TEORIE ČÍSEL

Pomocný text k přednášce pro postgraduální studenty
konané ve školním roce 1997/98.

Radan Kučera

Vysázeno systémem $\mathcal{AMS}$-TEX

1. Algebraická rozšíření

(dle Boreviče-Šafareviče, alg. doplněk, §2)

Obsahuje-li těleso K podtěleso k, hovoříme o rozšíření K/k. Jsou-li do sebe vložena tělesa tři: $k \subseteq L \subseteq K$, nazývá se L mezitěleso rozšíření K/k.

Každé rozšíření těles K/k lze studovat také jako vektorový prostor K nad k.

Definice. Rozšíření K/k se nazývá konečné, je-li K konečněrozměrný vektorový prostor nad k. Dimenze K nad k se nazývá stupěň rozšíření a značí se $[K : k]$. Libovolná baze K nad k se nazývá baze rozšíření K/k.

Věta 1. Nechť L je mezitěleso rozšíření K/k. Rozšíření K/k je konečné, právě když jsou obě rozšíření K/L i L/k konečná. V tomto případě platí

$$[K : k] = [K : L][L : k].$$

Důkaz. Nechť $\alpha_1, \ldots, \alpha_m$ je baze K/L, $\beta_1, \ldots, \beta_n$ baze L/k. Snadno se dokáže, že součiny $\alpha_i\beta_j$, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, n\}$ tvoří bazi K/k.

Nechť K/k je rozšíření. Prvek $\alpha \in K$ se nazývá algebraický nad k, existuje-li nenulový polynom $f(t) \in k[t]$, jehož kořenem je α. Mezi všemi normovanými polynomy z $k[t]$, jejichž kořenem je α, vyberme polynom $\varphi_\alpha(t)$ nejmenšího stupně. Protože každý takový $f(t)$ je dělitelný polynomem $\varphi_\alpha(t)$ (v opačném případě by nenulový zbytek po dělení $f(t)$ polynomem $\varphi_\alpha(t)$ měl kořen α a stupeň menší než $\varphi_\alpha(t)$), je touto podmínkou polynom $\varphi_\alpha(t)$ určen jednoznačně. Nazývá se minimální polynom prvku α nad k. Minimální polynom je vždy ireducibilní, neboť z rozkladu $\varphi_\alpha(t) = g(t)h(t)$ plyne, že α je kořenem buď $g(t)$ nebo $h(t)$. Libovolný prvek $\alpha \in k$ je algebraický nad k, jeho minimální polynom je $t - \alpha$. Prvek $\xi \in K$, který není algebraický nad k, se nazývá transcendentní nad K.

Příklad. Nalezněte minimální polynom φ_α čísla $\alpha = \sqrt{2 + \sqrt{2}}$ nad $\mathbb{Q}$.

Řešení. Platí $(\alpha^2 - 2)^2 = 2$. Je tedy α kořenem polynomu $x^4 - 4x^2 + 2$, který je ireducibilní podle Eisensteinova kriteria, proto je to hledaný minimální polynom.

Cvičení 1. Nalezněte minimální polynom φ_α čísla $\alpha = \sqrt{2} + \sqrt{3}$.

Rozšíření K/k se nazývá algebraické, je-li každé $\alpha \in K$ algebraické nad k.

Věta 2. Libovolné konečné rozšíření K/k je algebraické.

Důkaz. Nechť $n = [K : k]$. Libovolných $n + 1$ prvků tělesa K pak musí být k-lineárně závislých, proto pro libovolné $\alpha \in K$ existuje k-lineární závislost mezi prvky $1, \alpha, \alpha^2, \ldots, \alpha^n$, tedy existuje v $k[t]$ nenulový polynom stupně nejvýše n, jehož je α kořenem.

Věta 3. Nechť prvek α rozšíření K/k je algebraický nad k a nechť jeho minimální polynom $\varphi_\alpha(t)$ má stupeň m. Pak prvky $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ jsou k-lineárně nezávislé a všechny jejich k-lineární kombinace $a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}$ s koeficienty z k tvoří mezitěleso, označované $k(\alpha)$. Rozšíření $k(\alpha)/k$ je konečné a má stupeň m.

Důkaz. Zřejmě je popsané $k(\alpha)$ okruh: je-li $r(t)$ zbytek po dělení součinu polynomů $f(t), g(t) \in k[t]$ polynomem $\varphi_\alpha(t)$, pak $r(\alpha) = f(\alpha)g(\alpha)$ a $r(\alpha)$ je uvedeného tvaru. Je-li $f(t) \in k[t]$, $f(\alpha) \neq 0$, pak $f(t)$ a $\varphi_\alpha(t)$ jsou nesoudělné polynomy,

existují tedy z Bezoutovy rovnosti polynomy $g(t), h(t) \in k[t]$ tak, že $f(t)g(t) + \varphi_\alpha(t)h(t) = 1$, odkud $\frac{1}{f(\alpha)} = g(\alpha)$.

Definice. Rozšíření $k(\alpha)/k$ se nazývá jednoduché rozšíření.

Poznámka. Nechť $\alpha_1, \ldots, \alpha_s$ je konečný systém prvků tělesa K, které jsou všechny algebraické nad k; nechť $m_1, \ldots, m_s$ jsou stupně jejich minimálních polynomů vzhledem ke k. Pak množina všech k-lineárních kombinací prvků

$$\alpha_1^{r_1} \ldots \alpha_s^{r_s} \qquad (0 \leq r_1 < m_1, \ldots, 0 \leq r_s < m_s)$$

tvoří mezitěleso rozšíření K/k, které označujeme $k(\alpha_1, \ldots \alpha_s)$. Jde vlastně o těleso $k(\alpha_1) \ldots (\alpha_s)$. Jeho stupeň nad k není větší než $m_1 \ldots m_s$.

Libovolné mezitěleso L rozšíření K/k takové, že L/k je konečné, je možné zapsat ve tvaru $k(\alpha_1, \ldots \alpha_s)$ pro vhodné $\alpha_1, \ldots \alpha_s$.

Věta 4 (obecněji než v B-Š). Nechť $\sigma : k_1 \to k_2$ je izomorfismus těles, K_1/k_1, K_2/k_2 rozšíření těles. Pro i=1,2 nechť je zvolen prvek $\theta_i \in K_i$ algebraický nad k_i, přičemž $\varphi_{\theta_2} = \sigma(\varphi_{\theta_1})$. Pak existuje jediný izomorfismus $\tau : k_1(\theta_1) \to k_2(\theta_2)$ s vlastností $\tau|_{k_1} = \sigma$ a $\tau(\theta_1) = \theta_2$.

Důkaz. Je-li $m = \operatorname{st} \varphi_{\theta_1}$, pak

$$k(\theta_1) = \{a_0 + a_1\theta_1 + \cdots + a_{m-1}\theta_1^{m-1} | a_0, \ldots, a_{m-1} \in k\}$$

přičemž nutně

$$\tau(a_0 + a_1\theta_1 + \cdots + a_{m-1}\theta_1^{m-1}) = \sigma(a_0) + \sigma(a_1)\theta_2 + \cdots + \sigma(a_{m-1})\theta_2^{m-1}.$$

Protože $\varphi_{\theta_2} = \sigma(\varphi_{\theta_1})$, je τ požadovaný izomorfismus.

Doteď byla zkoumána rozšíření, obsažená v nějakém velkém předem daném tělese. Nyní přejděme k otázce konstrukce konečného rozšíření nad fixovaným tělesem k.

Věta 5. Nechť k je těleso. Pro libovolný ireducibilní polynom $\varphi(t)$ nad k stupně n existuje konečné rozšíření K/k stupně n, ve kterém má polynom $\varphi(t)$ kořen. Až na izomorfismus, nechávající prvky k na místě, je toto rozšíření K/k určeno jednoznačně. Je-li $\alpha \in K$, $\varphi(\alpha) = 0$, pak $K = k(\alpha)$.

Důkaz. Je-li $\varphi(t)$ ireducibilní polynom $k[t]$, je hlavní ideál $I = (\varphi(t))$ maximální ideál v $k[t]$, a tedy $K = k[t]/I$ je těleso. Po náležité identifikaci jde o rozšíření k, přičemž $\varphi(t + I) = \varphi(t) + I = 0 + I = 0$. Jednoznačnost plyne z věty 4.

Důsledek. Pro libovolný polynom $f(t) \in k[t]$ existuje rozšíření K/k, ve kterém se $f(t)$ rozkládá na lineární faktory.

Definice. Nechť $f(t) \in k[t]$. Rozšíření K tělesa k se nazývá rozkladové těleso f nad k, jestliže platí

1. f se v K rozkládá na lineární faktory,
2. je-li M mezitěleso K/k takové, že f se v M rozkládá na lineární faktory, pak $M = K$.

Poznámka: Rozkladové těleso f nad k je nad k generováno všemi kořeny f.

Tvrzení o izomorfismu rozkladových těles: Nechť $\sigma : k_1 \to k_2$ je izomorfismus těles, $f_1(t) \in k_1[t]$, $f_2(t) \in k_2[t]$ takové, že $\sigma(f_1) = f_2$. Pro $i = 1, 2$ nechť K_i je rozkladové těleso f_i nad k_i. Pak existuje, ne nutně jediný, izomorfismus $\tau : K_1 \to K_2$ s vlastností $\tau|_{k_1} = \sigma$.

Důkaz plyne indukcí z věty 4.

Těleso, nad kterým neexistují konečná rozšíření stupně většího než 1, se nazývá algebraicky uzavřené.

Definice. Nechť K/k je konečné rozšíření stupně n. Pro libovolné $\alpha \in K$ přiřazení $\xi \mapsto \alpha\xi$ definuje lineární transformaci K (jakožto vektorového prostoru nad k). Charakteristický polynom $f_\alpha(t)$ této lineární transformace se nazývá též charakteristický polynom prvku α vzhledem ke K/k. Je-li $\beta_1, \ldots, \beta_n$ baze rozšíření K/k, a platí-li

$$(*) \qquad \alpha\beta_i = \sum_{j=1}^{n} a_{ij}\beta_j, \qquad a_{ij} \in k,$$

pak dle definice $f_\alpha(t) = \det(tE - (a_{ij}))$, kde E je jednotková matice řádu n. Snadno se ověří, že $f_\alpha(t)$ nezávisí na volbě baze rozšíření K/k.

Věta 6. Nechť K/k je konečné rozšíření, $\alpha \in K$. Charakteristický polynom $f_\alpha(t)$ prvku α vzhledem ke K/k je mocninou jeho minimálního polynomu $\varphi_\alpha(t)$ prvku α nad k.

Důkaz. Nechť $\varphi_\alpha(t) = t^m + c_1 t^{m-1} + \cdots + c_m$. Dle věty 3 je $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$ baze $k(\alpha)/k$. Nechť $\beta_1, \ldots, \beta_s$ je nějaká baze $K/k(\alpha)$. Dle důkazu věty 1 je

$$\beta_1, \alpha\beta_1, \ldots, \alpha^{m-1}\beta_1, \ldots, \beta_s, \alpha\beta_s, \ldots, \alpha^{m-1}\beta_s$$

bazí K/k. Maticí lineární transformace $\xi \mapsto \alpha\xi$ bude v této bazi blokově diagonální matice, mající na diagonále s stejných bloků

$$\begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ -c_m & -c_{m-1} & -c_{m-2} & \ldots & -c_2 & -c_1 \end{pmatrix}.$$

Snadno se spočítá, že charakteristický mnohočlen takového bloku je právě $\varphi_\alpha(t)$. Odtud plyne věta.

Definice. Determinant $\det(a_{ij})$ matice (a_{ij}) z vyjádření (*) se nazývá norma, a její stopa $\mathrm{Sp}(a_{ij}) = \sum_{i=1}^{n} a_{ii}$ se nazývá stopa prvku $\alpha \in K$ vzhledem k rozšíření K/k. Normu a stopu budeme označovat $N_{K/k}(\alpha)$ a $\mathrm{Sp}_{K/k}(\alpha)$.

Snadno se ověří, že $N_{K/k}(\alpha)$ ani $\mathrm{Sp}_{K/k}(\alpha)$ nezávisí na volbě baze $\beta_1, \ldots, \beta_n$ rozšíření K/k. Pro $a \in k$ je matice lineární transformace $\xi \mapsto a\xi$ rovna diagonální matici aE. Proto pro $a \in k$ platí $N_{K/k}(a) = a^n$ a $\mathrm{Sp}_{K/k}(a) = na$. Protože při složení, resp. sečtení, lineárních transformací se jejich matice (ve zvolené pevné bazi) násobí, resp. sčítají, pro libovolné $\alpha, \beta \in K$ platí

$$N_{K/k}(\alpha\beta) = N_{K/k}(\alpha)N_{K/k}(\beta), \qquad \mathrm{Sp}_{K/k}(\alpha\beta) = \mathrm{Sp}_{K/k}(\alpha) + \mathrm{Sp}_{K/k}(\beta).$$

Matici lineární transformace $\xi \mapsto a\alpha\xi$, kde $a \in k$, $\alpha \in K$, je možné z matice lineární transformace $\xi \mapsto \alpha\xi$ získat vynásobením celé matice prvkem a. Proto pro $a \in k$, $\alpha \in K$, platí

$$\mathrm{Sp}_{K/k}(a\alpha) = a\,\mathrm{Sp}_{K/k}(\alpha).$$

Pro $\alpha \neq 0$ je zřejmě zobrazení $\xi \mapsto \alpha\xi$ bijektivní a proto $N_{K/k}(\alpha) \neq 0$. Ukázali jsme, že zobrazení $\alpha \mapsto N_{K/k}(\alpha)$ je homomorfismem multiplikativní grupy $K^\times$ tělesa K do multiplikativní grupy $k^\times$ tělesa k, kdežto zobrazení $\alpha \mapsto \mathrm{Sp}_{K/k}(\alpha)$ je lineární zobrazení K do k (kde K i k chápeme jako vektorové prostory nad k) neboli lineární funkce na vektorovém prostoru K nad k s hodnotami v k.

Věta 7. Nechť M/k je rozšíření, v němž se charakteristický polynom $f_\alpha(t)$ prvku $\alpha \in K$ vzhledem ke konečnému rozšíření K/k zcela rozkládá na lineární faktory:

$$f_\alpha(t) = (t-\alpha_1)\dots(t-\alpha_n).$$

Pak platí

$$N_{K/k}(\alpha) = \prod_{i=1}^{n} \alpha_i, \qquad \mathrm{Sp}_{K/k}(\alpha) = \sum_{i=1}^{n} \alpha_i$$

Důkaz. Je-li $f_\alpha(t) = \det(tE-(a_{ij})) = t^n + a_1 t^{n-1} + \dots + a_n$, pak $a_1 = -\,\mathrm{Sp}(a_{ij})$, $a_n = (-1)^n \det(a_{ij})$. Věta plyne z Viétových vztahů.

Věta 8. V označení věty 7 pro libovolný $\gamma = g(\alpha) \in K$, kde $g(t) \in k[t]$, platí, že jeho charakteristický polynom $f_\gamma(t)$ se v tělese M rozkládá ve tvaru

$$f_\gamma(t) = (t-g(\alpha_1))\dots(t-g(\alpha_n)).$$

Důkaz. Nejprve si všimněme, že z hlavní věty o symetrických polynomech plyne, že každý koeficient polynomu

$$(**) \qquad (t-g(\alpha_1))\dots(t-g(\alpha_n))$$

jakožto hodnota symetrického polynomu s koeficienty v k v prvcích $\alpha_1, \dots, \alpha_n$ patří do k (hodnoty elementárních symetrických polynomů v prvcích $\alpha_1, \dots, \alpha_n$ jsou podle Viétových vztahů až na znaménka koeficienty polynomu $f_\alpha(t) \in k[t]$). Nechť $\varphi_\gamma(t)$ je minimální polynom prvku γ nad k. Jestliže na rovnost $\varphi_\gamma(g(\alpha)) = 0$ aplikujeme izomorfismus $k(\alpha) \to k(\alpha_i)$, při kterém $\alpha \mapsto \alpha_i$ a prvky k zůstávají na místě, dostaneme $\varphi_\gamma(g(\alpha_i)) = 0$. Proto každý z kořenů polynomu (**) je kořenem ireducibilního polynomu $\varphi_\gamma(t)$, odkud plyne, že polynom (**) je mocninou polynomu $\varphi_\gamma(t)$. Nyní stačí užít větu 6 a porovnat stupně polynomů.

Nechť M je mezitěleso konečného rozšíření K/k. Zvolme bazi $\omega_1, \dots, \omega_n$ rozšíření M/k a bazi $\theta_1, \dots, \theta_m$ rozšíření K/M. Pro libovolné $\gamma \in K$ vyjádřeme

$$\gamma\theta_j = \sum_{s=1}^{m} \alpha_{js}\theta_s \qquad \alpha_{js} \in K,$$

$$\alpha_{js}\omega_i = \sum_{r=1}^{n} a_{jsir}\omega_r \qquad a_{jsir} \in k.$$

Protože

$$\gamma\omega_i\theta_j = \sum_{s=1}^{m}\sum_{r=1}^{n} a_{jsir}\omega_r\theta_s,$$

platí $\mathrm{Sp}_{K/k}(\gamma) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{jjii}$. Na druhou stranu také platí

$$\mathrm{Sp}_{M/k}\big(\mathrm{Sp}_{K/M}(\gamma)\big) = \mathrm{Sp}_{M/k}\big(\sum_{j=1}^{n}\alpha_{jj}\big) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{jjii}.$$

Pro libovolné $\gamma \in K$ tedy máme

$$\mathrm{Sp}_{K/k}(\gamma) = \mathrm{Sp}_{M/k}\big(\mathrm{Sp}_{K/M}(\gamma)\big).$$

Poznámka. Analogický vzorec platí také pro normy: je-li M mezitěleso rozšíření K/k, pak pro libovolné $\gamma \in K$ platí $N_{K/k}(\gamma) = N_{M/k}(N_{K/M}(\gamma))$. Důkaz tohoto tvrzení je složitější než předchozí důkaz pro stopy, je však elementární. (Návod: je vhodné nejprve tvrzení dokázat v případě, kdy je M jednoduché rozšíření k.)

Definice. Rozšíření K/k se nazývá separabilní, jestliže lineární funkce $\xi \mapsto \mathrm{Sp}_{K/k}(\xi)$ na vektorovém prostoru K nad k není identicky nulová, tj. existuje-li nějaké $\xi \in K$ s vlastností $\mathrm{Sp}_{K/k}(\xi) \neq 0$.

Jelikož jediný nenulový podprostor vektorového prostoru k nad k je celé k, z poznámky před větou 7 snadno plyne, že je-li K/k separabilní, pak lineární funkce $\alpha \mapsto \mathrm{Sp}_{K/k}(\alpha)$ je surjektivní. Proto pro libovolné mezitěleso M konečného rozšíření K/k platí, že K/k je separabilní právě když jsou obě rozšíření K/M a M/k separabilní.

Je-li K/k konečné rozšíření a je-li charakteristika tělesa k rovna nule, platí $\mathrm{Sp}_{K/k}(1) = [K : k] \neq 0$. Libovolné konečné rozšíření tělesa k charakteristiky nula je tedy separabilní. Totéž platí pro konečná rozšíření tělesa charakteristiky $p \neq 0$, jejichž stupeň není dělitelný p.

Zvolme v konečném separabilním rozšíření K/k bazi $\omega_1, \ldots, \omega_n$ a sestavme matici

$$\big(\mathrm{Sp}_{K/k}(\omega_i\omega_j)\big)_{i,j\in\{1,\ldots,n\}}.$$

Dokažme sporem, že tato matice je regulární. Předpokládejme tedy, že je singulární. Pak existují $c_1, \ldots, c_n \in k$, ne všechny nulové, tak, že

$$\sum_{j=1}^{n} c_j \,\mathrm{Sp}_{K/k}(\omega_i\omega_j) = 0$$

pro všechna $i = 1, \ldots, n$. Položme $\gamma = \sum_{i=1}^{n} c_i\omega_i$. Předchozí rovnost pak lze psát ve tvaru $\mathrm{Sp}(\gamma\omega_i) = 0$ pro všechna $i = 1, \ldots, n$. Protože $\gamma \neq 0$ (připomeňme, že případ $c_1 = \cdots = c_n = 0$ byl vyloučen), pro libovolné $\xi \in K$ lze psát $\xi\gamma^{-1} = \sum_{i=1}^{n} a_i\omega_i$ pro vhodná $a_i \in k$. Pak ovšem

$$\mathrm{Sp}_{K/k}(\xi) = \mathrm{Sp}_{K/k}\big(\sum_{i=1}^{n} a_i\omega_i\gamma\big) = \sum_{i=1}^{n} a_i \,\mathrm{Sp}_{K/k}(\omega_i\gamma) = 0,$$

což je spor.

Definice. Determinant

$$\det\big(\mathrm{Sp}_{K/k}(\omega_i\omega_j)\big)_{i,j\in\{1,\dots,n\}}$$

se nazývá diskriminant baze $\omega_1,\dots,\omega_n$ konečného separabilního rozšíření K/k a značí se $D(\omega_1,\dots,\omega_n)$.

Cvičení 2: Jsou-li $\omega_1,\dots,\omega_n$ a $\omega_1',\dots,\omega_n'$ dvě baze konečného separabilního rozšíření K/k, pak $\frac{D(\omega_1',\dots,\omega_n')}{D(\omega_1,\dots,\omega_n)}$ je druhá mocnina nenulového prvku z k. Dokažte.

Zvolme v konečném separabilním rozšíření K/k pevně bazi $\omega_1,\dots,\omega_n$. Pro libovolné prvky $c_1,\dots,c_n\in k$ existuje jediné $\alpha\in K$ takové, že $\mathrm{Sp}_{K/k}(\omega_i\alpha)=c_i$ pro každé $i=1,\dots,n$. Skutečně, napíšeme-li α ve tvaru $\alpha=\sum_{i=1}^n x_i\omega_i$, předchozí podmínky znamenají, že x_i jsou řešením soustavy n lineárních rovnic o n neznámých, přičemž determinant matice soustavy je $D(\omega_1,\dots,\omega_n)\neq 0$. Speciálně, v K lze najít jednoznačně určené prvky $\omega_1^*,\dots,\omega_n^*$ tak, že pro libovolné $i,j\in\{1,\dots,n\}$ platí

$$\mathrm{Sp}_{K/k}(\omega_i\omega_j^*)=\begin{cases}1 & \text{pro } i=j,\\ 0 & \text{pro } i\neq j.\end{cases}$$

Snadno se dokáže lineární nezávislost prvků $\omega_1^*,\dots,\omega_n^*$.

Definice. Baze $\omega_1^*,\dots,\omega_n^*$ konečného separabilního rozšíření K/k určená předešlou konstrukcí se nazývá duální bazí k bazi $\omega_1,\dots,\omega_n$.

Cvičení 3: Nechť K/k je konečné separabilní rozšíření a φ je lineární funkce na vektorovém prostoru K nad k. Dokažte, že pak existuje, a to jediné, $\alpha\in K$ tak, že pro libovolné $\theta\in K$ platí $\varphi(\theta)=\mathrm{Sp}_{K/k}(\alpha\theta)$.

Duální baze umožňuje zapsat explicitně koeficienty $a_i\in k$ z vyjádření $\alpha=\sum_{i=1}^n a_i\omega_i$. Snadno se ověří, že $a_i=\mathrm{Sp}(\alpha\omega_i^*)$ pro libovolné $i=1,\dots,n$.

Předpokládejme, že K/k je separabilní rozšíření a že minimální polynom nějakého algebraického prvku $\alpha\in K$ nad k se v nějakém rozšíření M/k, jehož mezitělesem je K, rozkládá na lineární činitele:

$$\varphi_\alpha(t)=(t-\alpha_1)\dots(t-\alpha_n).$$

Pak je $k(\alpha)/k$ konečné separabilní rozšíření a z vět 7 a 8 plyne

$$\mathrm{Sp}_{k(\alpha)/k}(\alpha^r)=\sum_{s=1}^n\alpha_s^r$$

pro libovolné přirozené číslo r. Proto pro diskriminant baze $1,\alpha,\dots,\alpha^{m-1}$ platí

$$\begin{aligned}D(1,\alpha,\dots,\alpha^{m-1}) &= \det\big(\mathrm{Sp}_{k(\alpha)/k}(\sum_{s=1}^n\alpha^{i+j})\big)_{i,j\in\{1,\dots,n\}}\\ &= \det(\alpha_s^i)\cdot\det(\alpha_s^j)=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2.\end{aligned}$$

Jelikož $D \neq 0$, platí $\alpha_i \neq \alpha_j$. Dokázali jsme následující výsledek.

Věta 9. Minimální polynom libovolného algebraického prvku ze separabilního rozšíření nemá násobné kořeny.

Poznámka. Právě vlastnost zmíněná ve větě 9 vysvětluje, proč se užívá termín „separabilní“: kořeny minimálního polynomu můžeme od sebe separovat.

Příklad. Uveďme si příklad nějakého konečného rozšíření, které není separabilní. Už víme, že musíme uvážit nějaké těleso charakteristiky $p \neq 0$ a že stupeň rozšíření musí být dělitelný p. Zvolme prvočíslo p libovolně a označme $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Nechť k je těleso racionálních funkcí nad $\mathbb{F}_p$ (tj. libovolný prvek tělesa k je podílem $\frac{f(x)}{g(x)}$ vhodných dvou polynomů $f(x), g(x) \in \mathbb{F}_p[x]$, $g(x) \neq 0$). Pak polynom $\varphi(t) = t^p - x$ je nemá v k kořen (předpokládejte kořen ve tvaru $\frac{f(x)}{g(x)}$, dosaďte, upravte a porovnejte stupně polynomů). Označme K jeho rozkladové těleso nad k. Pak $\varphi(t)$ má v K nějaký kořen ξ a platí $\varphi(t) = (t-\xi)^p$, neboť příslušné binomické koeficienty jsou dělitelné p a tedy jsou rovny nule v k. Je tedy minimální polynom prvku ξ nad k alespoň druhou mocninou polynomu $t - \xi$ a tedy má násobné kořeny. Rozšíření K/k tedy není separabilní. (Snadno lze též ukázat, že $\varphi(t)$ je ireducibilní nad k.)

Cvičení 4: Dokažte, že je-li K/k konečné rozšíření takové, že pro každé $\alpha \in K$ minimální polynom φ_α má ve svém rozkladovém tělese nad k pouze jednoduché kořeny, pak je K/k separabilní.

Věta 10. Každé konečné separabilní rozšíření K/k je jednoduché, tj. existuje $\gamma \in K$ tak, že $K = k(\gamma)$.

Důkaz. Je-li k konečné, je i K konečné a jeho multiplikativní grupa je cyklická. Za γ lze vzít generátor této cyklické grupy.

Nechť je k nekonečné. Omezíme se na adjunkci dvou prvků (dále indukcí). Nechť tedy $K = k(\alpha, \beta)$ a nechť L je rozkladové těleso polynomu $\varphi_\alpha \varphi_\beta$ nad K. Pak v L existuje rozklad

$$\varphi_\alpha(t) = (t - \alpha_1) \dots (t - \alpha_s),$$
$$\varphi_\beta(t) = (t - \beta_1) \dots (t - \beta_r),$$

kde $\alpha_1 = \alpha$ a $\beta_1 = \beta$. Navíc $\alpha_i \neq \alpha_j$ a $\beta_i \neq \beta_j$ kdykoli $i \neq j$. Protože je k nekonečné, existuje $c \in k$ tak, že $\gamma = \alpha + c\beta \neq \alpha_i + c\beta_j$, jestliže $(i, j) \neq (1, 1)$. Nechť $M = k(\gamma) \subseteq K$. Položme $\psi(t) = \varphi_\alpha(\gamma - ct) \in M[t]$. Pak $\psi(\beta) = 0$ a tedy ψ a φ_β jsou soudělné. Je-li $i \neq 1$, je $\varphi(\beta_i) \neq 0$ a tedy největší společný dělitel polynomů ψ a φ_β je polynom $t - \beta \in M[t]$. Odtud $\beta \in M$ a také $\alpha = \gamma - c\beta \in M$. Tedy $K = k(\alpha, \beta) \subseteq M$, tj. $K = k(\gamma)$.

Věta 11. Pro libovolné konečné separabilní rozšíření K/k stupně n existuje právě n (a ne více!) vnoření (tj. injektivních homomorfismů) do vhodného rozšíření M/k, při kterých se každý prvek z k zobrazí na sebe. Jsou-li $\sigma_1, \dots, \sigma_n$ tato vnoření, pak pro libovolné $\alpha \in K$ se jeho charakteristický polynom $f_\alpha(t)$ v M rozkládá na lineární činitele takto:

$$f_\alpha(t) = (t - \sigma_1(\alpha)) \dots (t - \sigma_n(\alpha)).$$

Důkaz. Podle věty 10 existuje $\gamma \in K$ tak, že $K = k(\gamma)$. Nechť M je rozkladové těleso minimálního polynomu $\varphi_\gamma(t)$ prvku γ. Libovolné vnoření $K \to M$ nechávající

prvky tělesa k na místě je určeno obrazem prvku γ, který se může zobrazit pouze na některý (avšak dle věty 4 na jakýkoli) z n různých (dle věty 9) kořenů $\gamma_1, \dots, \gamma_n$ polynomu $\varphi_\gamma(t)$. Podle věty 6 je charakteristický polynom

$$f_\alpha(t) = \varphi_\gamma(t) = (t-\gamma_1)\dots(t-\gamma_n),$$

přičemž při vhodném označení vnoření $\sigma_1, \dots, \sigma_n$ platí $\sigma_i(\gamma) = \gamma_i$ pro každé $i = 1, \dots, n$. Nechť nyní $\alpha \in K$ je libovolné. Pak existuje $g(t) \in k[t]$ tak, že $\alpha = g(\gamma)$. Potom pro každé $i = 1, \dots, n$ platí $g(\gamma_i) = g(\sigma_i(\gamma)) = \sigma_i(g(\gamma)) = \sigma_i(\alpha)$ a tvar rozkladu charakteristického polynomu $f_\alpha(t)$ plyne z věty 8.

Důsledek 1. V označení věty 11 platí

$$N_{K/k}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \qquad \mathrm{Sp}_{K/k}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Důsledek 2. Pro libovolné konečné rozšíření tělesa racionálních čísel existuje právě n různých vnoření do tělesa komplexních čísel.

2. Normální rozšíření a Galoisova korespondence

Definice: Rozšíření K/k se nazývá normální, jestliže každý ireducibilní polynom $f \in k[t]$, který má v K kořen, se v K rozkládá na lineární faktory.

Věta 1. Rozšíření K/k je konečné a normální, právě když je K rozkladové těleso nějakého polynomu nad k.

Důkaz. Je-li K/k konečné, je $K = k(\alpha_1, \dots, \alpha_s)$, z normality plyne, že K je rozkladové těleso polynomu $\varphi_{\alpha_1} \dots \varphi_{\alpha_s}$.

Naopak, nechť je K rozkladové těleso nějakého polynomu f nad k. Zvolme $\alpha \in K$, pak φ_α se rozkládá na lineární faktory ve svém rozkladovém tělese L nad K: $\varphi_\alpha(t) = (t-\alpha_1)\dots(t-\alpha_n)$, kde $\alpha = \alpha_1$. Budeme hotovi, ukážeme-li, že $\alpha_i \in K$ pro libovolné $i = 2, \dots, n$. Dle věty 4 existuje izomorfismus $\sigma : k(\alpha_1) \to k(\alpha_i)$ s vlastností $\sigma|_k = \mathrm{id}_k$ a $\sigma(\alpha_1) = \alpha_i$, mimo jiné tedy platí $[k(\alpha_1) : k] = [k(\alpha_i) : k]$. Pak $K = K(\alpha_1)$ je rozkladové těleso polynomu f nad $k(\alpha_1)$ a $K(\alpha_i)$ je rozkladové těleso polynomu f nad $k(\alpha_i)$. Ovšem $\sigma(f) = f$ a tedy podle tvrzení o izomorfismu rozkladových těles existuje izomorfismus $\tau : K \to K(\alpha_i)$ s vlastností $\tau|_{k(\alpha_1)} = \sigma$. Proto $[K : k(\alpha_1)] = [K(\alpha_i) : k(\alpha_i)]$. Odtud $[K(\alpha_i) : K] = \frac{[K(\alpha_i):k(\alpha_i)][k(\alpha_i):k]}{[K:k]} = \frac{[K:k(\alpha_1)][k(\alpha_1):k]}{[K:k]} = 1$, a tedy $\alpha_i \in K$.

Cvičení 5. Rozhodněte, zda rozšíření $\mathbb{Q}(\alpha)/\mathbb{Q}$, kde $\alpha = \sqrt{2+\sqrt{2}}$, je normální.

Věta 2. Nechť M je mezitěleso konečného normálního rozšíření K/k a nechť $\tau : M \to K$ je vnoření s vlastností $\tau|_k = \mathrm{id}_k$. Pak existuje izomorfismus $\sigma : K \to K$ takový, že $\sigma|_M = \tau$.

Důkaz. Podle věty 1 je K rozkladové těleso nějakého polynomu f nad k, a tedy i rozkladové těleso polynomu f nad M i nad $\tau(M)$. Přitom $\tau(f) = f$. Stačí užít tvrzení o izomorfismu rozkladových těles.

Věta 3. Nechť K/k je konečné normální rozšíření a nechť α, β jsou kořeny nějakého ireducibilního polynomu nad k. Pak existuje automorfismus τ tělesa K s vlastností $\tau|_k = \mathrm{id}_k$ a $\tau(\alpha) = \beta$.

Důkaz. Podle věty 4 z první kapitoly existuje izomorfismus $\sigma : k(\alpha) \to k(\beta)$ takový, že $\sigma|_k = \mathrm{id}_k$ a $\sigma(\alpha) = \beta$. Stačí užít větu 2.

Definice: Nechť K/k je algebraické rozšíření. Normální uzávěr rozšíření K/k je rozšíření N tělesa K takové, že platí
1. N/k je normální,
2. je-li M mezitěleso N/K takové, že M/k je normální, pak $M = N$.

Věta 4. Nechť K/k je konečné rozšíření. Pak existuje normální uzávěr N rozšíření K/k, který je konečným rozšířením tělesa k. Je-li M jiný normální uzávěr rozšíření K/k, pak existuje izomorfismus $\tau : N \to M$ s vlastností $\tau|_K = \mathrm{id}_K$.

Důkaz. Nechť $K = k(\alpha_1, \ldots, \alpha_n)$. Snadno se ověří, že rozkladové těleso N polynomu $f = \varphi_{\alpha_1} \ldots \varphi_{\alpha_n}$ nad k je normální uzávěr rozšíření K/k. Naopak, je-li M normální uzávěr rozšíření K/k, musí obsahovat rozkladové těleso polynomu f nad k, které je normálním rozšířením k. Věta plyne z tvrzení o izomorfismu rozkladových těles (která jsou také rozkladová tělesa nad K).

Cvičení 6. Nalezněte normální uzávěr rozšíření $\mathbb{Q}(\sqrt[10]{2})/\mathbb{Q}$.

Lemma 1. Nechť $k \subseteq K \subseteq N \subseteq M$ jsou tělesa, přičemž K/k je konečné rozšíření a N je normální uzávěr rozšíření K/k. Nechť $\tau : K \to M$ je vnoření s vlastností $\tau|_k = \mathrm{id}_k$. Pak $\tau(K) \subseteq N$.

Důkaz. Nechť $\alpha \in K$. Pak $0 = \tau(\varphi_\alpha(\alpha)) = \varphi_\alpha(\tau(\alpha))$, a tedy $\tau(\alpha) \in N$.

Věta 5. Nechť K/k je konečné rozšíření. Následující podmínky jsou ekvivalentní:
1. K/k je normální,
2. existuje normální rozšířením N/k s mezitělesem K takové, že pro každé vnoření $\tau : K \to N$ s vlastností $\tau|_k = \mathrm{id}_k$ platí $\tau(K) = K$,
3. pro každé rozšířením M/k s mezitělesem K a každé vnoření $\tau : K \to M$ s vlastností $\tau|_k = \mathrm{id}_k$ platí $\tau(K) = K$.

Důkaz. (1) $\implies$ (3): Plyne z předchozího lemmatu, neboť $[\tau(K) : k] = [K : k]$.

(3) $\implies$ (2): Stačí za M vzít normální uzávěr K/k, jehož existenci zaručuje věta 3.

(2) $\implies$ (1): Pro libovolné $\alpha \in K$ a libovolný kořen β polynomu φ_α platí $\beta \in N$. Podle věty 3 existuje automorfismus τ tělesa N s vlastností $\tau|_k = \mathrm{id}_k$ a $\tau(\alpha) = \beta$. Aplikací podmínky (2) na $\tau|_K$ dostáváme $\beta = \tau(\alpha) \in K$.

Definice. Rozšíření těles K/k se nazývá Galoisovo, je-li konečné, normální a separabilní. Pro Galoisova rozšíření definujeme Galoisovu grupu $\mathrm{Gal}(K/k)$ jako grupu všech automorfismů τ tělesa K s vlastností $\tau|_k = \mathrm{id}_k$.

Lemma 2. Nechť K/k je Galoisovo rozšíření. Pak platí $|\mathrm{Gal}(K/k)| = [K : k]$.

Důkaz. Plyne z věty 11 první kapitoly a věty 5.

Cvičení 7. Nechť L je mezitěleso rozšíření K/k. Rozhodněte, zda platí:
(a) je-li K/k Galoisovo, pak je L/k Galoisovo;
(b) je-li K/k Galoisovo, pak je K/L Galoisovo;
(c) jsou-li K/L i L/k obě Galoisova, pak je K/k Galoisovo.

Cvičení 8. Rozhodněte, zda platí: je-li N normální uzávěr konečného separabilního rozšíření K/k, pak je N/k Galoisovo.

Lemma 3. (Dedekind) Nechť K a L jsou tělesa. Pak libovolná množina různých vnoření $K \to L$ je lineárně nezávislá nad L.

Důkaz. Předpokládejme, že $\lambda_1, \dots, \lambda_n$ jsou různá vnoření $K \to L$, která jsou nad L lineárně závislá, ale jakýchkoli $n-1$ z nich už je lineárně nezávislých nad L. Existují tedy nenulová $a_1, \dots, a_n \in L$ tak, že pro každé $\alpha \in K$ platí

$$a_1\lambda_1(\alpha) + \cdots + a_n\lambda_n(\alpha) = 0.$$

Existuje $\beta \in K$ tak, že $\lambda_1(\beta) \neq \lambda_n(\beta)$. Proto $\beta \neq 0$. Navíc pro $\alpha\beta \in K$ platí

$$a_1\lambda_1(\alpha\beta) + \cdots + a_n\lambda_n(\alpha\beta) = 0,$$

tedy

$$a_1\lambda_1(\alpha)\lambda_1(\beta) + \cdots + a_n\lambda_n(\alpha)\lambda_n(\beta) = 0,$$

odečtením od $\lambda_1(\beta)$-násobku první rovnice dostáváme spor.

Věta 6. Nechť G je konečná podgrupa grupy automorfismů tělesa K a nechť

$$k = \{\alpha \in K;\, \forall \sigma \in G :\, \sigma(\alpha) = \alpha\}.$$

Pak platí $[K : k] = |G|$.

Důkaz. Nechť $G = \{\sigma_1, \dots, \sigma_n\}$.

1. Předpokládejme, že $[K : k] < n$. Nechť $x_1, \dots, x_m$ je baze K nad k. Jistě existují $y_1, \dots, y_n \in K$ ne všechny nulové tak, že pro každé $j = 1, \dots, m$ platí

$$\sum_{i=1}^{n} \sigma_i(x_j)y_i = 0.$$

Pro libovolné $\alpha \in K$ existují $a_1, \dots, a_m \in k$ tak, že $\alpha = \sum_{j=1}^{m} a_j x_j$. Pak platí

$$\sum_{i=1}^{n} \sigma_i(\alpha)y_i = \sum_{i=1}^{n} \sigma_i\Big(\sum_{j=1}^{m} a_j x_j\Big) y_i = \sum_{i=1}^{n}\sum_{j=1}^{m} a_j\sigma_i(x_j)y_i = 0,$$

což je spor s lemmatem 3.

2. Předpokládejme, že $[K : k] > n$. Položme $m = n+1$ a zvolme libovolně prvky $x_1, \dots, x_m \in K$ lineárně nezávislé nad k. Jistě existují $y_1, \dots, y_m \in K$ ne všechny nulové tak, že pro každé $i = 1, \dots, n$ platí

$$\sum_{j=1}^{m} \sigma_i(x_j)y_j = 0.$$

Případnou změnou $y_1, \dots, y_m \in K$ a záměnou indexů prvků $x_1, \dots, x_m$ lze dosáhnout toho, že $y_1 \neq 0$, $\dots$, $y_r \neq 0$, $y_{r+1} = \cdots = y_m = 0$ a že r je s touto vlastností nejmenší možné. Pro každé $\sigma \in G$ tedy platí

$$(*) \qquad \sum_{j=1}^{r} \sigma(x_j)y_j = 0.$$

Zvolme $\tau \in G$ libovolně a aplikujme jej na poslední rovnost. Dostaneme

$$\sum_{j=1}^{r} (\tau\sigma)(x_j)\tau(y_j) = 0.$$

Každý automorfismus v G lze napsat ve tvaru $\tau\sigma$ pro nějaké $\sigma \in G$, podle předchozí rovnosti tedy

$$\sum_{j=1}^{r} \sigma(x_j)\tau(y_j) = 0$$

pro každé $\sigma \in G$. Odečtením y_r-násobku této rovnosti od $\tau(y_r)$-násobku rovnosti (*), dostaneme

$$\sum_{j=1}^{r-1} \sigma(x_j)(\tau(y_r)y_j - y_r\tau(y_j)) = 0,$$

což podle definice čísla r je možné jen, je-li

$$\tau(y_r)y_j - y_r\tau(y_j) = 0$$

pro každé $j = 1, \ldots, r-1$, tj.

$$\tau(y_j y_r^{-1}) = y_j y_r^{-1}.$$

Přitom bylo $\tau \in G$ libovolné a tedy $z_j = y_j y_r^{-1} \in k$ pro každé $j = 1, \ldots, r$. Dosazením do (*) pro $\sigma = \mathrm{id}\,|_K$ dostaneme

$$\sum_{j=1}^{r} x_j z_j = 0,$$

což je spor s lineární nezávislostí $x_1, \ldots, x_r$ nad k.

Cvičení 9. V označení věty 6: dokažte, že K/k je Galoisovo.

Poznámka. Předchozí cvičení (spolu s větou 6) umožňuje následující charakterizaci Galoisových rozšíření (která je někdy v literatuře užívána jako definice Galoisova rozšíření): konečné rozšíření stupně n je Galoisovo, právě když existuje n různých automorfismů tělesa K, jejichž restrikce na k je identita.

Definice. Nechť K/k je Galoisovo rozšíření. Označme $G = \mathrm{Gal}(K/k)$. Je-li H podgrupa G, označme

$$H^{\perp} = \{\alpha \in K;\ \forall \sigma \in H : \sigma(\alpha) = \alpha\}.$$

Jistě je $H^{\perp}$ podtěleso tělesa K obsahující k; nazývá se těleso fixované H. Je-li L mezitěleso K/k, označme

$$L^{\perp} = \{\sigma \in G;\ \forall \alpha \in L : \sigma(\alpha) = \alpha\}.$$

Jistě je $L^{\perp}$ podgrupa grupy G; nazývá se podgrupa fixující L.

Definice. Nechť L_1, L_2 jsou mezitělesa rozšíření K/k. Kompozitem těles L_1, L_2 nazveme nejmenší podtěleso tělesa K obsahující $L_1 \cup L_2$. Značíme L_1L_2.

Poznámka. Kompozitum lze definovat i pro dvě rozšíření L_1/k, L_2/k, z nichž aspoň jedno je konečné a normální; pak je určeno jednoznačně až na izomorfismus.

Hlavní věta Galoisovy teorie. Nechť K/k je Galoisovo rozšíření. Označme $\mathcal{F}$ množinu všech mezitěles rozšíření K/k a $\mathcal{G}$ množinu všech podgrup grupy $G = \mathrm{Gal}(K/k)$. Pak platí:

1. Výše popsaná zobrazení $H \mapsto H^\perp$ a $L \mapsto L^\perp$ jsou navzájem inverzní bijekce mezi $\mathcal{F}$ a $\mathcal{G}$, přičemž pro libovolné $H_1, H_2 \in \mathcal{G}$ platí
$$H_1 \subseteq H_2 \iff H_1^\perp \supseteq H_2^\perp.$$
2. Jsou-li $L_1, L_2 \in \mathcal{F}$, pak
$$(L_1L_2)^\perp = L_1^\perp \cap L_2^\perp, \qquad (L_1 \cap L_2)^\perp = \langle L_1^\perp \cup L_2^\perp \rangle,$$
kde $\langle H \rangle$ značí podgrupu generovanou množinou $H \subseteq G$.
3. Je-li $L \in \mathcal{F}$, pak
$$[K : L] = |L^\perp|, \qquad [L : k] = \frac{|G|}{|L^\perp|}.$$
4. Je-li $L \in \mathcal{F}$, pak L/k je normální rozšíření, právě když $L^\perp$ je normální podgrupa grupy G (v obvyklém smyslu teorie grup).
5. Je-li $L \in \mathcal{F}$ a L/k je normální rozšíření, pak $\mathrm{Gal}(L/k)$ je izomorfní s faktorgrupou $G/L^\perp$, přičemž izomorfismus je indukován homomorfismem, který $\sigma \in G$ zobrazí na $\sigma|_L \in \mathrm{Gal}(L/k)$.

Důkaz. 1. Nechť $L \in \mathcal{F}$, pak K/L je konečné, separabilní (viz poznámku v první kapitole) a normální (plyne např. z věty 1), tedy Galoisovo, přitom $\mathrm{Gal}(K/L) = L^\perp$. Jistě $L \subseteq (L^\perp)^\perp$. Dle věty 6 platí $[K : (L^\perp)^\perp] = |L^\perp| = |\mathrm{Gal}(K/L)| = [K : L]$, kde poslední rovnost plyne z lemmatu 2. Proto $L = (L^\perp)^\perp$.

Nechť $H \in \mathcal{G}$. Jistě $H \subseteq (H^\perp)^\perp$. Z výše dokázaného $H^\perp = ((H^\perp)^\perp)^\perp$. Dle věty 6 platí $|H| = [K : H^\perp] = [K : ((H^\perp)^\perp)^\perp] = |(H^\perp)^\perp|$. Proto $H = (H^\perp)^\perp$.

Zřejmě z $H_1 \subseteq H_2$ plyne $H_1^\perp \supseteq H_2^\perp$ a odtud zase $(H_1^\perp)^\perp \subseteq (H_2^\perp)^\perp$. Stačí užít rovnost $H = (H^\perp)^\perp$.

2. Dokázali jsme, že svazy $(\mathcal{F}, \subseteq)$ a $(\mathcal{G}, \subseteq)$ jsou antiizomorfní. Stačí si uvědomit, že supremum ve svazu $(\mathcal{F}, \subseteq)$ odpovídá kompozitu těles a ve svazu $(\mathcal{G}, \subseteq)$ podgrupě generované sjednocením.

3. První rovnost je lemma 2, pro druhou stačí užít větu 1 z první kapitoly.

4. Pro libovolné $\tau \in G$ a libovolné $M \in \mathcal{F}$ dokažme $(\tau(M))^\perp = \tau M^\perp \tau^{-1}$. Z tím účelem označme $M' = \tau(M)$. Pro libovolné $\alpha \in M'$ existuje $\beta \in M$ s vlastností $\alpha = \tau(\beta)$. Pro každé $\sigma \in M^\perp$ pak platí $\tau\sigma\tau{-}1(\alpha) = \alpha$, a tedy $\tau M^\perp \tau^{-1} \subseteq (M')^\perp$. Podobně $\tau^{-1}(M')^\perp\tau \subseteq M^\perp$. Dohromady rovnost.

Je-li tedy L/k normální rozšíření, pak podle věty 5 je $\tau(L) = L$ pro každé $\tau \in G$, a tedy $L^\perp$ je normální podgrupa grupy G.

Naopak, nechť $L^\perp$ je normální podgrupa grupy G. Užijeme větu 5. Zvolme libovolně vnoření $\tau : L \to K$ splňující $\tau|_k = \mathrm{id}_k$. Podle věty 2 existuje $\sigma \in G$ tak, že $\sigma|_L = \tau$. Podle výše dokázaného $(\sigma(L))^\perp = \sigma L^\perp \sigma^{-1} = L^\perp$, neboť $L^\perp$ je normální

podgrupa. Podle části 1 této věty to znamená $\sigma(L) = L$, odkud $\tau(L) = L$. Z věty 5 výsledek.

5. Označme $G' = \mathrm{Gal}(L/k)$. Uvažme zobrazení $\phi : G \to G'$ dané restrikcí, tj. $\phi(\sigma) = \sigma|_L$ pro $\sigma \in G$. Zřejmě je ϕ homomorfismus, který je podle věty 2 surjektivní. Jádrem homomorfismu je zřejmě $L^\perp$.

Cvičení 10. Popište Galoisovu grupu normálního uzávěru N rozšíření:
(a) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$,
(b) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.

Cvičení 11. Nechť K/k je Galoisovo rozšíření takové, že $\mathrm{Gal}(K/k)$ je komutativní. Dokažte, že pak pro libovolná mezitělesa L_1, L_2 rozšíření K/k platí

$$[L_1L_2 : k][L_1 \cap L_2 : k] = [L_1 : k][L_2 : k].$$

Je předpoklad o komutativitě nutný?

3. Něco o oborech integrity

(dle Boreviče-Šafareviče, alg. doplněk, §3, část 3)

Definice. Nechť R je podokruh tělesa K. Prvek $\alpha \in K$ se nazývá celý vzhledem k R, je-li kořenem vhodného normovaného polynomu s koeficienty z okruhu R.

Zřejmě libovolný prvek z R je celý vzhledem k R.

Definice. Nechť R je podokruh tělesa K, nechť $\alpha_1, \ldots, \alpha_n \in K$. Množinu všech lineárních kombinací

$$a_1\alpha_1 + \cdots + a_n\alpha_n,$$

kde $a_1, \ldots, a_n \in R$, se nazývá R-modul v K s konečným počtem generátorů, prvky $\alpha_1, \ldots, \alpha_n$ se nazývají generátory tohoto R-modulu.

Věta 1. Je-li R-modul s konečným počtem generátorů současně okruhem, pak je libovolný jeho prvek celý vzhledem k R.

Důkaz. Nechť $\alpha_1, \ldots, \alpha_n$ jsou generátory modulu M, který je okruhem, nechť $\beta \in M$ je libovolné. Protože $\beta\alpha_i \in M$ pro libovolné $i = 1, \ldots, n$, existují $a_{ij} \in R$ tak, že

$$\beta\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$$

každé $i = 1, \ldots, n$. Odtud plyne $\det(\beta E - (a_{ij})) = 0$, kde E je jednotková matice n-tého řádu. Je tedy β kořenem normovaného polynomu $\det(tE - (a_{ij})) \in R[t]$.

Definice. Nechť R je podokruh tělesa K. Množina všech prvků $\alpha \in K$, které jsou celé vzhledem k R, se nazývá celý uzávěr okruhu R v tělese K. Okruh R se nazývá celouzavřený v K, splývá-li se svým celým uzávěrem v K.

Věta 2. Nechť R je podokruh tělesa K, pak celý uzávěr M okruhu R v tělese K tvoří okruh.

Důkaz. Nechť $\alpha, \beta \in M$ jsou libovolné. Pak existují $a_1, \ldots, a_m, b_1, \ldots, b_n \in R$ tak, že platí

$$\alpha^m = a_1 + a_2\alpha + \cdots + a_m\alpha^{m-1}, \qquad \beta^n = b_1 + b_2\beta + \cdots + b_m\beta^{m-1}.$$

Odtud plyne, že R-modul generovaný prvky $\alpha^i\beta^j$, kde $0 \le i < m$, $0 \le j < n$, tvoří okruh. Podle věty 1 jsou všechny jeho prvky celé, speciálně i $\alpha \pm \beta$ a $\alpha\beta$.

Definice. Obor integrity se nazývá celouzavřený, je-li celouzavřený ve svém podílovém tělese.

Věta 3. Nechť R je podokruh tělesa K, pak celý uzávěr M okruhu R v tělese K je celouzavřený v K.

Důkaz. Nechť $\vartheta \in K$ je libovolný celý prvek vzhledem k M, ukážeme, že $\vartheta \in M$. Existují tedy $\alpha_1, \dots, \alpha_n \in M$ takové, že

$$\vartheta^n = \alpha_1 + \alpha_2\vartheta + \cdots + \alpha_n\vartheta^{n-1}.$$

Pro každé $i = 1, \dots, n$ existuje přirozené číslo m_i a prvky $a_{i1}, \dots, a_{im_i} \in R$ tak, že platí

$$\alpha_i^{m_i} = \sum_{j=1}^{m_i} a_{ij}\alpha_i^{j-1}.$$

Pak R-modul, generovaný součiny

$$\alpha_1^{k_1} \dots \alpha_n^{k_n}\vartheta^k,$$

kde $0 \le k_1 < m_1, \dots, 0 \le k_n < m_n$, $0 \le k < n$, tvoří okruh. Stačí užít větu 1.

Lemma. Nechť R je obor integrity, který je celouzavřený ve svém podílovém tělese k. Nechť $f(t) \in R[t]$ je normovaný. Jestiže normovaný $g(t) \in k[t]$ je dělitelem polynomu $f(t)$, pak platí $g(t) \in R[t]$.

Důkaz. Nechť K je rozkladové těleso polynomu $f(t)$ nad k. Pak všechny kořeny polynomu $f(t)$ patří do celého uzávěru M okruhu R v K. Proto i kořeny polynomu $g(t)$ patří do M a tedy $g(t) \in M[t]$. Ovšem $k \cap M = R$, neboť R je celouzavřený.

Věta 4. Nechť je obor integrity R celouzavřený ve svém podílovém tělese k. Nechť K/k je algebraické rozšíření. Pak libovolný prvek $\alpha \in K$ je celý vzhledem k R, právě když koeficienty jeho minimálního mnohočlenu $\varphi_\alpha(t)$ nad k leží v R.

Důkaz. Věta plyne z předchozího lemmatu.

Cvičení 12. Nalezněte celý uzávěr $\mathbb{Z}$ v tělese
(a) $\mathbb{Q}(\sqrt{2})$;
(b) $\mathbb{Q}(\sqrt{5})$.

4. Některé aplikace Galoisovy teorie

Mějme v rovině s kartézskou soustavou souřadnic dáno konečně mnoho bodů a uvažme těleso k, které je nad $\mathbb{Q}$ generováno jejich souřadnicemi. Protože průsečík dvou přímek v rovině lze spočítat pomocí soustavy lineárních rovnic, průsečík dvou přímek proložených některými z daných bodů bude mít opět souřadnice v tělese k. Podobně, protože výpočet průsečíků dvou kružnic či kružnice a přímky v rovině vede na výpočet kořenů jedné kvadratické rovnice, snadno se usoudí, že pokud každá z kružnic měla střed v některém z daných bodů a nějakým daným bodem procházela, resp. přímka byla proložena dvojicí z daných bodů, pak vzniklé průsečíky mají obě souřadnice v nějakém rozšíření K tělesa k, přičemž buď $K = k$ (v případě,

kdy diskriminant uvažované kvadratické rovnice je druhou mocninou v k) anebo $[K : k] = 2$ (v opačném případě).

Předpokládejme, že na počátku máme konečnou množinu bodů s racionálními souřadnicemi a postupně k ní přidáváme průsečíky výše uvedenými konstrukcemi. Po konečně mnoha krocích uvažme těleso K, generované souřadnicemi vzniklých bodů. Je jasné, že $[K : \mathbb{Q}]$ je mocnina 2. To dokazuje neřešitelnost úlohy zdvojení krychle (tj. konstrukce poměru $\sqrt[3]{2} : 1$ kružítkem a pravítkem). Víme-li, že π je transcendentní číslo, vyplývá odtud neřešitelnost úlohy kvadratury kruhu (tj. konstrukce poměru $\pi : 1$ kružítkem a pravítkem).

Pro předchozí úvahy Galoisova teorie nebyla nutná, vystačili bychom prakticky s větou 1 z kapitoly 1; nyní se však budeme zabývat konstrukcí pravidelných n-úhelníků, kde Galoisovu teorii už využijeme.

Příklad. Nechť p je prvočíslo, $\zeta = e^{\frac{2\pi i}{p}}$. Těleso $\mathbb{Q}(\zeta)$ se nazývá p-té kruhové těleso. Ukažme, že $\mathbb{Q}(\zeta)/\mathbb{Q}$ je Galoisovo rozšíření a popišme jeho Galoisovu grupu $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Polynom

$$f(t) = t^{p-1} + t^{p-2} + \cdots + t + 1 = \frac{t^p - 1}{t - 1}$$

má kořen ζ a je ireducibilní nad $\mathbb{Q}$, neboť polynom

$$f(t + 1) = \sum_{j=1}^{p} \binom{p}{j} t^{j-1}$$

je ireducibilní podle Eisensteinova kriteria. Je tedy $\varphi_\zeta = f$ a platí $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p-1$. Protože

$$f(t) = \prod_{j=1}^{p-1} (t - \zeta^j),$$

je $\mathbb{Q}(\zeta)/\mathbb{Q}$ skutečně Galoisovo. Libovolné $\sigma \in G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ je jednoznačně určeno hodnotou $\sigma(\zeta)$, která je kořenem f, tj. platí $\sigma(\zeta) = \zeta^j$ pro jisté $j \in \{1, \ldots, p-1\}$. Snadno se vidí, že $\sigma \mapsto j$ indukuje injektivní homomorfismus $G \to (\mathbb{Z}/p\mathbb{Z})^\times$. Protože obě grupy mají $p - 1$ prvků, jde o izomorfismus. Protože $(\mathbb{Z}/p\mathbb{Z})^\times$ je multiplikativní grupa konečného tělesa $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, je cyklická, a tedy i G je cyklická grupa.

Poznámka. Situace z předchozího příkladu platí obecněji. Je-li m přirozené číslo, $\zeta = e^{\frac{2\pi i}{m}}$, pak m-té kruhové těleso $\mathbb{Q}(\zeta)$ je Galoisovo a pro jeho Galoisovu grupu $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ platí, že je izomorfní s grupou invertibilních prvků okruhu zbytkových tříd $\mathbb{Z}/m\mathbb{Z}$. Potíž spojená s přechodem od prvočísla p k obecnému m je spojena s důkazem toho, že $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(m)$, kde φ je Eulerova funkce.

Definice. Nechť m je přirozené číslo, $\zeta = e^{\frac{2\pi i}{m}}$. Polynom

$$\Phi_m = \prod_{\substack{j=1,\ldots,m \\ (j,m)=1}} (t - \zeta^j)$$

se nazývá m-tý kruhový polynom.

Věta 1. m-tý kruhový polynom má celočíselné koeficienty a je ireducibilní nad $\mathbb{Q}$ pro libovolné přirozené číslo m.

Důkaz. To, že m-tý kruhový polynom má celočíselné koeficienty, plyne indukcí z toho, že je normovaný a ze zřejmé identity $x^m - 1 = \prod_{d|m} \Phi_d$, kde v součinu d probíhá množinu všech kladných dělitelů čísla m. (Druhá možnost: místo indukce lze užít větu ze třetí kapitoly.)

Nechť p je libovolné prvočíslo nedělící m a uvažme kanonický homomorfismus $\mathbb{Z} \to \mathbb{F}_p$, který rozšíříme (po koeficientech) na homomorfismus $\mathbb{Z}[t] \to \mathbb{F}_p[t]$. Obraz polynomu f budeme značit $\bar{f}$. Pro libovolné $f, g \in \mathbb{Z}[t]$ platí $(\bar{f} + \bar{g})^p = \bar{f}^p + \bar{g}^p$. Odtud a z Fermatovy věty plyne $(\bar{f}(t))^p = \bar{f}(t^p)$. Označme $h(t) = t^m - 1$. Protože $p \nmid m$, je $\bar{h}$ nesoudělný se svou derivací a proto nemá násobný kořen. Protože $\Phi_m | h$, platí totéž i pro $\bar{\Phi}_m$.

Nechť ϑ je libovolný kořen polynomu Φ_m. Minimální polynom φ_ϑ je normovaný a dělí normovaný polynom $\Phi_m \in \mathbb{Z}[t]$, tj. $\Phi_m = g\varphi_\vartheta$ pro nějaký normovaný polynom $g \in \mathbb{Q}[t]$. Protože je okruh $\mathbb{Z}$ celouzavřený, podle věty z kapitoly 3 mají φ_ϑ i g celočíselné koeficienty.

Jistě $\Phi(\vartheta^p) = 0$. Ukážeme, že ϑ^p je kořen φ_ϑ. Předpokládejme naopak, že platí $g(\vartheta^p) = 0$, a označme $h(t) = g(t^p)$. Pak $h(\vartheta) = 0$ a tedy $h = q\varphi_\vartheta$, kde opět podle zmíněné věty q je normovaný polynom s celočíselnými koeficienty. Pak platí $\bar{q}(t) \cdot \bar{\varphi}_\vartheta(t) = \bar{h}(t) = \bar{g}(t^p) = (\bar{g}(t))^p$. Nechť $\psi(t) \in \mathbb{F}_p[t]$ je nějaký ireducibilní dělitel polynomu $\bar{\varphi}_\vartheta$ v $\mathbb{F}_p[t]$. Z uvedené rovnosti plyne $\psi | \bar{g}$ a tedy $\psi^2 | \bar{g}\bar{\varphi}_\vartheta = \bar{\Phi}_m$, což je spor s výše dokázaným faktem, že $\bar{\Phi}_m$ nemá násobné kořeny. Dokázali jsme, že $\varphi_{\vartheta^p} = \varphi_\vartheta$.

Nechť je nyní $\zeta = e^{\frac{2\pi i}{m}}$ a $j < m$ je libovolné přirozené číslo nesoudělné s m. Pak j je součinem prvočísel nesoudělných s m a podle výše dokázaného ζ^j je kořenem φ_ζ. Je tedy $\varphi_\zeta = \Phi_m$.

Důsledek. Nechť m je přirozené číslo a $\zeta = e^{\frac{2\pi i}{m}}$. Pak m-té kruhové těleso $\mathbb{Q}(\zeta)$ je Galoisovo, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(m)$ a pro jeho Galoisovu grupu $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ platí, že je izomorfní s grupou invertibilních prvků okruhu zbytkových tříd $\mathbb{Z}/m\mathbb{Z}$, kde izomorfismus je určen tím, že libovolný $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ s vlastností $\sigma(\zeta) = \zeta^s$ se zobrazí na třídu rozkladu obsahující s.

Definice. Prvočíslo p se nazývá Fermatovo, je-li tvaru $p = 2^n + 1$, kde n je přirozené číslo.

Cvičení 13. Dokažte, že je-li n přirozené číslo a $2^n + 1$ je prvočíslo, pak je n mocnina 2.

Poznámka. Dodnes se neví, je-li Fermatových prvočísel konečně nebo nekonečně mnoho. Jediná známá jsou 3, 5, 17, 257, 65537. Ví se ale, že případné další Fermatovo prvočíslo by muselo být větší než 10^{40000}.

Věta 2. Nechť m je přirozené číslo. Pak pravidelný m-úhelník lze sestrojit pomocí pravítka a kružítka, právě když je m tvaru

$$m = 2^e p_1 \dots p_s,$$

kde e je nezáporné celé číslo a $p_1, \dots, p_s$ jsou po dvou různá Fermatova prvočísla.

Důkaz. Je-li pravidelný m-úhelník sestrojitelný pomocí pravítka a kružítka, je podle předchozího důsledku $\varphi(m)$ mocnina 2 a tedy m je uvedeného tvaru.

Z Bezoutovy identity plyne, že jsou-li sestrojitelné pravidelný k-úhelník i pravidelný l-úhelník, kde k a l jsou nesoudělná přirozená čísla, pak je sestrojitelný i pravidelný kl-úhelník. Proto se stačí omezit na případ pravidelného p-úhelníka, kde $p = 2^n+1$ je Fermatovo prvočíslo. Označme $\zeta = e^{\frac{2\pi i}{p}}$. Galoisova grupa $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ je cyklická řádu 2^n, podle hlavní věty Galoisovy teorie tedy existují (jednoznačně určená) tělesa $K_0 = \mathbb{Q}$, $K_1, \ldots, K_n = \mathbb{Q}(\zeta)$ taková, že $K_0 \subset K_1 \subset \cdots \subset K_n$ a $[K_j : K_{j-1}] = 2$ pro každé $j = 1, \ldots, n$. Platí navíc $K_{n-1} = \mathbb{R} \cap \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta+\zeta^{-1}) = \mathbb{Q}(\cos\frac{2\pi}{p})$. Přitom libovolné $\alpha \in K_i$ je sestrojitelné pomocí dvou hodnot z K_{i-1}, neboť je kořenem kvadratické rovnice

$$x^2 - \mathrm{Sp}_{K_i/K_{i-1}}(\alpha)x + N_{K_i/K_{i-1}}(\alpha).$$

Příklad. Aplikujme předchozí konstrukci na příklad $p = 5$ (užíváme označení zavedené v předchozím důkaze). Pak $n = 2$, pro $\alpha = \zeta + \zeta^{-1} = 2\cos\frac{2\pi}{5}$ platí $\alpha^2 + \alpha = \zeta^2 + \zeta^{-2} + 2 + \zeta + \zeta^{-1} = 1$ a tedy $2\cos\frac{2\pi}{5}$ je kladný kořen rovnice $x^2 + x - 1$, tj. $\frac{1+\sqrt{5}}{2}$.

Cvičení 14. Nalezněte postup, jak zkonstruovat pravidelný 17-úhelník.

Nyní se zabývejme řešitelností algebraických rovnic, tedy problémem, díky kterému Galoisova teorie vznikla. Zajímá nás, zda pro daný polynom s komplexními koeficienty jsme schopni vyjádřit jeho kořeny pomocí nějakých algebraických výrazů s odmocninami, ve kterých vystupují koeficienty našeho polynomu (a snad ještě nějaká racionální čísla, tedy vlastně čísla z tělesa generovaného nad $\mathbb{Q}$ koeficienty daného polynomu). To jsou ovšem dost vágní pojmy, proto je třeba nejprve upřesnit definici toho, co nás zajímá. Pro jednoduchost se až do konce kapitoly omezíme na tělesa charakteristiky nula (není-li explicitně uvedeno jinak).

Definice. Rozšíření K/k se nazývá radikálové, je-li tvaru $K = k(\alpha_1, \ldots, \alpha_m)$, kde pro každé $i = 1, \ldots, m$ existuje přirozené číslo n_i tak, že platí

$$\alpha_1^{n_1} \in k \qquad \text{a} \qquad \alpha_i^{n_i} \in k(\alpha_1, \ldots \alpha_{i-1}) \quad \text{pro každé } i = 2, \ldots, m.$$

Cvičení 15. Je-li K/k radikálové rozšíření a N je normální uzávěr K/k, pak je N/k radikálové rozšíření. Dokažte.

Definice. Nechť $f(t) \in k[t]$, kde k je těleso charakteristiky nula. Nechť K je rozkladové těleso f nad k. Řekneme, že polynom f je řešitelný v radikálech nad k, existuje-li radikálové rozšíření L/k, které obsahuje K.

Poznámka. Dle cvičení 15 lze navíc požadovat, aby L/k v předchozí definici bylo i normální.

Definice. Nechť $f(t) \in k[t]$, kde k je těleso charakteristiky nula. Nechť K je rozkladové těleso f nad k. Grupu $\mathrm{Gal}(K/k)$ nazýváme Galoisova grupa polynomu f nad k.

Poznámka. Galoisova grupa polynomu f nad k je vlastně jistá grupa permutací kořenů f. Toto je právě způsob, jak Galois zavedl své grupy. A proč je zavedl? Objevil totiž, jak na Galoisově grupě polynomu f nad k poznat, že polynom f je řešitelný v radikálech nad k.

Definice. Řekneme, že grupa G je řešitelná, existuje-li konečná posloupnost jejích podgrup

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

tak, že
1. pro každé $i = 1, \ldots, n$ je grupa G_{i-1} normální podgrupa grupy G_i;
2. pro každé $i = 1, \ldots, n$ je faktorgrupa G_i/G_{i-1} komutativní.

Cvičení 16. Ukažte, že podmínky předchozí definice nezaručují, že grupy G_i jsou normálními podgrupami grupy G. (Návod: uvažte podgrupu normální podgrupy generované permutacemi $(1,2)(3,4)$ a $(1,3)(2,4)$ v grupě všech permutací množiny $\{1,2,3,4\}$.)

Cvičení 17. Nechť G je grupa, H podgrupa G a N normální podgrupa G. Dokažte, že platí:
1. je-li G řešitelná, je i H řešitelná;
2. je-li G řešitelná, je i G/N řešitelná;
3. jsou-li N i G/N řešitelné, je i G řešitelná.

Věta 3. Nad tělesem charakteristiky nula je polynom řešitelný v radikálech, právě když má nad tímto tělesem řešitelnou Galoisovu grupu.

Důkaz první implikace. Předpokládejme, že $f(t) \in k[t]$, kde k je těleso charakteristiky nula, je řešitelný v radikálech nad k a označme K rozkladové těleso f nad k. Pak existuje radikálové rozšíření L/k, které obsahuje K a je normální. L je tedy tvaru $L = k(\alpha_1, \ldots, \alpha_m)$, kde pro každé $i = 1, \ldots, m$ existuje přirozené číslo n_i tak, že platí

$$\alpha_1^{n_1} \in k \qquad \text{a} \qquad \alpha_i^{n_i} \in k(\alpha_1, \ldots \alpha_{i-1}) \quad \text{pro každé } i = 2, \ldots, m.$$

Snadno se vidí, že můžeme navíc předpokládat, že čísla n_i jsou dokonce prvočísla (jinak zvětšíme m a doplníme některé mocniny α_i jako další generátory L). Položme $L_0 = k$ a $L_i = k(\alpha_1, \ldots, \alpha_i)$ pro každé $i = 1, \ldots, m$, tedy $L_m = L$. Označme n nejmenší společný násobek čísel $n_1, \ldots, n_m$ a položme $\zeta = e^{\frac{2\pi i}{n}}$. Protože $k(\zeta)$ je rozkladové těleso polynomu Φ_n nad k, je $k(\zeta)/k$ normální a konečné (viz větu 1 kapitoly 2). Kompozitum dvou konečných normálních rozšíření je normální (opět z věty 1 kapitoly 2), proto je normální i rozšíření $L(\zeta)/k$. Restrikce $\mathrm{Gal}(k(\zeta)/k) \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ je injektivní homomorfismus a $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ je komutativní grupa, proto je

$$\mathrm{Gal}(k(\zeta)/k) \simeq \mathrm{Gal}(L(\zeta)/k)/\,\mathrm{Gal}(L(\zeta)/k(\zeta))$$

komutativní. Uvažme posloupnost podgrup

$$\{\mathrm{id}_{L(\zeta)}\} = \mathrm{Gal}(L(\zeta)/L_m(\zeta)) \subseteq \mathrm{Gal}(L(\zeta)/L_{m-1}(\zeta)) \subseteq \ldots \\ \cdots \subseteq \mathrm{Gal}(L(\zeta)/L_0(\zeta)) \subseteq \mathrm{Gal}(L(\zeta)/k).$$

Abychom ukázali, že $\mathrm{Gal}(L(\zeta)/k)$ je řešitelná, stačí pro každé $i = 1, \ldots, m$ dokázat, že $\mathrm{Gal}(L(\zeta)/L_i(\zeta))$ je normální podgrupa v $\mathrm{Gal}(L(\zeta)/L_{i-1}(\zeta))$ a že faktorgrupa $\mathrm{Gal}(L(\zeta)/L_{i-1}(\zeta))/\,\mathrm{Gal}(L(\zeta)/L_i(\zeta))$ je komutativní, což podle hlavní věty Galoisovy teorie znamená, že $L_i(\zeta)/L_{i-1}(\zeta)$ je normální rozšíření s komutativní Galoisovou grupou. Pro stručnost označme $M = L_{i-1}(\zeta)$, pak $L_i(\zeta) = M(\alpha_i)$. Jestliže $\alpha_i \in M$,

je věc zřejmá. Předpokládejme proto $\alpha_i \notin M$. Platí $\alpha_i^{n_i} \in M$. Označme $\xi = \zeta^{\frac{n}{n_i}}$. Polynom

$$g(t) = t^{n_i} - \alpha_i^{n_i} = \prod_{j=1}^{n_i}(t - \xi^j \alpha_i) \in M[t]$$

má kořen α_i, je tedy dělitelný minimálním mnohočlenem φ_{α_i} prvku α_i nad M. Proto všechny kořeny φ_{α_i} leží v $M(\alpha_i)$ a tedy $M(\alpha_i)/M$ je normální. Označme r stupeň φ_{α_i}, pak absolutní člen φ_{α_i} je roven $\zeta^s \alpha_i^r$ pro vhodné přirozené číslo s, odkud $\alpha_i^r \in M$. Jestliže $r < n_i$, pak existují $a, b \in \mathbb{Z}$ tak, že $ar + bn_i = 1$, neboť n_i je prvočíslo, odkud $\alpha_i = (\alpha_i^r)^a (\alpha_i^{n_i})^b \in M$, spor. Je tedy $r = n_i$ a $[M(\alpha_i) : M] = r$ je prvočíslo. Grupa prvočíselného řádu je ovšem cyklická a tedy komutativní. Důkaz první implikace je ukončen.

Pro důkaz druhé implikace věty 3 dokážeme nejprve dvě lemmata. Následující lemma bývá tradičně označováno jako Hilbertova věta 90, neboť tak bylo označeno v jeho knize Zahlbericht (1893).

Lemma 1. Nechť K/k je Galoisovo rozšíření s cyklickou Galoisovou grupou $G = \mathrm{Gal}(K/k)$ generovanou prvkem $\tau \in G$, přičemž k může být libovolné charakteristiky. Pak pro každé $\alpha \in K$ platí: norma $N_{K/k}(\alpha) = 1$, právě když existuje nenulové $\beta \in K$ tak, že $\alpha = \frac{\beta}{\tau(\beta)}$.

Důkaz. Označme $n = |G|$. Podle důsledku 1 věty 11 kapitoly 1 platí $N_{K/k}(\alpha) = \prod_{i=1}^{n} \tau^i(\alpha)$. Předpokládejme $N_{K/k}(\alpha) = 1$. Pro $\gamma \in K$ položme $\delta_0 = \alpha\gamma$ a pro každé $i = 1, \ldots, n-1$ nechť $\delta_i = \alpha\tau(\delta_{i-1})$. Pak platí $\delta_{n-1} = N_{K/k}(\alpha)\tau^{n-1}(\gamma) = \tau^{n-1}(\gamma)$. Označme $\beta = \sum_{i=0}^{n-1} \delta_i$. Chceme zvolit $\gamma \in L$ tak, aby $\beta \neq 0$. Předpokládejme, že to nejde, tj. že $\beta = 0$ pro každé $\gamma \in L$. Pak ale pro každé $\gamma \in L$ platí $\sum_{i=0}^{n-1} \lambda_i \tau^i(\gamma) = 0$, kde $\lambda_i = \prod_{j=0}^{i} \tau^j(\alpha) \in L$, což je spor s lemmatem 3 ze druhé kapitoly. Je-li $\gamma \in L$ zvoleno tak, že $\beta \neq 0$, platí

$$\tau(\beta) = \sum_{i=0}^{n-1} \tau(\delta_i) = \tau^n(\gamma) + \frac{1}{\alpha} \sum_{i=0}^{n-2} \delta_{i+1} = \frac{1}{\alpha} \sum_{i=0}^{n-1} \delta_i = \frac{\beta}{\alpha},$$

odkud $\alpha = \frac{\beta}{\tau(\beta)}$. Opačná implikace je snadná.

Lemma 2. Nechť K/k je Galoisovo rozšíření prvočíselného stupně $p = [K : k]$. Předpokládejme navíc, že charakteristika k není p a že polynom $t^p - 1$ se v k rozkládá na lineární činitele. Pak existuje $a \in k$ tak, že $K = k(\alpha)$, kde α je kořen polynomu $t^p - a$, který je ireducibilní nad k.

Důkaz. Galoisova grupa $G = \mathrm{Gal}(K/k)$ má prvočíselný řád, je tedy cyklická. Označme τ generátor grupy G. Kořeny polynomu $t^p - 1$ tvoří p-prvkovou podgrupu multiplikativní grupy tělesa k, tj. existuje $\varepsilon \in k$ tak, že $\varepsilon \neq 1$, $\varepsilon^p = 1$. Pak $N_{K/k}(\varepsilon) = \varepsilon^p = 1$ a podle předchozího lemmatu existuje $\alpha \in K$ tak, že $\varepsilon = \frac{\alpha}{\tau(\alpha)}$. Pak platí $\tau(\alpha^p) = \alpha^p$, a tedy $a = \alpha^p \in k$. Dále $k(\alpha) \neq k$, $[k(\alpha) : k] | [K : k] = p$, tedy $[k(\alpha) : k] = p$ a $t^p - a$ je minimální polynom prvku α.

Důkaz druhé implikace věty 3. Nechť $f(t) \in k[t]$, kde k je těleso charakteristiky nula, označme K rozkladové těleso f nad k, a předpokládejme, že grupa $G = \mathrm{Gal}(K/k)$ je řešitelná. Existuje tedy konečná posloupnost jejích podgrup

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

tak, že pro každé $i = 1, \dots, n$ je grupa G_{i-1} normální podgrupa grupy G_i a že pro každé $i = 1, \dots, n$ je faktorgrupa G_i/G_{i-1} komutativní. Můžeme dokonce navíc předpokládat, že faktorgrupy G_i/G_{i-1} mají prvočíselný řád (v opačném případě přidáme další podgrupy). Označíme-li $L_i = G_i^{\perp}$ pro každé $i = 1, \dots, n$, dostáváme posloupnost těles

$$k = L_n \subseteq L_{n-1} \subseteq \cdots \subseteq L_1 \subseteq L_0 = K,$$

přičemž pro každé $i = 1, \dots, n$ rozšíření L_{i-1}/L_i je normální prvočíselného stupně p_i. Označme n nejmenší společný násobek prvočísel $p_1, \dots, p_n$ a položme $\zeta = e^{\frac{2\pi i}{n}}$. Budeme hotovi, když dokážeme, že $K(\zeta)/k$ je radikálové rozšíření. Protože $k(\zeta)$ je rozkladové těleso polynomu Ψ_n nad k, je normální, a protože $\zeta^n \in k$, je radikálové. Bude stačit, ukážeme-li, že rozšíření $L_i(\zeta)/L_{i+1}(\zeta)$ je radikálové pro každé $i = 0, \dots, n-1$. To je jistě splněno, je-li $L_i(\zeta) = L_{i+1}(\zeta)$, proto předpokládejme $L_i(\zeta) \neq L_{i+1}(\zeta)$. Protože je $L_i(\zeta)$ kompozitum normálních rozšíření L_i a $L_{i+1}(\zeta)$ tělesa L_{i+1}, je $L_i(\zeta)/L_{i+1}$ normální (opět z věty 1 kapitoly 2). Proto je normální i rozšíření $L_i(\zeta)/L_{i+1}(\zeta)$. Restrikce $\mathrm{Gal}(L_i(\zeta)/L_{i+1}(\zeta)) \to \mathrm{Gal}(L_i/L_{i+1})$ je injektivní homomorfismus a tedy $[L_i(\zeta) : L_{i+1}(\zeta)] = p_i$. Označme $\xi = \zeta^{\frac{n}{p_i}}$. Polynom

$$t^{p_i} - 1 = \prod_{j=1}^{p_i} (t - \xi^j)$$

se v $L_{i+1}(\zeta)$ rozkládá na lineární činitele a podle lemmatu 2 je $L_i(\zeta)/L_{i+1}(\zeta)$ radikálové. Věta 3 je dokázána.

Definice. Nechť p je prvočíslo. Konečná grupa se nazývá p-grupa, je-li její řád (tj. počet prvků) mocnina p.

Definice. Nechť G je grupa. Centrum grupy G je množina

$$C = \{a \in G;\ \forall x \in G :\ a \cdot x = x \cdot a\}.$$

Lemma 3. Nechť p je prvočíslo. Libovolná konečná p-grupa je řešitelná.

Důkaz. Tvrzení plyne z toho, že centrum grupy je normální podgrupa (viz např. skriptum J. Rosický: Algebra, Brno 1982, věta 10.5 na str. 49) a že centrum konečné p-grupy je netriviální (tamtéž, věta 10.14 na str. 54).

Definice. Řekneme, že komplexní číslo α je sestrojitelné kružítkem a pravítkem, existuje-li radikálové rozšíření $K/\mathbb{Q}$ takové, že $\alpha \in K$ a $[K : \mathbb{Q}] = 2^r$ pro nějaké přirozené číslo r.

Cvičení 18. Nechť N je normální uzávěr radikálového rozšíření K/k. Je-li $[K : k]$ mocnina 2, pak je i $[N : k]$ mocnina 2. Dokažte. Ukažte rovněž, že pro libovolné liché prvočíslo analogické tvrzení neplatí.

Poznámka. V předchozím cvičení je předpoklad radikálového rozšíření podstatný, neboť například Galoisova grupa polynomu $x^4 + 3x^2 + 3x + 3$ je symetrická grupa S_4. Tento fakt však není tak snadné ověřit (viz konec této kapitoly).

Věta 4. Nechť α je algebraické komplexní číslo, φ_α jeho minimální polynom nad $\mathbb{Q}$. Pak α je sestrojitelné kružítkem a pravítkem, právě když Galoisova grupa polynomu φ_α je 2-grupa.

Důkaz. Plyne z věty 3 s přihlédnutím k cvičení 18 a lemmatu 3.

Zabývejme se nyní problémem, jak pro daný ireducibilní polynom určit jeho Galoisovu grupu. Už v předchozí poznámce jsme se zmínili o tom, že to může být nelehký úkol. Jeden velmi speciální případ řeší následující tvrzení.

Věta 5. Nechť p je prvočíslo a $f \in \mathbb{Q}[t]$ ireducibilní polynom stupně p, který má právě $p-2$ reálných kořenů. Pak Galoisova grupa polynomu f je symetrická grupa S_p.

Důkaz. Galoisova grupa polynomu f má řád dělitelný p, proto obsahuje prvek řádu p (viz např. zmíněné skriptum J. Rosického, důsledek 10.9 na str. 51), který na kořenech polynomu p musí účinkovat jako p-cyklus. Komplexní konjugovanost na nich účinkuje jako transpozice. Ovšem transpozice a p-cyklus spolu vygenerují celou S_p.

Příklad. Polynom $t^5 - 6t + 3$ není řešitelný v radikálech nad $\mathbb{Q}$.

Cvičení 19. Nechť $f(t) \in k[t]$ je ireducibilní polynom nad tělesem k charakteristiky nula. Rozložme

$$f(t) = (t - \alpha_1) \dots (t - \alpha_n)$$

v rozkladovém tělese K polynomu f nad k. Označme

$$\delta = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)$$

(pak δ^2 je diskriminant D polynomu f, přičemž $D = D(1, \alpha_1, \dots, \alpha_1^{n-1}) \in k$ - viz kapitola 1). Dokažte, že Galoisova grupa polynomu f nad k neobsahuje žádnou lichou permutaci, právě když $\delta \in k$ (což nastane právě tehdy, když D je druhou mocninou v k).

Poznámka. Protože Galoisova grupa ireducibilního polynomu je tranzitivní (tj. pro libovolnou dvojici jeho kořenů existuje automorfismus převádějící jeden na druhý), v případě ireducibilního kubického polynomu je Galoisovou grupou buď symetrická grupa S_3 nebo alternující grupa A_3 (tj. grupa sudých permutací). Tyto dva případy rozliší předchozí cvičení.

Zmiňme se na závěr o případu ireducibilního polynomu čtvrtého stupně. Jediné tranzitivní grupy permutací čtyř prvků jsou symetrická grupa S_4, alternující grupa A_4, Kleinova čtyřgrupa V (generovaná permutacemi $(1,2)(3,4)$ a $(1,3)(2,4)$), grupa symetrií čtverce D_8 (generovaná V a permutací $(1,2)$) a cyklická grupa C_4. Jde o to, jak mezi těmito pěti případy rozlišit. Nechť $f(t) = t^4 + pt^2 + qt + r \in \mathbb{Q}[t]$ je ireducibilní nad $\mathbb{Q}$. Označme jeho kořeny $\alpha_1, \dots, \alpha_4$ a položme

$$\begin{aligned}
\beta_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = -(\alpha_1 + \alpha_2)^2 \\
\beta_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) = -(\alpha_1 + \alpha_3)^2 \\
\beta_3 &= (\alpha_1 + \alpha_4)(\alpha_1 + \alpha_4) = -(\alpha_1 + \alpha_4)^2.
\end{aligned}$$

Cvičením na symetrické polynomy je ověření, že pak

$$g(t) = (t - \beta_1)(t - \beta_2)(t - \beta_3) = t^3 - 2pt^2 + (p^2 - 4r)t + q^2$$

(tzv. kubická rezolventa). Označme D diskriminant f, M rozkladové těleso g. Je možné dokázat, že Galoisova grupa polynomu f nad k je

- S_4 právě když D není druhou mocninou v $\mathbb{Q}$ a g je ireducibilní nad $\mathbb{Q}$;
- A_4 právě když D je druhou mocninou v $\mathbb{Q}$ a g je ireducibilní nad $\mathbb{Q}$;
- D_8 právě když D není druhou mocninou v $\mathbb{Q}$, g není ireducibilní nad $\mathbb{Q}$ a f je ireducibilní nad M;
- V právě když D je druhou mocninou v $\mathbb{Q}$ a g není ireducibilní nad $\mathbb{Q}$;
- C_4 právě když D není druhou mocninou v $\mathbb{Q}$, g není ireducibilní nad $\mathbb{Q}$ a f není ireducibilní nad M.

Poznámka. V rámci systému PARI-GP existuje funkce `galois(`f`)`, která pro ireducibilní polynom f nad $\mathbb{Q}$ stupně nejvýše 7 počítá jeho Galoisovu grupu nad $\mathbb{Q}$.

5. Rozložitelné formy

(důkazy viz Borevič-Šafarevič, kapitola 2, §§1–2)

Problémem, ze kterého teorie čísel historicky vznikla, je řešení diofantických rovnic. V následujícím textu se budeme zabývat diofantickou rovnicí speciálního tvaru: v $\mathbb{Z}$ budeme řešit rovnici

$$F(x_1, \ldots, x_n) = a,$$

kde a je racionální číslo a $F(x_1, \ldots, x_n)$ je forma (tj. nenulový homogenní polynom) s racionálními koeficienty. Uspokojivého výsledku dosáhneme v případě, kdy je forma $F(x_1, \ldots, x_n)$ ireducibilní nad $\mathbb{Q}$ (tj. je ireducibilní prvek v okruhu s jednoznačným rozkladem $\mathbb{Q}[x_1, \ldots, x_n]$), rozložitelná (tj. rozkládá se na lineární faktory v okruhu $K[x_1, \ldots, x_n]$ pro nějaké rozšíření $K/\mathbb{Q}$) a úplná (pro přesnou definici viz níže).

Definice. Dvě formy téhož stupně n s racionálními koeficienty se nazývají celočíselně ekvivalentní, pokud libovolnou z nich je možné získat lineární transformací s celočíselnými koeficienty z té druhé.

Příklad. Formy $x^2 + 7y^2 + z^2 - 6xy - 2xy + 6yz$ a $2u^2 - v^2$ jsou celočíselně ekvivalentní. Stačí uvážit transformace

$$\begin{aligned} x &= 3v \\ y &= u + v \\ z &= -u + v \end{aligned} \qquad \text{a} \qquad \begin{aligned} u &= -x + 2y + z \\ v &= x - y - z \end{aligned}$$

Lemma 1. Libovolná forma stupně n s racionálními koeficienty je celočíselně ekvivalentní s formou mající u n-té mocniny některé z proměnných nenulový koeficient.

Definice. Libovolné konečné rozšíření K tělesa $\mathbb{Q}$ se nazývá těleso algebraických čísel. Celý uzávěr $\mathbb{Z}$ v K (tj. okruh všech čísel tělesa K, které jsou celé vzhledem k $\mathbb{Z}$, viz kapitola 3) se nazývá okruh celých čísel tělesa K.

Upozornění. Těleso všech algebraických čísel není tělesem algebraických čísel.

Věta 1. Libovolná rozložitelná forma s racionálními koeficienty se rozkládá na lineární faktory už nad nějakým tělesem algebraických čísel.

Konstrukce. Nechť K je těleso algebraických čísel, $[K : \mathbb{Q}] = n$. Označme $\tau_1, \dots, \tau_n$ různá vnoření $K \to \mathbb{C}$ (viz větu 11 kapitoly 1). Zvolme $\mu_1, \dots, \mu_m \in K$ a položme

$$(*) \qquad F(x_1, \dots, x_m) = \prod_{j=1}^{n} (\tau_j(\mu_1)x_1 + \cdots + \tau_j(\mu_m)x_m).$$

Existuje $\theta \in K$ tak, že $K = \mathbb{Q}(\theta)$ (viz větu 10 kapitoly 1). Pak $\mu_1 = g_1(\theta)$, ..., $\mu_m = g_m(\theta)$ pro vhodné $g_1, \dots, g_m \in \mathbb{Q}[t]$. Označme $\theta_j = \tau_j(\theta)$. Protože koeficienty

$$F(x_1, \dots, x_m) = \prod_{j=1}^{n} (g_1(\theta_j)x_1 + \cdots + g_m(\theta_j)x_m)$$

jsou hodnotami symetrických polynomů v $\theta_1, \dots, \theta_n$ a minimální polynom $\varphi_\theta = \prod_{j=1}^{n}(t - \theta_j) \in \mathbb{Q}[t]$, má forma F racionální koeficienty. Navíc pro libovolná racionální čísla $a_1, \dots, a_m$ platí

$$F(a_1, \dots, a_m) = N_{K/\mathbb{Q}}(a_1\mu_1 + \cdots + a_m\mu_m)$$

podle důsledku 1 věty 11 kapitoly 1.

Věta 2. Je-li $\mu_1 = 1$ a $K = \mathbb{Q}(\mu_2, \dots, \mu_m)$, pak forma F určená předpisem (*) je ireducibilní nad $\mathbb{Q}$. Naopak, každá forma s racionálními koeficienty, která je ireducibilní nad $\mathbb{Q}$ a rozložitelná, je až na konstantní násobek celočíselně ekvivalentní s formou F tvaru (*), kde $\mu_1 = 1$ a $K = \mathbb{Q}(\mu_2, \dots, \mu_m)$.

Definice. Nechť K je těleso algebraických čísel. Podgrupa aditivní grupy tělesa K s konečně mnoha generátory se nazývá modul.

Poznámky. 1. Nechť K je těleso algebraických čísel. Je-li $\mu_1, \dots, \mu_m \in K$, pak modul generovaný $\mu_1, \dots, \mu_m$ je roven

$$\{a_1\mu_1 + \cdots + a_m\mu_m;\ a_1, \dots, a_m \in \mathbb{Z}\}.$$

Problém řešit v $\mathbb{Z}$ rovnici

$$F(x_1, \dots, x_n) = a,$$

kde $F(x_1, \dots, x_n)$ je ireducibilní nad $\mathbb{Q}$ rozložitelná forma s racionálními koeficienty, $a \in \mathbb{Q}$, jsme přeformulovali na problém v daném modulu algebraických čísel najít všechna čísla, jejichž norma je dané racionální číslo.

2. Zvolíme-li v daném modulu dva systémy generátorů a předpisem (*) k nim sestrojíme odpovídající formy, budou získané formy celočíselně ekvivalentní.

Definice. Nechť K je těleso algebraických čísel. Modul M v K se nazývá úplný, generuje-li celé K jakožto vektorový prostor nad $\mathbb{Q}$ (tj. existuje-li v něm $[K : \mathbb{Q}]$ čísel lineárně nezávislých nad $\mathbb{Q}$). Forma odpovídající předpisem (*) úplnému modulu, se nazývá úplná.

Poznámky. 1. Úplné formy stupně n je možné charakterizovat tím, že nejsou celočíselně ekvivalentní s žádnou formou s méně než n proměnnými.

2. Každý modul je konečně generovaná komutativní grupa bez torze (tj. jediný prvek konečného řádu je 0).

Definice. Nechť $(G,+)$ je konečně generovaná komutativní grupa bez torze, $\alpha_1,\dots,\alpha_n$ nějaký systém jejích generátorů. Řekneme, že systém $\alpha_1,\dots,\alpha_n$ je bazí grupy G, je-li $\mathbb{Z}$-lineárně nezávislý, tj. jestliže pro libovolné $a_1,\dots,a_n\in\mathbb{Z}$ platí

$$a_1\alpha_1+\dots+a_n\alpha_n=0 \implies a_1=\dots=a_n=0.$$

Věta 3. Každá konečně generovaná komutativní grupa bez torze má bazi. Všechny baze této grupy mají stejný počet prvků.

Definice. Počet prvků baze konečně generované komutativní grupy bez torze se nazývá rank této grupy.

Věta 4. Nechť G je konečně generovaná komutativní grupa bez torze, H její podgrupa. Pak H má bazi. Navíc platí: je-li $\omega_1,\dots,\omega_m$ libovolná baze grupy G, pak po vhodném přeindexování $\omega_1,\dots,\omega_m$ existuje baze $\eta_1,\dots,\eta_k$ podgrupy H tvaru

$$\begin{aligned}
\eta_1 &= c_{11}\omega_1 + c_{12}\omega_2 +\dots+ c_{1k}\omega_k +\dots+ c_{1m}\omega_m\\
\eta_2 &= \qquad\quad c_{23}\omega_2 +\dots+ c_{2k}\omega_k +\dots+ c_{2m}\omega_m\\
&\vdots\\
\eta_k &= \qquad\qquad\qquad\quad c_{kk}\omega_k +\dots+ c_{km}\omega_m
\end{aligned}$$

kde c_{ij} jsou celá čísla, $c_{ii}>0$ a $k\le m$.

Důsledek 1. Nechť G je konečně generovaná komutativní grupa bez torze s bazí $\omega_1,\dots,\omega_m$, H její podgrupa generovaná prvky $\eta_1,\dots,\eta_m\in G$. Nechť c_{ij} jsou celá čísla splňující $\eta_i=\sum_{j=1}^m c_{ij}\omega_j$ pro každé $i=1,\dots,n$. Pak platí:

(a) $|G/H|=\infty$, právě když $\det(c_{ij})=0$;
(b) je-li $\det(c_{ij})\neq 0$, pak $|G/H|=|\det(c_{ij})|$.

Důsledek 2. Libovolná podgrupa modulu v tělese algebraických čísel je opět modul.

Definice. Nechť M je úplný modul v tělese algebraických čísel K, $\alpha\in K$. Řekneme, že α je násobitel modulu M, platí-li $\alpha M\subseteq M$.

Poznámka. Je zřejmé, že množina všech násobitelů daného úplného modulu M v tělese algebraických čísel tvoří okruh s jedničkou. Nazýváme jej okruh násobitelů modulu M.

Definice. Úplný modul v tělese algebraických čísel K, který je okruh s jedničkou, se nazývá pořádek tělesa K.

Poznámka. Libovolný pořádek tělesa algebraických čísel K je podokruhem okruhu celých čísel tělesa K (viz kapitola 3).

Věta 5. Nechť K je těleso algebraických čísel, R pořádek tělesa K. Číslo $\alpha\in R$ je jednotkou (tj. invertibilním prvkem) okruhu R, právě když je norma $N_{K/\mathbb{Q}}(\alpha)=\pm1$.

Věta 6. Nechť K je těleso algebraických čísel. Pak okruh násobitelů libovolného úplného modulu v tělese K tvoří pořádek tělesa K. Naopak, každý pořádek tělesa K je okruh násobitelů nějakého úplného modulu (například sebe sama).

Definice. Nechť M je úplný modul v tělese algebraických čísel, $\mu, \nu \in M$. Řekneme, že μ a ν jsou asociované v modulu M, je-li podíl $\frac{\mu}{\nu}$ jednotkou okruhu násobitelů modulu M.

Věta 7. Nechť M je úplný modul v tělese algebraických čísel, $a \in \mathbb{Q}$. Pak v M existuje jen konečně mnoho po dvou neasociovaných čísel, jejichž norma je a.

Poznámka. Problém v daném modulu algebraických čísel najít všechna čísla, jejichž norma je dané racionální číslo, jsme rozložili na dva podproblémy:

1. najít v daném modulu oněch konečně mnoho po dvou neasociovaných čísel s danou normou;
2. najít v okruhu násobitelů daného modulu všechny jednotky s normou 1.

Definice. Nechť K je těleso algebraických čísel. Vnoření $\sigma : K \to \mathbb{C}$ se nazývá reálné, je-li $\sigma(K) \subset \mathbb{R}$, a komplexní v opačném případě. Je-li $\sigma : K \to \mathbb{C}$ komplexní vnoření, pak též vnoření $\bar{\sigma} : K \to \mathbb{C}$ určené předpisem $\bar{\sigma}(x) = \overline{\sigma(x)}$ je komplexní vnoření. Řekneme, že pak σ a $\bar{\sigma}$ tvoří pár sdružených komplexních vnoření.

Poznámky. 1.Existuje-li pro těleso algebraických čísel K právě s reálných vnoření $K \to \mathbb{C}$ a právě t párů sdružených komplexních vnoření $K \to \mathbb{C}$, pak $s + 2t = [K : \mathbb{Q}]$.

2. V tělese algebraických čísel K existuje jen konečně mnoho odmocnin z jedné (tj. čísel ζ, pro které existuje přirozené číslo m s vlastností $\zeta^m = 1$). Jestliže totiž $\cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m} \in K$, pak $\varphi(m)|[K : \mathbb{Q}]$. Navíc platí: existuje-li aspoň jedno reálné vnoření $K \to \mathbb{C}$, pak jediné odmocniny z jedné v K jsou 1 a -1.

Dirichletova věta o jednotkách. Nechť K je těleso algebraických čísel. Nechť existuje právě s reálných vnoření $K \to \mathbb{C}$ a právě t párů sdružených komplexních vnoření $K \to \mathbb{C}$. Nechť R je libovolný pořádek tělesa K. Pak existují takové jednotky $\varepsilon_1, \ldots, \varepsilon_r$ okruhu R, kde $r = s + t - 1$, že libovolnou jednotku ε okruhu R lze jednoznačně vyjádřit ve tvaru

$$\varepsilon = \zeta\varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r},$$

kde $a_1, \ldots, a_r \in \mathbb{Z}$ a $\zeta \in R$ je nějaká odmocnina z jedné.

Důkaz viz Borevič-Šafarevič, kapitola 2, §§3–4

6. Teorie divizorů v oborech integrity

(důkazy viz Borevič-Šafarevič, kapitola 3, §3)

Definice. Nechť D je komutativní pologrupa s jednotkovým prvkem e. Pro $a, b \in D$ řekneme, že a je dělitelem b (označíme $a|b$), jestliže existuje $c \in D$ tak, že $ac = b$. Řekneme, že $p \in D$ je ireducibilní, jestliže $p \nmid e$ a pro každé $a, b \in D$ z $p = ab$ plyne $a|e$ nebo $b|e$.

Definice. Řekneme, že D je pologrupa s jednoznačným rozkladem, jestliže D je komutativní pologrupa, ve které každý prvek a může být zapsán ve tvaru $a = p_1 \ldots p_r$, kde $r \geq 0$ a $p_1, \ldots, p_r \in D$ jsou ireducibilní (pro $r = 0$ je součin roven e) a navíc je tento rozklad určen jednoznačně až na pořadí činitelů.

Poznámka. V pologrupě s jednoznačným rozkladem je e jediný invertibilní prvek. Každá pologrupa s jednoznačným rozkladem je jednoznačně určena množinou

svých ireducibilních prvků. V pologrupě s jednoznačným rozkladem existuje největší společný dělitel a nejmenší společný násobek libovolné konečné množiny prvků.

Definice. Teorie divizorů oboru integrity R je homomorfismus $\delta : R^\times \to D$ multiplikativní pologrupy $R^\times$ do pologrupy D s jednoznačným rozkladem, který splňuje následující podmínky:

1. pro libovolné $\alpha, \beta \in R^\times$ platí $\alpha|\beta$ v R, právě když $\delta(\alpha)|\delta(\beta)$ v D;
2. pro libovolné $\alpha, \beta \in R$ a libovolné $c \in D$ platí: jestliže $c|\delta(\alpha)$ a $c|\delta(\beta)$, pak $c|\delta(\alpha \pm \beta)$;
3. pro libovolné $a, b \in D$ platí: jestliže $\{\alpha \in R^\times;\ a|\delta(\alpha)\} = \{\alpha \in R^\times;\ b|\delta(\alpha)\}$, pak $a = b$.

Poznámky. Prvky pologrupy D nazýváme divizory, ireducibilní prvky pologrupy D nazýváme prvodivizory. Obvykle označení homomorfismu δ vynecháváme a místo $\delta(\alpha)$ píšeme pouze (α) a hovoříme o hlavním divizoru. Pro $\alpha \in R$ a $a \in D$ klademe $a|\alpha$ právě když $\alpha = 0$ nebo $a|(\alpha)$ v D.

Cvičení 20. (L. Skula) Nechť R je obor integrity, D pologrupa s jednoznačným rozkladem, $\delta : R^\times \to D$ homomorfismus. Dokažte, že

(1) podmínka 3. v definici teorie divizorů je ekvivalentní s podmínkou: pro každé $a \in D$ existují $\alpha_1, \ldots, \alpha_n \in R^\times$ tak, že a je největší společný dělitel prvků $\delta(\alpha_1), \ldots, \delta(\alpha_n)$;
(2) platí-li pro homomorfismus δ podmínka 3. v definici teorie divizorů, pak pro každé $a \in D$ existují $\alpha_1, \ldots, \alpha_n, \beta \in R^\times$ tak, že $a\delta(\beta)$ je nejmenší společný násobek prvků $\delta(\alpha_1), \ldots, \delta(\alpha_n)$;
(3) podmínka 2. v definici teorie divizorů je důsledkem podmínek 1. a 3.

Poznámka. Výsledek obsažený v předchozím cvičení je přes svou jednoduchost významný: umožnil zobecnit pojem teorie divizorů z oborů integrity na komutativní pologrupy.

Cvičení 21. Mějme teorii divizorů oboru integrity R. Dokažte, že každý divizor je největší společný dělitel nějakých dvou hlavních divizorů.

Věta 1. Existuje-li pro obor integrity R teorie divizorů, je jediná. Přesněji: jsou-li $\delta_1 : R^\times \to D_1$ a $\delta_2 : R^\times \to D_2$ teorie divizorů, pak existuje izomorfismus $f : D_1 \to D_2$ takový, že $f \circ \delta_1 = \delta_2$.

Poznámka. Obory integrity, které mají teorii divizorů, se nazývají Krullovy okruhy.

Věta 2. Nechť R je obor integrity. Pak R je okruh s jednoznačným rozkladem, právě když pro R existuje teorie divizorů, v níž je každý divizor hlavní.

Věta 3. Nechť R je obor integrity, pro který existuje teorie divizorů, pak je R celouzavřený (ve svém podílovém tělese).

Definice. Nechť K je těleso. Zobrazení $\nu : K \to \mathbb{Z} \cup \{\infty\}$ se nazývá exponent tělesa K, jestliže platí

(1) $\nu(0) = \infty$, $\nu(K^\times) = \mathbb{Z}$;
(2) pro libovolné $\alpha, \beta \in K$ je $\nu(\alpha\beta) = \nu(\alpha) + \nu(\beta)$;
(3) pro libovolné $\alpha, \beta \in K$ je $\nu(\alpha + \beta) \geq \min\{\nu(\alpha), \nu(\beta)\}$.

Poznámky. 1. Je-li R je obor integrity, pro který existuje teorie divizorů, a p je prvodivizor, pak můžeme pro $\alpha \in R^\times$ definovat $\nu(\alpha)$ jako exponent, se kterým

vystupuje prvodivizor p v rozkladu divizoru (α). Pak ν splňuje předchozí podmínky (2) a (3) a platí $\nu(R^\times) = \mathbb{N} \cup \{0\}$. Definici ν pak lze rozšířit na celé podílové těleso K oboru integrity R takto: $\nu(0) = \infty$ a libovolné $\gamma \in K^\times$ zapíšeme ve tvaru $\gamma = \frac{\alpha}{\beta}$ a položíme $\nu(\gamma) = \nu(\alpha) - \nu(\beta)$. Snadno se ověří korektnost této definice i to, že ν je exponent tělesa K.

2. Máme-li teorii divizorů oboru integrity R, pak máme pro každý prvodivizor odpovídající exponent tělesa K, přičemž exponenty odpovídající různým prvodivizorům jsou různé. Na druhou stranu daná teorie divizorů je množinou všech exponentů odpovídajích prvodivizorům jednoznačně určena.

Věta 4. Nechť R je obor integrity s podílovým tělesem K, M nějaká množina exponentů tělesa K. K tomu, aby M byla množinou všech exponentů odpovídajích prvodivizorům nějaké teorie divizorů okruhu R, je nutné a stačí, aby platilo

(1) pro každé $\alpha \in R^\times$ existuje jen konečně mnoho $\nu \in M$ s vlastností $\nu(\alpha) \neq 0$;
(2) pro každé $\alpha \in K$ platí $\alpha \in R$ právě tehdy, když $\nu(\alpha) \geq 0$ pro všechny $\nu \in M$;
(3) pro libovolné různé exponenty $\nu_1, \ldots, \nu_m \in M$ a libovolná nezáporná celá čísla $k_1, \ldots, k_m$ existuje $\alpha \in R$ tak, že $\nu_1(\alpha) = k_1, \ldots, \nu_m(\alpha) = k_m$.

Cvičení 22. Absolutní hodnota určuje teorii divizorů $\mathbb{Z}^\times \to \mathbb{N}$. Ukažte, že libovolný exponent tělesa $\mathbb{Q}$ odpovídá nějakému prvodivizoru (tj. prvočíslu).

Cvičení 23. Je-li R obor integrity, pro který existuje teorie divizorů s konečně mnoha prvodivizory, pak je R okruh s jednoznačným rozkladem. Dokažte.

7. Exponenty

(podrobnější důkazy viz Borevič-Šafarevič, kapitola 3, §4)

Definice. Nechť ν je exponent tělesa K. Okruh

$$O_\nu = \{\alpha \in K;\, \nu(\alpha) \geq 0\}$$

se nazývá okruh exponentu ν.

Z vět 3 a 4 předchozí kapitoly plyne platnost následujících dvou vět:

Věta 1. Okruh O_ν exponentu ν tělesa K je celouzavřený v K.

Věta 2. Až na asociovanost existuje jediný ireducibilní prvek π okruhu O_ν (charakterizovaný podmínkou $\nu(\pi) = 1$). Libovolné nenulové $\alpha \in O_\nu$ lze (při zafixovaném π) jednoznačně vyjádřit ve tvaru $\alpha = \varepsilon\pi^m$, kde ε je jednotka okruhu O_ν a m nezáporné celé číslo.

Je zřejmé, že $I_\nu = \{\alpha \in K;\, \nu(\alpha) > 0\}$ je ideál okruhu O_ν, že $O_\nu \setminus I_\nu$ je grupa jednotek okruhu O_ν a že faktorokruh O_ν/I_ν je těleso.

Definice. Nechť ν je exponent tělesa K. Faktorokruh O_ν/I_ν se nazývá těleso zbytků exponentu ν.

Věta 3. Pro libovolné různé exponenty $\nu_1, \ldots, \nu_m$ tělesa K a libovolná celá čísla $k_1, \ldots, k_m$ existuje $\alpha \in K$ tak, že $\nu_1(\alpha) = k_1, \ldots, \nu_m(\alpha) = k_m$.

Důsledek. Nechť $\nu_1, \ldots, \nu_m$ jsou libovolné po dvou různé exponenty tělesa K, $O_{\nu_1}, \ldots, O_{\nu_m}$ jejich okruhy. Pak průnik $O = \cap_{i=1}^m O_{\nu_i}$ je okruh s jednoznačným

rozkladem na ireducibilní prvky. Přesněji: zvolíme-li libovolně $\pi_1, \dots, \pi_m \in K$ tak, aby platilo

$$\nu_i(\pi_j) = \begin{cases} 1, & \text{je-li } i = j, \\ 0, & \text{je-li } i \neq j, \end{cases}$$

pak libovolné $\alpha \in O$, $\alpha \neq 0$, lze jednoznačně vyjádřit ve tvaru $\alpha = \varepsilon \pi_1^{k_1} \dots \pi_m^{k_m}$, kde ε je jednotka okruhu O a $k_1, \dots, k_m$ nezáporná celá čísla.

Náznak důkazu věty 3. Indukcí vzhledem k m. Nejprve dokažme, že $\nu_1, \dots, \nu_m$ jsou $\mathbb{Q}$-lineárně nezávislé na $K^\times$. Kdyby ne, existovala by (případně po záměně indexů) čísla $a_2, \dots, a_m \in \mathbb{Q}$, alespoň jedno záporné, tak, že $\nu_1(\alpha) = \sum_{i=2}^m a_i \nu_i(\alpha)$ pro každé $\alpha \in K^\times$. Zvolme (indukční předpoklad) $\alpha_1, \alpha_2 \in K^\times$ tak, aby pro každé $i = 2, \dots, m$ platilo

$$\nu_i(\alpha_1) = \begin{cases} 0, & \text{je-li } a_i \geq 0, \\ 1, & \text{je-li } a_i < 0, \end{cases} \qquad \nu_i(\alpha_2) = \begin{cases} 1, & \text{je-li } a_i \geq 0, \\ 0, & \text{je-li } a_i < 0. \end{cases}$$

Pak $\nu_i(\alpha_1 + \alpha_2) = 0$ pro každé $i = 2, \dots, m$ a $\nu_1(\alpha_1 + \alpha_2) < 0$, spor.

Uvažme okruh $O = \cap_{i=1}^{m-1} O_{\nu_i}$ a jeho grupu jednotek E. Kdyby $\nu_m(E) = \{0\}$, dostali bychom, že ν_m je $\mathbb{Q}$-lineární kombinace $\nu_1, \dots, \nu_{m-1}$, což není možné.

Nechť $\pi_1, \dots, \pi_{m-1}$ vyhovují podmínkám důsledku pro $\nu_1, \dots, \nu_{m-1}$ (jejich existence plyne z indukčního předpokladu), označme $a_1 = \nu_m(\pi_1)$, $\dots$, $a_{m-1} = \nu_m(\pi_{m-1})$. Zvolme $\gamma \in E$ tak, aby $l = \nu_m(\gamma)$ bylo kladné a co nejmenší. Jestliže $l | a_1$, $\dots$, $l | a_{m-1}$, pak $l = 1$ z definice exponentu. V opačném případě dojdeme ke sporu: předpokládejme například, že $l \nmid a_1$ a uvažme $\alpha = \pi_1 (\pi_2 \cdot \ldots \cdot \pi_{m-1})^l \gamma^s$, kde s je zvoleno tak, aby $l' = a_1 + (a_2 + \dots + a_{m-1})l + sl$ splňovalo $0 < l' < l$. Pak $\nu_m(\alpha) = l'$ a $\nu_i(\alpha) > 0$ pro $i = 1, \dots, m-1$. Potom $\varepsilon = \gamma + \alpha \in E$ a platí $\nu_m = l'$, spor.

Je tedy $l = 1$ a lze předpokládat, že $\nu_m(\pi_i) = 0$ pro $i = 1, \dots, m-1$. Pak je $\alpha = \pi_1^{k_1} \dots \pi_{m-1}^{k_{m-1}} \gamma^{k_m}$ hledaný prvek a věta 3 je dokázána.

Věta 4 (o aproximaci). Pro libovolné různé exponenty $\nu_1, \dots, \nu_m$ tělesa K, libovolné $\alpha_1, \dots, \alpha_m \in K$ a libovolné přirozené číslo N existuje $\alpha \in K$ tak, že $\nu_1(\alpha - \alpha_1) \geq N$, $\dots$, $\nu_m(\alpha - \alpha_m) \geq N$.

Důkaz. Zvolme v K prvky splňující

$$\nu_i(\beta_j) = \begin{cases} -1, & \text{je-li } i = j, \\ 1, & \text{je-li } i \neq j, \end{cases}$$

a položme

$$\alpha = \sum_{i=1}^m \frac{\beta_i^k}{1 + \beta_i^k} \alpha_i,$$

kde $k \geq N - \min\{\nu_i(\alpha_j);\, 1 \leq i \leq m, 1 \leq j \leq m\}$. Pak α splňuje podmínky věty.

Poznámka. Nechť K/k je konečné rozšíření těles a ν exponent tělesa K. Protože K je celý uzávěr k v K, nemůže být $\nu(k) = \{0\}$ (z $k \subseteq O_\nu$ by dle věty 1 plynulo $K \subseteq O_\nu$, spor).

Zvolme $p \in k$ tak, aby $e = \nu(p)$ bylo kladné a co nejmenší. Pak $e|\nu(a)$ pro každé $a \in k$. Snadno se ověří, že $\nu_0 : k \to \mathbb{Z} \cup \{\infty\}$, určené předpisem $\nu_0(0) = \infty$ a $\nu_0(a) = \frac{\nu(a)}{e}$ pro $a \in k^\times$, je exponent tělesa k.

Definice. Jsou-li ν a ν_0 ve vztahu z předchozí poznámky, řekneme, že exponent ν_0 je indukován exponentem ν a že exponent ν je prodloužením exponentu ν_0. Číslo e se nazývá index větvení exponentu ν vzhledem k ν_0.

Lemma 1. Nechť K/k je konečné rozšíření těles stupně n a ν_0 exponent tělesa k. Pak existuje nejvýše n prodloužení exponentu ν_0 na těleso K.

Důkaz. Nechť $\nu_1, \ldots, \nu_m$ jsou různá prodloužení exponentu ν_0 na těleso K. Zvolme v K prvky splňující

$$\nu_i(\beta_j) = \begin{cases} 0, & \text{je-li } i = j, \\ 1, & \text{je-li } i \neq j. \end{cases}$$

Pak $\beta_1, \ldots \beta_m$ jsou k-lineárně nezávislé.

Lemma 2. Nechť K/k je konečné rozšíření těles a ν_0 exponent tělesa k. Uvažme okruh $O_{\nu_0} \subseteq k$ exponentu ν_0 tělesa k a označme O celý uzávěr okruhu O_{ν_0} v K. Je-li O okruh s jednoznačným rozkladem s právě m po dvou neasociovanými ireducibilními prvky, pak existuje právě m různých prodloužení $\nu_1, \ldots, \nu_m$ exponentu ν_0 na těleso K. Navíc platí $O = \cap_{i=1}^m O_{\nu_i}$.

Důkaz. Označme $\pi_1, \ldots, \pi_m$ ony ireducibilní prvky okruhu O. Podle věty 2 kapitoly 6 má O teorii divizorů s právě m prvodivizory $(\pi_1), \ldots, (\pi_m)$. Jsou-li $\nu_1, \ldots, \nu_m$ jim odpovídající exponenty, z věty 4 kapitoly 6 (podmínka 2) plyne $O = \cap_{i=1}^m O_{\nu_i}$. Zvolme ireducibilní prvek π okruhu O_{ν_0} (viz větu 2). Pak v O lze rozložit $\pi = \varepsilon \prod_{i=1}^m \pi_i^{e_i}$, kde ε je jednotka okruhu O a $e_1, \ldots, e_m$ jsou nezáporná celá čísla. Pro libovolné $\alpha \in O_{\nu_0}$ pak existuje rozklad $\alpha = \varepsilon\pi^s$, kde ε je jednotka okruhu O_{ν_0} (a tedy i O) a s nezáporné celé číslo. Pro libovolné $i = 1, \ldots, m$ pak $\nu_i(\alpha) = e_i\nu_0(\alpha)$, odkud $e_i \neq 0$ (viz předchozí poznámku) a tedy ν_i je prodloužení exponentu ν_0. Je-li ν libovolné prodloužení exponentu ν_0 na K, pak $O_{\nu_0} \subseteq O_\nu$, z věty 1 tedy $O \subseteq O_\nu$, odkud $\nu(\varepsilon) = 0$ pro každou jednotku ε okruhu O a dle věty 3 nemohou být exponenty $\nu, \nu_1, \ldots, \nu_m$ po dvou různé.

Lemma 3. Nechť ν_0 je exponent tělesa k. Uvažme okruh O_{ν_0}, ideál I_{ν_0} a těleso zbytků $\Sigma_0 = O_{\nu_0}/I_{\nu_0}$ exponentu ν_0. Nechť K/k je konečné rozšíření těles a O celý uzávěr okruhu O_{ν_0} v K. Je-li $|\Sigma_0| \geq [K : k]$ (například je-li Σ_0 nekonečné těleso), pak je okruh O euklidovský (a tedy s jednoznačným rozkladem) a platí, že v okruhu O existuje jen konečně mnoho po dvou neasociovaných ireducibilních prvků.

Důkaz. Pro $\alpha \in K^\times$ položme

$$||\alpha|| = 2^{\nu_0(N_{K/k}(\alpha))}.$$

Zřejmě platí $||\alpha\beta|| = ||\alpha|| \cdot ||\beta||$ pro libovolné $\alpha, \beta \in K^\times$. Nechť $\alpha, \beta \in K$, $\beta \neq 0$. Dokážeme existenci $\gamma, \rho \in K$ splňujících $\alpha = \beta\gamma + \rho$, přičemž $\rho = 0$ nebo $||\rho|| < ||\beta||$. Předpokládejme tedy $\beta \nmid \alpha$ a označme $\gamma = \frac{\alpha}{\beta} \notin O$. Charakteristický polynom

$$f(t) = t^n + c_1 t^{n-1} + \cdots + c_n \in k[t]$$

prvku γ vzhledem ke K/k není z $O_{\nu_0}[t]$. Proto $r = -\min\{\nu_0(c_i);\, 1 \le i \le n\} > 0$. Zvolme ireducibilní prvek π okruhu O_{ν_0} (viz větu 2). Pak $\varphi(t) = \pi^r f(t) \in O_{\nu_0}[t]$ má za alespoň jeden z koeficientů jednotku okruhu O_{ν_0}. Označme $\bar{\varphi}(t) \in \Sigma_0[t]$ jeho obraz v kanonickém homomorfismu. Pak stupeň st $\bar{\varphi}(t) < n = [K : k]$, existuje tedy $a \in O_{\nu_0}$ tak, že pro $\bar{a} \in \Sigma_0$ platí $\bar{\varphi}(\bar{a}) \neq 0$. Charakteristický polynom prvku $\gamma - a$ vzhledem ke K/k je $f(t + a)$, tedy

$$N_{K/k}(\gamma - a) = (-1)^n f(a) = (-1)^n \pi^{-r} \varphi(a),$$

odkud $||\gamma - a|| = 2^{-r} < 1$, a tedy $||\alpha - a\beta|| < ||\beta||$.

Pro libovolné $\alpha \in O^\times$ platí $\alpha | N_{K/k}(\alpha)$. Je-li π libovolný ireducibilní prvek O, pak $N_{K/k}(\pi) = \varepsilon \cdot p^f$, kde ε je jednotka okruhu O_{ν_0}, $p \in k$, $\nu_0(p) = 1$ (tj. p je ireducibilní prvek O_{ν_0}), $f \ge 1$. Protože je π ireducibilní, platí $\pi | p$, takových je však jen konečně mnoho.

Věta 5. Nechť K/k je konečné rozšíření těles a ν_0 exponent tělesa k. Uvažme okruh $O_{\nu_0} \subseteq k$ exponentu ν_0 tělesa k a označme O celý uzávěr okruhu O_{ν_0} v K. Pak platí

1. existuje alespoň jedno prodloužení ν exponentu ν_0 na těleso K;
2. jsou-li $\nu_1, \ldots, \nu_m$ všechna prodloužení exponentu ν_0 na těleso K, pak

$$O = \bigcap_{i=1}^{m} O_{\nu_i}.$$

Užitím důsledku věty 3 (s případným přihlédnutím k důkazu Lemmatu 2) z věty 5 plyne

Důsledek. V označení věty 5 platí: O je okruh s teorií divizorů určenou všemi prodlouženími $\nu_1, \ldots, \nu_m$ exponentu ν_0 na těleso K. Jestliže π je ireducibilní prvek okruhu O_{ν_0} a $\pi_1, \ldots, \pi_m$ ireducibilní prvky O (označené tak, že $\nu_i(\pi_i) = 1$) a rozložíme-li v O

$$\pi = \varepsilon \prod_{i=1}^{m} \pi_i^{e_i},$$

kde ε je jednotka okruhu O a $e_1, \ldots, e_m$ jsou nezáporná celá čísla, pak pro každé $i = 1, \ldots, m$ je $e_i > 0$ index větvení exponentu ν_i vzhledem k ν_0.

Důkaz věty 5. Indukcí vzhledem k $n = [K : k]$. Předpokládejme, že $n > 1$ a že věta 5 je dokázána pro všechna rozšíření libovolného tělesa k stupně menšího než n. Má-li těleso zbytků Σ_0 exponentu ν_0 alespoň n prvků, plyne věta z lemmat 3 a 2. Předpokládejme tedy, že $q = |\Sigma_0| < n$. Nad konečnými tělesy existují ireducibilní polynomy libovolného stupně, můžeme proto zvolit nějaký normovaný ireducibilní polynom $\bar{\varphi}(t) \in \Sigma_0[t]$ stupně $n - 1$ a k němu nějaký normovaný polynom $\varphi(t) \in O_{\nu_0}[t]$ stupně $n - 1$ tak, aby $\bar{\varphi}(t)$ byl jeho obrazem v kanonickém homomorfimsmu. Pak $\varphi(t)$ je ireducibilní nad O_{ν_0}. Uvažme nějaké rozšíření $K' = K(\theta)$ tělesa K, kde θ je kořen $\varphi(t)$. Pak $[K' : K] \le n - 1$ a pro $k' = k(\theta)$ platí $[k' : k] = n - 1$. Zvolme nějaké prodloužení ν_0' exponentu ν_0 na těleso k' (užíváme indukční předpoklad) a označme Σ_0' těleso zbytků exponentu ν_0'. Díky kanonickému vnoření $\Sigma_0 \to \Sigma_0'$ lze považovat Σ_0 za podtěleso tělesa Σ_0'. Pak $\Sigma_0(\bar{\theta}) \subseteq \Sigma_0'$ a $|\Sigma_0(\bar{\theta})| = q^{n-1} \ge n$.

Na druhou stranu $[K' : k'] \leq n$. Pro rozšíření K'/k' a exponent ν_0' tedy věta platí. Existuje tedy prodloužení ν' exponentu ν_0' na K'. Uvážíme-li exponent ν indukovaný exponentem ν' na K, dokázali jsme část 1.

Pro důkaz části 2 ukažme nejprve, že ν_0' je jediné prodloužení exponentu ν_0 na k'. Předpokládejme, že ν_0'' je jiné jeho prodloužení. Podle věty 3 existuje $\gamma \in k'$ tak, že $\nu_0'(\gamma) = 0$ a $\nu_0''(\gamma) > 0$. Pak lze jednoznačně psát $\gamma = \pi^r \sum_{i=0}^{n-2} c_i \theta^i$, kde π je ireducibilní prvek O_{ν_0}, $r \in \mathbb{Z}$, $c_i \in O_{\nu_0}$ pro všechna $i = \{0, \ldots, n-2\}$ a pro alespoň jedno $j = \{0, \ldots, n-2\}$ platí $\nu(c_j) = 0$. Označme $\alpha = \sum_{i=0}^{n-2} c_i \theta^i$. Pak $\bar{c}_j$ a proto i $\bar{\alpha} = \sum_{i=0}^{n-2} \bar{c}_i \bar{\theta}^i$ jsou nenulové prvky Σ_0'. Proto $\nu_0'(\alpha) = 0$. Analogicky $\nu_0''(\alpha) = 0$. Z $\nu_0'(\gamma) = 0$ plyne $r = 0$, odkud $\nu_0''(\gamma) = 0$, spor.

Z indukčního předpokladu pro k'/k je $O_{\nu_0'}$ celý uzávěr okruhu O_{ν_0} v k'. Označme O' celý uzávěr okruhu O_{ν_0} v K'. Protože celý uzávěr je celouzavřený (dokázali jsme v kapitole 3), je O' také celým uzávěrem okruhu $O_{\nu_0'}$ v K'. Nechť $\nu_1', \ldots, \nu_r'$ jsou všechna prodloužení exponentu ν_0' na K'. Protože pro rozšíření K'/k' a exponent ν_0' věta platí, je

$$O' = \bigcap_{i=1}^{r} O_{\nu_i'}.$$

Ovšem $\nu_1', \ldots, \nu_r'$ jsou také všechna prodloužení exponentu ν_0 na K'. Označíme-li $\nu_1, \ldots, \nu_m$ všechny po dvou různé exponenty na K indukované exponenty $\nu_1', \ldots, \nu_r'$, pak

$$O = O' \cap K = \bigcap_{i=1}^{r} (O_{\nu_i'} \cap K) = \bigcap_{i=1}^{m} O_{\nu_i}.$$

Kdyby existovalo nějaké prodloužení ν exponentu ν_0 na těleso K odlišné od exponentů $\nu_1, \ldots, \nu_m$, podle věty 3 by existovalo $\gamma \in K$ tak, že $\nu_1(\gamma) \geq 0, \ldots, \nu_m(\gamma) \geq 0, \nu(\gamma) < 0$, spor s inkluzí $O \subseteq O_\nu$, která plyne z celouzavřenosti O_ν. Věta 5 je dokázána.

Cvičení 24. Nechť K/k je Galoisovo rozšíření, $G = \mathrm{Gal}(K/k)$. Nechť ν_0 je exponent tělesa k a ν prodloužení exponentu ν_0 na těleso K. Pro libovolné $\sigma \in G$ a libovolné $\alpha \in K^\times$ položme $\nu^\sigma(\alpha) = \nu(\sigma(\alpha))$, $\nu^\sigma(0) = \infty$. Dokažte, že

(a) pro každé $\sigma \in G$ je ν^σ prodloužení exponentu ν_0 na těleso K;

(b) libovolné prodloužení exponentu ν_0 na těleso K je tvaru ν^σ pro nějaké $\sigma \in G$;

(c) všechna prodloužení exponentu ν_0 na těleso K mají týž index větvení;

(d) $D_\nu = \{\sigma \in G;\ \nu^\sigma = \nu\}$ je podgrupa grupy G (nazývá se dekompoziční grupa příslušná exponentu ν);

(e) D_ν odpovídá v Galoisově korespondenci nejmenšímu mezitělesu L rozšíření K/k takovému, že exponent tělesa L indukovaný exponentem ν lze jediným způsobem prodloužit na těleso K;

(f) $[L : k]$ je rovno počtu všech prodloužení exponentu ν_0 na těleso K;

(g) D_ν je normální podgrupa grupy G právě tehdy, když existuje $[L : k]$ různých prodloužení exponentu ν_0 na těleso L.

8. Teorie divizorů konečného rozšíření těles

(podrobnější důkazy viz Borevič-Šafarevič, kapitola 3, §5)

Věta 1. Nechť R_0 je obor integrity s podílovým tělesem k takový, že existuje teorie divizorů $R_0^\times \to D_0$; označme M_0 množinu všech exponentů odpovídajících prvodivizorům této teorie divizorů. Nechť K/k je konečné rozšíření. Pak množina M všech prodloužení všech exponentů z M_0 definuje teorii divizorů na celém uzávěru R okruhu R_0 v K.

Důkaz. Ověříme tři podmínky věty 4 kapitoly 6.

(2) Pro libovolné $\nu \in M$ platí $R_0 \subseteq O_\nu$ a podle věty 1 kapitoly 7 je $R \subseteq O_\nu$. Nechť $\alpha \in K$ splňuje $\nu(\alpha) \geq 0$ pro každé $\nu \in M$. Nechť $t^n + a_1 t^{n-1} + \cdots + a_n$ je minimální polynom α vzhledem ke k. Zvolme $\nu_0 \in M_0$ libovolně a označme $\nu_1, \ldots, \nu_m$ všechna prodloužení exponentu ν_0 na K. Protože $\alpha \in \cap_{i=1}^m O_{\nu_i}$, podle věty 5(2) kapitoly 7 je α z celého uzávěru okruhu O_{ν_0}, tedy $a_1, \ldots, a_n \in O_{\nu_0}$. Odtud $a_1, \ldots, a_n \in \cap_{\nu_0 \in M_0} O_{\nu_0} = R_0$. Proto $\alpha \in R$.

(1) Existuje jen konečně mnoho exponentů $\nu \in M$ s vlastností $\nu(a_n) \neq 0$. Jestliže $\nu(a_n) = 0$, pak $\nu(\alpha^{-1}) = \nu(a_n^{-1}(\alpha^{r-1} + \cdots + a_{r-1})) \geq 0$, tedy $\nu(\alpha) = 0$.

(3) Nechť $\nu_1, \ldots, \nu_m \in M$ a nechť $k_1, \ldots, k_m$ jsou nezáporná celá čísla. Bez újmy na obecnosti lze předpokládat, že pro každé $\nu_0 \in M_0$ jsou mezi vybranými exponenty buď žádné nebo všechna prodloužení ν_0 na K. Podle věty 3 kapitoly 7 existuje $\alpha \in K$ tak, že $\nu_1(\alpha) = k_1, \ldots, \nu_m(\alpha) = k_m$. Je-li $\alpha \in R$, jsme hotovi. Pokud ne, platí $\nu(\alpha) < 0$ pro konečně mnoho $\nu \in M$. Označme $r = -\min\{\nu(\alpha);\ \nu \in M\} > 0$. Podle věty 4 kapitoly 6 existuje $a \in R_0$ tak, že $\nu_0(a) = 0$ pro každý exponent ν_0 indukovaný některým z exponentů $\nu_1, \ldots, \nu_m$ a současně $\nu_0(a) = r$ pro každý exponent ν_0 indukovaný některým exponentem $\nu \in M$ s vlastností $\nu(\alpha) < 0$. Pak $a\alpha \in R$ má požadované vlastnosti.

Věta 2. Nechť K je těleso algebraických čísel, R okruh celých čísel tělesa K. Pak R má teorii divizorů, která je určena množinou všech exponentů tělesa K.

Důkaz. Plyne z cvičení 22 a předchozí věty.

Poznámka. Ve zbytku kapitoly budeme předpokládat, že R_0 je obor integrity s podílovým tělesem k takový, že existuje teorie divizorů $R_0^\times \to D_0$, že K/k je konečné rozšíření těles, že R je celý uzávěr okruhu R_0 v K a že $R^\times \to D$ je teorie divizorů. Protože $R_0 \subseteq R$, odpovídají prvkům $\alpha \in R_0^\times$ divizory v D_0 i v D. Budeme je rozlišovat indexy: $(\alpha)_k \in D_0$, $(\alpha)_K \in D$.

Věta 3. Existuje vnoření $D_0 \to D$ takové, že platí $(\alpha)_k \mapsto (\alpha)_K$ pro každé $\alpha \in R_0^\times$.

Důkaz. Zvolme libovolně prvodivizor $p \in D_0$ a uvažme příslušný exponent ν_0 na k. Nechť $\nu_1, \ldots, \nu_m$ jsou všechna prodloužení exponentu ν_0 na K a $e_1, \ldots, e_m$ příslušné indexy větvení. Označme $P_1, \ldots, P_m$ prvodivizory v D odpovídající exponentům $\nu_1, \ldots, \nu_m$. Přiřaďme $p \mapsto P_1^{e_1} \ldots P_m^{e_m}$. Toto přiřazení určí vnoření $D_0 \to D$, o kterém se snadno ukáže, že platí $(\alpha)_k \mapsto (\alpha)_K$ pro každé $\alpha \in R_0^\times$.

Věta 4. Existuje homomorfismus $N : D \to D_0$ takový, že platí $N((\alpha)_K) = (N_{K/k}(\alpha))_k$ pro každé $\alpha \in R^\times$.

Důkaz. Zvolme libovolně prvodivizor $p \in D_0$ a uvažme příslušný exponent ν_0 na k. Nechť $\nu_1, \ldots, \nu_m$ jsou všechna prodloužení exponentu ν_0 na K. Stejně jako v důsledku věty 5 kapitoly 7 označme $\pi_1, \ldots, \pi_m$ ireducibilní prvky okruhu $O =$

$\cap_{i=1}^m O_{\nu_i}$ (indexované tak, že $\nu_i(\pi_i) = 1$) a $P_1, \dots, P_m$ prvodivizory v D odpovídající exponentům $\nu_1, \dots, \nu_m$. Pro libovolné $i = 1, \dots, m$ je $N_{K/k}(\pi_i) \in O_{\nu_0}$ a tedy $d_i = \nu_0(N_{K/k}(\pi_i)) \geq 0$. Snadno se ukáže, že d_i nezávisí na konkrétní volbě π_i. Přiřaďme $P_i \mapsto p^{d_i}$. Toto přiřazení určí homomorfismus $D \to D_0$, pro který se snadno ověří, že platí $N((\alpha)_K) = (N_{K/k}(\alpha))_k$ pro každé $\alpha \in R^\times$.

Poznámka. V označení předchozího důkazu: Protože každý prvek dělí svoji normu, platí dokonce $d_i > 0$. Jestliže v O rozložíme ireducibilní prvek π okruhu O_{ν_0}, dostaneme podle důsledku věty 5 kapitoly 7

$$\pi = \varepsilon \prod_{i=1}^m \pi_i^{e_i},$$

kde ε je jednotka okruhu O a pro každé $i = 1, \dots, m$ je $e_i > 0$ index větvení exponentu ν_i vzhledem k ν_0. Nechť $n = [K : k]$. Přechodem k normě dostaneme

$$\pi^n = N_{K/k}(\pi) = N_{K/k}(\varepsilon) \prod_{i=1}^m N_{K/k}(\pi_i)^{e_i},$$

odkud aplikací exponentu ν_0 dostaneme identitu

$$[K : k] = \sum_{i=1}^m d_i e_i.$$

Definice. Pro libovolné $a \in D$ nazýváme $N(a)$ normou divizoru a vzhledem k rozšíření K/k. Chceme-li v případě potřeby vyznačit, o jaké rozšíření jde, píšeme $N_{K/k}(a)$.

Cvičení 25. Dokažte, že zobrazení konstruovaná v důkazech vět 3 a 4 jsou jediné homomorfismy splňující podmínky vět.

Poznámka. Do konce kapitoly zvolme libovolně, ale pevně prvodivizor $p \in D_0$ a uvažme příslušný exponent ν_0 na k. Nechť $\nu_1, \dots, \nu_m$ jsou všechna prodloužení exponentu ν_0 na K. Stejně jako v důsledku věty 5 kapitoly 7 označme π ireducibilní prvek okruhu O_{ν_0} a $\pi_1, \dots, \pi_m$ ireducibilní prvky okruhu $O = \cap_{i=1}^m O_{\nu_i}$ (indexované tak, že $\nu_i(\pi_i) = 1$) a $P_1, \dots, P_m$ prvodivizory v D odpovídající exponentům $\nu_1, \dots, \nu_m$.

Nechť $i \in \{1, \dots, m\}$ je libovolné. Protože pro libovolné $\alpha \in O_{\nu_0}$ platí $\nu_0(\alpha) > 0$ právě tehdy, když $\nu_i(\alpha) > 0$, existuje vnoření tělesa zbytků Σ_0 exponentu ν_0 do tělesa zbytků Σ_i exponentu ν_i. Pro libovolné $\alpha \in O_{\nu_i}$ budeme jeho obraz v Σ_i značit $\bar{\alpha}$. Je jasné, že pro každé $\alpha_1, \dots, \alpha_r \in O_{\nu_i}$ platí: jestliže $\alpha_1, \dots, \alpha_r$ jsou k-lineárně závislé, pak $\bar{\alpha}_1, \dots, \bar{\alpha}_r \in \Sigma_i$ jsou Σ_0-lineárně závislé. Proto Σ_i/Σ_0 je konečné rozšíření těles a platí $[\Sigma_i : \Sigma_0] \leq [K : k]$. V dalším textu budeme značit $f_i = [\Sigma_i : \Sigma_0]$.

Definice. Stupeň f_i rozšíření Σ_i/Σ_0 se nazývá stupeň inercie exponentu ν_i vzhledem k ν_0.

Poznámka. O stupni inercie (resp. indexu větvení) exponentu ν_i vzhledem k ν_0 někdy též hovoříme jako o stupni inercie (resp. indexu větvení) prvodivizoru P_i vzhledem k p.

Definice. Baze $\omega_1, \dots, \omega_n$ rozšíření K/k se nazývá fundamentální baze okruhu O vzhledem k O_{ν_0}, jestliže $\omega_1, \dots, \omega_n \in O$ a pro každé $\alpha \in O$ existuje vyjádření $\alpha = \sum_{i=1}^{n} a_i \alpha_i$ s koeficienty $a_i \in O_{\nu_0}$.

Poznámka pro znalé teorie R-modulů: fundamentální baze okruhu O vzhledem k O_{ν_0} existuje, právě když je O volný O_{ν_0}-modul.

Věta 5. Existuje-li fundamentální baze okruhu O vzhledem k O_{ν_0}, pak pro každé $i = 1, \dots, n$ platí $f_i = d_i$, tj. $\nu_0(N_{K/k}(\pi_i)) = [\Sigma_i : \Sigma_0]$.

Důkaz. Nechť $i \in \{1, \dots, n\}$ je libovolné. Z věty 4 kapitoly 7 plyne, že pro každé $\xi \in O_{\nu_i}$ existuje $\alpha \in K$ s vlastností $\nu_i(\alpha - \xi) \geq 1$ a $\nu_j(\alpha) \geq 0$ pro $j \neq i$. Pak je $\alpha \in O$ a platí $\bar{\alpha} = \bar{\xi}$. Odtud plyne, že je-li $\omega_1, \dots, \omega_n \in O$ fundamentální baze okruhu O vzhledem k O_{ν_0}, pak je $\bar{\omega}_1, \dots, \bar{\omega}_n \in \Sigma_i$ systém generátorů vektorového prostoru Σ_i nad Σ_0. Protože $f_i = [\Sigma_i : \Sigma_0]$, lze případným přeindexováním dosáhnout toho, že $\bar{\omega}_1, \dots, \bar{\omega}_{f_i}$ je baze vektorového prostoru Σ_i nad Σ_0 (tj. baze rozšíření Σ_i/Σ_0). Pro $j > f_i$ platí

$$\bar{\omega}_j = \sum_{s=1}^{f_i} \bar{\beta}_{js} \bar{\omega}_s$$

pro vhodné $\beta_{js} \in O_{\nu_0}$. Položme

$$\vartheta_j = \begin{cases} \omega_j & \text{je-li } 1 \leq j \leq f_i, \\ \omega_j - \sum_{s=1}^{f_i} \beta_{js} \omega_s & \text{je-li } f_i < j \leq n. \end{cases}$$

Je zřejmé, že $\vartheta_1, \dots, \vartheta_n \in O$ je fundamentální baze okruhu O vzhledem k O_{ν_0}. Ideál $\pi_i O$ všech prvků okruhu O dělitelných prvkem π_i se tedy skládá ze všech O_{ν_0}-lineárních kombinací prvků $\pi_i \vartheta_1, \dots, \pi_i \vartheta_n$. Na druhou stranu pro libovolné $a_1, \dots, a_n \in O_{\nu_0}$ platí $\sum_{j=1}^{n} a_j \vartheta_j \in \pi_i O$, právě když $\nu_i(a_1) > 0, \dots, \nu_i(a_{f_i}) > 0$, tj. právě když $\nu_0(a_1) > 0, \dots, \nu_0(a_{f_i}) > 0$, což znamená, že $a_1, \dots, a_n$ jsou všechny dělitelné π. Ideál $\pi_i O$ se tedy skládá ze všech O_{ν_0}-lineárních kombinací prvků $\pi\vartheta_1, \dots, \pi\vartheta_{f_i}, \vartheta_{f_i+1}, \dots, \vartheta_n$. Determinant matice přechodu mezi výše uvedenými O_{ν_0}-bazemi ideálu $\pi_i O$ je proto jednotka okruhu O_{ν_0}. Podle definice normy je $N_{K/k}(\pi_i) = \det(a_{st})$, kde $a_{st} \in k$ splňují

$$\pi_i \vartheta_s = \sum_{t=1}^{n} a_{st} \vartheta_t.$$

Zmíněná matice přechodu je matice (b_{st}), kde $b_{st} = a_{st}\pi^{-1}$, je-li $t \leq f_i$, a $b_{st} = a_{st}$, je-li $t > f_i$. Proto $N_{K/k}(\pi_i) = \det(a_{st}) = \pi^{f_i} \det(b_{st})$, odkud $\nu_0(N_{K/k}(\pi_i)) = f_i$, což jsme měli dokázat.

Věta 6. Je-li K/k separabilní, pak existuje fundamentální baze okruhu O vzhledem k O_{ν_0}.

Důkaz. Zvolme v K bazi $\alpha_1, \dots, \alpha_n \in O$. Díky separabilitě existuje duální baze $\alpha_1^*, \dots, \alpha_n^* \in K$, tj. taková baze, že platí pro každé $i, j \in \{1, \dots, n\}$

$$\mathrm{Sp}_{K/k}(\alpha_i \alpha_j^*) = \begin{cases} 1 & \text{je-li } i = j, \\ 0 & \text{je-li } i \neq j. \end{cases}$$

Je-li $\alpha \in O$ a platí-li $\alpha = \sum_{i=1}^{n} c_i \alpha_i^*$, kde $c_1, \ldots, c_n \in k$, platí $c_i = \mathrm{Sp}_{K/k}(\alpha\alpha_i) \in O_{\nu_0}$, neboť $\alpha\alpha_i \in O$. Pro každé $s = 1, \ldots, n$ označme ω_s některý prvek, který má mezi všemi prvky tvaru $\sum_{i=s}^{n} c_i \alpha_i^* \in O$, kde $c_i \in O_{\nu_0}$, minimální hodnotu $\nu_0(c_s)$. Snadno se ukáže, že $\omega_1, \ldots, \omega_n$ je fundamentální baze okruhu O vzhledem k O_{ν_0}.

Věta 7. Nechť K/k je separabilní, pak platí

$$[K : k] = \sum_{i=1}^{m} f_i e_i.$$

Důkaz. Plyne z vět 5 a 6 a poznámky za větou 4.

Lemma. Nechť K/k je separabilní. Existuje-li $\vartheta \in O$ tak, že $K = k(\vartheta)$ a že diskriminant $D(\varphi_\vartheta)$ minimálního polynomu φ_ϑ nad k je jednotkou okruhu O_{ν_0}, pak $1, \vartheta, \ldots, \vartheta^{n-1}$ je fundamentální baze okruhu O vzhledem k O_{ν_0}.

Důkaz. Věta 6 zaručuje existenci fundamentální baze $\omega_1, \ldots, \omega_n$ okruhu O vzhledem k O_{ν_0}. Označme C matici přechodu od baze $\omega_1, \ldots, \omega_n$ k bazi $1, \vartheta, \ldots, \vartheta^{n-1}$, tj. $C = (c_{ij})$, kde $c_{ij} \in O_{\nu_0}$ splňují $\vartheta^{i-1} = \sum_{j=1}^{n} c_{ij}\omega_j$. Podle výpočtů z první kapitoly pro diskriminanty jednotlivých bazí platí

$$D(\varphi_\vartheta) = D(1, \vartheta, \ldots, \vartheta^{n-1}) = (\det C)^2 D(\omega_1, \ldots, \omega_n).$$

Protože činitelé vpravo jsou z O_{ν_0} a na levé straně je jednotka tohoto okruhu, je i $\det C$ jednotkou tohoto okruhu a proto je $1, \vartheta, \ldots, \vartheta^{n-1}$ fundamentální baze okruhu O vzhledem k O_{ν_0}.

Věta 8. Nechť K/k je separabilní a nechť pro $\vartheta \in O$ platí, že $K = k(\vartheta)$ a že diskriminant $D(\varphi_\vartheta)$ minimálního polynomu φ_ϑ nad k je jednotkou okruhu O_{ν_0}. Rozložíme-li polynom $\bar{\varphi}_\vartheta \in \Sigma_0[t]$ na součin ireducibilních polynomů z $\Sigma_0[t]$, pak tito ireducibilní činitelé jsou po dvou různí a odpovídají jednotlivým prodloužením $\nu_1, \ldots, \nu_m$ exponentu ν_0 na K. Podrobněji: při vhodném indexování je zmíněný rozklad tvaru:

$$\bar{\varphi}_\vartheta(t) = \bar{g}_1(t) \cdot \ldots \cdot \bar{g}_m(t)$$

kde $g_1(t), \ldots, g_m(t) \in O_{\nu_0}[t]$ jsou vhodné normované polynomy, přičemž jejich obrazy v kanonickém homomorfismu $\bar{g}_1(t), \ldots, \bar{g}_m(t) \in \Sigma_0[t]$ jsou různé ireducibilní polynomy. Navíc pro každé $i = 1, \ldots, m$ platí:

1. stupeň inercie exponentu ν_i vzhledem k ν_0 je roven stupni polynomu $g_i(t)$;
2. index větvení exponentu ν_i vzhledem k ν_0 je roven 1;
3. ireducibilní prvek π_i okruhu O odpovídající prodloužení ν_i je největší společný dělitel (v O) prvků π a $g_i(\vartheta)$.

Důkaz. Platí $D(\bar{\varphi}_\vartheta) = \overline{D(\varphi_\vartheta)} \neq 0$ a tedy ireducibilní faktory dělící $\bar{\varphi}_\vartheta$ jsou po dvou různé.

Pro libovolný polynom $h(t) \in O_{\nu_0}[t]$ dokažme, že jsou-li $\bar{h}(t)$ a $\bar{g}_i(t)$ nesoudělné v $\Sigma_0[t]$, pak jsou také $h(\vartheta)$ a $g_i(\vartheta)$ nesoudělné v O. Skutečně, z nesoudělnosti $\bar{h}(t)$ a $\bar{g}_i(t)$ v $\Sigma_0[t]$ plyne existence $u(t), v(t), w(t) \in O_{\nu_0}[t]$ splňujících

$$h(t)u(t) + g_i(t)v(t) = 1 + \pi w(t).$$

Libovolný ireducibilní prvek v O je dělitelem π (viz důsledek věty 5 v kapitole 7), pokud by tedy dělil současně $h(\vartheta)$ a $g_i(\vartheta)$, musel by dělit i 1, spor.

Dokázali jsme, že $g_1(\vartheta), \dots, g_m(\vartheta)$ jsou po dvou nesoudělné prvky O.

Připusťme, že $g_i(\vartheta)$ je jednotka okruhu O, tj. že existuje $\xi \in O$ tak, že $g_i(\vartheta)\xi = 1$. Z lemmatu plyne existence polynomu $h(t) \in O_{\nu_0}[t]$ takového, že $\xi = h(\vartheta)$. Z $g_i(\vartheta)h(\vartheta) = 1$ pak plyne existence polynomu $q(t) \in O_{\nu_0}$ splňujícího $g_i(t)h(t) = 1 + \varphi_\vartheta(t)q(t)$. To však po aplikaci kanonickém homomorfismu dává $\bar{g}_i(t)\bar{h}(t) = 1 + \bar{g}_1(t) \cdot \ldots \cdot \bar{g}_m(t)\bar{q}(t)$, spor.

Pro každé $i \in \{1, \dots, m\}$ vybereme v O ireducibilní prvek π_i dělící $g_i(\vartheta)$ (zde na chvíli porušíme naši úmluvu, že po dvou neasociovaných ireducibilních prvků okruhu O je právě m a že $\pi_1, \dots \pi_m$ jsou už zvolené; při konstrukci $\pi_1, \dots \pi_m$ v tomto důkaze ještě zatím nevíme, že ireducibilních prvků v O není více). Z nesoudělnosti $g_1(\vartheta), \dots, g_m(\vartheta)$ plyne, že $\pi_1, \dots, \pi_m$ jsou po dvou neasociované. Pro každé $i \in \{1, \dots, m\}$ označme ν_i prodloužení exponentu ν_0 na K odpovídající π_i, f_i stupeň inercie a e_i index větvení exponentu ν_i vzhledem k ν_0. Dále s_i značí stupeň polynomu $g_i(t)$.

V tělese Σ_i exponentu ν_i jsou prvky $\bar{1}, \bar{\vartheta}, \dots, \bar{\vartheta}^{s_i-1}$ Σ_0-lineárně nezávislé, a tedy $s_i \le f_i$. Skutečně, pokud by pro polynom $h(t) \in O_{\nu_0}$ stupně menšího než s_i platilo $\bar{h}(\bar{\vartheta}) = 0$, pak by bylo $h(\vartheta) \in O$ dělitelné π_i, proto $h(\vartheta)$ a $g_i(\vartheta)$ by nebyly nesoudělné. Pak ale $\bar{g}_i(t)$ je dělitelem polynomu $\bar{h}(t)$ v $\Sigma_0[t]$ (viz začátek důkazu). Pak má ale $\bar{h}(t)$ nulové koeficienty.

Protože $\bar{\varphi}_\vartheta(t)$ je normovaný polynom stupně $[K : k]$ a rozkládá se na součin normovaných polynomů stupnů $s_1, \dots, s_m$, platí

$$[K : k] = \sum_{i=1}^{m} s_i \le \sum_{i=1}^{m} f_i \le \sum_{i=1}^{m} e_i f_i.$$

Z věty 7 plyne, že $\pi_1, \dots, \pi_m$ jsou všechny ireducibilní prvky okruhu O a že všechny výše uvedené nerovnosti jsou rovnostmi. Důkaz věty je ukončen.

Definice. Řekneme, že exponent ν_0 tělesa k je nerozvětvený v rozšíření K/k, mají-li všechna prodloužení exponentu ν_0 na K index větvení roven jedné. V opačném případě řekneme, že exponent ν_0 je v rozšíření K/k rozvětvený. Řekneme, že exponent ν_0 tělesa k je totálně rozvětvený v rozšíření K/k, existuje-li prodloužení exponentu ν_0 na K s indexem větvení $[K : k]$ (podle věty 7 je v případě separabilního rozšíření pak takové prodloužení jediné a má stupeň inercie roven jedné, totéž však lze dokázat i pro neseparabilní rozšíření).

Řekneme, že prvodivizor p okruhu R_0 je nerozvětvený (resp. rozvětvený, totálně rozvětvený) v rozšíření K/k, jestliže jemu odpovídající exponent je v rozšíření K/k nerozvětvený (resp. rozvětvený, totálně rozvětvený).

Důsledek. Je-li K/k separabilní rozšíření, pak existuje jen konečně mnoho rozvětvených prvodivizorů okruhu R_0.

Důkaz. Podle věty 10 kapitoly 1 existuje $\alpha \in K$ tak, že $K = k(\alpha)$. Případným vynásobením prvkem z R_0 lze dosáhnout toho, že $\alpha \in R$. Pak diskriminant minimálního polynomu φ_α je prvek z R_0, a proto je dělitelný jen konečně mnoha prvodivizory. Všechny ostatní prvodivizory jsou podle věty 8 nerozvětvené.

Cvičení 26. Užíváme označení z cvičení 24. Označme dále Σ_0 těleso zbytků exponentu ν_0 a Σ těleso zbytků exponentu ν. Předpokládejme navíc, že rozšíření Σ/Σ_0 je separabilní. Dokažte, že

(a) rozšíření Σ/Σ_0 je Galoisovo;
(b) předpisem $\bar\sigma(\bar\alpha) = \overline{\sigma(\alpha)}$ (kde $\alpha \in K$, $\nu(\alpha) \geq 0$, $\sigma \in D_\nu$) je korektně definováno zobrazení $\bar\sigma : \Sigma \to \Sigma$;
(c) pro libovolné $\sigma \in D_\nu$ je $\bar\sigma \in \mathrm{Gal}(\Sigma/\Sigma_0)$;
(d) předpis $\sigma \mapsto \bar\sigma$ je surjektivní homomorfismus grup $D_\nu \to \mathrm{Gal}(\Sigma/\Sigma_0)$;
(e) jádro tohoto homomorfismu I_ν (nazývá se inerční grupa příslušná exponentu ν) odpovídá v Galoisově korespondenci nejmenšímu mezitělesu L rozšíření K/k takovému, že exponent tělesa L indukovaný exponentem ν je totálně rozvětvený v rozšíření K/L;
(f) $[K : L]$ je rovno indexu větvení exponentu ν vzhledem k ν_0;
(g) všechna prodloužení exponentu ν_0 na K mají týž stupeň inercie.

9. Dedekindovy okruhy

(podrobnější důkazy viz Borevič-Šafarevič, kapitola 3, §6)

Definice. Nechť R je obor integrity s teorií divizorů $R^\times \to D$, $a \in D$ divizor. Okruhem zbytků R/a rozumíme faktorokruh $R/\bar a$, kde $\bar a$ je ideál prvků z R dělitelných a. Rovnosti v okruhu zbytků budeme často zapisovat pomocí kongruencí: pro $\alpha, \beta \in R$ znamená $\alpha \equiv \beta \pmod a$ totéž, co $\alpha + \bar a = \beta + \bar a$, totiž $a|\alpha - \beta$.

Věta 1. Nechť R je okruh celých čísel nějakého tělesa algebraických čísel K. Pro libovolný divizor a okruhu R je okruh zbytků R/a konečný.

Důkaz. Existuje $\alpha \in R^\times$ dělitelné a. Toto α dělí nějaké přirozené číslo n (například $|N_{K/\mathbb{Q}}(\alpha)|$). Pak $nR \subseteq \bar a$ a $|R/nR| = n^{[K:\mathbb{Q}]}$.

Věta 2. Nechť R je okruh celých čísel nějakého tělesa algebraických čísel K. Libovolný prvodivizor p okruhu R je dělitelem jediného prvočísla q. Okruh zbytků R/p je pak konečné těleso charakteristiky q.

Důkaz. Prvodivizoru p odpovídá exponent tělesa K, který je indukován nějakým exponentem tělesa $\mathbb{Q}$. Ten podle cvičení 22 odpovídá nějakému prvočíslu q. Okruh zbytků R/p je netriviální a nemá dělitele nuly, proto z věty 1 plyne, že jde o těleso. Přitom $q \in \bar p$.

Definice. Obor integrity R se nazývá Dedekindův, jestliže pro něj existuje teorie divizorů $R^\times \to D$ taková, že pro každý prvodivizor p je okruh zbytků R/p těleso.

Příklady. Dle věty 2 jsou okuhy celých čísel v tělesech algebraických čísel Dedekindovy. Dedekindův okruh je i okruh O_ν pro libovolný exponent ν na libovolném tělese K. Na začátku důkazu věty 5 minulé kapitoly jsme ukázali, že Dedekindův okruh je i celý uzávěr okruhu O_ν v libovolném konečném rozšíření tělesa K. Stejně se dokáže, že libovolný okruh s teorií divizorů, ve které je jen konečně mnoho prvodivizorů, je Dedekindův. Z Bezoutovy identity plyne, že okruh polynomů jedné proměnné nad libovolným tělesem je Dedekindův.

Dedekindovy okruhy naopak nejsou například okruh $\mathbb{Z}[x]$ nebo okruh $K[x, y]$ pro libovolné těleso K, přestože to jsou okruhy s jednoznačným rozkladem.

Cvičení 27. Nechť R je Dedekindův okruh a K jeho podílové těleso. Dokažte, že celý uzávěr okruhu R v libovolném konečném rozšíření tělesa K je opět Dedekindův okruh.

Poznámky. Dedekindův okruh bývá v literatuře většinou definován jiným ekvivalentním způsobem. Obvyklá definice je následující: obor integrity R se nazývá Dedekindův okruh, jestliže

1. každý vlastní prvoideál okruhu R je maximální;
2. okruh R je celouzavřený (ve svém podílovém tělese);
3. okruh R je Noetherovský, tj. libovolná rostoucí posloupnost ideálů okruhu R je konečná (jinými slovy, jsou-li $I_1 \subseteq I_2 \subseteq \dots$ ideály okruhu R, pak existuje přirozené číslo n tak, že $\bigcup_{t=1}^{\infty} I_t = I_n$).

V knize Kapitoly z obecné algebry od A. G. Kuroše (vyšlo v nakladatelství Academia v Praze roku 1977) je Dedekindův okruh definován jako obor integrity, v němž každý vlastní ideál lze vytvořit jako součin konečného počtu prvoideálů (součin ideálů A a B je ideál generovaný množinou součinů $\{\alpha\beta;\ \alpha \in A,\ \beta \in B\}$).

Lemma 1. Nechť R je Dedekindův okruh, p jeho prvodivizor, $\alpha \in R$ nedělitelné p a m přirozené číslo. Pak je kongruence $\alpha x \equiv 1 \pmod{p^m}$ řešitelná v R.

Důkaz provedeme indukcí, pro $m = 1$ plyne přímo z definice. Nechť lemma platí pro m, zvolme $\xi \in R$ tak, že $\alpha\xi \equiv 1 \pmod{p^m}$. Dále zvolme $\omega \in R$ tak, že $\nu_p(\omega) = m$ (zde i dále ν_p značí exponent příslušný prvodivizoru p). Pak divizor $(\omega) = p^m a$, kde divizor a není dělitelný p. Zvolme $\gamma \in R$ tak, že $\nu_p(\gamma) = 0$ a $a|\gamma$ (existence je zaručena větou 4 kapitoly 6). Pak $\omega|\gamma(\alpha\xi - 1)$, tj. existuje $\mu \in R$ tak, že $\omega\mu = \gamma(\alpha\xi - 1)$. Je vidět, že řešením konguence $\alpha x \equiv 1 \pmod{p^{m+1}}$ bude $x = \xi + \omega\lambda$, jestliže $\lambda \in R$ zvolíme tak, aby splňovalo $\alpha\gamma\lambda \equiv -\mu \pmod{p}$, což lze, neboť R/p je těleso.

Věta 3. Nechť R je Dedekindův okruh, $p_1, \dots p_m$ jeho různé prvodivizory, $\alpha_1, \dots,$ $\alpha_m \in R$ a $t_1, \dots, t_m$ přirozená čísla. Pak je systém kongruencí

$$x \equiv \alpha_i \pmod{p_i^{t_i}} \qquad i \in \{1, \dots, m\}$$

řešitelný v R.

Důkaz. Pro libovolné $i \in \{1, \dots, m\}$ zvolme $\beta_i \in R$ tak, aby $\nu_{p_j}(\beta_i) = t_j$ pro $j \in \{1, \dots, m\} \setminus \{i\}$ a $\nu_{p_i}(\beta_i) = 0$. Podle lemmatu 1 existuje $\xi_i \in R$ tak, že $\beta_i\xi_i \equiv \alpha_i \pmod{p_i^{t_i}}$. Řešením daného systému je pak $\sum_{i=1}^{m} \beta_i\xi_i$.

Věta 4. Nechť R je Dedekindův okruh, a jeho divizor, $\alpha, \beta \in R$, $\alpha \neq 0$. Pak je kongruence $\alpha x \equiv \beta \pmod{a}$ řešitelná, právě když je β dělitelné největším společným dělitelem divizorů (α) a a.

Důkaz. Větu dokážeme nejprve za předpokladu, že divizory (α) a a jsou nesoudělné. Nechť $a = \prod_{i=1}^{m} p_i^{t_i} = p_j^{t_j} a_j$, kde $p_1, \dots p_m$ jsou různé prvodivizory. Podle lemmatu 1 existují $\xi_i' \in R$ tak, že $\alpha\xi_i' \equiv \beta \pmod{p_i^{t_i}}$. Podle věty 3 existují $\xi_i \in R$ tak, že $\xi_i \equiv \xi_i' \pmod{p_i^{t_i}}$ a $\xi_i \equiv 0 \pmod{a_i}$. Součet $\xi = \sum_{i=1}^{m} \xi_i$ pak splňuje kongruenci $\alpha\xi \equiv \beta \pmod{a}$.

Přejděme nyní k obecnému případu. Označme $d = \prod_{i=1}^{m} p_i^{l_i}$ největší společný dělitel divizorů (α) a a. Má-li daná kongruence řešení, pak jistě $d|\beta$. Naopak, předpokládejme, že $d|\beta$. Podle věty 3 kapitoly 7 a věty 4 kapitoly 6 existuje v podílovém

tělese K okruhu R prvek μ takový, že $\nu_{p_i}(\mu) = -l_i$ pro každé $i \in \{1, \dots, m\}$ a současně $\nu_q(\mu) \geq 0$ pro všechny ostatní prvodivizory q. Protože $d|\beta$, platí $\mu\beta \in R$. Podobně $\mu\alpha \in R$ je nesoudělné s divizorem b určeným identitou $bd = a$. Podle první části důkazu existuje $\xi \in R$ splňující $\alpha\mu\xi \equiv \beta\mu \pmod{b}$. Pak $\nu_{p_i}(\alpha\xi - \beta) = \nu_{p_i}(\alpha\mu\xi - \beta\mu) + l_i \geq k_i$ a proto ξ splňuje kongruenci $\alpha\xi \equiv \beta \pmod{a}$.

Lemma 2. Nechť R je Dedekindův okruh, $\alpha_1, \dots, \alpha_m \in R^\times$ libovolné a d největší společný dělitel divizorů $(\alpha_1), \dots, (\alpha_m)$. Pak libovolné $\alpha \in R$ dělitelné d může být vyjádřeno ve tvaru

$$\alpha = \sum_{i=1}^{m} \xi_i \alpha_i, \qquad \xi_1, \dots, \xi_m \in R.$$

Důkaz provedeme indukcí, pro $m = 1$ je lemma zřejmé. Předpokládejme, že $m > 1$ a že lemma platí pro $m - 1$. Označme d_1 největší společný dělitel divizorů $(\alpha_1), \dots, (\alpha_{m-1})$. Pak je d největší společný dělitel divizorů d_1 a (α_m). Podle věty 4 existuje $\xi \in R$ tak, že $\alpha_m\xi \equiv \alpha \pmod{d_1}$. Lemma plyne z indukčního předpokladu pro $\alpha - \xi\alpha_m$.

Věta 5. Pro Dedekindův okruh R je zobrazení $a \mapsto \bar{a}$ izomorfismem pologrupy divizorů D na pologrupu všech nenulových ideálů okruhu R.

Důkaz. Z definice teorie divizorů plyne, že zobrazení $a \mapsto \bar{a}$ je injekce. Ukažme, že je to v případě Dedekindova okruhu též surjekce. Nechť A je libovolný nenulový ideál okruhu R. Pro libovolný prvodivizor p označme $a_p = \min\{\nu_p(\alpha);\, \alpha \in A\}$. Je zřejmé, že $a = \prod_p p^{a_p}$ je divizor. Přitom jistě $A \subseteq \bar{a}$. Nechť $\alpha \in \bar{a}$ je libovolný. Zvolme $\alpha_1, \dots, \alpha_m \in A$ tak, aby a byl největší společný dělitel divizorů $(\alpha_1), \dots, (\alpha_m)$. Podle lemmatu 2 existují $\xi_1, \dots, \xi_m \in R$ tak, že $\alpha = \sum_{i=1}^{m} \xi_i\alpha_i$, odkud $\alpha \in A$. Platí tedy $A = \bar{a}$.

Nechť a, b jsou libovolné divizory a označme $A = \bar{a}$, $B = \bar{b}$, $C = AB$, $c = ab$. Ukážeme $\bar{c} = C$. Platí

$$\begin{aligned}\min\{\nu_p(\gamma);\, \alpha \in C\} &= \min\{\nu_p(\alpha\beta);\, \alpha \in A,\, \beta \in B\} \\ &= \min\{\nu_p(\alpha);\, \alpha \in A\} + \min\{\nu_p(\beta);\, \beta \in B\},\end{aligned}$$

odkud plyne dokazované.

10. Divizory v tělesech algebraických čísel

(podrobnější důkazy viz Borevič-Šafarevič, kapitola 3, §7)

Definice. Nechť K je těleso algebraických čísel, R jeho okruh celých čísel. Pro libovolný divizor a okruhu R se norma $N_{K/\mathbb{Q}}(a)$ nazývá absolutní norma divizoru a (nehrozí-li nebezpečí nedorozumění, píšeme jen $N(a)$). Je to divizor okruhu $\mathbb{Z}$, tj. přirozené číslo. Podobně pro libovolný prvodivizor p okruhu R jeho stupeň inercie (resp. index větvení) vzhledem k rozšíření $K/\mathbb{Q}$ se nazývá absolutní stupeň inercie (resp. absolutní index větvení).

Poznámka. Podle věty 4 kapitoly 8 pro libovolné $\alpha \in R$ platí $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$.

Věta 1. Nechť K je těleso algebraických čísel, R jeho okruh celých čísel. Pro libovolný divizor a okruhu R platí $N(a) = |R/a|$, tj. absolutní norma je rovna počtu prvků okruhu zbytků.

Důkaz. Větu dokážeme nejprve pro prvodivizory. Nechť p je prvodivizor okruhu R a q jím dělitelné prvočíslo. Podle vět 5 a 6 (s přihlédnutím k důkazu věty 4) kapitoly 8 pak $N(p) = q^f$, kde f je absolutní stupeň inercie prvodivizoru p, tj. stupeň rozšíření Σ/Σ_0, kde Σ je těleso zbytků exponentu ν_p a Σ_0 je těleso zbytků exponentu ν_q. Snadno se vidí, že Σ_0 je těleso o q prvcích a tedy Σ je těleso o q^f prvcích. Věta bude pro prvodivizory dokázána, ukážeme-li, že R/p je izomorfní s Σ. Zvolme libovolně $\xi \in K$ tak, že $\nu_p(\xi) \geq 0$. Označme $r_1, \ldots, r_m$ všechny ty prvodivizory, pro které $k_i = \nu_{r_i}(\xi) < 0$. Podle věty 3 kapitoly 9 existuje $\gamma \in R$ tak, že $\gamma \equiv 1 \pmod{p}$ a $\gamma \equiv 0 \pmod{r_i^{-k_i}}$ pro každé $i = 1, \ldots, m$. Pak $\alpha = \xi\gamma \in R$ a $\nu_p(\alpha - \xi) > 0$. Věta je pro prvodivizory dokázána.

Předpokládejme nyní, že věta platí pro nějaké divizory a, b, a dokažme, že pak platí i pro jejich součin ab. Tím bude věta dokázána. Podle věty 4 kapitoly 6 existuje $\gamma \in R$ tak, že $a|\gamma$ a divizor $(\gamma)a^{-1}$ je nesoudělný s b. Nechť $\alpha_1, \ldots, \alpha_r$ (resp. $\beta_1, \ldots, \beta_s$), kde $r = N(\alpha)$ (resp. $s = N(\beta)$), je úplný systém zbyků okruhu R modulo a (resp. b). Ukážeme, že systém rs čísel

$$\alpha_i + \beta_j\gamma, \qquad i \in \{1, \ldots, r\},\ j \in \{1, \ldots, s\}$$

je úplný systém zbyků okruhu R modulo ab. Snadno se ověří, že tyto prvky jsou po dvou nekongruentní modulo ab. Nechť nyní $\alpha \in R$ je libovolné. Pak existuje $i \in \{1, \ldots, r\}$ tak, že $\alpha \equiv \alpha_i \pmod{a}$. Protože největší společný dělitel divizorů (γ) a ab je a, podle věty 4 kapitoly 9 existuje $\xi \in R$ tak, že $\gamma\xi \equiv \alpha - \alpha_i \pmod{ab}$. Pak existuje $j \in \{1, \ldots, s\}$ tak, že $\xi \equiv \beta_j \pmod{b}$, odkud $\alpha \equiv \alpha_i + \beta_j\gamma \pmod{ab}$.

Definice. Nechť K je těleso algebraických čísel, R jeho okruh celých čísel. Divizory a, b okruhu R se nazývají ekvivalentní, píšeme $a \sim b$, existují-li $\alpha, \beta \in R$ tak, že $(\alpha)a = (\beta)b$.

Poznámka. Snadno se vidí, že relace $\sim$ je skutečně relací ekvivalence na pologrupě divizorů D. Navíc lze na třídách ekvivalence zavést násobení pomocí reprezentantů, přičemž se snadno ověří, že vzniklá faktorpologrupa $D/\sim$ je komutativní grupa.

Definice. Grupa $D/\sim$ se nazývá grupa tříd divizorů okruhu R (popřípadě tělesa K). Počet prvků této grupy se nazývá počet tříd divizorů okruhu R (popřípadě tělesa K) a většinou se značí h.

Poznámka. Z věty 2 kapitoly 6 plyne, že R je okruh s jednoznačným rozkladem, právě když $h = 1$.

Cvičení 28. Nechť R je okruh celých čísel tělesa algebraických čísel K. Dokažte, že $h = 2$, právě když R není okruh s jednoznačným rozkladem, avšak libovolné dva rozklady téhož prvku z R na součin prvků ireducibilních v R mají týž počet činitelů (pro jednu implikaci užijte tvrzení (které jsme dosud nedokázali) že každá třída divizorů obsahuje nekonečně mnoho prvodivizorů).

Poznámka. Připomeňme definici diskriminantu tělesa algebraických čísel K. Protože okruh celých čísel R je modul (ve smyslu kapitoly 5), má bazi. Diskriminant této baze se nazývá diskriminant tělesa K a zřejmě je na konkrétním výběru baze okruhu R nezávislý.

Lemma. Nechť K je těleso algebraických čísel, d jeho diskriminant, R jeho okruh celých čísel, D pologrupa divizorů okruhu R, $n = [K : \mathbb{Q}]$. Nechť existuje právě s

reálných vnoření tělesa K a právě t párů komplexních vnoření (pak tedy $s+2t=n$). Pak v libovolné třídě rozkladu $D/\sim$ existuje divizor a, jehož absolutní norma

$$N(a) \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|d|}.$$

Důkaz je v podstatě založen na Minkowského větě o konvexním tělese a je veden podobným způsobem jako důkaz Dirichletovy věty o jednotkách. Tuto techniku jsme z časových důvodů vynechali a proto mohu čtenáře pouze odkázat na knihu Borevič-Šafarevič, kapitola 2, §§3–6.

Věta 2. Grupa tříd divizorů libovolného tělesa algebraických čísel je konečná.

Důkaz plyne z předchozího lemmatu vzhledem k tomu, že existuje vždy jen konečně mnoho divizorů s danou absolutní normou.

Věta 3. Nechť h je počet tříd divizorů tělesa algebraických čísel. Pak pro divizory okruhu celých čísel tohoto tělesa platí

(a) h-tá mocnina libovolného divizoru je hlavní divizor;
(b) je-li l přirozené číslo nesoudělné s h a je-li a takový divizor, že a^l je hlavní, pak také a je hlavní divizor.

Důkaz je zřejmý.

11. Charaktery konečných abelovských grup

Definice. Nechť G je abelovská grupa. Libovolný homomorfismus $G \to \mathbb{C}^\times$ nazýváme charakter grupy G.

Poznámka. Množina všech charakterů abelovské grupy G vzhledem k operaci násobení dané předpisem $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$ tvoří opět abelovskou grupu, kterou značíme $\widehat{G}$.

Lemma 1. Je-li G konečná abelovská grupa, pak $G \simeq \widehat{G}$ (nekanonicky).

Důkaz. Protože G je přímý součin aditivních grup tvaru $\mathbb{Z}/m\mathbb{Z}$, je $\widehat{G}$ přímý součin grup $\widehat{\mathbb{Z}/m\mathbb{Z}}$. Ale je-li $\chi \in \widehat{\mathbb{Z}/m\mathbb{Z}}$, pak je χ určeno hodnotou $\chi(1)$ (připomeňme, že $\mathbb{Z}/m\mathbb{Z}$ je aditivní). Protože $\chi(1)$ může být libovolná m-tá odmocnina z jedné, lemma platí pro $\mathbb{Z}/m\mathbb{Z}$ a tedy i pro G.

Důsledek. Je-li G konečná abelovská grupa, pak $G \simeq \widehat{\widehat{G}}$ (kanonicky).

Důkaz. Libovolné $g \in G$ určuje charakter g' grupy $\widehat{G}$ předpisem $g'(\chi) = \chi(g)$. Předpokládejme, že pro nějaké $g \in G$ platí $\chi(g) = 1$ pro všechna $\chi \in \widehat{G}$. Označme H podgrupu generovanou g. Pak $\widehat{G}$ lze chápat jako množinu různých charakterů faktorgrupy G/H, kterých je podle lemmatu nejvýše $|G/H|$, je tedy $H = \{1\}$. Předpis $g \mapsto g'$ proto určuje injekci $G \to \widehat{\widehat{G}}$. Protože $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$, jsme hotovi.

Definice. Pro libovolnou podgrupu H abelovské grupy G označme

$$H^\perp = \{\chi \in \widehat{G};\, \forall h \in H :\, \chi(h) = 1\}.$$

Poznámka. Zřejmě máme přirozený izomorfismus $H^\perp \simeq \widehat{G/H}$. Navíc pro libovolné podgrupy H_1, H_2 platí

$$H_1 \subseteq H_2 \quad \Longleftrightarrow \quad H_1^\perp \supseteq H_2^\perp.$$

Lemma 2. Pro libovolnou podgrupu H konečné abelovské grupy G platí $\widehat{H} \simeq \widehat{G}/H^\perp$.

Důkaz. Restrikce dává homomorfismus $\widehat{G} \to \widehat{H}$ s jádrem $H^\perp$. Zbývá ukázat surjektivitu, ovšem $|H^\perp| = |\widehat{G/H}| = |G/H| = |G|/|H|$ a proto $|\widehat{H}| = |H| = |G|/|H^\perp| = |\widehat{G}|/|H^\perp|$.

Lemma 3. Pro libovolnou podgrupu H konečné abelovské grupy G je $(H^\perp)^\perp = H$, kde jsme stotožnili $G = \widehat{\widehat{G}}$ a kde pro vnější kolmičku chápeme $H^\perp$ jako podgrupu grupy $\widehat{G}$.

Důkaz. Jako v předešlém důkaze se snadno spočítá, že obě grupy mají týž řád. Je-li $h \in H$, pak h jakožto prvek $\widehat{\widehat{G}}$ zobrazující libovolné $\chi \in \widehat{G}$ na $\chi(h)$ zobrazí všechny prvky $H^\perp$ na 1. Proto $H \subseteq (H^\perp)^\perp$.

Důsledek. $^\perp$ je tedy antiizomorfismus mezi svazem všech podgrup konečné abelovské grupy G a svazem všech podgrup její grupy charakterů $\widehat{G}$.

12. Dirichletovy charaktery

Definice. Dirichletův charakter je charakter grupy $(\mathbb{Z}/n\mathbb{Z})^\star$ pro nějaké $n \in \mathbb{N}$, tj. homomorfismus $\chi : (\mathbb{Z}/n\mathbb{Z})^\star \to \mathbb{C}^\times$. Je-li $n|m$, pak χ indukuje složením s kanonickým homomorfismem $(\mathbb{Z}/m\mathbb{Z})^\star \to (\mathbb{Z}/n\mathbb{Z})^\star$ homomorfismus $\chi : (\mathbb{Z}/m\mathbb{Z})^\star \to \mathbb{C}^\times$. Přitom jde vpodstatě o totéž zobrazení, můžeme tedy χ uvažovat podle libosti definovaný jak modulo m tak i modulo n. Pro jednoznačnost zavedeme konvenci, že pro dané χ budeme vždy uvažovat ten nejmenší možný modul a budeme jej nazývat konduktor Dirichletova charakteru χ a označovat f_χ.

Příklady. Existuje jediný Dirichletův charakter s konduktorem 1, kterému se říká jednotkový nebo též triviální charakter. Žádný Dirichletův charakter nemá konduktor 2. Pro konduktory 3, 4 a 12 existuje vždy po jednom Dirichletově charakteru, pro konduktor 5 existují právě 3.

Identifikace. Nechť χ je Dirichletův charakter s konduktorem f_χ. Pak χ identifikujeme se zobrazením $\mathbb{Z} \to \mathbb{C}$, které je určeno předpisem $a \mapsto \chi(a + f_\chi\mathbb{Z})$ pro $a \in \mathbb{Z}$ nesoudělné s f_χ a $a \mapsto 0$ pro $a \in \mathbb{Z}$ soudělné s f_χ.

Definice. Nechť χ a ψ jsou Dirichletovy charaktery. Označme n nejmenší společný násobek jejich konduktorů a uvažme je oba na okamžik jako charaktery grupy $(\mathbb{Z}/n\mathbb{Z})^\star$. Součinem $\chi\psi$ budeme rozumět Dirichletův charakter (s co nejmenším modulem) určený součinem obou charakterů v grupě $\widehat{(\mathbb{Z}/n\mathbb{Z})^\star}$.

Příklad. Zvolme například Dirichletovy charaktery χ, ψ, které jsou jednoznačně určeny podmínkou $f_\chi = 12$, $f_\psi = 3$. Pak $f_{\chi\psi} = 4$. Všimněte si, že pro $a \in \mathbb{Z}$ obecně neplatí $\chi(a)\psi(a) = (\chi\psi)(a)$, např. $\chi(9) = 0$, $\psi(9) = 0$, avšak $(\chi\psi)(9) = 1$.

Cvičení 29. Dokažte, že pro libovolné Dirichletovy charaktery χ, ψ a libovolné $a \in \mathbb{Z}$ platí, že je-li $\chi(a)\psi(a) \neq 0$, pak $\chi(a)\psi(a) = (\chi\psi)(a)$.

Cvičení 30. Dokažte, že množina všech Dirichletových charakterů tvoří grupu.

Cvičení 31. Dokažte, že pro libovolné Dirichletovy charaktery χ, ψ, jejichž konduktory jsou nesoudělné, platí $f_{\chi\psi} = f_\chi f_\psi$.

Opakování (viz důsledek věty 1 kapitoly 4). Nechť m je přirozené číslo a $\zeta_m = e^{\frac{2\pi i}{m}}$. Pak m-té kruhové těleso $\mathbb{Q}(\zeta_m)$ je Galoisovo, $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m)$ a pro

jeho Galoisovu grupu $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ platí, že je izomorfní s grupou invertibilních prvků okruhu zbytkových tříd $\mathbb{Z}/m\mathbb{Z}$, kde izomorfismus je určen tím, že libovolný automorfismus $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ s vlastností $\sigma(\zeta_m) = \zeta_m^s$ se zobrazí na třídu rozkladu obsahující s.

Označení. V dalším budeme m-té kruhové těleso značit $\mathbb{Q}_m$.

Věta 1. Pro libovolná přirozená čísla m, n platí

1. kompozitum $\mathbb{Q}_m\mathbb{Q}_n = \mathbb{Q}_{[m,n]}$, kde $[m,n]$ značí nejmenší společný násobek čísel m, n;
2. průnik $\mathbb{Q}_m \cap \mathbb{Q}_n = \mathbb{Q}_{(m,n)}$, kde (m,n) značí největší společný dělitel čísel m, n.

Důkaz. Je zřejmé, že $\mathbb{Q}_{(m,n)} \subseteq \mathbb{Q}_m \subseteq \mathbb{Q}_{[m,n]}$ a $\mathbb{Q}_{(m,n)} \subseteq \mathbb{Q}_n \subseteq \mathbb{Q}_{[m,n]}$. Z Bezoutovy identity plyne existence celých čísel a, b takových, že $(m,n) = am + bn$. Pak platí

$$\zeta_{[m,n]} = \zeta_{mn}^{(m,n)} = \zeta_{mn}^{am+bn} = \zeta_n^a \zeta_m^b \in \mathbb{Q}_m\mathbb{Q}_n\,,$$

odkud plyne 1. Označme $K = \mathbb{Q}_m \cap \mathbb{Q}_n$. Víme, že $\mathbb{Q}_{(m,n)} \subseteq K$. Dokážeme, že platí rovnost. Podle cvičení 11 (kapitola 2) platí

$$[\mathbb{Q}_{[m,n]} : \mathbb{Q}][K : \mathbb{Q}] = [\mathbb{Q}_m : \mathbb{Q}][\mathbb{Q}_n : \mathbb{Q}],$$

odkud

$$[K : \mathbb{Q}] = \frac{\varphi(m)\varphi(n)}{\varphi([m,n])} = \varphi((m,n)),$$

a tedy platí 2.

Věta 2 (Kronecker - Weber). Je-li $K/\mathbb{Q}$ konečné abelovské rozšíření, pak $K \subseteq \mathbb{Q}_n$ pro vhodné přirozené číslo n.

Důkaz svým rozsahem i hloubkou značně přesahuje rámec tohoto kurzu (důkaz je možné najít například ve Washingtonově knize, kde je mu věnováno asi deset stran ve 14. kapitole).

Definice. Nechť $K/\mathbb{Q}$ je konečné abelovské rozšíření, pak nejmenší přirozené číslo n splňující $K \subseteq \mathbb{Q}_n$ (jeho existence je zaručena větami 2 a 1) se nazývá konduktor tělesa K.

Příklad. Konduktorem tělesa $\mathbb{Q}(\sqrt{2})$ je 8.

Konstrukce. Nechť X je konečná grupa Dirichletových charakterů (tj. libovolná konečná podgrupa grupy všech Dirichletových charakterů). Nechť n je nejmenší společný násobek konduktorů f_χ pro všechny $\chi \in X$. Pro libovolné přirozené číslo m, které je násobkem čísla n, pak lze X chápat jako podgrupu grupy charakterů grupy $(\mathbb{Z}/m\mathbb{Z})^\star$, která je (přirozeně) izomorfní s grupou $\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})$. Pak ovšem X jednoznačně určí podgrupu $X^\perp$ grupy $\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})$ a tedy pomocí Galoisovy korespondence podtěleso K_X tělesa $\mathbb{Q}_m$ vztahem $\mathrm{Gal}(\mathbb{Q}_m/K_X) = X^\perp$. Přitom podle lemmat 1 a 2 kapitoly 11 platí, že

$$|X| = |\widehat{X}| = \frac{[\mathbb{Q}_m : \mathbb{Q}]}{|X^\perp|} = [K_X : \mathbb{Q}],$$

kde poslední rovnost plyne z hlavní věty Galoisovy teorie (kapitola 2, pozor na to, že tam mělo $^\perp$ jiný význam, než má zde).

Dokažme nyní, že těleso K_X je nezávislé na volbě m. Uvážíme výše uvedenou konstrukci pro $m = n$ a pro libovolný násobek m čísla n. Aby se nám konstrukce nepletly, budeme je odlišovat indexem: $X^{\perp_n}$ a $X^{\perp_m}$, $K_X^{(n)}$ a $K_X^{(m)}$. Protože konduktor libovolného $\chi \in X$ je dělitelem n, platí $\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q}_n) \subseteq X^{\perp_m}$, odkud $K_X^{(m)} \subseteq \mathbb{Q}_n$. Zvolme libovolně $\tau \in \mathrm{Gal}(\mathbb{Q}_n/K_X^{(m)})$. Pak existuje $\sigma \in \mathrm{Gal}(\mathbb{Q}_m/K_X^{(m)})$ s vlastností $\sigma|_{\mathbb{Q}_n} = \tau$ (viz větu 2 kapitoly 2). Protože $\sigma \in X^{\perp_m}$, je $\chi(\sigma) = 1$ pro každé $\chi \in X$. Pak ale také $\chi(\tau) = 1$ pro každé $\chi \in X$, odkud $\tau \in \mathrm{Gal}(\mathbb{Q}_n/K_X^{(n)})$. Dostáváme inkluzi mezi tělesy $K_X^{(n)} \subseteq K_X^{(m)}$, které mají týž stupeň, jsou tedy stejné.

Z věty Kroneckera - Webera, z hlavní věty Galoisovy teorie a z důsledku za lemmatem 3 kapitoly 11 plyne

Věta 3. Pro libovolné abelovské těleso K konečného stupně nad $\mathbb{Q}$ existuje jednoznačně určená konečná grupa Dirichletových charakterů X taková, že $K = K_X$. Pro libovolné konečné grupy Dirichletových charakterů X_1, X_2 platí

$$X_1 \subseteq X_2 \quad \Longleftrightarrow \quad K_{X_1} \subseteq K_{X_2}.$$

Důsledek. Ve výše uvedené jednojednoznačné korespondenci mezi konečnými grupami Dirichletových charakterů a abelovskými tělesy průniku grup odpovídá průnik těles, grupě generované sjednocením grup odpovídá kompositum těles.

Poznámka. Protože platí (v označení konstrukce)

$$\mathrm{Gal}(K_X/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q})/\,\mathrm{Gal}(\mathbb{Q}_m/K_X),$$

podle poznámky před lemmatem 2 kapitoly 11 platí

$$\widehat{\mathrm{Gal}(K_X/\mathbb{Q})} \simeq \mathrm{Gal}(\mathbb{Q}_m/K_X)^\perp = (X^\perp)^\perp = X$$

a tedy grupa charakterů Galoisovy grupy tělesa K_X je přirozeně izomorfní s grupou Dirichletových charakterů. Díky tomuto izomorfismu lze obé stotožnit: při tom pro $\chi \in X$ a $\sigma \in \mathrm{Gal}(K_X/\mathbb{Q})$ je definováno $\chi(\sigma)$ jako $\chi(\tau)$, kde $\tau \in \mathrm{Gal}(\mathbb{Q}_M/\mathbb{Q})$ je libovolný automorfismus takový, že restrikce $\tau|_{K_X} = \sigma$.

13. Frobeniův automorfismus

Označení. Konečné těleso o q prvcích značíme $\mathbb{F}_q$.

Věta 1. Nechť $\mathbb{F}_{q^n}/\mathbb{F}_q$ je konečné rozšíření konečných těles. Pak $\mathbb{F}_{q^n}/\mathbb{F}_q$ je Galoisovo rozšíření s cyklickou Galoisovou grupou generovanou tzv. Frobeniovým automorfismem tohoto rozšíření, který je určen předpisem $\mathrm{Frob}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = x^q$ pro libovolné $x \in \mathbb{F}_q$.

Důkaz. Je zřejmé, že $\mathrm{Frob}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ je skutečně automorfismus tělesa $\mathbb{F}_{q^n}$ a že vygeneruje cyklickou grupu automorfismů $\langle \mathrm{Frob}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \rangle$ řádu n. Navíc pro libovolné $x \in \mathbb{F}_q$ platí $\mathrm{Frob}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = x$, právě když $x \in \mathbb{F}_q$. Podle výsledku Cvičení 9 je $\mathbb{F}_{q^n}/\mathbb{F}_q$ Galoisovo rozšíření. Protože stupeň rozšíření $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, je $\langle \mathrm{Frob}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \rangle = \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

Poznámka. Nyní budeme aplikovat znalosti získané v cvičeních 24 a 26 na tělesa algebraických čísel.

Nechť K/k je Galoisovo rozšíření těles algebraických čísel (ne nutně abelovských), $G = \mathrm{Gal}(K/k)$. Nechť ν_0 je exponent tělesa k a ν nějaké prodloužení exponentu ν_0 na těleso K. Označme dále Σ_0 těleso zbytků exponentu ν_0 a Σ_ν těleso zbytků exponentu ν. Protože K i k jsou konečná rozšíření $\mathbb{Q}$, je ν prodloužením p-adického exponentu na $\mathbb{Q}$ pro nějaké vhodné prvočíslo p. Proto jsou Σ_ν i Σ_0 konečná rozšíření tělesa $\mathbb{Z}/p\mathbb{Z}$, jsou to tedy konečná tělesa (charakteristiky p). Podle věty 1 je tudíž rozšíření Σ_ν/Σ_0 Galoisovo.

Označme I_ν inerční grupu příslušnou exponentu ν a D_ν dekompoziční grupu příslušnou exponentu ν (vždy vzhledem k ν_0 neboli vzhledem k rozšíření K/k). Ve Cvičení 24(f) jsme ukázali, že existuje právě $g = |G/D_\nu|$ různých prodloužení exponentu ν_0 na K, a ve Cvičení 26(g,f), že všechna mají týž index větvení $e = |I_\nu|$ a týž stupeň inercie $f = |D_\nu/I_\nu|$. Navíc platí (viz Cvičení 24(a)): libovolné prodloužení exponentu ν_0 na K je tvaru ν^σ pro nějaké $\sigma \in G$ (kde ν^σ je definováno předpisem $\nu^\sigma(\alpha) = \nu(\sigma(\alpha))$).

Označme $O_\nu = \{\alpha \in K;\, \nu(\alpha) \geq 0\}$, $P_\nu = \{\alpha \in K;\, \nu(\alpha) > 0\}$ (pak tedy $\Sigma_\nu = O_\nu/P_\nu$). Zřejmě platí: σ^{-1} indukuje izomorfismus $\sigma^{-1} : O_\nu \to \sigma^{-1}O_\nu = O_{\nu^\sigma}$. Podle definice pro $\tau \in G$ platí $\tau \in D_\nu$, právě když $\tau O_\nu = O_\nu$. Je tedy

$$\begin{aligned}\tau \in D_{\nu^\sigma} &\iff \tau O_{\nu^\sigma} = O_{\nu^\sigma} \iff \tau\sigma^{-1}O_\nu = \sigma^{-1}O_\nu \iff \\ &\iff \sigma\tau\sigma^{-1}O_\nu = O_\nu \iff \sigma\tau\sigma^{-1} \in D_\nu.\end{aligned}$$

Je tedy $D_{\nu^\sigma} = \sigma^{-1}D_\nu\sigma$. Izomorfismus σ^{-1} zobrazí P_ν na $\sigma^{-1}P_\nu = P_{\nu^\sigma}$, tedy po faktorizaci dostaneme izomorfismus $\overline{\sigma^{-1}} : \Sigma_\nu \to \Sigma_{\nu^\sigma}$. Pro $\sigma \in D_\nu$ platí $\Sigma_\nu = \Sigma_{\nu^\sigma}$ a tedy přiřazení $\sigma \mapsto \bar\sigma$ dává homomorfismus $D_\nu \to \mathrm{Gal}(\Sigma_\nu/\Sigma_0)$. Dle definice jádrem tohoto homomorfismu je I_ν. Je-li tedy $\tau \in I_\nu$, je $\bar\tau = \mathrm{id}_{\Sigma_\nu}$. Pak ale $\sigma^{-1}\tau\sigma \in D_{\nu^\sigma}$ a platí $\overline{\sigma^{-1}\tau\sigma} = \mathrm{id}_{\Sigma_{\nu^\sigma}}$. Je tedy $\sigma^{-1}I_\nu\sigma \subseteq I_{\nu^\sigma}$, analogicky opačná inkluze, a tedy rovnost. Uvědomme si ještě následující zřejmou ale užitečnou ekvivalenci:

$$\tau \in I_{\nu^\sigma} \iff \tau \in D_{\nu^\sigma} \quad \wedge \quad \forall \alpha \in O_\nu : \nu(\alpha - \tau(\alpha)) > 0.$$

Protože $\mathrm{Frob}_{\Sigma_\nu/\Sigma_0}(x) = x^{|\Sigma_0|}$ a $\mathrm{Frob}_{\Sigma_{\nu^\sigma}/\Sigma_0}(x) = x^{|\Sigma_0|}$, dostáváme komutativní diagram

$$\begin{array}{ccc} \Sigma_\nu & \xrightarrow{\overline{\sigma^{-1}}} & \Sigma_{\nu^\sigma} \\ {\scriptstyle \mathrm{Frob}_{\Sigma_\nu/\Sigma_0}}\downarrow & & \downarrow{\scriptstyle \mathrm{Frob}_{\Sigma_{\nu^\sigma}/\Sigma_0}} \\ \Sigma_\nu & \xrightarrow[\overline{\sigma^{-1}}]{} & \Sigma_{\nu^\sigma} \end{array}$$

a tedy platí $\mathrm{Frob}_{\Sigma_{\nu^\sigma}/\Sigma_0} = \overline{\sigma^{-1}}\,\mathrm{Frob}_{\Sigma_\nu/\Sigma_0}\,\overline{\sigma}$.

Předpokládejme nyní, že exponent ν_0 je v K/k nerozvětvený, tj. $e = 1$. Pak jádro I_ν přirozeného surjektivního homomorfismu grup $D_\nu \to \mathrm{Gal}(\Sigma_\nu/\Sigma_0)$ je triviální, jde tedy o izomorfismus. Vzor Frobeniova automorfismu rozšíření Σ_ν/Σ_0 v tomto izomorfismu (tedy odpovídající prvek $D_\nu \subseteq \mathrm{Gal}(K/k)$) se nazývá Frobeniův automorfismus exponentu ν vzhledem k rozšíření K/k a značí se $\mathrm{Frob}(\nu, K/k)$, často též $\mathrm{Frob}(Q, K/k)$, kde Q je prvodivizor tělesa K odpovídající exponentu ν. Z výše dokázaného plyne $\mathrm{Frob}(\nu^\sigma, K/k) = \sigma^{-1}\,\mathrm{Frob}(\nu, K/k)\sigma$.

Je-li dokonce rozšíření K/k abelovské (tj. těleso K samo nemusí být abelovské, jen grupa $\mathrm{Gal}(K/k)$ musí být komutativní), pak všechna prodloužení exponentu ν_0 mají nejen stejné dekompoziční a inerční grupy, ale také týž Frobeniův automorfismus, který tedy závisí pouze na exponentu ν_0 a rozšíření K/k. V tomto případě se nazývá Artinův automorfismus a značí se $(q, K/k)$, kde q je prvodivizor tělesa k odpovídající exponentu ν_0. Tuto definici je pak možné rozšířit na tzv. Artinovo zobrazení, což je homomorfismus $D' \to \mathrm{Gal}(K/k)$, kde D' je podpologrupa pologrupy divizorů D tělesa k generovaná všemi prvodivizory nerozvětvenými v K/k. Toto zobrazení hraje klíčovou roli v tzv. „class field theory“.

Příklad. Nechť n je přirozené číslo nedělitelné prvočíslem p. Uvažme p-adický exponent ν_0 na $\mathbb{Q}$, rozšíření $\mathbb{Q}_n/\mathbb{Q}$ a označme ν nějaké prodloužení ν_0 na $\mathbb{Q}_n$. Chceme ukázat, že exponent ν_0 je nerozvětvený v $\mathbb{Q}_n/\mathbb{Q}$ a určit Artinův automorfismus $(p, \mathbb{Q}_n/\mathbb{Q})$. Označme Σ, resp. Σ_0 těleso zbytků exponentu ν, resp. ν_0. Je tedy $\Sigma_0 \simeq \mathbb{Z}/p\mathbb{Z}$ a $\Sigma \simeq \mathbb{F}_{p^f}$, kde f je (absolutní) stupeň inercie exponentu ν. Pro $\alpha \in O_\nu$ označme $\overline{\alpha} \in \Sigma$ třídu obsahující α. Protože

$$p \nmid n = \prod_{i=1}^{n-1} (1 - \zeta_n^i),$$

jsou $\overline{1}, \overline{\zeta_n}, \ldots, \overline{\zeta_n^{n-1}}$ různé prvky Σ, neboli $\nu(\zeta_n^i - \zeta_n^j) = 0$ pro $0 \le i < j < n$. Navíc p nedělí diskriminant $D(\Phi_n)$ minimálního polynomu Φ_n čísla ζ_n (připomeňme, že diskriminant je roven druhé mocnině součinu rozdílů kořenů, a tedy $\nu(D(\Phi_n)) = 0$). Můžeme tedy aplikovat větu 8 kapitoly 8 a dostáváme, že exponent ν_0 je skutečně nerozvětvený v $\mathbb{Q}_n/\mathbb{Q}$. Protože $\mathrm{Frob}_{\Sigma/\Sigma_0}(\overline{\zeta_n}) = \overline{\zeta_n}^p$ a $\overline{1}, \overline{\zeta_n}, \ldots, \overline{\zeta_n^{n-1}}$ jsou různé prvky Σ, dostáváme $\mathrm{Frob}(\nu, \mathbb{Q}_n/\mathbb{Q})(\zeta_n) = \zeta_n^p$. V přirozeném izomorfismu $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\star$ odpovídá Artinův izomorfismus $(p, \mathbb{Q}_n/\mathbb{Q})$ třídě $p + n\mathbb{Z}$. Určeme ještě stupeň inercie f. Protože je exponent ν_0 nerozvětvený, je inerční grupa triviální a tedy dekompoziční grupa je izomorfní $\mathrm{Gal}(\Sigma/\Sigma_0)$, je tedy cyklická řádu f generovaná Frobeniovým automorfismem. Jeho řád je ovšem týž jako řád třídy $p + n\mathbb{Z}$ v $(\mathbb{Z}/n\mathbb{Z})^\star$. Je tedy $f = \min\{j \in \mathbb{N};\ p^j \equiv 1 \pmod n\}$. Protože index dekompoziční grupy je počet prodloužení exponentu ν_0, vidíme, že těchto prodloužení (neboli prvodivizorů tělesa $\mathbb{Q}_n$ dělících prvočíslo p) je právě $\frac{\varphi(n)}{f}$ (což nyní rovněž plyne věty 7 kapitoly 8).

Konkrétní příklad. Zjistěme, jak se rozkládá prvočíslo 2 v okruhu celých čísel sedmého kruhového tělesa. Podle předchozího příkladu se rozkládá na součin dvou různých prvodivizorů, jejichž stupeň inercie je 3. Věta 8 kapitoly 8 ukazuje, jak je najít: je třeba rozložit kruhový polynom $\Phi_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ nad $\mathbb{Z}/2\mathbb{Z}$. Hledaný rozklad je

$$\Phi_7 \equiv (x^3 + x + 1)(x^3 + x^2 + 1) \pmod 2,$$

a tedy 2 se rozkládá na prvodivizory

$$(2) = (\zeta_7^3 + \zeta_7 + 1, 2)(\zeta_7^3 + \zeta_7^2 + 1, 2),$$

kde (α, β) značí nejmenšího společného dělitele divizorů (α) a (β). V tomto případě můžeme dokonce počítat dál, platí totiž $(\zeta_7^3 + \zeta_7 + 1)(\zeta_7^3 + \zeta_7^2 + 1) = 2\zeta_7^3$ a tedy

$2 = (1+\zeta_7+\zeta_7^3)(1+\zeta_7^{-1}+\zeta_7^{-3})$ je rozklad čísla 2 na prvočinitele (těleso $\mathbb{Q}_7$ má totiž počet tříd divizorů roven 1 a tedy okruh jeho celých čísel je okruh s jednoznačným rozkladem.

Věta 2. Nechť K, L jsou tělesa algebraických čísel taková, že obě rozšíření $KL/K \cap L$ a $L/K \cap L$ jsou Galoisova. Nechť ν je exponent kompozita KL, ν_L, resp. ν_K, ν_0 jím indukovaný exponent tělesa L, resp. K, $K \cap L$. Pak platí: je-li exponent ν_L nerozvětvený v $L/K \cap L$, pak je exponent ν nerozvětvený v KL/K.

Důkaz. Restrikce indukuje homomorfismus $\mathrm{Gal}(KL/K) \to \mathrm{Gal}(L/K \cap L)$, který je injektivní, neboť $\mathrm{Gal}(KL/K) \cap \mathrm{Gal}(KL/L) = \mathrm{Gal}(KL/KL) = \{\mathrm{id}_{KL}\}$ dle hlavní věty Galoisovy teorie. Jestliže $\tau \in \mathrm{Gal}(KL/K)$ patří do inerční grupy exponentu ν (vzhledem k rozšíření KL/K), pak platí $\tau O_\nu = O_\nu$ a pro každé $\alpha \in O_\nu$ je $\nu(\alpha - \tau(\alpha)) > 0$. Protože $O_{\nu_L} = L \cap O_\nu$ a $\tau L = L$, platí $\tau O_{\nu_L} = O_{\nu_L}$ a pro každé $\alpha \in O_{\nu_L}$ je $\nu_L(\alpha - \tau(\alpha)) > 0$. Odtud plyne, že $\tau|_L \in \mathrm{Gal}(L/K \cap L)$ patří do inerční grupy exponentu ν_L (vzhledem k rozšíření $L/K \cap L$). Věta plyne z toho, že počet prvků inerční grupy je právě index větvení.

Poznámka. Restrikce v předchozím důkaze indukuje izomorfismus: označme $P = K \cap L$. Dle věty 10 kapitoly 1 existuje $\theta \in L$ tak, že $L = P(\theta)$. Pak $KL = K(\theta)$. Označme φ_θ a ψ_θ minimalní polynomy θ vzhledem k L a KL. Platí $\psi_\theta | \varphi_\theta$ a $\varphi_\theta(t) = \prod_{\sigma \in \mathrm{Gal}(L/P)}(t - \sigma(\theta))$. Existuje tedy $Y \subseteq \mathrm{Gal}(L/P)$ tak, že $\psi_\theta(t) = \prod_{\sigma \in Y}(t - \sigma(\theta)) \in L[t]$. Ovšem $K[t] \cap L[t] = P[t]$, odkud $\varphi_\theta = \psi_\theta$ a $[KL : K] = \mathrm{st}\,\psi_\theta = \mathrm{st}\,\varphi_\theta = [L : P]$.

14. Pologrupa divizorů abelovských těles

V této kapitole nám půjde o to, popsat pologrupu divizorů abelovských těles. Protože pologrupa divizorů je volná, postačí popsat její generátory, tj. prvodivizory. Z věty 1 kapitoly 8 plyne, že každý prvodivizor dělí právě jedno prvočíslo, bude tedy stačit nalézt způsob, jakým se prvočísla v pologrupě divizorů rozkládají. Jde tedy o to, určit počet prodloužení p-adického exponentu a určit jejich indexy větvení a stupně inercie podobně jako jsme to udělali pro n-té kruhové těleso a prvočíslo p nedělící n v příkladě v minulé kapitole. Protože abelovská tělesa jsou Galoisova rozšíření $\mathbb{Q}$, jsou (pro dané těleso a dané p) tyto indexy větvení a stupně inercie stejné.

Definice. Nechť K/k je konečné rozšíření těles, ν exponent tělesa k. Řekneme, že se ν zcela rozkládá v rozšíření K/k, existuje-li $[K : k]$ různých prodloužení exponentu ν na K.

Poznámka. Podle lemmatu 1 kapitoly 7 exponent mít více prodloužení nemůže.

Věta 1. Nechť p je prvočíslo, $n \in \mathbb{N}$. V p^n-tém kruhovém tělese $\mathbb{Q}_{p^n}$ je p-adický exponent totálně rozvětvený.

Důkaz. Pro p^n-tý kruhový polynom Φ_{p^n} platí

$$\Phi_{p^n} = \frac{x^{p^n}-1}{x^{p^{n-1}}-1} = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \cdots + x^{p^{n-1}} + 1 = \prod_{\substack{j=1,\ldots,p^n \\ p \nmid j}} (x - \zeta_{p^n}^j).$$

Dosazením $x = 1$ dostaneme identitu

$$p = \prod_{\substack{j=1,\dots,p^n \\ p\nmid j}} (1 - \zeta_{p^n}^j).$$

Snadno se vidí, že podíl libovolných dvou činitelů v tomto součinu je jednotka okruhu celých čísel tělesa $\mathbb{Q}_{p^n}$. Přechodem k divizorům dostaneme

$$(p) = (1 - \zeta_{p^n})^{\phi(p^n)},$$

odkud plyne dokazované tvrzení.

Konstrukce. Rozložme přirozené číslo n na prvočinitele: $n = \prod_p p^{a_p}$. Díky přirozenému izomorfismu

$$(\mathbb{Z}/n\mathbb{Z})^\star \simeq \prod_p (\mathbb{Z}/p^{a_p}\mathbb{Z})^\star$$

můžeme každý Dirichletův charakter χ jednoznačně rozložit na součin $\chi = \prod_p \chi_p$, kde χ_p je Dirichletův charakter modulo p^{a_p}. Je-li X konečná grupa Dirichletových charakterů, označme $X_p = \{\chi_p;\ \chi \in X\}$, což je opět konečná grupa Dirichletových charakterů (ne nutně podgrupa grupy X).

Věta 2. Nechť X je konečná grupa Dirichletových charakterů a $K = K_X$ jí odpovídající abelovské těleso. Pak pro libovolné prvočíslo p platí: index větvení p-adického exponentu v rozšíření $K/\mathbb{Q}$ je roven počtu prvků grupy X_p.

Důkaz. Připomeňme, že jsou-li $F \subseteq F' \subseteq F''$ tělesa, je index větvení libovolného exponentu ν tělesa F'' vzhledem k rozšíření F''/F roven součinu jeho indexu větvení vzhledem k F''/F' a indexu větvení jím indukovaného exponentu vzhledem k F'/F.

Označme n nejmenší společný násobek konduktorů charakterů z X, je tedy $K \subseteq \mathbb{Q}_n$. Nechť $n = m \cdot p^a$, kde $p \nmid m$. Uvažme kompozitum $L = K\mathbb{Q}_m$. Pro grupu charakterů Y tělesa L pak platí $Y = X(\widehat{\mathbb{Z}/m\mathbb{Z}})^\star = X_p(\widehat{\mathbb{Z}/m\mathbb{Z}})^\star$. Označme $F = K_{X_p}$ těleso odpovídající grupě X_p. Je tedy $F \subseteq \mathbb{Q}_{p^a}$ a platí $L = FK$. V následujících úvahách hovoříme o větvení p-adického exponentu nebo jeho prodloužení. Dle příkladu z minulé kapitoly je v rozšíření $\mathbb{Q}_m/\mathbb{Q}$ nerozvětvený, proto je i v rozšíření $\mathbb{Q}_m/K \cap \mathbb{Q}_m$ nerozvětvený, podle věty 2 kapitoly 13 je i v rozšíření L/K nerozvětvený, má tedy v rozšířeních $K/\mathbb{Q}$ a $L/\mathbb{Q}$ týž index větvení e. Protože je v rozšíření $\mathbb{Q}_m/\mathbb{Q}$ nerozvětvený, podle zmíněné věty je i v rozšíření L/F nerozvětvený a tedy e je i index větvení v rozšíření $F/\mathbb{Q}$. Podle věty 1 je v rozšíření $F/\mathbb{Q}$ totálně rozvětvený, a tedy $e = [F : \mathbb{Q}] = |X_p|$, což jsme měli dokázat.

Důsledek. Nechť X je konečná grupa Dirichletových charakterů a $K = K_X$ jí odpovídající abelovské těleso. Pak pro libovolné prvočíslo p platí: p je v $K/\mathbb{Q}$ nerozvětvené, právě když $\chi(p) \neq 0$ pro všechny charaktery $\chi \in X$.

Důkaz. Platí: p je v $K/\mathbb{Q}$ rozvětvené, právě když $|X_p| > 1$, tj. právě když existuje $\chi \in X$ tak, že $\chi_p \neq 1$, tj. právě když existuje $\chi \in X$ tak, že $p|f_\chi$, tj. právě když existuje $\chi \in X$ tak, že $\chi(p) = 0$.

Věta 3. Nechť X je konečná grupa Dirichletových charakterů a $K = K_X$ jí odpovídající abelovské těleso. Nechť p je prvočíslo; položme

$$Y = \{\chi \in X;\, \chi(p) \neq 0\}, \qquad Z = \{\chi \in X;\, \chi(p) = 1\}.$$

Pak K_Y je největší mezitěleso rozšíření $K/\mathbb{Q}$, v němž se p-adický exponent nevětví a K_Z je největší mezitěleso rozšíření $K/\mathbb{Q}$, v němž se p-adický exponent zcela rozkládá. Označme I_p, resp. D_p inerční, resp. dekompoziční grupu odpovídající p-adickému exponentu. Pak platí

$$I_p \simeq X/Y, \qquad D_p \simeq X/Z, \qquad Y/Z \text{ je cyklická},$$

a tedy $|X/Y|$ je index větvení, $|Y/Z|$ je stupeň inercie a $|Z|$ počet prodloužení p-adického exponentu na K.

Důkaz. Označme ν nějaké prodloužení p-adického exponentu na K. Z cvičení 26(e,f) víme, že I_p odpovídá v Galoisově korespondenci nejmenšímu mezitělesu L rozšíření $K/\mathbb{Q}$ takovému, že exponent ν je totálně rozvětvený v K/L a platí, že $[K : L]$ je index větvení ν v $K/\mathbb{Q}$. Je tedy p-adický exponent nerozvětvený v $L/\mathbb{Q}$ (zde užíváme toho, že $\mathrm{Gal}(K/\mathbb{Q})$ je komutativní, a tedy všechna prodloužení p-adického exponentu mají v $L/\mathbb{Q}$ týž index větvení) a ze všech mezitěles rozšíření $K/\mathbb{Q}$ je L maximální s touto vlastností. Podle předchozího důsledku je K_Y největší mezitěleso rozšíření $K/\mathbb{Q}$ s touto vlastností, a proto platí $L = K_Y$.

Grupu X lze chápat jako $\widehat{\mathrm{Gal}(K/\mathbb{Q})}$ (viz poznámku na konci kapitoly 12), přitom Y odpovídá $\mathrm{Gal}(K/L)^\perp$. Podle lemmat 2 a 1 kapitoly 11 je

$$X/Y = \widehat{\mathrm{Gal}(K/\mathbb{Q})}/\,\mathrm{Gal}(K/L)^\perp \simeq \widehat{\mathrm{Gal}(K/L)} \simeq \mathrm{Gal}(K/L) = I_p,$$

a tedy $|X/Y|$ je index větvení p-adického exponentu v rozšíření $K/\mathbb{Q}$.

Označme n nejmenší společný násobek konduktorů charakterů z Y, je tedy $L \subseteq \mathbb{Q}_n$ a $p \nmid n$. Pro libovolné mezitěleso M rozšíření $L/\mathbb{Q}$ platí, že Artinovy automorfismy splňují $(p, M/\mathbb{Q}) = (p, \mathbb{Q}_n/\mathbb{Q})|_M$ (uvědomte si, že to zřejmě platí pro Frobeniovy automorfismy v rozšířeních těles zbytků). Označme U grupu Dirichletových charakterů odpovídající tělesu M: je tedy U podgrupa Y a platí $M = K_U$. Chápeme-li Dirichletův charakter $\chi \in U$ jako charakter na grupě $\mathrm{Gal}(M/\mathbb{Q})$ (dle poznámky na konci kapitoly 12), platí $\chi((p, M/\mathbb{Q})) = \chi((p, \mathbb{Q}_n/\mathbb{Q})) = \chi(p)$. Protože p-adický exponent se nevětví v $M/\mathbb{Q}$, je zde jeho inerční grupa triviální a dekompoziční grupa je generovaná příslušným Frobeniem=Artinem. Protože index dekompoziční grupy je počet různých prodloužení, je jasné, že se p-adický exponent v rozšíření $M/\mathbb{Q}$ zcela rozkládá, právě když Artinův automorfismus $(p, M/\mathbb{Q}) = \mathrm{id}_M$. Protože U je grupa charakterů grupy $\mathrm{Gal}(M/\mathbb{Q})$, nastane poslední podmínka, právě když $\chi(p) = 1$ pro každé $\chi \in U$. Ze všech podgrup U grupy X splňujících tuto podminku je zřejmě největší podgrupa Z, a tedy K_Z je největší mezitěleso rozšíření $K/\mathbb{Q}$, v němž se p-adický exponent zcela rozkládá. Označme $\sigma = (p, K_Y/\mathbb{Q})$. V grupě Y charakterů grupy $\mathrm{Gal}(K_Y/\mathbb{Q})$ je $Z = \langle\sigma\rangle^\perp$ a tedy podle lemmatu 2 kapitoly 11 je

$$Y/Z = \widehat{\mathrm{Gal}(K_Y/\mathbb{Q})}/\langle\sigma\rangle^\perp \simeq \widehat{\langle\sigma\rangle}$$

cyklická grupa, jejíž řád je stupeň inercie p-adického exponentu. Odtud plyne, že exponent tělesa K_Z indukovaný exponentem ν lze jediným způsobem prodloužit na těleso K; navíc je jistě těleso K_Z nejmenší s touto vlastností. Podle cvičení 24 v Galoisově korespondenci nejmenšímu mezitělesu L rozšíření $K/\mathbb{Q}$ takovému, že exponent tělesa L indukovaný exponentem ν lze jediným způsobem prodloužit na těleso K, odpovídá dekompoziční grupa D_p. Podobně jako pro inerční grupu proto máme

$$X/Z = \widehat{\mathrm{Gal}(K/\mathbb{Q})}/\,\mathrm{Gal}(K/K_Z)^\perp \simeq \widehat{\mathrm{Gal}(K/K_Z)} \simeq \mathrm{Gal}(K/K_Z) = D_p.$$

Věta je dokázána.

15. Riemannova funkce ζ

Definice. Riemannova funkce ζ je komplexní funkce komplexní proměnné s daná v polorovině $\mathrm{Re}\, s > 1$ řadou

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Poznámka. Užijeme-li zřejmou nerovnost platnou pro reálné $s > 1$

$$\sum_{n=2}^{\infty} \frac{1}{n^s} = \zeta(s) - 1 < \int_1^{\infty} x^{-s} dx = \frac{1}{s-1} < \zeta(s),$$

dostaneme

$$\tfrac{1}{s-1} < \zeta(s) < \tfrac{s}{s-1} \qquad \text{neboli} \qquad 1 < (s-1)\zeta(s) < s.$$

Protože pro komplexní s platí $|n^s| = n^{\mathrm{Re}\, s}$, řada v předchozí definici v polorovině $\mathrm{Re}\, s > 1$ konverguje absolutně a také stejnoměrně na každé kompaktní podmnožině této oblasti. Je tedy $\zeta(s)$ na této oblasti holomorfní (tj. analytická).

Lemma 1. (Dirichletovo kriterium) Nechť $\{c_n\}_{n=1}^{\infty}$ je nerostoucí posloupnost nezáporných reálných čísel taková, že $\lim_{n\to\infty} c_n = 0$. Nechť $\{a_n\}_{n=1}^{\infty}$ je posloupnost komplexních čísel taková, že posloupnost částečných součtů $s_n = \sum_{j=1}^{n} a_j$ je ohraničená. Pak řada $\sum_{n=1}^{\infty} c_n a_n$ konverguje.

Důkaz. Existuje tedy kladné reálné h tak, že $|s_n| < h$ pro všechna n. Pak

$$\sum_{j=1}^{n} (c_j - c_{j+1})|s_j| \le h(c_1 - c_{n+1}) < hc_1,$$

a tedy $\sum_{j=1}^{n}(c_j - c_{j+1})s_j$ konverguje absolutně. Označme $r_n = \sum_{j=1}^{n} c_j a_j$, $t_n = \sum_{j=1}^{n}(c_j - c_{j+1})s_j$. Platí $r_n = t_{n-1} + c_n s_n$, proto $\lim_{n\to\infty} r_n = \lim_{n\to\infty} t_n$.

Lemma 2. Funkci ζ lze analyticky prodloužit na polorovinu $\mathrm{Re}\, s > 0$ s jediným jednoduchým pólem v $s = 1$, kde má residuum 1.

Důkaz. Označme

$$\zeta_2(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}, \qquad \zeta_3(s) = \frac{1}{1^s} + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} + \dots$$

Pro $\operatorname{Re} s > 1$ platí

$$\zeta_2(s) = \big(1 - \tfrac{1}{2^{s-1}}\big)\zeta(s), \qquad \zeta_3(s) = \big(1 - \tfrac{1}{3^{s-1}}\big)\zeta(s).$$

Podle Dirichletova kriteria[1] konvergují sumy v definicích $\zeta_2(s)$ i $\zeta_3(s)$ lokálně stejnoměrně pro $\operatorname{Re} s > 0$, obě funkce jsou tedy v této oblasti holomorfní. Přitom $2^{s-1} = 1$, právě když $s = 1 + \frac{2\pi i n}{\ln 2}$ pro $n \in \mathbb{Z}$ a $3^{s-1} = 1$, právě když $s = 1 + \frac{2\pi i m}{\ln 3}$ pro $m \in \mathbb{Z}$, což může nastat současně jen pro $s = 1$. Z výše uvedené rovnosti plyne, že $\lim_{s\to 1}(s-1)\zeta(s)$ existuje a z poznámky před lemmatem 1 plyne $\lim_{s\to 1}(s-1)\zeta(s) = 1$.

Lemma 3. Pro $\operatorname{Re} s > 1$ absolutně konverguje nekonečný součin (v němž p probíhá všechna prvočísla)

$$\prod_p \Big(1 - \frac{1}{p^s}\Big)^{-1} = \zeta(s).$$

Důkaz. Protože $|\frac{1}{p^s}| < 1$, platí $\ln\big(1 - \frac{1}{p^s}\big)^{-1} = \sum_{m=1}^{\infty} \frac{1}{m p^{ms}}$. Nekonečný součin konverguje právě když konverguje $\sum_p \sum_{m=1}^{\infty} \frac{1}{m p^{ms}}$. Označme $t = \operatorname{Re} s$. Platí

$$\sum_p \sum_{m=1}^{\infty} \big|\tfrac{1}{m p^{ms}}\big| = \sum_p \sum_{m=1}^{\infty} \tfrac{1}{m p^{mt}} < \sum_p \sum_{m=1}^{\infty} \tfrac{1}{p^{mt}} = \sum_p \tfrac{1}{p^t - 1} < \sum_p \tfrac{2}{p^t} < \sum_{n=1}^{\infty} \tfrac{2}{n^t},$$

což konverguje, a tedy odhadovaná dvojná suma konverguje absolutně. Díky větě o jednoznačném rozkladu na prvočinitele v $\mathbb{N}$ pro libovolné přirozené číslo N platí

$$\Big|\prod_{p\le N} \big(1 - \tfrac{1}{p^s}\big)^{-1} - \zeta(s)\Big| \le \sum_n \frac{1}{n^t},$$

kde v poslední sumě n probíhá všechna přirozená čísla dělitelná aspoň jedním prvočíslem větším než N. Tato suma konverguje k 0 pro $N \to \infty$.

Poznámka. Všimněme si, že řada

$$\sum_p \sum_{m=2}^{\infty} \tfrac{1}{m p^{ms}}$$

pro $\operatorname{Re} s > \frac{1}{2}$ konverguje absolutně, neboť

$$\sum_p \sum_{m=2}^{\infty} \big|\tfrac{1}{m p^{ms}}\big| < \sum_p \sum_{m=2}^{\infty} \tfrac{1}{p^{mt}} = \sum_p \tfrac{1}{p^t(p^t-1)} < \sum_p \tfrac{2}{p^{2t}} < \sum_{n=1}^{\infty} \tfrac{2}{n^{2t}},$$

[1] Pro řadu $\zeta_2(s)$, kde $s = r + it$, $r, t \in \mathbb{R}$, $r > 0$, položte $c_n = n^{-\frac{r}{2}}$, $a_n = (-1)^n n^{-\frac{r}{2} - it}$ a pro libovolné $m \in \mathbb{N}$ odhadněte částečný součet takto: $|\sum_{n=2}^{m} a_n| - 1 \le |\sum_{k=0}^{[m/2]-1} a_{m-2k} - a_{m-2k-1}| = |\frac{s}{2} + it| \cdot |\sum_{k=0}^{[m/2]-1} \int_{m-2k-1}^{m-2k} x^{-1-\frac{s}{2}} (\cos(\frac{t}{2\pi}\ln x) + i\sin(\frac{t}{2\pi}\ln x))dx| < |\frac{s}{2} + it|\sqrt{2} \cdot \int_1^{\infty} x^{-1-\frac{s}{2}} dx = |\frac{s}{2} + it| 2\sqrt{2} s^{-1}$.

což pro $\operatorname{Re} s > \frac{1}{2}$ konverguje. Zavedeme-li označení $f(s) \sim g(s)$ pro dvě funkce, jejichž rozdíl je funkce holomorfní v $s = 1$, platí $\ln \zeta(s) \sim \sum_p \frac{1}{p^s}$. Ze dříve dokázaného plyne $\zeta(s) \sim \frac{1}{s-1}$ a $\ln \zeta(s) \sim \ln \frac{1}{s-1}$.

16. Dedekindova funkce ζ_K

Definice. Nechť K je těleso algebraických čísel, Dedekindova funkce ζ_K je komplexní funkce komplexní proměnné s daná v polorovině $\operatorname{Re} s > 1$ nekonečným součinem

$$\zeta_K(s) = \prod_{\wp} \Big(1 - \frac{1}{N(\wp)^s}\Big)^{-1},$$

kde $\wp$ probíhá v součinu všechny prvodivizory tělesa K a $N(a) = N_{K/\mathbb{Q}}(a)$ značí absolutní normu divizoru a.

Poznámka. Pro Riemannovu ζ funkci platí $\zeta = \zeta_{\mathbb{Q}}$. Označme $n = [K : \mathbb{Q}]$. Protože každý prvodivizor tělesa K dělí jediné prvočíslo a pro libovolné prvočíslo p existuje nejvýše n prvodivizorů tělesa K dělících p, přičemž jejich norma je mocnina p, platí v oblasti $\operatorname{Re} s > 1$

$$\sum_{\wp} \sum_{m=1}^{\infty} \Big|\tfrac{1}{mN(\wp)^{ms}}\Big| < n \sum_{p} \sum_{m=1}^{\infty} \tfrac{1}{mp^{m \operatorname{Re} s}} = n \ln \zeta(\operatorname{Re} s),$$

kde ve druhé dvojné sumě p probíhalo přes všechna prvočísla. Pak lze stejně jako v lemmatu 3 minulé kapitoly dokázat, že nekonečný součin v předchozí definici konverguje absolutně a že platí následující věta, která bývá často užívána pro definici Dedekindovy funkce ζ_K, zatímco rovnost, kterou jsme pro definici užili my, se nazývá Eulerova identita.

Věta 1. Pro Dedekindovu funkci ζ_K tělesa algebraických čísel K platí, že v polorovině $\operatorname{Re} s > 1$ je dána absolutně konvergentní řadou

$$\zeta_K(s) = \sum_{a} \frac{1}{N(a)^s},$$

kde a probíhá v sumě všechny divizory tělesa K.

Poznámka. Stejně jako v lemmatu 3 minulé kapitoly se ukáže, že platí

$$\ln \zeta_K(s) \sim \sum_{\wp} \frac{1}{N(\wp)^s},$$

kde $\wp$ probíhá v sumě přes všechny prvodivizory, které se v $K/\mathbb{Q}$ nevětví (větvících se je přece jen konečně mnoho) a mají stupeň inercie roven 1 (ty s větším stupněm inercie lze zahrnout do součtu, který je holomorfní pro $\operatorname{Re} s > \frac{1}{2}$).

Definice. Nechť K je těleso algebraických čísel. Nechť existuje právě s reálných vnoření $\sigma_1, \ldots, \sigma_s : K \to \mathbb{C}$ a právě t párů sdružených komplexních vnoření $\tau_1, \bar{\tau}_1, \ldots, \tau_t, \bar{\tau}_t : K \to \mathbb{C}$. Označme E grupu jednotek tělesa K (tj. grupu jednotek okruhu celých čísel tohoto tělesa). Z Dirichletovy věty o jednotkách (viz konec kapitoly 5) víme, že E je konečně generovaná grupa, jejíž rank je $r = s + t - 1$.

Zvolme pevně nějaké fundamentální jednotky $\varepsilon_1, \ldots, \varepsilon_r$ (tj. jednotky, které spolu s odmocninami z jedné ležícími v K generují E). Uvažme matici

$$\begin{pmatrix} \ln|\sigma_1(\varepsilon_1)| & \ldots & \ln|\sigma_s(\varepsilon_1)| & \ln|\tau_1(\varepsilon_1)^2| & \ldots & \ln|\tau_t(\varepsilon_1)^2| \\ \vdots & & \vdots & \vdots & & \vdots \\ \ln|\sigma_1(\varepsilon_r)| & \ldots & \ln|\sigma_s(\varepsilon_r)| & \ln|\tau_1(\varepsilon_r)^2| & \ldots & \ln|\tau_t(\varepsilon_r)^2| \end{pmatrix}$$

Pro libovolné $\alpha \in K$ platí

$$\sum_{j=1}^{s} \ln|\sigma_j(\alpha)| + \sum_{j=1}^{t} \ln|\tau_j(\alpha)^2| = \ln|N_{K/\mathbb{Q}}(\alpha)|$$

(viz větu 11 kapitoly 1), a tedy součet všech prvků libovolného řádku předchozí matice je roven nule. Proto absolutní hodnota determinantu je pro všechny její čtvercové podmatice řádu r stejná. Při přechodu k jiné soustavě fundamentálních jednotek je každá z matic rovna té druhé vynásobené zleva vhodnou čtvercovou maticí s celočíselnými prvky, proto zmíněná společná absolutní hodnota determinantů všech čtvercových podmatic řádu r nezávisí na konkrétní volbě fundamentálních jednotek. Tato hodnota se nazývá regulátor tělesa K.

Poznámka. Je možné dokázat (a v průběhu důkazu Dirichletovou věty o jednotkách je to zapotřebí), že regulátor tělesa algebraických čísel je nenulový.

Věta 2. (Analytický vzorec pro počet tříd divizorů) Nechť existuje právě s reálných vnoření a právě t párů sdružených komplexních vnoření tělesa algebraických čísel K do tělesa komplexních čísel. Označme R regulátor tělesa K, w počet odmocnin z jedné ležících v K a d diskriminant tělesa K (viz poznámku před lemmatem kapitoly 10). Pro Dedekindovu funkci ζ_K platí

$$\lim_{z \to 1_+} (z-1)\zeta_K(z) = \frac{2^{s+t}\pi^t R}{w\sqrt{|d|}} \cdot h,$$

kde h je počet tříd divizorů tělesa K.

Důkaz je v podstatě založen na Minkowského větě o konvexním tělese. Z časových důvodů mohu čtenáře pouze odkázat na knihu Borevič-Šafarevič, kapitola 5, §1. Zmiňme se jen o tom detailu důkazu, jak se v úpravách funkce ζ_K objeví h: řada z věty 1 se sčítá zvlášť přes jednotlivé třídy divizorů a ukáže se, že odpovídající limita je pro všechny třídy stejná a je rovna zlomku z tvrzení věty.

Poznámka. O Dedekindově funkci ζ_K lze dokázat mnohem více – lze ji analyticky prodloužit na celé $\mathbb{C}$ až na jednoduchý pól v 1, navíc splňuje následující funkcionální rovnici: při označení věty 2 položme

$$A = 2^{-t}\pi^{-t-\frac{s}{2}}\sqrt{|d|},$$
$$F(z) = A^z\,\Gamma\left(\tfrac{z}{2}\right)^s\,\Gamma(z)^t\,\zeta_K(z),$$

kde $\Gamma(z) = \int_0^\infty e^{-y}y^{z-1}dy$ pro $\operatorname{Re} z > 0$. Pak platí: existuje analytické prodloužení funkce $F(z)$ na celé $\mathbb{C}$ s výjimkou $z = 0$ a $z = 1$, kde má jednoduché póly, a

platí $F(z) = F(1-z)$ pro všechna $z \in \mathbb{C}$. (Zmínku o tomto tvrzení lze najít v knize Washingtona, poznámka za větou 4.5, jeho důkaz v knize S. Lang, Algebraic Number Theory, GTM 110, Springer-Verlag, 1986, kapitola XIII.)

17. Dedekindova funkce pro abelovská tělesa

Lemma. Nechť G je konečná abelovská grupa, $\widehat{G}$ její grupa charakterů s triviálním (tj. jednotkovým) charakterem χ_0. Pak pro libovolné $g \in G$ a libovolné $\psi \in \widehat{G}$ platí

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} |G| & \text{je-li } g = 1, \\ 0 & \text{jinak,} \end{cases} \qquad \sum_{h\in G} \psi(h) = \begin{cases} |G| & \text{je-li } \psi = \chi_0, \\ 0 & \text{jinak.} \end{cases}$$

Důkaz. Vzhledem k dualitě (důsledek za lemmatem 1 kapitoly 11) stačí ukázat jen první z identit. Je-li $g = 1$, plyne tvrzení ze zmíněného lemmatu. Nechť tedy $g \neq 1$. Dle důkazu zmíněného důsledku existuje charakter $\chi_1 \in \widehat{G}$ tak, že $\chi_1(g) \neq 1$. Platí

$$\sum_{\chi\in\widehat{G}} \chi(g) = \sum_{\chi\in\widehat{G}} (\chi_1\chi)(g) = \chi_1(g) \sum_{\chi\in\widehat{G}} \chi(g),$$

odkud plyne tvrzení.

Definice. Pro libovolný Dirichletův charakter χ definujeme L-funkci mocninnou řadou

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

(kde užíváme konvence $\chi(n) = 0$ pro n soudělné s konduktorem f_χ).

Poznámka. Pro triviální charakter χ_0 je tedy $L(s,\chi_0) = \zeta(s)$, pro netriviální charaktery suma na pravé straně konverguje lokálně stejnoměrně pro $\operatorname{Re} s > 0$ dle Dirichletova kriteria s přihlédnutím k předchozímu lemmatu, jde tedy v této polorovině o holomorfní funkci.

Věta 1. Nechť χ je libovolný Dirichletův charakter. Pro $\operatorname{Re} s > 1$ absolutně konverguje nekonečný součin (v němž p probíhá všechna prvočísla)

$$\prod_p \Big(1 - \frac{\chi(p)}{p^s}\Big)^{-1} = L(s,\chi).$$

Důkaz se provede stejně jako u lemmatu 3 kapitoly 14.

Věta 2. Nechť X je konečná grupa Dirichletových charakterů, $K = K_X$ jí odpovídající abelovské těleso. Pak platí

$$\zeta_K(s) = \prod_{\chi\in X} L(s,\chi).$$

Důkaz. Stačí porovnávat součiny odpovídající pevně zvolenému prvočíslu p, tj. ukázat, že platí

$$\prod_{\wp|p} \Big(1 - \frac{1}{N(\wp)^s}\Big)^{-1} = \prod_{\chi\in X} \Big(1 - \frac{\chi(p)}{p^s}\Big)^{-1}.$$

Předpokládejme, že divizor (p) se v pologrupě divizorů tělesa K rozkládá ve tvaru $(p) = \wp_1^e \dots \wp_g^e$ a že stupeň inercie prvodivizorů $\wp_1, \dots, \wp_g$ je f, tj. $N(\wp_1) = \dots = N(\wp_g) = p^f$. Pak levou stranu lze upravit do tvaru

$$\prod_{\wp|p} \Big(1 - \frac{1}{N(\wp)^s}\Big)^{-1} = (1 - p^{-fs})^{-g}.$$

Podle věty 3 kapitoly 14 obsahuje podgrupa $Y = \{\chi \in X;\, \chi(p) \neq 0\}$ právě fg charakterů a jádro homomorfismu $Y \to \mathbb{C}^\times$ určeného předpisem $\chi \mapsto \chi(p)$ má právě g prvků (tímto homomorfismem se grupa Y zobrazí na grupu f-tých odmocnin z jedné v $\mathbb{C}$). Proto platí

$$\prod_{\chi \in X} \Big(1 - \frac{\chi(p)}{p^s}\Big)^{-1} = (1 - p^{-fs})^{-g}.$$

Věta 3. Pro libovolný netriviální Dirichletův charakter χ platí $L(1, \chi) \neq 0$.

Důkaz. Nechť X je grupa generovaná charakterem χ, $n = |X|$ a $K = K_X$ těleso odpovídající X. Podle věty 2 platí

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi) = \zeta(s) \prod_{j=1}^{n-1} L(s, \chi^j).$$

Přitom $\zeta(s)$ má v $s = 1$ jednoduchý pól a pro $j = 1, \dots, n-1$ jsou funkce $L(s, \chi^j)$ v polorovině $\operatorname{Re} s > 0$ holomorfní. Kdyby $L(1, \chi) = 0$, byla by v $s = 1$ holomorfní i Dirichletova funkce $\zeta_K(s)$, což by bylo ve sporu s větou 2 minulé kapitoly.

Věta 4. (Dirichletova věta o aritmetické posloupnosti.) Nechť n je přirozené číslo, a celé číslo s n nesoudělné. Pak existuje nekonečně mnoho prvočísel kongruentních s a modulo n.

Důkaz. Pro libovolný Dirichletův charakter χ platí

$$\ln L(s, \chi) = -\sum_p \ln(1 - \chi(p)p^{-s}) = \sum_p \sum_{m=1}^{\infty} \frac{\chi(p)^m p^{-sm}}{m} \sim \sum_p \frac{\chi(p)}{p^s},$$

přičemž pro $\operatorname{Re} s > 1$ konvergují všechny uvedené sumy absolutně. Pro všechny Dirichletovy charaktery, jejichž konduktor je dělitelem n, vynásobíme předchozí vztah $\chi(a)^{-1}$ a sečteme:

$$\sum_\chi \chi(a)^{-1} \ln L(s, \chi) \sim \sum_\chi \chi(a)^{-1} \sum_p \frac{\chi(p)}{p^s} = \varphi(n) \sum_{p \equiv a \,(\mathrm{mod}\, n)} \frac{1}{p^s}$$

podle lemmatu. Na druhou stranu

$$\sum_\chi \chi(a)^{-1} \ln L(s, \chi) \sim \ln \zeta(s) \sim -\ln(s-1)$$

(viz konec kapitoly 15 a poznámku za definicí L-funkce). Odtud plyne věta.

Poznámka. Ačkoli předchozí věta je tvrzení z elementární teorie čísel, není znám žádný její elementární důkaz.

Definice. Nechť M množina je prvočísel. Pokud existuje limita

$$\lim_{s\to 1_+} \frac{\sum_{p\in M} p^{-s}}{-\ln(s-1)},$$

nazývá se tato limita Dirichletova hustota množiny M.

Poznámka. V předchozím důkaze jsme spočítali, že pro nesoudělná přirozená čísla a, n má množina prvočísel ve zbytkové třídě $a+n\mathbb{Z}$ hustotu $\frac{1}{\varphi(n)}$. Jsou tedy prvočísla do zbytkových tříd rozdělena „rovnoměrně“. Analogicky lze definovat Dirichletovu hustotu množiny prvodivizorů tělesa algebraických čísel jako limitu

$$\lim_{s\to 1_+} \frac{\sum_{\wp\in M} N(\wp)^{-s}}{-\ln(s-1)}.$$

Platí věta (pro jejíž důkaz by bylo nutné studovat charaktery na grupě tříd divizorů a zavést pro ně L-funkce) tvrdící, že hustota prvodivizorů v každé třídě divizorů pevně zvoleného tělesa algebraických čísel je stejná. Tento výsledek byl potřeba pro jednu implikaci ve cvičení 28.

18. Gaussovy sumy

Definice. Dirichletův charakter χ se nazývá lichý, resp. sudý, je-li $\chi(-1) = -1$, resp. $\chi(-1) = 1$.

Cvičení 32. Nechť X je konečná grupa Dirichletových charakterů, K_X jí odpovídající těleso. Dokažte, že

(a) je-li $K_X \subset \mathbb{R}$, pak X obsahuje pouze sudé charaktery;
(b) neplatí-li $K_X \subset \mathbb{R}$, pak X obsahuje polovinu sudých a polovinu lichých charakterů.

Definice. Nechť χ je Dirichletův charakter, f_χ jeho konduktor, $\zeta = e^{2\pi i/f_\chi}$. Pro libovolné $a \in \mathbb{Z}$ definujeme Gaussovu sumu $\tau_a(\chi)$ předpisem

$$\tau_a(\chi) = \sum_{t \bmod^\star f_\chi} \chi(t)\zeta^{at},$$

kde t probíhá nějakou redukovanou soustavu zbytků modulo f_χ (tj. z každé zbytkové třídy modulo f_χ, která obsahuje čísla nesoudělná s f_χ, je vybráno jedno číslo). Klademe $\tau(\chi) = \tau_1(\chi)$.

Lemma 1. Pro libovolný Dirichletův charakter χ o konduktoru $f = f_\chi$ a libovolné $a \in \mathbb{Z}$ platí: je-li a soudělné s f, pak $\tau_a(\chi) = 0$; je-li a nesoudělné s f, pak $\tau_a(\chi) = \chi(a)^{-1}\tau(\chi)$. Speciálně $\overline{\tau(\chi)} = \chi(-1)\tau(\bar\chi)$.

Důkaz. Je-li $d = (a, f) > 1$, pak existuje $n \in \mathbb{Z}$ tak, že $(n, f) = 1$, $n \equiv 1 \pmod{\frac{f}{d}}$ a $\chi(n) \neq 1$ (z definice konduktoru). Platí $\frac{an}{d} \equiv \frac{a}{d} \pmod{\frac{f}{d}}$, tedy $an \equiv a \pmod f$, odkud $\zeta^{an} = \zeta^a$, a proto

$$\tau_a(\chi) = \sum_{t \bmod^\star f_\chi} \chi(t)\zeta^{at} = \sum_{t \bmod^\star f_\chi} \chi(tn)\zeta^{atn} = \chi(n) \sum_{t \bmod^\star f_\chi} \chi(t)\zeta^{at} = \chi(n)\tau_a(\chi),$$

odkud $\tau_a(\chi) = 0$. Nechť $(a, f) = 1$, pak platí

$$\chi(a)\tau_a(\chi) = \sum_{t \bmod^\star f_\chi} \chi(at)\zeta^{at} = \tau(\chi).$$

Poslední tvrzení dostaneme pro $a = -1$, neboť $\overline{\tau(\chi)} = \tau_{-1}(\bar\chi)$.

Lemma 2. Pro libovolný Dirichletův charakter χ s konduktorem $f = f_\chi$ platí $|\tau(\chi)| = \sqrt{f}$.

Důkaz. Dle lemmatu 1 platí

$$\begin{aligned}\varphi(f)|\tau(\chi)|^2 &= \sum_{b=1}^{f} |\tau_b(\chi)|^2 = \sum_{b=1}^{f} \sum_{a \bmod^\star f_\chi} \chi(a)\zeta^{ab} \sum_{c \bmod^\star f_\chi} \bar\chi(c)\zeta^{-bc} \\ &= \sum_{a \bmod^\star f_\chi} \sum_{c \bmod^\star f_\chi} \chi(a)\bar\chi(c) \sum_{b=1}^{f} \zeta^{b(a-c)} \\ &= f \sum_{a \bmod^\star f_\chi} \chi(a)\bar\chi(a) = f\varphi(f).\end{aligned}$$

Věta 1. Pro libovolný netriviální Dirichletův charakter χ o konduktoru $f = f_\chi$ platí

$$L(1, \chi) = \frac{\pi i \tau(\chi)}{f^2} \sum_{a=1}^{f} \bar\chi(a)a,$$

je-li χ lichý, a

$$L(1, \chi) = -\frac{\tau(\chi)}{f} \sum_{a=1}^{f-1} \bar\chi(a) \ln|1 - \zeta^a|,$$

je-li χ sudý, kde $\zeta = e^{2\pi i/f}$.

Důkaz. Platí

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{\substack{n \in \mathbb{N} \\ (n,f)=1}} \frac{\tau_n(\bar\chi)}{n\tau(\bar\chi)}$$

podle lemmatu 1. Z definice $\tau_n(\chi)$

$$L(1, \chi) = \frac{1}{\tau(\bar\chi)} \sum_{a \bmod^\star f} \bar\chi(a) \sum_{n=1}^{\infty} \frac{\zeta^{an}}{n}.$$

Řada $\sum_{n=1}^{\infty} \frac{z^n}{n}$ konverguje v kruhu $|z| < 1$ k té větvi logaritmu $-\ln(1 - z)$, jejíž imaginární část leží v intervalu $(-\frac{\pi}{2}, \frac{\pi}{2})$. Podle Abelovy věty o konvergenci na hranici kruhu platí

$$\sum_{n=1}^{\infty} \frac{\zeta^{an}}{n} = -\ln(1 - \zeta^a).$$

Je tedy

$$L(1,\chi) = -\tfrac{1}{\tau(\bar\chi)} \sum_{a \bmod^\star f} \bar\chi(a) \ln(1-\zeta^a).$$

Předpokládejme nejdříve, že χ je sudý. Pak pro libovolné a platí $\chi(-a) = \chi(a)$ a $\ln(1-\zeta^a)+\ln(1-\zeta^{-a}) = 2\ln|1-\zeta^a|$. Podle lemmat 1 a 2 dostáváme $\tau(\bar\chi) = \overline{\tau(\chi)} = \frac{f}{\tau(\chi)}$, odkud plyne výsledek.

Předpokládejme nyní, že χ je lichý. Pak pro libovolné a platí $\chi(-a) = -\chi(a)$. Je-li navíc $0 < a < f$, pak

$$1-\zeta^a = e^{a\pi i/f}(e^{-a\pi i/f} - e^{a\pi i/f}) = -2i \sin\tfrac{a\pi}{f}(\cos\tfrac{a\pi i}{f} + i \sin\tfrac{a\pi i}{f})$$

a tedy

$$\ln(1-\zeta^a) = \ln(2\sin\tfrac{a\pi}{f}) + i\pi(\tfrac{a}{f} - \tfrac{1}{2}).$$

Odtud plyne

$$L(1,\chi) = -i\pi \tfrac{1}{\tau(\bar\chi)} \sum_{a \bmod^\star f} \bar\chi(a)(\tfrac{a}{f} - \tfrac{1}{2}).$$

Podle lemmat 1 a 2 dostáváme $\tau(\bar\chi) = -\overline{\tau(\chi)} = -\frac{f}{\tau(\chi)}$, odkud plyne výsledek, přihlédneme-li k $\sum_{a \bmod^\star f} \bar\chi(a) = 0$ (viz lemma kapitoly 17).

Poznámka. Předchozí věta nám umožňuje spočítat limitu z věty 2 kapitoly 16 (tj. reziduum Dedekindovy ζ-funkce v 1) pro abelovská tělesa. Je-li X konečná grupa Dirichletových charakterů a $K = K_X$ jí odpovídající abelovské těleso, pak platí dle věty 2 kapitoly 17 a lemmatu 2 kapitoly 15

$$\lim_{z\to 1_+} (z-1)\zeta_K(z) = \prod_{\chi \in X\setminus\{\chi_0\}} L(1,\chi),$$

kde χ_0 značí triviální charakter.

Vzorec z věty 2 kapitoly 16 lze pro abelovská tělesa ještě dále upravit, uveďme si bez důkazu některé další výsledky:

Je-li X konečná grupa Dirichletových charakterů a $K = K_\chi$ jí odpovídající abelovské těleso, pak

$$\prod_{\chi\in X} \tau(\chi) = \begin{cases} \sqrt{|d|} & \text{je-li } K_X \subset \mathbb{R} \\ i^{|X|/2}\sqrt{|d|} & \text{jinak.} \end{cases}$$

Odtud plyne snadný vzorec pro výpočet diskriminantu abelovského tělesa: $|d| = \prod_{\chi\in X} f_\chi$.

Je-li $K = K_X$ reálné (tj. všechny $\chi \in X$ jsou sudé), platí

$$Rh = \prod_{\chi\in X\setminus\{\chi_0\}} \frac{1}{2}\tau(\bar\chi)L(1,\chi) = \prod_{\chi\in X\setminus\{\chi_0\}} \big(-\frac{1}{2}\sum_{a=1}^{f_\chi-1} \bar\chi(a)\ln|1-\zeta_{f_\chi}^a|\big),$$

a tedy jediný problém při vyčíslení h je výpočet regulátoru R.

Není-li $K = K_X$ reálné a je-li Y podgrupa sudých charakterů grupy X, pak pro počet tříd divizorů h^+ maximálního reálného podtělesa $K^+ = K_Y$ tělesa K platí $h^+|h$. Vydělením vzorce z věty 2 kapitoly 16 pro K a K^+ dostaneme

$$h^- = \frac{h}{h^+} = Qw \prod_{\chi \in X \setminus Y} \Big(-\frac{1}{2f_\chi} \sum_{a=1}^{f_\chi} \bar{\chi}(a)a\Big),$$

kde w je počet odmocnin z jedné ležících v K a Q je tzv. Hasseův index jednotek (jde o index podgrupy generované všemi jednotkami v K^+ a všemi odmocninami z jedné v K v grupě všech jednotek tělesa K, platí $Q = 1$ nebo $Q = 2$). Tento index se objeví ve vzorci podílem regulátoru R tělesa K a regulátoru R^+ tělesa K^+:

$$\frac{R}{R^+} = \frac{2^{|X|/2}}{2Q}.$$

19. Kruhové jednotky

Lemma 1. Nechť G je konečná komutativní grupa, $f : G \to \mathbb{C}$ zobrazení. Pak platí

$$\det\big(f(gh^{-1})\big)_{g,h\in G} = \prod_{\chi\in\widehat{G}} \sum_{g\in G} f(g)\chi(g)$$
$$\det\big(f(gh^{-1}) - f(g)\big)_{g,h\in G\setminus\{1\}} = \prod_{\chi\in\widehat{G}\setminus\{\chi_0\}} \sum_{g\in G} f(g)\chi(g),$$

kde v determinantech jsou řádky i sloupce uspořádány stejným lineárním uspořádáním na G a χ_0 značí triviální charakter na G.

Důkaz. Označme $M = (\chi(g))_{\chi\in\widehat{G},g\in G}$. Protože $M \cdot M^T$ dle lemmatu kapitoly 17 je $|G|$-násobek permutační matice, platí $|\det M| = |G|^{|G|/2}$. Označme $A = (f(gh^{-1}))_{g,h\in G}$. Pro $B = (b_{\chi,h})_{\chi\in\widehat{G},h\in G} = M \cdot A$ platí

$$b_{\chi,h} = \sum_{g\in G} f(gh^{-1})\chi(g) = \sum_{g\in G} f(g)\chi(gh) = \chi(h) \sum_{g\in G} f(g)\chi(g),$$

a tedy

$$\det M \cdot \det A = \det M \cdot \prod_{\chi\in\widehat{G}} \sum_{g\in G} f(g)\chi(g),$$

odkud plyne první identita. Nyní dokažme druhou. Bez újmy na obecnosti můžeme předpokládat, že $\sum_{g\in G} f(g) \neq 0$. V opačném případě totiž můžeme zobrazení f pozměnit přičtením nějaké konstanty, což evidentně nezmění hodnotu determinantu a podle lemmatu kapitoly 17 ani pravou stranu identity. Pak můžeme druhou identitu odvodit z první takto: přičtěme všechny řádky determinantu k řádku s indexem 1, vytkněme $\sum_{g\in G} f(g)$ z tohoto řádku (zůstanou tam jedničky), odečtěme sloupec s indexem 1 od všech ostatních sloupců a rozviňme determinant podle řádku s indexem 1.

Cvičení 33. Nechť $k \subseteq L \subseteq K$ jsou tělesa algebraických čísel, $\alpha \in K$. Pak pro normy platí

$$N_{K/k}(\alpha) = N_{L/k}(N_{K/L}(\alpha)).$$

(Návod: předpokládejte nejprve, že K/k je Galoisovo rozšíření.)

Definice. Nechť K je abelovské těleso, E jeho grupa jednotek. Pro libovolné přirozené číslo n označme $\zeta_n = e^{2\pi i/n}$, n-té kruhové těleso $\mathbb{Q}_n = \mathbb{Q}(\zeta_n)$ a $K_n = K \cap \mathbb{Q}_n$. Pro libovolné celé číslo a nedělitelné n je $1 - \zeta_n^a$ nenulové číslo v $\mathbb{Q}_n$ a tedy $N_{\mathbb{Q}_n/K_n}(1 - \zeta_n^a) \in K_n^\times \subseteq K^\times$. Označme D podgrupu multiplikativní grupy $K^\times$ generovanou

$$\{-1\} \cup \{N_{\mathbb{Q}_n/K_n}(1 - \zeta_n^a);\ n \in \mathbb{N},\ a \in \mathbb{Z},\ n \nmid a\}.$$

Průnik $C = E \cap D$ se nazývá grupa kruhových jednotek tělesa K.

Poznámky. 1. Libovolná odmocnina z jedné, která leží v K, je kruhová jednotka tělesa K. Skutečně, je-li $\zeta_d \in K$, pak $K_d = \mathbb{Q}_d$ a $\frac{1-\zeta_d}{1-\zeta_d^{-1}} = -\zeta_d \in C$.

2. Je-li $d = (a, n) > 1$, pak pro $a' = \frac{a}{d}$, $n' = \frac{n}{d}$, platí $1 - \zeta_n^a = 1 - \zeta_{n'}^{a'}$, a tedy podle cvičení 33 a poznámky za větou 2 kapitoly 13

$$\begin{aligned} N_{\mathbb{Q}_n/K_n}(1 - \zeta_n^a) &= N_{\mathbb{Q}_n/K_n}(1 - \zeta_{n'}^{a'}) = N_{\mathbb{Q}_{n'}K_n/K_n}(N_{\mathbb{Q}_n/\mathbb{Q}_{n'}K_n}(1 - \zeta_{n'}^{a'})) \\ &= N_{\mathbb{Q}_{n'}K_n/K_n}(1 - \zeta_{n'}^{a'})^{[\mathbb{Q}_n:\mathbb{Q}_{n'}K_n]} = N_{\mathbb{Q}_{n'}/K_{n'}}(1 - \zeta_{n'}^{a'})^{[\mathbb{Q}_n:\mathbb{Q}_{n'}K_n]}. \end{aligned}$$

V předchozí definici tedy stačí vzít pouze čísla a nesoudělná s n.

Lemma 2. Nechť přirozené číslo n není mocninou prvočísla. Pak pro libovolné celé číslo a nesoudělné s n je $1 - \zeta_n^a$ jednotka tělesa $\mathbb{Q}_n$.

Důkaz. Připomeňme, že pro m-tý kruhový polynom

$$\Phi_m(x) = \prod_{\substack{j=1,\dots,m \\ (j,m)=1}} (x - \zeta_m^j)$$

platí identita $x^n - 1 = \prod_{d|n} \Phi_d(x)$, a tedy

$$x^{n-1} + x^{n-2} + \cdots + x + 1 = \prod_{1 \neq d|n} \Phi_d(x),$$

odkud dosazením $x = 1$ dostáváme

$$n = \prod_{1 \neq d|n} \Phi_d(1).$$

Pro libovolné prvočíslo p platí $\Phi_{p^r}(1) = p$ (viz důkaz věty 1 kapitoly 14) a tedy $\Phi_n(1) = \pm 1$ (indukcí bychom snadno dostali $\Phi_n(1) = 1$). Ovšem

$$\Phi_n(1) = \prod_{\substack{j=1,\dots,n \\ (j,n)=1}} (1 - \zeta_n^j).$$

Poznámka. Jestliže přirozené číslo n je mocninou prvočísla, pak čísla tvaru $1-\zeta_n^a$, kde celé číslo a je nesoudělné s n, nejsou jednotky tělesa $\mathbb{Q}_n$. Podíl libovolných dvou těchto čísel však jednotkou tělesa $\mathbb{Q}_n$ je. Plyne to z věty 1 kapitoly 14.

Věta 1. Nechť $n > 1$ je přirozené číslo, p prvočíslo, a celé číslo nesoudělné s pn. Pak platí

$$N_{\mathbb{Q}_{pn}/\mathbb{Q}_n}(1-\zeta_{pn}^a) = \begin{cases} 1-\zeta_n^a & \text{jestliže } p|n, \\ \frac{1-\zeta_n^a}{1-\zeta_n^{ap'}} & \text{jestliže } p \nmid n, \end{cases}$$

kde celé číslo p' splňuje $pp' \equiv 1 \pmod n$.

Důkaz. Platí $\mathrm{Gal}(\mathbb{Q}_{pn}/\mathbb{Q}_n) = \{\sigma_t;\ t \in \mathbb{Z},\ (t,pn) = 1,\ t \equiv 1 \pmod n\}$, kde $\sigma_t \in \mathrm{Gal}(\mathbb{Q}_{pn}/\mathbb{Q})$ je určeno podmínkou $\sigma_t(\zeta_{pn}) = \zeta_{pn}^t$. Proto platí

$$N_{\mathbb{Q}_{pn}/\mathbb{Q}_n}(1-\zeta_{pn}^a) = \prod_{\substack{t \bmod^\star pn \\ t \equiv 1 \pmod n}} (1-\zeta_{pn}^{at}).$$

Předpokládejme nejdříve, že $p|n$. Pak t je nesoudělné s pn, právě když je nesoudělné s n, a tedy

$$N_{\mathbb{Q}_{pn}/\mathbb{Q}_n}(1-\zeta_{pn}^a) = \prod_{\substack{0 \le t < pn \\ t \equiv 1 \pmod n}} \left(\zeta_{pn}^a(\zeta_{pn}^{-a} - \zeta_{pn}^{a(t-1)})\right) = \prod_{r=0}^{p-1} \left(\zeta_{pn}^a(\zeta_{pn}^{-a} - \zeta_{pn}^{arn})\right)$$
$$= \zeta_n^a \prod_{r=0}^{p-1} (\zeta_{pn}^{-a} - \zeta_p^{ar}) = \zeta_n^a(\zeta_n^{-a} - 1) = 1 - \zeta_n^a.$$

Nyní se zabývejme případem, kdy $p \nmid n$. Jediný rozdíl oproti předchozí situaci je v tom, že pro $r = 0, 1, \ldots, p-1$ nemusí být $1+nr$ nesoudělné s pn. Určitě je toto číslo nesoudělné s n, pro některé r však může být dělitelné p, a to právě pro to jediné r, pro které $1 + nr \equiv 0 \pmod p$, tj. $1 + nr \equiv pp' \pmod{pn}$. Je tedy

$$\begin{aligned} & N_{\mathbb{Q}_{pn}/\mathbb{Q}_n}(1-\zeta_{pn}^a) \\ &= \prod_{\substack{t \bmod^\star pn \\ t \equiv 1 \pmod n}} \left(\zeta_{pn}^a(\zeta_{pn}^{-a} - \zeta_{pn}^{a(t-1)})\right) \\ &= (1-\zeta_{pn}^{app'})^{-1} \prod_{r=0}^{p-1} \left(\zeta_{pn}^a(\zeta_{pn}^{-a} - \zeta_{pn}^{arn})\right) \\ &= (1-\zeta_n^{ap'})^{-1}\zeta_n^a \prod_{r=0}^{p-1} (\zeta_{pn}^{-a} - \zeta_p^{ar}) \\ &= (1-\zeta_n^{ap'})^{-1}\zeta_n^a(\zeta_n^{-a} - 1) = (1-\zeta_n^a)(1-\zeta_n^{ap'})^{-1}. \end{aligned}$$

Důsledek. V definici kruhových jednotek stačí brát jen ta n, která jsou děliteli konduktoru f tělesa K, přesněji: D je generováno množinou

$$\{-1\} \cup \{N_{\mathbb{Q}_n/K_n}(1-\zeta_n^a);\ 1 < n|f,\ (n, \tfrac{f}{n}) = 1,\ a \in \mathbb{Z},\ (a,n) = 1\} \cup \mathbb{Q}^\times.$$

Důkaz. Pro libovolné $n \in \mathbb{N}$ označme $d = (n, f)$. Pak $K_n = K \cap \mathbb{Q}_n = (K \cap \mathbb{Q}_f) \cap \mathbb{Q}_n = K \cap \mathbb{Q}_d = K_d$ podle věty 1 kapitoly 12. Pak podle cvičení 33 pro libovolné celé číslo a nesoudělné s n platí

$$N_{\mathbb{Q}_n/K_n}(1-\zeta_n^a) = N_{\mathbb{Q}_d/K_d}(N_{\mathbb{Q}_n/\mathbb{Q}_d}(1-\zeta_n^a)).$$

Je-li $d > 1$, tvrzení plyne indukcí z věty 1. Je-li naopak $d = 1$, pak $N_{\mathbb{Q}_n/K_n}(1-\zeta_n^a) = N_{\mathbb{Q}_n/\mathbb{Q}}(1-\zeta_n^a) = \Phi_n(1)$. Pro libovolné $m|f$, $m > 1$, označme n největšího dělitele čísla f dělitelného pouze prvočísly dělícími m. Z věty 1 plyne $N_{\mathbb{Q}_n/\mathbb{Q}_m}(1-\zeta_n^a) = 1-\zeta_m^a$ pro libovolné $a \in \mathbb{Z}$ nesoudělné s f a tedy generátory tvaru $1-\zeta_m^a$ takové, že $(m, \frac{f}{m}) > 1$, lze vypustit.

Věta 2. Nechť K je abelovské těleso, f jeho konduktor. Grupa kruhových jednotek tělesa K je generována následující konečnou množinou generátorů:

$$\{-1\} \cup \{\varepsilon_{n,a};\ 1 < n|f,\ (n, \tfrac{f}{n}) = 1,\ a \in \mathbb{Z},\ (a,n) = 1\},$$

kde

$$\varepsilon_{n,a} = \begin{cases} N_{\mathbb{Q}_n/K_n}(1-\zeta_n^a) & \text{pokud } n \text{ není mocninou prvočísla,} \\ N_{\mathbb{Q}_n/K_n}\big((1-\zeta_n^a)(1-\zeta_n)^{-1}\big) & \text{pokud } n \text{ je mocninou prvočísla.} \end{cases}$$

Důkaz. Má-li být nějaký součin mocnin generátorů D z předchozího důsledku jednotkou tělesa K, musí být norma tohoto součinu vzhledem k $K/\mathbb{Q}$ jednotkou $\mathbb{Q}$, tj. ± 1. V tom případě to je součin mocnin generátorů zmíněných ve větě. Naopak každé $\varepsilon_{n,a}$ je jednotka tělesa K.

Lemma 3. Nechť χ je Dirichletův charakter s konduktorem f_χ, nechť $m, f \in \mathbb{N}$ jsou taková, že $m|f$ a $f_\chi|f$. Pak platí

$$\sum_{a \bmod^\star f} \chi(a) \ln|1-\zeta_m^a| = \begin{cases} \frac{\varphi(f)}{\varphi(m)} \sum_{b \bmod^\star m} \chi(b) \ln|1-\zeta_m^b| & \text{pokud } f_\chi|m, \\ 0 & \text{pokud } f_\chi \nmid m. \end{cases}$$

Důkaz. Předpokládejme nejdříve, že $f_\chi|m$. Pak v sumě sčítanec odpovídající a je určen pouze zbytkovou třídou modulo m, v níž a leží. Kanonický homomorfismus $(\mathbb{Z}/f\mathbb{Z})^\star \to (\mathbb{Z}/m\mathbb{Z})^\star$ je surjektivní, proto na libovolnou třídu $b + m\mathbb{Z}$ se zobrazí právě $\frac{\varphi(f)}{\varphi(m)}$ tříd $a + f\mathbb{Z}$.

Předpokládejme nyní, že $f_\chi \nmid m$. Uvažme diagram

$$\begin{array}{ccccc} (\mathbb{Z}/f\mathbb{Z})^\star & \longrightarrow & (\mathbb{Z}/f_\chi\mathbb{Z})^\star & \xrightarrow{\chi} & \mathbb{C}^\times \\ \downarrow & & & & \\ (\mathbb{Z}/m\mathbb{Z})^\star & & & & \end{array}$$

Existuje celé číslo $c \equiv 1 \pmod m$ nesoudělné s f takové, že $\chi(c) \neq 1$. V opačném případě by totiž $f_\chi|m$. Odtud plyne

$$\chi(c) \sum_{a \bmod^\star f} \chi(a) \ln|1-\zeta_m^a| = \sum_{a \bmod^\star f} \chi(ac) \ln|1-\zeta_m^{ac}| = \sum_{a \bmod^\star f} \chi(a) \ln|1-\zeta_m^a|.$$

Lemma 4. Nechť χ je netriviální Dirichletův charakter s konduktorem f_χ, nechť m je přirozené číslo takové, že $f_\chi | m$. Označme m', resp. f'_χ, součin všech prvočísel dělících m, resp. f_χ. Jestliže prvočíslo p a přirozené číslo d splňují $f'_\chi | d$ a $pd | m'$, pak platí

$$\sum_{\substack{b=1,\dots,m\\(b,pd)=1}} \chi(b) \ln|1-\zeta_m^b| = (1-\chi(p)) \sum_{\substack{b=1,\dots,m\\(b,d)=1}} \chi(b) \ln|1-\zeta_m^b|.$$

Důkaz. Platí

$$\sum_{\substack{b=1,\dots,m\\(b,d)=1}} \chi(b) \ln|1-\zeta_m^b| - \sum_{\substack{b=1,\dots,m\\(b,pd)=1}} \chi(b) \ln|1-\zeta_m^b| = \sum_{\substack{b=1,\dots,m\\(b,d)=1\\p|b}} \chi(b) \ln|1-\zeta_m^b|$$

$$= \sum_{\substack{c=1,\dots,\frac{m}{p}\\(c,d)=1}} \chi(cp) \ln|1-\zeta_m^{cp}| = \chi(p) \sum_{\substack{c=1,\dots,\frac{m}{p}\\(c,d)=1}} \chi(c) \ln \prod_{i=1}^{p} |1-\zeta_m^c \zeta_p^i|$$

$$= \chi(p) \sum_{\substack{c=1,\dots,\frac{m}{p}\\(c,d)=1}} \sum_{i=1}^{p} \chi(c+i\tfrac{m}{p}) \ln|1-\zeta_m^{c+i\frac{m}{p}}| = \chi(p) \sum_{\substack{b=1,\dots,m\\(b,d)=1}} \chi(b) \ln|1-\zeta_m^b|,$$

odkud plyne lemma.

Důsledek. Nechť χ je netriviální Dirichletův charakter s konduktorem f_χ, nechť m je přirozené číslo takové, že $f_\chi | m$. Pak platí

$$\sum_{b \bmod^\star m} \chi(b) \ln|1-\zeta_m^b| = \Big(\prod_{p|m}(1-\chi(p))\Big) \sum_{\substack{b=1,\dots,m\\(b,f_\chi)=1}} \chi(b) \ln|1-\zeta_m^b|,$$

kde v součinu probíhá p všechna prvočísla dělící m.

Důkaz. Indukcí dostaneme z lemmatu 4 uvedený vzorec, v němž však v součinu bude p probíhat prvočísla $p|m$, $p \nmid f_\chi$. Avšak pro $p|f_\chi$ je příslušný činitel roven 1.

Lemma 5. Nechť χ je netriviální sudý Dirichletův charakter s konduktorem f_χ, nechť m je přirozené číslo takové, že $f_\chi | m$. Pak platí

$$\sum_{\substack{b=1,\dots,m\\(b,f_\chi)=1}} \chi(b) \ln|1-\zeta_m^b| = -\tau(\chi) L(1,\bar\chi),$$

kde $\tau(\chi)$ značí Gaussovu sumu a $L(1,\chi)$ je hodnota příslušné L-funkce.

Důkaz. Platí

$$\sum_{\substack{b=1,\dots,m\\(b,f_\chi)=1}} \chi(b) \ln|1-\zeta_m^b| = \sum_{a \bmod^\star f_\chi} \chi(a) \sum_{c=1}^{m/f_\chi} \ln|1-\zeta_m^{a+cf_\chi}|$$

$$= \sum_{a \bmod^\star f_\chi} \chi(a) \ln\Big|\prod_{c=1}^{m/f_\chi} (1-\zeta_m^a \zeta_{m/f_\chi}^c)\Big|$$

$$= \sum_{a \bmod^\star f_\chi} \chi(a) \ln|1-\zeta_{f_\chi}^a| = -\frac{f_\chi}{\tau(\bar\chi)} L(1,\bar\chi)$$

podle věty 1 kapitoly 18. Lemma plyne z lemmat 1 a 2 kapitoly 18.

Věta 3. (Ramachandra) Nechť K je reálné abelovské těleso. Rozložme konduktor f tělesa K na prvočinitele: $f = \prod_{i=1}^{s} p_i^{e_i}$, kde $p_1, \dots, p_s$ jsou různá prvočísla, $e_1, \dots, e_s \in \mathbb{N}$. Pro libovolné $I \subseteq \{1, \dots, s\}$ položme $m_I = \prod_{i \in I} p_i^{e_i}$. Označme

$$\vartheta = N_{\mathbb{Q}_f/K}\Big(\prod_{\emptyset \neq I \subseteq \{1,\dots,s\}} (1 - \zeta_{m_I})\Big), \qquad \varepsilon_\sigma = \frac{\sigma^{-1}(\vartheta)}{\vartheta}$$

pro každé $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Pak platí $\varepsilon_\sigma \in C$ a označíme-li C' grupu generovanou v E všemi jednotkami ε_σ, kde $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{\mathrm{id}_K\}$, spolu se všemi odmocninami z jedné ležícími v K, pak má C' v E konečný index

$$|E/C'| = 2^{|X|-1} h \cdot \prod_{i=1}^{s} \prod_{\substack{\chi \in X \setminus \{\chi_0\} \\ p_i \nmid f_\chi}} (\varphi(p_i^{e_i}) + 1 - \chi(p_i)),$$

kde X značí grupu Dirichletových charakterů odpovídající K (tj. $K = K_X$), χ_0 je triviální charakter, f_χ je konduktor charakteru χ a φ je Eulerova funkce.

Důkaz. To, že $\varepsilon_\sigma \in C$, plyne z věty 2. Označme W grupu všech odmocnin z jedné, které leží v K. Pak $W \subseteq C$ (viz poznámku 1 za definicí kruhových jednotek) a platí, že E/W a C'/W jsou konečně generované komutativní grupy bez torze. Zřejmě platí $E/C' \simeq (E/W)/(C'/W)$. Tento index spočteme pomocí důsledku 1 věty 4 kapitoly 5. Označme $r = [K : \mathbb{Q}] - 1$ a zvolme fundamentální jednotky (tj. generátory E/W, viz definici regulátoru v kapitole 16) $\eta_1, \dots, \eta_r$. Pak existují celá čísla $a_{j,\sigma}$ a $\rho_\sigma \in W$ tak, že pro každé $\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \setminus \{\mathrm{id}_K\}$ platí

$$\varepsilon_\sigma = \rho_\sigma \prod_{j=1}^{r} \eta_j^{a_{j,\sigma}},$$

odkud plyne pro libovolné $\tau \in \mathrm{Gal}(K/\mathbb{Q})$

$$\ln|\tau(\varepsilon_\sigma)| = \sum_{j=1}^{r} a_{j,\sigma} \ln|\tau(\eta_j)|,$$

maticově

$$(\ln|\tau(\varepsilon_\sigma)|)_{\sigma,\tau \in \mathrm{Gal}(K/\mathbb{Q})\setminus\{\mathrm{id}_K\}} = (a_{j,\sigma})_{\substack{\sigma \in \mathrm{Gal}(K/\mathbb{Q})\setminus\{\mathrm{id}_K\} \\ j=1,\dots,r}} \cdot (\ln|\tau(\eta_j)|)_{\substack{j=1,\dots,r \\ \tau \in \mathrm{Gal}(K/\mathbb{Q})\setminus\{\mathrm{id}_K\}}}.$$

Ovšem podle důsledku 1 věty 4 kapitoly 5 platí $|\det(a_{j,\sigma})_{\sigma,j}| = |E/C'|$ a podle definice regulátoru $R = |\det(\ln|\tau(\eta_j)|)_{j,\tau}|$, tedy

$$\det(\ln|\tau(\varepsilon_\sigma)|)_{\sigma,\tau \in \mathrm{Gal}(K/\mathbb{Q})\setminus\{\mathrm{id}_K\}} = |E/C'| \cdot R.$$

Na druhou stranu

$$\begin{aligned}\det(\ln|\tau(\varepsilon_\sigma)|)_{\sigma,\tau \in \mathrm{Gal}(K/\mathbb{Q})\setminus\{\mathrm{id}_K\}} &= \det(\ln|\tau\sigma^{-1}(\vartheta)| - \ln|\tau(\vartheta)|)_{\sigma,\tau \in \mathrm{Gal}(K/\mathbb{Q})\setminus\{\mathrm{id}_K\}} \\ &= \prod_{\chi \in X \setminus \{\chi_0\}} \sum_{\tau \in \mathrm{Gal}(K/\mathbb{Q})} \chi(\tau) \ln|\tau(\vartheta)|\end{aligned}$$

podle lemmatu 1, v němž klademe $f(\tau) = \ln|\tau(\vartheta)|$, neboť X je možné identifikovat s grupou charakterů na $\mathrm{Gal}(K/\mathbb{Q})$ (viz konec kapitoly 12). Ovšem

$$\begin{aligned}\sum_{\tau\in\mathrm{Gal}(K/\mathbb{Q})}\chi(\tau)\ln|\tau(\vartheta)| &= \sum_{\tau\in\mathrm{Gal}(K/\mathbb{Q})}\chi(\tau)\sum_{\sigma\in\mathrm{Gal}(\mathbb{Q}_f/K)}\ln\Big|\prod_{\emptyset\neq I\subseteq\{1,\dots,s\}}\tau\sigma(1-\zeta_{m_I})\Big|\\ &= \sum_{a \bmod^\star f}\chi(a)\ln\Big|\prod_{\emptyset\neq I\subseteq\{1,\dots,s\}}(1-\zeta_{m_I}^a)\Big|\\ &= \sum_{\emptyset\neq I\subseteq\{1,\dots,s\}}\sum_{a \bmod^\star f}\chi(a)\ln\big|1-\zeta_{m_I}^a\big|\\ &= \sum_{\substack{\emptyset\neq I\subseteq\{1,\dots,s\}\\ f_\chi\mid m_I}}\tfrac{\varphi(f)}{\varphi(m_I)}\sum_{b \bmod^\star f_\chi}\chi(b)\ln\big|1-\zeta_{m_I}^b\big|\end{aligned}$$

podle lemmatu 3. Důsledek lemmatu 4 a lemma 5 pak dají

$$\begin{aligned}&\sum_{\tau\in\mathrm{Gal}(K/\mathbb{Q})}\chi(\tau)\ln|\tau(\vartheta)|\\ &\quad= \sum_{\substack{\emptyset\neq I\subseteq\{1,\dots,s\}\\ f_\chi\mid m_I}}\tfrac{\varphi(f)}{\varphi(m_I)}\Big(\prod_{p\mid m_I}(1-\chi(p))\Big)\sum_{\substack{b=1,\dots,m_I\\(b,f_\chi)=1}}\chi(b)\ln\big|1-\zeta_{m_I}^b\big|\\ &\quad= -\tau(\chi)L(1,\bar\chi)\sum_{\substack{\emptyset\neq I\subseteq\{1,\dots,s\}\\ f_\chi\mid m_I}}\Big(\prod_{i\in\{1,\dots,s\}\setminus I}\varphi(p_i^{e_i})\Big)\Big(\prod_{i\in I}(1-\chi(p_i))\Big)\\ &\quad= -\tau(\chi)L(1,\bar\chi)\prod_{\substack{i\in\{1,\dots,s\}\\ p_i\nmid f_\chi}}(\varphi(p_i^{e_i})+1-\chi(p_i))\end{aligned}$$

Dosazením dostaneme

$$|E/C'|\cdot R = \Big|\prod_{\chi\in X\setminus\{\chi_0\}}\Big(-\tau(\chi)L(1,\bar\chi)\prod_{\substack{i\in\{1,\dots,s\}\\ p_i\nmid f_\chi}}(\varphi(p_i^{e_i})+1-\chi(p_i))\Big)\Big|.$$

Dle vzorce na konci kapitoly 18 platí

$$\prod_{\chi\in X\setminus\{\chi_0\}}\tau(\chi)L(1,\bar\chi) = 2^{|X|-1}Rh,$$

odkud plyne věta.

Důsledek. Nechť K je abelovské těleso. Grupa kruhových jednotek C tělesa K má konečný index v grupě E všech jednotek tohoto tělesa.

Důkaz. Stačí ukázat, že obě grupy E a C mají týž rank. Jestliže K není reálné, pak mají grupa jednotek K a grupa jednotek jeho maximálního reálného podtělesa $K^+ = K\cap\mathbb{R}$ týž rank (viz Dirichletovu větu o jednotkách), přitom grupa kruhových jednotek tělesa K^+ je podgrupou grupy kruhových jednotek tělesa K. Stačí tedy větu dokázat pro reálná K. To však plyne z předchozí věty.

Věta 4. Nechť p je liché prvočíslo, $n \in \mathbb{N}$. Pro index grupy kruhových jednotek p^n-tého kruhového tělesa $\mathbb{Q}_{p^n}$ platí

$$|E/C| = h^+,$$

kde h^+ značí počet tříd divizorů tělesa $\mathbb{Q}_{p^n} \cap \mathbb{R} = \mathbb{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1})$.

Důkaz. Označme E grupu jednotek tělesa $K = \mathbb{Q}_{p^n}$, W grupu odmocnin z jedné v tomto tělese; je tedy W generovaná -1 a $\zeta = \zeta_{p^n}$. Dále $E^+ = E \cap \mathbb{R}$ značí grupu jednotek tělesa $K^+ = \mathbb{Q}_{p^n} \cap \mathbb{R}$. Označme dále C, resp. C^+, grupy kruhových jednotek tělesa K, resp. K^+. Užijme větu 3 pro těleso K^+. Pak $\vartheta = N_{K_K^+}(1-\zeta) = (1-\zeta)(1-\zeta^{-1})$. Pro libovolný automorfismus $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$, určený předpisem $\sigma^{-1}(\zeta) = \zeta^s$, platí

$$\varepsilon_\sigma = \frac{(1-\zeta^s)(1-\zeta^{-s})}{(1-\zeta)(1-\zeta^{-1})} = \zeta^{(1-s)}\frac{(1-\zeta^s)^2}{(1-\zeta)^2} = \eta_\sigma^2,$$

kde

$$\eta_\sigma = \zeta^{(1-s)/2}\frac{(1-\zeta^s)}{(1-\zeta)} \in E^+.$$

Dle věty 3 pro grupu C' generovanou v E^+ množinou $\{-1\} \cup \{\varepsilon_\sigma;\ \sigma \in G\}$ platí $|E^+/C'| = 2^{[K^+:\mathbb{Q}]-1}h^+$. Odtud plyne, že pro grupu C'' generovanou v E^+ množinou $\{-1\} \cup \{\eta_\sigma;\ \sigma \in G\}$ platí $|E^+/C''| = |E/C'|/|C''/C'| = h^+$, neboť $|C''/C'| = 2^{[K^+:\mathbb{Q}]-1}$. Věta bude dokázána, ukážeme-li, že $|E/C| = |E^+/C''|$. Nejprve ukažme, že $C = WC''$. Podle věty 2 je C generováno -1 a jednotkami $(1-\zeta_{p^r}^a)(1-\zeta_{p^r})^{-1}$, kde přirozené číslo $r \le n$ a celé číslo a není dělitelné p. Podle věty 1 platí

$$(1-\zeta_{p^r}^a)(1-\zeta_{p^r})^{-1} = N_{\mathbb{Q}_{p^n}/\mathbb{Q}_{p^r}}\big((1-\zeta_{p^n}^a)(1-\zeta_{p^n})^{-1}\big),$$

a tedy $(1-\zeta_{p^r}^a)(1-\zeta_{p^r})^{-1} \in WC''$. Opačná inkluze je zřejmá. Pro důkaz věty nyní postačí dokázat $E = WE^+$. Inkluze $WE^+ \subseteq E$ je jasná. Pro důkaz opačné inkluze bude zapotřebí dokázat následující dvě lemmata, proto nyní důkaz věty 4 přerušíme s tím, že bude dokončen, jakmile dokážeme lemma 7.

Lemma 6. Nechť p je liché prvočíslo, $n \in \mathbb{N}$. Pak okruhem celých čísel tělesa $K = \mathbb{Q}_{p^n}$ je okruh $\mathbb{Z}[\zeta] = \{f(\zeta);\ f(x) \in \mathbb{Z}[x]\}$, kde $\zeta = \zeta_{p^n}$.

Důkaz. Protože $K = \mathbb{Q}(\zeta) = \mathbb{Q}(1-\zeta)$ je těleso stupně $s = \varphi(p^n)$ (viz důsledek věty 1 kapitoly 4), tvoří $1, 1-\zeta, (1-\zeta)^2, \ldots, (1-\zeta)^{s-1}$ bazi K (jakožto vektorového prostoru nad $\mathbb{Q}$). Nechť α je celé číslo tělesa K. Pak existují racionální čísla $a_0, a_1, \ldots, a_{s-1}$ tak, že

$$(*) \qquad \alpha = \sum_{i=0}^{s-1} a_i(1-\zeta)^i.$$

Chceme ukázat $a_i \in \mathbb{Z}$. Podle věty 1 kapitoly 14 se prvočíslo p totálně větví v K, neboť pro divizory platí $(p) = (1-\zeta)^s$. Uvažme exponent ν tělesa K příslušný prvku $1-\zeta$; ν je tedy jediné prodloužení p-adického exponentu na K. Platí tedy

$\nu(1-\zeta)=1$. Protože $\nu(a)\equiv 0 \pmod s$ pro libovolné $a\in\mathbb{Q}$, je $\nu(a_i(1-\zeta)^i)\equiv i \pmod s$. Proto v součtu (*) mají sčítanci různou hodnotu exponentu ν a tedy

$$0\le\nu(\alpha)=\min_{0\le i<s}(i+\nu(a_i)).$$

Proto $\nu(a_i)\ge 0$ pro každé $i=0,1,\dots,s-1$. Upravme (*) do tvaru

$$\alpha=\sum_{i=0}^{s-1}b_i\zeta^i,$$

kde $b_i\in\mathbb{Q}$ nemají p ve jmenovateli. Pro libovolné $\sigma\in G=\mathrm{Gal}(K/\mathbb{Q})$ pak platí

$$\sigma(\alpha)=\sum_{i=0}^{s-1}b_i\sigma(\zeta)^i.$$

Protože $|G|=s$, můžeme z těchto s lineárních rovnic spočítat b_i pomocí $\sigma(\alpha)$. Matice soustavy je

$$(\sigma(\zeta)^i)_{\sigma\in G,\,i=0,1,\dots,s-1},$$

její diskriminant je Vandermondův, tedy roven součinu rozdílů $\sigma(\zeta)-\tau(\zeta)$:

$$\det(\sigma(\zeta)^i)_{\sigma\in G,\,i=0,1,\dots,s-1}=\prod_{\substack{1\le i<j<p^n\\ p\nmid ij}}(\zeta^j-\zeta^i),$$

ovšem $1-\zeta^{j-i}$ je dělitelem p v okruhu celých čísel tělesa K (viz důkaz zmíněné věty 1 kapitoly 14) a tedy uvedený Vandermondův determinant je součin vhodné jednotky tělesa K s nějakou mocninou čísla $1-\zeta$. Vynásobíme-li matici inverzní k matici soustavy vhodnou mocninou prvočísla p, dostaneme matici, jejíž prvky jsou celá algebraická čísla. Proto pro čísla b_i vypočtená z uvedené soustavy lineárních rovnic platí: b_i je rovno celému algebraickému číslu vydělenému nějakou mocninou prvočísla p. Protože víme z předchozího, že b_i je racionální číslo, jehož jmenovatel není dělitelný p, platí $b_i\in\mathbb{Z}$.

Lemma 7. Nechť p je liché prvočíslo, $n\in\mathbb{N}$, E grupa jednotek tělesa $K=\mathbb{Q}_{p^n}$, W grupa odmocnin z jedné v tomto tělese, $E^+=E\cap\mathbb{R}$. Pak pro libovolnou jednotku $\varepsilon\in E$ existují $\rho\in W$ a $\eta\in E^+$ tak, že $\varepsilon=\rho\eta$.

Důkaz. Označme $\alpha=\frac{\varepsilon}{\bar\varepsilon}$, kde jednotka $\bar\varepsilon$ je komplexně konjugovaná s ε. Pak α je celé algebraické číslo takové, že pro libovolné $\sigma\in G=\mathrm{Gal}(\mathbb{Q}_{p^n}/\mathbb{Q})$ platí $|\alpha^\sigma|=1$ (zde jsme využili toho, že restrikce komplexní konjugovanosti je prvek G, a toho, že G je komutativní grupa). Pak minimální mnohočleny $\varphi_{\alpha^r}\in\mathbb{Z}[x]$, kde $r\in\mathbb{N}$, mají koeficienty omezené v absolutní hodnotě. Ovšem takových mnohočlenů je jen konečně mnoho a proto se musí začít opakovat. To znamená, že $\alpha\in W$, tedy $\alpha=\pm\zeta^a$ pro nějaké celé číslo a. Předpokládejme nejprve, že $\alpha=-\zeta^a$. Podle lemmatu 6 existují $b_i\in\mathbb{Z}$ tak, že

$$\varepsilon=\sum_{i=0}^{\varphi(p^n)-1}b_i\zeta^i,$$

Pak platí

$$\varepsilon \equiv \sum_{i=0}^{\varphi(p^n)-1} b_i \equiv \bar{\varepsilon} = -\zeta^{-a}\varepsilon \equiv -\varepsilon \pmod{1-\zeta},$$

odkud $1-\zeta|(2\varepsilon)$, spor. Je tedy $\alpha = \zeta^a$. Nechť $c \in \mathbb{Z}$ splňuje $2c \equiv a \pmod{p^n}$. Pak pro $\eta = \zeta^{-c}\varepsilon$ platí $\bar{\eta} = \eta$ a tedy $\eta \in E^+$.

Poznámka. Z důsledku věty 3 plyne konečnost grupy E/C pro libovolné abelovské těleso. Díky větě 4 víme, že v některých speciálních případech je znám i vzorec pro počet prvků této faktorgrupy. Speciální případ věty 4 pro p-té kruhové těleso $\mathbb{Q}_p$, kde p je prvočíslo, znal již Kummer (místo o počtu prvků faktorgrupy psal o podílu regulátoru jednotek, kterým teď říkáme kruhové, a regulátoru všech jednotek, což je však totéž – viz důkaz věty 3). Vzorec z věty 4 byl zobecněn Sinnottem (1978) na případ obecného kruhového tělesa: je-li přirozené číslo $m \not\equiv 2 \pmod 4$, pak pro m-té kruhové těleso $\mathbb{Q}_m$ platí $|E/C| = 2^a h^+$, kde h^+ je počet tříd divizorů tělesa $\mathbb{Q}_m^+ = \mathbb{Q}_m \cap \mathbb{R}$ a číslo a je určeno počtem g prvočísel dělících m takto: je-li $g = 1$, pak $a = 0$, je-li $g > 1$, pak $a = 2^{g-2} + 1 - g$. V roce 1980 Sinnott zobecnil svůj vzorec na libovolné abelovské těleso, opět je index určen jako součin h^+ s jistým výrazem, který již počet tříd divizorů neobsahuje. Toto zobecnění však není explicitní, zmíněný výraz totiž obsahuje počty prvků jistých konečných faktorgrup, které bývá velmi nesnadné určit (v podstatě jde o kohomologické grupy).

Je jasné, že někdy lze získat jistou informaci o počtu tříd divizorů studiem kruhových jednotek; pokud bychom například pro p-té kruhové těleso našli nějakou jednotku ε, která by nebyla kruhová, znamenalo by to, že pro nějaké přirozené číslo $r > 1$ je jednotka ε^r kruhová, a je-li r nejmenší s touto vlastností, pak $r|h^+$. V současné době však nikdo neví, jak takové nekruhové jednotky konstuovat (výjimkou jsou snad reálná kvadratická tělesa, pro které je znám algoritmus na výpočet fundamentální jednotky pomocí řetězových zlomků).

20. Některé nezbytnosti z algebraické geometrie

V celé kapitole předpokládáme, že K je těleso.

Definice. n-rozměrným afinním prostorem nad K rozumíme kartézskou mocninu K^n. Budeme jej značit $A^n(K)$, tj.

$$A^n(K) = \{(x_1, \dots, x_n);\, x_1, \dots, x_n \in K\}.$$

Definice. n-rozměrným projektivním prostorem nad K rozumíme rozklad na množině $K^{n+1} - \{(0, \dots, 0)\}$ příslušný ekvivalenci $\sim$ definované takto: pro libovolné $(n+1)$-tice $(x_1, \dots, x_{n+1})$, $(y_1, \dots, y_{n+1}) \in K^{n+1}$ položíme $(x_1, \dots, x_{n+1}) \sim (y_1, \dots, y_{n+1})$ právě tehdy, když existuje $\lambda \in K^\times$, které pro každé $i \in \{1, \dots, n+1\}$ splňuje podmínku $x_i = \lambda y_i$. Tento n-rozměrný projektivní prostor nad K budeme značit $P^n(K)$, třídu rozkladu (tj. bod projektivního prostoru) obsahující $(n+1)$-tici $(x_1, \dots, x_{n+1})$ budeme značit $[x_1, \dots, x_{n+1}]$.

Poznámka. Nechť $x_1, \dots, x_{n+1} \in K$, přičemž alespoň jedno z nich je různé od nuly. Jestliže $x_{n+1} \neq 0$, pak platí $[x_1, \dots, x_{n+1}] = [\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}}, 1]$, čímž je pevně dán bod $(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}}) \in A^n(K)$. Jestliže naopak $x_{n+1} = 0$, určuje

$[x_1, \ldots, x_{n+1}]$ jednoznačně bod $[x_1, \ldots, x_n] \in P^{n-1}(K)$. Můžeme tedy n-rozměrný projektivní prostor „rozdělit“ na n-rozměrný afinní prostor a na „část nevlastních bodů“, kterou je $(n-1)$-rozměrný projektivní prostor. Toto rozdělení *není* kanonické – lze to provést mnoha způsoby.

Poznámka. Je-li dán homogenní polynom $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ o $n+1$ proměnných nad K stupně k a bod $[x_1, \ldots, x_{n+1}] \in P^n(K)$, má smysl se ptát, zda $F(x_1, \ldots, x_{n+1}) = 0$. Je-li totiž $[x_1, \ldots, x_{n+1}] = [y_1, \ldots, y_{n+1}]$, pak existuje $\lambda \in K^\times$, které pro každé $i \in \{1, \ldots, n+1\}$ splňuje podmínku $x_i = \lambda y_i$. Pak ovšem $F(x_1, \ldots, x_{n+1}) = F(\lambda y_1, \ldots, \lambda y_{n+1}) = \lambda^k \cdot F(y_1, \ldots, y_{n+1})$ a tedy $F(x_1, \ldots, x_{n+1}) = 0$ právě když $F(y_1, \ldots, y_{n+1}) = 0$.

Definice. Nechť $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k. Množina

$$\mathcal{C} = \{[x_1, \ldots, x_{n+1}] \in P^n(K);\ F(x_1, \ldots, x_{n+1}) = 0\}$$

se nazývá nadplocha stupně k v $P^n(K)$. Je-li $n = 2$, hovoříme také o křivce stupně k v $P^2(K)$.

Poznámka. Parciální derivací homogenního mnohočlenu je opět homogenní mnohočlen. Má proto smysl následující definice.

Definice. Nechť $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k a

$$\mathcal{C} = \{[x_1, \ldots, x_{n+1}] \in P^n(K);\ F(x_1, \ldots, x_{n+1}) = 0\}$$

příslušná nadplocha. Bod $[x_1, \ldots, x_{n+1}] \in \mathcal{C}$ se nazývá singulární, jestliže pro každé $i \in \{1, \ldots, n+1\}$ platí

$$\frac{\partial F}{\partial x_i}(x_1, \ldots, x_{n+1}) = 0.$$

Nadplocha $\mathcal{C}$ se nazývá singulární, existuje-li alespoň jeden její singulární bod.

Příklad. Uvažme reálnou projektivní rovinu $P^2(\mathbb{R})$. Abychom se vyhnuli indexům, budeme psát x, y, z místo t_1, t_2, t_3. Kubický mnohočlen $F_1(x, y, z) = x^3 + x^2 z - y^2 z$ nám definuje kubickou křivku $\mathcal{C}_1$ (tj. křivku stupně 3)

$$\mathcal{C}_1 = \{[x, y, z] \in P^2(\mathbb{R});\ F_1(x, y, z) = 0\}.$$

Jistě $[0, 0, 1] \in \mathcal{C}_1$. Tento bod je singulární, neboť

$$\frac{\partial F_1}{\partial x} = 3x^2 + 2xz, \quad \frac{\partial F_1}{\partial y} = -2yz, \quad \frac{\partial F_1}{\partial z} = x^2 - y^2.$$

Je tedy $\mathcal{C}_1$ singulární křivka. Uvažme nyní mnohočlen $F_2(x, y, z) = x^3 + xz^2 - y^2 z$ a příslušnou kubickou křivku

$$\mathcal{C}_2 = \{[x, y, z] \in P^2(\mathbb{R});\ F_2(x, y, z) = 0\}.$$

Hledejme singulární body na $\mathcal{C}_2$. Platí

$$\frac{\partial F_2}{\partial x} = 3x^2 + z^2, \quad \frac{\partial F_2}{\partial y} = -2yz, \quad \frac{\partial F_2}{\partial z} = 2xz - y^2.$$

Z $\frac{\partial F_2}{\partial x} = 0$ plyne $x = 0$ a $z = 0$, pak ale z $\frac{\partial F_2}{\partial z} = 0$ plyne i $y = 0$. Singulární bod na $\mathcal{C}_2$ tedy neexistuje a proto $\mathcal{C}_2$ není singulární křivka.

Definice. Eliptická křivka nad K je uspořádaná dvojice $(\mathcal{E}, O)$, kde $\mathcal{E}$ je nesingulární kubická křivka v $P^2(K)$ a $O \in \mathcal{E}$.

Poznámka. Je možné zavést pojem biracionální ekvivalence dvou křivek, spočívající v tom, že existují transformace prostoru převádějící jednu křivku na druhou a obráceně, přičemž tyto transformace jsou „pěkné“ v tom smyslu, že transformační rovnice jsou dány homogenními polynomy téhož stupně nad K. Precizní zavedení tohoto pojmu je však časově náročné a proto od něj upouštím. Tento pojem je zde zapotřebí pouze proto, abychom si ukázali, že vlastně neztrácíme nic na obecnosti, omezíme-li se na eliptické křivky speciálního tvaru. Nebudeme tedy ani dokazovat následující větu.

Věta. Libovolná eliptická křivka nad K je biracionálně ekvivalentní s nějakou eliptickou křivkou $(\mathcal{E}, O)$ následujícího tvaru (přičemž transformace převádějí vyznačený bod jedné křivky na vyznačený bod druhé křivky)

$$\mathcal{E} = \{[x, y, z] \in P^2(K);\ F(x, y, z) = 0\},$$

kde

$$F(x, y, z) = y^2 z + a_1 xyz + a_2 yz^2 - x^3 - a_3 x^2 z - a_4 xz^2 - a_5 z^3,$$

$a_1, \ldots, a_5 \in K$ a $O = [0, 1, 0]$.

Poznámka. Každá eliptická křivka ve výše uvedeném tvaru má jeden nevlastní bod (totiž O) a v afinní části je dána rovnicí

$$y^2 + a_1 xy + a_2 y = x^3 + a_3 x^2 + a_4 x + a_5.$$

Tato rovnice se nazývá Weierstrassova rovnice. Pokud charakteristika tělesa K není ani 2 ani 3, lze Weierstrassovu rovnici dále zjednodušit. Můžeme pak totiž předpokládat, že $a_1 = a_2 = a_3 = 0$ a tedy Weierstrassova rovnice je tvaru $y^2 = x^3 + a_4 x + a_5$.

21. Aritmetika eliptických křivek

V celé kapitole předpokládáme, že K je těleso charakteristiky různé od 2 a 3 a že je dána eliptická křivka $(\mathcal{E}, O)$, kde $O = [0, 1, 0]$ a $\mathcal{E}$ je dána Weierstrassovou rovnicí

$$y^2 = x^3 + ax + b,$$

kde $a, b \in K$. Jak plyne z následující věty, důsledkem našich předpokladů je, že $4a^3 + 27b^2 \neq 0$.

Věta. Rovnice $y^2 = x^3 + ax + b$ je Weierstrassovou rovnicí nějaké eliptické křivky, právě když platí $4a^3 + 27b^2 \neq 0$.

Důkaz. Položme $F(x, y, z) = y^2 z - x^3 - axz^2 - bz^3$. Platí

$$\frac{\partial F}{\partial x} = -3x^2 - az^2, \quad \frac{\partial F}{\partial y} = 2yz, \quad \frac{\partial F}{\partial z} = y^2 - 2axz - 3bz^2.$$

Předpokládejme, že $[x, y, z]$ je singulární bod. Pak $z = 0$ implikuje $x = y = 0$, spor. Je tedy $z \neq 0$. Proto $y = 0$ a pro $\gamma = \frac{x}{z}$ platí $3\gamma^2 = -a$, $2a\gamma = -3b$. Jestliže $a = 0$, pak také $b = 0$. Naopak pro $a = b = 0$ je bod $[0, 0, 1]$ singulární. Zabývejme se dále případem $a \neq 0$. Platí $\gamma = -\frac{3b}{2a}$, $\gamma^2 = -\frac{a}{3} = \frac{9b^2}{4a^2}$, tj. $4a^3 + 27b^2 = 0$. Zbývá ověřit, že $[\gamma, 0, 1]$ vyhovuje rovnici, což je snadné:

$$\gamma^3 + a\gamma + b = \left(-\tfrac{3b}{2a}\right)\left(-\tfrac{a}{3}\right) + a\left(-\tfrac{3b}{2a}\right) + b = \tfrac{b}{2} - \tfrac{3b}{2} + b = 0.$$

Poznámka. Naším cílem je definovat na $\mathcal{E}$ grupovou operaci $+$. Je třeba tedy najít nějaký předpis, jak dvěma bodům z $\mathcal{E}$ přiřadit třetí. Máme-li dány dva různé body z $\mathcal{E}$, můžeme jimi vést přímku. Dosazením rovnice této přímky do Weierstrassovy rovnice získáme kubickou rovnici, jejíž dva kořeny známe. Existuje proto třetí kořen, který lze snadno spočítat. Tento třetí kořen odpovídá třetímu průsečíku přímky s eliptickou křivkou (který může popřípadě i splynout s některým z daných bodů).

Podobně můžeme postupovat i v případě, kdy vezmeme dvakrát týž bod z $\mathcal{E}$: sestrojíme v tomto bodě tečnu k $\mathcal{E}$. Protože K nemusí být těleso reálných čísel, je možná vhodné upřesnit, co rozumíme touto tečnou: je to taková přímka, že po dosazení její rovnice do rovnice eliptické křivky dostaneme kubickou rovnici, ve které bod dotyku odpovídá kořenu alespoň dvojnásobnému. Zbylý kořen pak odpovídá dalšímu průsečíku přímky s eliptickou křivkou (který by opět mohl splynout s daným bodem).

V obou případech nám dvojice bodů z $\mathcal{E}$ určila další bod z $\mathcal{E}$. Tato binární operace by nám však nevytvořila z $\mathcal{E}$ grupu (je zřejmé, že tato operace obecně nemá neutrální prvek).

Operaci $+$ na $\mathcal{E}$ definujeme takto: pro libovolné body $A, B \in \mathcal{E}$ označme C bod z $\mathcal{E}$ jimi určený. Součtem $A + B$ pak nazveme bod z $\mathcal{E}$ určený body C a O.

Příklad. Nevlastní přímka $z = 0$ má s $\mathcal{E}$ trojnásobný bod dotyku O: dosazením $z = 0$ do rovnice $y^2z = x^3 + axz^2 + bz^3$ dostaneme rovnici $x^3 = 0$, která má trojnásobný kořen $x = 0$. Proto pro $A = B = O$ je i $C = O$ a tedy i $A + B = O$. Je tedy $O + O = O$.

Uvažme případ $A = O$, $B \neq O$. Pak $B = [\alpha, \beta, 1]$ pro vhodné α, $\beta \in K$. Přímka určená body O, B má rovnici $x = \alpha z$ (nevlastním bodem této přímky je O, vlastní body jsou $[\alpha, y, 1]$ pro všechna $y \in K$). Je zřejmé, že $C = [\alpha, -\beta, 1]$ a že třetí bod na přímce určené C a O je B. Ověřili jsme tedy, že platí $O + B = B$.

Je zřejmé, že operace $+$ je komutativní. Víme tedy, že $(\mathcal{E}, +)$ je komutativní grupoid s neutrálním prvkem O a že pro každý bod $A \in \mathcal{E}$ existuje bod $B \in \mathcal{E}$ splňující $A + B = O$ (je-li $A = O$, vezmeme $B = O$; je-li $A = [\alpha, \beta, 1]$, vezmeme $B = [\alpha, -\beta, 1]$).

Poznámka. K důkazu tvrzení, že $(\mathcal{E}, +)$ je komutativní grupa, je třeba dokázat, že $+$ je asociativní operace. To ale není snadné a omezíme se pouze na konstatování tohoto faktu bez důkazu.

Věta. Na eliptické křivce $(\mathcal{E}, O)$ nad K definujeme operaci $+$ takto:

1. Pro libovolné $A \in \mathcal{E}$ klademe $A + O = O + A = A$.
2. Pro libovolné $A = [\alpha, \beta, 1] \in \mathcal{E}$ je také $B = [\alpha, -\beta, 1] \in \mathcal{E}$ a klademe $A + B = O$. (Tento bod B pak označujeme $-A$.)

3. Pro libovolné $A = [\alpha, \beta, 1] \in \mathcal{E}$, $B = [\gamma, \delta, 1] \in \mathcal{E}$ takové, že $B \neq -A$, položme

$$k = \begin{cases} \frac{\beta-\delta}{\alpha-\gamma} & \text{je-li } A \neq B, \\ \frac{3\alpha^2+a}{2\beta} & \text{je-li } A = B, \end{cases}$$
$$\sigma = k^2 - \alpha - \gamma,$$
$$\tau = -\beta + k(\alpha - \sigma),$$

pak platí $[\sigma, \tau, 1] \in \mathcal{E}$ a klademe $A + B = [\sigma, \tau, 1] \in \mathcal{E}$.
Pak $(\mathcal{E}, +)$ je komutativní grupa.

Poznámky. Důkaz toho, že $+$ je asociativní operace, je mimo možnosti naší přednášky. Eliptické křivky tvoří komutativní grupu i nad tělesy charakteristiky 2 a 3. Je však třeba uvažovat obecnější tvar Weierstrassovy rovnice a proto i vzorce popisující sčítání bodů jsou komplikovanější.

22. Body konečného řádu na eliptických křivkách

Ve Weierstrassově teorii eliptických funkcí je dokázáno, že máme-li dvě komplexní čísla g_2, g_3 taková, že polynom $4x^3 - g_2 x - g_3$ nemá násobný kořen (tj. $g_2^3 - 27g_3^2 \neq 0$), pak můžeme pomocí jistých určitých integrálů najít komplexní čísla ω_1, ω_2, nazývané periody. Tyto periody jsou $\mathbb{R}$-lineárně nezávislé a v aditivní grupě komplexních čísel generují podgrupu

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2;\, n_1, n_2 \in \mathbb{Z}\}.$$

Takovým podgrupám $\mathbb{C}$ říkáme mřížka (anglicky lattice). Ačkoli lze generátory L zvolit různými způsoby, ukazuje se, že mřížka L jednoznačně určuje čísla g_2, g_3 pomocí vzorců

$$g_2 = 60 \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^4}, \qquad g_3 = 140 \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^6}.$$

Pomocí mřížky L můžeme definovat Weierstrassovu $\wp$ funkci předpisem

$$\wp(u) = \frac{1}{u^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right).$$

Platí, že řada definující Weierstrassovu $\wp$ funkci konverguje absolutně a stejnoměrně na každé kompaktní podmnožině $\mathbb{C} \setminus L$ a definuje meromorfní funkci na $\mathbb{C}$, která má dvojnásobný pól s nulovým residuem v každém bodě L a jinde póly nemá.

Definice. Nechť $L \subseteq \mathbb{C}$ je mřížka. Eliptická funkce (vzhledem k L) je meromorfní funkce $f(z)$, která je periodická vzhledem k L, tj. pro kterou platí $f(z + \omega) = f(z)$ pro každé $\omega \in L$, $z \in \mathbb{C}$.

Weierstrassova $\wp$ funkce je tedy sudá eliptická funkce. Platí dokonce, že libovolnou sudou eliptickou funkci lze získat dosazením funkce $\wp$ do vhodné racionální lomené funkce. Protože $\wp' = \frac{d\wp}{du}$ je lichá eliptická funkce, z předchozího plyne,

že $(\wp')^2$ lze vyjádřit racionální lomenou funkcí pomocí funkce $\wp$. Toto vyjádření můžeme dokonce popsat explicitně pomocí g_2, g_3: platí

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3.$$

Pro libovolné komplexní číslo $u \notin L$ tedy dostáváme bod (s komplexními souřadnicemi)

$$P(u) = (\wp(u), \wp'(u))$$

na eliptické křivce

$$\mathcal{E}: \quad y^2 = 4x^3 - g_2x - g_3,$$

přitom pro $u \in L$ dodefinujeme $P(u)$ jako nevlastní bod na zmíněné křivce. Tím jsme definovali zobrazení $P : \mathbb{C} \to \mathcal{E}(\mathbb{C})$. Napoprve asi překvapí, že toto zobrazení je homomorfismus aditivních grup, tj. že platí

$$P(u_1 + u_2) = P(u_1) + P(u_2),$$

kde na levé straně je sčítání komplexních čísel, kdežto + na pravé straně znamená sčítání bodů na eliptické křivce (kde bod O je nevlastní). Proto máme izomorfismus grup $\mathbb{C}/L \simeq \mathcal{E}(\mathbb{C})$. Uvědomme si, že grupa $\mathbb{C}/L$ je izomorfní s přímým součinem dvou kopií grupy $\mathbb{R}/\mathbb{Z}$, neboli součinem dvou jednotkových kružnic v $\mathbb{C}$ (chápaných jako multiplikativní grupy), tj. je to torus.

Tvrzení. Nechť $\mathcal{E}(\mathbb{C})$ je eliptická křivka (daná Weierstrassovou rovnicí), označme $\mathcal{E}(\mathbb{C})[n]$ podgrupu grupy $\mathcal{E}(\mathbb{C})$ složenou z těch bodů, jejichž řád (v této grupě) dělí n. Pak $\mathcal{E}(\mathbb{C})[n]$ je přímý součin dvou cyklických grup řádu n.

Pro libovolné těleso algebraických čísel K platí $K \subseteq \mathbb{C}$. Jsou-li koeficienty Weierstrassovy rovnice prvky K, má smysl hovořit o podgrupě $\mathcal{E}(K)$ grupy $\mathcal{E}(\mathbb{C})$ (do které patří kromě nevlastního bodu O právě ty body $\mathcal{E}(\mathbb{C})$, které mají souřadnice v K).

Předpokládejme nyní, že $K/\mathbb{Q}$ je Galoisovo rozšíření a že koeficienty Weierstrassovy rovnice jsou racionální čísla. Pro libovolné $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ a libovolné $P \in \mathcal{E}(K)$ definujeme $\sigma(P) \in \mathcal{E}(K)$ takto: $\sigma(O) = O$ a pro $P \neq O$, $P = (x, y)$ klademe $\sigma(P) = (\sigma(x), \sigma(y))$. Snadno se ověří, že $\sigma : \mathcal{E}(K) \to \mathcal{E}(K)$ je grupový homomorfismus.

Tvrzení. Nechť $\mathcal{E}$ je eliptická křivka dána Weierstrassovou rovnicí

$$y^2 = x^3 + ax^2 + bx + c$$

s $a, b, c \in \mathbb{Q}$. Pak platí

1. Je-li $P = (x_1, y_1) \in \mathcal{E}(\mathbb{C})$ bod řádu n, pak x_1 a y_1 jsou algebraická čísla.
2. Nechť $\{(x_1, y_1), \ldots, (x_m, y_m), O\} = \mathcal{E}(\mathbb{C})[n]$. (Z předchozího víme, že $m = n^2 - 1$.) Označme $K = \mathbb{Q}(\mathcal{E}[n]) = \mathbb{Q}(x_1, y_1, \ldots, x_m, y_m)$ těleso generované souřadnicemi všech bodů, jejich řád dělí n. Pak platí, že $K/\mathbb{Q}$ je Galoisovo rozšíření.

Cvičení 34. Nechť n_1, n_2 jsou nesoudělná přirozená čísla. Dokažte, že pak $\mathbb{Q}(\mathcal{E}[n_1 n_2])$ je kompositum těles $\mathbb{Q}(\mathcal{E}[n_1])$, $\mathbb{Q}(\mathcal{E}[n_2])$.

Pro libovolné $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ máme definován automorfismus grupy $\mathcal{E}(K)$. Protože prvek řádu n se automorfismem zobrazí na prvek téhož řádu, dostáváme zúžením automorfismus grupy $\mathcal{E}(\mathbb{C})[n]$. To je však součin dvou cyklických grup řádu n. Označme P_1, P_2 generátory $\mathcal{E}(\mathbb{C})[n]$. Protože automorfismus je určen obrazy generátorů, pro určení $\sigma : \mathcal{E}(\mathbb{C})[n] \to \mathcal{E}(\mathbb{C})[n]$ stačí znát celá čísla a_σ, b_σ, c_σ, d_σ splňující

$$\sigma(P_1) = a_\sigma P_1 + b_\sigma P_2 \qquad \sigma(P_2) = c_\sigma P_1 + d_\sigma P_2.$$

Naopak zbytkové třídy modulo n obsahující čísla $a_\sigma, b_\sigma, c_\sigma, d_\sigma$ jsou automorfismem σ určeny jednoznačně. Snadno se ověří, že přiřazení

$$\rho_n : \sigma \mapsto \begin{pmatrix} a_\sigma & c_\sigma \\ b_\sigma & d_\sigma \end{pmatrix}$$

je vnoření (tj. injektivní homomorfismus) $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, kde $\mathrm{GL}_2(R)$ značí multiplikativní grupu všech 2×2 matic s prvky v okruhu R, jejichž determinant je jednotka okruhu R.

Poznámka. Vnoření nějaké studované grupy do jiné jednodušší se nazývají reprezentace, proto ρ_n se nazývá Galoisova reprezentace. O užitečnosti reprezentací jsme se už přesvědčili, uvědomme si, že reprezentací je námi užívaný izomorfismus $\mathrm{Gal}(\mathbb{Q}_m/\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^\star$. Jak vyplyne z následujících příkladů, ρ_n bijekcí být nemusí.

Příklad 1. Uvažme eliptickou křivku

$$\mathcal{E} : y^2 = x(x-1)(x-2).$$

Pak $\mathcal{E}(\mathbb{C})[2] = \{O, (0,0), (1,0), (2,0)\}$ se skládá výhradně z racionálních bodů. Je tedy $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}$, $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2])/\mathbb{Q}) = \{\sigma_0\}$ a $\rho_2(\sigma_0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Příklad 2. Uvažme eliptickou křivku

$$\mathcal{E} : y^2 = x^3 + x.$$

Pak $\mathcal{E}(\mathbb{C})[2] = \{O, (0,0), (i,0), (-i,0)\}$. Je tedy $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(i)$, $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2])/\mathbb{Q}) = \{\sigma_0, \sigma_1\}$ obsahuje dva prvky, identitu σ_0 a komplexní konjugovanost σ_1. Zvolme generátory například takto: $P_1 = (0,0)$, $P_2 = (i,0)$. Pak $\sigma_1(P_1) = P_1$, $\sigma_1(P_2) = (-i,0) = P_1 + P_2$, tedy

$$\rho_2(\sigma_0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \rho_2(\sigma_1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Příklad 3. Uvažme eliptickou křivku

$$\mathcal{E} : y^2 = x^3 - 2.$$

Pak $\mathcal{E}(\mathbb{C})[2] = \{O, (\sqrt[3]{2}, 0), (\zeta\sqrt[3]{2}, 0), (\zeta^2\sqrt[3]{2}, 0)\}$, kde $\zeta = \frac{-1+\sqrt{-3}}{2}$. Odtud plyne $\mathbb{Q}(\mathcal{E}[2]) = \mathbb{Q}(\zeta, \sqrt[3]{2})$, $\mathrm{Gal}(\mathbb{Q}(\mathcal{E}[2])/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, kde σ a τ jsou určeny podmínkami

$$\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}, \qquad \tau(\sqrt[3]{2}) = \sqrt[3]{2},$$
$$\sigma(\zeta) = \zeta, \qquad \tau(\zeta) = \zeta^2.$$

Zvolme generátory například takto: $P_1 = (\sqrt[3]{2}, 0)$, $P_2 = (\zeta\sqrt[3]{2}, 0)$. Pak

$$\rho_2(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \qquad \rho_2(\tau) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Body konečného řádu v aditivní grupě vhodné eliptické křivky lze užít ke konstrukci abelovských rozšíření kvadratického imaginárního tělesa podobně jako body konečného řádu v multiplikativní grupě jednotkové kružnice (tj. odmocniny z jedné) jsme využili ke konstrukci abelovských rozšíření racionálních čísel. Ukažme si tuto konstrukci v jednom speciálním případě, totiž pro těleso $\mathbb{Q}(i)$.

Uvažme eliptickou křivku $\mathcal{C} : y^2 = x^3 + x$. Zobrazení $\phi : \mathcal{C}(\mathbb{C}) \to \mathcal{C}(\mathbb{C})$ definované předpisem $\phi(O) = O$ a $\phi(P) = (-x, iy)$ pro $P = (x, y)$ je zřejmě grupový homomorfismus (uvědomte si, že grupová operace je definována tak, že body P a $-P$ jsou bodu se stejnou x-ovu a opačnou y-ovou souřadnicí a že platí $P_1 + P_2 + P_3 = O$ právě když body P_1, P_2, P_3 leží na jedné přímce; obě tyto podmínky zobrazení ϕ zachová). Protože $\phi(\phi(P)) = -P$ pro každé $P \in \mathcal{C}(\mathbb{C})$, je ϕ automorfismus grupy $\mathcal{C}(\mathbb{C})$.

Nechť $K/\mathbb{Q}$ je Galoisovo rozšíření takové, že $i \in K$ a nechť $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Víme, že σ určí automorfismus grupy $\mathcal{C}(K)$, zúžení ψ na $\mathcal{C}(K)$ je také automorfismem této grupy. Zjistěme, kdy platí $\sigma \circ \phi = \phi \circ \sigma$. Nechť $P = (x, y) \in \mathcal{C}(K)$ je libovolný. Pak platí

$$\sigma(\phi(P)) = \sigma(-x, iy) = (-\sigma(x), \sigma(i)\sigma(y)),$$
$$\phi(\sigma(P)) = \phi(\sigma(x), \sigma(y)) = (-\sigma(x), i\sigma(y)).$$

Podmínka $\sigma \circ \phi = \phi \circ \sigma$ je tedy splněna, jestliže $\sigma(i) = i$, tj. jestliže $\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i))$. Proto budeme moci využít ψ pro studium $\mathrm{Gal}(K/\mathbb{Q}(i))$.

Věta 1. Nechť $\mathcal{C}$ je eliptická křivka $y^2 = x^3 + x$. Pro každé přirozené číslo n označme $K_n = \mathbb{Q}(i)(\mathcal{C}[n])$ těleso generované i a souřadnicemi bodů křivky $\mathcal{C}$, jejichž řád dělí n. Pak platí: $K_n/\mathbb{Q}$ je Galoisovo rozšíření a grupa $\mathrm{Gal}(K_n/\mathbb{Q}(i))$ je komutativní.

Důkaz. Zvolíme-li pevně generátory P_1, P_2 grupy $\mathcal{C}(\mathbb{C})[n]$, určí ψ podmínkami

$$\psi(P_1) = aP_1 + bP_2 \qquad \psi(P_2) = cP_1 + dP_2$$

matici

$$A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Podle předchozího výpočtu víme, že pro libovolné $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q}(i))$ platí

$$A\rho_n(\sigma) = \rho_n(\sigma)A.$$

Protože ρ_n je vnoření, plyne věta z následujících lemmat.

Lemma 1. Nechť A je jako ve větě, ℓ prvočíslo dělící n. Pak A není skalární matice modulo ℓ, tj. je splněna aspoň jedna z podmínek

$$b \not\equiv 0 \pmod{\ell}, \qquad c \not\equiv 0 \pmod{\ell}, \qquad a \not\equiv d \pmod{\ell}.$$

Důkaz. Předpokládejme naopak, že pro nějaké prvočíslo $\ell | n$ a nějaké přirozené číslo m platí

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} \pmod{\ell}.$$

Pak pro každé $P \in \mathcal{C}[\ell]$ platí $\phi(P) = mP$. Označme τ prvek $\mathrm{Gal}(K_n/\mathbb{Q})$ odpovídající komplexní konjugovanosti (při nějakém zafixovaném vložení $K_n \to \mathbb{C}$). Protože $\tau(i) = -i$, pro libovolné $P = (x, y) \in \mathcal{C}[\ell]$ platí

$$\tau(\phi(P)) = \tau(-x, iy) = (\tau(-x), \tau(iy)) = (-\tau(x), -i\tau(y)) = -\phi(\tau(P)),$$

a tedy

$$m\tau(P) = \tau(mP) = \tau(\phi(P)) = -\phi(\tau(P)) = -m\tau(P),$$

odkud $2m\tau(P) = O$ pro každé $P \in \mathcal{C}[\ell]$, a tedy $2mP = O$ pro každé $P \in \mathcal{C}[\ell]$, neboť τ jen permutuje prvky $\mathcal{C}[\ell]$. Platí tedy $\ell | 2m$. Kdyby $\ell | m$, platilo by $\phi(P) = O$ pro každé $\mathcal{C}[\ell]$, což není možné, neboť $\phi(\phi(P) = -P$. Je tedy $\ell = 2$, což se snadno vyvrátí výpočtem: v označení příkladu 2 odpovídá ϕ matice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Lemma 2. Nechť $A \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ je matice, která A není skalární maticí modulo ℓ pro žádné prvočíslo ℓ dělící n. Pak

$$\{B \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \ AB = BA\}$$

je abelovská podgrupa grupy $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Důkaz. Lze snadno (i když poněkud zdlouhavě) provést metodami lineární algebry (viz Silverman, Tate, Rational points on elliptic curves, str. 208-210).

Poznámka. Námi dokázanou větu 1 lze obrátit, značně hluboká je následující věta (srovnejte s větou Kroneckera-Webera).

Věta 2. Nechť $\mathcal{C}$ je eliptická křivka $y^2 = x^3 + x$. Pro každé přirozené číslo n označme $K_n = \mathbb{Q}(i)(\mathcal{C}[n])$ těleso generované i a souřadnicemi bodů křivky $\mathcal{C}$, jejichž řád dělí n. Pak platí: pro libovolné Galoisovo rozšíření $F/\mathbb{Q}(i)$ takové, že $\mathrm{Gal}(F/\mathbb{Q}(i))$ je komutativní, existuje přirozené číslo n tak, že $F \subseteq K_n$.

Poznámka. Pokusme se stručně shrnout, jak vypadá zobecnění vět 1 a 2 pro ostatní imaginární kvadratická tělesa. Nejprve zmiňme výsledek tzv. „class field theory“ (český překlad „teorie těles tříd“ se nevžil). Nechť K je těleso algebraických čísel. Pak existuje těleso H, které je největší těleso obsahující K takové, že H/K je Galoisovo rozšíření s komutativní Galoisovou grupou a současně v H/K není rozvětvený žádný prvodivizor tělesa K. Těleso H se nazývá Hilbertovo těleso tříd tělesa K a jeho nejdůležitější vlastnost je ta, že grupa tříd divizorů tělesa K je izomorfní s Galoisovou grupou $\mathrm{Gal}(H/K)$, přičemž izomorfismus je dán Artinovým zobrazením (viz kapitolu 13).

Nechť K je nyní libovolné imaginární kvadratické těleso, R jeho okruh celých čísel. Pak R je mřížka v $\mathbb{C}$, proto pomocí vzorců z úvodu kapitoly pro $L = R$ dostaneme komplexní čísla g_2, g_3 a tedy i eliptickou křivku

$$\mathcal{E} : \quad y^2 = 4x^3 - g_2 x - g_3$$

s diskriminantem $\Delta = g_2^3 - 27g_3^2$ a tzv. j-invariantem $j = \frac{1728g_2^3}{\Delta}$. Tato křivka je analyticky izomorfní (tj. biracionálně ekvivalentní, přičemž neutrální bod jedné křivky je převáděn na neutrální bod druhé) s eliptickou křivkou zadanou rovnicí s koeficienty v $K(j)$, konkrétně s

$$\mathcal{E}' : \quad y^2 + xy = x^3 - \tfrac{36}{j-1728}x - \tfrac{1}{j-1728},$$

je-li $j \neq 0$, $j \neq 1728$ (pro $j = 0$ je třeba vzít křivku danou rovnicí $y^2 + y = x^3$, pro $j = 1728$ zase nám známou $y^2 = x^3 + x$).

Pak platí, že j je celé algebraické číslo, že $[K(j) : K] = [\mathbb{Q}(j) : \mathbb{Q}]$ a že $H = K(j)$ je Hilbertovo těleso tříd tělesa K.

Pro libovolné přirozené číslo n označme $H_n = H(\mathcal{E}'[n])$. Pak platí, že H_n/K je Galoisovo rozšíření a $\mathrm{Gal}(H_n/H)$ je komutativní (přitom $\mathrm{Gal}(H_n/K)$ být komutativní nemusí). Naopak, libovolné abelovské rozšíření tělesa K je podtělesem tělesa H_n pro vhodné n. Všimněte si, že pro $j = 1728$ jde o obsah vět 1 a 2, pro obecnější případ, kdy $j \in \mathbb{Q}$, jde o jejich přesnou analogii. Jestliže však $j \notin \mathbb{Q}$, platí $H \neq K$. Situaci však lze pro $j \notin \mathbb{Q}$ zachránit takto: místo tělesa H_n uvažujeme těleso H'_n vzniklé přidáním k H nikoli obou souřadnic těch bodů $\mathcal{E}'$, jejichž řád dělí n, ale jen x-ových souřadnic těchto bodů. Pak abelovská rozšíření tělesa K jsou právě podtělesa těles H'_n.

23. Modulární křivky

Uvažme dvě eliptické křivky $\mathcal{E}_1$, $\mathcal{E}_2$ a jim odpovídající mřížky L_1, L_2. Platí věta tvrdící, že $\mathcal{E}_1$ je analyticky izomorfní s $\mathcal{E}_2$, právě když mřížky L_1 a L_2 jsou podobné (tj. existuje nenulové $\alpha \in \mathbb{C}$ tak, že $L_1 = \alpha L_2$).

Pro danou mřížku L a dané přirozené číslo $k > 1$ označme

$$G_{2k}(L) = \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^{2k}}$$

(srovnejte s g_2, g_3 ze začátku kapitoly 22). Dále položme

$$\Delta(L) = (60G_4(L))^3 - 27(140G_6(L))^2, \qquad j(L) = 1728(60G_4(L))^3(\Delta(L))^{-1}$$

(všimněte si, že $\Delta(L)$ je diskriminant a $j(L)$ je j-invariant eliptické křivky odpovídající mřížce L).

Snadno se ověří, že platí

$$G_{2k}(\alpha L) = \alpha^{-2k}G_{2k}(L), \qquad \Delta(\alpha L) = \alpha^{-12}\Delta(L), \qquad j(\alpha L) = j(L).$$

Definiční obor těchto funkcí je množina mřížek. Je jasné, že funkci j lze uvažovat na rozkladu množiny mřížek podle ekvivalence dané podobností. (Poznamenejme, že všechny uvedené funkce jsou příklady tzv. modulárních forem.)

Označme

$$\mathbb{H} = \{\tau \in \mathbb{C};\ \mathrm{Im}(\tau) > 0\}, \qquad \text{a} \qquad L_\tau = \mathbb{Z} + \mathbb{Z}\tau$$

pro $\tau \in \mathbb{H}$. Dále položme

$$G_{2k}(\tau) = G_{2k}(L_\tau), \qquad \Delta(\tau) = \Delta(L_\tau), \qquad j(\tau) = j(L_\tau).$$

Je zřejmé, že každá mřížka je podobná s L_τ pro vhodné $\tau \in \mathbb{H}$. Promysleme si, kdy jsou dvě mřížky L_τ, $L_{\tau'}$ pro $\tau, \tau' \in \mathbb{H}$ podobné. Je to právě tehdy, když existuje nenulové $\alpha \in \mathbb{C}$ tak, že $\mathbb{Z}\alpha + \mathbb{Z}\alpha\tau' = \mathbb{Z} + \mathbb{Z}\tau$, tj. právě když existují $a, b, c, d \in \mathbb{Z}$ tak, že

$$\tau'\alpha = a\tau + b, \qquad \alpha = c\tau + d$$

a $ad - bc = \pm 1$. Přitom podmínka $\tau, \tau' \in \mathbb{H}$ implikuje $ad - bc > 0$. Jsou tedy L_τ, $L_{\tau'}$ pro $\tau, \tau' \in \mathbb{H}$ podobné, právě když $\tau' = \frac{a\tau+b}{c\tau+d}$, kde $a, b, c, d \in \mathbb{Z}$ splňují $ad - bc = 1$. Dostáváme tedy, že grupa

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; \, a, b, c, d \in \mathbb{Z}, \, ad - bc = 1 \right\}$$

účinkuje na $\mathbb{H}$ transformací

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathbb{H} \to \mathbb{H} \qquad \gamma(\tau) = \frac{a\tau + b}{c\tau + d}.$$

Přitom zřejmě triviální účinek mají pouze matice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Faktorizací podle podgrupy mající tyto dva prvky dostaneme tzv. modulární grupu $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$.

Tvrzení. Pro zmíněnou akci $\mathrm{SL}_2(\mathbb{Z})$ na $\mathbb{H}$ platí:

(a) Pro libovolné $\tau \in \mathbb{H}$ existuje jeho okolí U tak, že pro libovolné $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma \neq \pm\gamma'$ platí, že γU a $\gamma' U$ jsou disjunktní.

(b) Oblast $F = \{\tau \in \mathbb{H}; \, |\mathrm{Re}(\tau)| \leq \frac{1}{2}, \, |\tau| \geq 1\}$ je fundamentální oblastí pro $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$, tj. kanonické zobrazení $F \to \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ je surjekce a jeho restrikce na vnitřek F je injekce.

(c) Označme $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$; pak $S^2 = -1$ a $(ST)^3 = -1$. Platí, že $\mathrm{PSL}_2(\mathbb{Z})$ je grupa generovaná prvky S a ST volně vzhledem k relacím $S^2 = 1$ a $(ST)^3 = 1$.

(d) Zobrazení

$$j : \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \to \mathbb{C}$$

je komplexní analytický izomorfismus (otevřených) Riemannových ploch.

Máme tedy bijekci mezi Riemannovou plochou $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ a rozkladem množiny všech eliptických křivek nad $\mathbb{C}$ na třídy analyticky izomorfních křivek. Pro libovolné $\tau \in \mathbb{H}$ bodu $\tau \,(\mathrm{mod}\, \mathrm{SL}_2(\mathbb{Z}))$ odpovídá třída eliptických křivek analyticky izomorfních s $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$. Přitom platí, že v této třídě existuje eliptická křivka s rovnicí s koeficienty z tělesa $\mathbb{Q}(j(\tau))$.

Definice. Pro libovolné přirozené číslo n definujme podgrupu $\Gamma_0(N)$ grupy $\mathrm{SL}_2(\mathbb{Z})$ takto:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}); \, N | c \right\}.$$

Uvažme nyní $\mathbb{H}/\Gamma_0(N)$. Pak máme přirozené zobrazení $\mathbb{H}/\Gamma_0(N) \to \mathbb{H}/\operatorname{SL}_2(\mathbb{Z})$ a tedy opět libovolnému $\tau \in \mathbb{H}$ bodu $\tau \,(\mathrm{mod}\, \Gamma_0(N))$ máme přiřazenu třídu eliptických křivek analyticky izomorfních s $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$. Toto zobrazení samozřejmě pro $N > 1$ už není bijekce. Bod $\tau \,(\mathrm{mod}\, \Gamma_0(N))$ v sobě obsahuje ještě další informaci. Ukažme si jakou. Zvolme pevně

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

a uvažme zobrazení $f : \mathbb{C} \to \mathbb{C}$ dané předpisem $f(z) = \frac{z}{c\tau+d}$. Protože $\mathbb{Z}+\mathbb{Z}\tau = \mathbb{Z}(a\tau+b)+\mathbb{Z}(c\tau+d)$, platí $f(\mathbb{Z}+\mathbb{Z}\tau) = \mathbb{Z}+\mathbb{Z}\gamma(\tau)$ a tedy f indukuje zobrazení

$$\bar{f} : \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau) \to \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\gamma(\tau)).$$

Zřejmě $\{0, \frac{1}{N}, \frac{2}{N}, \ldots, \frac{N-1}{N}\}$ je podgrupa řádu N grupy $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$. Ukážeme, že platí $\bar{f}(\frac{t}{N} \,(\mathrm{mod}\, \mathbb{Z}+\mathbb{Z}\tau)) = \frac{at}{N} \,(\mathrm{mod}\, \mathbb{Z}+\mathbb{Z}\gamma(\tau))$. Totiž $N|bc = 1-ad$ a platí

$$f\big(\frac{t}{N}\big) - \frac{at}{N} = \frac{t}{N(c\tau+d)} - \frac{at}{N} = \frac{(at\frac{c}{N})\tau - t\frac{1-ad}{N}}{c\tau+d} \in f(\mathbb{Z}+\mathbb{Z}\tau) = \mathbb{Z}+\mathbb{Z}\gamma(\tau).$$

Dostali jsme, že akce libovolného $\gamma \in \Gamma_0(N)$ nechává podgrupu $\{0, \frac{1}{N}, \frac{2}{N}, \ldots, \frac{N-1}{N}\}$ na místě. Je však možné dokázat více, jak ukazuje následující věta.

Věta. Nechť $N \in \mathbb{N}$. Existuje hladká afinní křivka $Y_0(N)$ definovaná nad $\mathbb{Q}$ (tj. určena polynomiálními rovnicemi s racionálními koeficienty) a komplexní analytický izomorfismus

$$j_N : \mathbb{H}/\Gamma_0(N) \to Y_0(N)$$

takový, že platí: nechť $\tau \in \mathbb{H}/\Gamma_0(N)$ a nechť $K = \mathbb{Q}(j_N(\tau))$, pak τ jednoznačně odpovídá jisté třídě rozkladu množiny všech dvojic $(\mathcal{E}, C)$, kde $\mathcal{E}$ je eliptická křivka nad $\mathbb{C}$ a C její cyklická podgrupa řádu N, podle ekvivalence $\sim$ dané podmínkou $(\mathcal{E}, C) \sim (\mathcal{E}', C')$, právě když existuje analytický izomorfismus $\mathcal{E} \to \mathcal{E}'$ zobrazující C na C'. V této třídě existuje dvojice $(\mathcal{E}, C)$ taková, že rovnice $\mathcal{E}$ má koeficienty v K a body z C mají souřadnice v K.

Komplexní přímka $\mathbb{C} = Y_0(1)$ má přirozenou kompaktifikaci – projektivní přímku $P^1(\mathbb{C})$, vzniklou přidáním jediného bodu k $\mathbb{C}$. Proto je jasné, že přirozenou kompaktifikací $\mathbb{H}/\operatorname{SL}_2(\mathbb{Z})$ dostaneme přidáním jediného bodu. Podobně ke křivce $Y_0(N)$ existuje její přirozená kompaktifikace $X_0(N)$. Křivka $X_0(N)$ je příkladem tzv. modulárních křivek. Některé modulární křivky jsou samy eliptické (například $X_0(11)$ je eliptická křivka), pro některé další existuje surjektivní zobrazení $\phi : X_0(N) \to \mathcal{E}$ definované pomocí polynomů s racionálními koeficienty do nějaké eliptické křivky $\mathcal{E}$ nad $\mathbb{Q}$ (tj. $\mathcal{E}$ je určena rovnicí s racionálními koeficienty). Pokud pro eliptickou křivku $\mathcal{E}$ nad $\mathbb{Q}$ pro nějaké N takové zobrazení ϕ existuje, řekneme, že $\mathcal{E}$ je Weilova křivka. Je jasné, že Weilova křivka je bohatší o strukturu modulární křivky přenesenou na ni zobrazením ϕ a že tuto strukturu bude asi možné využít při studiu aritmetiky této křivky.

Hypotéza (Taniyama – Weil). Každá eliptická křivka definovaná nad $\mathbb{Q}$ je Weilova křivka.

Nedávno byla tato hypotéza dokázána pro tzv. semistabilní eliptické křivky A. Wilesem.

Definice. Pro danou eliptickou křivku $\mathcal{E}$ definovanou nad $\mathbb{Q}$ vyberme mezi všemi eliptickými křivkami, které jsou s ní izomorfní nad $\mathbb{Q}$ (tj. izomorfismus je zadán pomocí polynomů s racionálními koreficienty) a jejichž rovnice má celočíselné koeficienty, tu eliptickou křivku, která má nejmenší absolutní hodnotu diskriminantu. Pro libovolné prvočíslo p můžeme koeficienty této rovnice nahradit příslušnou zbytkovou třídou modulo p a uvažovat tak tuto rovnici nad tělesem $\mathbb{Z}/p\mathbb{Z}$. Pokud p nedělí diskriminant vybrané eliptické křivky, získaná rovnice je rovnicí eliptické křivky nad $\mathbb{Z}/p\mathbb{Z}$. Pokud naopak p dělí zmíněný diskriminant, určí získaná rovnice kubickou singulární křivku nad $\mathbb{Z}/p\mathbb{Z}$. Taková křivka má právě jeden singulární bod, v němž má buď dvě různé tečny nebo jednu dvojnásobnou tečnu. Řekneme, že $\mathcal{E}$ je semistabilní, jestliže pro žádné prvočíslo p nenastane případ dvojnásobné tečny.

Z Wilesova důkazu hypotézy Taniyamy a Weila byla jako důsledek získána velká Fermatova věta; už dříve se vědělo, že z případného protipříkladu k velké Fermatově větě lze konstruovat příklad semistabilní eliptické křivky, která nemůže být modulární (viz přiložený Rokytův překlad pořadu odvysílaného BBC pro pro širší veřejnost, další podrobnosti lze najít v článku J. Nekováře „Modulární křivky a Fermatova věta“, Mathematica Bohemica 119 (1994), str. 79-96, kterým doplňuje zprávu K. A. Ribeta „Wiles dokázal Taniyamovu hypotézu; důsledkem je Fermatova věta“, str. 75-78 tamtéž).

Literatura

Z. I. Borevič, R. I. Šafarevič: Teorie čísel, Nauka, Moskva 1964

J. H. Silverman, J. Tate: Rational points on Elliptic Curves, UTM, Springer, 1992.

J. H. Silverman: The arithmetic of elliptic curves, GTM 106, Springer, 1986.

I. Stewart: Galois Theory, second edition, T. J. Press, Padstow (Great Britain) 1989

L. Washington: Introduction to Cyclotomic Fields, GTM 83, Springer-Verlag 1982, 1996