1. přednáška 11. října 2007.

Budu přednášet podle knihy D. A. Marcus, *Number Fields*, Springer 1977. Probereme zhruba prvních 5 kapitol (Ch. 1: A special case of Fermat's conjecture, Ch. 2: Number fields and number rings, Ch. 3: Prime decomposition in number rings, Ch. 4: Galois theory applied to prime decomposition, Ch. 5: The ideal class group and the unit group).

2. přednáška 18. října 2007. Opakování komutativní algebry podle apendixu 1.

okruh: komutativní s 1, *těleso*: rovněž komutativní, *obor (integrity)*: okruh bez dělitelů nuly ($ab = 0 \Rightarrow a = 0 \vee b = 0$).

$I \subset R$ je *ideál* v okruhu R: aditivní podgrupa uzavřená na všechny násobky ($a, b \in I, r \in R \Rightarrow a - b, ra \in I$). Pro ideál I máme faktorokruh R/I na třídách kongruence $a \equiv b \bmod I \iff a - b \in I$.

Sčítání a násobení ideálů: pro ideály I a J se ideál $I + J = \{a + b \mid a \in I, b \in J\}$, resp. ideál $IJ = \{a_1b_1 + a_2b_2 + \ldots + a_kb_k \mid a_i \in I, b_i \in J\}$ nazývá *součtem*, resp. *součinem* ideálů I a J. Podobně pro více ideálů.

Druhy ideálů I: *triviální* ($I = \{0\}$ a $I = R$), *hlavní* ($I = (a) = \{ra \mid r \in R\}$, tj. I je generovaný jediným prvkem $a \in R$), *maximální* ($I \neq R$ a $I \subset J \Rightarrow J = I \vee J = R$) a *prvoideály* ($ab \in I \Rightarrow a \in I \vee b \in I$).

- I je maximální $\iff$ R/I je těleso.
- I je prvoideál $\iff$ R/I je obor integrity.

Každý maximální ideál je tedy prvoideál. Jak uvidíme, v oborech hlavních ideálů to platí i naopak. Každý ideál různý od R je obsažený v maximálním ideálu (podle Zornova lemmatu, tj. axiomu výběru, protože sjednocení řetězce ideálů je ideál).

Ideály I a J jsou *nesoudělné*, když $I + J = R$. Lehce se ukáže, že pro nesoudělné ideály I a J máme $I \cap J = IJ$ a totéž platí pro více po dvou nesoudělných ideálů. *Čínská věta o zbytku* v okruhu $\mathbf{Z}$ říká, že pro $m = m_1m_2 \ldots m_k$, kde $m_i \in \mathbf{N}$ jsou po dvou nesoudělná čísla, je zobrazení

$$a \bmod m \mapsto (a \bmod m_1, \ldots, a \bmod m_k)$$

izomorfismem okruhů $\mathbf{Z}_m$ a $\mathbf{Z}_{m_1} \times \ldots \times \mathbf{Z}_{m_k}$ (hlavní výsledek je surjektivita, ostatní je jasné). Pro obecný okruh R máme následující zobecnění.

- *Čínská věta o zbytku pro ideály*: Jsou-li $I_1, \ldots, I_k$ po dvou nesoudělné ideály v okruhu R a $J = I_1I_2 \ldots I_k = I_1 \cap I_2 \cap \ldots \cap I_k$, je zobrazení

  $$a \bmod J \mapsto (a \bmod I_1, \ldots, a \bmod I_k)$$

  izomorfismem okruhů R/J a $R/I_1 \times \ldots \times R/I_k$.

Ukažme surjektivitu v případě $k = 2$. Protože $I_1 + I_2 = R$, máme $a_1 + a_2 = 1$ pro nějaké $a_i \in I_i$. Pro dané $r_1, r_2 \in R$ pak prvek $r = r_1 a_2 + r_2 a_1$ splňuje $r \equiv r_1 \bmod I_1$ a $r \equiv r_2 \bmod I_2$. Pro $k > 2$ se postupuje indukcí založenou na tom, že když je I nesoudělný s každým ideálem $J_1, \ldots, J_r$, pak je I nesoudělný i s $J_1 \cap J_2 \cap \ldots \cap J_k$.

Řekneme, že obor R je *obor hlavních ideálů* (OHI), když je každý ideál v R hlavní.

- V OHI je každý prvoideál maximální.

Vskutku, když $I \subset J$ a I je prvoideál, máme $I = (a)$ a $J = (b)$ pro nějaké $a, b \in R$. Tedy $a = bc$ pro nějaké $c \in R$ a $b \in I \vee c \in I$. První případ dává $I = J$ a druhý $c = ad$ pro nějaké $d \in R$. Pak $a = bad$ a $1 = bd$ (jsme v oboru integrity, můžeme krátit), b je jednotka a $J = R$. Ještě jednodušeji se ukáže, že

- V OHI je každý ideál generovaný ireducibilním prvkem maximální a tedy prvoideál.

Dělí-li tedy ireducibilní prvek součin několika prvků, musí dělit jeden z nich. Konečně

- Každý OHI je *noetherovský*, tj. každý řetězec ideálů $I_1 \subset I_2 \subset I_3 \subset \ldots$ se od nějakého indexu j dál stabilizuje, $I_j = I_{j+1} = \cdots$.

Stačí se podívat na sjednocení $I = I_1 \cup I_2 \cup \ldots$, což je ideál generovaný nějakým prvkem a. Protože $a \in I_j$ pro nějaké j, od indexu j dál se ideály I_i rovnají I.

Řekneme, že obor R je *obor s jednoznačnými (ireducibilními) rozklady* (OJR), když každý prvek a v R, který není jednotka, má rozklad na součin ireducibilních prvků a jsou-li

$$a = b_1 b_2 \ldots b_k = c_1 c_2 \ldots c_l$$

dva takové rozklady na součin ireducibilních prvků, potom $k = l$ a pro nějakou permutaci π čísel $1, 2, \ldots, k$ pro každé $i = 1, 2, \ldots, k$ máme rovnost $b_i e_i = c_{\pi(i)}$, kde e_i je jednotka. (Připomeňme si, že *jednotky*, tj. invertibilní prvky v R, tvoří multiplikativní podgrupu a že $a \in R$ je *ireducibilní*, když v každém multiplikativním rozkladu $a = bc$ je b nebo c jednotka.)

- R je OHI $\Rightarrow$ R je OJR.

Dokažme nejprve existenci a pak jednoznačnost ireducibilních rozkladů v R. Kdyby prvek a neměl rozklad na součin ireducibilních prvků, mohli bychom sestrojit takovou nekonečnou posloupnost prvků $a_1 = a, a_2, a_3, \ldots$, že vždy a_{i+1} dělí a_i, ale ne naopak. Ideály $I_i = (a_i)$ by pak tvořily ostře rostoucí řetězec $I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \ldots$, který ale neexistuje, protože R je noetherovský (viz výše), spor. Nechť $a = b_1 b_2 \ldots b_k = c_1 c_2 \ldots c_l$ jsou dva rozklady na součiny ireducibilních prvků. Protože b_1 dělí součin $c_1 c_2 \ldots c_l$, musí b_1 dělit nějaký prvek $c_{\pi(1)}$ (viz výše) a máme $b_1 e_1 = c_{\pi(1)}$, kde e_1 je jednotka. Prvky $b_1 e_1$ a $c_{\pi(1)}$ z rovnosti zkrátíme a podobně pokračujeme dále. Po k krocích dostaneme rovnost $1 = 1$.

Tudíž $b_i e_i = c_{\pi(i)}$ pro každé $i = 1, 2, \ldots, k = l$ pro nějakou permutaci π a jednotky e_i.

Řekneme, že obor R je *euklidovský*, když existuje takové zobrazení $n : R \to \mathbf{N}_0$, že pro každé dva prvky $a, b \in R, b \neq 0$ existují prvky $c, d \in R$ tak, že $a = bc + d$ a $d = 0$ nebo $n(d) < n(b)$.

- R je euklidovský $\Rightarrow$ R je OHI a tedy i OJR.

Stačí uvážit $b \in I$ s nejmenší hodnotou $n(b)$. Prvek b musí dělit každý prvek a v I a $I = (b)$. Příklady euklidovských oborů jsou okruhy $\mathbf{Z}$, $F[x]$ (kde F je těleso) a $\mathbf{Z}[i]$.

Jednoduchá postačující podmínka existence ireducibilních rozkladů je tato.

- Nechť existuje zobrazení $n : R\backslash\{0\} \to \mathbf{N}$, které je multiplikativní ($n(ab) = n(a)n(b)$) a splňuje implikaci $n(a) = 1 \Rightarrow a$ je jednotka (opačná implikace plyne z multiplikativity). Pak každý prvek v oboru R, který není jednotka, má rozklad na součin ireducibilních prvků.

Dokáže se to lehce indukcí podle hodnoty $n(a)$. Příkladem takových R jsou obory $R = \mathbf{Z}[\sqrt{d}]$, kde $d \in \mathbf{Z}$ není čtverec. Položíme

$$n(a + b\sqrt{d}) = |(a + b\sqrt{d})(a - b\sqrt{d})| = |a^2 - db^2|.$$

Zobrazení $n(\cdot)$ má patrně obě vlastnosti, takže v každém oboru $\mathbf{Z}[\sqrt{d}]$ existují ireducibilní rozklady. Klasický příklad $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ v $\mathbf{Z}[\sqrt{-5}]$ ale ukazuje, že vždy nejsou jednoznačné. Pomocí zobrazení $n(a + b\sqrt{-5}) = a^2 + 5b^2$ se snadno ukáže, že prvky $2, 3, 1 + \sqrt{-5}$ a $1 - \sqrt{-5}$ jsou ireducibilní v $\mathbf{Z}[\sqrt{-5}]$, ale 2 se z $1 + \sqrt{-5}$ ani z $1 - \sqrt{-5}$ nedostane vynásobením jednotkou (a totéž platí pro 3). Prvek 6 má v $\mathbf{Z}[\sqrt{-5}]$ dva podstatně odlišné ireducibilní rozklady. Okruh $\mathbf{Z}[\sqrt{-5}]$ tedy není OJR a tím spíše není OHI a ani euklidovský.

Nechť $F \subset G$ jsou tělesa a $\alpha \in G$ je algebraický nad F (tj. $p(\alpha) = 0$ pro nějaký nenulový polynom $p \in F[x]$).

- Pak okruh $F[\alpha] = \{q(\alpha) \mid q \in F[x]\} \subset G$ je těleso, to jest $F[\alpha] = F(\alpha) = \{q(\alpha) \mid q \in F(x)\} \subset G$.

Máme totiž izomorfismus $F[\alpha] \cong F[x]/I$, kde I je ideál polynomů v $F[x]$ anulujících se na α. I je zřejmě prvoideál a tedy je maximální ($F[x]$ je euklidovský obor a tedy OHI). Takže $F[x]/I$ je těleso.

Eisensteinovo kritérium praví, že celočíselný polynom, jehož všechny koeficienty kromě vedoucího jsou dělitelné nějakým prvočíslem, jehož čtverec ale nedělí konstantní koeficient, je nutně ireducibilní v $\mathbf{Z}[x]$. V okruzích máme toto zobecnění.

- *Eisensteinovo kritérium pro polynomy v $R[x]$.* Nechť M je maximální ideál v okruhu R a koeficienty polynomu $p(x) = a_n x^n + \ldots + a_1 x + a_0$ z $R[x]$ splňují, že $a_n \notin M$, $a_i \in M$ pro $i < n$ a $a_0 \notin M^2 = MM$. Potom je $p(x)$ ireducibilní v $R[x]$.

3. přednáška 25. října 2007. Opakování Galoisovy teorie podtěles C podle apendixu 2.

K otázkám z minulé přednášky. Okruh mocninných řad

$$\mathbf{C}[[x]] = \{\textstyle\sum_{n\geq 0} a_n x^n \mid a_n \in \mathbf{C}\}$$

je OJR a noetherovský (S. Lang, *Algebra*, Springer 2002, 3. vydání, Věty 9.3 a 9.4 v kapitole IV). Okruh „polynomů“ s racionálními exponenty

$$\mathbf{C}[x^q,\ q \in \mathbf{Q}, q \geq 0]$$

nemá ireducibilní rozklady (a není tedy noetherovský): je v něm nekonečný řetězec vlastních dělitelností $x^{1/2}|x$, $x^{1/3}|x^{1/2}$, $x^{1/4}|x^{1/3}$, atd.

Pro tělesa K a L značení $K \subset L$ znamená, že K je podtěleso L, mluvíme o *rozšíření těles*. Rozšíření těles $K \subset L$ je *konečné*, když má L jako vektorový prostor nad K konečnou dimenzi. Tuto dimenzi označujeme $[L : K]$ a nazýváme *stupeň L nad K*. Rozšíření $K \subset L$ je *algebraické*, když je každý prvek L algebraický nad K. Konečné rozšíření je algebraické a rozšíření $K \subset K[\alpha]$, kde α je algebraický nad K, je konečné. Pro podtělesa $K \subset \mathbf{C}$ dokážeme, že každé konečné rozšíření K je tvaru $K[\alpha]$. Pro řetězce rozšíření máme multiplikativní vztah mezi jednotlivými stupni:

- $K \subset L \subset M \Rightarrow [M : K] = [M : L][L : K]$, jakmile je jedna strana rovnice definovaná (tj. rozšíření $K \subset M$ je konečné nebo obě rozšíření $K \subset L$ a $L \subset M$ jsou konečná).

Snadno se totiž ověří, že báze B pro L nad K a báze C pro M nad L dávají bázi $\{bc \mid b \in B, c \in C\}$ pro M nad K. Díky této rovnici odvodíme, že algebraické prvky tvoří podtěleso.

- Pro prvky α, β z L algebraické nad K, kde $K \subset L$, jsou i prvky $\alpha+\beta, \alpha\beta$ a α/β algebraické nad K. Prvky L algebraické nad K tvoří podtěleso tělesa L.

Skutečně, $K \subset K[\alpha]$ a $K[\alpha] \subset (K[\alpha])[\beta] = K[\alpha, \beta]$ jsou konečná rozšíření, takže i rozšíření $K \subset K[\alpha, \beta]$ je konečné a tedy algebraické. (Algebraičnost podílu $1/\beta$ se pro algebraický prvek $\beta \neq 0$ dokáže přímo.)

Pokud $K \subset L$ a prvek α z L je algebraický nad K, máme $K[\alpha] \cong K[x]/I$, kde I je ideál polynomů z $K[x]$ anulujících se na α. Protože $K[x]$ je euklidovský a tedy OHI, je I generovaný jediným monickým polynomem $p(x)$, který se nazývá *minimální polynom* α nad K.

- Ekvivalentní definice: $p \in K[x]$ je minimální polynom α nad $K \iff p$ je monický polynom s nejmenším stupněm splňující $p(\alpha) = 0 \iff p$ je monický ireducibilní polynom splňující $p(\alpha) = 0$.

Minimální polynom je určený jednoznačně. Poslední definice ukazuje, že p je minimální polynom každého svého kořene. Má-li K nulovou charakteristiku, má minimální polynom jakožto ireducibilní polynom pouze jednoduché kořeny. (Nechť má p z $K[x]$ násobný kořen α. Derivace p' je nenulový polynom se stupněm o 1 menším než p—to pro nenulovou charakteristiku může selhat—a $p'(\alpha) = 0$. Minimální polynom α má tedy menší stupeň než polynom p a dělí ho, takže p je reducibilní.) Nechť je α algebraický nad K, pak jeho *stupeň* nad K, $\deg_K(\alpha)$, je stupeň jeho minimálního polynomu nad K. Následující rovnost je jasná.

- Když je α algebraický nad K, pak $\deg_K(\alpha) = [K[\alpha] : K]$.

V dalším pracujeme pro jednoduchost jen s tělesy obsaženými v tělese komplexních čísel $\mathbf{C}$.

Tedy $\mathbf{Q} \subset K \subset \mathbf{C}$ pro každé uvažované těleso K, které je proto nekonečné a má nulovou charakteristiku. Každý minimální polynom má také jednoduché kořeny. Pokud $K \subset L$ je konečné rozšíření ($L \subset \mathbf{C}$) a $\alpha \in L$ má nad K minimální polynom $p(x)$, nazveme kořeny $p(x)$ (leží v $\mathbf{C}$) *prvky konjugovanými s* α neboli *konjugáty* α nad K. Jak víme, $p(x)$ je minimální polynom každého svého kořene, takže jeho kořeny jsou vzájemně konjugované.

Vnoření tělesa K do $\mathbf{C}$ je injektivní homomorfismus těles $\tau : K \to \mathbf{C}$. Příkladem vnoření je každé identické zobrazení (máme $K \subset \mathbf{C}$), komplexní konjugace $a + bi \mapsto a - bi$ na $K = \mathbf{Q}[i]$ nebo zobrazení $\tau : K = \mathbf{Q}[2^{1/3}] \to \mathbf{C}$ definované pomocí

$$a + b2^{1/3} + c2^{2/3} \mapsto a + b\omega 2^{1/3} + c\omega^2 2^{2/3},\ a, b, c \in \mathbf{Q},\ \omega = \exp(2\pi i/3).$$

Vnoření τ tedy nahrazuje prvek $2^{1/3}$ konjugátem $\omega 2^{1/3}$, minimální polynom $2^{1/3}$ nad $\mathbf{Q}$ je $x^3 - 2 = (x - 2^{1/3})(x - \omega 2^{1/3})(x - \omega^2 2^{1/3})$. Všimněte si, že v prvních dvou příkladech jde o automorfismy, K se zobrazuje na K. Ve třetím příkladu τ automorfismem není, $K \subset \mathbf{R}$ ale $\tau(K) \not\subset \mathbf{R}$.

- Nechť $K \subset L$ je konečné rozšíření. Pak každé vnoření K do $\mathbf{C}$ má přesně $n = [L : K]$ různých rozšíření na vnoření L do $\mathbf{C}$. Speciálně, (i) L má přesně n vnoření do $\mathbf{C}$, která jsou identická na K, a (ii) když $[K : \mathbf{Q}] = n$, pak má K přesně n vnoření do $\mathbf{C}$.

Důsledek (i) je jasný, (ii) plyne z toho, že každé vnoření do $\mathbf{C}$ je nutně identické na $\mathbf{Q}$. Důkaz postupuje indukcí podle stupně n. Stačí se omezit na případ $L = K[\alpha]$, kde α je algebraický nad K stupně n. Nechť $p \in K[x]$ je minimální polynom α nad K, $\sigma : K \to \mathbf{C}$ je dané vnoření a $\tau : L \to \mathbf{C}$ je jeho rozšíření. Aplikace τ na identitu $p(\alpha) = 0$ ukazuje, že $\beta = \tau(\alpha)$ je kořenem polynomu $q(x) = \sigma p(x) \in \sigma(K)[x]$, který vznikne aplikací σ na koeficienty p. Polynom q má stupeň n a je ireducibilní, má tedy n různých jednoduchých kořenů. Pro τ tak máme přesně n možností, protože τ je jednoznačně určeno hodnotami na K, jež se shodují se σ, a hodnotou na α, což je jeden z n kořenů polynomu q.

Konjugáty a vnoření spolu úzce souvisejí:

- Uvažme konečné rozšíření $K \subset L = K[\alpha]$. Konjugáty prvku α nad K jsou přesně jeho obrazy $\sigma(\alpha)$ ve vnořeních $\sigma : L \to \mathbf{C}$ bodově fixujících K.

Vskutku, když σ aplikujeme na identitu $p(\alpha) = 0$, kde $p \in K[x]$ je minimální polynom α, dostaneme identitu $p(\sigma(\alpha)) = 0$, takže $\sigma(\alpha)$ je konjugát prvku α. Naopak, nechť β je konjugát α. Zobrazení $\sigma : K[\alpha] \to \mathbf{C}$ definované pomocí $r(\alpha) \mapsto r(\beta)$, kde $r \in K[x]$, je injektivní homomorfismus, který je identický na K a posílá α na β. Korektnost definice homomorfismu σ (prvky $K[\alpha]$ mají mnoho vyjádření ve tvaru $r(\alpha)$) a jeho injektivita plynou z faktu, že pro každé dva polynomy r, s z $K[x]$ platí $r(\alpha) = s(\alpha) \iff r(\beta) = s(\beta)$, neboť ideály polynomů v $K[x]$ anulujících se na α, resp. na β, splývají, jsou oba generované minimálním polynomem α.

Nyní dokážeme, že každé konečné rozšíření podtělesa $\mathbf{C}$ vznikne adjunkcí jediného prvku. Platí to obecněji pro tělesa s nulovou charakteristikou.

- Každé konečné rozšíření $K \subset L$ podtěles $\mathbf{C}$ je tvaru $L = K[\alpha]$ pro vhodný prvek α z L. Těleso L má tedy nad K bázi $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, kde $n = [L : K]$.

Opět indukce podle stupně n. Stačí se omezit na případ $L = (K[\alpha])[\beta] = K[\alpha, \beta]$. Ukážeme, že pro skoro všechna q z K, s možnou výjimkou $n^2 - n$ hodnot, máme $L = K[\alpha + q\beta]$ (využíváme, že těleso K je nekonečné). Nechť $K[\alpha + q\beta] \neq L$, tj. $K[\alpha + q\beta]$ je vlastní podtěleso tělesa L. Uvažme n vnoření L do $\mathbf{C}$, která jsou identická na K. Jejich zúžení na $K[\alpha + q\beta]$ nemohou být vzájemně různá, protože $[K[\alpha + q\beta] : K] < n$. Máme tedy dvě různá vnoření L do $\mathbf{C}$, řekněme σ a τ, která jsou na K identická a na $K[\alpha + q\beta]$ se rovnají, tj. $\sigma(\alpha + q\beta) = \tau(\alpha + q\beta)$. Odtud $\sigma(\alpha) - \tau(\alpha) = q(\sigma(\beta) - \tau(\beta))$. Rovnosti $\sigma(\alpha) = \tau(\alpha)$ a $\sigma(\beta) = \tau(\beta)$ nemohou současně nastat, to by se σ a τ rovnaly na celém $L = K[\alpha, \beta]$. Ve vyjádření

$$q = \frac{\sigma(\alpha) - \tau(\alpha)}{\sigma(\beta) - \tau(\beta)}$$

tak nedělíme nulou. Zjistili jsme, že

$$q \in K,\ K[\alpha + q\beta] \neq L \Rightarrow q \in M = \{\tfrac{\sigma(\alpha)-\tau(\alpha)}{\sigma(\beta)-\tau(\beta)} \mid \sigma, \tau \in S, \sigma(\beta) \neq \tau(\beta)\},$$

kde S je n-prvková množina vnoření L do $\mathbf{C}$, jež jsou identická na K. Zřejmě $|M| \leq n(n-1) = n^2 - n$.

4. přednáška 1. listopadu 2007.

$K \subset L$ je *normální rozšíření*, když každé z $n = [L : K]$ vnoření $\sigma : L \to \mathbf{C}$ fixujících bodově K zobrazuje L do L, tj. $\sigma(L) \subset L$. Protože $[\sigma(L) : K] = [L : K] = n$, máme pak nutně $\sigma(L) = L$ a všechna tato vnoření jsou automorfismy L fixující bodově K.

- Rozšíření těles $K \subset L$ je normální $\iff$ těleso L má přesně $[L : K]$ automorfismů fixujících bodově K $\iff$ všechny konjugáty prvků z L (vzhledem ke K) leží opět v L.

První ekvivalenci jsme právě dokázali. Druhá je vidět z vyjádření $L = K[\alpha] = \{r(\alpha) \mid r \in K[x]\}$ pro nějaký prvek α z L. Konjugát prvku $\beta = r(\alpha)$ z L je tedy $\sigma(\beta) = \sigma(r(\alpha)) = r(\sigma(\alpha))$, kde σ je vnoření L do $\mathbf{C}$ bodově fixující K, a leží v $K[\sigma(\alpha)] = \sigma(L)$. Je-li $K \subset L$ normální, leží všechny $\sigma(\beta)$ v $\sigma(L) = L$. Leží-li všechny $\sigma(\beta)$ v L, platí to speciálně pro $\beta = \alpha$ a máme $\sigma(L) = \sigma(K[\alpha]) = K[\sigma(\alpha)] \subset L$ pro každé σ.

V rozšíření $K \subset L$, jež není normální, nemůžeme vnoření L do $\mathbf{C}$ bodově fixující K skládat, což je nevýhoda: pro x v L nemá $\sigma(\tau(x))$ vždy smysl, protože $\tau(x)$ vždy neleží v L. Nicméně lze L konečně rozšířit na normální rozšíření K.

- Pro každé konečné rozšíření $K \subset L$ existuje takové konečné rozšíření $L \subset M$, že $K \subset M$ i $L \subset M$ jsou normální rozšíření.

M definujeme jako $M = K[\alpha_1, \alpha_2, \ldots, \alpha_n]$, kde α_i jsou všechny konjugáty prvku α, jehož adjunkcí vzniklo L, $L = K[\alpha]$ a $[L : K] = n$. Aplikace vnoření $\sigma : M \to \mathbf{C}$, jež je identické na K, na prvek $\beta = r(\alpha_1, \ldots, \alpha_n)$ z M, kde $r \in K[x_1, \ldots, x_r]$, způsobí jen permutaci konjugátů α_i: $\sigma(r(\alpha_1, \ldots, \alpha_n)) = s(\alpha_1, \ldots, \alpha_n)$, kde s vznikne z polynomu r odpovídající permutací proměnných. Takže $\sigma(\beta)$ je v M a M je normální rozšíření K. Podle definice je pak automaticky i normálním rozšířením L.

Galoisova grupa konečného rozšíření $K \subset L$ je množina $G = \mathrm{Gal}(L/K)$ všech automorfismů $\sigma : L \to L$, které bodově fixují K, spolu s operací $\circ$ skládání zobrazení. $(G, \circ)$ je zjevně grupa. Je-li $K \subset L$ normální, máme $|G| = [L : K] = n$, řád grupy je roven stupni L nad K. Pro podmnožinu $H \subset G$ (typicky podgrupu) uvažme množinu

$$F = \mathrm{Fix}(H) = \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ pro každé } \sigma \in H\}.$$

F je zřejmě podtělesem L a nadtělesem K, $K \subset F \subset L$, a nazývá se *fixním tělesem* množiny H.

- Nechť $K \subset L$ je normální rozšíření a $G = \mathrm{Gal}(L/K)$. Potom $\mathrm{Fix}(G) = K$ a pro každou vlastní podgrupu H grupy G je $\mathrm{Fix}(H)$ vlastní nadtěleso tělesa K.

Vskutku, kdyby $\mathrm{Fix}(G)$ bylo vlastní nadtěleso K, měli bychom příliš mnoho vnoření L do $\mathbf{C}$ bodově fixujících $\mathrm{Fix}(G)$, totiž $|G| = [L : K] > [L : \mathrm{Fix}(G)]$. Nechť H je vlastní podgrupa grupy G a, pro spor, $\mathrm{Fix}(H) = K$. Vezmeme $\alpha \in L$ tak, že $L = K[\alpha]$ a uvážíme polynom

$$p(x) = \prod_{\sigma \in H} (x - \sigma(\alpha)).$$

Patrně $p(\alpha) = 0$ a $p \in K[x]$ (koeficienty p jsou symetrické funkce hodnot $\sigma(\alpha)$, $\sigma \in H$, které jsou aplikací libovolného τ z H jen permutovány, takže každé τ

koeficienty fixuje a ty tak leží ve $\mathrm{Fix}(H) = K$). Stupeň p je ale příliš malý na to, aby α mohlo být jeho kořenem: $\deg(p) = |H| < |G| = [L : K]$.

Odtud se dokáže následující tvrzení, pro podrobnosti odkazujeme do Marcusovy knihy.

- *Galoisova korespondence.* Nechť $K \subset L$ je normální rozšíření a $G = \mathrm{Gal}(L/K)$. Zobrazení $F \mapsto \mathrm{Gal}(L/F)$ a $H \mapsto \mathrm{Fix}(H)$ mezi

  $$\{F \mid K \subset F \subset L\} \quad \text{a} \quad \{H \mid H \text{ je podgrupa } G\}$$

  jsou vzájemně inverzní a představují bijekci mezi oběma množinami. Když je $K \subset F$ normální, odpovídá v ní mezitělesu F normální podgrupa $H = \mathrm{Gal}(L/F)$ grupy G a máme izomorfismus grup $G/H \cong \mathrm{Gal}(F/K)$, který je zprostředkovaný zúžením příslušných automorfismů L na F.

Číselná tělesa.

Číselným tělesem K rozumíme konečné rozšíření tělesa racionálních čísel. Takže $\mathbf{Q} \subset K \subset \mathbf{C}$ a stupeň $[K : \mathbf{Q}] = n$ je konečný. Speciálně je K nekonečné, má charakteristiku nula, $K = \mathbf{Q}[\alpha]$ pro jediné $\alpha \in \mathbf{C}$ a každý prvek K je algebraický nad $\mathbf{Q}$. Komplexní čísla algebraická nad $\mathbf{Q}$ jsou stručně *algebraická čísla*. Jak víme, tvoří podtěleso tělesa $\mathbf{C}$. Každé číselné těleso je tedy podtělesem tělesa algebraických čísel.

Dva důležité typy číselných těles jsou kvadratická tělesa a kruhová tělesa. *Kvadratické těleso* je rozšíření stupně dvě, $K = \mathbf{Q}[\sqrt{d}]$, kde $d \in \mathbf{Z}$ je bezčtvercové celé číslo různé od 1. Pro $d < 0$ máme imaginární kvadratická tělesa a pro $d > 0$ reálná. *Kruhové těleso* je rozšíření $K = \mathbf{Q}[\omega]$, kde $\omega = \exp(2\pi i/m)$ je primitivní m-tá odmocnina z jedné a $m \in \mathbf{N}$. Později dokážeme, že $[K : \mathbf{Q}] = \varphi(m)$, kde hodnota Eulerovy funkce $\varphi(m)$ je počet čísel v $[m] = \{1, 2, \ldots, m\}$ nesoudělných s m.

Obor celých čísel číselného tělesa. V $\mathbf{Q}$ sedí obor integrity celých čísel $\mathbf{Z}$ (který je euklidovský, tedy OHI a OJR). Jakou má obdobu v číselném tělese K? Jak se to v ní má s ireducibilními rozklady? To jsou klíčové otázky této přednášky.

Máme $K = \mathbf{Q}[\alpha]$ pro nějaké algebraické číslo α a lze tipovat, že by obdoba $\mathbf{Z}$ v K mohl být obor integrity $\mathbf{Z}[\alpha]$. To je ale pravda jen někdy. Uvedeme přesnou definici. Uvažme množinu *celých algebraických čísel*, či stručněji *celistvých čísel*

$$\mathcal{A} = \{\alpha \in \mathbf{C} \mid p(\alpha) = 0 \text{ pro nenulový monický polynom } p \in \mathbf{Z}[x]\}.$$

Celistvá čísla jsou tedy kořeny monických nenulových celočíselných polynomů, tvoří podmnožinu algebraických čísel. Například zlatý řez $\beta = (1+\sqrt{5})/2$ (kořen $x^2 - x - 1$) je celistvé číslo. Pro číselné těleso K definujeme *obor celých čísel* O_K tělesa K jako průnik

$$O_K = \mathcal{A} \cap K.$$

O_K, správná analogie $\mathbf{Z}$ v K, tedy sestává z celistvých čísel ležících v K.

Celistvá čísla tvoří podokruh $\mathbf{C}$, takže každý obor O_K je podokruhem (samozřejmě podoborem integrity) svého číselného tělesa K.

- Nechť $\alpha, \beta \in \mathbf{C}$ jsou celistvá čísla. Pak $\alpha \pm \beta$ a $\alpha\beta$ jsou rovněž celistvá čísla.

Dokážeme to pomocí oboru $\mathbf{Z}[\alpha, \beta]$. Můžeme předpokládat, že $\alpha\beta \neq 0$. Protože α a β je celistvé, máme vyjádření

$$\alpha^m = a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0 \quad \text{a} \quad \beta^n = b_{n-1}\beta^{n-1} + \ldots + b_1\beta + b_0,$$

kde $a_i, b_i \in \mathbf{Z}$ a $m, n \in \mathbf{N}$. Opakovaným nahrazováním α^m a β^n uvedenými výrazy vyjádříme každý prvek $\mathbf{Z}[\alpha, \beta]$ ve tvaru

$$\sum_{j=1}^{mn} c_j\delta_j, \ c_j \in \mathbf{Z},$$

kde $\delta_1, \delta_2, \ldots, \delta_{mn}$ je libovolné pevné pořadí mn prvků $\alpha^i\beta^j, 0 \leq i < m, 0 \leq j < n$. Položíme $\gamma = \alpha \pm \beta$ (argument pro $\gamma = \alpha\beta$ je stejný). Pro každé δ_i je $\gamma\delta_i \in \mathbf{Z}[\alpha, \beta]$, takže pro $i = 1, 2, \ldots, mn$ máme vyjádření

$$\gamma\delta_i = \sum_{j=1}^{mn} c_{i,j}\delta_j, \quad c_{i,j} \in \mathbf{Z}.$$

Zapsáno maticově,

$$\gamma v = Av,$$

kde $A = (c_{i,j}) \in \mathbf{Z}^{mn\times mn}$ je čtvercová matice a $v = (\delta_i) \in \mathbf{C}^{mn}$ sloupcový vektor. To upravíme na

$$(\gamma I - A)v = \overline{0},$$

kde I je jednotková matice tvaru $mn \times mn$ a $\overline{0}$ sloupec mn nul. Ale v není nulový vektor, takže matice $\gamma I - A$ musí být singulární a

$$\det(\gamma I - A) = 0.$$

Matice $\gamma I - A$ má na diagonále prvky $\gamma - c_{i,i}$ a mimo ni celá čísla $-c_{i,j}$. V rozvoji determinantu dostaneme jediný člen γ^{mn} a ostatní ve tvaru $d\gamma^i$ s $d \in \mathbf{Z}$ a $0 \leq i < mn$. Vidíme, že γ je kořenem monického celočíselného polynomu stupně mn a je tedy celistvé.

- Každé celistvé číslo má celočíselný minimální polynom.

To hned vyplývá z tzv. Gaussova lemmatu: Jsou-li $p(x)$ a $q(x)$ racionální monické polynomy a $r(x)$ celočíselný monický polynom, přičemž $p(x)q(x) = r(x)$, pak $p(x)$ a $q(x)$ musejí být celočíselné polynomy. Pro jeho důkaz viz Marcusovu knihu.

Odtud plyne, že pro $K = \mathbf{Q}$ je $O_K = \mathbf{Z}$, jak by člověk čekal (jediné monické celočíselné polynomy stupně 1 jsou $x + a$ s $a \in \mathbf{Z}$). Jako cvičení si dokažte, že pro kvadratické těleso $K = \mathbf{Q}[\sqrt{d}]$ je

$$O_K = \mathbf{Z}[\sqrt{d}] \quad \text{pro} \quad d \not\equiv 1 \pmod 4$$

a

$$O_K = \mathbf{Z}[\tfrac{1}{2}, \sqrt{d}] \quad \text{pro} \quad d \equiv 1 \pmod 4.$$

Pro kruhové těleso $K = \mathbf{Q}[\omega]$ je vždy $O_K = \mathbf{Z}[\omega]$, ale dokázat to není snadné, snad se k tomu dostaneme.

5. přednáška 8. listopadu 2007. Stopa, norma, diskriminant.

V dalším je K číselné těleso stupně n, O_K je obor celých čísel v K a $\sigma_1, \dots, \sigma_n$ jsou vnoření K do $\mathbf{C}$ (jedno σ_i je identita). Víme, že K je vektorový prostor dimenze n nad $\mathbf{Q}$. Každý prvek K tak lze vyjádřit jako racionální lineární kombinaci $c_1\alpha_1 + \dots + c_n\alpha_n$, $c_i \in \mathbf{Q}$, v nějaké bázi $\{\alpha_1, \dots, \alpha_n\}$ (a takových bází je spousta). Díky následujícímu pozorování existují báze ležící v O_K.

- Pro každé algebraické číslo α z $\mathbf{C}$ existuje přirozené číslo m tak, že $m\alpha$ je celistvé číslo. Každé algebraické číslo α lze tedy vyjádřit jako $\alpha = \beta/m$, kde β je celistvé a jmenovatel m je z $\mathbf{N}$.

Rovnost $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$, kde α_i jsou z $\mathbf{Q}$, stačí vynásobit m^n, kde m je společný násobek jmenovatelů koeficientů a_i, a dostaneme rovnost $(m\alpha)^n + ma_{n-1}(m\alpha)^{n-1} + \dots + m^n a_0 = 0$ ukazující celistvost $m\alpha$.

Je-li $\alpha_1, \dots, \alpha_r$ konečný seznam algebraických čísel a $m_i\alpha_i$ je celistvé pro m_i z $\mathbf{N}$, pak je $m\alpha_i = (m_1 m_2 \dots m_r)\alpha_i$ celistvé pro každé $i = 1, \dots, r$. Tak dostaneme bázi vektorového prostoru K splňující $\{\alpha_1, \dots, \alpha_n\} \subset O_K$. Pak

$$\{c_1\alpha_1 + \dots + c_n\alpha_n \mid c_i \in \mathbf{Q}\} = K \quad \text{a} \quad \{c_1\alpha_1 + \dots + c_n\alpha_n \mid c_i \in \mathbf{Z}\} \subset O_K.$$

Cílem dnešní přednášky je dokázat existenci tzv. *celistvé báze*, pro níž místo poslední inkluze nastává rovnost a každé číslo v O_K je celočíselnou lineární kombinací jejích prvků.

Za tím účelem zavedeme dvě důležitá zobrazení $T, N : K \to \mathbf{C}$, *stopu* a *normu*, definovaná jako

$$T(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \dots + \sigma_n(\alpha) \quad \text{a} \quad N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\dots\sigma_n(\alpha).$$

Například pro kvadratické těleso $K = \mathbf{Q}[\sqrt{d}]$ máme

$$T(a + b\sqrt{d}) = 2a \quad \text{a} \quad N(a + b\sqrt{d}) = a^2 - db^2.$$

Hned uvidíme, že stopa a norma jsou racionální čísla, a na O_K jsou jejich hodnoty celočíselné. Z definice plyne, že stopa je lineární zobrazení a norma je multiplikativní:

$$T(r\alpha + s\beta) = rT(\alpha) + sT(\beta) \quad \text{a} \quad N(\alpha\beta) = N(\alpha)N(\beta), \ r, s \in \mathbf{Q}.$$

Dále, pro r v $\mathbf{Q}$ máme $T(r) = nr$ a $N(r) = r^n$.

- Nechť α z K má stupeň d (nutně dělitel stupně $n = [K : \mathbf{Q}]$) a minimální polynom $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, $a_i \in \mathbf{Q}$. Potom

$$T(\alpha) = (n/d)t(\alpha) = -(n/d)a_{d-1} \quad \text{a} \quad N(\alpha) = n(\alpha)^{n/d} = a_0^{n/d},$$

  kde $t(\alpha)$ je součet a $n(\alpha)$ součin konjugátů α.

Hodnoty $\sigma_i(\alpha)$ pro $i = 1, 2, \ldots, n$ totiž probíhají všech d konjugátů α a každý z nich n/d krát ($\mathbf{Q}[\alpha]$ má d vnoření do $\mathbf{C}$ a každé z nich má n/d rozšíření na vnoření K do $\mathbf{C}$). Součet (resp. součin) konjugátů α, což jsou kořeny $p(x)$, je podle Viètových vztahů mezi kořeny a koeficienty polynomu roven $-a_{d-1}$ (resp. a_0).

- Pro α z K leží $T(\alpha)$ a $N(\alpha)$ v $\mathbf{Q}$ a pro α z O_K leží $T(\alpha)$ a $N(\alpha)$ v $\mathbf{Z}$.

To hned plyne z předchozí formule pro stopu a normu.

Pomocí normy lze nalézt jednotky v O_K a dokazovat ireducibilitu.

- Nechť α je z O_K a p z $\mathbf{N}$ je prvočíslo. Pak

$$\alpha \text{ je jednotka } \Leftrightarrow N(\alpha) = \pm 1 \quad \text{a} \quad N(\alpha) = \pm p \Rightarrow \ \alpha \text{ je ireducibilní.}$$

Z $\alpha\beta = 1$, $\beta \in O_K$, aplikací normy máme, že $N(\alpha)N(\beta) = N(1) = 1$, a vzhledem k celočíselnosti obě hodnoty normy musejí být ± 1. Naopak, z $\pm 1 = N(\alpha) = \alpha\sigma_2(\alpha)\ldots\sigma_n(\alpha_n)$ máme, že α je jednotka, neboť $\sigma_2(\alpha)\ldots\sigma_n(\alpha_n)$ je součin konjugátů α (s možnými opakováními), které jsou v O_K a jejich součin rovněž. Pokud α má normu $\pm p$ a $\alpha = \beta\gamma$ v O_K, aplikace normy dává rozklad $\pm p = N(\beta)N(\gamma)$ v $\mathbf{Z}$, a tak $N(\beta)$ nebo $N(\gamma)$ je ± 1 a β nebo γ je jednotka.

Takže třeba prvek $9 + \sqrt{10}$ je ireducibilní v $\mathbf{Z}[\sqrt{10}]$ (O_K pro $K = \mathbf{Q}[\sqrt{10}]$), neboť má prvočíselnou normu $9^2 - 10 \cdot 1^2 = 71$. Jako další příklad se podíváme na jednotky v oborech celých čísel kvadratických těles $K = \mathbf{Q}[\sqrt{d}]$. Pro $d \equiv 1 \bmod 4$ je $O_K = \mathbf{Z}[(1+\sqrt{d})/2]$ a jinak $O_K = \mathbf{Z}[\sqrt{d}]$. Norma prvku $(a+b\sqrt{d})/2$, resp. $a + b\sqrt{d}$, je $(a^2 - db^2)/4$, resp. $a^2 - db^2$. Pro $d < 0$ je diofantická rovnice $N((a + b\sqrt{d})/2) = \pm 1$, resp. $N(a + b\sqrt{d}) = \pm 1$, s neznámými $a, b \in \mathbf{Z}$ triviální, jen s konečně mnoha řešeními. Řešení ukazují, že pro $d \neq -1, -3$ jsou jen dvě jednotky ± 1, pro $d = -1$ čtyři jednotky $i, -i, -1, 1$ (čtvrté odmocniny z 1) a pro $d = -3$ šest jednotek ± 1 a $(\pm 1 \pm \sqrt{-3})/2$ (šesté odmocniny z 1). A $d > 0$? Diofantická rovnice $N(\alpha) = \pm 1$ je pak netriviální a teorie Pellovy rovnice praví, že pro každé bezčtvercové d z $\mathbf{N}$ je nekonečně mnoho řešení. Pro $d > 0$ je proto grupa jednotek v O_K nekonečná. Například pro $d = 2$ jsou jednotkami v $\mathbf{Z}[\sqrt{2}]$ přesně čísla $\pm a_k \pm b_k\sqrt{2}$, kde $a_k + b_k\sqrt{2} = (1 + \sqrt{2})^k$ a k probíhá $\mathbf{N}_0$.

Relativní stopa T_K^L a *relativní norma* N_K^L se pro konečné rozšíření $K \subset L$ definují jako

$$T_K^L(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha) \quad \text{a} \quad N_K^L(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\ldots\sigma_n(\alpha),$$

kde σ_i jsou teď vnoření L do $\mathbf{C}$ bodově fixující K. Vlastnosti relativní stopy a normy jsou analogické vlastnostem standardní stopy a normy. Totiž T_K^L je K-lineární zobrazení; N_K^L je multiplikativní; pro r z K je $T(r) = nr$ a $N(r) = r^n$,

kde $n = [L : K]$; $T_K^L(\alpha) = -(n/d)a_{d-1}$ a $N_K^L(\alpha) = a_0^{n/d}$, kde $d = [K[\alpha] : K]$ a a_{d-1} a a_0 jsou příslušné koeficienty minimálního polynomu α vzhledem ke K; $T_K^L(\alpha)$ a $N_K^L(\alpha)$ leží v K a pro α v O_L leží v O_K.

- V řetězci rozšíření $K \subset L \subset M$ relativní stopa a norma splňují rovnosti $T_K^M(\alpha) = T_K^L(T_L^M(\alpha))$ a $N_K^M(\alpha) = N_K^L(N_L^M(\alpha))$ (tranzitivita).

Důkaz je v Marcusově knize.

Diskriminant n-tice $\alpha_1, \alpha_2, \ldots, \alpha_n$ prvků z K (připomínáme, že $n = [K : \mathbf{Q}]$) je čtverec determinantu matice všech n^2 konjugátů prvků α_j:

$$\mathrm{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) := \det{}^2((\sigma_i(\alpha_j))_{i,j=1}^n).$$

Díky čtverci nezávisí hodnota diskriminantu na pořadí prvků α_j a vnoření σ_i. Matice konjugátů má položky v $\mathbf{C}$ a diskriminant by tak mohl být komplexní číslo, ale ve skutečnosti je racionální a pro α_j z O_K je diskriminant celé číslo. To je vidět z alternativní formule

- $\mathrm{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det((T(\alpha_i\alpha_j))_{i,j=1}^n)$.

Položíme-li totiž $d = \mathrm{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ a $M = (\sigma_i(\alpha_j))_{i,j=1}^n$, máme $d = \det^2(M) = \det(M)\det(M) = \det(M^t)\det(M) = \det(M^tM)$. Na místě i, j matice M^tM je prvek

$$\sigma_1(\alpha_i)\sigma_1(\alpha_j) + \sigma_2(\alpha_i)\sigma_2(\alpha_j) + \cdots + \sigma_n(\alpha_i)\sigma_n(\alpha_j),$$

což je právě $\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j) = T(\alpha_i\alpha_j)$. Odtud, vzhledem k hodnotám stopy,

- hodnota diskriminantu leží v $\mathbf{Q}$ a jsou-li jeho argumenty z O_K, leží v $\mathbf{Z}$.

Ukážeme, že n-tice prvků z K má nulový diskriminant, právě když je lineárně závislá nad $\mathbf{Q}$. Nechť w je sloupcový vektor $(\beta_1, \ldots, \beta_n)^t$ a v je sloupcový vektor $(\alpha_1, \ldots, \alpha_n)^t$, kde β_i a α_i jsou z K, a platí

$$w = Nv, \quad \text{kde} \quad N = (c_{i,j})_{i,j=1}^n \in \mathbf{Q}^{n\times n}.$$

Jinak řečeno, každé β_i je lineární kombinací prvků $\alpha_1, \ldots, \alpha_n$ s racionálními koeficienty.

- Potom máme vztah

$$\mathrm{disc}(\beta_1, \beta_2, \ldots, \beta_n) = \det{}^2(N) \cdot \mathrm{disc}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Skutečně, aplikace σ_j na rovnost $\beta_i = c_{i,1}\alpha_1 + \cdots + c_{i,n}\alpha_n$, $c_{i,j} \in \mathbf{Q}$, dává tutéž rovnost pro j-té konjugáty: $\sigma_j(\beta_i) = c_{i,1}\sigma_j(\alpha_1) + \cdots + c_{i,n}\sigma_j(\alpha_n)$. Takže i $\sigma_j(w) = N\sigma_j(v)$. Celkem pro transponované matice konjugátů $M_\alpha = (\sigma_i(\alpha_j))_{i,j=1}^n$ a $M_\beta = (\sigma_i(\beta_j))_{i,j=1}^n$ máme vztah $M_\beta^t = NM_\alpha^t$. Aplikací determinantu a umocněním na druhou dostáváme vztah mezi diskriminanty obou n-tic.

Abychom dokázali, že nulovost diskriminantu je ekvivalentní s lineární závislostí nad $\mathbf{Q}$, potřebujeme ještě nalézt bázi vektorového prostoru K s nenulovým diskriminantem.

- Nechť $K = \mathbf{Q}[\alpha]$, takže $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ je $\mathbf{Q}$-báze K. Pak

$$\operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \prod_{1 \le r < s \le n} (\alpha_r - \alpha_s)^2 = \pm N(p'(\alpha)) \neq 0,$$

  kde α_r jsou konjugáty α (které jsou vzájemně různé), $p(x)$ je minimální polynom α a znaménko je $+$, právě když $n \equiv 0, 1 \bmod 4$.

První rovnost se dostane aplikací formule pro van der Mondův determinant

$$\det \begin{pmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{pmatrix} = \prod_{1 \le r < s \le n} (x_r - x_s)$$

dosazením $\alpha_i = \sigma_i(\alpha)$ za x_i a umocněním na druhou. Druhá rovnost. Zderivováním $p(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)$ podle x podle Leibnizova pravidla a dosazením α_i za x dostáváme n rovností

$$p'(\alpha_i) = (\alpha_i - \alpha_1) \ldots (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}) \ldots (\alpha_i - \alpha_n),$$

jejichž vynásobením máme

$$N(p'(\alpha)) = \prod_{1 \le r \neq s \le n} (\alpha_r - \alpha_s)$$

(použili jsme, že $\sigma_i(r(\alpha)) = r(\sigma_i(\alpha))$ pro r z $\mathbf{Q}[x]$). Tento součin $n(n-1)$ činitelů je přesně roven hořejšímu součinu $n(n-1)/2$ čtverců, když $n(n-1)/2 \equiv 0 \bmod 2$, a jinak má opačné znaménko—dostáváme podmínku na n modulo 4.

Důsledek:

- prvky $\alpha_1, \ldots, \alpha_n$ z K jsou nad $\mathbf{Q}$ lineárně nezávislé, právě když máme $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) \neq 0$.

Jsou-li totiž nad $\mathbf{Q}$ lineárně závislé, máme stejnou závislost i pro jejich i-té konjugáty a tedy i pro řádky matice konjugátů M, a pak $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det^2(M) = 0$. Naopak, jsou-li nad $\mathbf{Q}$ lineárně nezávislé, jejich sloupcový vektor w vznikne lineární transformací $w = Nv$ ze sloupcového vektoru v báze $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ prostřednictvím vhodné matice $N \in \mathbf{Q}^{n \times n}$ s nenulovým determinantem. Tedy $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det^2(N) \cdot \operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \neq 0$, protože oba činitelé jsou nenuloví.

Nyní dokážeme existenci celistvé báze O_K.

- Obor celých čísel O_K číselného tělesa K má celistvou bázi, to jest, existuje n-tice prvků $\alpha_1, \ldots, \alpha_n$ (v O_K) tak, že $O_K = \{c_1\alpha_1 + \cdots + c_n\alpha_n \mid c_i \in \mathbf{Z}\}$.

Uvážíme n-tice prvků z O_K s nenulovým diskriminantem. Nějaké existují, protože K má nad $\mathbf{Q}$ báze ležící v O_K, a ty, jak jsme právě ukázali, mají nenulový

diskriminant. Hodnoty těchto diskriminantů jsou nenulová celá čísla, takže můžeme vzít n-tici $\alpha_1, \ldots, \alpha_n$ z O_K, která má $|\mathrm{disc}(\alpha_1, \ldots, \alpha_n)| > 0$ nejmenší. Ukážeme, že je hledanou celistvou bází. Je jistě bazí K nad $\mathbf{Q}$. Předpokládejme pro spor, že nějaké γ z O_K má ve vyjádření $\gamma = c_1\alpha_1 + \cdots + c_n\alpha_n$, $c_i \in \mathbf{Q}$, některý koeficient, například c_1, neceločíselný. Pak lze psát $c_1 = d_1 + \theta$, kde d_1 je ze $\mathbf{Z}$ a $0 < \theta < 1$. Uvážíme novou n-tici $\beta_1, \ldots, \beta_n$,

$$\beta_1 = \theta\alpha_1 + c_2\alpha_2 + \cdots + c_n\alpha_n = \gamma - d_1\alpha_1,\ \beta_2 = \alpha_2,\ \ldots,\ \beta_n = \alpha_n.$$

Opět $\beta_i \in O_K$ pro každé i. Protože nová n-tice vznikla ze staré lineární transformací

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} \theta & c_2 & \ldots & c_n \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix},$$

podle pravidla o transformaci diskriminantů

$$\mathrm{disc}(\beta_1, \ldots, \beta_n) = \det^2(N) \cdot \mathrm{disc}(\alpha_1, \ldots, \alpha_n) = \theta^2 \mathrm{disc}(\alpha_1, \ldots, \alpha_n).$$

Takže

$$0 < |\mathrm{disc}(\beta_1, \ldots, \beta_n)| < |\mathrm{disc}(\alpha_1, \ldots, \alpha_n)|,$$

což je spor s minimalitou $|\mathrm{disc}(\alpha_1, \ldots, \alpha_n)|$.

6. přednáška 15. listopadu 2007. Tři diofantické rovnice.

7. přednáška 22. listopadu 2007.

Přednáška odpadla.

8. přednáška 29. listopadu 2007. Základní věta aritmetiky v Dedekindových oborech.

Cílem této přednášky je dokázat následující větu.

- Každý nenulový ideál I oboru celých čísel O_K číselného tělesa K má až na pořadí činitelů jednoznačné vyjádření $I = P_1P_2 \ldots P_k$ jako součin prvoideálů.

Prvoideály oboru R rozumíme *netriviální prvoideály*, tedy $P \neq (0), R$. Prázdným součinem prvoideálů rozumíme triviální ideál R. R je tedy součinem prvoideálů, prázdným. Tuto základní větu dokážeme abstraktněji pro obecnější třídu oborů než jsou O_K, pro Dedekindovy obory.

Dedekindův obor je obor R splňující tyto tři podmínky:

1. R je noetherovský.

2. Každý prvoideál v R je maximální ideál.

3. R je celistvě uzavřený ve svém podílovém tělese K: každý prvek z K, který je kořenem monického polynomu s koeficienty v R, leží v R.

První podmínka znamená, že každý ideál v R je konečně generovaný. Ekvivalentně, v R nejsou nekonečné ostře rostoucí řetězce ideálů a ještě jinak řečeno, každá neprázdná množina ideálů má maximální prvek vzhledem k $\subset$.

Nejprve dokážeme, že

- každý obor celých čísel O_K číselného tělesa je Dedekindův.

Podmínka 1. Celý O_K je konečně generovaný, protože O_K má celistvou bázi s $n = [K : \mathbf{Q}]$ prvky. O_K je tedy (vzhledem ke sčítání) volná Abelova grupa s n generátory. Ideál I je její podgrupa. Není těžké ukázat, že tím pádem je I volnou Abelovou grupou s nejvýše n generátory a je konečně generovaný (dokonce nad $\mathbf{Z}$, stačilo by nad O_K).

Podmínka 2. Nechť I je nenulový ideál v O_K. Ukážeme, že O_K/I je konečný okruh. Tím budeme s druhou podmínkou hotovi, protože pro prvoideál P v O_K dostaneme konečný obor integrity O_K/P a ten díky konečnosti musí být těleso, takže P je maximální ideál. (Pro každý obor integrity S a nenulový prvek a z S je zobrazení $x \mapsto ax$ z S do S injektivní. Pro konečný S musí být i surjektivní, takže v S existuje b splňující $ab = 1$. Každý nenulový prvek S má inverz a S je tedy těleso.) Konečnost O_K/I plyne z vyjádření O_K pomocí celistvé báze $\alpha_1, \ldots, \alpha_n$ jako lineárních kombinací $\sum_1^n a_i\alpha_i$, $a_i \in \mathbf{Z}$, a z faktu, že I obsahuje nějaké přirozené číslo m. Pak $(m) \subset I$ a $|O_K/I| \leq |O_K/(m)| = m^n$. Proč mají I a $\mathbf{N}$ neprázdný průnik? Nechť α je nenulový prvek z I. Je to celistvé číslo, takže $\alpha^k + a_{k-1}\alpha^{k-1} + \ldots + a_0 = 0$ pro nějaká celá čísla a_i, přičemž můžeme díky nenulovosti α předpokládat, že i $a_0 \neq 0$. Pak ale $m = |a_0| = \pm(-a_1\alpha - \ldots - a_{k-1}\alpha^{k-1} - \alpha^k)$ je v I i v $\mathbf{N}$.

Podmínka 3. Podobně jako jsme dokázali, že celistvá čísla (kořeny monických polynomů s celočíselnými koeficienty) tvoří okruh, dá se dokázat, že kořeny monických polynomů s celistvými koeficienty jsou opět celistvá čísla. Podílové těleso O_K je K (každé α z K je tvaru β/m pro β v O_K a m v $\mathbf{N}$). Pokud je tedy α v K a je kořenem monického polynomu s koeficienty v O_K, jsou koeficienty celistvá čísla a α je tedy rovněž celistvé, takže v O_K.

Přejdeme k obecnému Dedekindovu oboru R s podílovým tělesem K. K důkazu existence a jednoznačnosti rozkladů ideálů v R na součiny prvoideálů potřebujeme následující základní výsledek.

- Pro každý ideál I v Dedekindově oboru existuje ideál J tak, že IJ je hlavní ideál.

Důkaz. Vezmeme nenulový prvek α z I a uvážíme prvky

$$J = \{\beta \in R \mid \beta I \subset (\alpha)\}.$$

Patrně je J ideál a $\alpha \in J$, takže $J \neq (0)$. Je jasné, že $IJ \subset (\alpha)$. Dokážeme, že platí rovnost $IJ = (\alpha)$. K tomu potřebujeme dvě lemmata.

- První lemma. V Dedekindově oboru každý nenulový ideál obsahuje součin prvoideálů.

Pokud je množina nenulových ideálů R neobsahujících žádný součin prvoideálů neprázdná, vezmeme její maximální prvek I (díky noetherovosti R) a dostaneme následující spor. Patrně $I \neq R$ (samotný R je prázdým součinem prvoideálů) a I není prvoideál. Takže existují dva prvky α, β v $R\backslash I$, že $\alpha\beta$ je v I. V inkluzi jsou ideály $I + (\alpha)$ a $I + (\beta)$ ostře větší než I, a tak $I + (\alpha) \supset P_1P_2 \dots P_s$ a $I+(\beta) \supset Q_1Q_2 \dots Q_t$ pro nějaké prvoideály P_i a Q_i. Pak ale $P_1 \dots P_sQ_1 \dots Q_t \subset (I + (\alpha))(I + (\beta)) \subset I$, což je spor.

- Druhé lemma. Pro každý vlastní ideál I v Dedekindově oboru R s podílovým tělesem K existuje prvek γ v $K\backslash R$ splňující $\gamma I \subset R$.

Vezmeme libovolné nenulové b z I. Podle prvního lemmatu $(b) \supset P_1P_2 \dots P_r$ pro nějaké prvoideály P_i. Vybereme součin s nejmenším r (patrně $r \geq 1$, protože I je vlastní). Vlastní ideál I je obsažený v nějakém maximálním ideálu P, jenž je nutně prvoideál. Protože $P_1P_2 \dots P_r \subset (b) \subset I \subset P$, platí $P_i \subset P$ a tedy $P_i = P$ pro nějaké i (prvoideály v Dedekindově oboru jsou maximální ideály), řekněme $P = P_1$. (Kdyby $P_i \not\subset P$ pro každé i, vybereme z každého prvoideálu P_i prvek ležící mimo P. Součin těchto prvků je v P, tudíž i jeden z nich, spor. Takže $P_i \subset P$ pro nějaké i.) Máme

$$P_1P_2 \dots P_r \subset (b) \subset I \subset P_1.$$

Díky minimalitě r můžeme zvolit prvek a v $P_2 \dots P_r\backslash(b)$. Prvek $\gamma = a/b$ má obě požadované vlastnosti: patrně $a/b \in K$ a nelze $a/b \in R$ neboť a není v (b), dále $aI \subset P_2 \dots P_rI \subset P_2 \dots P_rP_1 \subset (b)$, takže $(a/b)I \subset R$.

Dokončíme důkaz toho, že $IJ = (\alpha)$, kde I, α, J jsou zavedeny výše. Položíme $A = \frac{1}{\alpha}IJ$. Protože $IJ \subset (\alpha)$, je $A \subset R$. Dále je A ideál. Předpokládejme pro spor, že A je vlastní, to jest, $A \neq R$ (čili $IJ \neq (\alpha)$). Podle druhého lemmatu vezmeme γ v $K\backslash R$, že $\gamma A \subset R$. Pak

$$(\gamma J)I = \gamma IJ = \gamma\alpha A = \alpha\gamma A \subset \alpha R = (\alpha)$$

a podle definice J to znamená, že $\gamma J \subset J$. Ideál J je konečně generovaný, $J = \langle\beta_1, \dots, \beta_t\rangle$. Nechť je v sloupcový vektor generátorů β_i. Vztah $\gamma J \subset J$ znamená, že

$$\gamma v = Mv$$

pro nějakou matici M v $R^{t\times t}$. Nyní postupujeme opět stejně, jako při důkazu toho, že celistvá čísla tvoří okruh (ve čtvrté přednášce). Protože v není nulový vektor ($J \neq (0)$), máme rovnost $\det(\gamma E_t - M) = 0$, kde E_t je jednotková matice. Tato rovnost dává pro γ polynomiální rovnici $\gamma^t + \dots = 0$ s koeficienty v R.

Podle třetí vlastnosti Dedekindova oboru leží γ v R, což je spor. Tedy $A = R$ a $IJ = (\alpha)$.

Než pro Dedekindovy obory dokážeme ZVA, odvodíme dva důsledky. A, B, C označují ideály v Dedekindově oboru.

- (krácení ideálů) Z $AB = AC$ plyne $B = C$.
- (dělitelnost ideálů) Pro dané A a B existuje C tak, že $A = BC$, právě když $A \subset B$.

Vezmeme ideál J tak, že $AJ = (\alpha)$ je hlavní. Pak $(\alpha)B = JAB = JAC = (\alpha)C$ a v $(\alpha)B = (\alpha)C$ už lze hlavní ideál (α) zkrátit na $B = C$. Nechť $A = BC$. Protože $BC \subset B \cap C$, máme $A \subset B$. Naopak, nechť $A \subset B$. Vezmeme ideál J tak, že $BJ = (\alpha)$, a položíme $C = \frac{1}{\alpha}JA$. Patrně $C \subset \frac{1}{\alpha}JB = R$ a C je ideál. Dále $BC = \frac{1}{\alpha}BJA = RA = A$.

- Každý nenulový ideál I v Dedekindově oboru má až na pořadí činitelů jednoznačné vyjádření $I = P_1P_2 \dots P_k$ jako součin prvoideálů. Speciálně to platí pro obory celých čísel O_K číselných těles K.

Existence rozkladu. Pro spor nechť existuje nenulový ideál, který není součinem prvoideálů. Vezmeme maximální takový ideál M vzhledem k inkluzi (noetherovost). Patrně $M \neq R$ (R je totiž prázdným součinem prvoideálů). P buď maximální ideál, tedy prvoideál, obsahující M. Podle druhého důsledku máme $M = PI$ pro nějaký ideál I. Kdyby $I = M$, krácením máme $P = R$, což je spor. Inkluze $M \subset I$ je proto ostrá a I je součinem prvoideálů. Takže i $M = PI$ je součinem prvoideálů, což je spor.

Jednoznačnost rozkladu plyne hned z krácení ideálů: pokud $P_1P_2 \dots P_r = Q_1Q_2 \dots Q_s$ pro nějaké prvoideály P_i a Q_j, pak P_1 dělí součin $Q_1Q_2 \dots Q_s$ a musíme tedy nastat $P_1 = Q_{i_1}$ (viz důkaz druhého lemmatu výše). Prvoideály P_1 a Q_{i_1} na obou stranách rovnosti zkrátíme a pokračujeme stejně dál. Nakonec skončíme u rovnosti $R = R$. Takže $r = s$ a s-tice $Q_1, Q_2, \dots, Q_s$ je permutací r-tice $P_1, P_2, \dots, P_r$.

9. přednáška 6. prosince 2007.

Přednáška odpadla.

10. přednáška 13. prosince 2007. Rozklady prvoideálů v rozšířeních.

Nechť $K \subset L$ je rozšíření číselných těles a $R = O_K \subset S = O_L$ je rozšíření jejich oborů celých čísel. Pro prvoideál P v R—připomínáme, že prvoideálem

rozumíme netriviální prvoideál, různý od (0) a R—uvážíme rozklad jím generovaného ideálu SP v S na prvoideály Q_i v S (Q_i jsou vzájemně různé a exponenty e_i jsou v $\mathbf{N}$):

$$SP = Q_1^{e_1} Q_2^{e_2} \dots Q_r^{e_r}.$$

(SP je nejmenší ideál v S obsahující P a skládá se z konečných součtů typu $s_1 p_1 + \dots + s_k p_k$, $s_i \in S$ a $p_i \in P$.)

- Q buď prvoideál v S, jeden z prvoideálů Q_i. Řekneme, že Q *je nad* P, popřípadě, že P *je pod* Q.

Budeme zkoumat vlastnosti těchto rozkladů P na prvoideály širšího oboru S. Dokážeme o nich pět základních výsledků. Nejprve ale ekvivalentní formulace relace „být nad“, resp. „být pod“.

- Q buď prvoideál v S a P prvoideál v R. Pak: Q je nad $P \iff Q$ dělí $SP \iff PS \subset Q \iff P \subset Q \iff Q \cap K = P \iff Q \cap R = P$.

Tyto ekvivalence ponecháváme jako cvičení.

Uvedeme čtyři ze slíbených základních výsledků o rozkladech

$$SP = Q_1^{e_1} Q_2^{e_2} \dots Q_r^{e_r},$$

pátý až na příští přednášce. Není-li řečeno jinak, K, L, R, S jsou jako výše. Pro prvoideál P v R označíme M_P množinu všech nad ním ležících prvoideálů v S.

- První výsledek. Množiny M_P jsou konečné, neprázdné a disjunktní a tvoří rozklad množiny všech prvoideálů v S, takže každý prvoideál v S leží právě v jedné z nich.

Konečnost M_P je zřejmá. Nechť pro spor $M_P = \emptyset$, to jest $SP = S$, ekvivalentně $1 \in SP$. Podle druhého lemmatu na předchozí přednášce ale existuje takový prvek γ v $K \backslash R$, že $\gamma P \subset R$. Pak $\gamma \in \gamma PS \subset RS = S$, takže γ je celistvé číslo a leží (neboť je v K) i v R, spor. Je-li Q v M_P, máme (podle hořejších ekvivalencí) $Q \cap R = P$, takže Q nemůže ležet v jiné množině $M_{P'}$. Zbývá ukázat, že libovolný prvoideál Q v S leží v nějaké množině M_P. Položíme $P = Q \cap R$. Je jasné, že P je prvoideál, ale je nutné ukázat, že $P \neq R, (0)$. Ovšem $P \neq R$, neboť $1 \notin P$, protože $1 \notin Q$. Pro důkaz, že $P \neq (0)$, vezmeme nenulové α z Q (což lze díky $Q \neq (0)$) a ukážeme, že jeho relativní norma $\gamma = N_K^L(\alpha)$ je nenulový prvek P. Máme

$$\gamma = \prod_{\sigma} \sigma(\alpha) = \alpha \prod_{\sigma \neq id} \sigma(\alpha) = \alpha\beta,$$

kde σ probíhá všechna vnoření L do $\mathbf{C}$ bodově fixující K. Zřejmě $\gamma \neq 0$ a γ je v R (podle vlastností relativní normy). Dále je β celistvé číslo (je součinem celistvých čísel) a leží v L, protože $\beta = \gamma/\alpha$. Takže β leží v S a $\gamma = \alpha\beta \in QS = Q$. Tedy $\gamma \in Q \cap R = P$ a $\gamma \neq 0$.

Pro druhý výsledek uvážíme pro P pod Q faktorokruhy R/P a S/Q. Jsou to konečná tělesa (P a Q jsou prvoideály, takže v Dedekindově oboru maximální

ideály, a konečnost jsme ukázali minule). Dále je těleso R/P prostřednictvím homomorfismu $r+P \mapsto r+S$ injektivně vnořeno do tělesa S/Q (jádro je podle hořejších ekvivalencí $(R \cap Q)+P = P+P = P$), a tak ho můžeme brát jako podtěleso. Máme tak konečné rozšíření konečných těles $R/P \subset S/Q$ stupně

$$f = f(Q|P) := [S/Q : R/P].$$

Tomuto číslu se říká *stupeň setrvačnosti Q nad P*.

- Druhý výsledek. Nechť $SP = Q_1^{e_1}Q_2^{e_2}\dots Q_r^{e_r}$ je rozklad prvoideálu na prvoideály ležící nad ním, $f_i = f(Q_i|P)$ jsou stupně setrvačnosti a $n = [L:K]$. Potom platí identita

$$n = e_1f_1 + e_2f_2 + \ldots + e_rf_r.$$

Dokážeme ji doufejme na příští přednášce.

- Třetí výsledek. Je-li rozšíření $K \subset L$ normální, jsou v $SP = Q_1^{e_1}Q_2^{e_2}\dots Q_r^{e_r}$ všechny exponenty $e_i = e$ stejné a taktéž i stupně setrvačnosti $f_i = f(Q_i|P) = f$. Pak $SP = (Q_1Q_2\dots Q_r)^e$ a $[L:K] = ref$.

Uvážíme $n = [L:K]$ automorfismů σ tělesa L bodově fixujících K a ukážeme, že tranzitivně operují na množině M_P (prvoideálů nad P). Pak pro libovolné dva prvoideály Q a Q' nad P existuje takové σ, že $\sigma(Q) = Q'$. Protože $\sigma(S) = S$ a $\sigma(P) = P$, aplikací σ na rozklad $SP = Q_1^{e_1}Q_2^{e_2}\dots Q_r^{e_r}$ máme

$$SP = \sigma(S)\sigma(P) = \sigma(SP) = \sigma(Q_1^{e_1}Q_2^{e_2}\dots Q_r^{e_r}) = \sigma(Q_1)^{e_1}\sigma(Q_2)^{e_2}\dots\sigma(Q_r)^{e_r}.$$

Vzhledem k jednoznačnosti rozkladu SP na prvoideály v S máme $e(Q'|P) = e(\sigma(Q)|P) = e(Q|P)$. Automorfismus σ pak zprostředkuje i izomorfismus těles S/Q a S/Q'. Tedy i $f(Q|P) = [S/Q : R/P] = [S/Q' : R/P] = f(Q'|P)$.

Zbývá dokázat existenci σ posílajícího Q na Q'. Předpokládejme pro spor, že $Q' \neq \sigma(Q)$ pro každé σ. Díky čínské větě o zbytku potom existuje α z Q', které není ani v jednom prvoideálu $\sigma(Q)$ (α vezmeme jako řešení soustavy kongruencí $\alpha \equiv 0 \bmod Q'$, $\alpha \equiv 1 \bmod \sigma(Q)$). Hodnota relativní normy

$$\gamma = N_K^L(\alpha) = \prod_\sigma \sigma(\alpha) = \alpha \prod_{\sigma \neq id} \sigma(\alpha)$$

leží v P, protože γ je v R i v Q' (α násobíme prvkem S). Ovšem pro každé σ je $\alpha \notin \sigma(Q)$, tedy i $\sigma^{-1}(\alpha) \notin Q$ a $\sigma(\alpha) \notin Q$ (když σ probíhá $\mathrm{Gal}(L/K)$, probíhá ji i σ^{-1}). Pak ale, protože Q je prvoideál,

$$\gamma = \prod_\sigma \sigma(\alpha) \notin Q,$$

což je spor s $\gamma \in P = Q \cap R$.

Řekneme, že (K, L, R, S jsou opět jako výše) prvoideál P v R *se štěpí* v S (nebo v L), pokud pro nějaký prvoideál Q nad P máme $e(Q|P) \geq 2$. Jinak

řečeno, rozklad SP na prvoideály v S není bezčtvercový. Jak uvidíme, existuje jen konečně mnoho prvoideálů v R štěpících se v S a stačí to dokázat pro $K = \mathbf{Q}$. Skoro všechny prvoideály v R tedy mají v S bezčtvercový rozklad $SP = Q_1 Q_2 \dots Q_r$.

- Čtvrtý výsledek. Uvažme rozšíření číselných těles $\mathbf{Q} \subset K$ a jejich oborů celých čísel $\mathbf{Z} \subset R = O_K$. Pak pro prvočísla p v $\mathbf{Z}$ máme implikaci

$$p\mathbf{Z} \text{ se štěpí v } R \Rightarrow p \text{ dělí } \mathrm{disc}(R).$$

Nechť se $p\mathbf{Z}$ štěpí v R, takže (po případném přečíslování prvoideálů nad $p\mathbf{Z}$) máme rozklad $pR = P_1^{e_1} P_2^{e_2} \dots P_r^{e_r}$ s $e_1 \geq 2$. Vezmeme prvek

$$\alpha \in P_1^{e_1-1} P_2^{e_2} \dots P_r^{e_r} \setminus P_1^{e_1} P_2^{e_2} \dots P_r^{e_r} = P_1^{e_1-1} P_2^{e_2} \dots P_r^{e_r} \setminus pR.$$

Prvek α leží v každém P_i nad $p\mathbf{Z}$, ale ne v pR. Vyjádříme ho jako lineární kombinaci $\alpha = m_1\alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n$, $m_i \in \mathbf{Z}$, prvků celistvé báze oboru R (zde $n = [K : \mathbf{Q}]$). Protože $\alpha \notin pR$, ne všechny m_i jsou násobky p, např. m_1 není dělitelné p. Podle transformačního vzorce pro diskriminanty n-tic pak máme

$$\mathrm{disc}(\alpha, \alpha_2, \dots, \alpha_n) = m_1^2 \cdot \mathrm{disc}(\alpha_1, \alpha_2, \dots, \alpha_n) = m_1^2 \cdot \mathrm{disc}(R).$$

Protože p nedělí m_1, stačí ukázat, že p dělí celé číslo $\mathrm{disc}(\alpha, \alpha_2, \dots, \alpha_n)$.

Toto celé číslo je čtverec determinantu $n \times n$ matice $M = (\sigma_i(\beta_j))_{i,j=1}^n$, kde $\sigma_1, \dots, \sigma_n$ jsou všechna vnoření K do $\mathbf{C}$ a $\beta_1 = \alpha, \beta_2 = \alpha_2, \dots, \beta_n = \alpha_n$. Máme

$$\det(M) = \sum \pm \sigma_{i_1}(\alpha)\sigma_{i_2}(\alpha_2) \dots \sigma_{i_n}(\alpha_n),$$

kde sčítáme přes všech $n!$ permutací $i_1, \dots, i_n$ čísel $1, \dots, n$. Když $\mathbf{Q} \subset K$ není normální rozšíření, octnou se některé hodnoty $\sigma_i(\beta_j)$ mimo K a z hlediska K a ideálů P_i o nich nelze nic říci. Přejdeme proto k dalšímu rozšíření $\mathbf{Q} \subset K \subset L$, kde $\mathbf{Q} \subset L$ je normální (viz výsledek na 4. přednášce). Každé vnoření σ_i rozšíříme na automorfismus L.

Nechť Q je nějaký pevný prvoideál v $S = O_L$ ležící nad $p\mathbf{Z}$. Když ukážeme, že $\sigma_i(\alpha)$ je v Q pro každé i, budeme hotovi. Každý součin $\sigma_{i_2}(\alpha_2) \dots \sigma_{i_n}(\alpha_n)$ je v S (je to celistvé číslo ležící v L), a tak je každý sčítanec $\det(M)$ i $\det(M)$ sám a $\det(M)^2$ v Q. Pak

$$\mathrm{disc}(\alpha, \alpha_2, \dots, \alpha_n) = \det(M)^2 \in Q \cap \mathbf{Z} = p\mathbf{Z}$$

a p dělí $\mathrm{disc}(\alpha, \alpha_2, \dots, \alpha_n)$ a tedy i $\mathrm{disc}(R)$.

Ovšem $\sigma_i(\alpha) \in Q$ je ekvivalentní s $\alpha \in \sigma_i^{-1}(Q)$. Zobrazení σ_i^{-1} je automorfismus z $\mathrm{Gal}(L/\mathbf{Q})$ (σ_i^{-1} ale může být různé od všech σ_j), takže $\sigma_i^{-1}(Q)$ je prvoideál v S ležící nad $p\mathbf{Z}$. Průnik $\sigma_i^{-1}(Q) \cap R$ je prvoideál v R ležící nad $p\mathbf{Z}$, takže $\sigma_i^{-1}(Q) \cap R = P_j$ pro nějaké j. Tedy $\alpha \in \sigma_i^{-1}(Q) \cap R$, protože α je ve všech prvoideálech P_j. Důkaz je úplný.

Ze čtvrtého výsledku plyne hned toto.

- Nechť $R \subset S$ jsou obory celých čísel číselných těles $K \subset L$. Jen konečně mnoho prvoideálů v R se štěpí v S.

Nechť se tedy P štěpí v S, Q je prvoideál v S s $e(Q|P) \geq 2$ a p je (jednoznačně určené) prvočíslo v $\mathbf{Z}$ ležící pod P. Pak $e(Q|p\mathbf{Z}) = e(Q|P)e(P|p\mathbf{Z}) \geq 2$. Takže se $p\mathbf{Z}$ štěpí v S a podle čtvrtého výsledku p dělí $\mathrm{disc}(S)$. Máme tak jen konečně mnoho prvočísel p (totiž prvočinitele $\mathrm{disc}(S)$) ležících pod prvoideály v R štěpícími se v S. Nad každým z nich ale leží jen konečně mnoho prvoideálů v R, takže množina prvoideálů R štěpících se v S je konečná.

11. přednáška 20. prosince 2007. Rozklady prvoideálů v rozšířeních.

Důkaz druhého výsledku. Dokážeme *n-e-f identitu*

$$n = e_1 f_1 + e_2 f_2 + \ldots + e_r f_r,$$

kde $n = [L : K]$ a $e_i = e(Q_i|P), f_i = f(Q_i|P)$ jsou indexy štěpení a stupně setrvačnosti prvoideálů v S ležících nad prvoideálem P v R, tedy

$$PS = Q_1^{e_1} Q_2^{e_2} \ldots Q_r^{e_r}$$

a $f_i = [S/Q_i : R/P]$, přičemž $R \subset S$ jsou obory celých čísel číselných těles $K \subset L$.

Tuto identitu budeme dokazovat současně s následujícími třemi vlastnostmi normy ideálu.

- Pro nenulový ideál I v $R = O_K$ definujeme $\|I\| := |R/I|$ (jak víme, tento faktorokruh je konečný, protože $I \cap \mathbf{N} \neq \emptyset$). Pak
  1. $\|IJ\| = \|I\| \cdot \|J\|$ pro každé dva takové ideály,
  2. $\|IS\| = \|I\|^n$ (první norma je v S, druhá v R) a
  3. pro každý nenulový prvek α v R máme $\|\alpha R\| = |N(\alpha)| = |N_{\mathbf{Q}}^K(\alpha)|$.

Multiplikativita normy ideálu 1. Pro nesoudělné ideály I a J, tedy $I + J = R$ a $I \cap J = IJ$, plyne hned z čínské věty o zbytku, podle níž $R/IJ \cong R/I \times R/J$. Pro obecný případ stačí ještě dokázat, že

$$\|P^m\| = \|P\|^m$$

pro každý prvoideál P v R. Pro libovolný nenulový ideál I v R a jeho rozklad na prvoideály $I = P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k}$ pak máme

$$\|I\| = \|P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k}\| = \|P_1\|^{a_1} \|P_2\|^{a_2} \ldots \|P_k\|^{a_k},$$

což (spolu s jednoznačností rozkladu na prvoideály) dává multiplikativitu $\|\cdot\|$ pro každé dva ideály.

Pro ideály $I \subset J \subset R$ máme izomorfismus $R/I \cong R/J \times J/I$. Tedy

$$\|P^m\| = |R/P^m| = |R/P| \cdot |P/P^2| \cdot \ldots \cdot |P^{m-1}/P^m|.$$

Protože $\|P\| = |R/P|$, stačí dokázat, že $|P^k/P^{k+1}| = |R/P|$ pro každé k. Dokážeme izomorfismus $R/P \cong P^k/P^{k+1}$. Vezmeme $\alpha \in P^k \backslash P^{k+1}$, pak $a + P \mapsto \alpha a + \alpha P$ je izomorfismus mezi $R/P \cong \alpha R/\alpha P$ (zde stačí, že $\alpha \neq 0$). Protože $\alpha R \subset P^k$, zobrazení $a \mapsto a + P^{k+1}$ je homomorfismus mezi αR a P^k/P^{k+1}, s jádrem $\alpha R \cap P^{k+1} = \alpha P$ a obrazem $(\alpha R + P^{k+1})/P^{k+1} = P^k/P^{k+1}$ (první je NSN a druhé NSD ideálů αR a P^{k+1}, a nejvyšši mocnina P dělící αR je P^k). Podle věty o homomorfismu máme $\alpha R/\alpha P \cong P^k/P^{k+1}$. Složením obou izomorfismů máme $R/P \cong P^k/P^{k+1}$. Tím je dokázána multiplikativita normy ideálu.

Důkaz druhého výsledku pro $K = \mathbf{Q}$. Pak $P = p\mathbf{Z}$ pro nějaké prvočíslo p v $\mathbf{N}$. Víme, že $\|pS\| = p^n$ (protože S má celistvou bázi o n prvcích). Aplikací normy na rozklad $pS = Q_1^{e_1} \ldots Q_r^{e_r}$ díky multiplikativité máme

$$p^n = \|pS\| = \prod_{i=1}^{r} \|Q_i\|^{e_i} = \prod_{i=1}^{r} (p^{f_i})^{e_i} = p^{e_1 f_1 + \ldots + e_r f_r}$$

($\|Q_i\| = |S/Q_i|$, S/Q_i obsahuje $R/P = \mathbf{Z}/p\mathbf{Z}$ jako podtěleso, přičemž $f_i = [S/Q_i : \mathbf{Z}/p\mathbf{Z}]$, a $|\mathbf{Z}/p\mathbf{Z}| = p$). Takže $n = e_1 f_1 + \ldots + e_r f_r$.

Vlastnost normy ideálu 2. Rovnost $\|IS\| = \|I\|^n$ stačí dokázat pro prvoideál $I = P$, obecně plyne rozkladem na prvoideály. Okruh S/PS obsahuje R/P jako podtěleso (prostřednictvím monomorfismu $a + P \mapsto a + PS$) a S/PS je vektorový prostor nad R/P. Ukážeme, že má dimenzi $n = [L : K]$.

Nejprve ukážeme, že S/PS má nad R/P dimenzi nejvýše n.

12. přednáška 3. ledna 2008. Grupa tříd ideálů.

K je číselné těleso stupně n nad $\mathbf{Q}$ a $R = O_K$ jeho obor celých čísel.

- Množina tříd ekvivalence (nenulových) ideálů podle relace

$$I \sim J \iff aI = bJ, \text{ pro nějaké } a, b \in R^*,$$

je vzhledem k operaci násobení ideálů konečná Abelova grupa.

Nejprve ověříme, že $\sim$ je relace ekvivalence. Reflexivita a symetrie jsou zřejmé, tranzitivita víceméně též: $aI = bJ$ a $cJ = dK$ dávají $acI = bcJ = bdK$. Dále je $\sim$ kongruence vzhledem k násobení ideálů: $aI = bJ$ a $cK = dL$ dávají $acIK = (aI)(cK) = (bJ)(dL) = bdJL$. Asociativita a komutativita násobení ideálů a tedy i jejich tříd jsou zřejmé. Ukážeme, že množina všech hlavních ideálů v R je třída ekvivalence a že je v grupě tříd neutrálním prvkem. To druhé je jasné: $(a)I = aI$, takže $(a)I \sim I$. Dále $(a) \sim (b)$ pro každé dva prvky a, b v R^*,

protože $b(a) = (ab) = a(b)$. Zbývá ukázat, že ideál ekvivalentní hlavnímu ideálu je hlavní. Z $aI = bR$ pro nenulové a, b v R máme, že $b = ac$ pro nějaké c v I. Pro každé x v I tak $ax = by = acy$ pro nějaké y v R a vidíme, že $x = cy$ a $I = (c)$. Konečně, jak už jsme dříve ukázali, pro každý nenulový ideál I v R existuje ideál J, že IJ je hlavní ideál. Každá třída ideálů má tedy inverzní prvek.

Nyní dokážeme, že tato grupa je konečná, protože v každém R existuje jen konečně mnoho tříd ideálů. Dokážeme to ve třech krocích.

- 1. Existuje konstanta $\lambda > 0$ (závisející jen na K) tak, že každý nenulový ideál I v R obsahuje nenulový prvek α splňující

$$|N(\alpha)| \leq \lambda \|I\|.$$

2. Pro tutéž konstantu $\lambda > 0$ platí, že každá třída ideálů C obsahuje ideál J splňující $\|J\| \leq \lambda$.
3. Počet tříd ideálů je konečný.

1. Nechť $\alpha_1, \ldots, \alpha_n$ je celistvá báze R a $\sigma_1, \ldots, \sigma_n$ jsou vnoření K do $\mathbf{C}$. Ukážeme, že za λ lze vzít

$$\lambda = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i(\alpha_j)|.$$

Buď dán ideál $I \neq (0)$. Vezmeme (jednoznačně určené) m v $\mathbf{N}$ tak, že $m^n \leq \|I\| < m^{n+1}$. Protože je v množině

$$\{m_1\alpha_1 + \ldots + m_n\alpha_n \mid m_i \in \mathbf{Z}, 0 \leq m_i < m\}$$

$m^{n+1} > \|I\| = |R/I|$ (po dvou různých) prvků, některé dva z nich jsou kongruentní modulo I. Jejich odečtením dostaneme nenulový prvek

$$\alpha = m_1\alpha_1 + \ldots + m_n\alpha_n, \ m_i \in \mathbf{Z}, |m_i| \leq m$$

ležící v I. Pro jeho normu máme

$$|N(\alpha)| = |\sigma_1(\alpha)| \ldots |\sigma_n(\alpha)| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} |m_j| \cdot |\sigma_i(\alpha_j)| \leq m^n \lambda \leq \lambda \|I\|.$$

2. Buď dána třída ideálů C. Vezmeme inverzní třídu C^{-1}, v ní libovolný ideál I a v něm, podle bodu 1, nenulový prvek α splňující $|N(\alpha)| \leq \lambda \|I\|$. Protože $(\alpha) \subset I$, ideál I dělí hlavní ideál (α) a máme rovnost $(\alpha) = IJ$ pro nějaký ideál J. Odtud plyne (vzhledem k $I \in C^{-1}$), že $J \in C$. Multiplikativita normy ideálů dává

$$\lambda \|I\| \geq |N(\alpha)| = \|(\alpha)\| = \|I\| \cdot \|J\|, \quad \text{takže} \quad \|J\| \leq \lambda.$$

3. Podle bodu 2 z každé třídy ideálů C můžeme vybrat reprezentanta J s malou normou, $\|J\| \leq \lambda$. Uvidíme, že pro každou konstantu $c > 0$ jen konečně mnoho ideálů má normu nejvýše c. Tím bude konečnost počtu tříd dokázaná.

Vzhledem k jednoznačnému rozkladu ideálů na prvoideály stačí dokázat, že jen konečně mnoho prvoideálů P má normu nejvýše c (v rozkladu $I = P_1^{e_1} \dots P_r^{e_r}$ multiplikativita normy dává pro $\|I\| \leq c$ odhady $\|P_i\| \leq c$ a $e_i \leq \log_2 c$, takže na výběr je jen konečně mnoho množin $\{P_1, \dots, P_r\}$ a exponentů e_i). Ovšem každý prvoideál P v R leží nad jednoznačně určeným prvočíslem p v $\mathbf{Z}$, $P \cap \mathbf{Z} = p\mathbf{Z}$, a z $\|P\| \leq c$ plyne i $p \leq c$ (protože $\|P\| = |R/P| = |\mathbf{Z}/p\mathbf{Z}|^f = p^f \geq p$, kde f je stupeň setrvačnosti P nad p). Prvočísel nepřesahujících c je jen konečně mnoho a nad každým z nich leží jen konečně mnoho prvoideálů P, takže P s $\|P\| \leq c$ je konečně mnoho a stejně tak všech ideálů I s $\|I\| \leq c$.

Grupu tříd ideálů využijeme při nalezení celočíselných řešení jedné diofantické rovnice.

- Rovnice $x^2 + 5 = y^3$ nemá v oboru celých čísel žádné řešení.

13. přednáška 10. ledna 2008. Grupa jednotek.

V poslední přednášce určíme grupu jednotek oboru celých čísel číselného tělesa.

- *Dirichletova věta o jednotkách.* Nechť K je číselné těleso s r reálnými a $2s$ nereálnými vnořeními do $\mathbf{C}$. Grupa jednotek $(U, \cdot)$ oboru celých čísel $R = O_K$ tělesa K je izomorfní součinu $W \times V$, kde W je konečná cyklická grupa a $V = \mathbf{Z}^{r+s-1}$ je volná Abelova grupa ranku $r + s - 1$. Podrobněji, v U existuje $(r + s - 1)$-tice tzv. *fundamentálních jednotek* $u_1, u_2, \dots, u_t$, $t = r + s - 1$, generujících U:

  $$U = \{\zeta u_1^{a_1} u_2^{a_2} \dots u_t^{a_t} \mid \zeta \in J \cap K, a_i \in \mathbf{Z}\},$$

  kde J je množina všech komplexních odmocnin z 1. Korespondence $U \leftrightarrow (J \cap K) \times \mathbf{Z}^t$, $u \leftrightarrow (\zeta, a_1, \dots, a_t)$ je navíc bijekce.

Důkaz věty využívá multiplikativně-aditivní homomorfismus

$$\mathrm{Log}: \ K^* \to \mathbf{R}^{r+s}$$

definovaný jako

$$\mathrm{Log}(a) = (\log|\sigma_1(a)|, \dots, \log|\sigma_r(a)|, \log|\tau_1(a)|^2, \dots, \dots, \log|\tau_s(a)|^2),$$

kde $\sigma_1, \dots, \sigma_r$ jsou reálná a $\tau_1, \overline{\tau_1}, \dots, \tau_s, \overline{\tau_s}$ nereálná vnoření K do $\mathbf{C}$. Zobrazení Log má tyto tři vlastnosti:

- 1. Pro $a, b \in K^*$ máme $\mathrm{Log}(ab) = \mathrm{Log}(a) + \mathrm{Log}(b)$, takže

  $$\mathrm{Log} : (K^*, \cdot) \to (\mathbf{R}^{r+s}, +)$$

  je homomorfismus grup.
  2. Obraz jednotek $\mathrm{Log}(U)$ je obsažený v nadrovině

  $$H = \{x \in \mathbf{R}^{r+s} \mid x_1 + x_2 + \ldots + x_{r+s} = 0\}.$$

3. Každá omezená podmnožina $X \subset \mathbf{R}^{r+s}$ má v R konečný vzor: množina $\mathrm{Log}^{-1}(X) \cap R$ je konečná.

Vlastnost 1 je důsledkem identit $\log(xy) = \log x + \log y$ pro $x, y > 0$, $\sigma(ab) = \sigma(a)\sigma(b)$ a $|\tau|^2 = \tau\overline{\tau}$ pro a, b v K a σ, τ vnoření K do $\mathbf{C}$. Vlastnost 2 plyne opět z definice Log a toho, že $|N(a)| = |\sigma_1(a)| \dots |\tau_s(a)|^2 = 1$ pro každou jednotku a v U. Vlastnost 3 plyne z toho, že $|\mathrm{Log}^{-1}(X) \cap R| = |Y \cap \Lambda_R|$, kde $Y \subset \mathbf{R}^n = \mathbf{R}^{r+2s}$ je vzor $X \subset \mathbf{R}^{r+s}$ v zobrazení

$$(x_1, x_2, \dots, x_n) \mapsto (\log|x_1|, \dots, \log|x_r|, \log(x_{r+1}^2 + x_{r+2}^2), \dots, \log(x_{n-1}^2 + x_n^2))$$

a $\Lambda_R = F(R)$ je mřížka v $\mathbf{R}^n$ odpovídající R. X je omezená, omezená je tedy i Y a průnik $Y \cap \Lambda_R$ je konečný, v důsledku následující charakterizace mřížek v řeči topologických grup.

- Množina Λ v $\mathbf{R}^n$ je mřížka, právě když je Λ *diskrétní podgrupa* aditivní grupy $(\mathbf{R}^n, +)$: $x - y \in \Lambda$ pro každé dva prvky $x, y \in \Lambda$ a existuje takové $\delta > 0$, že $\Lambda \cap \{x \in \mathbf{R}^n \mid \|x\| < \delta\} = \{(0, 0, \dots, 0)\}$.

Poslední podmínka diskrétnosti Λ ekvivalentně znamená, že pro každou omezenou množinu X v $\mathbf{R}^n$ je průnik $\Lambda \cap X$ konečný. Důkaz přenecháváme posluchači jako cvičení.

Vezmeme zúžení Log na U, které označíme Log_U:

$$\mathrm{Log}_U : U \to H \subset \mathbf{R}^{r+s}$$

je opět multiplikativně-aditivní homomorfismus. Máme

$$U/W \cong V \quad \text{a} \quad U \cong W \times V,$$

kde $W = \mathrm{Log}_U^{-1}(\{(0, 0, \dots, 0)\})$ je jádro a $V = \mathrm{Log}_U(U)$ obraz homomorfismu Log_U. Podíváme se na W. Podle vlastnosti 3 to je konečná multiplikativní podgrupa U. Odtud už snadno plyne, že W se skládá z odmocnin z 1 ležících v K a že W je cyklická. (Každý prvek ve W má konečný řád, je to tedy odmocnina z 1. Naopak každá odmocnina z 1 ležící v K leží i ve W. Dále je W generovaná prvkem $w \in W \backslash \{1\}$ s nejmenším argumentem $\arg(w) > 0$.) Podíváme se na obraz V. Je to diskrétní podgrupa $(\mathbf{R}^{r+s}, +)$ (V je jistě podgrupa $(R^{r+s}, +)$, dokonce $(H, +)$, a podle vlastnosti 3 je pro každou omezenou $X \subset \mathbf{R}^{r+s}$ průnik $\mathrm{Log}_U(U) \cap X$ konečný.) Podle hořejší charakterizace mřížek je tedy V mřížka v $\mathbf{R}^{r+s}$ a

$$\mathrm{Log}_U(U) = V = \{a_1 v_1 + \dots + a_k v_k \mid a_i \in \mathbf{Z}\}$$

pro nějakých k vektorů $v_1, \dots, v_k$ z $\mathbf{R}^{r+s}$ lineárně nezávislých nad $\mathbf{R}$. Protože $V \subset H$, kde H je nadrovina, máme $k \leq r + s - 1$. Zbývá dokázat, že V má nejvyšší možnou dimenzi $r + s - 1$. Ukážeme, že v U leží $t = r + s - 1$ jednotek $u_1, \dots, u_t$, které jsou muliplikativně nezávislé—$u_1^{a_1} u_2^{a_2} \dots u_t^{a_t} = 1$, $a_i \in \mathbf{Z}$, pouze pro všechny a_i rovné nule. Dokážeme více: v U nalezneme $r + s - 1$ jednotek u_i, jejichž obrazy $\mathrm{Log}(u_i)$ v $\mathbf{R}^{r+s}$ jsou lineárně nezávislé nad $\mathbf{R}$. Tím bude důkaz

Dirichletovy věty hotov (bijektivnost korespondence $u \leftrightarrow (\zeta, a_1, \ldots, a_t)$ plyne z mupliplikativní nezávislosti fundamentálních jednotek).

Tyto muliplikativně nezávislé jednotky nalezneme ve třech krocích.

- 1. Existuje konstanta $c > 0$ závisející pouze na tělese K, že pro každé α v R^* a každé k v $\mathbf{N}$, $1 \leq k \leq r+s$, existuje β v R^*, že

  $$|N(\beta)| \leq c \quad \text{a} \quad \mathrm{Log}(\beta) < \mathrm{Log}(\alpha)$$

  v každé souřadnici, s možnou výjimkou k-té.
  2. Pro každé k v $\mathbf{N}$, $1 \leq k \leq r+s$, existuje taková jednotka u v U, že

  $$\mathrm{Log}(u) < (0, 0, \ldots, 0)$$

  v každé souřadnici, až na k-tou (která je nutně kladná).
  3. V U existuje $t = r+s-1$ jednotek $u_1, u_2, \ldots, u_t$, jejichž logaritmické souřadnice $\mathrm{Log}(u_i)$ jsou lineárně nezávislé nad $\mathbf{R}$.

1. Buďte dány k a $\alpha \in R^*$. Nechť $\mathrm{Log}(\alpha) = (a_1, a_2, \ldots, a_{r+s})$. Fixujeme kladné konstanty $c_1, c_2, \ldots, c_{r+s}$ tak, že $0 < c_i < \mathrm{e}^{a_i}$ pro každé i různé od k a $c_k > 0$ je dostatečně velké. V $\mathbf{R}^n$ vezmeme konvexní množinu E danou nerovnostmi

$$|x_1| \leq c_1, \ldots, |x_r| \leq c_r \quad \text{a} \quad x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \ldots, x_{r+2s-1}^2 + x_{r+2s}^2 \leq c_{r+s}.$$

E je souměrná podle počátku a má objem $\mathrm{vol}(E) = 2^r \pi^s c_1 c_2 \ldots c_{r+s}$. Vezmeme $c_k > 0$ tak velké, že

$$\mathrm{vol}(E) \geq 2^n \mathrm{vol}(\Lambda_R) = 2^{n-s} \sqrt{|\mathrm{disc}(R)|},$$

kde $\Lambda_R \subset \mathbf{R}^n$ je mřížka odpovídající R. Konstantu $c_k > 0$ stačí tedy zvolit tak, že

$$c_1 c_2 \ldots c_{r+s} = (2/\pi)^s \sqrt{|\mathrm{disc}(R)|}.$$

Podle Minkowského věty pak v Λ_R existuje nenulový vektor v ležící i v E. Nechť β je prvek R odpovídající v. Patrně $\beta \neq 0$,

$$\mathrm{Log}(\beta) \leq (\log c_1, \ldots, \log c_{r+s}) < (a_1, \ldots, a_{r+s}) = \mathrm{Log}(\alpha)$$

v každé souřadnici kromě snad k-té, a

$$\begin{aligned} |N(\beta)| &= |\sigma_1(\beta)| \ldots |\sigma_r(\beta)| \cdot |\tau_1(\beta)|^2 \ldots |\tau_s(\beta)|^2 \\ &\leq c_1 \ldots c_{r+s} \\ &= (2/\pi)^s \sqrt{|\mathrm{disc}(R)|}. \end{aligned}$$

Jako výchozí konstantu lze tedy zvolit

$$c = (2/\pi)^s \sqrt{|\mathrm{disc}(R)|}.$$

2. Pro dané k a libovolný výchozí prvek $\alpha_1 \in R^*$ podle bodu 1 sestrojíme takovou posloupnost $\alpha_1, \alpha_2, \ldots$ v R^*, že pro každé i platí $|N(\alpha_i)| \leq c$ a

$\mathrm{Log}(\alpha_{i+1}) < \mathrm{Log}(\alpha_i)$ v každé souřadnici kromě k-té. Víme, že $\|(\alpha_i)\| = |N(\alpha_i)|$ a že v R je jen konečně mnoho ideálů s normou menší než pevná konstanta. Proto existují indexy $j < k$ tak, že $(\alpha_j) = (\alpha_k)$, to jest $\alpha_j = u\alpha_k$, kde u je jednotka v U. Její logaritmické souřadnice jsou

$$\mathrm{Log}(u) = \mathrm{Log}(\alpha_j) - \mathrm{Log}(\alpha_k) < (0, 0, \ldots, 0)$$

až na k-tou.

3. Podle bodu 2 vezmeme v U takové jednotky $u_1, u_2, \ldots, u_{r+s}$, že $\mathrm{Log}(u_i) < (0, 0, \ldots, 0)$ v každé souřadnici až na i-tou, která je nutně kladná, protože součet všech souřadnic je nulový. Uvidíme, že $(r + s) \times (r + s)$ matice

$$A = (\mathrm{Log}(u_i))_{i=1}^{r+s} = (a_{i,j})_{i,j=1}^{r+s}$$

má hodnost $r + s - 1$, protože jejích prvních $r + s - 1$ sloupců je lineárně nezávislých. Připomínáme, že A má na hlavní diagonále kladná čísla, mimo ni záporná čísla a řádkové součty jsou nulové. Pro spor vezmeme lineární kombinaci prvních $r + s - 1$ sloupců s koeficienty $d_1, \ldots, d_{r+s-1}$, ne všemi nulovými, která je nulový vektor. Vynásobením této kombinace vhodným číslem dosáhneme, že $|d_i| \leq 1$ pro každé i a $d_k = 1$ pro nějaké k, $1 \leq k \leq r + s - 1$. V k-tém řádku lineární kombinace pak ale máme spor:

$$0 = \sum_{k=1}^{r+s-1} d_j a_{k,j} \geq \sum_{k=1}^{r+s-1} a_{k,j} > \sum_{k=1}^{r+s} a_{k,j} = 0.$$

Prvních $r + s - 1$ sloupců matice A je tedy lineárně nezávislých a seznam $u_1, u_2, \ldots, u_{r+s}$ obsahuje $r + s - 1$ jednotek s lineárně nezávislými logaritmickými souřadnicemi. Nalezli jsme fundamentální jednotky a důkaz Dirichletovy věty je hotový.