.2 Cvičení 2

Gaussovo lemma, Čínská zbytková věta, využití Zornova lemmatu

1. Buď R gaussovský obor a T jeho podílové těleso. Pro každý ireducibilní polynom $f \in T[x]$ existuje $u \in T\backslash\{0\}$ takové, že uf je ireducibilní prvek $R[x]$.

Řešení. Berme $u := \prod_p p^{-c_p(f)}$. Tento součin dává smysl, protože jen konečně mnoho prvočinitelů p může dát nenulový obsah polynomu, jelikož v každém jmenovateli každého koeficientu se účastní jen konečně mnoho prvočinitelů. Pak dostaneme $c_p(uf) = v_p(u) + c_p(f) = 0$ pro každé p, takže $uf \in R[x]$ je primitivní. Jelikož je zároveň ireducibilní v $T[x]$, je podle Gaussova lemmatu ireducibilní v $R[x]$.

2. Buď K těleso. Pak $K[x, y]$ i $K[x_1, x_2, \dots]$ (nekonečně mnoho proměnných) jsou gaussovské, ale $K[x, y]$ není obor hlavních ideálů (ale je noetherovský) a $K[x_1, x_2, \dots]$ není noetherovský ani obor hlavních ideálů.

Řešení. Z Gaussova lemmatu platí „R gaussovský $\implies$ $R[x]$ gaussovský“. Víme, že $K[x]$ je OHI, takže gaussovský, takže i $K[x, y] \simeq K[x][y]$ je gaussovský.

Podobně je gaussovský i každý $K[x_1, \dots, x_n]$. Toho využijeme pro $K[x_1, \dots]$, každý jeho prvek f používá jen konečně mnoho proměnných, takže sám leží v nějakém $K[x_1, \dots, x_n]$. To je gaussovské, takže tu máme jednoznačný rozklad. Navíc víme, že nemůže fungovat žádný rozklad, který by použil některou další proměnnou – měli bychom vůči ní už nutně kladný stupeň, kdežto f má vůči x_i, $i > n$ nulový stupeň. Jednoznačný rozklad f v $K[x_1, \dots, x_n]$ tak zůstává jednoznačný v $K[x_1, \dots]$.

$K[x, y]$ není OHI, protože (x, y), tj. ideál generovaný prvky x a y, nemůže být hlavní. Kdyby totiž $(x, y) = (f)$ pro nějaké $f \in K[x, y]$, muselo by být $f \mid x$, takže $\deg_y(f) \leq \deg_y(x) = 0$, tedy f je konstantní vzhledem k y. Zcela analogicky je ale f konstantní vůči x. Je to tedy konstanta $f \in K$, což je spor, protože v (x, y) žádné konstanty neleží (každý člen obsahuje x nebo y v kladné mocnině). Tím spíše už ani $K[x_1, x_2, \dots]$ nemůže být OHI.

Noetherovskost: Hilbertova věta o bázi říká „R noetherovský $\implies$ $R[x]$ noetherovský“. Těleso K je triviálně noetherovské (má jen dva ideály), tedy $K[x]$ je noetherovský, tedy $K[x, y] \simeq K[x][y]$ je noetherovský. Naopak $K[x_1, x_2, \dots]$ není noetherovský, protože máme řetězec ideálů

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots \subsetneq (x_1, \dots, x_n) \subsetneq \cdots$$

3. Popiš všechny ideály v okruhu $\mathbb{Z}/(150)$ a charakterizuj, které dvojice z nich jsou komaximální.

Řešení. Ideály v $\mathbb{Z}/(150)$ jsou tvaru $I/(150)$, kde I jsou ideály $(150) \subset I < \mathbb{Z}$. Protože $\mathbb{Z}$ je OHI, jsou tato I přesně tvaru (d) pro $d \mid 150 = 2 \cdot 3 \cdot 5^2$. Dva takové $I_1/(150)$, $I_2/(150)$ jsou komaximální, právě když jsou I_1, I_2 komaximální v $\mathbb{Z}$, což nastává tehdy, když jsou jejich generátory ($I_1 = (d_1)$, $I_2 = (d_2)$) nesoudělné – tedy např. $(2)/(150)$ a $(3)/(150)$ nebo $(6)/(150)$ a $(25)/(150)$.

4. Buď R okruh. Pomocí Zornova lemmatu dokaž, že každý vlastní ideál je obsažený v nějakém maximálním ideálu.

Řešení. Buď dán ideál $I \subsetneq R$. Uvažme

$$\mathcal{A} := \{\text{ideál } J \mid I \subset J \subsetneq R\}$$

uspořádané inkluzí. Zjevně $I \in \mathcal{A}$, takže tato částečně uspořádaná množina je neprázdná. Kdykoliv je $\mathcal{B} \subset \mathcal{A}$ řetězec, položme $\tilde{J} := \bigcup \mathcal{B}$. To je ideál (viz první cvičení) a zjevně obsahuje I. Kdyby nebyl vlastní, pak by obsahoval 1, takže by 1 musela ležet už v nějakém $J \in \mathcal{B}$, což nelze. Tedy $J \in \mathcal{A}$. Tím jsou ověřeny podmínky Zornova lemmatu, tedy máme v $\mathcal{A}$ nějaké maximální M.

Tvrdíme, že je to maximální ideál. Kdyby nebyl, pak existuje nějaký ideál I', že $M \subsetneq I' \subsetneq R$. Jenže potom by I' byl vlastní a obsahoval I, takže $I' \in \mathcal{A}$, což je spor s maximalitou M. Takže M je skutečně maximální ideál obsahující I.

5. Použij důkaz Čínské zbytkové věty (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?

Řešení. Jeden směr izomorfismu $\mathbb{Z}/(mn) \to \mathbb{Z}/(n) \times \mathbb{Z}/(m)$ je triviální:

$$z + (mn) \mapsto (z + (n),\ z + (m)).$$

Abychom našli opačný izomorfismus $(a+(n), b+(m)) \mapsto ???+(mn)$, potřebujeme $z_1+(mn) \in \mathbb{Z}/(mn)$ takové, že $z_1 \mapsto (1, 0)$, a obdobně nějaké $z_2 \mapsto (0, 1)$. K tomu se hodí Bézoutova věta, protože když $xn + ym = 1$, pak stačí vzít $z_1 = ym$ a $z_2 = xn$.

Spustíme tedy rozšířený Eukleidův algoritmus na $n = 16$ a $m = 35$:

	35	1	0
	16	0	1
2	3	1	−2
5	1	−5	11

Tudíž $11 \cdot 16 + (-5) \cdot 35 = 1$. Vezmeme tedy $z_1 = (-5) \cdot 35 = -175$, $z_2 = 11 \cdot 16 = 176$, což dává explicitní izomorfismus

$$\begin{aligned} \mathbb{Z}/(n) \times \mathbb{Z}/(m) &\to \mathbb{Z}/(mn), \\ (a + (n), b + (n)) &\mapsto -175a + 176b + (mn). \end{aligned}$$

(Bézoutovy koeficienty vůbec nejsou jednoznačné, takže jako celá čísla bychom zde mohli zvolit i jiná čísla, nicméně jejich zbytkové třídy mod (mn) by měly být stále stejné.)

6. Uvědom si, že v uspořádané množině $\mathcal{A}$ může existovat i nespočetný řetězec $\mathcal{B}$, na jehož indexování nestačí přirozená čísla. Najdi pár příkladů takové situace. (Není v tom žádný chyták, jen by si člověk neměl utvořit představu, že v Zornovi stačí vyřešit řetězce indexované přirozenými čísly.)

Řešení. Třeba reálná čísla s jakýmkoliv uspořádáním, nebo potenční množina $\mathbb{R}$ uspořádaná inkluzí, nebo cokoliv jinačího. Gurmáni si též mohou představit svůj oblíbený obludně veliký kardinál či ordinál.

7. Nahlédni, že je-li $\varphi : R \to S$ homomorfismus okruhů, pak vztahy $\psi(r) := \varphi(r)$ pro $r \in R$ a $\psi(x) := x$ splňuje právě jeden homomorfismus $\psi : R[x] \to S[x]$. Navíc je ψ injektivní/surjektivní, právě když φ je injektivní/surjektivní.

Řešení. Pro obecné $f = \sum_{i=0}^{d} r_i x^i \in R[x]$ položme prostě

$$\psi(f) = \sum_{i=0}^{d} \varphi(r_i) x^i.$$

Že ψ respektuje sčítání je přímočaré, násobení je o něco méně přímočaré, ale stále snadné (koeficienty součiny polynomů jsou nějaké výrazy obnášející násobení a sčítání, což homomorfismus φ obojí zachovává). Jelikož jen aplikujeme φ „po koeficientech“, zachování injektivity/surjektivity je taky jasné.

8. Ať je R okruh a $I_1, \dots, I_n$ po dvou komaximální ideály v R. Uvědom si, že z ČZV máme speciálně izomorfismus multiplikativních grup $(R/(I_1 \cdots I_n))^\times \simeq (R/I_1)^\times \times \cdots \times (R/I_n)^\times$. Jako aplikaci tohoto faktu si rozmysli, že pro lichá prvočísla $p \neq q$ nemůže být grupa $(\mathbb{Z}/(pq))^\times$ cyklická.

Řešení. Okruhová struktura už v sobě obsahuje strukturu multiplikativní grupy, takže jejich izomorfismus je jen zeslabením plné ČZV. Následně řád $(a, b) \in \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$ je nejmenším společným násobkem řádů a a b. Kvůli $\gcd(p-1, q-1) \geq 2$ pak řád nemůže dosáhnout $(p-1)(q-1)$.

9. Dokaž Zornovým lemmatem: ve vektorovém prostoru lze libovolnou lineárně nezávislou množinu rozšířit na bázi.

Řešení. Uvažuj lineárně nezávislé nadmnožiny dané množiny uspořádané inkluzí a použij Zornovo lemma. Maximální mezi nimi musí být i generující, jinak by nebyla maximální.

10. 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 $x, y \in M$.

Řešení. Částečné uspořádání je relace, tj. nějaká podmnožina $M \times M$, takže je samotné můžeme uspořádávat inkluzí. Mějme tedy

$$\mathcal{A} := \{\preceq \supset \leq \mid \preceq \text{ je částečné uspořádání množiny } M\}.$$

Podobně jako v předchozích ukázkách ověříme podmínky Zornova lemmatu; horní závorou řetězce je vždy jeho sjednocení. Pak máme v $\mathcal{A}$ nějaké maximální $\trianglelefteq$. Pro spor nechť není lineární, tedy nechť je v něm nějaká neporovnatelná dvojice x, y, tedy ani (x, y), ani (y, x) není prvek $\trianglelefteq$. Pak si můžeme vybrat, aby y bylo větší než x, a přidat tento vztah spolu se všemi okamžitými důsledky z tranzitivity. Formálně řečeno, vezmeme

$$\widetilde{\trianglelefteq} := \trianglelefteq \cup \{(a, b) \mid a, b \in M,\ a \trianglelefteq x,\ y \trianglelefteq b\}$$

a tvrdíme, že to je opět částečné uspořádání, což bude spor s maximalitou $\trianglelefteq$.

- Reflexivita: jasná, všechny dvojice (m, m) už v $\trianglelefteq$ byly.
- Antisymetrie: aby neplatila, muselo by už dříve v $\trianglelefteq$ ležet nějaké (b, a). Pak aby ale díky $y \trianglelefteq b \trianglelefteq a \trianglelefteq x$ musely být y a x porovnatelné, což je spor.
- Tranzitivita: aby neplatila, musíme mít nějaká $k, \ell, m \in M$ tak, že $k \mathrel{\widetilde{\trianglelefteq}} \ell$, $\ell \mathrel{\widetilde{\trianglelefteq}} m$, ale nikoliv $k \mathrel{\widetilde{\trianglelefteq}} m$. Pokud budeme používat jen porovnání, která už byla v $\trianglelefteq$, nic se nezměnilo, takže BÚNO uvažujme, že $(k, \ell) \in \widetilde{\trianglelefteq}$ je jedna z dvojic tvaru (a, b), co jsme přidali, tedy $k \trianglelefteq x$ a $y \trianglelefteq \ell$. Odkud pochází dvojice $(\ell, m) \in \widetilde{\trianglelefteq}$? Pokud už bylo $\ell \trianglelefteq m$, pak máme jednoduše $y \trianglelefteq \ell \trianglelefteq m$, takže $y \trianglelefteq m$, takže i (k, m) bude jedna z dvojic, které jsme přidali do $\widetilde{\trianglelefteq}$. Naopak pokud by měla (ℓ, m) být jedna z dvojic, co jsme přidali, znamená to $\ell \trianglelefteq x$ a $y \trianglelefteq m$. Ale už jsme měli i $y \trianglelefteq \ell$, takže dohromady $y \trianglelefteq \ell \trianglelefteq x$, což znamená, že x, y byly porovnatelné.

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 $R[x]$.

Řešení. Viz Tvrzení 1.16b ve skriptech.

12. * Buď F konečné těleso. Nahlédni, že libovolné zobrazení $f : F \to F$ lze zapsat polynomem.

Řešení. Polynomy $x - a$ pro $a \in F$ jsou vzájemně nesoudělné. Můžeme tedy použít Čínskou zbytkovou větu: když položíme kongruence $f \equiv F(a) \pmod{x-a}$, bude existovat polynom, který je všechny splňuje. Jenže $f \equiv f(a) \pmod{x-a}$, takže takový polynom se bude ve všech bodech shodovat s F.

13. * (Eisensteinovo kritérium) Mějme primitivní polynom $f = a_n x^n + \cdots + a_1 x + a_0$ s celočíselnými koeficienty a prvočíslo p. Dokaž, že pokud $p \nmid a_n$, $p \mid a_i$ pro $i = 0, 1, \dots, n-1$ a $p^2 \nmid a_0$, pak je f ireducibilní nad $\mathbb{Z}$. Zkus se zamyslet nad zobecněním pro obecný obor integrity R namísto $\mathbb{Z}$.

Řešení. Pro spor je f reducibilní, tedy $f = gh$. Pak musí g i h být primitivní, takže pro reducibilitu musí být nekonstantní. Vše zmodulíme p, obrazy našich polynomů (v $\mathbb{Z}_p[x]$) budeme značit vlnkou. Pak $\tilde{f} = \tilde{g}\tilde{h}$. Jenže ze zadání je $\tilde{f} = a_n x^n$. Víme, že $\mathbb{Z}_p[x]$ je eukleidovský, tedy i OHI, tedy i gaussovský, takže z jednoznačných rozkladů musí být $\tilde{g} = b_k x^k$, $\tilde{h} = c_\ell x^\ell$, kde $k+\ell = n$. Z nekonstantnosti dále $k, \ell \geq 1$. Pak ale p dělilo oba absolutní členy v g i h, takže a_0 musí být násobek p^2 – to je spor.

14. * 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.

Řešení. Standardně pomocí Zornova lemmatu zkonstruujeme ideál, který je maximální *mezi těmi ideály, jež nejsou konečně generované*, nazvěme ho P. Poté zbývá dokázat, že tento ideál je prvoideál. K tomu je potřeba postupovat sporem a využít toho, že každý větší ideál už musí být konečně generovaný. Zde je osnova důkazu postupující podle této (https://math.stackexchange.com/a/146899) odpovědi na stackexchangi – dorozmyšlení jednotlivých kroků je ponecháno čtenáři:

1) Když pro spor P nebude prvoideál, vezmi $x, y \in R$ takové, že $xy \in P$, ale $x, y \notin P$.
2) $P + (y)$ je nad P, takže už je konečně generovaný: $P + (y) = (p_1 + r_1 y, \ldots, p_n + r_n y)$.
3) $P_y := \{s \in R \mid sy \in P\}$ je ideál a leží nad P, takže opět $P_y = (s_1, \ldots, s_m)$.
4) Vezmi libovolné $p \in P$, vyjádři ho jako prvek $P + (y)$ pomocí generátorů.
5) Příslušnou lineární kombinaci $r_1, \ldots, r_n$ vyjádři jako prvek P_y pomocí generátorů.
6) $P = (p_1, \ldots, p_n, s_1, \ldots, s_m)$, spor.

6.3 Cvičení 3

kořenová a rozkladová nadtělesa, algebraický uzávěr, Galoisova grupa, separabilita

1. Buď α algebraický prvek nad tělesem T. Pak $[T(\alpha) : T] = \deg m_{\alpha,T}$.

Řešení. Buď $n := \deg m_{\alpha,T}$. Tvrdím, že $1, \alpha, \ldots, \alpha^{n-1}$ je báze $T(\alpha)$ jako vektorového prostoru nad T. Že je to generující množina: stačí nagenerovat libovolnou mocninu α^k. Pro $k \leq n-1$ to umíme triviálně. Minimální polynom říká, že

$$\alpha^n + (\text{nějaká lineární kombinace } 1, \ldots, \alpha^{n-1}) = 0,$$

takže $\alpha^n =$ nějaká lineární kombinace $1, \ldots, \alpha^{n-1}$, takže každou vyšší mocninu α dovedeme přepsat na lineární kombinaci menších – dostatečným opakování získáme lineární kombinace $1, \ldots, \alpha^{n-1}$. Že je to lineárně nezávislá množina: T-lineární kombinace $1, \ldots, \alpha^{n-1}$ je jen hodnota nějakého polynomu stupně $\leq n-1$ v α. Pokud je to netriviální kombinace (ne samé nuly), pak je to nenulový polynom, takže z minimality $m_{\alpha,T}$ nemůže mít α jako kořen.

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

Řešení.

a) Kořeny $x^2 + 3$ jsou $\pm\sqrt{-3}$. Máme $\mathbb{R}(\sqrt{-3}) = \mathbb{R}(-\sqrt{-3}) = \mathbb{C}$, takže $\mathbb{C}$ je kořenové nadtěleso a rovnou i rozkladové nadtěleso. $x^2 + 3$ je kvadratický a nemá v $\mathbb{R}$ kořen, takže je ireducibilní. $\mathbb{C} \supset \mathbb{R}$ pak jako kořenové nadtěleso kvadratického ireducibilního polynomu má stupeň 2.
$\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ je dvouprvková: jedním automorfismem je identita, druhým komplexní sdružení $z \mapsto \overline{z}$. Že se jedná o automorfismy: u id je to triviální, u komplexního sdružení víme např. z algebry, že respektuje sčítání i násobení, reálná čísla fixuje a navíc je to bijekce, tedy skutečně je to $\mathbb{R}$-automorfismus tělesa $\mathbb{C}$. Že další automorfismy neexistují: víme, že v rozšíření stupně 2 se musí Galoisova grupa injektivně vnořovat do S_2. To je ale dvouprvková grupa, takže víc než dva prvky v $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ mít nemůžeme.

b) f má kořeny ± 1, což jsou oba prvky $\mathbb{Q}$. Kořenovým i rozkladovým nadtělesem je tak pouze $\mathbb{Q}$ samo, stupeň rozšíření je 1 a Galoisova grupa je triviální.

c) Tato část už je těžší a snáze se bude řešit s pokročilejšími nástroji z přednášky. Tedy bez důkazu: rozkladová nadtělesa jsou tři – $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{2})$, $\mathbb{Q}(e^{\frac{-2\pi i}{3}}\sqrt[3]{2})$. Každé je stupně 3 (kořenová rozšíření ireducibilního polynomu stupně 3), ale Galoisovy grupy mají triviální. Rozkladové nadtěleso je $\mathbb{Q}(e^{\frac{2\pi i}{3}}, \sqrt[3]{2})$ a má stupeň šest. Jeho Galoisova grupa je šestiprvková a izomorfní S_3. Lze ji nagenerovat dvěma prvky, z nichž jeden fixuje $\sqrt[3]{2}$ a komplexně sdružuje $e^{\frac{2\pi i}{3}}$ na $e^{\frac{-2\pi i}{3}}$, zatímco druhý fixuje $e^{\frac{2\pi i}{3}}$ a rotuje $\sqrt[3]{2}$ na $e^{\frac{2\pi i}{3}}\sqrt[3]{2}$.

3. 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.

Řešení. Nejprve baby verze, když se zároveň jedná o konečná rozšíření (konečné rozšíření je nutně algebraické – viz **5.**). Pak prostě můžeme říci, že

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

je konečné, tedy $V \supset T$ je algebraické.

Nyní dospělá verze s potenciálně nekonečnými rozšířeními. Berme $\alpha \in V$ a ukažme, že je algebraické nad T. Víme, že je algebraické nad U, takže je kořenem nějakého

$$f = u_n x^n + \cdots + u_1 x + u_0 \in U[x].$$

Zjevně je potom tedy α také algebraické nad $T(u_n, \ldots, u_1, u_0)$. Pak je $T(\alpha, u_n, \ldots, u_0)$ algebraické nad $T(u_n, \ldots, u_0)$, což je algebraické nad T (bo je to podtěleso U). Toto jsou už ale určitě konečná rozšíření, takže z baby verze je $T(\alpha, u_n, \ldots, u_0)$ algebraické rozšíření T, takže α je algebraické nad T.

4. Buď $U \supset T$ rozšíření těles a $\alpha \in U$ kořen *nějakého* separabilního $f \in T[x]$. Potom už je α separabilní nad T.

Řešení. $m_{\alpha,T} \mid f$. Nyní kdyby $m_{\alpha,T}$ měl v $\overline{T}$ násobný kořen, měl by ho dělitelností i f, spor.

5. Rozšíření těles konečného stupně je nutně algebraické.

Řešení. Buď $[U : T] < \infty$. Pak ale pro každé $a \in U$ máme $T(a) \subset U$, takže

$$[T(a) : T] \leq [U : T] < \infty,$$

což znamená, že a je algebraické nad T.

6. Mějme rozšíření těles $V \supset U \supset T$. Pak $[V : T] = [V : U] \cdot [U : T]$.

Řešení. Buď $n := [U : T]$, $m := [V : U]$. Dále zvolme $\{u_i\}_{i=1}^n$ bázi U jako vektorového prostoru nad T a $\{v_j\}_{j=1}^m$ bázi V jako vektorového prostoru nad U. Tvrdím, že $\{u_i v_j\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}}$ je báze V jako vektorového prostoru nad T. Že je generující: libovolné $v \in V$ nejdřív vyjádříme jako

$$v = \sum_{j=1}^{m} \alpha_j \cdot v_j,$$

kde α_j jsou koeficienty náležící U. Každý z nich proto můžeme vyjádřit jako

$$\alpha_j = \sum_{i=1}^{n} \beta_{i,j} u_i,$$

takže následně máme

$$v = \sum_{i=1}^{n}\sum_{j=1}^{m} \beta_{i,j} \cdot u_i v_j.$$

Že je nezávislá: nechť je

$$0 = \sum_{i=1}^{n}\sum_{j=1}^{m} \beta_{i,j} \cdot u_i v_j$$

a ukažme, že všechna $\beta_{i,j}$ musí být nulová. V sumě můžeme posbírat $\alpha_j := \sum_{i=1}^{n} \beta_{i,j} u_i \in U$, pak máme $0 = \sum_{j=1}^{m} \alpha_j v_j$, což z lineární nezávislosti báze $\{v_j\}$ značí $\alpha_1 = \cdots = \alpha_m = 0$. Obdobně pro každé $j = 1, \ldots, m$ značí $0 = \sum_{i=1}^{n} \beta_{i,j} u_i$ díky lineární nezávislosti $\{u_i\}$, že všechna $\beta_{i,j}$ jsou nulová.

7. 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.

Řešení. Být algebraickým uzávěrem tělesa znamená být jeho algebraickým rozšířením a zároveň být algebraicky uzavřené. Algebraická uzavřenost je jen vlastnost tělesa K, která nezávisí na tom, nad kterým menším tělesem se na něj díváme. V důsledku **3.** je dále $K \supset T$ algebraické, právě když je $K \supset U$ algebraické.

8. Buď $\varphi : K \to R$ homomorfismus okruhů. Připomeň si, že když K je těleso, musí φ být prosté.

Řešení. $\operatorname{Ker}\varphi$ je ideál v K, jenže tělesa mají jen dva ideály (nulový ideál a celé těleso). Přitom z definice okruhového homomorfismu je $\varphi(1_K) = 1_R$, takže $1 \notin \operatorname{Ker}\varphi$, tedy $\operatorname{Ker}\varphi = 0$.

9. 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) $f(x) = x^2 + 1,\ T = \mathbb{Z}_7$,
**d) $f(x) = x^n - 1,\ T = \mathbb{Q},\ n \in \mathbb{N}$.

Řešení. a) kořenové = rozkladové = $\mathbb{Q}(i)$, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, $\operatorname{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{\mathrm{id}, (z \mapsto \overline{z})\} \simeq \mathbb{Z}_2$.

b) Kořenové může být $\mathbb{Q}(1) = \mathbb{Q}(-1) = \mathbb{Q}$ (stupeň rozšíření 1, Galoisova grupa triviální), nebo $\mathbb{Q}(i) = \mathbb{Q}(-i)$, což už jsme viděli. Rozkladové je $\mathbb{Q}(i)$.

c) Kořenové i rozkladové je $\mathbb{Z}_7(i)$. Co to znamená? Prostě k $\mathbb{Z}_7$, kde polynom $x^2 + 1$ neměl kořen, přidáme prvek i, kterému přisoudíme vlastnost $i^2 = -1$. Výsledkem je těleso se $7^2 = 49$ prvky. Stupeň rozšíření je 2, Galoisova grupa dvouprvkové (identita a „komplexní sdružení“ $a + bi \mapsto a - bi$ pro $a, b \in \mathbb{Z}_7$).

d) Označme $\zeta_n := e^{\frac{2\pi i}{n}}$. Pak jsou kořenovými nadtělesy všechna $\mathbb{Q}(\zeta_n^j)$. To je vše obsaženo v $\mathbb{Q}(\zeta_n)$, což je tedy rozkladové nadtěleso. (Pro j soudělná s n bude $\mathbb{Q}(\zeta_n^j)$ různé od $\mathbb{Q}(\zeta_n)$, takže pro „hodně složená“ n můžeme dostat spoustu vzájemně neizomorfních kořenových rozšíření.

Určit stupně ve vší obecnosti je těžké: platí (těžká) věta říkající, že minimální polynom ζ_n (tzv. n-tý cyklotomický polynom) má stupeň $\varphi(n)$, z čehož plyne $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Dokonce potom platí $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

10. Buďte $S \supset T$ tělesa, S algebraicky uzavřené a $U = \{\alpha \in S \mid \alpha \text{ algebraické nad } T\}$. Pak je U algebraický uzávěr T. (tvrzení 2.7 ze skript)

Řešení. Důkaz je ve skriptech...

11. Buďte T, U tělesa charakteristiky 0. Pak $\mathbb{Q} \subset T, U$ a každý homomorfismus $\varphi : T \to U$ je $\mathbb{Q}$-homomorfismem. (V charakteristice p má stejnou vlastnost těleso $\mathbb{Z}_p$.)

Řešení. Z definice homomorfismu musí být $\varphi(1) = 1$. Pak dostaneme snadno taky $\varphi(2) = \varphi(1+1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$, takto indukcí získáme $\varphi(n) = n$ pro všechna přirozená n. Posléze víme

$0 = \varphi(0) = \varphi(n + (-n)) = \varphi(n) + \varphi(-n) = n + \varphi(-n)$, takže nutně $\varphi(-n) = -n$. Tudíž máme $\varphi(n) = n$ pro každé celé číslo n. Pak pro $\frac{p}{q} \in \mathbb{Q}$ podobně získáme

$$p = \varphi(p) = \varphi\left(q \cdot \frac{p}{q}\right) = \varphi(q) \cdot \varphi\left(\frac{p}{q}\right) = q \cdot \varphi\left(\frac{p}{q}\right),$$

takže $\varphi\left(\frac{p}{q}\right) = \frac{p}{q}$. Tedy skutečně φ fixuje všechna racionální čísla.

12. Prvek α je algebraický nad tělesem T, právě když $T(\alpha) = T[\alpha]$.

Řešení. Buď $\beta \in T[\alpha]$ nenulové. Pak má minimální polynom $m_{\beta,T}$ nenulový absolutní člen (jinak by $x \mid m_{\beta,T}$), takže

$$m_{\beta,T}(x) = \sum_{i=0}^{n} b_i x^i,$$

kde $b_0 \neq 0$. Potom ale můžeme upravit $\frac{1}{\beta} = -\sum_{i=1}^{n} b_i \beta^{i-1}$. Podobně naopak z vyjádření inverzu získáme zpátky minimální polynom.

13. * Žádné konečné těleso není algebraicky uzavřené.

Řešení. Mějme konečně těleso F a nechť $n := |F|$. Jeho multiplikativní grupa je $(n-1)$-prvková, z Lagrangeovy věty tak $a^{n-1} = 1$ pro $a \in F \setminus \{0\}$. Z toho už domyslíme, že $a^n = a$ pro každé $a \in F$. Takže polynom $x^n - x$ má za kořen každý prvek F, což ale znamená, že polynom $x^n - x + 1$ nemá v F žádné kořeny – F tak nemůže být algebraicky uzavřené.

14. * Buď p prvočíslo, $T = \mathbb{Z}_p(y)$ a $U = T(\sqrt[p]{y})$. Urči $[U : T]$, $[U : T]_s$ a $\mathrm{Gal}(U/T)$.

Řešení. $\sqrt[p]{y}$ je kořenem $x^p - y$, což je ireducibilní použitím Eisensteinova kritéria nad OHI $\mathbb{Z}_p[y]$ (s výpomocí Gaussova lemmatu se získá i ireducibilita nad $\mathbb{Z}_p(y)$), takže už se jedná o minimální polynom. Rovnou tedy máme $[U : T] = p$. Přitom ale $x^p - y = (x - \sqrt[p]{y})^p$ (v charakteristice p je umocňování na p homomorfismus), takže tento minimální polynom má je jeden unikátní kořen. Jakýkoliv T-homomorfismus $U \to \overline{T}$ tedy musí $\sqrt[p]{y}$ poslat znovu na $\sqrt[p]{y}$, což značí, že jediným takovým T-homomorfismem je identita. Tedy $[U : T]_s = 1$. Vzhledem k $[U : T]_s \geq \#\,\mathrm{Gal}(U/T)$ pak musí Galoisova grupa být triviální.

15. * Algebraický uzávěr nekonečného tělesa T má stejnou mohutnost jako T.

6.4 Cvičení 4

rozšíření separabilní, normální, jednoduchá a Galoisova

1. Buď $U \supset T$ rozšíření konečného stupně. Dokaž, že je Galoisovo, právě když $[U : T] = \#\,\mathrm{Gal}(U/T)$.

Řešení. Položme sérii nerovností:

$$[U : T] \overset{(1)}{\geq} [U : T]_s = \#\left\{T\text{-homomorfismy } U \to \overline{T}\right\} \overset{(2)}{\geq}$$
$$\overset{(2)}{\geq} \#\left\{T\text{-homomorfismy } U \to U\right\} \overset{2.25}{=} \#\left\{T\text{-automorfismy } U \to U\right\} =$$
$$= \#\,\mathrm{Gal}(U/T).$$

Jednu z pozdějších rovností obstarává Lemma 2.25 ze skript (můžeme použít, protože konečný stupeň implikuje algebraičnost). V (1) nastává rovnost, právě když je $U \supset T$ separabilní, zatímco v (2) nastává rovnost, právě když je $U \supset T$ normální. Vzhledem k tomu, že už máme dán konečný stupeň

rozšíření, Galoisovskost nastane právě tehdy, když je rozšíření i separabilní a normální, tedy právě když nastanou rovnosti v (1) a (2), tedy právě když $[U : T] = \#\operatorname{Gal}(U/T)$.

2. (zachovávání a skládání význačných vlastností) Buďte $V \supset U \supset T$ rozšíření těles. Víš-li, že rozšíření $V \supset T$ má vlastnost X, rozhodni, zda nutně musí i $V \supset U$ či $U \supset T$ mít vlastnost X. Víš-li, že obě $V \supset U$, $U \supset T$ mají vlastnost X, rozhodni, zda ji nutně musí mít i $V \supset T$.

a) $X =$ konečného stupně,
b) $X =$ algebraické,
c) $X =$ separabilní,
d) $X =$ normální,
e) $X =$ Galoisovo.

Řešení.

a) Obě dílčí rozšíření musí být konečného stupně, naopak pokud obě jsou, pak je i $V \supset T$ konečného stupně.
b) Stejně tak jsou obě dílčí rozšíření algebraická a jejich algebraičnost už implikuje algebraičnost $V \supset T$ (viz minulé cvičení).
c) Obě dílčí rozšíření musí být separabilní: $\alpha \in V$ je kořenem separabilního $f \in T[x]$, což je i $\in U[x]$; zato $\beta \in U$ je separabilní nad T čistě z $\beta \in V$. V opačném směru: pro $[V : T] < \infty$ to snadno plyne pomocí stupňů separability. V obecném případě, je-li $\gamma \in V$, pak je separabilní nad U, tedy kořenem jistého $f = a_n x^n + \cdots + a_1 x + a_0 \in U[x]$, takže separabilní nad $T(a_0, \ldots, a_n)$. Víme, že $T(a_0, \ldots, a_n) \supset T$ i $T(\gamma, a_0, \ldots, a_n) \supset T(a_0, \ldots, a_n)$ jsou separabilní a konečných stupňů, takže už je γ separabilní nad T.
d) $V \supset U$ musí být normální (U-homomorfismus je speciálně i T-homomorfismus), $U \supset T$ ne nutně (např. $\mathbb{Q}(\omega, \sqrt[3]{2}) \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$). Podobně $\mathbb{Q}(\sqrt[4]{2}) \supset \mathbb{Q}(\sqrt{2}) \supset \mathbb{Q}$ ukazuje, že $V \supset T$ nemusí být normální, i když $V \supset U$ i $U \supset T$ jsou.
e) Jen poskládáme odpovědi z konečného stupně, separability a normálnosti. $V \supset U$ musí být Galoisovo, $U \supset T$ ne nutně, obrácená implikace taky neplatí (stejné protipříklady jako u normality).

3. Rozhodni o následujících rozšířeních, které z význačných vlastností z úlohy **2.** mají a které ne:
a) $\mathbb{C} \supset \mathbb{R}$, b) $\mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$, *c) $\mathbb{Z}_p(x) \supset \mathbb{Z}_p$, *d) $\overline{\mathbb{Q}} \supset \mathbb{Q}$.

Řešení.

a) $[\mathbb{C} : \mathbb{R}] = 2$, tedy je to rozšíření konečného stupně, speciálně tak i algebraické. Separabilitu máme zdarma díky charakteristice 0 a normální je třeba díky tomu, že $\mathbb{C}$ je rozkladové nadtěleso polynomu $x^2 + 1$ nad $\mathbb{R}$. Posléze jde i o Galoisovo rozšíření.
b) Stupeň je $3 < \infty$, tedy jde určitě o algebraické rozšíření. Separabilita je zdarma díky charakteristice, avšak rozšíření není normální – polynom $x^3 - 2$ má v rozšíření jeden kořen, ale zbylé dva ne. Posléze tedy rozšíření nemůže být ani Galoisovo.
c) Jako vektorový prostor nad $\mathbb{Z}_p$ má už $\mathbb{Z}_p[x]$ nekonečnou dimenzi, což se může jedině zvětšit přechodem k podílovému tělesu $\mathbb{Z}_p(x)$. Nejedná se tedy o rozšíření konečného stupně. Dále prvek $x \in \mathbb{Z}_p(x)$ není kořenem žádného nenulového polynomu ze $\mathbb{Z}_p[y]$, takže se nejedná o algebraické rozšíření. V důsledku toho ani nemá smysl mluvit o separabilitě nebo normálnosti, tedy ani o Galoisovskosti.
d) Algebraický uzávěr v sobě obsahuje všechna algebraická rozšíření, a ty umíme určitě konstruovat libovolně velká, musí tedy být $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. (Lze si ale rozmyslet, že dimenze $\overline{\mathbb{Q}}$ jako vektorového prostoru nad $\mathbb{Q}$ je jen spočetná, protože samo $\overline{\mathbb{Q}}$ má jen spočetně mnoho prvků.) Přímo z definice algebraického uzávěru musí jít o algebraické rozšíření. Potom je zadarmo i separabilní, protože charakteristika 0. Normálnosti bude taky platit triviálně: když rozbalíme definici normálnosti, pak v tomhle případě to znamená, zdali každý $\mathbb{Q}$-homomorfismus (T-homomorfismus) $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ (zde myšleno $U \to \overline{T}$) je ve skutečnosti $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ (zde myšleno $U \to U$),

což platí naprosto tautologicky. Rozšíření tedy je normální, ale nebude Galoisovo, protože nemá konečný stupeň.

4. Buď $V \supset T$ Galoisovo rozšíření a $V \supset U \supset T$. Dokaž, že $[U : T] = \frac{\#\operatorname{Gal}(V/T)}{\#\operatorname{Gal}(V/U)}$.

Řešení. Podle **2.**d) je i $V \supset U$ Galoisovo rozšíření, takže z **1.** dostaneme

$$\frac{\#\operatorname{Gal}(V/T)}{\#\operatorname{Gal}(V/U)} = \frac{[V : T]}{[V : U]} = [U : T].$$

5. Buď $f \in T[x]$ polynom s rozkladem na navzájem neasociované ireducibilní polynomy $f = f_1 \cdots f_k$. Uvažujme Galoisovu grupu rozkladového nadtělesa f nad T jako grupu permutací na množině kořenů f. Nahlédni, že každá z těchto permutací musí mít alespoň k cyklů.

Řešení. Jelikož jsou jednotlivá f_i navzájem neasociovaná, jejich množiny kořenů A_i jsou navzájem disjunktní (když totiž $\alpha \in A_i \cap A_j$, už to znamená $m_{\alpha,T} \mid f_i, f_j$). Přitom ale víme, že každý T-automorfismus permutuje kořeny stejného ireducibilního polynomu z $T[x]$ jen mezi sebou. Takže každý prvek Gal bude permutovat každé A_i jen uvnitř A_i. V každé A_i se přitom musí vyskytnout alespoň jeden cyklus (je to neprázdná množina), takže celkem půjde o $\geq k$ permutací.

6. (opakování z přednášky) Buď U těleso, $G < \operatorname{Aut}(U)$ podgrupa a $T \subset U$ podtěleso. Potom platí $\operatorname{Gal}(U/\operatorname{Fix}(U, G)) \supset G$ a $\operatorname{Fix}(U, \operatorname{Gal}(U/T)) \supset T$.

Řešení. Po rozbalení definic zjevné: např. $\operatorname{Fix}(U, \operatorname{Gal}(U/T))$ je množina těch prvků $u \in U$, že $\varphi(u) = u$ pro každé $\varphi \in \operatorname{Gal}(U/T)$. Ale prvky Galoisovy grupy nechávají prvky T na místě, tedy $\varphi(t) = t$ pro každé $t \in T$, což už implikuje $T \subset \operatorname{Fix}(U, \operatorname{Gal}(U/T))$.

7. Budiž $U \supset T$ separabilní rozšíření konečného stupně. Nahlédni, že existuje těleso V takové, že $U \subset V$, $[V : T] \leq ([U : T])!$ a rozšíření $V \supset T$ je Galoisovo.

Řešení. Z přednášky je separibilní rozšíření konečného stupně jednoduché, mějme tedy $U = T(\alpha)$. To je kořenové nadtěleso polynomu $m_{\alpha,T}$ nad T, uvažujme tedy také jeho rozkladové nadtěleso, které označíme V. To je určitě nadtěleso U a je normální. Nechť $n = [U : T] = \deg m_{\alpha,T}$. Víme, že $m_{\alpha,T}$ je separabilní, protože α je separabilní nad T, takže $m_{\alpha,T}$ má n různých kořenů $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$. Všechny tyto prvky jsou separabilní nad T, protože mají tentýž (separabilní) polynom. Tedy $V = T(\alpha_1, \ldots, \alpha_n)$ vzniká přidáním několika separabilních prvků, je to tedy separabilní rozšíření T. Dohromady tak už je i konečného stupně (přidali jsme konečně mnoho algebraických prvků), a tedy Galoisovo.

Konečně odhadněme $[V : T]$. To je totéž, co $\#\operatorname{Gal}(V/T)$, ale tato grupa se vnořuje do grupy permutací na množině $\{\alpha_1, \ldots, \alpha_n\}$, kterážto má řád $n!$. Dokonce tedy můžeme říct

$$[V : T] \mid ([U : T])!.$$

8. Podle lemmatu 2.25, je-li $U \supset T$ algebraické rozšíření, pak už musí každý T-homomorfismus $\varphi : U \to U$ být dokonce T-automorfismus. Rozmysli si, že algebraičnost je nutná – pro $T = \mathbb{Z}_p$, $U = T(x)$ (těleso racionálních funkcí) najdi T-homomorfismus $\varphi : U \to U$, který není T-automorfismus.

Řešení. Generický prvek U je tvaru $\frac{f}{g}$, $f, g \in T[x]$, $g \neq 0$. Zaveďme homomorfismus

$$\begin{aligned} \varphi : U &\to U, \\ \frac{f}{g} &\mapsto \frac{f(x^2)}{g(x^2)}, \end{aligned}$$

tedy „místo x píšeme x^2“. Snadno se nahlédne, že toto nezávisí na konkrétním zapsání zlomku $\frac{f}{g}$ a jedná se o homomorfismus (dosazování zachovává operace). Přitom ale evidentně není surjektivní:

$x \in U$ nikdy nezapíšeme jako podíl dvou polynomů obsahujících jen sudé mocniny x: v rovnici $f(x^2) = x \cdot g(x^2)$ má levá strana sudý stupeň, zatímco pravá lichý stupeň.

9. Buď T těleso s $\operatorname{char} T \neq 2$ a $a, b \in T$ prvky s $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin T$. Pak $[T(\sqrt{a}, \sqrt{b}) : T] = 4$.
* Můžeš zkusit dokázat $\operatorname{Gal}(T(\sqrt{a}, \sqrt{b})/T) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Řešení. Uvažujme $T \subset T(\sqrt{a}) \subset T(\sqrt{a}, \sqrt{b})$. Pokaždé rozšiřujeme o odmocninu něčeho, co leží v předchozím tělese, takže každý ze stupňů dvou dílčích rozšíření je buď 2, nebo 1. Abychom ukázali, že oba jsou 2, stačí nahlédnout $\sqrt{a} \notin T$ a $\sqrt{b} \notin T(\sqrt{a})$. První neležení máme hned ze zadání, pro to druhé pro spor předpokládejme, že $\sqrt{b} = u + v\sqrt{a}$ pro nějaká $u, v \in T$. Úpravami pak máme

$$\begin{aligned} \sqrt{b} - v\sqrt{a} &= u, \\ b - 2v\sqrt{ab} + v^2 a &= u^2, \\ 2v\sqrt{ab} &= u^2 - v^2 a - b. \end{aligned}$$

Rozlišme dva případy: pokud $v = 0$, pak jsme vyjádřením $\sqrt{b} = u$ ve skutečnosti měli $\sqrt{b} \in T$, což je spor. V opačném případě $v \neq 0$ a vzhledem k zadané charakteristice $\neq 2$ máme i $2 \neq 0$, takže získáme

$$\sqrt{ab} = \frac{u^2 - v^2 a - b}{2v} \in T,$$

což je opět spor.

Dohromady tak muselo být $\sqrt{b} \notin T(\sqrt{a})$, což už implikuje $[T(\sqrt{a}, \sqrt{b}) : T(\sqrt{a})] = 2$. Tedy $[T(\sqrt{a}, \sqrt{b}) : T] = 2 \cdot 2 = 4$.

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. * (existence separabilního uzávěru) Buď $U \supset T$ rozšíření těles. Všechny prvky $\alpha \in U$, jež jsou separabilní nad T, tvoří podtěleso U.

Řešení. Položme $V := \{\alpha \in U \mid \alpha \text{ je separabilní nad } T\}$. Chceme jen ukázat, že tahle množina je uzavřená na tělesové operace. Mějme tedy nějaká $\alpha, \beta \in V$. To jsou separabilní prvky nad T, z přednášky tedy víme, že $T(\alpha, \beta) \supset T$ bude separabilní rozšíření. Přitom ale všechny možné operace (součty, součiny, inverzy, ...), co můžeme s α, β vyrobit, budou ležet v $T(\alpha, \beta)$, takže taky budou separabilní, takže budou opět ležet ve V, což jsme chtěli.

12. * Buď p prvočíslo, $U = \mathbb{Z}_p(x, y)$, $T = \mathbb{Z}_p(x^p, y^p)$. Dokaž, že rozšíření $U \supset T$ není jednoduché.

Řešení. Nechť pro spor $U = T(f/g)$, kde $f, g \in \mathbb{Z}_p[x, y]$, $g \neq 0$. Zapišme

$$f = \sum_{i,j \geq 0} c_{ij} x^i y^j,$$

kde koeficienty c_{ij} jsou ze $\mathbb{Z}_p$. V charakteristice p je umocňování na p homomorfismus, takže

$$f^p = \sum_{i,j \geq 0} c_{ij}^p (x^p)^i (y^p)^j \in \mathbb{Z}_p[x^p, y^p].$$

Obdobně $g^p \in \mathbb{Z}_p[x^p, y^p]$, takže $(f/g)^p \in T$. To značí, že $[U : T] \leq p$.

Ukážeme, že stupeň rozšíření je ve skutečnosti větší. Platí, že x má v $T[z]$ minimální polynom $z^p - x^p$ (notačně to může být trochu matoucí, ale je to jen aplikace Eisenstein a Gaussova lemmatu, kterou jsme už několikrát viděli – protože x^p, ač z hlediska notace vypadá rozložitelně, je v $\mathbb{Z}_p[x^p, y^p]$ prvočinitel). Podobně bude mít y nad $T(x)$ minimální polynom $z^p - y^p$, takže dostaneme

$$[U : T] = [T(x, y) : T] = [T(x, y) : T(x)] \cdot [T(x) : T] = p^2,$$

což je spor s $[U : T] \leq p$.

6.5 Cvičení 5

počítání Galoisových grup, Galoisova korespondence

1. Urči, zda je Galoisovu grupu $T \supset \mathbb{Q}$ a všechna tělesa U, $T \supset U \supset \mathbb{Q}$, jestliže

a) $T = \mathbb{Q}(i, \sqrt{2})$,

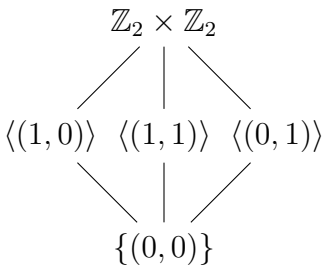
b) $T =$ rozkladové nadtěleso $x^3 - 2$ nad $\mathbb{Q}$.

Řešení. a) Zjevně máme $[T : \mathbb{Q}] = [T : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$, navíc jde o rozkladové nadtěleso polynomu $(x^2 - 2)(x^2 + 1)$, tedy je normální, separabilní (charakteristika 0) a konečného stupně, tedy Galoisovo. Hned tedy víme, že $\#\operatorname{Gal}(T/\mathbb{Q}) = 4$. Zároveň jakýkoliv $\mathbb{Q}$-automorfismus $\varphi \in \operatorname{Gal}(T/\mathbb{Q})$ má dvě možnosti kam poslat $\sqrt{2}$ a dvě kam poslat i. Mají-li skutečně vzniknout 4 automorfismy, musí každá kombinace těchto dvou možností dát validní automorfismus, tedy máme čtyři automorfismy tvaru

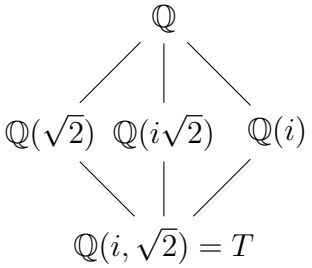
$$\begin{aligned} \sigma_{a,b} : T &\to T, \\ i &\mapsto (-1)^a i, \\ \sqrt{2} &\mapsto (-1)^b \sqrt{2} \end{aligned}$$

pro $a, b \in \mathbb{Z}_2$. Snadno nahlédneme, že skládání bude odpovídat sčítání dvojic (a, b) v grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$, tedy $\operatorname{Gal}(T/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

K určení podtěles prozkoumejme podgrupy $\mathbb{Z}_2 \times \mathbb{Z}_2$. Zjevně kromě triviálních $\mathbb{Z}_2 \times \mathbb{Z}_2$ a $\{(0,0)\}$ můžeme mít jen dvouprvkové podgrupy, přitom ale vše kromě $(0,0)$ má řád 2, takže každý ze tří nenulových prvků generuje dvouprvkovou podgrupu. Tedy:

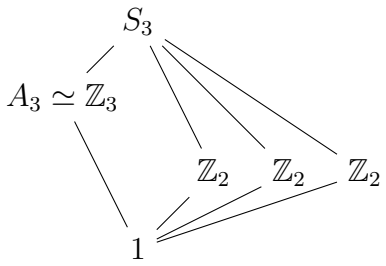


Aplikujeme nyní Galoisovu korespondenci, pokud zachováme orientaci diagramu, pak u vzniklých Fixů budeme kreslit větší tělesa níže. U triviálních podgrup víme okamžitě, že příslušný Fix musí být $\mathbb{Q}$ resp. T, zatímco u dvouprvkových podgrup snadno Fix určíme, neboť se fixování identitou je triviální, takže zbývá vždy jen jedna podmínka, např. $\operatorname{Fix}(T, \langle\sigma_{1,0}\rangle) = \operatorname{Fix}(T, i \mapsto -i) = \mathbb{Q}(\sqrt{2})$, protože $\sqrt{2}$ je fixovaná a už generuje rozšíření stupně 2, což víme, že má vyjít. Podobně dostaneme i zbylé Fixy:

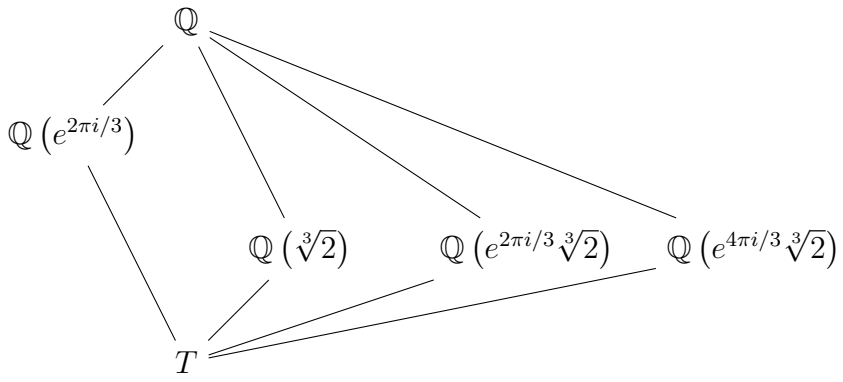


b) Na předchozích cvičeních jsme už viděli, že $T = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ a že $[T : \mathbb{Q}] = 6$. Jedná se o Galoisovo rozšíření, přitom se ale šestiprvková $\operatorname{Gal}(T/\mathbb{Q})$ má vnořovat do S_3 (permutace tří kořenů $x^3 - 2$), takže už musí být $\operatorname{Gal}(T/\mathbb{Q}) \simeq S_3$.

S_3 má následující strukturu podgrup: jedinou podgrupou řádu 3 je grupa generovaná kterýmkoliv ze dvou trojcyklů, což je shodou okolností taky alternující grupa A_3. Řádu 2 jsou jen podgrupy generované každou ze tří transpozic, tyto jsou samozřejmě izomorfní $\mathbb{Z}_3$. Schématicky tedy můžeme kreslit:



Jak nyní určit Fixy? Dvouprvkové grupy jsou generované transpozicemi dvou kořenů a mají odpovídat kubickému rozšíření – do toho ale přesně sedí těleso generované třetím kořenem, který transpozice nechává na místě. Naproti tomu Fix od A_3 má být kvadratické rozšíření $\mathbb{Q}$, a vzhledem k tomu, že víme, že má být jen jedno, stačí si všimnout podtělesa $\mathbb{Q}\left(e^{2\pi i/3}\right)$. Tedy:



2. Pro rozšíření těles $U \supset T$ urči $[U : T]$ spolu s bází U jako vektorového prostoru nad T, rozhodni, zda jde o Galoisovo rozšíření, a pokud ano, urči také všechna tělesa V, $U \supset V \supset T$, jestliže

a) $U = \mathbb{Q}(\sqrt{2}, e^{2\pi i/3})$, $T = \mathbb{Q}$,
b) $U = \mathbb{Q}(\sqrt[3]{3})$, $T = \mathbb{Q}$,
c) $U = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $T = \mathbb{Q}$,
d) $U = \mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)$, $T = \mathbb{Q}$.

Řešení. Uvádím jen Galoisovy grupy a mezitělesa, pokud nejsou příliš komplikovaná.

a) Trikově si lze povšimnout $\mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{-3})$, takže $U = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$. Podobně jako v **1.**a) vyjde $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, mezitělesa jsou $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-6})$, $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$.

b) Není Galoisovo, protože $x^3 - 3$ má ještě další dva komplexní kořeny, které budou v $U \subset \mathbb{R}$ chybět.

c) $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_2^3$. Mezitěles bude mnoho; pokud jsem se nepřepočítal, tak sedm stupně 2 a sedm stupně 1:

$$\mathbb{Q}(\sqrt{2}),\quad \mathbb{Q}(\sqrt{3}),\quad \mathbb{Q}(\sqrt{5}),\quad \mathbb{Q}(\sqrt{6}),\quad \mathbb{Q}(\sqrt{10}),\quad \mathbb{Q}(\sqrt{15}),\quad \mathbb{Q}(\sqrt{30}),$$
$$\mathbb{Q}(\sqrt{3}, \sqrt{5}),\quad \mathbb{Q}(\sqrt{2}, \sqrt{5}),\quad \mathbb{Q}(\sqrt{2}, \sqrt{3}),\quad \mathbb{Q}(\sqrt{5}, \sqrt{6}),\quad \mathbb{Q}(\sqrt{3}, \sqrt{10}),\quad \mathbb{Q}(\sqrt{2}, \sqrt{25}),$$
$$\mathbb{Q}(\sqrt{6}, \sqrt{10}).$$

d) Není Galoisovo. Zjevně je $\sqrt{1+\sqrt{2}}$ kořenem $(x^2-1)^2 - 2$, což můžeme při substituci $x = y + 1$ přepsat jako $(y^2+2y)^2 - 2 = y^4 + 4y^3 + 4y^2 - 2$, což je ireducibilní dle Eisensteinova kritéria s $p = 2$, tedy už $(x^2-1)^2 - 2$ musí být minimálním polynomem $\sqrt{1+\sqrt{2}}$. Jeho dalším kořenem je ale také třeba $\sqrt{1-\sqrt{2}} \notin \mathbb{R}$, přitom však $U \subset \mathbb{R}$, což už dosvědčuje, že U není normální.

3. Buď U rozkladové nadtěleso polynomu f nad tělesem T. Urči U, $[U:T]$, bázi U nad T a $\mathrm{Gal}(U/T)$ (můžeš se taky zamyslet nad tělesy V, $U \supset V \supset T$, ale mnohdy vypadají dost ošklivě), jestliže

a) $f = x^2 - 5$, $T = \mathbb{Q}$,
b) $f = x^3 - 2$, $T = \mathbb{Q}(e^{2\pi i/3})$,
c) $f = (x^2-3)(x^2-5)$, $T = \mathbb{Q}(\sqrt{2})$,
*d) $f = (x^2-1)^2 - 2$, $T = \mathbb{Q}$.

Řešení. a) $U = T(\sqrt{5})$, $[U:T] = 2$, $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_2$, mezitělesa jsou jen triviální.
b) $U = T(\sqrt[3]{2})$, $[U:T] = 3$, $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_3$, mezitělesa jsou jen triviální.
c) $[U:T] = 4$, $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_2^2$, mezitělesa jsou triviální a $T(\sqrt{3})$, $T(\sqrt{15})$, $T(\sqrt{5})$.
d) $U = T(\sqrt{1+\sqrt{2}}, i)$, $[U:T] = 8$, $\mathrm{Gal}(U/T) \simeq D_8$, mezitělesa vypadají komplikovaně, proto si je dovolím vynechat.

4. Mějme tělesa $V \supset U \supset T$ taková, že jak $V \supset T$, tak $U \supset T$ jsou normální rozšíření. Pak $\mathrm{Gal}(V/U) \triangleleft \mathrm{Gal}(V/T)$ a $\mathrm{Gal}(V/T)/\mathrm{Gal}(V/U) \simeq \mathrm{Gal}(U/T)$.

Řešení. Uvážím zobrazení definované restrikcí

$$\mathrm{Gal}(V/T) \to \mathrm{Gal}(U/T),$$
$$\varphi \mapsto \varphi|_U .$$

Nejprve zdůvodním, že $\varphi|_U$ je skutečně T-homomorfismus $U \to U$. T-homomorfismus je jasný. Pak určitě přinejmenším víme, že je to T-homomorfismus $U \to \overline{T}$. Definicí normality je tedy ve skutečnosti $U \to U$. Je to tělesový homomorfismus, takže i prosté T-lineární zobrazení. U má nad T konečnou dimenzi, takže lineární endomorfismus je prostý, právě když je na, tedy právě když je to automorfismus. Tím je dokázáno, že $\varphi|_U$.

Že restrikce zachová skládání automorfismů, je zřejmé. Máme tedy homomorfismus grup. Tvrdím, že je surjektivní, buď tedy dáno $\varphi \in \mathrm{Gal}(U/T)$ a najdu jeho vzor. Buď $V = T(\alpha)$ (Galoisovo rozšíření, tedy speciálně spearabilní konečného stupně). Pak je V rozkladové nadtěleso polynomu $m_{\alpha,T}$ nad T. Podle tvrzení 2.5 ze skript ale umíme T-izomorfismus $U =: T_1 \to T_2 := U$ rozšířit na nějaké ψ mezi rozkladovými nadtělesy polynomu f resp. $\varphi(f)$. Jenže f má koeficienty z T, takže $\varphi(f) = f$, a rozkladové nadtěleso f nad U je určitě V (je rozkladové už nad T). Takže jsme $\varphi : U \to U$ rozšířili nad $\psi : V \to V$, což jsme chtěli.

Tedy máme surjektivní homomorfismus grup. Co je jeho jádro? $\varphi|_U = \mathrm{id}_U$ nastává právě tehdy, když φ nechává U na msítě, tedy $\varphi \in \mathrm{Gal}(V/U)$. Jádro je tedy $\mathrm{Gal}(V/U) \leq \mathrm{Gal}(V/T)$, což z této podgrupy okamžitě činí podgrupu normální a navíc máme první větou o izomorfismu

$$\mathrm{Gal}(V/T)/\mathrm{Gal}(V/U) \simeq \mathrm{Gal}(U/T),$$

jak jsme chtěli.

5. Uvažujme cyklotomická tělesa.
a) Připomeň si, že $\mathrm{Gal}\left(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}\right) \simeq \mathbb{Z}_n^\times$. Předpokládej, že už víš $[\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q}] = \varphi(n)$.
b) Buď U rozkladové nadtěleso $x^{20} - 1$ nad $\mathbb{Q}(i)$. Urči $\mathrm{Gal}(U/\mathbb{Q}(i))$ a všechna mezitělesa V, $U \supset V \supset \mathbb{Q}(i)$.
c) * Buď U kořenové nadtěleso $x^3 + x^2 - 2x - 1$ nad $\mathbb{Q}$. Urči $\mathrm{Gal}(U/\mathbb{Q})$.

Řešení. a) Buď $\zeta := e^{2\pi i/n}$. Víme, že toto je kořenem n-tého cyklotomického polynomu, jehož kořeny jsou přesně ζ^k pro $k \in \mathbb{Z}_n^*$. Z toho jednak plyne, že $\mathbb{Q}(\zeta)$ je rovnou i rozkladové nadtěleso n-tého cyklotomického polynomu, takže je to Galoisovo rozšíření $\mathbb{Q}$. Také ale máme nanejvýš $\varphi(n)$ možných obrazů pro ζ, jmenovitě jednotlivá ζ^k, $k \in \mathbb{Z}_n^*$, takže všechna tato k musí dát automorfismus. Při skládání uvidíme

$$\zeta \mapsto \zeta^{k_1} \mapsto (\zeta^{k_1})^{k_2} = \zeta^{(k_1 k_2)},$$

z čehož je hned už vidět $\mathrm{Gal}\left(\mathbb{Q}(e^{2\pi i/n})/\mathbb{Q}\right) \simeq \mathbb{Z}_n^\times$.

b) Víme, že $\mathrm{Gal}(U/\mathbb{Q}) \simeq \mathbb{Z}_{20}^*$ a $\mathrm{Gal}(U/\mathbb{Q}(i))$ je její podgrupou. Potřebujeme tedy automorfismus zadaný pomocí $\zeta \mapsto \zeta^k$, $k \in \{1,3,7,9,11,13,17,19\}$ takový, že $i \mapsto i$. Díky $i = \zeta^5$ to znamená $i^k = i$, tedy $k \equiv 1 \pmod 4$, což nám ponechá pogrupu tvaru $\{1,9,13,17\} \simeq \mathbb{Z}_5^* \simeq \mathbb{Z}_4$ (jelikož $13^2 \equiv 9$, musí už 13 mít řád 4). To má tedy jen jednu netriviální podgrupu $\{1,9\}$.

Tvrdím, že příslušný Fix mohu popsat třeba jako $T(\zeta^4 + \zeta^{-4} - \zeta^8 - \zeta^{-8})$. K tomu si všimněme, že $\zeta \mapsto \zeta^9 = -\zeta^-4$, takže $\zeta^4 \mapsto (-1)^4\zeta^{-4}$, z čehož se

$$\zeta^4 + \zeta^{-4} - \zeta^8 - \zeta^{-8} \mapsto \zeta^{-4} + \zeta^4 - \zeta^{-8} - \zeta^8$$

fixuje. Tento výraz je ve skutečnosti roven $\sqrt{5}$ (jde to vykoukat z poznatků z druhácké Teorie čísel o Gaussových charakterech[1]), takže jediným netriviálním tělesem ležícím mezi U a $\mathbb{Q}(i)$ je $\mathbb{Q}(i,\sqrt{5})$.

c) Označme $\zeta := e^{2\pi i/7}$ a podívejme se na úlohu uvnitř $V := \mathbb{Q}(\zeta)$. Tvrdím, že $U = \mathbb{Q}(\zeta + \zeta^{-1})$. Že $\zeta + \zeta^{-1}$ je kořenem f se dověří dosazením, stejně tak se ověří, že dalšími dvěma kořeny jsou $\zeta^2 + \zeta^{-2}$ a $\zeta^3 + \zeta^{-3}$. Snadno taky vyjádříme, že tyto už leží v $\mathbb{Q}(\zeta + \zeta^{-1})$ skrze

$$\zeta^2 + \zeta^{-2} = (\zeta + \zeta^{-1})^2 - 2, \qquad \zeta^3 + \zeta^{-3} = (\zeta + \zeta^{-1})^3 - 3(\zeta + \zeta^{-1}).$$

Potom už vidíme, že máme Galoisovo rozšíření (rozkladové nadtěleso) stupně 3 (je to zároveň kořenové a f je ireducibilní, např. vyzkoušením všech možností z věty o racionálním kořeni), takže už musí být $\mathrm{Gal}(U/\mathbb{Q}) \simeq \mathbb{Z}_3$ (jediná trojprvková grupa). Z toho také plyne, že U nemá žádná netriviální podtělesa.

6. Mějme rozšíření $U \supset \mathbb{Q}$ konečného stupně, které ale není normální. Zamysli se, jestli přesto nedovedeme *nějak* pomocí Galoisovy korespondence najít všechna tělesa V, $U \supset V \supset \mathbb{Q}$. Obecněji uvažuj totéž pro rozšíření $U \supset T$, jež je separabilní a konečného stupně, ale není normální.

Řešení. Minule jsme viděli, že k separabilnímu rozšíření $U \supset T$ umíme najít $V \supset U$ tak, že $V \supset T$ je Galoisovo. Potom můžeme spočíst $\mathrm{Gal}(V/T)$ a hledat podtělesa většího V pomocí Galoisovy korespondence. Přitom ta z nich, která budou dokonce podtělesy U, budou odpovídat nadgrupám podgrupy $\mathrm{Gal}(V/U) < \mathrm{Gal}(V/T)$.

7. * Buď U rozkladové nadtěleso polynomu f nad tělesem T. Urči U, $[U:T]$, bázi U nad T a $\mathrm{Gal}(U/T)$ a všechna tělesa V, $U \supset V \supset T$, jestliže

a) $f = x^3 - 5$, $T = \mathbb{Z}_7$,
b) $f = x^4 - 3$, $T = \mathbb{Z}_5$,
c) $f = x^{p^k} - x$, $T = \mathbb{Z}_p$.

Řešení. a) f nemá v T kořen a je kubický, takže už je ireducibilní. Jelikož jsou 1, 2 a 4 třetí odmocniny z jedničky v $\mathbb{Z}_7$, je-li α kořenem f, pak jsou jimi i 2α a 4α, takže kořenové nadtěleso $\mathbb{Z}_7(\alpha)$ bude i rozkladové U. Z toho $[U:T] = 3$, takže Galoisova grupa je $\mathbb{Z}_3$ a nemáme žádná netriviální mezitělesa.

b) f nemá v T kořen a rozepsání rovnic plynoucích z rozkladu $x^4 - 3 = (x^2 - ax + b)(x^2 - cx + d)$ ukáže, že takový rozklad neexistuje, takže f je ireducibilní. Nyní jsou 1, 2, 3, 4 primitivní odmocniny z jedničky v $\mathbb{Z}_5$, takže pro kořen α polynomu f už násobky α představují všechny kořeny, tedy opět je kořenové nadtěleso $\mathbb{Z}_5(\alpha)$ rovnou i rozkladové. Pak vidíme $[U:T] = 4$. Automorfismy musí odpovídat $\alpha \mapsto k\alpha$, $k = 1,2,3,4$, což bude při skládání vypadat jako

$$\alpha \mapsto k_1\alpha \mapsto k_1(k_2\alpha) = (k_1k_2)\alpha,$$

z čehož je vidět $\mathrm{Gal}(U/T) \simeq \mathbb{Z}_5^* \simeq \mathbb{Z}_4$. Dvouprvkovou podgrupou je zde $\{1,4\}$. Čtyřka odpovídá $\alpha \mapsto 4\alpha = -\alpha$, takže se v tomto automorfismu musí fixovat α^2. To je kořenem kvadratického polynomu $x^2 - 3$, takže skutečně obdržíme kvadratické rozšíření

$$\mathrm{Fix}(U, \{1,4\}) = \mathbb{Z}_5(\alpha^2).$$

[1] Taky bych očekával, že to člověk uvidí, pokud bude dost dlouho zírat na pravidelný pětiúhelník.

c) V charakteristice p je $a \mapsto a^p$ okruhový homomorfismus (respektuje násobení i sčítání), takže i jeho k-násobné složení $a \mapsto a^{p^k}$ bude homomorfismus. Sama množina kořenů $f = x^{p^k} - x$ je tedy uzavřená na sčítání, násobení i multiplikativní inverzy, tvoří tedy těleso. To pak tedy má p^k prvků, tedy je to rozšíření $\mathbb{Z}_p$ stupně k. Homomorfismus $a \mapsto a^p$ je automorfismem a jeho skládáním vyrobíme k-různých automorfismů (protože teprve k-násobné složení $a \mapsto a^{p^k} = a$ je identita). To znamená, že Galoisova grupa je cyklická. Podtělesy jsou rozkladová nadtělesa polynomů $f_\ell = x^{p^\ell} - x$ pro $\ell \mid k$.

8. ** Nahlédni, že pokud $\mathrm{Gal}(T/\mathbb{Q}) \simeq A_4$, pak neexistuje žádné těleso U, $T \supset U \supset \mathbb{Q}$ se stupněm $[U : \mathbb{Q}] = 2$. Pokud si věříš, zkus dokázat, že rozkladové nadtěleso $f = x^4 + 8x + 12$ nad $\mathbb{Q}$ je příkladem takového T. (Mně se to zatím nepovedlo dokázat, ale podle důvěryhodného zdroje by to měla být pravda.)

Řešení. Galoisovou korespondencí odpovídají mezitělesa v $T \supset \mathbb{Q}$ podgrupám v $\mathrm{Gal}(T/\mathbb{Q})$. Stupeň $[U : \mathbb{Q}] = 2$ by musel odpovídat podgrupě $\mathrm{Gal}(T/\mathbb{Q})$ indexu 2, jenže A_4 žádné takové nemá.

Důkaz, že Galoisova grupa A_4 skutečně nastane pro rozkladové nadtěleso $f = x^4 + 8x + 12$, může horlivý zájemce najít zde:
https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquartic.pdf (Example 3.3)

6.6 Cvičení 6

algebraické množiny, Hilbertova věta o nulách, radikály

1. Rozhodni, které z následujících množin jsou algebraické:

a) $\{(t, t^2, t^3) \in K^3 \mid t \in K\}$,
b) $\{(\cos t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$,
c) $\mathbb{Z}$ jako podmnožina $\mathbb{R}$,
d) * $\mathbb{Z}^2$ jako podmnožina $\mathbb{R}^2$,
e) * $\{(t, \sin t) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$.

Řešení. Všude nechť X značí zadanou množinu.

a) Tvrdím $X = V(x^2 - y, x^3 - z)$, což dosvědčí, že X je algebraická. Dokažme dvě inkluze. Každý bod tvaru (t, t^2, t^3) bude nulou obou dvou polynomů, protože

$$(t)^2 - (t^2) = 0, \qquad (t)^3 - (t^3) = 0,$$

tedy $X \subset (x^2 - y, x^3 - z)$. Pro opačnou inkluzi, ať v $(a, b, c) \in K^3$ nabývají nuly oba polynomy $x^2 - y$, $x^3 - z$. To značí, že

$$b = a^2, \qquad c = a^3,$$

označíme-li tedy $t := a$, pak už bude $(a, b, c) = (t, t^2, t^3) \in X$, čímž je dokázáno $X = V(x^2 - y, x^3 - z)$.

b) $X = V(x^2 + y^2 - 1)$, tedy je to algebraická množina. Inkluze $\subset$ je jasná z Pythagorejské rovnosti $(\cos t)^2 + (\sin t)^2 = 1$. Pro opačnou inkluzi, ať $(a, b) \in \mathbb{R}^2$ splňuje $a^2 + b^2 - 1 = 0$, potom

$$1 = a^2 + b^2 \geq a^2,$$

tedy $|a| \leq 1$. Tedy a leží v obrazu funkce $\cos : \mathbb{R} \to [-1, 1]$, existuje proto $t \in \mathbb{R}$ takové, že $a = \cos t$. Pak platí

$$a^2 + (\sin t)^2 = (\cos t)^2 + (\sin t)^2 = 1,$$

porovnáním rovností tak $b^2 = (\sin t)^2$. Nyní pokud $b = \sin t$, pak $(a, b) = (\cos t, \sin t) \in X$, naopak když $b = -\sin t$, potom $(a, b) = (\cos(-t), \sin(-t)) \in X$. Tím je dohromady dokázáno i $V(x^2 + y^2 - 1) \subset X$.

c) Není algebraická. Pro spor ať $X = \mathbb{Z} = V(I)$ pro nějaký ideál $I \leq \mathbb{R}[x]$. Kdyby $I = (0)$, pak $V(I) = \mathbb{R} \neq \mathbb{Z}$. Tedy I obsahuje nějaký nenulový polynom f. Prvky $V(I)$ pak musí být jeho kořeny

(ne nutně všechny kořeny, máme jen inkluzi), ale nenulový polynom má jen konečně mnoho kořenů, tedy $V(I) \subset V(f)$ je konečná, což ale $\mathbb{Z}$ není, tedy spor.

d) X není algebraická. Pokud by byla, muselo by $V(I(X)) = X$, stačí tedy ukázat $V(I(X)) \supsetneq X$. Ať je $f(x,y) \in I(X)$. Uvažme polynom $f(x,0) \in \mathbb{R}[x]$ vzniklý dosazením nuly za y a ponecháním x jako neznámé. Tento polynom má míti nulovou hodnotu v každém celém čísle, tedy má mít nekonečně mnoho kořenů. Ale jediným polynomem jedné proměnné s nekonečně mnoha kořeny je nulový polynom, tedy $f(x,0) = 0 \in \mathbb{R}[x]$. To už ale značí, že f se nuluje na celé přímce $\mathbb{R} \times \{0\}$. Toto jsme provedli pro libovolné $f \in I(X)$, tedy $\mathbb{R} \times \{0\} \subset V(I(X))$, což už implikuje $V(I(X)) \supsetneq X$, jak jsme chtěli. (Opakovaným použitím téže myšlenky bychom dokonce mohli dokázat $I(X) = (0)$.)

e) X není algebraická, lze dokázat podobně jako d). Ve zkratce, uvážením $f(x,b)$ pro konstanty $b \in [-1,1]$ zjistíme, že cokoliv z $I(X)$ už by se nulovalo na celém $\mathbb{R} \times [-1,1]$, což dá spor s algebraičností. (Podobné úvahy lze vést dále a ukázat, že ve skutečnosti $I(X) = (0)$.)

2. (protipříklad Hilbertovy věty bez algebraické uzavřenosti) Najdi v $\mathbb{R}[x]$ maximální ideál, který neobsahuje žádný lineární polynom.

Řešení. Funguje třeba (x^2+1): faktorokruh je $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$, což je těleso, takže je to maximální ideál. Lineární polynom však neobsahuje, protože (nenulový) násobek kvadratického polynomu bude mít stupeň ≥ 2.

3. *Jacobsonův radikál* okruhu R definujeme jako $\mathcal{J}(R) := \bigcap_{M<R \text{ maximální}} M$. Nahlédni, že $a \in \mathcal{J}(R)$, právě když je $1 - ar$ jednotka pro každé $r \in R$.

Řešení. Zaprvé buď $a \in \mathcal{J}(R)$ a $r \in R$ libovolné a dokažme, že $1 - ar$ je jednotka. Pro spor ať $1 - ar$ není jednotka, to znamená, že $(1 - ar)$ je vlastní ideál v R. Každý vlastní ideál je obsažen v nějakém maximálním, mějme tedy $(1 - ar) \subseteq M < R$ pro M maximální ideál. Pak ale $1 - ar \in M$ a zároveň $a \in \mathcal{J}(R) \subset M$, v důsledku tedy i $1 = (1 - ar) + r \cdot a \in M$, což je spor. Tudíž $1 - ar$ musela být jednotka.

Za druhé buď $1 - ar$ jednotkou pro všechna r a dokažme, že $a \in \mathcal{J}(R) = \bigcap_{M \text{ maximální}} M$. Pro spor ať tomu tak není, tedy existuje maximální ideál M takový, že $a \notin M$. To znamená $a + M \neq 0 + M$ ve faktorokruhu R/M, což je maximalitou M těleso. Pak existuje $b + M \in R/M$ splňující $(a + M)(b + M) = 1 + M$, neboli pro kterýkoliv reprezentant $b \in R$ je $1 - ab \in M$. To už ale značí, že při volbě $r := b$ nebude $1 - ab$ jednotkou, protože $(1 - ab) \subsetneq R$.

4. Urči v oboru celých čísel $\mathbb{Z}$

a) $\sqrt{(0)}$, $\mathcal{J}(\mathbb{Z})$,

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) $\mathcal{J}(\mathbb{Z}/(100))$,

d) * kdy je ${}^{(\mathbb{Z}/(n))}/_{\mathcal{J}(\mathbb{Z}/(n)}$ těleso.

Řešení. a) (0) (protože $\mathbb{Z}$ je obor, určitě tedy nemá jiné nilpotentní prvky než 0 samotnou), (0) (nenulové číslo nemůže být dělitelné všemi prvočísly),

b) (5), (5), (10), (10), $(\prod_i p_i)$. Stačí dokázat poslední, obecný tvar: pokud $r := \max r_i$, pak $(\prod_i p_i)^r \in (\prod_i p_i^{r_i})$, tedy $(\prod_i p_i) \subset \sqrt{(\prod_i p_i^{r_i})}$ naopak ale pro $a^n \in \sqrt{(\prod_i p_i^{r_i})}$ nutně musí být $p_i \mid a^n$, tedy $p_i \mid a$ pro všechna i, tedy už $a \in (\prod_i p_i)$.

c) (10)/(100), protože $\mathbb{Z}/(100)$ má jako jediné maximální ideály (2)/(100) a (5)/(100).

d) Je to přesně pro $n = p^k$, p prvočíslo, $k \geq 1$. Aby se jednalo o těleso, má $\mathcal{J}(\mathbb{Z}/(n))$ být maximální ideál v $\mathbb{Z}/(n)$, tedy zde musí existovat právě jeden maximální ideál (protože průnik dvou či více maximálních ideálů už nemůže být maximální). Maximální ideály v $\mathbb{Z}/(n)$ odpovídají maximálním ideálům v $\mathbb{Z}$ obsahujícím (n), tedy prvočíslům dělícím n, takže přesně potřebujeme, aby bylo n násobkem pouze jednoho prvočísla.

5. V oboru $\mathbb{C}[x]$ polynomů nad komplexními čísly

a) spočítej $\sqrt{(0)}$, $\mathcal{J}(\mathbb{C}[x])$, $\sqrt{(x-3)^5(x-1)^4(x^3+2)}$, $\sqrt{(x^6-x^4-x^2+1)}$,
b) dokaž, že $\sqrt{(p)} = (\frac{p}{\mathrm{NSD}(p,p')})$, kde $p \in \mathbb{C}[x]$.

Řešení. $\mathbb{C}[x]$ je obor hlavních ideálů stejně jako $\mathbb{Z}$, úplně stejně tedy platí $\sqrt{(\prod_i g_i^{e_i})} = (\prod_i g_i)$ pro g_i navzájem neasociované ireducibilní polynomy.

a) Jsme v oboru ideálů, takže $\sqrt{(0)} = (0)$. Polynomy tvaru $x - c$ jsou určitě ireducibilní, takže $(x - c)$ je maximální ideál, takže každý prvek $\mathcal{J}(\mathbb{C}[x])$ musí mít za kořeny všechna komplexní čísla – může to tedy být jen nulový polynom, protože nenulový polynom jedné proměnné má jen konečně mnoho kořenů. Tedy $\mathcal{J}(\mathbb{C}[x]) = (0)$. Konečně skrze ireducibilní rozklad určíme

$$\begin{aligned}
\sqrt{(x-3)^5(x-1)^4(x^3+2)} &= \sqrt{(x-3)^5(x-1)^4(x+\sqrt[3]{2})(x+e^{2\pi i/3}\sqrt[3]{2})(x+e^{4\pi i/3}\sqrt[3]{2})} = \\
&= \left((x-3)(x-1)(x+\sqrt[3]{2})(x+e^{2\pi i/3}\sqrt[3]{2})(x+e^{4\pi i/3}\sqrt[3]{2})\right) = \\
&= \left((x-3)(x-1)(x^3+2)\right), \\
\sqrt{(x^6-x^4-x^2+1)} &= \sqrt{(x^2-1)(x^4-1)} = \sqrt{(x-1)^2(x+1)^2(x-i)(x+i)} = \\
&= ((x-1)(x+1)(x-i)(x+i)) = (x^4-1).
\end{aligned}$$

b) Ať je $p = \prod_i g_i^{e_i}$ rozklad na ireducibilní polynomy pro $p \neq 0$ (pro nulový polynom se tvrzení přímočaře ověří), pak víme $\sqrt{(p)} = (\prod_i g_i)$. Stačí tedy dokázat

$$\mathrm{NSD}(p, p') = \prod_i g_i^{e_i - 1}.$$

Zjevně musí $\mathrm{NSD}(p, p')$ dělit p, proto víme, že v rozkladu stačí uvažovat ireducibilní polynomy g_i, ne žádné další; zbývá tedy ukázat, že každý se vyskytne s exponentem $e_i - 1$. Zvolme pevně jedno i a označme $h := \frac{p}{g_i^{e_i}}$. Potom Leibnizovým pravidlem

$$p' = (g_i^{e_i} h) = (g_i^{e_i})' h + g_i^{e_i} h' = e_i g_i^{e_i - 1} h + g_i^{e_i} h' = g_i^{e_i - 1} \left(e_i h + g_i h'\right).$$

Derivace je tedy dělitelná g_i v $(e_i - 1)$-té mocnině, ale nikoliv v e_i-té, protože to by znamenalo $g_i \mid e_i h + g_i h'$, tudíž $g_i \mid e_i h$, což neplatí, protože e_i je konstanta a h je součinem samých ireducibilních polynomů neasociovaných s g_i. Tímto je důkaz hotov.

6. 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.

Řešení. a) Analogicky s úlohou 1a) lze dokázat, že $V(x^2 - y) = \{(t, t^2) \mid t \in \mathbb{C}\}$. Dokažme, že pokud se nějaký polynom $f \in \mathbb{C}[x, y]$ nuluje na celé této množině, pak je to násobek $x^2 - y$. Uvažujme $\tilde{f} := f(x, x^2) \in \mathbb{C}[x]$. Potom platí $\tilde{f}(t) = f(t, t^2)$, takže pokud $f \in I(V(x^2 - y))$, pak $\tilde{f}(t) = 0$. To znamená, že $\tilde{f}$ je polynom jedné proměnné, který má nekonečně mnoho kořenů, takovým je ale jen $\tilde{f} = 0$. Tím tedy víme $f(x, x^2) = 0$, na což můžeme nahlížet tak, že x^2 je kořenem $f \in (\mathbb{C}[x])[y]$, takže můžeme vytknout kořenový dvojčlen $y - x^2$:

$$f = (y - x^2) \cdot f_0 \qquad \text{pro nějaké } f_0 \in (\mathbb{C}[x])[y] = \mathbb{C}[x, y].$$

To už přesně znamená, že $f \in (x^2 - y)$, tedy jsme dokázali inkluzi $I(V(x^2 - y)) \subseteq (x^2 - y)$. Opačná inkluze je triviální, takže máme dokázánu rovnost.

Nyní ukažme ireducibilitu $V(x^2 - y)$. K tomu nechť $V(x^2 - y) = A \cup B$ pro nějaké algebraické množiny A, B a dokažme, že nutně jedna z A, B je rovna $V(x^2 - y)$. Víme, že $V(x^2 - y) = \{(t, t^2) \mid t \in \mathbb{C}\}$ je nekonečná množina, takže alespoň jedna z A, B je nekonečná, BÚNO ať je to

A. Potom ale nutně $I(A) \subseteq (x^2 - y)$ skrze analogický důkaz k předchozímu odstavci: tam jsme jako kořeny t polynomu $\tilde{f}$ mohli brát všechna komplexní čísla, ale bohatě nám stačilo, že *nějakých nekonečně mnoho* komplexních čísel jsou kořeny. Každý bod v A je tvaru (t, t^2) a takové t bude kořenem $\tilde{f}$ pro každé $f \in I(A)$, takže opět budeme mít $I(A) \subseteq (x^2 - y)$. Aplikováním V na inkluzi $I(A) \subseteq (x^2 - y)$ dostaneme

$$V(x^2 - y) \subseteq V(I(A)) = A$$

(využíváme toho, že V obrací inkluze a že $V(I(A)) = A$ pro algebraickou množinu A), takže už nutně $V(x^2 - y) = A$, jak jsme chtěli dokázat. Tedy $V(x^2 - y)$ je ireducibilní.

b) Zde prostě řešíme soustavu polynomálních rovnic

$$\begin{aligned} y^4 - x^2 &= 0, \\ y^4 - x^2y^2 + xy^2 - x^3 &= 0 \end{aligned}$$

nad $\mathbb{C}$. První rovnice se faktorizuje na $(y^2 - x)(y^2 + x) = 0$, takže stačí zvlášť řešit případy $y^2 \mp x = 0$. V těch můžeme pomocí $y^2 = \pm x$ zjednodušovat druhou rovnici na

$$\begin{aligned} (\pm x)^2 - x^2(\pm x) + x(\pm x) - x^3 &= 0, \\ x^2(1 \mp x \pm 1 - x) &= 0, \\ x^2(1 - x)(1 \pm 1) &= 0. \end{aligned}$$

Zde už je vidět, že pro $\pm = +$ řešíme $2x^2(1 - x) = 0$, což má (dvojnásobný) kořen 0 a dále kořen 1. Naproti tomu pro $\pm = -1$ se celá rovnice trivializuje, což znamená, že každá dvojice (x, y) splňující $y^2 = -x$ je řešením druhé rovnice. Z prvního případu tak máme konečně mnoho řešení, zatímco z druhého celou křivku nulových bodů. Dohromady:

$$V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) = \{(0, 0), (1, 1), (1, -1)\} \cup V(y^2 + x).$$

Jednobodové množiny jsou vždy algebraické a ireducibilní, zatímco $V(y^2 + x) = \{(-t^2, t) \mid t \in \mathbb{C}\}$ je ireducibilní (lze dokázat podobně jako v podúloze a)), takže máme ireducibilní rozklad

$$V(y^4 - x^2, y^4 - x^2y^2 + xy^2 - x^3) = \{(0, 0)\} \cup \{(1, 1)\} \cup \{(1, -1)\} \cup V(x^2 + y).$$

7. Je-li K konečné těleso, pak je každá podmnožina v K^n algebraická.

Řešení. Jednobodové množiny jsou algebraické, protože

$$\{(a_1, \ldots, a_n)\} = V(x_1 - a_1, \ldots, x_n - a_n).$$

Dále víme, že sjednocení dvou algebraických množin je algebraická množina, protože $V(IJ) = V(I) \cup V(J)$. Snadnou indukcí z toho plyne, že libovolné sjednocení konečně mnoha algebraických množin je opět algebraická množina. Pokud se tedy pohybujeme nad konečným tělesem K, pak pro libovolnou neprázdnou $A \subseteq K^n$ máme

$$A = \bigcup_{(a_1, \ldots, a_n) \in A} \{(a_1, \ldots, a_n)\},$$

což je konečné sjednocení algebraických množin, čili algebraická množina. (Prázdná množina je také algebraická skrze $\emptyset = V(1)$.)

8. Nahlédni, že pro ideál $I < R$ je $\sqrt{I}$ roven $\pi^{-1}(\sqrt{0/I})$, kde $\pi : R \twoheadrightarrow R/I$ je přirozená projekce.

Řešení. $a^n \in I \iff \pi(a)^n = 0$.

9. Buď K nekonečné těleso a $V = \{(t, t^2, t^3, \ldots, t^n) \mid t \in K\} \subset K^n$. Urči $I(V)$ (s důkazem!) a na základě úlohy z DÚ (V ireducibilní $\iff$ $I(V)$ prvoideál) vyvoď, že V je ireducibilní.

Řešení. (náznak) Platí $I(V) = (x_1^k - x_k \mid x = 2, \dots, n) =: P$, což je prvoideál, protože $K[x_1, \dots, x_n]/P \simeq K[x_1]$ je obor integrity (izomorfismus je $f+P \mapsto f(x_1, x_1^2, \dots, x_1^n)$). Skrz ekvivalenci z domácího úkolu tedy vidíme, že V je ireducibilní množina.

10. Rozmysli si následující charakterizace ideálů pomocí faktorokruhů: $I < R$ je
- maximální, právě když jsou všechny nenulové prvky R/I invertibilní,
- prvoideál, právě když je součin nenulových prvků v R/I vždy nenulový,
- radikálový, právě když je mocnina nenulového prvku v R/I vždy nenulová.

Řešení. První dvě odrážky říkají jen věci, které už známe: I je maximální, právě když je R/I těleso, resp. I je prvoideál, právě když je R/I obor integrity.

I je radikálový, právě když $\sqrt{I} = I$, tedy když $(\exists n)(a^n \in I) \iff a \in I$. Když totéž přeformulujeme ve faktorokruhu, tak chceme, aby pro libovolné $a + I \in R/I$ platilo, že

$$(\exists n)((a+I)^n = 0 + I) \iff a + I = 0 + I.$$

To ale přesně říká, že mocnina může být nulová pouze tehdy, když už její základ byl nulový, tedy že mocnina nenulového prvku v R/I už je nenulová.

11. 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.

Řešení. V $\mathbb{R}$ jsou druhé mocniny nezáporné, tudíž pro $(a, b) \in \mathbb{R}^2$ nastane $f(a, b) = 0$ právě tehdy, když $b = 0$ a zároveň $a(a-1) = 0$, tedy $V(f) = \{(0, 0), (1, 0)\}$, což je zjevně reducibilní množina.

Naproti tomu f je ireducibilní: pro spor at není, pak se rozkládá na $f = gh$, kde g i h jsou nekonstantní. Vzhledem k $\deg_y(f) = 2$ by pak BÚNO g mělo $\deg_y(g) \leq 1$. Díváme-li se na f jako na prvek $\mathbb{R}[x][y]$, pak má vedoucí koeficient jedna, tedy $\deg_y(g) = 0$ by znamenalo $g \mid 1$, tedy g je konstantní, což je spor.

Tedy musíme mít $\deg_y(g) = \deg_y(h) = 1$. Přitom f je ve smyslu $f \in \mathbb{R}[x][y]$ monický, tedy i g, h musí být monické, neboli

$$g = y + g_0, \qquad h = y + h_0$$

pro nějaká $g_0, h_0 \in \mathbb{R}[x]$. Pak už nám porovnání koeficientů v

$$y^2 + x^2(x-1)^2 = f = (y + g_0)(y + h_0) = y^2 + (g_0 + h_0)y + g_0 h_0$$

dá $h_0 = -g_0$ a následně $(x(x-1))^2 = g_0 h_0 = -g_0^2$. Je-li nyní $a \in \mathbb{R}$ vedoucí koeficient g_0, pak máme vzetím vedoucích koeficientů na obou stranách $1 = -a^2$, což zjevně reálné číslo nemůže splnit.

Tedy dohromady je f ireducibilní, jak jsme chtěli.

6.7 Cvičení 7

Algebraická teorie čísel

1. Najdi všechny jednotky v $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ pro $D = -2, -3, -7$.
* Pokud už jsi někdy viděl(a) Pellovu rovnici, zkus i $D = 2, 5$.

Řešení. Stačí řešit rovnici $N(\omega) = 1$ pro $\omega \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. Např. pro $x + y\frac{1+\sqrt{-3}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ pak řešíme rovnici $x^2 + xy + y^2 = 1$. Tu upravíme na $\left(x + \frac{y}{2}\right)^2 + \frac{3}{4}y^2 = 1$, z čehož $y^2 \leq \frac{4}{3}$, takže $|y| \leq 1$ a snadno již dořešíme. Vyjde, že v $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$ existuje šest jednotek: ± 1 a $\frac{\pm 1 \pm \sqrt{-3}}{2}$. Pro $D = -2$ i $D = -7$ podobným postupem vyjde, že jednotkami jsou jen ± 1.

Pro kladné D je potřeba znát teorii kolem Pellovy rovnice (viz druháckou Teorii čísel), jednotkami jsou pak (až na znaménko) mocniny fundamentálního jednotky. Pro $D = 2$ to budou $\pm(1 + \sqrt{2})^n$, $n \in \mathbb{Z}$, pro $D = 7$ zase $\pm(8 + 3\sqrt{7})^n$, $n \in \mathbb{Z}$.

2. Ireducibilní prvky pro $K = \mathbb{Q}(\sqrt{-14})$:

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.

Řešení. a) Dejme tomu, že $\alpha = \beta\gamma$. Pak $p = N(\beta)N(\gamma)$ je rozklad prvočísla na součin, čili jedno z $N(\beta)$, $N(\gamma)$ je ± 1. BÚNO ať $N(\beta) = \pm 1$. Pak je β jednotka, čili vyplývá, že α nejde rozložit na součin dvou nejednotek, čili je to ireducibilní prvek.

b) Třeba $N(3+\sqrt{-14}) = 3^2 + 14 = 23$.

c) Normy v K jsou jen nezáporné, protože x^2+14y^2 je pozitivně definitní kvadratická forma. Jelikož $N(3) = 9 = 3^2$, jediný způsob, jak by 3 mohla být reducibilní, by bylo, kdyby se rozkládala na součin dvou prvků normy 3. Ale žádný takový v $\mathcal{O}_K$ neexistuje, protože $x^2+14y^2 = 3$ nemá v $\mathbb{Z}$ řešení: odhadneme $3 \geq 14y^2$, takže $|y| < 1$, takže $y = 0$, následně ale $x^2 = 3$ nelze. Proto se 3 nemůže v $\mathcal{O}_K$ netriviálně rozkládat.

Podobně $N(1+\sqrt{-14}) = 15 = 3\cdot 5$, takže aby $1+\sqrt{-14}$ bylo reducibilní, muselo by se rozkládat na součin prvků norem 3 a 5. Ale už víme, že prvky s normou 3 v $\mathcal{O}_K$ neexistují.

d) Na levé straně už víme, že 3 je ireducibilní. Dokážeme, že i $5\pm 2\sqrt{-14}$ jsou ireducibilní. Obě mají normu $5^2 + 14\cdot 2^2 = 81 = 3^4$. Jak by se $5\pm 2\sqrt{-14}$ mohlo rozkládat? Chceme ukázat, že pouze na prvek normy 1 krát prvek normy 81. Stačí tedy vyloučit rozklady s normami $3\cdot 27$ nebo $9\cdot 9$.

Rozklad s normami $3\cdot 27$ nepřipadá v úvahu, protože už víme, že prvky normy 3 neexistují. Pro vyloučení druhého nejdřív tvrdíme, že normu 9 má v $\mathcal{O}_K$ pouze ± 3. K tomu řešme rovnici $x^2+14y^2 = 9$. Opět odhadneme $|y| < 1$, čili $y = 0$ a řešíme $x^2 = 9$, což má jako řešení pouze $x = \pm 3$. Tedy pokud by se $5\pm 2\sqrt{-14}$ mělo rozložit na součin prvků s normami 9, muselo by to až na znaménko být $3\cdot 3$. To ale neplatí, vidíme, že ± 3 nedělí $5\pm 2\sqrt{-14}$, vyvodíme tedy závěr, že $5\pm 2\sqrt{-14}$ je ireducibilní.

Tím je ověřeno, že 81 má v $\mathcal{O}_K$ dva různé rozklady na součin ireducibilních prvků, určitě to tedy není gaussovský obor.

3. Hlavní ideály pro $K = \mathbb{Q}(\sqrt{-14})$:
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) Dokaž, že $(2+\sqrt{-14}, 7+2\sqrt{-14}) = (3, 1-\sqrt{-14})$ a že jde o vlastní ideál, který není hlavní.

Řešení. a) Dokážeme rovnost ideálů jako dvě inkluze. Jedna je snadná:

$$3-\sqrt{-14} = (20+\sqrt{-14}) - (17+2\sqrt{-14}),$$

takže $(3-\sqrt{-14}) \subseteq (17+2\sqrt{-14}, 20+\sqrt{-14})$. Pro druhou implikaci chceme ukázat, že $17+2\sqrt{-14}$ i $20+\sqrt{-14}$ jsou násobky $3-\sqrt{-14}$. Nepotřebujeme znát přesně kolikanásobky to jsou, proto se jen podívejme ve faktorokruhu $\mathcal{O}_K/(3-\sqrt{-14})$. V tom platí $\sqrt{-14} \equiv 3$, takže spolu s $3-\sqrt{-14} \mid N(3-\sqrt{-14}) = 23$ získáme

$$17+2\sqrt{-14} \equiv 17+2\cdot 3 = 23 \equiv 0, \qquad 20+\sqrt{-14} \equiv 20+3 = 23 \equiv 0,$$

tedy skutečně $17+2\sqrt{-14}, 20+\sqrt{-14} \in (3-\sqrt{-14})$, takže $(17+2\sqrt{-14}, 20+\sqrt{-14}) \subseteq (3-\sqrt{-14})$.

b) Pro spor ať $(2, \sqrt{-14}) = (\alpha)$. Pak musí být $N(\alpha)$ společným dělitelem $N(2) = 4$ i $N(\sqrt{-14}) = 14$, tedy $N(\alpha) \mid 2$. Podobně jako v předchozí úloze snadno ukážeme, že prvky s normou 2 neexistují, takže zbývá jako jediná možnost $N(\alpha) = 1$. Potom $\alpha \mid 1$, takže můžeme BÚNO brát $\alpha = 1$.

Tedy by muselo být $(2, \sqrt{-14}) = \mathcal{O}_K$. Jenže obecný prvek ideálu $(2, \sqrt{-14})$ je nějaké

$$(a+b\sqrt{-14})\cdot 2 + (c+d\sqrt{-14})\cdot\sqrt{-14} = (2a-14d) + (2b+c)\sqrt{-14},$$

což má vždy sudou racionální část, takže takto nelze vyjádřit např. 1, což je spor s $(2, \sqrt{-14}) = \mathcal{O}_K$. Tedy $(2, \sqrt{-14})$ musí být nehlavní.

c) Nejprve ověřme rovnost ideálů, opět jako dvě inkluze. Postupně máme

$$2+\sqrt{-14} = 3+(1-\sqrt{-14}) \in (3, 1-\sqrt{-14}),$$
$$7+2\sqrt{-14} = 2(2+\sqrt{-14})+3 \in (3, 1-\sqrt{-14}),$$

takže $(2+\sqrt{-14}, 7+2\sqrt{-14}) \subseteq (3, 1-\sqrt{-14})$. Z opačné strany pak

$$3 = (7+2\sqrt{-14}) - 2(2+\sqrt{-14}) \in (2+\sqrt{-14}, 7+2\sqrt{-14}),$$
$$1-\sqrt{-14} = 3-(2+\sqrt{-14}) \in (2+\sqrt{-14}, 7+2\sqrt{-14}),$$

takže $(3, 1-\sqrt{-14}) \subseteq (2+\sqrt{-14}, 7+2\sqrt{-14})$.

Dále ať pro spor $(3, 1-\sqrt{-14}) = (\alpha)$. Pak musí $N(\alpha) \mid \mathrm{NSD}(N(3), N(1-\sqrt{-14})) = \mathrm{NSD}(9, 15) = 3$. Jelikož prvky normy 3 neexistují, znamenalo by to $N(\alpha) = 1$, takže $(3, 1-\sqrt{-14}) = \mathcal{O}_K$. To uvedeme ve spor nahlédnutím, že všechny prvky $(3, 1-\sqrt{-14})$ mají normu dělitelnou třemi. K tomu uvažujme $3\beta + (1-\sqrt{-14})\gamma$, pak počítáním ve faktorokruhu $\mathcal{O}_K/(3)$ máme

$$N(3\beta+(1-\sqrt{-14})\gamma) = (3\beta+(1-\sqrt{-14})\gamma)(3\beta'+(1+\sqrt{-14})\gamma') \equiv$$
$$\equiv (1-\sqrt{-14})\gamma(1+\sqrt{-14})\gamma' = N(1-\sqrt{-14})N(\gamma) = 15N(\gamma) \equiv 0 \pmod 3.$$

To už znamená, že např. $1 \notin (3, 1-\sqrt{-14})$, tedy máme spor a tento ideál nemohl být hlavní.

4. Násobení ideálů pro $K = \mathbb{Q}(\sqrt{-14})$:

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.

Řešení. a) Před vynásobením zvolíme pro ideály hezčí sadu generátorů:

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

Poté roznásobíme generátory každý s každým, čímž dostaneme výsledek zapsaný pomocí čtyř generátorů:

$$(3, 2+\sqrt{-14})(6, 2-\sqrt{-14}) = (18, 6-3\sqrt{-14}, 12+6\sqrt{-14}, 18).$$

Nyní tento zápis zjednodušíme. Duplicitní 18 můžeme vynechat, dále lze vytknout 3, takže

$$(18, 6-3\sqrt{-14}, 12+6\sqrt{-14}, 18) = 3\cdot(6, 2-\sqrt{-14}, 4+2\sqrt{-14}).$$

Zde nyní upravíme $(2-\sqrt{-14}, 4+2\sqrt{-14}) = (2-\sqrt{-14}, 8)$, takže

$$3\cdot(6, 2-\sqrt{-14}, 4+2\sqrt{-14}) = 3\cdot(6, 8, 2-\sqrt{-14}).$$

Už v $\mathbb{Z}$ platí $(6, 8) = (2)$, takže tím spíš v $\mathcal{O}_K$, nakonec tedy upravíme

$$3\cdot(6, 8, 2-\sqrt{-14}) = 3\cdot(2, 2-\sqrt{-14}) = 3\cdot(2, \sqrt{-14}) = (6, 3\sqrt{-14}).$$

b) Podle Tvrzení 4.11 bude $II' = (N(3), \mathrm{Tr}(3\cdot(1-\sqrt{-14})), N(1+\sqrt{-14})) = (9, 6, 15)$. To je ideál generovaný celými čísly, takže výsledek bude generovaný jejich NSD ve smyslu $\mathbb{Z}$, takže $II' = (3)$. Ideál $I' = (3, 1-\sqrt{-14})$ už jsme viděli v **3.**c), odkud víme, že není hlavní, takže ani I nemůže být hlavní.

Konečně, předpokládejme pro spor, že $I = I'$. Pak $I = (3, 1+\sqrt{-14}, 1-\sqrt{-14})$. Pak ale

$$1 = 3-(1+\sqrt{-14})-(1-\sqrt{-14}) \in I,$$

tedy $I = \mathcal{O}_K$, což je v rozporu s $NI = 3$.

c) Ukažme $NJ = 5$. To spočteme pomocí $JJ' = (N(5), \mathrm{Tr}(5 \cdot (1 - \sqrt{-14})), N(1 + \sqrt{-14})) = (25, 10, 15)$, což opět spočteme pomocí NSD v $\mathbb{Z}$ jako (5). S tímto už upravíme

$$IJI'J' = (II')(JJ') = (3)(5) = (15).$$

Jedním ireducibilním rozkladem 15 je $3 \cdot 5$. O 3 už víme, že je ireducibilní, a o 5 to dokážeme obdobně: kdyby se netriviálně rozkládala, muselo by to být na součin prvků normy 5, ale takové neexistují, protože $x^2 + 14y^2 = 5$ nemá řešení.

Pro druhý rozklad ukažme, že $IJ = (1 + \sqrt{-14})$. Ideál nalevo rozepíšeme jako

$$IJ \quad = \quad (3, 1 + \sqrt{-14})(5, 1 + \sqrt{-14}) \quad = \quad (15, 3 + 3\sqrt{-14}, 5 + 5\sqrt{-14}, (1 + \sqrt{-14})^2).$$

Jelikož $N(1 + \sqrt{-14}) = 15$, všechny čtyři z těchto generátorů jsou násobky $1 + \sqrt{-14}$, takže určitě $(1+\sqrt{-14}) \mid IJ$. Kdyby v této dělitelnosti nenastala rovnost, muselo by být $N(IJ) > N((1+\sqrt{-14}))$. Obě tyto normy jsou ale rovny 15, takže už musela nastat rovnost.

(Alternativně si stačí uvědomit, že z $3 \cdot (1 + \sqrt{-14})$ a $5 \cdot (1 + \sqrt{-14})$ už lze nakombinovat $1 \cdot (1 + \sqrt{-14})$.)

d) Nahlédněme obecněji, že ideál s prvočíselnou normou $NI = p$ musí být prvoideálem (neplatí to ale obráceně – existují prvoideály, jejichž norma není prvočíslo!). Jelikož $NI = 3$ a $NJ = 5$, pokryje toto oba naše ideály.

Uvažme rozklad I je prvočinitele, nechť je to $I = P_1 \cdots P_k$. Norma je multiplikativní, takže pak $p = NI = NP_1 \cdots NP_k$. Prvoideály jsou vždy vlastní ideály, takže máme vždy $NP_i > 1$. Pak se ale v součinu může vyskytovat jen jeden člen, jinak bychom netriviálně rozložili prvočíslo. Tedy $k = 1$ a $I = P_1$ je prvoideál.

5. Buď G podgrupa aditivní grupy $\mathbb{Z}^n$, kde $n \in \mathbb{N}$. Dokaž, že $G \simeq \mathbb{Z}^m$ pro nějaké m, $0 \leq m \leq n$. Jako důsledek nahlédni, že libovolný ideál v $\mathcal{O}_K$ lze zapsat nanejvýš dvěma generátory.

Řešení. Nejprve, ať G uvažovaná jako množina vektorů $\mathbb{Q}$-vektorového prostoru $\mathbb{Q}^n$ generuje nějaký podprostor V, a nechť tento prostor je m-dimenzionální. Ukážeme, že pak $G \simeq \mathbb{Z}^m$.

Postupujme indukcí podle m. Pro $m = 0$ je tvrzení zřejmé, protože $G = 0$. Pro $m = 1$ nám G generuje pouze přímku, můžeme proto na této přímce zvolit nejkratší nenulový vektor b. Každý další prvek $g \in G$ musí být celočíselný násobek b, protože jinak by $g - k \cdot b$ pro nějaké vhodné k byl kratší než b.

Nyní ať $m \geq 2$. Z generující množiny G vektorového prostoru V vyberme nějakou bázi $c_1, \ldots, c_m$. Nechť pak V' je lineární obal $c_1, \ldots, c_{m-1}$ a posléze $G' := G \cap V'$. Určitě $c_1, \ldots, c_{m-1} \in G'$, takže G' generuje V', podle indukčního předpokladu tak $G' \simeq \mathbb{Z}^{m-1}$, což znamená, že G' je volná abelovská grupa s nějakou bází $b_1, \ldots, b_{m-1}$. Dále už stačí jen vybrat vhodné $b_m \in G$ tak, aby $b_1, \ldots, b_m$ byla báze G jako volné abelovské grupy.

Se standardním skalárním součinem zúženým z $\mathbb{Q}^n$ musí mít V' uvnitř V jednodimenzionální ortogonální doplněk – ať je generovaný nějakým vektorem x. BÚNO jej přenásobme společným násobkem jmenovatelů vyskytujících se v jeho souřadnicích, takže pak $x \in \mathbb{Z}^n$. Jelikož je x normální vektor k V', je vzdálenost jakéhokoliv vektoru od V' přímo úměrná jeho skalárnímu součinu s x. Zvolme tedy nějaký prvek $b_m \in G \setminus G'$, který minimalizuje $|x \cdot b_m|$. To určitě lze, protože všechny hodnoty $x \cdot b_m$ jsou celočíselné.

Dokažme, že nyní množina $b_1, \ldots, b_{m-1}, b_m$ generuje G. Protože je to zároveň $\mathbb{Q}$-lineárně nezávislá množina, bude už to pak automaticky báze G jako volné abelovské grupy. Uvažme libovolné $g \in G$. Protože $b_1, \ldots, b_m$ je určitě přinejmenším báze V, můžeme vyjádřit

$$g = q_1 b_1 + \cdots + q_m b_m$$

pro jednoznačně určená $q_1, \ldots, q_m \in \mathbb{Q}$. Chceme dokázat, že to ve skutečnosti jsou celá čísla. Nejprve nechť pro spor $q_m \notin \mathbb{Z}$. Pak můžeme uvážit

$$\tilde{g} := g - \lfloor q_m \rfloor b_m \in G \setminus G',$$

což potom dá $|x \cdot \tilde{g}| = (q_m - \lfloor q_m \rfloor)\,|x \cdot b_m| < |x \cdot b_m|$, což je spor s volbou b_m. Máme tak $q_m \in \mathbb{Z}$. Následně pak $g - q_m b_m$ leží v G, ale zároveň v V', tudíž leží v G', a musí tak mít celočíselné souřadnice vůči $b_1, \ldots, b_{m-1}$, takže $q_1, \ldots, q_{m-1} \in \mathbb{Z}$. Dohromady jsme tak dokázali, že G je volná abelovská grupa s bází $b_1, \ldots, b_m$.

6. 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 $m \mid \alpha$ v $\mathcal{O}_K$, právě když $m \mid a, b$ v $\mathbb{Z}$. Nahlédni, že pro $D \equiv 1 \pmod 4$ nemusí totéž platit pro $m \mid a + b\sqrt{D}, a, b \in \mathbb{Z}$.

Řešení. Podle věty 4.3 víme, že $\mathcal{O}_K = \mathbb{Z}[\omega]$. Jelikož je ω celistvý prvek nad $\mathbb{Z}$ a má kvadratický minimální polynom, víme, že $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega$ ve smyslu abelovských grup, tj. že $\mathcal{O}_K$ je volná abelovská grupa s volnou bází 1, ω. Jinými slovy, $a + b\omega$ pro $a, b \in \mathbb{Q}$ je prvkem $\mathcal{O}_K$, právě pokud $a, b \in \mathbb{Z}$. Z toho už (pro $m \neq 0$)

$$m \mid a + b\omega \iff \frac{a}{m} + \frac{b}{m}\omega \in \mathcal{O}_K \iff \frac{a}{m}, \frac{b}{m} \in \mathbb{Z} \iff m \mid a, b.$$

Pro $m = 0$ stačí argumentovat

$$0 \mid a + b\omega \iff a + b\omega = 0 \iff a = b = 0,$$

protože 1, ω je $\mathbb{Q}$-lineární báze K.

Pro $D \equiv 1 \pmod 4$ už totéž nutně neplatí s $\sqrt{D}$ místo ω, protože např. $2 \mid 1 + \sqrt{D}$ v $\mathcal{O}_K$, protože $\frac{1+\sqrt{D}}{2} = \omega \in \mathcal{O}_K$, ale přitom $2 \nmid 1$.

7. Vyřeš diofantické rovnice $x^2 + 1 = y^5$, $x^2 + 3 = y^3$ a $x^2 + 4 = y^3$.

Řešení. Jako ukázkový příklad vyřešme $x^2 + 1 = y^5$, tvrdíme, že jediným řešením je $(x, y) = (0, 1)$. Levou stranu rozložíme v $\mathbb{Z}[i]$ jako $(x + i)(x - i) = y^5$. Jelikož je $\mathbb{Z}[i]$ gaussovský obor (resp. rovnou i OHI, $\mathbb{Q}(i)$ má třídové číslo 1), využijeme jednoznačný rozklad: pokud ukážeme, že závorky na levé straně jsou nesoudělné, pak už musí každá z nich být sama o sobě pátou mocninou, možná až na přenásobení jednotkou.

Ať je d nějaký společný dělitel $x + i$ a $x - i$. Potom musí být i $d \mid (x + i) - (x - i) = 2i$, takže by bylo $N(d) \mid N(2i) = 4$. Chceme ukázat, že jedinou možností je $N(d) = 1$, načež je d jednotka, takže $x + i$, $x - i$ jsou nesoudělná. Ať tedy pro spor $N(d) \neq 1$, pak už nutně $2 \mid N(d)$. To znamená $2 \mid N(x + i) = x^2 + 1 = y^5$, takže y je sudé. Pak je x liché, takže modulo 4 dostaneme

$$2 \equiv x^2 + 1 \equiv y^5 \equiv 0 \pmod 4,$$

což je spor. Takže jsou $x + i$, $x - i$ skutečně nesoudělná.

Pak je tedy $x + i$ pátá mocnina krát jednotka, tedy $x + i = u\alpha^5$ pro nějaké $\alpha \in \mathbb{Z}[i]$ a nějaké $u \in \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Protože je $\mathbb{Z}[i]^\times$ čtyřprvková (dokonce cyklická) grupa, platí $u = u^5$, takže můžeme zjednodušit $x + i = (u\alpha)^5$. Označíme-li pak $u\alpha = a + bi$, $a, b \in \mathbb{Z}$, můžeme rozepsat

$$x + i = (a + bi)^5 = (a^5 - 10a^3b^2 + 5a^4b) + (5a^4b - 10a^2b^3 + b^5)i.$$

Porovnáním imaginárních částí pak máme rovnici

$$1 = 5a^4b - 10a^2b^3 + b^5 = b(5a^4 - 10a^2b^2 + b^4).$$

Z toho $b \mid 1$, tedy $b = \pm 1$. Pro $b = -1$ dostaneme

$$-1 = 5a^4 - 10a^2 + 1,$$

což nemůže platit modulo 5. Pro $b = 1$ zase dostaneme

$$1 = 5a^4 - 10a^2 + 1,$$

což se zjednoduší na $a^2(a^2 - 2) = 0$. Pro celočíselné a bude $a^2 - 2$ vždy nenulové, takže jediným řešením je $a = 0$. Dohromady jsme tak dostali, že musí být $a + bi = i$, z čehož dopočítáme

$$x + i = (a + bi)^5 = i^5 = i,$$

tedy $x = 0$ a následně $y = 1$.

8. Dokaž, že $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\sqrt{D}]$, resp. $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ pro $D \equiv 2, 3$, resp. $1 \pmod 4$.

Řešení. Ať $K = \mathbb{Q}(\sqrt{D})$, kde D je bezčtvercové celé číslo. $\alpha \in K$ je celistvé nad $\mathbb{Z}$, právě pokud jeho minimální polynom nad $\mathbb{Q}$ má celočíselné kořeny. Dejme nejprve stranou racionální α: podle věty o racionálním kořeni je $\alpha \in \mathbb{Q}$ celistvé nad $\mathbb{Z}$ jen tehdy, když $\alpha \in \mathbb{Z}$. Dále tedy uvažujme $\alpha \in K \setminus \mathbb{Q}$. Takové α má minimální polynom

$$(x - \alpha)(x - \alpha') = x^2 - x(\alpha + \alpha') + \alpha\alpha' = x^2 - x\,\mathrm{Tr}(\alpha) + N(\alpha).$$

Takže α bude celistvé, právě když $\mathrm{Tr}(\alpha)$ i $N(\alpha)$ budou celá čísla. (Pozor, tohle je specifické pro kvadratická číselná tělesa, v tělesech vyššího stupně celočíselnost normy a stopy obecně nestačí...)

Mějme tedy $\alpha = a + b\sqrt{D}$. Nejprve díky $\mathbb{Z} \ni \mathrm{Tr}(\alpha) = 2a$ musí být a celé číslo či polovina lichého čísla. Nejprve nechť $a \in \mathbb{Z}$. Potom díky $\mathbb{Z} \ni N(\alpha) = a^2 - Db^2$ musí být taky $Db^2 \in \mathbb{Z}$. To pomocí p-valuací znamená totéž jako $v_p(Db^2) \geq 0$ pro každé p, přičemž valuaci na levé straně rozepíšeme jako $v_p(D) + 2v_p(b)$. Předpokládáme, že D je bezčtvercové celé číslo, takže $v_p(D)$ může být jen 0 nebo 1. Každopádně tak

$$v_p(b) \geq -\frac{1}{2}v_p(D) \geq -\frac{1}{2},$$

takže $v_p(b) \geq 0$, tudíž b je celočíselné. V tomto případě jsme tedy dospěli k $\alpha \in \mathbb{Z}[\sqrt{D}]$, což jsou pro libovolné D vždy celistvé prvky (např. protože $\sqrt{D}$ je celistvé a $\mathcal{O}_K$ je okruh).

Nyní uvažujme případ, kdy $a = \ell/2$ pro nějaké liché ℓ. Ukážeme, že toto může nastat jen pro $D \equiv 1 \pmod 4$ a že toto pak vynutí, aby $b = m/2$, kde m je liché. Toto tedy bude odpovídat $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$. Ať $m := 2b$, potom máme $2\alpha = \ell + m\sqrt{D}$. Bylo-li α celistvé, 2α musí být taky celistvé, a protože ℓ je celé, stejně jako v předchozím odstavci odvodíme $m \in \mathbb{Z}$. Zbývá tak ukázat, že m musí být liché a D musí být $1 \pmod 4$. K tomu počítejme modulo 4: jelikož $N(2\alpha) = 4N(\alpha)$ a $N(\alpha)$ bylo celé číslo, máme

$$0 \equiv N(\ell + m\sqrt{D}) = \ell^2 - Dm^2 \equiv 1 - Dm^2 \pmod 4.$$

Pro sudé m by bylo $m^2 \equiv 0$, což dá spor v předchozí kongruenci, takže určitě musí být m liché. Pak je $m^2 \equiv 1$, takže obdržíme $1 - D \equiv 0$, takže $D \equiv 1$.

Následně už jen ověříme, že všechny prvky $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ jsou pro $D \equiv 1 \pmod 4$ skutečně celistvé. K tomu stačí ověřit, že samo $\frac{1+\sqrt{D}}{2}$ je celistvé, což ale plyne z toho, že má stopu $1 \in \mathbb{Z}$ a normu $\frac{1-D}{4} \in \mathbb{Z}$.

9. Buď $K = \mathbb{Q}(\sqrt{D})$. Je-li $P < \mathcal{O}_K$ nenulový prvoideál a $\alpha \in \mathcal{O}_K$, potom $\alpha^{NP} \equiv \alpha \pmod P$.

Řešení. Stačí vědět, že faktorokruh $\mathcal{O}_K/P$ má právě NP prvků. Pokud je $\alpha \equiv 0 \pmod P$, pak je závěr zřejmý. Jinak je α nenulové v konečném tělese $\mathcal{O}_K/P$. Leží tedy v jeho multiplikativní

grupě, která má $NP-1$ prvků, takže Lagrangeovou větou z teorie grup máme $\alpha^{NP-1} \equiv 1 \pmod{P}$. Přenásobení této kongruence pomocí α pak dá kýžený závěr.

10. Buď R gaussovský obor a T jeho podílové těleso. Je-li $u \in T$ celistvé nad R, pak $u \in R$.

Řešení. Stačí ukázat $v_p(u) \geq 0$ pro všechny prvočinitele p. Pro spor ať tedy $v := v_p(u) < 0$ pro nějaké p. Ať je u kořenem monického polynomu $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$, kde $c_i \in R$. Pak tedy

$$u^n + c_{n-1}u^{n-1} + \cdots + c_1 u + c_0 = 0.$$

Jelikož $c_i \in R$, máme $v_p(c_i) \geq 0$. Na levé straně má u^n valuaci $n \cdot v$, zatímco každý další člen $c_i u^i$ má valuaci $i \cdot v + v_p(c_i) \geq iv$. Jelikož $v < 0$, máme $iv > nv$, takže u^n má ostře nižší valuaci než všechny ostatní členy na levé straně. V důsledku toho bude mít celá levá strana valuaci nv. To ale znamená $nv = v_p(0) = \infty$, což je spor.

11. * Je dáno prvočíslo $p > 5$ a přirozené k takové, že $p \mid k^2 + 5$. Dokaž, že existují přirozená m, n splňující $p^2 = m^2 + 5n^2$. Předpokládej, že víš, že třídová grupa $\mathbb{Z}[\sqrt{-5}]$ je dvouprvková.

Řešení. Označme $K = \mathbb{Q}(\sqrt{-5})$, pak $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Zadaná podmínka říká, že k je kořenem x^2+5 nad $\mathbb{F}_p$, takže podle věty 4.20 se (p) v $\mathcal{O}_K$ rozkládá jako součin dvou prvoideálů PP'. Rozmyslíme si, že to jsou dva různé prvoideály: jelikož $p \nmid 5$, nemůže být $k \equiv 0 \pmod{p}$, takže k není kořenem derivace $(x^2+5)' = 2x$ (máme $p > 5$, takže taky $p \nmid 2$), takže to není dvojitý kořen $x^2 + 5$.

Nyní tedy $N(P) = p$. Samo P možná je hlavní ideál a možná taky není. Jelikož je ale třídová grupa dvouprvková, druhá mocnina jakéhokoliv ideálu musí být v třídové grupě triviální, tedy druhá mocnina jakéhokoliv ideálu je hlavní ideál. Můžeme tedy vzít $P^2 = (\alpha)$ pro nějaké $\alpha \in \mathcal{O}_K$. Jelikož $P \neq P'$, máme $(p) = PP' \nmid P^2 = (\alpha)$, takže rozepíšeme-li $\alpha =: x + y\sqrt{-5}$, pak p nedělí alespoň jedno z x, y. Máme

$$p^2 = N(P)^2 = N(P^2) = N(\alpha) = x^2 + 5y^2.$$

Takže kdyby p dělilo jedno z x, y, muselo by dělit i to druhé. Takže $p \nmid x, y$, speciálně jsou pak x i y nenulová. Vzetím $m := |x|$, $n := |y|$ je pak úloha vyřešena.

12. ** Zkus si rozmyslet, že když $D \equiv 1 \pmod{4}$, pak $\mathbb{Z}[\sqrt{D}]$ nikdy nemůže být gaussovský obor.

Řešení. Pro $D \equiv 1 \pmod{4}$ víme, že $\frac{1+\sqrt{D}}{2} \in \mathbb{Q}(\sqrt{D})$ je celistvé nad $\mathbb{Z}$, ale neleží v $\mathbb{Z}[\sqrt{D}]$. Přitom je ale $\mathbb{Q}(\sqrt{D})$ podílové těleso $\mathbb{Z}[\sqrt{D}]$, takže podle úlohy **10.** nemůže $\mathbb{Z}[\sqrt{D}]$ být gaussovský.

7. Domácí úkoly

Ve verzi ze zimního semestru 2023/2024.

7.1 Domácí úkol 1

1. Uvažujme okruh R. Dokažte, že R je obor integrity, právě když $R[x]$ je obor integrity.

2. Buď R okruh. Dokažte, že je-li $R[x]$ noetherovský, pak je i R noetherovský.

3. Buď R gaussovský obor a uvažujme polynomy $f, g \in R[x]$, které jsou v tomto okruhu nesoudělné. Dokažte, že ideál $(f, g) < R[x]$ obsahuje nějaký nenulový prvek R.

4. Buď R okruh a $I, J < R$ komaximální ideály. Dokažte, že pro libovolná přirozená čísla m, n jsou ideály I^m, J^n komaximální.

5. *Multiplikativní množinou* v okruhu R myslíme takovou $S \subset R$, která je neprázdná, neobsahuje 0 a je uzavřená na násobení. Pomocí Zornova lemmatu (bez použití lemmatu 1.24 ve skriptech) dokažte: je-li $S \subset R$ multiplikativní množina a ideál $I < R$ splňuje $I \cap S = \emptyset$, pak existuje prvoideál $P \supset I$ splňující $P \cap S = \emptyset$.

7.2 Domácí úkol 2

1. Najděte $\alpha \in \mathbb{C}$ takové, že $\mathbb{Q}(\sqrt{2}, \sqrt{7}) = \mathbb{Q}(\alpha)$. (Dokazujte prosím pečlivě, neopírejte se o „zřejmá“ tvrzení, která nejsou zřejmá.)

2. Buď U těleso a $G < \mathrm{Aut}(U)$. Dokažte, že potom pro všechna $\varphi \in \mathrm{Aut}(U)$ platí $\mathrm{Fix}(U, \varphi G \varphi^{-1}) = \varphi\left(\mathrm{Fix}(U, G)\right)$.

3. Buď T rozkladové nadtěleso polynomu $x^4 - 5$ nad $\mathbb{Q}$. Určete stupeň rozšíření $[T : \mathbb{Q}]$.

4. Pro všechna možná kořenová nadtělesa U polynomu $x^4 + x^3 + x^2 + x + 1$ nad $\mathbb{Q}$ popište $\mathrm{Gal}(U/\mathbb{Q})$ a najděte nějakou „známou“ grupu, které je izomorfní.

7.3 Domácí úkol 3

1. Buď V rozkladové nadtěleso polynomu $f(x) = x^4 - 2$ nad tělesem $\mathbb{Q}$. Rozhodněte, zda je $V \supset \mathbb{Q}$ Galoisovo rozšíření, a určete $\mathrm{Gal}(V/\mathbb{Q})$. Nalezněte všechna tělesa T taková, že $V \supset T \supset \mathbb{Q}$, $[V : T] = 2$ a zároveň je $T \supset \mathbb{Q}$ normální rozšíření.

2. Buď P prvoideál v okruhu R a I, J vlastní ideály v R. Dokažte:
a) $\sqrt{I} \subseteq P$, právě když $I \subseteq P$.
b) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

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

4. Buďte $R \subset S \subset T$ obory. Dokažte:

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

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

c) $\sqrt{3\sqrt[4]{5} + 6\sqrt[7]{8}}$ je celistvý prvek nad $\mathbb{Z}$.