Masarykova Univerzita
Přírodovědecká fakulta

Stickelbergerův ideál

Diplomová práce

Tomáš Hanžl

2004

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně s využitím uvedených literárních zdrojů.

Poděkování

Děkuji doc. RNDr. Radanu Kučerovi, CSc. za cenné rady a připomínky.

Obsah

1 Úvod

Při řešení diofantických rovnic je často užitečné pracovat s většími okruhy než jsou celá čísla. Ukazuje se, že takovými okruhy jsou okruhy celých algebraických čísel v konečných rozšířeních racionálních čísel. V těchto okruzích obecně neplatí věta o jednoznačnosti rozkladu na prvočinitele, platí zde však jednoznačnost rozkladu nenulových ideálů na prvoideály. Je proto přirozené pracovat s hlavními ideály namísto prvků příslušného okruhu. Z nejednoznačnosti rozkladů též vyplývá, že ne každý ideál je hlavní. Pologrupu nenulových ideálů můžeme rozložit podle podpologrupy hlavních ideálů a získat tzv. grupu tříd ideálů. Grupa tříd ideálů není dána explicitně, proto jsou jakékoli informace o ní užitečné. Těmito informacemi mohou být např. její anihilátory, tj. automorfismy, které aplikací na libovolný ideál dávají ideál hlavní. Stickelbergerův ideál je ideálem grupového okruhu nad Galoisovou grupou zmíněného algebraického rozšíření, který právě takovéto anihilátory obsahuje.

Cílem této práce je kompaktní formou prezentovat Stickelbergerův ideál a jeho rozšířenou verzi definovanou W. Sinnottem a dokázat, že prvky Stickelbergerova ideálu jsou anihilátory grupy tříd ideálů.

Od čtenáře se předpokládá základní znalost algebraických struktur v rozsahu magisterského studia algebry a Galoisovy teorie. Je třeba se orientovat v teorii grup, okruhů a těles. Též je vhodné znát pojmy modul a vektorový prostor.

2 Nezbytné minimum z algebry

U čtenáře předpokládáme znalosti algebry v rozsahu publikace [7]. Dále předpokládáme základní znalosti z teorie rozšíření těles a Galoisovy teorie, přesto potřebné výsledky stručně shrneme v této kapitole. Všechna tvrzení uvedeme bez důkazů. Úvod do teorie těles lze nastudovat např. z [1]. Základy Galoisovy teorie pak např. z [1] nebo z [6].

2.1 Rozšíření těles

Připomeňme, že *těleso* F je komutativní okruh s jedničkou, kde má každý nenulový prvek inverzi vzhledem k násobení.

Definice. *Charakteristika tělesa* $\mathrm{char}(F)$ je definována jako nejmenší přirozené číslo p splňující $p \cdot 1 = 0$, pokud takové p existuje. V opačném případě klademe $\mathrm{char}(F) = 0$. Snadno se vidí, že charakteristika tělesa je buď nula nebo prvočíslo.

Definice. Podtěleso tělesa F generované jedničkou se nazývá *základní těleso* tělesa F. Je-li $\mathrm{char}(F) = 0$, je základní těleso izomorfní s $\mathbb{Q}$, pro $\mathrm{char}(F) = p$ je základní těleso izomorfní se $\mathbb{Z}/p\mathbb{Z}$.

Definice. Je-li F podtěleso nějakého tělesa E, říkáme, že E je *rozšířením tělesa* F, nebo též, že E/F je *rozšíření těles*. Vždy lze E chápat jako vektorový prostor nad F. Jeho dimenzi nazýváme *stupeň rozšíření*, značíme $[E : F]$.

Pohled na E/F jako na vektorový prostor nám dovoluje používat termíny z lineární algebry jako jsou např. báze nebo lineární nezávislost.

Je-li E/F rozšíření těles a $\alpha \in E$, pak nejmenší podtěleso E obsahující F i α značíme $F(\alpha)$. Obdobně značení rozšíříme i pro více prvků z tělesa E.

Definice. Nechť jsou K_1 a K_2 podtělesa tělesa K. Nejmenší podtěleso tělesa K, které obsahuje K_1 i K_2 nazýváme *kompozitum* těles K_1 a K_2, značíme K_1K_2. Zřejmě se jedná o průnik všech takových podtěles tělesa K.

Definice. Nechť E/F je rozšíření těles a nechť $f(x)$ je polynom s koeficienty v F. Těleso E nazveme *rozkladové těleso* polynomu $f(x)$, pokud se $f(x)$ v E dá rozložit na součin lineárních polynomů a v žádném vlastním podtělese tělesa E se takto rozložit nedá.

Platí, že pro libovolné těleso F a polynom $f(x) \in F[x]$ existuje rozšíření E tělesa F, které je rozkladovým tělesem polynomu $f(x)$. Toto těleso je navíc určeno jednoznačně až na izomorfismus, jehož zúžení na F je identita.

Definice. Polynom nad tělesem F se nazývá *separabilní*, pokud ve svém rozkladovém tělese nemá násobné kořeny. Rozšíření E/F se nazývá separabilní, je-li každý prvek tělesa E kořenem nějakého separabilního polynomu z $f(x) \in F[x]$.

Nad tělesem charakteristiky 0 je každý ireducibilní polynom separabilní. Nad tělesem charakteristiky p je ireducibilní polynom $f(x)$ separabilní, právě když není tvaru $f(x) = g(x^p)$ pro žádný polynom $g(x)$.

Každé konečné rozšíření konečného tělesa je separabilní. Konečná rozšíření $\mathbb{Q}$ jsou rovněž separabilní.

2.2 Základy Galoisovy teorie

Galoisova teorie zkoumá automorfismy těles. Přesněji, je-li E/F konečné rozšíření těles, $\mathrm{Aut}(E/F)$ je množina automorfismů $E \to E$, které jsou na F identické. Snadno se ověří, že $\mathrm{Aut}(E/F)$ spolu s operací skládání zobrazení tvoří grupu.

Je-li H podgrupa grupy $\mathrm{Aut}(E/F)$, tvoří množina prvků E, které všechny automorfismy z H nechávají na místě, podtěleso tělesa E. Nazýváme jej *fixní těleso* grupy H.

Definice. Je-li $|Aut(E/F)| = [E : F] \in \mathbb{N}$, říkáme, že je rozšíření E/F *Galoisovo* a grupu automorfismů $\mathrm{Aut}(E/F)$ nazýváme jeho *Galoisovou grupou*. Značíme $\mathrm{Gal}(E/F)$.

Věta 2.2.1. *Rozšíření E/F je Galoisovo právě tehdy, když je E rozkladovým tělesem nějakého separabilního polynomu nad F.*

Věta 2.2.2. *Je-li E/F konečné rozšíření konečných těles, je Galoisova grupa* $\mathrm{Gal}(E/F)$ *cyklická, generovaná tzv.* Frobeniovým automorfismem*, což je zobrazení*

$$a \mapsto a^q,$$

kde $q = |F|$.

Věta 2.2.3 (Hlavní věta Galoisovy teorie). *Nechť E/F je Galoisovo rozšíření s Galoisovou grupou G. Pak existuje bijekce mezi tělesy K splňující $F \subseteq K \subseteq E$ a podgrupami H grupy G daná vztahy*

$$K \;\to\; \begin{array}{c}\textit{podgrupa grupy } G \textit{ obsahující prvky}\\ \textit{které jsou na } K \textit{ identitami}\end{array}$$

$$\textit{fixní těleso grupy } H \;\leftarrow\; H.$$

Tyto vztahy jsou navzájem inverzní a nazývají se Galoisova korespondence*. Nechť těleso K odpovídá podgrupě H. Platí*

(1) *Pokud podtělesa K_1 a K_2 odpovídají po řadě podgrupám H_1 a H_2, platí $K_1 \subseteq K_2$ právě tehdy, když $H_1 \supseteq H_2$.*
(2) *$[E : K] = |H|$ a $[K : F] = [G : H]$, kde $[G : H]$ je index podgrupy G v H (tj. počet levých tříd rozkladu G/H).*
(3) *E/K je vždy Galoisovo s Galoisovou grupou H.*
(4) *K/F je Galoisovo, právě když je H normální podgrupou grupy G. V tomto případě je Galoisova grupa $Gal(K/F)$ izomorfní s faktorgrupou G/H.*

(5) *Nechť podtělesa K_1 a K_2 odpovídají po řadě podgrupám H_1 a H_2. Pak průnik $K_1 \cap K_2$ odpovídá grupě $\langle H_1, H_2 \rangle$ generované oběma grupami a kompozitum K_1K_2 odpovídá průniku $H_1 \cap H_2$. Svaz všech podtěles tělesa E obsahujících F je tedy duální ke svazu všech podgrup grupy G.*

Následující tvrzení bude velmi užitečné v kapitole 5

Věta 2.2.4. *Nechť K_1, K_2 jsou podtělesa nějakého tělesa K taková, že obě rozšíření $K_1/(K_1 \cap K_2)$, $K_2/(K_1 \cap K_2)$ jsou Galoisova. Pak jsou Galoisova i rozšíření K_1K_2/K_1 a K_1K_2/K_2 a platí*

$$\mathrm{Gal}(K_1K_2/K_1) \cong \mathrm{Gal}(K_2/(K_1 \cap K_2)), \qquad \mathrm{Gal}(K_1K_2/K_2) \cong \mathrm{Gal}(K_1/(K_1 \cap K_2))$$

Věta 2.2.5. *Nechť E/F je Galoisovo rozšíření a $F \subseteq K \subseteq E$ je takové, že K/F je též Galoisovo. Pak pro libovolný automorfismus $\sigma \in \mathrm{Gal}(E/F)$ platí, že jeho* restrikce $\sigma|_K$ *je automorfismus z* $\mathrm{Gal}(K/F)$.

Definice. Označme $\zeta_n = e^{2\pi i/n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ primitivní n-tou odmocninu z jedné. Rozšíření $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ je Galoisovo (to dokážeme v odstavci 3.5) a budeme jej nazývat *n-té kruhové rozšíření.*

Definice. Rozšíření E/F nazveme *abelovské*, je-li grupa $\mathrm{Gal}(E/F)$ abelovská, tj. komutativní.

Následující větu lze najít např. v [2].

Věta 2.2.6 (Kronecker-Weber). *Těleso F je abelovské rozšíření $\mathbb{Q}$ právě tehdy, když je obsaženo v nějakém kruhovém rozšíření $\mathbb{Q}$.*

Průnik dvou kruhových rozšíření je opět kruhové rozšíření. Nejmenší takové m, že $F \subseteq \mathbb{Q}(\zeta_m)$ nazveme *konduktor* tělesa F.

3 Algebraická teorie čísel

V této kapitole poskytneme základy algebraické teorie čísel. V prvních dvou odstavcích uvedeme základní pojmy a jejich vlastnosti. Ve zbytku kapitoly se budeme věnovat faktorizaci ideálů v konečných rozšířeních racionálních čísel. Zvláště se zaměříme na kruhová tělesa.

Všechny výsledky uvedené v této kapitole lze najít např. v [3].

3.1 Algebraická a celá algebraická čísla

V první části této kapitoly se budeme věnovat algebraickým a celým algebraickým číslům. Hlavními výsledky budou tvrzení, že algebraická čísla tvoří těleso a celá algebraická čísla okruh.

Definice. Komplexní číslo α nazveme *algebraické*, je-li kořenem nějakého polynomu s racionálními koeficienty.

Komplexní číslo α nazveme *celé algebraické*, je-li kořenem nějakého normovaného polynomu (tj. polynomu s koeficientem u nejvyšší mocniny rovným jedné) s celočíselnými koeficienty.

Ukážeme, že charakteristickou vlastností celých algebraických čísel je to, že jejich minimální polynomy mají celočíselné koeficienty.

Lemma 3.1. *Nechť $f(x), g(x)$ jsou polynomy s celočíselnými koeficienty a nechť p je prvočíslo, které dělí všechny koeficienty polynomu $fg(x)$. Pak p dělí všechny koeficienty jednoho z polynomů $f(x), g(x)$.*

Důkaz. Označme $f(x) = a_s x^s + \cdots + a_1 x + a_0$, $g(x) = b_t x^t + \cdots + b_1 x + b_0$. Sporem předpokládejme, že existují i, j takové, že $p \nmid a_i$ a $p \nmid b_j$. Vezměme minimální takové i, j. Je ihned vidět, že koeficient u x^{i+j} polynomu $fg(x)$ není dělitelný p, což je spor. □

Tvrzení 3.1.1. *Algebraické číslo $\alpha \in \mathbb{C}$ je celé algebraické právě tehdy, když má jeho minimální polynom nad $\mathbb{Q}$ celočíselné koeficienty.*

Důkaz. Pokud má minimální polynom pro α celočíselné koeficienty, je podle definice α celé algebraické.

Naopak nechť $h(x) \in \mathbb{Z}[x]$ je normovaný polynom, jehož kořenem je α, který je minimálního stupně mezi všemi takovými polynomy ze $\mathbb{Z}[x]$. Minimální polynom $m(x)$ prvku α však musí dělit $h(x)$ (v opačném případě by jejich největší společný dělitel měl nižší stupeň než $m(x)$ a měl by kořen α). Sporem předpokládejme, že $h(x)$ není minimální, tedy existuje polynom $f(x) \in \mathbb{Q}[x]$ stupně alespoň jedna, takový, že $h(x) = m(x)f(x)$. Zřejmě jsou $m(x)$ i $f(x)$ normované. Nechť A, B jsou přirozená čísla taková, že $Am(x)$ a $Bf(x)$ jsou polynomy s celočíselnými koeficienty, jejichž největší společný dělitel je (v každém polynomu) roven jedné. Z definice $h(x)$ vidíme, že $A > 1$, proto existuje prvočíslo p dělící A. Celkově tak dostáváme, že p dělí všechny koeficienty součinu $Am(x) \cdot Bf(x)$, proto podle předchozího lemmatu dělí všechny koeficienty jednoho z polynomů $Am(x)$, $Bf(x)$, což je spor s volbou A, B. □

Přímým důsledkem tohoto faktu je následující tvrzení.

Tvrzení 3.1.2. *Racionální číslo r je celé algebraické právě tehdy, když je celé.*

Definice. Podmnožina $V \subseteq \mathbb{C}$ se nazývá $\mathbb{Q}$-*modul*, jestliže platí

(i) $\gamma_1, \gamma_2 \in V$ implikuje $\gamma_1 \pm \gamma_2 \in V$.
(ii) Je-li $\gamma \in V$ a $r \in \mathbb{Q}$, je i $r\gamma \in V$.
(iii) Existují čísla $\gamma_1, \gamma_2, \ldots, \gamma_l \in V$ taková, že lze každý prvek $\gamma \in V$ psát ve tvaru $\gamma = \sum_{i=1}^{l} r_i\gamma_i$, kde $r_i \in \mathbb{Q}$.

Jinak řečeno $V \subseteq \mathbb{C}$ je $\mathbb{Q}$-modul, pokud je to konečněrozměrný vektorový prostor nad $\mathbb{Q}$.

Jsou-li $\gamma_1, \ldots, \gamma_l \in \mathbb{C}$, snadno se vidí, že množina $\{\sum_{i=1}^{l} r_i\gamma_i | r_i \in \mathbb{Q}\}$ je $\mathbb{Q}$-modul; budeme jej značit $[\gamma_1, \ldots, \gamma_l]$.

Tvrzení 3.1.3. *Nechť $V = [\gamma_1, \ldots, \gamma_l]$ a nechť α je komplexní číslo s vlastností $\alpha\gamma \in V$ pro všechna $\gamma \in V$. Pak je α algebraické číslo.*

Důkaz. $\alpha\gamma_i \in V$ pro $i = 1, 2, \ldots, l$. Tedy $\alpha\gamma_i = \sum_{j=1}^{l} a_{ij}\gamma_j$, kde $a_{ij} \in \mathbb{Q}$. Odsud $0 = \sum_{j=1}^{l}(a_{ij} - \delta_{ij}\alpha)\gamma_j$, kde $\delta_{ij} = 0$ pro $i \neq j$ a $\delta_{ij} = 1$ pro $i = j$. Matice $(a_{ij} - \delta_{ij}\alpha)$ je tedy singulární a její determinant je roven nule. Rozepsáním determinantu vidíme, že α je kořenem polynomu stupně l a je tedy algebraické číslo. □

Tvrzení 3.1.4. *Množina všech algebraických čísel tvoří podtěleso $\mathbb{C}$.*

Důkaz. Nechť jsou α_1, α_2 algebraická čísla. Ukážeme, že pak jsou algebraická i čísla $\alpha_1 + \alpha_2$ a $\alpha_1\alpha_2$.

Nechť je α_1 kořenem nějakého polynomu stupně r s racionálními koeficienty a α_2 je kořenem nějakého polynomu stupně s s racionálními koeficienty. Označme $\mathbb{Q}$-modul generovaný součiny $\alpha_1^i\alpha_2^j$, kde $0 \leq i < r$ a $0 \leq j < s$, jako V. Snadno se ukáže, že pro libovolné $\gamma \in V$ je $\alpha_1\gamma \in V$ a $\alpha_2\gamma \in V$. Tedy i $(\alpha_1 + \alpha_2)\gamma \in V$ a $(\alpha_1\alpha_2)\gamma \in V$. Pomocí tvrzení 3.1.3 tak dostáváme, že jsou $\alpha_1 + \alpha_2$ i $\alpha_1\alpha_2$ skutečně algebraická čísla.

Konečně, je-li $\alpha \neq 0$ algebraické číslo, musíme ukázat, že i α^{-1} je algebraické. Nechť $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, kde všechna $a_i \in \mathbb{Q}$. Pak $a_0(\alpha^{-1})^n + a_1(\alpha^{-1})^{n-1} + \cdots + a_{n-1}\alpha^{-1} + a_n = 0$. Proto je α^{-1} také algebraické. □

K důkazu, že celá algebraická čísla tvoří okruh, stačí mírně modifikovat předchozí úvahy.

Definice. Podmnožina $W \subseteq \mathbb{C}$ se nazývá $\mathbb{Z}$-*modul*, jestliže platí

(i) $\gamma_1, \gamma_2 \in W$ implikuje $\gamma_1 \pm \gamma_2 \in W$.
(ii) Existují čísla $\gamma_1, \gamma_2, \ldots, \gamma_l \in W$ taková, že lze každý prvek $\gamma \in W$ psát ve tvaru $\gamma = \sum_{i=1}^{l} b_i\gamma_i$, kde $b_i \in \mathbb{Z}$.

Tvrzení 3.1.5. *Nechť W je $\mathbb{Z}$-modul a nechť je ω komplexní číslo s vlastností $\omega\gamma \in W$ pro všechna $\gamma \in W$. Pak je ω celé algebraické číslo.*

Důkaz. Důkaz se provede stejně jako v případě tvrzení 3.1.3 s tím rozdílem, že nyní je $a_{ij} \in \mathbb{Z}$. Rozepsáním determinantu v rovnosti $\det(a_{ij} - \delta_{ij}\omega) = 0$ dostaneme, že ω je kořenem normovaného polynomu c celočíselnými koeficienty a je tedy celé algebraické. □

Tvrzení 3.1.6. *Množina celých algebraických čísel tvoří podokruh* $\mathbb{C}$.

Důkaz. Důkaz se provede s využitím předchozího tvrzení stejným způsobem, jako byl proveden důkaz tvrzení 3.1.4 s využitím tvrzení 3.1.3. □

Označme Ω *okruh celých algebraických čísel* . Podobně jako v $\mathbb{Z}$ můžeme i zde zavést pojem kongruence. Pro $\omega_1, \omega_2, \gamma \in \Omega$ je $\omega_1 \equiv \omega_2 \pmod{\gamma}$ pokud platí $\omega_1 - \omega_2 = \gamma\alpha$, kde $\alpha \in \Omega$. Důkazy všech formálních vlastností celočíselných kongruencí lze snadno rozšířit na Ω.

Ještě poznamenejme, že tato definice nekoliduje s definicí kongruence v $\mathbb{Z}$. Každá celočíselná kongruence totiž zřejmě platí i v Ω. Na druhou stranu, jsou-li a, b, c celá čísla, pro něž platí $a \equiv b \pmod{c}$ v Ω, je $a - b = c\alpha$, kde $\alpha \in \Omega$. Je tedy α celé algebraické číslo a zároveň racionální. Podle tvrzení 3.1.2 musí být celé.

Tvrzení 3.1.7. *Nechť* $\omega_1, \omega_2, \ldots \omega_l \in \Omega$ *a* $p \in \mathbb{Z}$ *je prvočíslo. Pak*

$$(\omega_1 + \omega_2 + \cdots + \omega_l)^p \equiv \omega_1^p + \omega_2^p + \cdots + \omega_l^p \pmod{p}$$

Důkaz. Zřejmě stačí provést důkaz pro $l = 2$, pro větší l lze snadno postupovat indukcí.

$(\omega_1 + \omega_2)^p = \sum_{k=0}^{p} \binom{p}{k} \omega_1^k \omega_2^{p-k}$. Snadno se vidí, že $p | \binom{p}{k}$ pro $1 \leq k \leq p-1$, proto jsou všechny členy s výjimkou krajních dělitelné p a celý součet je kongruentní $\omega_1^p + \omega_2^p$ modulo p. □

3.2 Norma, stopa, diskriminant

V tomto odstavci zavedeme některé důležité pojmy vztahující se k obecným konečným rozšířením těles.

Nechť L/K je konečné rozšíření těles; jeho stupeň označme $n = [L : K]$. Dále nechť $\alpha_1, \alpha_2, \ldots, \alpha_n$ je báze L jakožto vektorového prostoru nad K a $\alpha \in L$. Násobení prvkem α je zřejmě lineární transformace prostoru L, proto můžeme psát

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

kde $a_{ij} \in K$.

Definice. *Normu* α vzhledem k rozšíření L/K, značeno $N_{L/K}(\alpha)$, definujeme jako determinant matice (a_{ij}). *Stopu* α vzhledem k témuž rozšíření, $\mathrm{tr}_{L/K}(\alpha)$, definujeme jako stopu matice (a_{ij}), tj. $tr_{L/K}(\alpha) = a_{11} + a_{22} + \cdots + a_{nn}$.

Snadno se ověří, že norma ani stopa nezávisí na volbě báze. Pokud pracujeme s jedním rozšířením, zpravidla mluvíme pouze o normě či stopě prvku. V dalších úvahách, pokud nebude explicitně uvedeno jinak, bude rozšíření L/K zvoleno pevně, proto nebudeme vyznačovat rozšíření ani v indexech N a tr. Následující tvrzení jsou též snadno ověřitelná.

Je-li $\alpha, \beta \in L$ a $a \in K$, platí $N(\alpha\beta) = N(\alpha)N(\beta)$, $\mathrm{tr}(\alpha+\beta) = \mathrm{tr}(\alpha) + \mathrm{tr}(\beta)$, $N(a\alpha) = a^n N(\alpha)$, $tr(a\alpha) = a\,\mathrm{tr}(\alpha)$. Pokud je tedy $\alpha \neq 0$, je $N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$. Odsud je-li $\alpha \neq 0$, je $N(\alpha) \neq 0$ a $N(\alpha^{-1}) = N(\alpha)^{-1}$.

Nechť L/K je Galoisovo rozšíření s Galoisovou grupou G. Označme $m(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$ minimální polynom pro $\alpha \in L$ nad K. Prvky $1, \alpha, \alpha^2, \ldots, \alpha^{k-1}$ tvoří bázi rozšíření $K(\alpha)/K$. Nechť $\gamma_1, \gamma_2, \ldots, \gamma_m \in K$, kde $m = n/k$, tvoří bázi rozšíření $L/K(\alpha)$. Pak prvky $\alpha^i\gamma_j$ pro $0 \leq i \leq k-1$ a $1 \leq j \leq m$ tvoří jistě bázi rozšíření L/K. Vzhledem k této bázi je matice lineárního zobrazení odpovídajícího násobení prvkem α blokově diagonální s m bloky

$$B = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & 0 & 1 \\ -b_0 & -b_1 & -b_2 & \cdots & -b_{k-1} \end{pmatrix}$$

odkud

$$N_{L/K}(\alpha) = ((-1)^n b_0)^m = \prod_{i=1}^{k} \alpha_i^m \quad \text{a}$$

$$\mathrm{tr}_{L/K}(\alpha) = -mb_{k-1} = m\sum_{i=1}^{k} \alpha_i,$$

kde α_i jsou právě různé kořeny polynomu $m(x)$; jistě všechny leží v L.

Z Galoisovy teorie víme, že libovolný automorfismus $\tau \in G$ permutuje kořeny $m(x)$ a navíc pro každé $i \in \mathbb{N}$, $1 \leq i \leq k$ existuje automorfismus, který zobrazuje α na α_i. Automorfismus τ však fixuje součin $\prod_{\sigma\in G} \alpha^\sigma$, a proto pro libovolné $i \in \mathbb{N}$, $1 \leq i \leq k$ existuje právě m automorfismů posílajících α na α_i. Odsud dostáváme identity

$$\mathrm{tr}(\alpha) = \sum_{\sigma\in G} \alpha^\sigma$$

$$N(\alpha) = \prod_{\sigma\in G} \alpha^\sigma.$$

Jestliže je L/K separabilní, tr není identicky rovno nule. Pokud je $\mathrm{char}\, K = 0$, plyne to z toho, že $\mathrm{tr}(1) = n \neq 0$.

Pokud je L/K konečné rozšíření konečných těles, je podle předchozích vzorců $\mathrm{tr}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{f-1}}$, kde $q = |K|$ a $|L| = q^f$. Nulovost stopy by znamenala, že jsou všechny prvky tělesa L kořeny polynomu stupně q^{f-1}, což není možné.

Poznamenejme, že platí i opačný směr, tj. jestliže není stopa identicky nulová, je příslušné rozšíření separabilní.

Definice. Pro libovolnou n-tici $\alpha_1, \alpha_2, \ldots, \alpha_n$ prvků z L definujeme jejich *diskriminant* $\Delta(\alpha_1, \ldots, \alpha_n)$ jako determinant matice $(\mathrm{tr}(\alpha_i\alpha_j))$.

Tvrzení 3.2.1. *Je-li $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$, pak $\alpha_1, \ldots, \alpha_n$ tvoří bázi L/K. Pokud je L/K separabilní a $\alpha_1, \ldots, \alpha_n$ tvoří bázi L/K, je $\Delta(\alpha_1, \ldots, \alpha_n) \neq 0$.*

Důkaz. Předpokládejme, že $\alpha_1, \ldots, \alpha_n$ jsou lineárně závislé, tj. existují $a_1, \ldots, a_n \in K$ ne všechna rovná nule taková, že $\sum_{i=1}^n a_i\alpha_i = 0$. Vynásobme tuto rovnici α_j a aplikujme stopu. Takto dostaneme

$$\sum_{i=1}^n a_i \,\mathrm{tr}(\alpha_i, \alpha_j) = 0 \quad \text{pro } j = 1, 2, \ldots, n.$$

Matice $(\mathrm{tr}(\alpha_i\alpha_j))$ je tedy singulární a její determinant je roven nule.

Naopak předpokládejme, že $\alpha_1, \ldots, \alpha_n$ tvoří bázi L/K a $\Delta(\alpha_1, \ldots, \alpha_n) = 0$. Pak má ovšem systém lineárních rovnic

$$\sum_{i=1}^n x_i \,\mathrm{tr}(\alpha_i\alpha_j) = 0 \quad \text{pro } j = 1, 2, \ldots, n$$

netriviální řešení $x_i = a_i \in K$, $i = 1, \ldots, n$. Nechť $\alpha = \sum_{i=1}^n a_i\alpha_i \neq 0$. Pak $\mathrm{tr}(\alpha\alpha_j) = 0$ pro $j = 1, \ldots, n$, a protože je $\alpha_1, \ldots, \alpha_n$ báze, je $\mathrm{tr}(\alpha\beta) = 0$ pro všechna $\beta \in L$. Stopa tr je tedy identicky nulová, což je spor se separabilitou rozšíření L/K. □

Tvrzení 3.2.2. *Nechť jsou $\alpha_1, \ldots, \alpha_n$ a $\beta_1, \ldots, \beta_n$ báze L/K a nechť $\alpha_i = \sum_{j=1}^n a_{ij}\beta_j$, $a_{ij} \in K$. Pak $\Delta(\alpha_1, \ldots, \alpha_n) = \det(a_{ij})^2\Delta(\beta_1, \ldots, \beta_n)$.*

Důkaz. Aplikujme stopu na obě strany rovnosti $\alpha_i\alpha_k = \sum_{j=1}^n \sum_{l=1}^n a_{ij}a_{kl}\beta_j\beta_l$. Označme $A = (\mathrm{tr}(\alpha_i\alpha_j))$, $B = (\mathrm{tr}(\beta_i\beta_j))$, $C = (a_{ij})$. Máme tedy rovnost matic $A = CBC^T$, kde C^T je transponovaná matice C. Uvážíme-li determinant obou stran, dostáváme požadované (zřejmě $\det C^T = \det C$). □

Tvrzení 3.2.3. *Nechť je L/K Galoisovo a $\alpha_1, \ldots, \alpha_n \in L$. Označíme-li prvky Galoisovy grupy $\mathrm{Gal}(L/K)$ jako $\sigma_1, \ldots, \sigma_n$, platí*

$$\Delta(\alpha_1, \ldots, \alpha_n) = \det(\alpha_i^{\sigma_j})^2.$$

Důkaz. $\mathrm{tr}(\alpha_i\alpha_j) = \alpha_i^{\sigma_1}\alpha_j^{\sigma_1} + \cdots + \alpha_i^{\sigma_n}\alpha_j^{\sigma_n}$. Označme $A = (\mathrm{tr}(\alpha_i\alpha_j))$ a $B = (\alpha_i^{\sigma_j})$. Pak $A = BB^T$. Porovnáním determinantů obou stran rovnosti dostaneme požadované. □

Tvrzení 3.2.4. *Nechť $\beta \in L$ je taková, že jsou $1, \beta, \ldots, \beta^{n-1}$ lineárně nezávislé nad K. Označme $f(x) \in K[x]$ minimální polynom pro β nad K. Pak je-li L/K separabilní, platí*

$$\Delta(1, \beta, \ldots, \beta^{n-1}) = (-1)^{(n(n-1))/2} N(f'(\beta)),$$

kde $f'(x)$ je formální derivace polynomu $f(x)$.

Důkaz. Matice $((\beta^{\sigma_j})^i)$, kde $j = 1, \ldots, n$ a $i = 0, \ldots, n$ je Vandermondeova typu a její determinant je tedy roven

$$\prod_{i<j}(\beta^{\sigma_j} - \beta^{\sigma_i}).$$

S využitím předchozího tvrzení máme

$$\Delta(1, \beta, \ldots, \beta^{n-1}) = (-1)^{(n(n-1))/2} \prod_{i\neq j}(\beta^{\sigma_j} - \beta^{\sigma_i}).$$

Konečně, $f(x) = \prod_{i=0}^{n-1}(x - \beta^{\sigma_i})$, a tedy pro libovolné $1 \leq j \leq n$ platí

$$f'(\beta^{\sigma_j}) = \prod_{i\neq j}(\beta^{\sigma_j} - \beta^{\sigma_i}).$$

Vezmeme-li součin těchto identit přes j od 1 do n, dostáváme požadované, neboť $f'(\beta^{\sigma_j}) = (f'(\beta))^{\sigma_j}$. □

3.3 Faktorizace v algebraických číselných tělesech

Tento odstavec představuje těžiště celé kapitoly. Dokážeme zde větu o jednoznačnosti rozkladu nenulových vlastních ideálů na prvoideály v algebraických číselných tělesech.

Pro úplnost na začátku připomeneme některé pojmy týkající se ideálů. Omezíme se pouze na komutativní okruhy, neboť s jinými se v textu nesetkáme.

Definice. Nechť R je komutativní okruh. Jeho podmnožina I se nazývá *ideál*, pokud $\alpha, \beta \in I$, $r \in R$ implikuje $\alpha + \beta \in I$ a $r\alpha \in I$.

Definice. Průnik libovolného neprázdného systému ideálů je zřejmě ideál. Ideál generovaný množinou prvků $M \subseteq R$ je průnikem všech ideálů obsahujících M. Ideál nazveme *hlavní*, je-li generován jednoprvkovou množinou $\{\alpha\}$ pro nějaké $\alpha \in R$; značíme jej (α). Ideál $I \neq R$ se nazývá *maximální*, pokud neexistuje, žádný ideál J, $I \subsetneq J \subsetneq R$. Konečně *prvoideál* P je takový ideál, pro který je splněna podmínka, že pro libovolná $a, b \in R$ taková, že $ab \in P$ platí $a \in P$ nebo $b \in P$.

Definice. Jsou-li I, J ideály komutativního okruhu R. Definujeme jejich součet a součin vztahy

$$I + J = \{a + b | a \in I, b \in J\}$$
$$IJ = \{a_1 b_1 + \cdots + a_t b_t | a_i \in I, b_i \in J\}.$$

Snadno se ověří, že jde opět o ideály.

V okruzích celých algebraických čísel lze definovat pojem norma i pro ideály.

Definice. Nechť L/K Galoisovo rozšíření, takové, že je $L/\mathbb{Q}$ je konečné, D je okruh celých algebraických čísel tělesa L a σ je libovolný automorfismus z $\mathrm{Gal}(L/K)$. Je-li I ideál okruhu D, pak je zřejmě množina

$$\sigma I = \{\sigma\alpha | \alpha \in I\}$$

opět ideál okruhu D. *Normu ideálu* I vzhledem k rozšíření L/K definujeme vztahem

$$N_{L/K} I = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma I.$$

Snadno se vidí, že je $N_{L/K} I$ opět ideál. Mimoto definujeme ještě *absolutní normu* ideálu $I \subseteq D$, značeno $\mathbf{N}I$, jako počet prvků D/I.

Nyní se již budeme věnovat konečným rozšířením racionálních čísel.

Definice. Podtěleso K komplexních čísel nazveme *algebraické číselné těleso* , je-li stupeň rozšíření $[K : \mathbb{Q}]$ konečný.

Vezměme těleso K pevně a označme D okruh celých algebraických čísel v K. Pojmy norma a stopa zavedené v předchozí kapitole budeme nadále používat vzhledem k pevně zvolenému rozšíření $K/\mathbb{Q}$, a proto opět nebudeme rozšíření explicitně vyznačovat v indexech.

D obecně není okruh s jednoznačných rozkladem. Má však vlastnost, že se dá každý jeho nenulový vlastní ideál psát jednoznačným způsobem jako součin prvoideálů. To budeme nyní dokazovat.

V dalších úvahách bude pojem „ideál“ vždy znamenat nenulový ideál. Někdy budeme používat spojení „ideál číselného tělesa“ namísto ideálu příslušného okruhu celých algebraických čísel. Protože však tělesa nemají vlastní ideály, nemůže dojít k nedorozumění.

Lemma 3.2. *Nechť $\beta \in K$. Pak existuje $b \in \mathbb{Z}$, $b \neq 0$ takové, že $b\beta \in D$.*

Důkaz. Nechť β splňuje rovnici

$$a_n\beta^n + a_{n-1}\beta^{n-1} + \cdots + a_1\beta + a_0 = 0,$$

kde $a_i \in \mathbb{Z}$ pro $i = 0, \ldots, n$. Vynásobením celým číslem a_n^{n-1} dostáváme

$$(a_n\beta)^n + a_{n-1}(a_n\beta)^{n-1} + a_{n-1}a_n(a_n\beta)^{n-2} + \cdots + a_1a_n^{n-2}(a_n\beta) + a_0a_n^{n-1} = 0.$$

Odsud $a_n\beta \in D$. □

Tvrzení 3.3.1. *Každý ideál A okruhu D obsahuje bázi K nad $\mathbb{Q}$.*

Důkaz. Nechť $\beta_1, \ldots, \beta_n$ je báze K nad $\mathbb{Q}$. Podle předcházejícího lemmatu existuje $b \in \mathbb{Z}$ takové, že $b\beta_1, \ldots, b\beta_n \in D$. Zvolme libovolné nenulové $\alpha \in A$. Pak prvky $b\beta_1\alpha, \ldots, b\beta_n\alpha$ leží v A a tvoří bázi K nad $\mathbb{Q}$ □

V dalších úvahách budeme používat některé pojmy z předchozí části. Pro $\alpha \in K$ leží $N(\alpha)$ i $\mathrm{tr}(\alpha)$ v $\mathbb{Z}$. Libovolný automorfismus z $\mathrm{Gal}(K/\mathbb{Q})$ nechává stopu i normu na místě, tedy $N(\alpha), \mathrm{tr}(\alpha) \in \mathbb{Q}$. Norma i stopa jsou však rovny součinu, resp. součtu celých algebraických čísel, jsou tedy samy celé algebraické a tedy podle 3.1.2 leží v $\mathbb{Z}$. Odsud též plyne, že je-li $\alpha_1, \ldots, \alpha_n$ báze K nad $\mathbb{Q}$ a všechna α_i jsou celá, pak $\Delta(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$.

Před formulací následujícího tvrzení poznamenejme, že diskriminant báze může být i záporný. Například diskriminant báze $1, i$ rozšíření $\mathbb{Q}(i)/\mathbb{Q}$ je roven -4.

Tvrzení 3.3.2. *Nechť je A ideál okruhu D a nechť je $\alpha_1, \ldots, \alpha_n \in A$ báze $K/\mathbb{Q}$ s minimálním $|\Delta(\alpha_1, \ldots, \alpha_n)|$. Pak $A = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$.*

Důkaz. Absolutní hodnota diskriminantů celočíselných bazí je vždy přirozené číslo, tedy jistě existuje báze s $|\Delta(\alpha_1, \ldots, \alpha_n)|$ minimálním.

Zvolme libovolné $\alpha \in A$ a pišme $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$, kde $a_i \in \mathbb{Q}$. Chceme ukázat, že $a_i \in \mathbb{Z}$. Sporem předpokládejme, že tomu tak není. Bez újmy na obecnosti můžeme předpokládat, že $a_1 \notin \mathbb{Z}$. Nechť $a_1 = m + \theta$, kde $m \in \mathbb{Z}$ a $0 < \theta < 1$. Označme $\beta_1 = \alpha - m\alpha_1, \beta_2 = \alpha_2, \ldots, \beta_n = \alpha_n$. Pak $\beta_1, \ldots, \beta_n \in A$ a navíc tvoří bázi $K/\mathbb{Q}$. Protože $\beta_1 = \theta\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, je matice přechodu od báze (α_i) k bázi (β_i)

$$\begin{pmatrix} \theta & a_2 & a_3 & \cdots & a_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Podle tvrzení 3.2.2 platí $\Delta(\beta_1, \ldots, \beta_n) = \theta^2\Delta(\alpha_1, \ldots, \alpha_n)$, což je ve sporu s minimalitou $\Delta(\alpha_1, \ldots, \alpha_n)$, neboť $0 < \theta < 1$. Musí být tedy všechna $a_i \in \mathbb{Z}$ a $A = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$. □

Tvoří-li prvky $\alpha_1, \ldots, \alpha_n \in A$ bázi K nad $\mathbb{Q}$ a $A = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$, říkáme, že $\alpha_1, \ldots, \alpha_n$ je *celočíselná báze* A. Z tvrzení 3.2.2 plyne, že diskriminanty dvou celočíselných bazí se rovnají. Tato společná hodnota se označuje jako *diskriminant* A (psáno $\Delta(A)$). Diskriminant $\delta_K = \Delta(D)$ má zvláštní význam a bývá nazýván *diskriminantem rozšíření* $K/\mathbb{Q}$.

Nyní použijeme tvrzení 3.3.2 k odvození několika důležitých vlastností okruhu D. Připomeňme, že ideálem rozumíme nenulový ideál.

Lemma 3.3. *Je-li $A \subseteq D$ ideál, pak $A \cap \mathbb{Z} \neq 0$.*

Důkaz. Nechť $\alpha \in A$, $\alpha \neq 0$. Pak existují čísla $a_i \in \mathbb{Z}$ taková, že

$$\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0.$$

Navíc můžeme předpokládat, že $a_0 \neq 0$, neboť se pohybujeme v tělese. Pak ale $0 \neq a_0 \in A \cap \mathbb{Z}$. □

Tvrzení 3.3.3. *Pro libovolný ideál $A \subseteq D$ je faktorokruh D/A konečný.*

Důkaz. Podle předchozího lemmatu existuje $a \in A \cap \mathbb{Z}$, $a \neq 0$. Nechť (a) je hlavní ideál generovaný a v D. Protože se $D/(a)$ přirozeně zobrazuje na D/A, stačí ukázat konečnost $D/(a)$. Ve skutečnosti ukážeme, že má $D/(a)$ právě a^n prvků.

Podle tvrzení 3.3.2 můžeme psát $D = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_n$, kde ω_i je nějaká celočíselná báze D. Nechť $S = \{\sum_{i=1}^n \gamma_i\omega_i | \gamma_i \in \mathbb{Z}, 0 \leq \gamma_i < a\}$. Ukážeme, že S je množina různých reprezentantů tříd $D/(a)$. Nechť $\omega = \sum_{i=1}^n m_i\omega_i \in D$ $(m_i \in \mathbb{Z})$. Pišme $m_i = q_i a + \gamma_i$, kde $0 \leq \gamma_i < a$. Pak zřejmě $\omega \equiv \sum_{i=1}^n \gamma_i\omega_i \pmod{a}$, tedy každá třída $D/(a)$ obsahuje nějaký prvek z S. Jsou-li $\sum_{i=1}^n \gamma_i\omega_i$ a $\sum_{i=1}^n \gamma_i'\omega_i$ dva různé prvky S, které leží ve stejné třídě $D/(a)$, musí být $\sum_{i=1}^n (\gamma_i - \gamma_i')\omega_i = a \cdot \sum_{i=1}^n c_i\omega_i$, pro nějaká $c_i \in \mathbb{Z}$. Z lineární nezávislosti ω_i tak dostáváme, že $a | \gamma_i - \gamma_i'$ pro všechna i. Odsud $\gamma_i = \gamma_i'$, neboť $0 \leq \gamma_i, \gamma_i' < a$. Množina S je tedy množinou reprezentantů tříd $D/(a)$ a $|D/(a)| = a^n$, což jsme chtěli ukázat. □

Důsledek. *D je Noetherovský okruh, t.j. libovolný řetězec ideálů $A_1 \subset A_2 \subset A_3 \subset \cdots$ je konečný.*

Důkaz. Protože je D/A_1 konečný, existuje jen konečně mnoho ideálů obsahujících A_1. □

Důsledek. *Každý prvoideál v D je maximální.*

Důkaz. Je-li P prvoideál, pak D/P je konečný obor integrity. Lze snadno ověřit, že takový okruh už musí být tělesem. Proto je D/P těleso a P je maximální. □

Lemma 3.4. *Nechť $A \subseteq D$ je ideál. Pokud $\beta \in K$ je takové, že $\beta A \subseteq A$, pak $\beta \in D$.*

Důkaz. Podle tvrzení 3.3.2 je A konečně generovaný $\mathbb{Z}$ modul, lemma tedy plyne přímo z tvrzení 3.1.5. □

Lemma 3.5. *Jsou-li A, B ideály v D takové, že $A = AB$, je $B = D$.*

Důkaz. Zvolme v A nějakou celočíselnou bázi $\alpha_1, \ldots, \alpha_n$. Díky tomu, že $A = AB$, lze najít prvky $b_{ij} \in B$ takové, že $\alpha_i = \sum_{j=1}^n b_{ij}\alpha_j$. Z toho plyne, že determinant matice $(b_{ij}) - E_n$ je roven nule (E_n je jednotková matice řádu n). Roznásobením determinantu získáme vyjádření jedničky jako lineární kombinace součinů prvků B. Tedy $1 \in B$, odkud $B = D$. □

Tvrzení 3.3.4. *Nechť $A, B \subseteq D$ jsou ideály a nechť $\omega \in D$ je takové, že $(\omega)A = BA$. Pak $(\omega) = B$.*

Důkaz. Je-li $\beta \in B$, platí $(\beta/\omega)A \subseteq A$ a tedy podle lemmatu 3.4 $\beta/\omega \in D$. Odsud $B \subseteq (\omega)$ a tedy $\omega^{-1}B \subseteq D$ je ideál. Protože je $A = \omega^{-1}BA$, z lemmatu 3.5 dostáváme, že $\omega^{-1}B = D$ a tedy $B = (\omega)$, jak jsme chtěli. □

Následující pojem hraje důležitou roli v algebraické teorii čísel.

Definice. Říkáme, že dva ideály $A, B \subseteq D$ jsou ekvivalentní, $A \sim B$, jestliže existují nenulová $\alpha, \beta \in D$ taková, že $(\alpha)A = (\beta)B$. Snadno se ověří, že relace $\sim$ je relací ekvivalence. Její třídy rozkladu se nazývají *třídy ideálů*. Počet tříd ideálů budeme značit h_K.

Je dobré si uvědomit, že $h_K = 1$ právě tehdy, když je D okruh hlavních ideálů. Pokud je totiž $h_K = 1$ a A libovolný ideál v D, musí existovat $\alpha, \beta \in D$ taková, že $(\alpha)A = (\beta)D = (\beta)$. Odsud $\beta/\alpha \in A$ a $A = (\beta/\alpha)$ je hlavní. Naopak, pokud je D okruh hlavních ideálů, je zřejmé, že $h_K = 1$.

Počet tříd ideálů lze tedy v jistém smyslu chápat jako míru toho, jak moc se liší D od okruhu hlavních ideálů, tedy od okruhu s jednoznačným rozkladem.

Nyní ukážeme, že h_K je konečné.

Lemma 3.6. *Existuje přirozené číslo M závisející pouze na K s následující vlastností. Pro libovolná $\alpha, \beta \in D$, $\beta \neq 0$ existuje přirozené číslo $t \leq M$ a prvek $\omega \in D$ tak, že*

$$|N(t\alpha - \omega\beta)| < |N(\beta)|.$$

Důkaz. Nejdříve mírně přeformulujeme znění lemmatu. Označíme-li $\gamma = \alpha/\beta \in K$, pak stačí dokázat, že pro libovolné $\gamma \in K$ existuje přirozené $t \leq M$ a $\omega \in D$ tak, že

$$|N(t\gamma - \omega)| < 1.$$

Nechť je $\omega_1, \omega_2, \ldots, \omega_n$ celočíselná báze D. Pro $\gamma \in K$ pišme $\gamma = \sum_{i=1}^n \gamma_i \omega_i$, kde $\gamma_i \in \mathbb{Q}$. Označíme-li $G = \mathrm{Gal}(K/\mathbb{Q})$, platí

$$|N(\gamma)| = \left| \prod_{\sigma \in G} \left(\sum_{i=1}^n \gamma_i \omega_i^\sigma \right) \right| \leq C \left(\max_{i=1\ldots n} |\gamma_i| \right)^n, \qquad (*)$$

kde $C = \prod_{\sigma \in G} (\sum_{i=1}^n |\omega_i^\sigma|)$. Zvolme libovolně celé číslo $m > \sqrt[n]{C}$ a položme $M = m^n$.

Pro libovolné $\gamma \in K$ opět označme $\gamma = \sum_{i=1}^n \gamma_i \omega_i$ a pišme $\gamma_i = a_i + b_i$, kde $a_i \in \mathbb{Z}$ a $0 \leq b_i < 1$. Označme $[\gamma] = \sum_{i=1}^n a_i \omega_i$ a $\{\gamma\} = \sum_{i=1}^n b_i \omega_i$. Pak platí $\gamma = [\gamma] + \{\gamma\}$, kde $[\gamma] \in D$ a $\{\gamma\}$ má souřadnice v intervalu $[0, 1)$.

Nechť ϕ je zobrazení z K do $\mathbb{R}^n$ definované předpisem $\phi(\sum_{i=1}^n \gamma_i \omega_i) = (\gamma_1, \gamma_2, \ldots, \gamma_n)$. Pak pro libovolné $\gamma \in K$ leží $\phi(\{\gamma\})$ v jednotkové n-rozměrné krychli. Rozdělme tuto krychli na m^n menších krychlí o hraně $1/m$ a uvažme body $\phi(\{k\gamma\})$ pro $1 \leq k \leq m^n + 1$. Z Dirichletova principu musí existovat $1 \leq l < h \leq m^n + 1$ taková, že $\phi(\{l\gamma\})$ a $\phi(\{h\gamma\})$ leží ve stejné menší krychli. Pišme $h\gamma = [h\gamma] + \{h\gamma\}$ a $l\gamma = [l\gamma] + \{l\gamma\}$. Odečtením dostaneme $t\gamma = \omega + \delta$, kde $t = h - l \leq m^n = M$, $\omega \in D$ a všechny souřadnice δ jsou v absolutní hodnotě menší než $1/m$.

Podle $(*)$ je $N(\delta) \leq C(1/m)^n = C/m^n < 1$. □

Věta 3.3.5. *Počet tříd ideálů tělesa K je konečný.*

Důkaz. Nechť A je ideál v D. Pro libovolné $\alpha \in A$, $\alpha \neq 0$ je $|N(\alpha)|$ přirozené číslo. Zvolme $\beta \in A$, $\beta \neq 0$ tak, že $|N(\beta)|$ je minimální. Podle předchozího lemmatu pro libovolné $\alpha \in A$ existují $t \in \mathbb{N}$, $t \leq M$ a $\omega \in D$ taková, že $|N(t\alpha - \omega\beta)| < |N(\beta)|$. Protože však $t\alpha - \omega\beta \in A$, musí být $t\alpha - \omega\beta = 0$. Tedy $t\alpha \in (\beta)$, odkud $M!A \subseteq (\beta)$. Označme $B = (1/\beta)M!A \subseteq D$. Pak B je ideál v D a $M!A = (\beta)B$. Protože je $\beta \in A$, leží $M!\beta$ v $(\beta)B$ a tedy $M! \in B$. Podle tvrzení 3.3.3 může být $M!$ obsaženo pouze v konečně mnoha ideálech. Ukázali jsme tedy, že $A \sim B$, kde B je jeden z konečně mnoha ideálů. Odsud již vidíme, že h_K je konečné. □

Následuje zajímavé a důležité tvrzení, které dostaneme aplikací předchozí věty.

Tvrzení 3.3.6. *Pro libovolný ideál $A \subseteq D$ existuje $k \in \mathbb{N}$, $1 \leq k \leq h_K$ takové, že ideál A^k je hlavní.*

Důkaz. Uvažme množinu ideálů $\{A^i | 1 \leq i \leq h_K + 1\}$. Alespoň dva ideály z této množiny musí ležet ve stejné třídě ideálů, označme $A^i \sim A^j$ pro $1 \leq i < j \leq h_K + 1$. Z definice $\sim$ musí existovat $\alpha\beta \in D$ taková, že $(\alpha)A^i = (\beta)A^j$. Označme $k = j - i$ a $B = A^k$. Ukážeme, že ideál B je hlavní.

Protože $(\alpha)A^i = (\beta)BA^i$, vidíme, že $(\alpha/\beta)A^i \subseteq A^i$ a tedy podle lemmatu 3.4 je $\alpha/\beta \in D$. Označíme-li $\omega = \alpha/\beta$, pak $(\omega)A^i = BA^i$ a podle tvrzení 3.3.4 $B = (\omega)$. □

Definice. Množina tříd ideálů spolu s operací násobení definovanou pomocí reprezentantů tvoří grupu. Tuto grupu nazýváme *grupa tříd ideálů*.

Snadno se ověří, že takto definované násobení je skutečně nezávislé na volbě reprezentantů. Asociativita plyne z asociativity násobení ideálů, jednotkový prvek představuje třída obsahující D (to je třída obsahující právě hlavní ideály) a podle předešlého tvrzení je inverzí k $[A]$ prvek $[A^{k-1}]$, kde $[A]$ značí třídu ideálů příslušnou ideálu A a k je takové, že A^k je hlavní ideál.

Studium grupy tříd ideálů bude hlavní náplní kapitoly 5. Nyní obrátíme pozornost opět k faktorizaci ideálů.

Tvrzení 3.3.7. *Nechť A, B, C jsou ideály v D, pro které platí $AB = AC$. Pak $B = C$.*

Důkaz. Podle tvrzení 3.3.6 existuje k takové, že $A^k = (\alpha)$, kde $\alpha \in D$. Vynásobme obě strany rovnice $AB = AC$ ideálem A^{k-1}. Dostáváme $(\alpha)B = (\alpha)C$, odkud $B = C$. □

Tvrzení 3.3.8. *Jsou-li A a B ideály v D takové, že $A \subseteq B$, pak existuje ideál C takový, že $A = BC$.*

Důkaz. Podobně jako v předchozím důkazu existuje $k \in \mathbb{N}$ takové, že $B^k = (\beta)$. Protože $A \subseteq B$, platí $B^{k-1}A \subseteq B^k = (\beta)$ a tedy $C = 1/\beta \cdot B^{k-1}A \subseteq D$ je ideál. Zbývá jen ověřit $BC = 1/\beta \cdot B^k A = 1/\beta \cdot (\beta)A = A$. □

Ideál B tedy obsahuje ideál A, právě když jej dělí.

Tvrzení 3.3.9. *Každý vlastní ideál v D se dá napsat jako součin prvoideálů.*

Důkaz. Nechť je A vlastní ideál v D. Protože je faktorokruh D/A konečný, je A obsažen v nějakém maximálním ideálu P_1 (za použití Zornova lemmatu se dá ukázat, že v libovolném komutativním okruhu s jedničkou je každý vlastní ideál obsažen v nějakém maximálním). Podle předchozího tvrzení je $A = P_1B_1$ pro nějaký ideál B_1. Pokud je B_1 vlastní, je opět obsažen v nějakém maximálním ideálu P_2, a tedy $A = P_1P_2B_2$. Pokud je $B_2 \neq D$, proces znovu opakujeme. Platí však $A \subset B_1 \subset B_2 \subset \cdots$, kde všechny inkluze jsou ostré, a tedy podle důsledku tvrzení 3.3.3 je $B_t = D$ pro nějaké $t \in \mathbb{N}$. Přepsáním máme $A = P_1P_2 \cdots P_t$. □

Nechť P je prvoideál. V řetězci $P \supset P^2 \supset P^3 \supset \cdots$ jsou všechny inkluze ostré, neboť v případě, že by $P^i = P^{i+1}$ pro nějaké $i \in \mathbb{N}$, platilo by $PP^i = P^i$ a tedy $P = D$ podle lemmatu 3.5. Má proto smysl následující definice.

Definice. Nechť P je prvoideál a A ideál v D. Pak $\operatorname{ord}_P A$ je definován jako jediné nezáporné celé číslo t, pro které $P^t \supseteq A$ a zároveň $P^{t+1} \not\supseteq A$.

Tvrzení 3.3.10. *Nechť jsou P, P' prvoideály a A, B ideály v D. Pak*

(a) $\operatorname{ord}_P P = 1$
(b) *Pro $P' \neq P$ je* $\operatorname{ord}_P P' = 0$
(c) $\operatorname{ord}_P AB = \operatorname{ord}_P A + \operatorname{ord}_P B$

Důkaz.

(a) První tvrzení je zřejmé.
(b) Předpokládejme že $\operatorname{ord}_P P' > 0$. Pak $P \supseteq P'$. Protože je P' maximální, musí být $P = P'$, což je spor s předpokladem.
(c) Označme $t = \operatorname{ord}_P A$ a $s = \operatorname{ord}_P B$. Podle tvrzení 3.3.8 můžeme psát $A = P^t A_1$ a $B = P^s B_1$, kde $P \not\supseteq A_1$, $P \not\supseteq B_1$.
Máme tedy $AB = P^{s+t} A_1 B_1$. Předpokládejme, že $P^{s+t+1} \supseteq AB$. Pak $AB = P^{s+t+1} C$ a tedy podle tvrzení 3.3.7 $PC = A_1 B_1$. Odsud $P \supseteq A_1 B_1$, ale protože je P prvoideál, musí být buď $P \supseteq A_1$ nebo $P \supseteq B_1$. To je spor. Máme tedy $\operatorname{ord}_P AB = \operatorname{ord}_P A + \operatorname{ord}_P B$.

□

Věta 3.3.11 (Jednoznačnost rozkladu). *Nechť $A \subset D$ je ideál. Pak $A = \prod P^{a(P)}$, kde součin jde přes všechny prvoideály v D, a $a(P)$ jsou nezáporná celá čísla, která jsou rovna nule až na konečně mnoho případů. Konečně, čísla $a(P)$ jsou jednoznačně určena rovností $a(P) = \operatorname{ord}_P A$.*

Důkaz. Podle tvrzení 3.3.9 lze psát A v uvedeném tvaru. Nechť P_0 je libovolný prvoideál. Aplikujme ord_{P_0} na obě strany rovnosti $A = \prod P^{a(P)}$. Za pomoci tvrzení 3.3.10 dostáváme

$$\operatorname{ord}_{P_0} A = \sum_{P|A} a(P) \operatorname{ord}_{P_0} P = a(P_0).$$

□

3.4 Větvení a stupně inercie prvoideálů

Nyní se budeme zabývat podrobněji faktorizací ideálů pD, kde p je prvočíslo.

Nechť P je prvoideál v D. Podle lemmatu 3.3 je $P \cap \mathbb{Z} \neq \emptyset$. Protože je $P \cap \mathbb{Z}$ zřejmě prvoideál v $\mathbb{Z}$, musí být tvaru (p) pro nějaké prvočíslo p.

Definice. Číslo $e = \mathrm{ord}_P(p)$ se nazývá *index větvení* prvoideálu P (zde (p) značí hlavní ideál generovaný p v D).

D/P je konečné těleso obsahující $\mathbb{Z}/p\mathbb{Z}$. Počet prvků D/P tedy musí být tvaru p^f pro nějaké $f \in \mathbb{N}$. Číslo f se nazývá *stupeň inercie* prvoideálu P.

Nechť $p \in \mathbb{Z}$ je prvočíslo. Označme $P_1, \ldots, P_g$ prvoideály v D dělící (p). Dále označme e_i a f_i index větvení, resp. stupeň inercie prvoideálu P_i pro $1 \leq i \leq g$. Podle věty 3.3.11 platí $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$. Mezi čísly e_i, f_i a g existuje zajímavý vztah (připomeňme, že $n = [K : \mathbb{Q}]$).

Věta 3.4.1. $\sum_{i=1}^{g} e_i f_i = n$.

Důkaz prozatím odložíme; nejprve dokážeme dvě užitečná tvrzení.

Tvrzení 3.4.2. *Nechť je R komutativní okruh s jedničkou. Nechť $A_1, A_2, \ldots, A_g$ jsou ideály takové, že $A_i + A_j = R$ pro $i \neq j$. Označme $A = A_1 A_2 \cdots A_g$. Pak*

$$R/A \cong R/A_1 \oplus R/A_2 \oplus \cdots \oplus R/A_g.$$

Důkaz. Nechť je ψ_i přirozené zobrazení R do R/A_i. Definujme zobrazení

$$\psi : R \to R/A_1 \oplus R/A_2 \oplus \cdots \oplus R/A_g$$

předpisem

$$\psi(\gamma) = (\psi_1(\gamma), \psi_2(\gamma), \ldots, \psi_g(\gamma)).$$

Ukážeme, že je ψ surjektivní a jeho jádro je A.

K důkazu surjektivity ψ stačí ukázat, že pro libovolná $\gamma_1, \gamma_2, \ldots, \gamma_g \in R$ je řešitelná soustava kongruencí $x \equiv \gamma_i \pmod{A_i}$, $1 \leq i \leq g$.

Roznásobením součinu $(A_1 + A_2)(A_1 + A_3) \cdots (A_1 + A_g) = R$ vidíme, že všechny sčítance s výjimkou posledního leží pod A_1. Tedy $A_1 + A_2 A_3 \cdots A_g = R$. Proto musí existovat $v_1 \in A_1$ a $u_1 \in A_2 A_3 \cdots A_g$ tak, že $u_1 + v_1 = 1$. Pak ale $u_1 \equiv 1 \pmod{A_1}$ a $u_1 \equiv 0 \pmod{A_i}$ pro $i \neq 1$. Podobně pro každé $1 \leq j \leq g$ existuje u_j takové, že $u_j \equiv 1 \pmod{A_j}$ a $u_j \equiv 0 \pmod{A_i}$ pro $i \neq j$. Potom je ovšem $x = \gamma_1 u_1 + \gamma_2 u_2 + \cdots + \gamma_g u_g$ řešením naší soustavy kongruencí.

Nyní zkoumejme jádro ψ. Zřejmě $\mathrm{Ker}\,\psi = A_1 \cap A_2 \cap \cdots A_g$. Musíme dokázat, že za daných předpokladů je průnik ideálů roven jejich součinu. To ukážeme indukcí. Předpokládejme, že $g = 2$. Pak $A_1 + A_2 = R$ a tedy existují $a_1 \in A_1$ a $a_2 \in A_2$ tak, že $a_1 + a_2 = 1$. Je-li $a \in A_1 \cap A_2$, je $a = a a_1 + a a_2 \in A_1 A_2$. Máme tedy $A_1 \cap A_2 \subseteq A_1 A_2$. Opačná inkluze je zřejmá.

Nyní nechť $g > 2$. Pak je podle indukčního předpokladu $A_1 \cap A_2 \cap \cdots \cap A_g = A_1 \cap A_2 A_3 \cdots A_g$. Avšak $A_1 + A_2 A_3 \cdots A_g = R$ podle první části důkazu, a proto $A_1 \cap A_2 A_3 \cdots A_g = A_1 A_2 \cdots A_g$. Tím je důkaz hotov. □

Toto tvrzení se nazývá *Čínská zbytková věta pro okruhy*. Nyní se od obecných komutativních okruhů vrátíme zpět k D.

Tvrzení 3.4.3. *Nechť je $P \subset D$ prvoideál a $|D/P| = p^f$. Pak $|D/P^e| = p^{ef}$ pro libovolné $e \in \mathbb{N}$.*

Důkaz. Pro $e = 1$ není o čem diskutovat. Je-li $e > 1$, D/P^e obsahuje P^{e-1}/P^e. Podle zákonů o izomorfismu je $(D/P^e)/(P^{e-1}/P^e) \cong D/P^{e-1}$. Stačí tedy ukázat, že P^{e-1}/P^e má p^f prvků; zbytek se provede snadno indukcí.

Protože je inkluze $P^e \subset P^{e-1}$ vlastní, existuje prvek $\alpha \in P^{e-1}$ takový, že $\alpha \notin P^e$. Ukážeme, že $(\alpha) + P^e = P^{e-1}$. Protože $P^e \subseteq (\alpha) + P^e$, musí být $(\alpha) + P^e$ mocninou P. Z toho, že $(\alpha) + P^e \subseteq P^{e-1}$ už nutně $(\alpha) + P^e = P^{e-1}$.

Uvažme zobrazení z D do P^{e-1}/P^e dané předpisem $\gamma \mapsto \gamma\alpha + P^e$. Z předchozí úvahy plyne, že se jedná o surjektivní homomorfismus. Prvek $\gamma \in D$ leží v jeho jádru, právě když $\gamma\alpha \in P^e$, tj. pokud $\mathrm{ord}_P(\gamma\alpha) \geq e$. Z vlastností ord máme postupně $\mathrm{ord}_P(\gamma\alpha) = \mathrm{ord}_P(\gamma) + \mathrm{ord}_P(\alpha) = \mathrm{ord}_P(\gamma) + e - 1$. Prvek γ tedy leží v jádru našeho homomorfismu, právě když $\mathrm{ord}_P(\gamma) \geq 1$, což je ekvivalentní faktu $\gamma \in P$. Odsud $D/P \cong P^{e-1}/P^e$ a tedy $|P^{e-1}/P^e| = p^f$. □

Nyní jsme již připraveni dokázat větu 3.4.1. Připomeňme, že $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$. Není obtížné ověřit, že $P_i^{e_i} + P_j^{e_j} = D$ pro $i \neq j$. Podle tvrzení 3.4.2 je tedy

$$D/(p) \cong D/P_1^{e_1} \oplus D/P_2^{e_2} \oplus \cdots \oplus D/P_g^{e_g}.$$

V důkazu tvrzení 3.3.3 bylo zmíněno, že $|D/(p)| = p^n$. Na druhou stranu z tvrzení 3.4.3 víme, že $|D/P_i^{e_i}| = p^{e_i f_i}$. Odsud

$$p^n = p^{e_1 f_1} p^{e_2 f_2} \cdots p^{e_g f_g}.$$

Tedy $n = e_1 f_1 + e_2 f_2 + \cdots + e_g f_g$, což jsme měli dokázat. □

Pokud je rozšíření $K/\mathbb{Q}$ Galoisovo, dá se věta 3.4.1 zesílit. Předpokládejme tedy, že je $K/\mathbb{Q}$ Galoisovo a označme G jeho Galoisovu grupu. Připomeňme, že pro libovolné $\sigma \in G$ značíme ideál $\sigma A = \{\sigma\alpha | \alpha \in A\}$. Platí $\sigma D = D$ a tedy $D/\sigma A = \sigma D/\sigma A \cong D/A$. Odsud plyne, že pokud je P prvoideál, je i σP prvoideál.

Tvrzení 3.4.4. *Nechť je $p \in \mathbb{Z}$ prvočíslo. Dále nechť jsou P_i, P_j různé prvoideály v D dělící p. Pak existuje $\sigma \in G$ takové, že $\sigma P_i = P_j$.*

Důkaz. Předpokládejme, že existuje prvoideál P_0 dělící p, který se nevyskytuje v $\{\sigma P_i | \sigma \in G\}$. Tvrzení 3.4.2 nám zaručuje existenci $\alpha \in D$, které splňuje $\alpha \equiv 0 \pmod{P_0}$ a $\alpha \equiv 1 \pmod{\sigma P_i}$ pro všechna $\sigma \in G$.

Pak $\alpha \in P_0$ a tedy $N(\alpha) = \prod_{\sigma \in G} \sigma\alpha \in P_0 \cap \mathbb{Z} = p\mathbb{Z}$. Odsud plyne, že $N(\alpha) \in P_i$ a tedy $\sigma\alpha \in P_i$ pro nějaké $\sigma \in G$, neboť P_i je prvoideál. Pak ale $\alpha \in \sigma^{-1} P_i$, což je ve sporu s faktem $\alpha \equiv 1 \pmod{\sigma^{-1} P_i}$. □

Věta 3.4.5. *Nechť $K/\mathbb{Q}$ je Galoisovo rozšíření. Nechť $p \in \mathbb{Z}$ je prvočíslo, které se v D rozkládá $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$. Pak $e_1 = e_2 = \cdots = e_g$ a $f_1 = f_2 = \cdots = f_g$. Označíme-li tyto společné hodnoty e a f, platí $efg = n$.*

Důkaz. Pro libovolný index i existuje $\sigma \in G$ tak, že $\sigma P_1 = P_i$. Z faktu $D/P_1 \cong D/\sigma P_1 = D/P_i$ je vidět, že $f_1 = f_2 = \cdots = f_g$.

Stejný automorfismus σ aplikujme na obě strany rozkladu $(p) = P_1^{e_1} P_2^{e_2} \cdots P_g^{e_g}$. Dostáváme

$$(p) = (\sigma P_1)^{e_1} (\sigma P_2)^{e_2} \cdots (\sigma P_g)^{e_g}$$

Za jednoznačnosti rozkladu plyne $e_i = \mathrm{ord}_{P_i}(p) = \mathrm{ord}_{\sigma P_1}(p) = e_1$. Všechna e_i se tedy musí rovnat.

Konečně identita $\sum_{i=1}^{n} e_i f_i = n$ má v našem případě tvar $efg = n$. □

3.5 Faktorizace v kruhových tělesech

Nechť m je přirozené číslo a $\zeta_m = e^{2\pi i/m}$. Čísla ζ_m^t pro $t = 1, \ldots, m-1$ jsou právě kořeny polynomu $x^m - 1$. Máme tedy $x^m - 1 = (x-1)(x-\zeta_m)\cdots(x-\zeta_m^{m-1})$ a těleso $K_m = \mathbb{Q}(\zeta_m)$[1] je rozkladové těleso separabilního polynomu $x^m - 1$. Rozšíření $K_m/\mathbb{Q}$ je tedy Galoisovo.

Těleso K_m nazýváme *m-té kruhové těleso*. Nyní popíšeme podrobněji Galoisovu grupu $G = \mathrm{Gal}(K_m/\mathbb{Q})$.

Definice. Na přirozených číslech zavádíme *Eulerovu funkci* ϕ následujícím způsobem. Pro libovolné $m \in \mathbb{N}$ je $\phi(m)$ počet celých čísel mezi 1 a m včetně nesoudělných s m. Jinak řečeno $\phi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$.

Tvrzení 3.5.1. *Existuje prostý homomorfismus $\theta : G \to (\mathbb{Z}/m\mathbb{Z})^\times$ takový, že pro libovolné $\sigma \in G$ platí*

$$\sigma\zeta_m = \zeta_m^{\theta(\sigma)}.$$

Důkaz. Protože $\zeta_m^m = 1$, máme $(\sigma\zeta_m)^m = 1$. Odsud $\sigma\zeta_m = \zeta_m^{\theta(\sigma)}$, kde $\theta(\sigma)$ je celé číslo modulo m. Označíme-li $\tau = \sigma^{-1}$, máme $\zeta_m = \tau\sigma\zeta_m = \tau(\zeta_m^{\theta(\sigma)}) = \zeta_m^{\theta(\sigma)\theta(\tau)}$. Odsud plyne, že $\theta(\sigma)\theta(\tau) = [1]_m$, kde $[1]_m$ je třída v $\mathbb{Z}/m\mathbb{Z}$ obsahující číslo 1. Obrazy θ jsou tedy skutečně invertibilními prvky v $\mathbb{Z}/m\mathbb{Z}$. Na druhou stranu se snadno ověří, že θ je homomorfismus grup. Konečně $\theta(\sigma) = [1]_m$ implikuje $\sigma\zeta_m = \zeta_m$, odkud plyne, že σ je identita na K_m, neboť ζ_m generuje celé K_m nad $\mathbb{Q}$. Homomorfismus θ je tedy prostý. □

Důsledek. *$[K_m : \mathbb{Q}]$ dělí $\phi(m)$.*

Později ukážeme, že ve skutečnosti $[K_m : \mathbb{Q}] = \phi(m)$

Definice. Označme $\Phi_m(x) = \prod_{(a,m)=1}(x - \zeta_m^a)$, kde $1 \le a \le m$. Polynom $\Phi_m(x)$ nazveme *m-tý kruhový polynom.*

Kořeny $\Phi_m(x)$ jsou právě primitivní m-té odmocniny z jedné, tj. ty řádu m. Stupeň polynomu $\Phi_m(x)$ je zřejmě $\phi(m)$.

Tvrzení 3.5.2. $x^m - 1 = \prod_{d|m} \Phi_d(x)$

[1] Označení $K_m = \mathbb{Q}(\zeta_m)$ budeme používat ve zbytku textu.

Důkaz.

$$x^m - 1 = \prod_{i=0}^{m-1}(x - \zeta_m^i) = \prod_{d|m} \prod_{(i,m)=d} (x - \zeta_m^i),$$

kde $0 \leq i \leq m-1$. Stačí, když ukážeme, že $\prod_{(i,m)=d}(x - \zeta_m^i) = \Phi_{m/d}(x)$. To plyne z následujícího.

Je-li $(i,m) = d$, označme $i = dj$. Pak $\zeta_m^i = \zeta_m^{dj} = \zeta_{m/d}^j$ a navíc $(j, m/d) = 1$. Celkem tedy

$$\prod_{(i,m)=d} (x - \zeta_m^i) = \prod_{(j,m/d)=1} (x - \zeta_{m/d}^j) = \Phi_{m/d}(x).$$

□

Důsledek. $\Phi_m(x) \in \mathbb{Z}[x]$.

Důkaz. Toto dokážeme indukcí vzhledem k m. Pro $m = 1$ máme $\Phi_1(x) = x - 1$. Předpokládejme, že tvrzení platí pro všechna přirozená čísla menší než m. Podle tvrzení 3.5.2 je $\Phi_m(x) = (x^m - 1)/f(x)$, kde $f(x)$ je normovaný polynom, který má podle indukčního předpokladu celočíselné koeficienty. „Ručním“ vydělením získáme $\Phi_m(x) \in \mathbb{Z}[x]$. □

Ukážeme ještě jiný důkaz s využitím Galoisovy teorie. Každé $\sigma \in G$ permutuje primitivní m-té odmocniny z jedné. Koeficienty $\Phi_m(x)$ jsou tedy fixovány celou G a musí ležet v $\mathbb{Q}$. Protože jsou to však zřejmě celá algebraická čísla, musí ležet v $\mathbb{Z}$.

Tvrzení 3.5.3. *Nechť je p prvočíslo takové, že $p \nmid m$ a nechť je P prvoideál v D_m, který dělí (p). Pak prvky $1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{m-1}$ leží v navzájem různých zbytkových třídách D_m/P. Je-li f stupeň inercie P, pak $p^f \equiv 1 \pmod m$.*

Důkaz. Pro $w \in D_m$ označme $\overline{w}$ příslušnou zbytkovou třídu v D_m/P.

Podělme obě strany rovnosti $x^m - 1 = \prod_{i=0}^{m-1}(1 - \zeta_m^i)$ polynomem $x - 1$. Dostáváme

$$1 + x + \cdots + x^{m-1} = \prod_{i=1}^{m-1}(x - \zeta_m^i).$$

Po dosazení $x = 1$ máme $m = \prod_{i=1}^{m-1}(1-\zeta_m^i)$. Tedy $\overline{m} = \prod_{i=1}^{m-1} \overline{(1 - \zeta_m^i)}$. Protože $\overline{m} \neq \overline{0}$, musí být $\overline{\zeta_m^i} \neq \overline{1}$ pro $1 \leq i \leq m-1$ a tedy $\overline{\zeta_m^i} \neq \overline{\zeta_m^j}$ pro $0 \leq i < j \leq m-1$.

Prvky $\{\zeta_m^i | 0 \leq i \leq m-1\}$ tvoří podgrupu řádu m v multiplikativní grupě D_m/P, která má řád $p^f - 1$. Proto $m | p^f - 1$ a tedy $p^f \equiv 1 \pmod m$. □

Věta 3.5.4. *m-tý kruhový polynom $\Phi_m(x)$ je ireducibilní v $\mathbb{Z}[x]$.*

Důkaz. Nechť $f(x) \in \mathbb{Z}[x]$ je normovaný ireducibilní polynom ζ_m. Polynom $f(x)$ má podle tvrzení 3.1.1 celočíselné koeficienty, neboť ζ_m je algebraické celé číslo. Je-li p prvočíslo, $p \nmid m$, ukážeme, že ζ_m^p je také kořen $f(x)$.

Nechť P je nějaký prvoideál v D_m dělící (p). Opět pro $w \in D_m$ označme $\overline{w}$ příslušnou zbytkovou třídu v D_m/P. Máme $x^m - 1 = f(x)g(x)$ v $\mathbb{Z}[x]$ a tedy $x^m - \overline{1} = \overline{f}(x)\overline{g}(x)$

v $(\mathbb{Z}/p\mathbb{Z})[x]$. Podle tvrzení 3.5.3 jsou kořeny $x^m - \overline{1}$ v D_m/P různé. Odsud plyne, že $\overline{f}(x)$ a $\overline{g}(x)$ nemají žádný společný kořen. Předpokládejme, že $f(\zeta_m^p) \neq 0$. Pak $g(\zeta_m^p) = 0$ a tedy $\overline{g}(\overline{\zeta_m^p}) = 0$. Koeficienty $\overline{g}(x)$ leží v $\mathbb{Z}/p\mathbb{Z}$ a jsou tedy podle malé Fermatovy věty rovny svým p-tým mocninám. Odsud s použitím tvrzení 3.1.7 dostáváme $\overline{0} = \overline{g}(\overline{\zeta_m^p}) = \overline{g}(\overline{\zeta_m})^p$ a tedy $\overline{0} = \overline{g}(\overline{\zeta_m})$. Pak ale $\overline{f}(\overline{\zeta_m}) \neq \overline{0}$, což je spor s $f(\zeta_m) = 0$. Ukázali jsme tedy, že $f(\zeta_m^p) = 0$.

Ve skutečnosti jsme ukázali, že pokud je ζ libovolná primitivní m-tá odmocnina z jedné, která je kořenem $f(x)$, je i ζ^p primitivní m-tá odmocnina z jedné a je kořenem $f(x)$, a to pro libovolné prvočíslo $p \nmid m$. Odsud plyne, že i pro každé $a \in \mathbb{Z}$, $(a, m) = 1$, je ζ_m^a kořenem $f(x)$. Tedy $\deg f(x) \geq \phi(m)$. Na druhou stranu $\Phi_m(\zeta_m) = 0$, odkud $f(x)|\Phi_m(x)$ a tedy $\deg f(x) \leq \deg \Phi_m(x) = \phi(m)$. Celkem tedy $\Phi_m(x) = f(x)$. □

Důsledek (1). $[K_m : \mathbb{Q}] = \phi(m)$

Důsledek (2). *Zobrazení θ definované ve tvrzení 3.5.1 je izomorfismus $G \cong (\mathbb{Z}/m\mathbb{Z})^\times$.*

Důkaz. Obě grupy mají $\phi(m)$ prvků. Z toho, že θ je injektivní, přímo plyne, že musí být i surjektivní. □

Z tohoto důsledku vidíme, že pro libovolné $a \in \mathbb{Z}$, $(a, m) = 1$ existuje $\sigma_a \in G$ tak, že $\sigma_a\zeta = \zeta^a$. Zobrazení $[a]_m \mapsto \sigma_a$ je ve skutečnosti homomorfismus $(\mathbb{Z}/m\mathbb{Z})^\times$ do G, který je inverzí k θ ($[a]_m$ značí zbytkovou třídu a modulo m).

Je-li p prvočíslo, které nedělí m, má zvláštní význam automorfismus σ_p. Jeho studiu se budeme věnovat nyní.

Lemma 3.7. *Nechť je $K/\mathbb{Q}$ těleso algebraických čísel stupně n. Označme D okruh algebraických celých čísel v K a zvolme libovolnou bázi $\alpha_1, \alpha_2, \ldots, \alpha_n \in D$ pro $K/\mathbb{Q}$. Dále označme $\Delta = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ diskriminant této báze. Pak $\Delta D \subseteq \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$.*

Důkaz. Nechť $w \in D$. Můžeme psát $w = \sum_{i=1}^n r_i\alpha_i$, kde $r_i \in \mathbb{Q}$. Vynásobme obě strany α_j a aplikujme stopu. Dostáváme

$$\operatorname{tr}(w\alpha_j) = \sum_{i=1}^n r_i \operatorname{tr}(\alpha_i\alpha_j). \qquad (*)$$

Prvky $\operatorname{tr}(w\alpha_j)$ a $\operatorname{tr}(\alpha_i\alpha_j)$ jsou celá čísla, neboť jsou to stopy celých algebraických čísel. Ze soustavy $(*)$ pro $j = 1, \ldots, n$ dostáváme použitím Cramerova pravidla, že každé r_i je tvaru celé číslo dělené Δ. Celkem tedy $\Delta w = \sum_{i=1}^n \Delta r_i\alpha_i \in \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2 + \cdots + \mathbb{Z}\alpha_n$. □

Lemma 3.8. *Diskriminant $\Delta = \Delta(1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\phi(m)-1})$ dělí $m^{\phi(m)}$.*

Důkaz. Zderivujme obě strany rovnosti $x^m - 1 = \Phi_m(x)g(x)$. Dostaneme

$$mx^{m-1} = \Phi'_m(x)g(x) + \Phi_m(x)g'(x).$$

Dosazením $x = \zeta_m$ máme $m\zeta_m^{m-1} = \Phi'_m(\zeta_m)g(\zeta_m)$. Nyní aplikujme na obě strany normu. Podle věty 3.5.4 je $1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}$ báze K_m nad $\mathbb{Q}$ a tedy podle tvrzení 3.2.4 a faktu, že $N(\zeta_m) = \pm 1$, dostáváme $\pm m^{\phi(m)} = \pm\Delta \cdot N(g(\zeta_m))$. □

Tvrzení 3.5.5. *Nechť je p prvočíslo, které nedělí m a nechť je w celé algebraické číslo v K_m. Pak existuje prvek $\sum_{i=0}^{\phi(m)} a_i\zeta_m^i \in \mathbb{Z}[\zeta_m]$ takový, že platí $w \equiv \sum_{i=0}^{\phi(m)} a_i\zeta_m^i \pmod p$.*

Důkaz. Označme opět $\Delta = \Delta(1, \zeta_m, \ldots, \zeta_m^{\phi(m)-1}) \in \mathbb{Z}$. Podle lemmatu 3.8 víme, že $p \nmid \Delta$. Musí tedy existovat $\Delta' \in \mathbb{Z}$ takové, že $\Delta'\Delta \equiv 1 \pmod p$. Odsud $w \equiv \Delta'\Delta w \pmod p$. Podle lemmatu 3.7 je tedy $\Delta w \in \mathbb{Z}[\zeta_m]$ a též $\Delta'\Delta w \in \mathbb{Z}[\zeta_m]$. □

Poznamenejme, že ve skutečnosti $D = \mathbb{Z}[\zeta_m]$, avšak toto není snadné dokázat pro obecná m. Poznamenejme jen, že nám ve všech úvahách stačí fakt $\mathbb{Z}[\zeta_m] \subseteq D$, který plyne z toho, že je D okruh.

Důsledek. *Nechť p je prvočíslo, $p \nmid m$ a $n \in \mathbb{N}$ je takové, že $p^n \equiv 1 \pmod m$. Pak pro každé $w \in D$ platí $w^{p^n} \equiv w \pmod p$.*

Důkaz. Podle předchozího tvrzení lze psát $w \equiv \sum a_i\zeta_m^i$, kde $a_i \in \mathbb{Z}$. Protože $a_i^p \equiv a_i \pmod p$, musí platit $w^p \equiv \sum a_i\zeta_m^{pi} \pmod p$. Pokud tento proces zopakujeme n-krát, dostaneme $w^{p^n} \equiv \sum a_i\zeta_m^{p^n i} = w \pmod p$. □

Tvrzení 3.5.6. *Je-li p prvočíslo nedělící m, pak se žádný prvoideál P v D_m dělící (p) nevětví.*

Důkaz. Předpokládejme, že se P větví. Pak $(p) \subseteq P^2$. Nechť $w \in D_m$ leží v P a neleží v P^2. Podle předchozího důsledku $w^{p^n} \equiv w \pmod p$ a tedy i $w^{p^n} \equiv w \pmod{P^2}$. Protože je $p^n \geq 2$, je $w^{p^n} \in P^2$, odkud $w \in P^2$, což je spor. □

Později uvidíme, že „téměř“ platí i obrácení tohoto tvrzení (viz. tvrzení 3.5.10).

Připomeňme, že pro prvočíslo p nedělící m máme automorfismus σ_p, který ζ_m zobrazuje na ζ_m^p.

Tvrzení 3.5.7. *Pro všechna $w \in D_m$ platí $\sigma_p w \equiv w^p \pmod p$.*

Důkaz. Podle tvrzení 3.5.5 můžeme psát $w \equiv \sum a_i\zeta_m^i \pmod p$, kde $a_i \in \mathbb{Z}$. Aplikujme σ_p na obě strany této kongruence. Dostáváme $\sigma_p w \equiv \sum a_i\zeta_m^{pi} \pmod p$. Protože je $a_i \in \mathbb{Z}$, platí $\sum a_i\zeta_m^{pi} \equiv \sum a_i^p\zeta_m^{pi} \equiv (\sum a_i\zeta_m^i)^p \pmod p$. Tedy $\sigma_p w \equiv w^p \pmod p$, což jsme měli dokázat. □

Důsledek. *Nechť je P prvoideál v D_m obsahující p, pak $\sigma_p P = P$.*

Důkaz. Pro $w \in P$ máme $\sigma_p(w) \equiv w^p \equiv 0 \pmod P$ a tedy $\sigma_p P \subseteq P$. Protože je $\sigma_p P$ maximální ideál, musí být $\sigma_p P = P$. □

Věta 3.5.8. *Nechť je p prvočíslo, $p \nmid m$. Označme f řád p modulo m, tj. nejmenší přirozené číslo takové, že $p^f \equiv 1 \pmod m$. Pak se (p) v okruhu celých algebraických čísel tělesa K_m rozkládá*

$$(p) = P_1 P_2 \cdots P_g,$$

kde stupeň inercie každého P_i je roven f a $g = \phi(m)/f$.

Důkaz. Přímo z toho, jak je definováno plyne, že f je řád automorfismu σ_p.

Označíme-li f_1 stupeň inercie prvoideálu P_1, máme $p^{f_1} = |D_m/P_1|$. Protože je D_m/P_1 konečné těleso, platí $w^{p^{f_1}} \equiv w \pmod{P_1}$ pro všechna $w \in D_m$ a f_1 je nejmenší číslo s touto vlastností.

Podle důsledku tvrzení 3.5.5 je $w \equiv w^{p^f} \pmod{P_1}$ pro všechna $w \in D_m$. Odsud $f_1 \leq f$.

Na druhou stranu $\zeta_m^{p^{f_1}} \equiv \zeta_m \pmod{P_1}$ implikuje $\zeta_m^{p^{f_1}} = \zeta_m$ podle tvrzení 3.5.3. Odsud $p^{f_1} \equiv 1 \pmod{m}$ a $f \leq f_1$.

Vidíme tedy, že $f = f_1 =$ stupeň inercie P_1; každý prvoideál P_i má tedy stupeň inercie roven f. Z tvrzení 3.5.6 víme, že se žádný z prvoideálů P_i, $1 \leq i \leq g$ nevětví. Použitím vztahu $efg = \phi(m)$ tak dostáváme $g = \phi(m)/f$. □

Důsledek. *Se stejným označením jako ve znění předchozí věty nechť P je jedním z P_i. Definujme $G(P) = \{\sigma \in G | \sigma P = P\}$. Platí, že $G(P)$ je cyklická grupa generovaná automorfismem σ_p.*

Grupa $G(P)$ se nazývá *dekompoziční grupa* prvoideálu P. Dekompoziční grupu lze zřejmě definovat i pro obecná Galoisova rozšíření algebraických číselných těles.

Důkaz. Z důsledku tvrzení 3.5.7 víme, že $\sigma_p \in G(P)$. Nechť $\langle \sigma_p \rangle$ je cyklická podgrupa G generovaná σ_p. Pak $\langle \sigma_p \rangle \subseteq G(P)$. Podle tvrzení 3.4.4 je $g|G(P)| = \phi(m)$. Tedy $|G(P)| = \phi(m)/g = f = |\langle \sigma_p \rangle|$ a jsme hotovi. □

Věta 3.5.8 dává dostatečnou informaci o faktorizaci těch prvočísel, které nedělí m. Nyní odvodíme faktorizaci p v K_p.

Tvrzení 3.5.9. *Nechť je l prvočíslo. Pak platí, že se (l) v K_l zcela větví. Přesněji, nechť $L = (1 - \zeta_l)$. Pak je L prvoideál v K_l a $(l) = L^{l-1}$, přičemž stupeň inercie L je roven 1.*

Důkaz. Stejným způsobem jako v důkazu tvrzení 3.5.3 odvodíme rovnost $l = \prod_{i=1}^{l-1}(1 - \zeta_l^i)$.

Označme $u_i = (1 - \zeta_l^i)/(1 - \zeta_l) = 1 + \zeta_l + \zeta_l^2 + \cdots + \zeta_l^{i-1}$. Ukážeme, že u_i je jednotka okruhu celých algebraických čísel v K_l. Protože $l \nmid i$, musí existovat $j \in \mathbb{Z}$ takové, že $ij \equiv 1 \pmod{l}$. Tedy

$$u_i^{-1} = (1 - \zeta_l)/(1 - \zeta_l^i) = (1 - \zeta_l^{ij})/(1 - \zeta_l^i) = 1 + \zeta_l^i + \zeta_l^{2i} + \cdots + \zeta_l^{(j-1)i}$$

je celé algebraické číslo, odkud plyne, že u_i je skutečně jednotka.

Po dosazení máme $l = \prod_{i=1}^{l-1}(1 - \zeta_l^i) = (1 - \zeta_l)^{l-1} \prod_{i=1}^{l-1} u_i$ a tedy $(l) = L^{l-1}$. Užitím vztahu $efg = \phi(l) = l - 1$ dostáváme, že $e = l - 1$, $f = 1$ a $g = 1$. Proto je L skutečně prvoideál stupně 1. □

Tvrzení 3.5.10. *Nechť P je prvoideál v K_m a označme $P \cap \mathbb{Z} = p\mathbb{Z}$. Je-li p liché, pak se P větví právě tehdy, když $p|m$. V případě $p = 2$ se P větví, právě když $4|m$.*

Důkaz. Z tvrzení 3.5.6 víme, že pokud $p \nmid m$, P se nevětví.

Nejprve předpokládejme, že p je liché a $p|m$. Pak $K_p \subseteq K_m$. Označme D_p a D_m příslušné okruhy celých algebraických čísel těles K_p a K_m. Podle předchozího tvrzení je $pD_p =$

$(1-\zeta_p)^{p-1}$. Pišme $(1-\zeta_p)D_m = P_1P_2\cdots P_t$, kde všechna P_i jsou ne nutně různé prvoideály v D_m. Pak $pD_m = (P_1P_2\cdots P_t)^{p-1}$. Protože $p-1>1$, plyne odsud, že se všechny prvoideály dělící (p) větví.

Nyní předpokládejme, že $p=2$. Pokud $2|m$, ale $4\nmid m$, lze psát $m=2m_0$, kde m_0 je liché. V tomto případě je $-\zeta_{m_0}$ primitivní m-tá odmocnina z jedničky a tedy $K_m = K_{m_0}$. Protože však $2\nmid m_0$, dostáváme z tvrzení 3.5.6, že se P nevětví.

Konečně nechť $p=2$ a $4|m$. Pak $\zeta_4 = \sqrt{-1} = i \in K_m$. Protože $(1-i)^2 = -2i$, vidíme, že $2D_m = ((1-i)D_m)^2$, odkud podobně jako v prvním případě plyne, že se všechny prvoideály dělící (2) větví. □

Nechť p je prvočíslo, které nedělí m. Pro pozdější využití ještě odvodíme, jak se (p) rozkládá v tělese $\mathbb{Q}(\zeta_p,\zeta_m)$.

Lemma 3.9. *Nechť m a n jsou přirozená nesoudělná čísla. Pak $\mathbb{Q}(\zeta_m,\zeta_n) = \mathbb{Q}(\zeta_{mn})$.*

Důkaz. Zřejmě platí $\mathbb{Q}(\zeta_m,\zeta_n)\subseteq\mathbb{Q}(\zeta_{mn})$, neboť $\zeta_{mn}^m = \zeta_n$ a $\zeta_{mn}^n = \zeta_m$.

Na druhou stranu, protože $(m,n)=1$, musí existovat celá čísla u,v taková, že $um+vn=1$. Tedy $\zeta_{mn} = \zeta_{mn}^{um}\zeta_{mn}^{vn} = \zeta_n^u\zeta_m^v \in \mathbb{Q}(\zeta_m,\zeta_n)$. □

Tvrzení 3.5.11. *Nechť p je prvočíslo, $p\nmid m$. Označme D_{mp} okruh celých algebraických čísel v K_{mp}. Pak*

$$pD_{mp} = (P_1P_2\cdots P_g)^{p-1},$$

kde P_i jsou různé prvoideály stupně $f=\phi(m)/g$. Navíc platí, že f je právě řád p modulo m.

Důkaz. Protože $K_p\subseteq K_{mp}$, je index větvení každého prvoideálu dělícího (p) dělitelný $(p-1)$. Tedy

$$pD_{mp} = (P_1P_2\cdots P_{g'})^{e'(p-1)}, \qquad (*)$$

kde všechny P_i jsou po dvou různé prvoideály stupně f' a $e'\in\mathbb{N}$.

Označme D_m okruh celých algebraických čísel v K_m. Podle věty 3.5.8 se (p) v D_m rozkládá

$$pD_m = P_1'P_2'\cdots P_g',$$

kde P_i' jsou prvoideály v D_m stupně $f=\phi(m)/g$ a platí, že f je řád p modulo m.

Pro libovolný prvoideál $\mathfrak{P}$ v D_{mp}, který dělí P_i' platí $P_i' = \mathfrak{P}\cap D_m$. Rozklady P_i' a P_j' v D_{mp} pro $i\neq j$ proto nemají žádné společné prvoideály. Z $(*)$ tedy plyne $f'\geq f$ a $g'\geq g$.

Konečně opět z $(*)$ za použití lemmatu 3.9 postupně dostáváme

$$(p-1)\phi(m) = \phi(pm) = e'(p-1)f'g' \geq e'(p-1)f\frac{\phi(m)}{f},$$

odkud $e'\leq 1$. Tedy $e=1$ u všech zmíněných nerovností nastává rovnost, tj. $f'=f$ a $g'=g$. Tím je důkaz hotov. □

4 Gaussovy sumy

Tato kapitola uvádí pojem Gaussových sum, které jsou důležitou součástí studia diofantických rovnic. V prvním odstavci poskytneme nutné minimum z teorie charakterů, v dalším odstavci zadefinujeme Gaussovy sumy nad obecným konečným tělesem. V poslední, nejrozsáhlejší, části se budeme věnovat faktorizaci význačných Gaussových sum v kruhových tělesech. Tuto faktorizaci v další kapitole využijeme k důkazům anihilace grupy tříd ideálů číselných abelovských rozšíření.

Výsledky z teorie Gaussových sum lze najít např. v [3]. Odvození Stickelbergerovy relace v odstavci 4.3 je však obecnější, což využijeme v poslední kapitole.

4.1 Charaktery

V této a následující sekci budeme pracovat s pevným konečným tělesem; označme jej $\mathbb{F}$. Jeho charakteristiku označme p a počet jeho prvků $q = p^f$.

Definice. Zobrazení χ z $\mathbb{F}^\times$ do $\mathbb{C}^\times$ nazveme *multiplikativní charakter*, pokud splňuje

$$\chi(ab) = \chi(a)\chi(b) \qquad \text{pro všechna } a, b \in \mathbb{F}^\times,$$

neboli je to homomorfismus příslušných multiplikativních grup.

Speciálně značíme ε triviální charakter, tj. charakter splňující $\varepsilon(a) = 1$ pro všechna $a \in \mathbb{F}^\times$.

Někdy je vhodné rozšířit definiční obor charakterů na celé $\mathbb{F}$. Pro $\chi \neq \varepsilon$ definujeme $\chi(0) = 0$. Pro ε definujeme $\varepsilon(0) = 1$.

Nejprve uvedeme některé základní vlastnosti multiplikativních charakterů.

Tvrzení 4.1.1. *Nechť χ je multiplikativní charakter a $a \in \mathbb{F}^\times$. Pak*

(a) $\chi(1) = 1$.
(b) $\chi(a)$ *je* $(q-1)$*-tá odmocnina z jedné.*
(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$ *(pruh zde značí komplexní konjugaci).*

Důkaz.

(a) $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. Odsud $\chi(1) = 1$, neboť $\chi(1) \neq 0$.
(b) $\chi(a)^{q-1} = \chi(a^{q-1}) = \chi(1) = 1$. Použili jsme fakt, že $q-1$ je řád grupy $\mathbb{F}^\times$.
(c) $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$. Tedy $\chi(a)^{-1} = \chi(a^{-1})$. Rovnost $\chi(a)^{-1} = \overline{\chi(a)}$ plyne z toho, že $\chi(a)$ je komplexní číslo s absolutní hodnotou rovnou jedné.

□

Tvrzení 4.1.2. *Nechť χ je netriviální multiplikativní charakter. Pak* $\sum_{t\in\mathbb{F}} \chi(t) = 0$

Důkaz. Nechť $a \in \mathbb{F}$ je takové, že $\chi(a) \neq 1$ (pokud by neexistovalo, znamenalo by to $\chi = \varepsilon$). Označme $T = \sum_{t\in\mathbb{F}} \chi(t)$. Pak

$$\chi(a)T = \sum_{t\in\mathbb{F}} \chi(a)\chi(t) = \sum_{t\in\mathbb{F}} \chi(at) = T,$$

odkud $T = 0$. Poslední rovnost plyne z toho, že pokud t probíhá $\mathbb{F}$, probíhá i at celé $\mathbb{F}$. □

Definice. Zobrazení ψ z $\mathbb{F}$ do $\mathbb{C}^\times$ nazveme *aditivní charakter*, pokud splňuje

$$\psi(a+b) = \psi(a)\psi(b) \qquad \text{pro všechna } a, b \in \mathbb{F}.$$

Tentokrát jde tedy o homomorfismus z aditivní grupy F.

Triviálním aditivním charakterem nazýváme konstantní zobrazení $\psi(a) = 1$ pro všechna $a \in \mathbb{F}$.

Opět uvedeme některé vlastnosti aditivních charakterů.

Tvrzení 4.1.3. *Nechť ψ je aditivní charakter a $a \in \mathbb{F}$. Pak*

(a) $\psi(0) = 1$.
(b) $\psi(a)$ *je p-tá odmocnina z jedné.*
(c) $\psi(-a) = \psi(a)^{-1} = \overline{\psi(a)}$.

Důkaz. Dokáže se analogicky jako v případě multiplikativních charakterů. □

Tvrzení 4.1.4. *Je-li ψ netriviální aditivní charakter. Pak $\sum_{t\in\mathbb{F}} \psi(t) = 0$ a pro libovolné $x, y \in \mathbb{F}$ platí $\sum_{t\in\mathbb{F}} \psi(t(x-y)) = \delta(x,y)q$, kde $\delta(x,y) = 1$ pro $x = y$ a $\delta(x,y) = 0$ jinak.*

Důkaz. Podobně jako v případě multiplikativních charakterů zvolme libovolné $a \in \mathbb{F}$ takové, že $\psi(a) \neq 1$ a označme $T = \sum_{t\in\mathbb{F}} \psi(t)$. Pak

$$\psi(a)T = \sum_{t\in\mathbb{F}} \psi(a)\psi(t) = \sum_{t\in\mathbb{F}} \psi(a+t) = T,$$

neboť zřejmě $a + t$ probíhá celé $\mathbb{F}$. Protože $\psi(a) \neq 1$, musí být $T = 0$.

Je-li $x \neq y$, máme z podobných důvodů $\sum_{t\in\mathbb{F}} \psi(t(x-y)) = T = 0$. Pro $x = y$ je součet roven $q \cdot 1 = q$. Tím je důkaz hotov. □

Jsou-li χ a λ multiplikativní charaktery, můžeme zadefinovat jejich součin jako zobrazení $\chi\lambda$ dané předpisem $\chi\lambda(a) = \chi(a)\lambda(a)$ pro všechna $a \in \mathbb{F}^\times$. Podobně můžeme definovat zobrazení χ^{-1} předpisem $\chi^{-1}(a) = \chi(a)^{-1}$ pro všechna $a \in \mathbb{F}^\times$. Snadno se ověří, že takto definovaná zobrazení jsou opět multiplikativní charaktery. Množina všech multiplikativních charakterů tedy tvoří grupu.

Podobně můžeme naložit i s aditivními charaktery. Pro libovolné dva aditivní charaktery ψ, ϕ definujeme $\psi\phi(a) = \psi(a)\phi(a)$ a $\psi^{-1}(a) = \psi(a)^{-1}$ pro všechna $a \in \mathbb{F}$. Aditivní charaktery tedy také tvoří grupu. Můžeme proto používat např. označení ψ^a, kde $a \in \mathbb{F}$, značící aditivní charakter definovaný vztahem $\psi^a(t) = \psi(at)$.

4.2 Gaussovy sumy

Definice. Nechť χ je multiplikativní charakter na $\mathbb{F}$ a ψ je aditivní charakter na $\mathbb{F}$. *Gaussovou sumou* příslušnou charakterům χ a ψ nazýváme číslo

$$g(\chi,\psi)=\sum_{t\in\mathbb{F}}\chi(t)\psi(t).$$

Tvrzení 4.2.1. *Pro libovolný multiplikativní charakter $\chi\neq\varepsilon$ a libovolný aditivní charakter ψ a $a\in\mathbb{F}^\times$ platí*

$$g(\chi,\psi^a)=\chi(a)^{-1}g(\chi,\psi).$$

Důkaz.

$$g(\chi,\psi^a)=\sum_{t\in\mathbb{F}}\chi(t)\psi^a(t)=\sum_{t\in\mathbb{F}}\chi(t)\psi(at)$$

$$=\chi(a)^{-1}\sum_{t\in\mathbb{F}}\chi(at)\psi(at)=\chi(a)^{-1}g(\chi,\psi)$$

Poslední rovnost plyne opět z úvahy, že pokud t probíhá $\mathbb{F}$, probíhá i at celé $\mathbb{F}$. □

Tvrzení 4.2.2. *Je-li χ netriviální multiplikativní charakter a ψ netriviální aditivní charakter, pak $|g(\chi,\psi)|=\sqrt{q}$.*

Důkaz. Vyjádříme sumu $\sum_{a\in\mathbb{F}}g(\chi,\psi^a)\overline{g(\chi,\psi^a)}$ dvěma způsoby.

Je-li $a\neq 0$, je podle tvrzení 4.2.2 $\underline{g(\chi,\psi^a)}=\chi(a)^{-1}g(\chi,\psi)$ a $\overline{g(\chi,\underline{\psi^a})}=\overline{\chi(a)^{-1}g(\chi,\psi)}=\chi(a)\overline{g(\chi,\psi)}$. Celkem tedy $g(\chi,\psi^a)\overline{g(\chi,\psi^a)}=\chi(a)^{-1}\chi(a)g(\chi,\psi)\overline{g(\chi,\psi)}=|g(\chi,\psi)|^2$. Pro $a=0$ máme podle tvrzení 4.1.2 $g(\chi,\psi)=0$. Celkový součet je tedy roven $\sum_{a\in\mathbb{F}^\times}|g(\chi,\psi)|^2=(q-1)|g(\chi,\psi)|^2$

Na druhou stranu

$$g(\chi,\psi^a)\overline{g(\chi,\psi^a)}=\sum_{x\in\mathbb{F}}\sum_{y\in\mathbb{F}}\chi(x)\overline{\chi(y)}\psi(a(x-y)).$$

Sečtením přes $a\in\mathbb{F}$ dostaneme za použití tvrzení 4.1.4

$$\sum_{a\in\mathbb{F}}g(\chi,\psi^a)\overline{g(\chi,\psi^a)}=\sum_{x\in\mathbb{F}}\sum_{y\in\mathbb{F}}\chi(x)\overline{\chi(y)}\delta(x,y)q=(q-1)q.$$

Porovnáním obou výsledků dostáváme $(q-1)|g(\chi,\psi)|^2=(q-1)q$ odkud $|g(\chi,\psi)|=\sqrt{q}$. □

Tvrzení 4.2.3. *Nechť χ je netriviální multiplikativní charakter a ψ je libovolný aditivní charakter. Pak pro příslušnou Gaussovu sumu platí*

$$\overline{g(\chi,\psi)}=\chi(-1)g(\chi^{-1},\psi).$$

Důkaz.

$$\overline{g(\chi,\psi)} = \sum_{t\in\mathbb{F}} \overline{\chi(t)}\,\overline{\psi(t)} = \sum_{t\in\mathbb{F}} \chi(t)^{-1}\psi(-t) = \chi(-1)\sum_{t\in\mathbb{F}} \chi^{-1}(-t)\psi(-t) = \chi(-1)g(\chi^{-1},\psi),$$

neboť $t \mapsto -t$ je bijekce na $\mathbb{F}$ a $\chi^{-1}(-1) = \chi(-1) = \pm 1$. □

Tvrzení 4.2.4. *Nechť χ, λ jsou netriviální multiplikativní charaktery takové, že $\chi\lambda \neq \varepsilon$ a ψ je libovolný netriviální aditivní charakter. Pak číslo*

$$\frac{g(\chi,\psi)g(\lambda,\psi)}{g(\chi\lambda,\psi)}$$

je celé algebraické a leží v K_{q-1}.

Důkaz. Jednoduchými úpravami postupně dostáváme

$$g(\chi,\psi)g(\lambda,\psi) = \left(\sum_{x\in\mathbb{F}} \chi(x)\psi(x)\right)\left(\sum_{y\in\mathbb{F}} \lambda(y)\psi(y)\right) =$$

$$= \sum_{x,y\in\mathbb{F}} \chi(x)\lambda(y)\psi(x+y) = \sum_{t\in\mathbb{F}} \left(\sum_{x+y=t} \chi(x)\lambda(y)\right)\psi(t).$$

Pro $t = 0$ je výraz roven $\sum_{x\in\mathbb{F}} \chi(x)\lambda(-x) = \lambda(-1)\sum_{x\in\mathbb{F}} \chi\lambda(x) = 0$ podle tvrzení 4.1.2. Pro $t \neq 0$ pišme $x = tx'$ a $y = ty'$. Po dosazení máme

$$g(\chi,\psi)g(\lambda,\psi) = \sum_{t\in\mathbb{F}} \left(\sum_{x'+y'=1} \chi\lambda(t)\chi(x')\lambda(y')\right)\psi(t) = g(\chi\lambda,\psi)\sum_{x'+y'=1} \chi(x')\lambda(y').$$

Výraz $J(\chi,\lambda) = \sum_{x+y=1} \chi(x)\lambda(y)$ se nazývá *Jacobiho suma* a má velký význam při řešení diofantických rovnic. Ihned je vidět, že $J(\chi,\lambda) \in K_{q-1}$ a že je celé algebraické. Podle tvrzení 4.2.2 je $g(\chi\lambda,\psi) \neq 0$ a tedy $\frac{g(\chi,\psi)g(\lambda,\psi)}{g(\chi\lambda,\psi)} = J(\chi,\lambda)$. Tím je důkaz hotov. □

4.3 Faktorizace Gaussových sum v kruhových tělesech

V teto sekci odvodíme faktorizaci speciálních Gaussových sum v kruhových tělesech. Od počátku zvolme pevně přirozené číslo m a označme D_m okruh celých algebraických čísel v tělese $K_m = \mathbb{Q}(\zeta_m)$. Dále zvolme v D_m pevně prvoideál P, který neobsahuje m. Nyní zadefinujeme charaktery příslušné prvoideálu P.

Označme $P \cap \mathbb{Z} = p\mathbb{Z}$, $F = D_m/P$, $|F| = p^f = q$. Pak na F definujeme multiplikativní charakter χ_P takto: Pro libovolné $t \in F^\times$ je $\chi_P(t)$ rovno takové m-té odmocnině z jedné, že platí

$$\overline{\chi_P(t)} = t^{(q-1)/m},$$

kde $\overline{\chi_P(t)}$ je zbytková třída příslušná $\chi_P(t)$ v D_m/P. Obvyklým způsobem pak dodefinujeme $\chi_P(0) = 0$.

Musíme ukázat, že předepsaná m-tá odmocnina z jedné existuje. Všechny prvky z $F^\times$ splňují rovnici $x^{q-1}-1=0$. Z tvrzení 3.5.3 víme, že $m|q-1$ a tedy

$$x^{q-1}-1=\prod_{i=0}^{m-1}(x^{(q-1)/m}-\overline{\zeta_m^i}).$$

Podle tvrzení 3.5.3 též víme, že je tato m-tá odmocnina z jedné určena jednoznačně. Zbývá ověřit, že je χ_P skutečně multiplikativní charakter; to je však snadné. Poznamenejme ještě, že χ_P má jakožto prvek grupy multiplikativních charakterů řád m. Skutečně, je-li g prvek $F^\times$ řádu $q-1$, je $\overline{\chi_P(g)}$ řádu m.

Aditivní charakter příslušný prvoideálu P definujeme pro libovolné $t\in F$ vztahem

$$\psi_P(t)=\zeta_p^{\mathrm{tr}(t)},$$

kde $\mathrm{tr}: F\to\mathbb{Z}/p\mathbb{Z}$ je zobrazení stopy, tj. $\mathrm{tr}(t)=t+t^p+\cdots+t^{p^{f-1}}$.

Nyní již můžeme pro libovolné $a\in\mathbb{Z}$, $m\nmid a$ definovat Gaussovu sumu $g_a(P)=g(\chi_P^{-a},\psi_P)=\sum_{t\in F}\chi_P^{-a}(t)\psi_P(t)$. Dále označme $\Phi_a(P)=g_a(P)^m$.

Tvrzení 4.3.1. *Pro libovolné celé číslo a, $m\nmid a$ platí*

(a) $g_a(P)\in D_{mp}$
(b) $|g_a(P)|^2=q$
(c) $\Phi_a(P)\in D_m$

Důkaz.

(a) $\chi_P(t)^{-a}\in D_m\subset D_{mp}$ a $\psi_P(t)\in D_p\subset D_{mp}$
(b) χ_P je řádu m, proto je χ_P^a netriviální. Stopa není identicky nulová a tedy ψ_P je též netriviální. Výsledek plyne přímo z tvrzení 4.2.2.
(c) Libovolný prvek $\sigma_c\in\mathrm{Gal}(K_{mp}/K_m)$ splňuje $\sigma_c(\zeta_m)=\zeta_m$ a tedy $c\equiv 1\pmod m$. Připomeňme, že podle sekce 3.5 je $(c,mp)=1$, odkud $(c,p)=1$. Pro libovolné $t\in F$ tedy platí $\chi_P^{-a}(t)^{\sigma_c}=\chi_P^{-a}(t)$ a $\psi_P(t)^{\sigma_c}=\psi_P(t)^c=\psi_P(\overline{c}t)$. Celkově máme

$$g_a(P)^{\sigma_c}=\sum_{t\in F}\chi_P^{-a}(t)\psi_P(\overline{c}t)=\chi_P^a(\overline{c})g_a(P),$$

kde $\overline{c}$ je zbytková třída příslušná c v D_m/P (zřejmě $\overline{c}\neq 0$).
Po umocnění na m-tou dostáváme $\Phi_a(P)^{\sigma_c}=\Phi_a(P)$ odkud $\Phi_a(P)\in K_m$.

□

V dalším budeme zkoumat faktorizaci $g_a(P)$. Nejprve uvedeme tři pomocná tvrzení, která použijeme později.

Lemma 4.1. *Nechť $p>1$ je přirozené číslo. Pak lze každé kladné celé číslo a psát jednoznačně ve tvaru $a=\sum_{i=0}^n a_ip^i$, kde $0\le a_i<p$.*

Důkaz. Zřejmě existuje jediné nezáporné celé n s vlastností $p^n \le a < p^{n+1}$. Můžeme tedy psát $a = a_n p^n + r$, kde $0 \le r < p^n$. Jistě je a_n menší než p (jinak by bylo $a \ge p^{n+1}$). Tento proces můžeme opakovat pro r namísto a; po konečném počtu kroků dostaneme požadovaný tvar.

Zbývá dokázat jednoznačnost. Nechť $\sum a_i p^i = \sum b_i p^i$, kde $0 \le a_i, b_i < p$. Sporem předpokládejme, že tato vyjádření nejsou shodná. Vezměme nejmenší takové k, pro které $a_k \ne b_k$. Protože $0 < |a_k - b_k| < p$, platí $p \nmid (a_k - b_k)$, odkud $p^{k+1} \nmid (\sum a_i p^i - \sum b_i p^i) = 0$. Spor. □

Definice. Nechť $q = p^f$. Pro $0 \le a < q-1$ pišme $a = \sum_{i=0}^{f-1} a_i p^i$, kde $0 \le a_i < p$ a definujeme $S(a) = \sum_{i=0}^{f-1} a_i$. Pro libovolné kladné celé a definujeme $S(a) = S(r)$, kde $a \equiv r \pmod{q-1}$, $0 \le r < q-1$.

Definice. Pro libovolné reálné číslo x definujeme, jeho *celou část* $[x]$ jako to jediné celé číslo, které splňuje $0 \le x - [x] < 1$. *Necelou část* z čísla x, značeno $\langle x \rangle$, definujeme vztahem $\langle x \rangle = x - [x]$.

Lemma 4.2. *Pro libovolné celé číslo a platí*

$$S(a) = (p-1) \sum_{i=0}^{f-1} \left\langle \frac{p^i a}{q-1} \right\rangle.$$

Důkaz. Obě strany rovnosti se nezmění přičtením libovolného násobku $(q-1)$ k a. Můžeme tedy předpokládat $0 \le a < q-1$.

Pišme $a = a_0 + a_1 p + \cdots + a_{f-1} p^{f-1}$, kde $0 \le a_i < p$. Uvážíme-li, že $p^f = q \equiv 1 \pmod{q-1}$, dostáváme

$$\begin{array}{lcll} a & = & a_0 + a_1 p + \cdots + a_{f-1} p^{f-1} & \\ pa & \equiv & a_{f-1} + a_0 p + \cdots + a_{f-2} p^{f-1} & \pmod{q-1} \\ p^2 a & \equiv & a_{f-2} + a_{f-1} p + \cdots + a_{f-3} p^{f-1} & \pmod{q-1} \\ \text{atd.} & & & \end{array}$$

Pravé strany těchto kongruencí jsou menší než $q-1$, proto je $\langle p^i a/(q-1) \rangle$ rovno pravé straně i-té kongruence podělené $q-1$. Celkem tedy

$$\sum_{i=0}^{f-1} \left\langle \frac{p^i a}{q-1} \right\rangle = \frac{1}{q-1} S(a)(1 + p + \cdots + p^{f-1}) = S(a)/(p-1)$$

což jsme chtěli dokázat. □

Lemma 4.3. $\sum_{a=1}^{q-2} S(a) = \frac{f(p-1)(q-2)}{2}$

Důkaz. Pišme znovu $a = a_0 + a_1 p + \cdots + a_{f-1} p^{f-1}$, kde $0 \le a_i < p$. Uvažme navíc, že $q - 1 = (p-1) + (p-1)p + \cdots + (p-1)p^{f-1}$. Odsud $q - 1 - a = (p - 1 - a_0) + (p - 1 - a_1)p + \cdots + (p - 1 - a_{f-1})p^{f-1}$ a tedy

$$S(a) + S(q - 1 - a) = f(p-1)$$

Sečtením přes a od 1 do $q-2$ dostaneme $2 \cdot \sum_{a=1}^{q-2} S(a) = f(p-1)(q-2)$. □

Gaussova suma $g_a(P)$ je prvkem tělesa K_{mp}. Odvození faktorizace $\Phi_a(P)$ však vyžaduje práci ve větším tělese $K_{(q-1)p}$. Výhodou je, že můžeme používat $(q-1)$-té odmocniny z jedné. S přibývajícím počtem těles je však třeba zvýšené opatrnosti na to, v jakém tělese se právě pohybujeme. Následující diagram osvětluje situaci a bude užitečný v dalších úvahách.

$$\begin{array}{ccccc}
\wp & \subset & D_{(q-1)p} & \to & D_{(q-1)p}/\wp \\
| & & | & & | \\
\mathfrak{P} & \subset & D_{q-1} & \to & D_{q-1}/\mathfrak{P} \\
| & & | & & | \\
P & \subset & D_m & \to & D_m/P \\
| & & | & & | \\
(p) & \subset & \mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z}
\end{array}$$

V tomto diagramu jsou (p), P, $\mathfrak{P}$ a $\wp$ prvoideály příslušných okruhů celých čísel. Připomínáme, že $p \nmid m$, f je řád p modulo m, tedy $p^f \equiv 1 \pmod m$ a $q = p^f$. Dále označme $\lambda_p = 1 - \zeta_p$.

Lemma 4.4.

(1) $\operatorname{ord}_\wp(pD_{(q-1)p}) = p-1$
(2) $\operatorname{ord}_\wp(\lambda_p D_{(q-1)p}) = 1$
(3) $\operatorname{ord}_\wp(P) = p-1$

Důkaz.

(1) Protože $\wp$ leží nad p, musí být obsaženo v rozkladu $pD_{(q-1)p}$. Z tvrzení 3.5.11 (m nahrazeno $q-1$) máme přímo $\operatorname{ord}_\wp(pD_{(q-1)p}) = p-1$.
(2) Podle téhož tvrzení a tvrzení 3.5.9 je $pD_{(q-1)p} = (pD_p)D_{(q-1)p} = \lambda_p^{p-1} D_{(q-1)p} = (\wp_1 \cdots \wp_h)^{p-1}$, kde např. $\wp_1 = \wp$. Je tedy $\lambda_p D_{(q-1)p} = (\wp_1 \cdots \wp_h)$. Odsud máme $\operatorname{ord}_\wp(\lambda_p D_{(q-1)p}) = 1$.
(3) Podle věty 3.5.8 a tvrzení 3.5.11 máme rovnosti $PP_2 \cdots P_h \cdot D_{(q-1)p} = pD_{(q-1)p} = (\wp\wp_2 \cdots \wp_h)^{p-1}$, kde prvoideály v obou rozkladech jsou různé a $P, P_2, \ldots, P_h$ jsou po dvou nesoudělné. Musí tedy platit $PD_{(q-1)p} = \wp^{p-1}$, odkud přímo dostáváme $\operatorname{ord}_\wp(P) = p-1$.

□

Lemma 4.5. *Zobrazení $\tau : D_m/P \to D_{q-1}/\mathfrak{P}$ dané pro libovolné $\alpha \in D_m$ předpisem $\tau(\alpha + P) = \alpha + \mathfrak{P}$ je izomorfismus $D_m/P \cong D_{q-1}/\mathfrak{P}$.*

Důkaz. Zřejmě je τ dobře definovaný homomorfismus těles neboť $\mathfrak{P}|P$. Jsou-li $\alpha, \beta \in D_m$ taková, že $\alpha \equiv \beta \pmod{\mathfrak{P}}$, je $\alpha - \beta \in \mathfrak{P} \cap D_m = P$ a tedy $\alpha \equiv \beta \pmod P$, čím jsme dokázali, že je τ prosté. K důkazu surjektivity stačí vzhledem ke konečnosti obou těles ověřit, že mají stejný počet prvků. Podle věty 3.5.8 je $|D_{q-1}/\mathfrak{P}| = p^{f'}$, kde f' je nejmenší kladné celé číslo takové, že $p^{f'} \equiv 1 \pmod{q-1}$. Protože $q = p^f$, jistě platí i $p^f \equiv 1 \pmod{q-1}$ a tedy $f' \le f$, odkud $f' = f$. Celkově $|D_{q-1}/\mathfrak{P}| = p^f = |D_m/P|$. □

Můžeme tedy ztotožnit zbytkovou třídu příslušnou α v D_m/P a třídu příslušnou α v $D_{q-1}/\mathfrak{P}$. Protože nemůže dojít k dvojznačnosti, budeme obě třídy značit $\overline{\alpha}$.

Na $\mathfrak{F} = D_{q-1}/\mathfrak{P}$ nyní zadefinujeme multiplikativní charakter $\chi_\mathfrak{P}$ podobně jako v tělese K_m, tj. pro libovolné $t \in \mathfrak{F}$ je $\chi_\mathfrak{P}(t)$ taková $(q-1)$-tá odmocnina z jedné, že platí $\overline{\chi_\mathfrak{P}(t)} = t$ (pruh zde značí příslušnou zbytkovou třídu v $D_{q-1}/\mathfrak{P}$).

Lemma 4.6. *Pro $\alpha \in D_m$ platí $\chi_\mathfrak{P}(\overline{\alpha})^{(q-1)/m} = \chi_P(\overline{\alpha})$.*

Důkaz. Platí $\chi_\mathfrak{P}(\overline{\alpha}) \equiv \alpha \pmod{\mathfrak{P}}$ a $\chi_P(\overline{\alpha}) \equiv \alpha^{(q-1)/m} \pmod{P}$. Podobně jako v důkazu lemmatu 4.5 víme, že v D_m jsou kongruence modulo P a modulo $\mathfrak{P}$ ekvivalentní. Umocníme-li první zmíněnou na $\frac{q-1}{m}$, dostáváme

$$\chi_\mathfrak{P}(\overline{\alpha})^{(q-1)/m} \equiv \chi_P(\overline{\alpha}) \pmod{P}.$$

Obě strany jsou však m-tými odmocninami z jedné; zbytkové třídy různých m-tých odmocniny z jedné jsou podle tvrzení 3.5.3 různé. Kongruence tedy přechází v rovnost. □

Lemma 4.7. *Pro libovolné celé číslo i platí $\chi_\mathfrak{P}(\overline{\zeta_{q-1}^i}) = \zeta_{q-1}^i$.*

Důkaz. Výrazy jsou kongruentní modulo $\mathfrak{P}$ a oba jsou $(q-1)$-tými odmocninami z jedné. Musí se tedy rovnat. □

Definice. Nechť a je celé číslo. Na $\mathfrak{F} = D_{q-1}/\mathfrak{P}$ definujeme $\mathfrak{g}_a = g(\chi_\mathfrak{P}^{-a}, \psi_\mathfrak{P}) = \sum_{t\in\mathfrak{F}} \chi_\mathfrak{P}^{-a}(t)\psi_\mathfrak{P}(t)$.

Uvážíme-li, že pro libovolné $\alpha \in D_m$ je $\psi_\mathfrak{P}(\overline{\alpha}) = \psi_P(\overline{\alpha})$, pomocí lemmatu 4.6 dostáváme, že $g_a(P) = \mathfrak{g}_{a(q-1)/m}$.

Věta 4.3.2. *Pro $1 \le a < q-1$ je $\operatorname{ord}_\wp(\mathfrak{g}_a) = S(a)$.*

Důkaz. Nejprve dokážeme, že $\operatorname{ord}_\wp(\mathfrak{g}_1) = 1$. Podle definice je

$$\mathfrak{g}_1 = \sum_{t\in\mathfrak{F}} \chi(t)^{-1}\zeta_p^{\operatorname{tr}(t)}.$$

Pomocí lemmatu 4.7 a tvrzení 3.5.3 tuto sumu převedeme na sumu přes mocniny ζ_{q-1}. Nechť m_i je kladné celé číslo takové, že

$$\zeta_p^{m_i} = \zeta_p^{\operatorname{tr}(\overline{\zeta_{q-1}})}.$$

Připomeňme, že $\zeta_p = 1 - \lambda_p$. Pak

$$\mathfrak{g}_1 = \sum_{i=0}^{q-2} \zeta_{q-1}^{-i}(1-\lambda_p)^{m_i}$$

Pomocí binomické věty dostáváme $(1-\lambda_p)^{m_i} \equiv (1 - m_i\lambda_p) \pmod{\wp^2}$ a tedy

$$\mathfrak{g}_1 \equiv -\left(\sum_{i=0}^{q-2} m_i\zeta_{q-1}^{-i}\right)\lambda_p \pmod{\wp^2}.$$

Nyní $m_i\lambda_p \equiv (\zeta_{q-1}^i + \zeta_{q-1}^{pi} + \cdots + \zeta_{q-1}^{p^{f-1}i})\lambda_p \pmod{\wp^2}$. Po dosazení

$$\mathfrak{g}_1 \equiv -\sum_{i=0}^{q-2} \zeta_{q-1}^{-i}(\zeta_{q-1}^i + \zeta_{q-1}^{pi} + \cdots + \zeta_{q-1}^{p^{f-1}i})\lambda_p \pmod{\wp^2}.$$

Součet $\sum_{i=0}^{q-2} \zeta_{q-1}^{(p^j-1)i}$ je pro $j = 1, 2, \ldots, f-1$ roven nule a pro $j = 0$ je roven $q-1$. Jelikož je $q = p^f \equiv 0 \pmod{\wp}$, celkově dostáváme

$$\mathfrak{g}_1 \equiv \lambda_p \pmod{\wp^2}.$$

Z lemmatu 4.4 části (2) vidíme, že $\lambda_p \in \wp$, ale $\lambda_p \notin \wp^2$. Musí tedy být $\mathrm{ord}_\wp(\mathfrak{g}_1) = 1$.

Označme nyní $s(a) = \mathrm{ord}_\wp(g_a)$. Uvedeme několik vlastností funkce $s(a)$.

$$s(a+b) \le s(a) + s(b) \text{ za předpokladu } 1 \le a, b, a+b < q-1. \tag{1}$$

Je jednoduchou aplikací tvrzení 4.2.4

$$s(a+b) \equiv s(a) + s(b) \pmod{p-1} \tag{2}$$

S ohledem na tvrzení 4.2.4 stačí ukázat, že $\mathrm{ord}_\wp J(\chi_\mathfrak{P}^{-a}, \chi_\mathfrak{P}^{-b})$ je dělitelné $p-1$. To však plyne ze třetí části lemmatu 4.4 neboť opět podle tvrzení 4.2.4 leží $J(\chi_\mathfrak{P}^{-a}, \chi_\mathfrak{P}^{-b})$ v D_{q-1}.

$$s(pa) = s(a) \tag{3}$$

$\mathfrak{g}_{pa} = \sum_{t\in\mathfrak{F}} \chi_\mathfrak{P}(t)^{-pa}\psi(t) = \sum_{t\in\mathfrak{F}} \chi(t^p)^{-a}\psi(t^p)$. Použili jsme vztah $\mathrm{tr}(t) = \mathrm{tr}(t^p)$, jehož platnost lze snadno ověřit z definice stopy. Zobrazení $t \mapsto t^p$ je bijekce tělesa $\mathfrak{F}$ (složením se zobrazením $t \mapsto t^{p^{f-1}}$ získáme identitu), proto $\mathfrak{g}_{pa} = \mathfrak{g}_a$ a $s(pa) = s(a)$.

Na začátku důkazu jsme ukázali, že $s(1) = 1$. Užitím (1) a (2) dostaneme, že $s(a) = a$ pro $1 \le a < p$. Pro a mezi 1 a $q-1$ pišme $a = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}, 0 \le a_i < p$. Užitím (1) a (3) dostáváme

$$s(a) \le \sum_{j=0}^{f-1} s(a_j p^j) = \sum_{j=0}^{f-1} s(a_j) = \sum_{j=0}^{f-1} a_j = S(a)$$

Máme tedy $s(a) \le S(a)$ pro všechna uvažovaná a. K důkazu celého tvrzení již stačí (s ohledem na lemma 4.3) ukázat, že

$$\sum_{a=1}^{q-2} s(a) = \frac{f(p-1)(q-2)}{2}$$

Podle tvrzení 4.2.3 a 4.2.2 je $\mathfrak{g}_a\mathfrak{g}_{q-1-a} = \mathfrak{g}_a\mathfrak{g}_{-a} = \chi_\mathfrak{P}(-1)^a q = \chi_\mathfrak{P}(-1)^a p^f$. Aplikujeme-li $\mathrm{ord}_\wp$, za pomocí lemmatu 4.4 dostáváme

$$s(a) + s(q-1-a) = f(p-1)$$

Sečtením přes a jdoucí od 1 po $q-2$ dostáváme $\sum_{a=1}^{q-2} s(a) = \sum_{a=1}^{q-2} S(a)$ a tedy $s(a) = S(a)$ pro $1 \le a < q-1$, což jsme měli dokázat. □

Důsledek. *Pro libovolné celé číslo a, $m \nmid a$ platí* $\operatorname{ord}_P(\Phi_a(P)) = \frac{m}{p-1} S(a\frac{q-1}{m})$

Důkaz. Obě strany se nezmění, přičteme-li k a libovolný násobek čísla m, můžeme tedy předpokládat, že $1 \leq a < m$. Z lemmatu 4.4, části (3) plyne $(p-1)\operatorname{ord}_P(\Phi_a(P)) = \operatorname{ord}_\wp(\Phi_a(P))$. Víme však také, že $\operatorname{ord}_\wp(\Phi_a(P)) = m \operatorname{ord}_\wp(\mathfrak{g}_a(P)) = mS(a\frac{q-1}{m})$ (poslední rovnost plyne z předchozí věty, neboť $g_a(P) = \mathfrak{g}_{a(q-1)/m}$). □

Tento důsledek je prvním krokem k požadovanému rozkladu $(\Phi_a(P))$ na prvoideály v D_m.

Nyní, protože je podle tvrzení 4.2.2 $\Phi_a(P)\overline{\Phi_a(P)} = q^m = p^{fm}$, platí, že všechny prvoideály z D_m vyskytující se v rozkladu $(\Phi_a(P))$ dělí (p). Je-li P' jiný prvoideál obsahující p, podle tvrzení 3.4.4 existuje automorfismus $\sigma_t \in \operatorname{Gal}(K_m/\mathbb{Q})$ takový, že $P' = P^{\sigma_t^{-1}}$. Pro $1 \leq t < m$, $(t,m) = 1$ označme $P_t = P^{\sigma_t^{-1}}$.

Lemma 4.8. *Pro libovolné celé číslo a, $m \nmid a$ platí* $\operatorname{ord}_{P_t}(\Phi_a(P)) = \frac{m}{p-1} S(at\frac{q-1}{m})$

Důkaz. Aplikací σ_t máme

$$\operatorname{ord}_{P_t}(\Phi_a(P)) = \operatorname{ord}_P(\Phi_a(P)^{\sigma_t}).$$

Protože je $(m,p) = 1$, existuje celé číslo t' tak, že $t' \equiv t \pmod m$ a $t' \equiv 1 \pmod p$. Pak

$$g_a(P)^{\sigma_{t'}} = \left(\sum_{r\in F} \chi_P^{-a}(r)\psi(r)\right)^{\sigma_{t'}} = \sum_{r\in F} \chi_P(r)^{-at}\psi(r) = g_{at}^m(P),$$

odkud máme $\Phi_a(P)^{\sigma_t} = \Phi_a(P)^{\sigma_{t'}} = \Phi_{at}(P)$ a tedy podle předchozího důsledku

$$\operatorname{ord}_P(\Phi_a(P)^{\sigma_t}) = \operatorname{ord}_P(\Phi_{at}(P)) = \frac{m}{p-1} S\left(at\,\frac{q-1}{m}\right).$$

□

Definice. Nechť G je konečná abelovská multiplikativní grupa a R komutativní okruh. Množinu všech výrazů $\sum_{g\in G} a_g g$, nazýváme *grupový okruh* grupy G s koeficienty v R a značíme jej $R[G]$. Okruhové operace definujeme následovně

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g$$
$$\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g = \sum_{g\in G} c_g g,$$

kde $c_g = \sum_{fh=g} a_f b_h$. Snadno se ověří, že jde opravdu o komutativní okruh.

Označme $G = \mathrm{Gal}(K_m/\mathbb{Q})$. Prvky grupového okruhu $\mathbb{Q}[G]$ jsou tedy tvaru

$$\theta = \sum_{\sigma \in G} a_\sigma \sigma.$$

Přestože jsou tyto součty formální, přirozeně definujeme akci θ na libovolném $\alpha \in K_m$ předpisem

$$\alpha^\theta = \alpha^{\sum_{\sigma\in G} a_\sigma \sigma} = \prod_{\sigma \in G} (\alpha^\sigma)^{a_\sigma}.$$

Definice. Pro libovolná $m \in \mathbb{N}$ a $a \in \mathbb{Z}$ definujeme $\theta_m(a)$ jako prvek grupového okruhu $\mathbb{Q}[G]$ předpisem

$$\theta_m(a) = \sum_{(t,m)=1} \left\langle \frac{at}{m} \right\rangle \sigma_t^{-1},$$

kde sčítáme přes všechna $t \in \mathbb{Z}$, $1 \le t < n$. Prvek $\theta_m(a)$ nazýváme *Stickelbergerův prvek.*

Věta 4.3.3 (Stickelbergerova relace). *Nechť P je prvoideál v D_m, který neobsahuje m a a je celé číslo $m \nmid a$. Pak*

$$(\Phi_a(P)) = P^{m\theta_m(a)}$$

Důkaz. Připomeňme, že

$$G = \{\sigma_i | 1 \le i < m, (i,m) = 1\}$$
$$G(P) = \{\sigma \in G | P^\sigma = P\} = \langle \sigma_p \rangle$$

(podle důsledku věty 3.5.8).

Nechť jsou $P^{\sigma_{t_1}^{-1}}, P^{\sigma_{t_2}^{-1}}, \ldots, P^{\sigma_{t_g}^{-1}}$ všechny různé prvoideály v D_m dělící (p). Pak jsou $\sigma_{t_1}^{-1}, \ldots, \sigma_{t_g}^{-1}$ právě zástupci různých tříd $G/G(P)$ a tedy $t_1, \ldots, t_g$ spadají do různých zbytkových tříd v $(\mathbb{Z}/m\mathbb{Z})^\times/\langle p \rangle$. Odsud plyne, že pro každé $t \in \mathbb{Z}$, $1 \le t < m$, $(t,m) = 1$ existují $1 \le i \le g$ a $0 \le j \le f-1$ taková, že $t = t_i p^j$. Tato i, j jsou navíc jednoznačně určená.

Platí tedy $(\Phi_a(P)) = P^{\gamma'}$, kde (podle lemmatu 4.8)

$$\gamma' = \frac{m}{p-1} \sum_{i=1}^{g} S\left(at_i \frac{q-1}{m}\right) \sigma_{t_i}^{-1}.$$

S použitím lemmatu 4.2 dále dostáváme

$$\gamma' = m \sum_{i=1}^{g} \sum_{j=0}^{f-1} \left\langle \frac{at_i p^j}{m} \right\rangle \sigma_{t_i}^{-1}.$$

Protože je automorfismus σ_p na P identický, má γ na P stejný efekt jako

$$\gamma = m \sum_{i=1}^{g} \sum_{j=0}^{f-1} \left\langle \frac{at_i p^j}{m} \right\rangle \sigma_{t_i}^{-1} \sigma_{p^j}^{-1} = m \sum_{(t,m)=1} \left\langle \frac{at}{m} \right\rangle \sigma_t^{-1}.$$

□

Stickelbergerova relace je základním stavebním kamenem pro důkaz anihilace grupy tříd ideálů kruhových těles Stickelbergerovým ideálem, jak uvidíme v následující kapitole. Poznamenejme jen, že je také užitečná při studiu zákonů reciprocity (viz. např. [3] nebo [5]).

5 Stickelbergerův ideál

V této, poslední kapitole zavedeme Stickelbergerův ideál a jeho rozšířenou verzi definovanou Sinnottem v [8]. Ukážeme, že libovolný prvek Stickelbergerova ideálu anihiluje grupu tříd ideálů abelovských rozšíření racionálních čísel. Kapitolu zakončíme ilustrativním příkladem. Stickelbergerův ideál v původním tvaru uvádíme z historických důvodů a též pro srovnání s jeho rozšířenou verzí.

K důkazům anihilace je zapotřebí tzv. Čebotarevova věta o hustotě, přesněji řečeno, její důsledek, který zformulujeme bez důkazu. Podrobnější informace lze nalézt např. v [2].

Tvrzení 5.0.4. *Nechť $k/\mathbb{Q}$ je abelovské rozšíření těles. Pak existuje v každé třídě grupy tříd ideálů nekonečně mnoho prvoideálů, které se v okruhu celých čísel tělesa k zcela rozkládají, tj. jejich stupeň inercie a index větvení jsou rovny jedné.*

Protože existuje vždy jen konečně mnoho prvoideálů obsahujících předem zvolené číslo $n \in \mathbb{N}$, můžeme navíc předpokládat, že v každé třídě existuje nekonečně mnoho prvoideálů, které se zcela rozkládají a které neobsahují n.

5.1 Stickelbergerův ideál

V prvním odstavci se budeme zabývat Stickelbergerovým ideálem, který je definován např. v [3] nebo v [9], a ukážeme, že anihiluje grupu tříd ideálů v kruhových tělesech.

Zvolme opět pevně přirozené číslo $m > 1$. Připomeňme označení $K_m = \mathbb{Q}(\zeta_m)$, $D_m =$ okruh celých algebraických čísel v K_m, $G = \mathrm{Gal}(K_m/\mathbb{Q})$. V souladu s odstavcem 4.3 označme

$$\theta = \theta_m(1) = \sum_{(t,m)=1} \left\langle \frac{t}{m} \right\rangle \sigma_t^{-1},$$

kde t probíhá celá čísla v intervalu $1, \ldots, m-1$ nesoudělná s m.

Definice. V grupovém okruhu $\mathbb{Z}[G]$ definujeme ideál I vztahem

$$I = \theta\mathbb{Z}[G] \cap \mathbb{Z}[G]$$

a nazýváme jej *Stickelbergerův ideál.*

S využitím faktorizace Gaussových sum v kruhových tělesech odvozené v předchozí kapitole je důkaz anihilace relativně snadný.

V $\mathbb{Z}[G]$ definujme ideál $J = \langle b - \sigma_b | m \in \mathbb{Z}, (b,m) = 1 \rangle$, tj. ideál generovaný výrazy $b - \sigma_b$. Ideál J je generován prvky $b - \sigma_b$ pro $b \in \mathbb{Z}$, $(b,m) = 1$ již jako $\mathbb{Z}$-modul. To plyne z identity

$$\sigma_c(b - \sigma_b) = b\sigma_c - \sigma_{bc} = (bc - \sigma_{bc}) - b(c - \sigma_c).$$

Poznamenejme, že $m \in J$, neboť $m = ((b+m) - \sigma_{b+m}) - (b - \sigma_b)$.

Lemma 5.1. $I = \theta J$.

Důkaz. Nejprve dokážeme inkluzi $\theta J \subseteq I$. Stačí zřejmě ukázat, že pro libovolné $b \in \mathbb{Z}$, $(b,m)=1$ leží $(b-\sigma_b)\theta$ v $\mathbb{Z}[G]$.

$$\begin{aligned}(b-\sigma_b)\theta &= \sum_{(t,m)=1} b\left\langle \frac{t}{m}\right\rangle \sigma_t^{-1} - \sum_{(t,m)=1}\left\langle \frac{t}{m}\right\rangle \sigma_t^{-1}\sigma_b \\ &= \sum_{(t,m)=1} b\left\langle \frac{t}{m}\right\rangle \sigma_t^{-1} - \sum_{(t,m)=1}\left\langle \frac{bt}{m}\right\rangle \sigma_{bt}^{-1}\sigma_b \\ &= \sum_{(t,m)=1}\left(b\left\langle \frac{t}{m}\right\rangle - \left\langle \frac{bt}{m}\right\rangle\right)\sigma_t^{-1}\end{aligned}$$

Je vidět, že koeficienty u všech σ_t^{-1} jsou celočíselné.

Naopak, nechť $\beta = \sum_{(t,m)=1} b_t\sigma_t \in \mathbb{Z}[G]$ je takové, že $\beta\theta \in \mathbb{Z}[G]$. Pak

$$\beta\theta = \left(\sum_{(t,m)=1} b_t\sigma_t\right)\left(\sum_{(s,m)=1}\left\langle \frac{s}{m}\right\rangle \sigma_s^{-1}\right) = \sum_{(t,m)=1}\sum_{(s,m)=1} b_t\left\langle \frac{s}{m}\right\rangle \sigma_t\sigma_s^{-1}.$$

Nechť $1 \le c \le m-1$ je takové, že $s \equiv ct \pmod m$. Po dosazení máme

$$\beta\theta = \sum_{(c,m)=1}\sum_{(t,m)=1} b_t\left\langle \frac{ct}{m}\right\rangle \sigma_c^{-1}.$$

Automorfismy σ_c jsou po dvou různé. Má-li mít $\beta\theta$ celočíselné koeficienty, musí být zejména koeficient u identity (σ_1^{-1}) celočíselný. Tedy $\sum_{(t,m)=1} b_t\langle\frac{t}{m}\rangle \in \mathbb{Z}$ neboli $\sum_{(t,m)=1} tb_t \equiv 0 \pmod m$.

Pišme nyní

$$\beta\theta = \left(\sum_{(t,m)=1} b_t\sigma_t\right)\theta = -\left(\sum_{(t,m)=1} b_t(t-\sigma_t)\right)\theta + \left(\sum_{(t,m)=1} tb_t\right)\theta.$$

První suma leží v J a druhá suma je násobkem m, proto též leží v J. □

Lemma 5.2. *Nechť P je prvoideál v D_m, který neobsahuje m a $g(P) = g_1(P)$ je Gaussova suma definovaná v odstavci 4.3. Dále nechť b je celé číslo nesoudělné s pm. Pak $g(P)^{b-\sigma_b} \in K_m$.*

Důkaz. Podobně jako v důkazu tvrzení 4.3.1 (c) vezměme libovolný automorfismus $\sigma_c \in \mathrm{Gal}(K_{mp}/K_m)$. Víme, že $g(P)^{\sigma_c} = \chi_P(\overline{c})g(P)$. Protože χ_P je m-tá odmocnina z jedné, je $\chi_P^b = \chi_P^{\sigma_b}$, odkud plyne $(g(P)^{b-\sigma_b})^{\sigma_c} = g(P)^{b-\sigma_b}$. □

Věta 5.1.1. *Stickelbergerův ideál anihiluje grupu tříd ideálů D_m. Jinak řečeno, je-li $\beta \in J$ a A libovolný ideál v D_m, je ideál $A^{\beta\theta}$ hlavní.*

Důkaz. Podle důsledku Čebotarevovy věty o hustotě existuje v každé třídě ideálů prvoideál, který neobsahuje m. Stačí tedy dokázat tvrzení pro prvoideály P neobsahující m. Nechť b je nesoudělné s m. Můžeme předpokládat, že $(b, pm) = 1$, neboť kdyby bylo $p|b$, vezmeme $b' = b + m$ (ze Stickelbergerovy relace plyne, že je ideál $P^{m\theta}$ hlavní). Označme $\beta = b - \sigma_b$. Ze Stickelbergerovy relace též plyne, že

$$P^{m\beta\theta} = (\Phi_1(P)^\beta) = (g(P)^{m\beta}).$$

Podle lemmatu 5.2 leží $g(P)^\beta \in K_m$, proto můžeme díky jednoznačné faktorizaci psát $P^{\beta\theta} = (g(P)^\beta)$, což je hlavní ideál. Jsou-li $\alpha, \beta \in I$, snadno se vidí, že

$$P^{(\alpha+\beta)\theta} = (g(P)^{\alpha+\beta}),$$

čímž je důkaz hotov, neboť libovolný prvek z J je součtem konečně mnoha prvků tvaru $\pm(b - \sigma_b)$. □

Na závěr poznamenejme, že lze snadno rozšířit definici Stickelbergerova ideálu i na obecná abelovská tělesa k. Označme m konduktor tělesa k. Pak lze restrikci automorfismů z $\mathrm{Gal}(K_m/\mathbb{Q})$ na $\mathrm{Gal}(k/\mathbb{Q})$ rozšířit na homomorfismus příslušných grupových okruhů (viz. též následující odstavec) a definovat Stickelbergerův prvek θ' jako restrikci θ. Stickelbergerův ideál pak zavádíme přirozeně vztahem $S = \theta'\mathbb{Z}[G] \cap \mathbb{Z}[G]$, kde $G = \mathrm{Gal}(k/\mathbb{Q})$. Důkaz anihilace grupy tříd ideálů lze snadno odvodit z vlastností restrikce.

5.2 Rozšířený Stickelbergerův ideál

V tomto odstavci zadefinujeme rozšířený Stickelbergerův ideál, jak jej definoval Sinnott v [8]. Ukážeme, jak lze definovat Stickelbergerovy prvky v libovolném abelovském rozšíření a samozřejmě opět dokážeme, že i tento obecně větší Stickelbergerův ideál anihiluje grupu tříd ideálů.

Nechť L je abelovské těleso a M je jeho podtěleso. Označme $R_L = \mathbb{Z}[\mathrm{Gal}(L/\mathbb{Q})]$, $R_M = \mathbb{Z}[\mathrm{Gal}(M/\mathbb{Q})]$. Restrikce automorfismů L do M indukuje zobrazení

$$\mathrm{res}_{L/M} : R_L \to R_M.$$

Snadno se vidí, že je toto zobrazení homomorfismus okruhů. Dále budeme potřebovat zobrazení *korestrikce*

$$\mathrm{cor}_{L/M} : R_M \to R_L$$

definované pro libovolné $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ vztahem

$$\mathrm{cor}_{L/M}(\sigma) = \sum_{\tau|_M = \sigma} \tau,$$

kde sčítáme přes všechny automorfismy $\tau \in \mathrm{Gal}(L/\mathbb{Q})$, jejichž restrikce na M je rovna σ. Jinak řečeno, je-li $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ a $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ takové, že $\sigma = \mathrm{res}_{L/M}\,\tau$, platí

$$\mathrm{cor}_{L/M}(\sigma) = \tau \cdot \sum_{\rho \in \mathrm{Gal}(L/M)} \rho.$$

Poznamenejme, že korestrikce je pouze homomorfismem aditivních grup.

Pro libovolné automorfismy $\alpha \in \mathrm{Gal}(M/\mathbb{Q})$, $\beta \in \mathrm{Gal}(L/\mathbb{Q})$ platí následující vztahy

$$\mathrm{cor}_{L/M}(\alpha \cdot \mathrm{res}_{L/M}\,\beta) = \mathrm{cor}_{L/M}(\alpha) \cdot \beta.$$

Označme $\alpha' \in \mathrm{Gal}(L/\mathbb{Q})$ libovolný automorfismus, jehož restrikce na M je α. Pak je levá strana identity rovna $\alpha'\beta \sum_\rho \rho$ a pravá strana rovna $\alpha' \sum_\rho \rho \cdot \beta$, kde obě sumy jdou přes všechny automorfismy $\rho \in \mathrm{Gal}(L/M)$.

Dále platí identity

$$\begin{aligned}\mathrm{res}_{L/M}(\mathrm{cor}_{L/M}(\alpha)) &= |H|\alpha\\ \mathrm{cor}_{L/M}(\mathrm{res}_{L/M}(\beta)) &= s(H)\beta\end{aligned}$$

kde $H = \mathrm{Gal}(L/M)$, $s(H) = \sum_{\sigma\in H} \sigma$. Oba vztahy plynou přímo z definice.

V následujících úvahách se budeme pohybovat v několika tělesech. Pro přehlednost zavedeme následující označení. V centru pozornosti bude abelovské těleso k s konduktorem m. Kruhová tělesa budeme značit stejně jako v předchozím textu K_n, navíc označíme $k_n = K_n \cap k$. Příslušné Galoisovy grupy označíme $G = \mathrm{Gal}(k/\mathbb{Q})$ a $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$. Pro automorfismy budeme používat tzv. Artinův symbol (t, K). Pro libovolné $t \in \mathbb{Z}$, $n \in \mathbb{N}$, $(t, n) = 1$ automorfismus (t, K_n) zobrazuje ζ_n na ζ_n^t a pro libovolné $t \in \mathbb{Z}$, $(t, m) = 1$ automorfismem (t, k) rozumíme restrikci automorfismu (t, K_m) na těleso k.

Všechna rozšíření, se kterými budeme pracovat jsou abelovská, neboť jsou vždy podtělesy kruhových rozšíření $\mathbb{Q}$, která jsou abelovská.

Definice. Připomeňme, že pro libovolná $n \in \mathbb{N}$ a $a \in \mathbb{Z}$ definujeme *Stickelbergerův prvek* $\theta_n(a) \in \mathbb{Q}[G_n]$ vztahem

$$\theta_n(a) = \sum_{(t,n)=1} \left\langle \frac{at}{n} \right\rangle (t, K_n)^{-1}$$

Pomocí restrikce a korestrikce přeneseme tento prvek do tělesa k. Označme

$$\theta'_n(a) = \mathrm{cor}_{k/k_n}\,\mathrm{res}_{K_n/k_n}(\theta_n(a)).$$

Zřejmě je $\theta'_n(a)$ prvkem $\mathbb{Q}[G]$. Označme S' abelovskou grupu v $\mathbb{Q}[G]$ generovanou prvky $\theta'_n(a)$ pro všechna $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Grupa S' je dokonce modul nad $\mathbb{Z}[G]$, což plyne ze vztahu

$$(t, K_n)\theta_n(a) = \theta_n(at)$$

pro $(t, n) = 1$, což implikuje

$$(t, k_n)\,\mathrm{res}_{K_n/k_n}\,\theta_n(a) = \mathrm{res}_{K_n/k_n}\,\theta_n(at)$$

pro $(t, mn) = 1$, odkud

$$(t, k)\theta'_n(a) = \mathrm{cor}_{k/k_n}((t, k_n)\,\mathrm{res}_{K_n/k_n}\,\theta_n(a)) = \theta'_n(at)$$

pro $(t, mn) = 1$.

Stickelbergerův ideál S příslušný tělesu k definujeme jako průnik $S = S' \cap \mathbb{Z}[G]$.

Věta 5.2.1. *Stickelbergerův ideál S anihiluje grupu tříd ideálů. Jinými slovy, je-li θ libovolný prvek S a $\mathfrak{a}$ libovolný ideál v k, je $\mathfrak{a}^\theta$ hlavní ideál.*

Důkaz této věty obsáhne zbytek odstavce. Nejprve opět odvodíme některé vlastnosti význačných Gaussových sum.

Nechť $n \in \mathbb{N}$, $\mathfrak{P}$ je prvoideál z K_n nedělící n. V souladu s odstavcem 4.3 definujeme na tělese $F = D_n/\mathfrak{P}$ multiplikativní charakter $\chi_\mathfrak{P}$; je tedy splněna kongruence

$$\chi_\mathfrak{P}(\overline{t}) \equiv t^{(Q-1)/n} \pmod{\mathfrak{P}}, \quad t \in D_n^\times, t \notin \mathfrak{P} \tag{1}$$

kde $Q = \mathbf{N}\mathfrak{P} = |F|$ je absolutní norma prvoideálu $\mathfrak{P}$.

Stejným způsobem pak definujeme na F aditivní charakter $\psi(t) = \zeta_p^{\mathrm{tr}(\overline{t})}$ a Gaussovu sumu

$$g_n(a, \mathfrak{P}) = g_a(\mathfrak{P}) = g(\chi_\mathfrak{P}^{-a}, \psi_\mathfrak{P}). \tag{2}$$

Je-li σ automorfismus z $\mathrm{Gal}(K_{np}/K_n)$, můžeme psát $\sigma = (t, K_{np})$, kde $t \in \mathbb{Z}$, $(t, p) = 1$ a $t \equiv 1 \pmod{n}$. V důkazu tvrzení 4.3.1 (c) jsme odvodili mimo jiné, že

$$g_n(a, \mathfrak{P})^\sigma = \chi_\mathfrak{P}(\overline{t})^a g_n(a, \mathfrak{P}). \tag{3}$$

Dále víme, že $g_n(a, \mathfrak{P})^n$ leží v K_n a $(g_n(a, \mathfrak{P})^n)$ se v K_n rozkládá

$$(g_n(a, \mathfrak{P})^n) = \mathfrak{P}^{n\theta_n(a)}. \tag{4}$$

Zkoumejme nyní, jak se na $g_n(a, \mathfrak{P})$ chovají automorfismy, které fixují K_p. Nechť je σ libovolný automorfismus z $\mathrm{Gal}(K_{np}/K_p)$. Protože $K_n \cap K_p = \mathbb{Q}$ a $K_nK_p = K_{np}$, je $\mathrm{Gal}(K_{np}/K_p) \cong \mathrm{Gal}(K_n/\mathbb{Q})$ a tedy existuje t nesoudělné s n takové, že $\sigma|_{K_n} = (t, K_n)$. Zřejmě je t určeno jednoznačně modulo n.

S tímto označením můžeme psát

$$g_n(a, \mathfrak{P})^\sigma = g_n(a, \mathfrak{P}^\sigma) = g_n(at, \mathfrak{P}). \tag{5}$$

Platí totiž $g_n(a, \mathfrak{P})^\sigma = \sum_{x \in F} (\chi_\mathfrak{P}(x)^{-a})^\sigma \psi_\mathfrak{P}(x)^\sigma = \sum_{x \in F} \chi_\mathfrak{P}(x)^{-at} \psi_\mathfrak{P}(x) = g_n(at, \mathfrak{P})$. Dále označme $F' = D_n/\mathfrak{P}^\sigma$ a tr' zobrazení stopy v tělese F'. Pak je σ izomorfismus těles $F \to F'$. Nechť $\alpha \in D_m$ je takové, že $\overline{\alpha} = x \in F$. Pak platí

$$\chi_\mathfrak{P}(x) \equiv \alpha^{\frac{Q-1}{n}} \pmod{\mathfrak{P}}. \tag{$*$}$$

Aplikací σ na $(*)$ dostaneme

$$(\chi_\mathfrak{P}(x))^\sigma \equiv (\alpha^\sigma)^{\frac{Q-1}{n}} \pmod{\mathfrak{P}^\sigma}.$$

Substitucí $\mathfrak{P} = \mathfrak{P}^\sigma$, $x = x^\sigma$ do $(*)$ získáme

$$\chi_{\mathfrak{P}^\sigma}(x^\sigma) \equiv (\alpha^\sigma)^{\frac{Q-1}{n}} \pmod{\mathfrak{P}^\sigma}.$$

Odsud $\chi_{\mathfrak{P}^\sigma}(x^\sigma) = (\chi_{\mathfrak{P}}(x))^\sigma$, neboť jsou obě strany n-té odmocniny z jedné, a proto kongruence přechází v rovnost.

Též můžeme odvodit

$$\psi_{\mathfrak{P}^\sigma}(x^\sigma) = \zeta_p^{\mathrm{tr}'\, x^\sigma} = \zeta_p^{(\mathrm{tr}\, x)^\sigma} = \zeta_p^{\mathrm{tr}\, x} = \psi_{\mathfrak{P}}(x),$$

neboť stopa leží v $\mathbb{Z}/p\mathbb{Z}$.

Celkem tedy

$$\begin{aligned} g_n(a, \mathfrak{P}^\sigma) &= \sum_{y \in F'} \chi_{\mathfrak{P}^\sigma}(y)^{-a} \psi_{\mathfrak{P}^\sigma}(y) = \sum_{x \in F} \chi_{\mathfrak{P}^\sigma}(x^\sigma)^{-a} \psi_{\mathfrak{P}^\sigma}(x^\sigma) = \sum_{x \in F} (\chi_{\mathfrak{P}}(x)^{-a})^\sigma \psi_{\mathfrak{P}}(x) \\ &= g_n(at, \mathfrak{P}). \end{aligned}$$

Pokud zvolíme a a n pevně, můžeme se na $g_n(a, \mathfrak{P})$ dívat jako na funkci prvoideálů K_n, které nedělí n. Můžeme ji tedy multiplikativně rozšířit na obecné ideály nesoudělné s n.

Nechť $\mathfrak{p}$ je prvoideál našeho abelovského tělesa k, který nedělí n. Pak $N_{k/k_n}\mathfrak{p}$ je ideál tělesa $k_n = k \cap K_n$, tedy i ideál tělesa K_n. Definujme

$$g_n'(a, \mathfrak{p}) = g_n(a, N_{k/k_n}\mathfrak{p}). \tag{6}$$

Nyní uvedeme několik vlastností $g_n'(a, \mathfrak{p})$, které vesměs plynou z předchozích vlastností $g_n(a, \mathfrak{p})$.

Začneme s tím, že $g_n'(a, \mathfrak{p})$ leží v $k_n K_p$, kde p je prvočíslo obsažené v $\mathfrak{p}$. Skutečně, $g_n'(a, \mathfrak{p})$ zřejmě leží v K_{np}, neboť všechny prvoideály K_n dělící $N_{k/k_n}\mathfrak{p}$ obsahují p. Libovolný automorfismus $\sigma \in \mathrm{Gal}(K_{np}/k_n K_p)$ však fixuje $N_{k/k_n}\mathfrak{p}$ a tedy i $g_n'(a, \mathfrak{p})$.

Dále ukážeme, že $g_n'(a, \mathfrak{p})^n$ leží v k_n a jako prvek k má rozklad

$$(g_n'(a, \mathfrak{p})^n) = \mathfrak{p}^{n\theta_n'(a)}. \tag{7}$$

Skutečně přímo z definice plyne, že $g_n'(a, \mathfrak{p})^n$ leží v K_n, proto leží i v $k_n K_p \cap K_n = k_n$. Pro stručnost označme $\gamma = g_n'(a, \mathfrak{p})^n$, $\gamma \in k_n$. Jako prvek K_n se γ rozkládá

$$(\gamma) = (N_{k/k_n}\mathfrak{p})^{n\theta_n(a)}.$$

V k_n má tedy rozklad

$$(\gamma) = (N_{k/k_n}\mathfrak{p})^{\mathrm{res}_{K_n/k_n}\, n\theta_n(a)}.$$

Konečně v k se γ rozkládá

$$(\gamma) = (\mathfrak{p})^{\mathrm{cor}_{k/k_n}\, \mathrm{res}_{K_n/k_n}\, n\theta_n(a)} = \mathfrak{p}^{\theta_n'(a)},$$

což jsme chtěli.

Lemma 5.3. *Nechť jsou $n \geq 1$, a celá čísla a nechť p je prvočíslo, které nedělí n. Dále nechť $\mathfrak{p}$ je prvoideál v k obsahující p. Pak číslo $g_n'(a, \mathfrak{p})$ definované vztahem (6) leží v $k_n K_p$ a jeho n-tá mocnina leží v k_n. Faktorizace $g_n'(a, \mathfrak{p})$ v k je dána vztahem (7).*

Nechť $\sigma \in \mathrm{Gal}(kK_p/k)$. Pak

$$g_n'(a,\mathfrak{p})^\sigma = \zeta g_n'(a,\mathfrak{p}),$$

kde ζ je odmocnina z jedné ležící v k a je určena následujícími podmínkami. Nechť t je celé číslo, pro které platí

$$\zeta_p^\sigma = \zeta_p^t$$

(t je určeno jednoznačně modulo p). Dále nechť v_n je celé číslo takové, že

$$N_{K_n/k_n}(\zeta_n) = \zeta_n^{v_n}$$

(v_n je jednoznačně určeno modulo n). Pak ζ je taková odmocnina z jedné v k, jejíž řád není dělitelný p a která splňuje kongruenci

$$\zeta \equiv t^{a(q-1)v_n/n} \pmod{\mathfrak{p}}, \tag{8}$$

kde $q = \mathbf{N}\mathfrak{p}$ je absolutní norma prvoideálu $\mathfrak{p}$.

Důkaz. První část lemmatu byla diskutována v předchozích úvahách. Zbývají ověřit vlastnosti ζ.

Nejprve ukážeme jednoznačnost volby ζ. Platí $\zeta^n \equiv 1 \pmod{\mathfrak{p}}$, odkud $\zeta = \zeta_n^c$, neboť ζ nemá řád dělitelný p. Jsou-li tedy ζ, ζ' dvě n-té odmocniny z jedné z k_n takové, že $\zeta \equiv \zeta' \pmod{\mathfrak{p}}$, musí být též $\zeta \equiv \zeta' \pmod{\mathfrak{p}_n}$, kde $\mathfrak{p}_n$ je ten jediný prvoideál z k_n, který je dělitelný $\mathfrak{p}$. Odsud plyne, že $\zeta \equiv \zeta' \pmod{\mathfrak{P}}$ pro nějaký prvoideál $\mathfrak{P}$ z K_n a tedy podle tvrzení 3.5.3 máme $\zeta = \zeta'$.

Nechť f je jmenovatel zlomku v_n/n v základním tvaru. Z definice v_n vidíme, že f-té odmocniny z jedné leží v k_n, tedy i v k. Pravá strana (8) má jistě v tělese zbytků modulo $\mathfrak{p}$ řád dělící f. Musí tedy existovat f-tá odmocnina z jedné $\zeta \in k$ splňující (8).

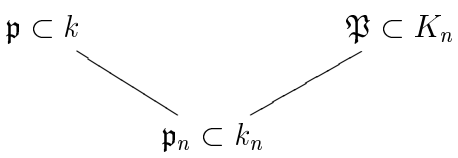
Znění lemmatu nezávisí na konkrétní volbě čísla t splňujícího $\zeta_p^\sigma = \zeta_p^t$. Zvolíme si jej tedy následujícím způsobem. Protože $g_n'(a,\mathfrak{p})$ leží v k_nK_p, $g_n'(a,\mathfrak{p})^\sigma$ závisí pouze na $\sigma|_{k_nK_p}$, což je automorfismus z $\mathrm{Gal}(k_nK_p/k_n)$. Díky tomu, že $p \nmid n$, je $\mathrm{Gal}(K_{np}/K_n) \cong \mathrm{Gal}(k_nK_p/k_n)$. Zvolme tedy celé číslo t nesoudělné s np, splňující $t \equiv 1 \pmod{n}$ a

$$\sigma|_{k_nK_p} = (t, K_{np})|_{k_nK_p}.$$

Pak

$$\zeta_p^\sigma = \zeta_p^t, \qquad g_n'(a,\mathfrak{p})^\sigma = g_n'(a,\mathfrak{p})^{(t,K_{np})}.$$

Rozložme nyní zpět $g_n'(a,\mathfrak{p})$ na původní Gaussovy sumy, abychom mohli použít vztah (3). Do konce odstavce nechť je $\mathfrak{p}_n$ prvoideál v k_n obsahující $\mathfrak{p}$ a $\mathfrak{P}$ prvoideál v K_n dělící $\mathfrak{p}_n$.



Ostatní prvoideály z K_n dělící $\mathfrak{p}_n$ jsou tvaru $\mathfrak{P}^\tau$ pro nějaké $\tau \in \mathrm{Gal}(K_n/k_n)$ (důkaz tvrzení 3.4.4 projde i pro rozšíření K_n/k_n namísto $K/\mathbb{Q}$). Nechť X je množina celých čísel nesoudělných s n takových, že se dá každý prvoideál z K_n dělící $\mathfrak{p}$ psát jednoznačně ve tvaru $\mathfrak{P}^{(x,K_n)}$ pro nějaké $x \in X$.

Označíme-li u celé číslo, pro něž platí $N_{k/k_n}\mathfrak{p} = \mathfrak{p}_n^u$, máme za použití (5) a (6) postupně

$$g'_n(a,\mathfrak{p}) = g_n(a,\mathfrak{p}_n^u) = \prod_{x\in X} g_n(a,\mathfrak{P}^{(x,K_n)})^u = \prod_{x\in X} g_n(ax,\mathfrak{P})^u.$$

Nyní na obě strany aplikujme (t, K_{np}). S pomocí vztahu (3) dostáváme

$$g'_n(a,\mathfrak{p})^{(t,K_{np})} = \zeta g'_n(a,\mathfrak{p}),$$

kde

$$\zeta = \prod_{x\in X} \chi_{\mathfrak{P}}(\overline{t})^{axu}$$

Podle (1) lze ζ charakterizovat jako n-tou odmocninu z jedné splňující kongruenci

$$\zeta \equiv t^b \pmod{\mathfrak{P}}, \tag{9}$$

kde

$$b = au\frac{Q-1}{n}\sum_{x\in X} x, \quad Q = \mathbf{N}\mathfrak{P}.$$

Protože je t celé číslo, stačí zkoumat $b \bmod (p-1)$. Označme q_n absolutní normu $\mathfrak{p}_n$. Pak je $Q = q_n^v$ pro nějaké celé číslo $v \geq 1$ a

$$Q - 1 = (q_n - 1)(1 + q_n + \cdots + q_n^{v-1})$$

a tedy

$$b = au\frac{q_n-1}{n}\sum_{x\in X}\sum_{i=0}^{v-1} xq_n^i.$$

Automorfismy (xq_n^i, K_n) pro $x \in X$ a $0 \leq i < v$ jsou právě všechny po dvou různé prvky grupy $\mathrm{Gal}(K_n/k_n)$. Skutečně, (q_n, K_n) je řádu v, neboť (q_n, K_n) je na $F = D_n/\mathfrak{P}$ právě Frobeniovým automorfismem vzhledem k rozšíření těles $F/\mathfrak{F}$, kde $\mathfrak{F} = \mathfrak{D}_n/\mathfrak{p}_n$ a $\mathfrak{D}_n$ je okruh celých algebraických čísel tělesa k_n. Automorfismus (q_n, K_n) tedy generuje dekompoziční grupu $\mathfrak{p}_n$ v $\mathrm{Gal}(K_n/k_n)$ a automorfismy (x, K_n) jsou právě reprezentanti různých tříd $\mathrm{Gal}(K_n/k_n)$ faktorizované podle této dekompoziční grupy. Odsud

$$\sum_{x\in X}\sum_{i=0}^{v-1} xq_n^i \equiv v_n \pmod{n},$$

a tedy

$$b \equiv au\frac{q_n-1}{n}v_n \pmod{q_n-1}.$$

Označme f jmenovatel zlomku v_n/n v základním tvaru. Víme, že f-té odmocniny z jedné jsou prvky k_n a leží v různých zbytkových třídách modulo $\mathfrak{p}$, neboť $p \nmid n$ implikuje $p \nmid f$. Zbytková třída příslušná ζ_f tedy generuje f-prvkovou podgrupu multiplikativní grupy tělesa $\mathfrak{F} = \mathfrak{D}_n/\mathfrak{p}_n$, odkud $f|(q_n - 1)$. Výraz $(q_n - 1)v_n/n$ je tedy celé číslo.

Nyní z faktu $q = q_n^u$ dostáváme

$$\frac{q-1}{q_n-1} = 1 + q_n + \cdots q_n^{u-1} \equiv u \pmod{q_n - 1},$$

odkud

$$b \equiv a\frac{q-1}{n}v_n \pmod{q_n - 1}. \tag{10}$$

Protože platí $t^{q_n-1} \equiv 1 \pmod{p}$, ze vztahů (9) a (10) plyne, že je ζ jediná n-tá odmocnina z jedné v K_n splňující kongruenci

$$\zeta \equiv t^{a\frac{q-1}{n}v_n} \pmod{\mathfrak{P}}.$$

Odsud ihned vidíme, že $\zeta^f = 1$ a tedy $\zeta \in k_n$. Protože leží obě strany této kongruence v k_n, musí být kongruentní i modulo $\mathfrak{p}_n$, potažmo modulo $\mathfrak{p}$. □

Lemma 5.4. *Nechť*

$$\theta = \sum_i b_i \theta'_{n_i}(a_i) = \sum_{\sigma \in G} a_\sigma \sigma^{-1},$$

kde $a_i, b_i, n_i \geq 1$ jsou celá čísla a $a_\sigma \in \mathbb{Q}$. Pak $\theta \in S$ právě tehdy, když je $a_{\mathrm{id}} \in \mathbb{Z}$.

Důkaz. Zřejmě platí

$$\theta_n(at) - t\theta_n(a) \in \mathbb{Z}[G_n]$$

pro $(t, n) = 1$. Proto i

$$\theta'_n(at) - t\theta'_n(a) \in \mathbb{Z}[G]$$

pro $(t, mn) = 1$.

Definujme nyní zobrazení $\phi : S' \to K_n$ předpisem

$$\phi(\theta) = \phi\big(\sum_{\sigma \in G} a_\sigma \sigma^{-1}\big) = e^{2\pi i a_1}.$$

Označme $N = m\prod_i n_i$. Pro $(t, N) = 1$ tak platí $(t, k)\theta - t\theta \in \mathbb{Z}[G]$ odkud

$$\phi((t,k)\theta) = \phi(t\theta) = \phi(\theta)^t = \phi(\theta)^{(t,k)}.$$

To implikuje

$$\phi(\sigma\theta) = \phi(\theta)^\sigma$$

pro všechna $\sigma \in G$. Je-li totiž $(t, m) = 1$, podle Čínské zbytkové věty existuje t' takové, že $t' \equiv t \pmod{m}$ a $(t, N) = 1$. Je-li tedy $\phi(\theta) = 1$, neboli $a_{\mathrm{id}} \in \mathbb{Z}$, musí být $a_\sigma \in \mathbb{Z}$ pro všechna $\sigma \in G$. □

Věta 5.2.1 je přímým důsledkem následujícího tvrzení.

Tvrzení 5.2.2. *Nechť je θ prvek S' a pišme*

$$\theta = \sum_i b_i \theta'_{n_i}(a_i), \tag{11}$$

kde b_i, a_i a $n_i \geq 1$ jsou celá čísla pro všechna i z nějaké konečné indexové množiny. Označme N součin všech n_i. Výrazu (11) můžeme přiřadit funkci $g(\mathfrak{p})$ definovanou pro všechny prvoideály $\mathfrak{p}$ ležící v k, které neobsahují N, vztahem

$$g(\mathfrak{p}) = \prod_i g'_{n_i}(a_i, \mathfrak{p})^{b_i}.$$

Pak θ je prvkem Stickelbergerova ideálu S právě tehdy, když $g(\mathfrak{p})$ leží v $k^\times$ pro všechny prvoideály $\mathfrak{p}$ z k neobsahující N. V tom případě navíc platí

$$\mathfrak{p}^\theta = (g(\mathfrak{p})).$$

Důkaz. Na úvod jen poznamenejme, že hodnoty funkce $g(\mathfrak{p})$ závisí na konkrétním volbě vyjádření θ v (11).

Označme obvyklým způsobem p ono jediné prvočíslo ležící v $\mathfrak{p}$. Každé $g'_{n_i}(a_i, \mathfrak{p})$ leží v $k_{n_i}K_p$, proto $g(\mathfrak{p})$ leží v kK_p. Nechť je σ libovolný automorfismus z $\mathrm{Gal}(kK_p/k)$ a nechť t je celé číslo splňující

$$\zeta_p^\sigma = \zeta_p^t.$$

Z lemmatu 5.3 plyne, že

$$g(\mathfrak{p})^\sigma = \zeta g(\mathfrak{p}),$$

kde ζ je jednoznačně určená odmocnina z jedné v k, jejíž řád není dělitelný p, splňující kongruenci

$$\zeta \equiv t^b \pmod{\mathfrak{p}},$$

kde

$$b = \sum_i a_i \frac{q-1}{n_i} v_{n_i} b_i, \qquad q = \mathbf{N}\mathfrak{p}.$$

Je-li tedy

$$\sum_i a_i \frac{v_{n_i}}{n_i} b_i \in \mathbb{Z}, \tag{12}$$

platí $b \equiv 0 \pmod{q-1}$ a $t^b \equiv 1 \pmod{p}$ pro libovolné t nesoudělné s p. Platí-li tedy (12), leží $g(\mathfrak{p})$ v k.

Naopak nechť je p prvočíslo, které se v k zcela rozkládá. Pak je $k \cap K_p = \mathbb{Q}$ a tedy $\mathrm{Gal}(kK_p/k) \cong \mathrm{Gal}(K_p/\mathbb{Q})$. Proto může t nabývat libovolné hodnoty nesoudělné s p. Protože $g(\mathfrak{p})$ leží v k, musí být $b \equiv 0 \pmod{p-1}$. V našem případě je ale $q = p$, odkud přímo plyne 12. Celkem jsme tedy dokázali, že $g(\mathfrak{p})$ leží v k pro všechny prvoideály $\mathfrak{p}$ nedělící N právě tehdy, když platí (12).

Předpokládejme nyní, že $\theta \in S$. Píšeme-li

$$\theta = \sum_{\sigma \in G} t_\sigma \sigma^{-1}, \quad t_q \in \mathbb{Q},$$

z lemmatu 5.4 víme, že $\theta \in S \Leftrightarrow t_{\mathrm{id}} \in \mathbb{Z}$. Z definic $\theta_n(a)$ a $\theta'_n(a)$ snadno vyjádříme

$$t_{\mathrm{id}} = \sum_i b_i \sum_{\substack{t \bmod n_i \\ (t,k_{n_i})=\mathrm{id}}} \left\langle \frac{a_i t}{n_i} \right\rangle,$$

odkud

$$t_{\mathrm{id}} \equiv \sum_i b_i \frac{a_i}{n_i} \sum_{\substack{t \bmod n_i \\ (t,k_{n_i})=\mathrm{id}}} t \equiv \sum_t b_i \frac{a_i}{n_i} v_{n_i} \pmod{\mathbb{Z}}.$$

Celkem jsme dokázali, že θ leží v S právě tehdy, když platí (12).

Zbývá dokázat druhou část tvrzení. Z lemmatu 5.3 plyne, že $g(\mathfrak{p})^N$ leží v k a rozkládá se následovně

$$(g(\mathfrak{p})^N) = \prod_i \mathfrak{p}^{N\theta'_{n_i}(a_i)b_i} = \mathfrak{p}^{N\theta}.$$

Pokud navíc leží θ v S, leží $g(\mathfrak{p})$ v k a tedy

$$(g(\mathfrak{p})) = \mathfrak{p}^\theta.$$

□

Důkaz věty 5.2.1. Čebotarevova věta o hustotě nám zaručuje v každé třídě ideálů existenci prvoideálu $\mathfrak{p}$, který neobsahuje předem dané číslo N. Pro takové prvoideály však byla věta dokázána v předchozím tvrzení. □

5.3 Příklad

V posledním odstavci ukážeme na konkrétním příkladu, že může být rozšířený Stickelbergerův ideál skutečně větší než původní Stickelbergerův ideál. U čtenáře předpokládáme zkušenosti s počítáním Galoisových grup zejména pro kvadratická a kruhová rozšíření.

Budeme počítat v tělese

$$k = \mathbb{Q}(\sqrt{-3}, \sqrt{-7}).$$

Těleso k je kompozitum dvou kvadratických rozšíření a je tedy abelovské.

Nejprve vypočítáme Stickelbergerův ideál v původním smyslu. Platí $\mathbb{Q}(\sqrt{-3}) = K_3$, neboť $\zeta_3 - \overline{\zeta_3} = \sqrt{-3}$. Na tělese $\mathbb{Z}/7\mathbb{Z}$ označme χ příslušný Legendrův symbol, tj. jediný multiplikativní charakter řádu 2. Aditivní charakter ψ pak definujeme vztahem $\psi(\overline{t}) = \zeta_7^t$ pro libovolné $t \in \mathbb{Z}$ a označme $g = g(\chi, \psi)$. Podle tvrzení 4.2.3 platí $\overline{g} = -g$ a podle tvrzení 4.2.2 je $g\overline{g} = 7$, odkud $g = \pm\sqrt{-7}$ a tedy $\mathbb{Q}(\sqrt{-7})$ je ono jediné kvadratické

podtěleso tělesa K_7 (jedinečnost plyne z toho, že $\mathrm{Gal}(K_7/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$ má pouze jednu dvouprvkovou podgrupu). Protože $k \not\subseteq K_3$ ani $k \not\subseteq K_7$, je konduktor tělesa k roven 21.

Galoisova grupa $\mathrm{Gal}(k/\mathbb{Q})$ je rovna $\{\mathrm{id}, \sigma, \tau, \sigma\tau\}$, kde

$$\begin{aligned} \sigma &: \sqrt{-3} \mapsto -\sqrt{-3} & \qquad \tau &: \sqrt{-3} \mapsto \sqrt{-3} \\ \sigma &: \sqrt{-7} \mapsto \sqrt{-7} & \qquad \tau &: \sqrt{-7} \mapsto -\sqrt{-7}. \end{aligned}$$

Neboli např. $\sigma = (8, K_{21})|_k$ a $\tau = (13, K_{21})|_k$; to jsou automorfismy, které jsou vždy na jednom z podtěles K_3, K_7 identické a na druhém působí jako komplexní konjugace. Pro úplnost dodejme, že např. $\sigma\tau = (20, K_{21})|_k$. Všechny automorfismy jsou řádu 2 (jsou tedy zejména shodné se svými inverzemi).

Spočítejme ještě Galoisovu grupu $\mathrm{Gal}(K_{21}/k)$. Galoisova grupa $\mathrm{Gal}(K_7/\mathbb{Q}(\sqrt{-7}))$ je rovna $\{(1, K_7), (2, K_7), (4, K_7)\}$, neboť právě automorfismy, které jsou druhými mocninami, fixují $\sqrt{-7}$. Z faktu $\mathbb{Q}(\sqrt{-3}) = K_3$ snadno odvodíme, že $\mathrm{Gal}(K_{21}/k) = \{(1, K_{21}), (16, K_{21}), (4, K_{21})$.

S těmito informacemi již můžeme spočítat

$$\begin{aligned} \theta = \theta'_{21}(1) &= \mathrm{res}_{K_{21}/k}\, \theta_{21}(1) = \mathrm{res}_{K_{21}/k} \sum_{(t,21)=1} \left\langle \frac{t}{21} \right\rangle (t, K_{21})^{-1} \\ &= \frac{1+16+4}{21}\mathrm{id} + \frac{8+2+11}{21}\sigma + \frac{13+19+10}{21}\tau + \frac{20+5+17}{21}\sigma\tau = \mathrm{id} + \sigma + 2\tau + 2\sigma\tau. \end{aligned}$$

Vidíme, že $\theta \in \mathbb{Z}[G]$, proto je Stickelbergerův ideál roven $I = \theta\mathbb{Z}[G]$. Prvky grupového okruhu $\mathbb{Z}[G]$ budeme pro stručnost značit jako vektory o čtyřech složkách, které budou určovat po řadě koeficienty u id, σ, τ a $\sigma\tau$. S tímto označením je $\theta = (1, 1, 2, 2)$, $\sigma\theta = \theta$ a $\tau\theta = (2, 2, 1, 1)$. Jako abelovská grupa je tedy ideál I generovaný prvky $(1, 1, 2, 2)$, $(2, 2, 1, 1)$. Neobsahuje tak např. normu (prvek $(1, 1, 1, 1)$).

Nyní obrátíme pozornost k Sinnottově definici Stickelbergerova ideálu. Připomeňme, že Stickelbergerův ideál $S \subseteq \mathbb{Z}[G]$ je definován jako průnik $S' \cap \mathbb{Z}[G]$, kde S' je ideál grupového okruhu $\mathbb{Q}[G]$ generovaný Stickelbergerovými prvky $\theta'_n(a)$ pro $a \in \mathbb{Z}$, $n \in \mathbb{N}$. Kučera v [4] dokázal, že je ideál S' generován jako abelovská grupa již množinou

$$\{\sigma\theta'_n(1); n|m, \sigma \in G\} \cup \{\frac{1}{2}N_k\},$$

kde m je konduktor tělesa k a $N_k = \sum_{\sigma \in G_k} \sigma$ je norma vzhledem k rozšíření $k/\mathbb{Q}$.

Ideál S' tedy stačí generovat jako modul nad $\mathbb{Z}[G]$ prvky $\theta'_{21}(1), \theta'_3(1), \theta'_7(1), \frac{1}{2}N_k$. Po-

stupně spočítáme

$$\begin{aligned}
\theta'_{21}(1) &= \theta,\\
\theta'_3(1) &= \mathrm{cor}_{k/K_3}\,\theta_3(1) = \mathrm{cor}_{k/K_3}\,\frac{1}{3}\mathrm{id} + \frac{2}{3}(2, K_3) = \frac{1}{3}(\mathrm{id} + \tau) + \frac{2}{3}(\sigma + \sigma\tau)\\
&= \frac{1}{3}(1, 2, 1, 2) = \gamma,\\
\theta'_7(1) &= \mathrm{cor}_{k/k_7}\,\mathrm{res}_{K_7/k_7}\,\theta_7(1) = \mathrm{cor}_{k/k_7}\left(\frac{1+2+4}{7}\mathrm{id} + \frac{3+5+6}{7}(6, K_7)\right)\\
&= (\mathrm{id} + \sigma) + 2(\tau + \sigma\tau) = \theta.\\
\frac{1}{2}N_k &= \frac{1}{2}(1, 1, 1, 1)
\end{aligned}$$

Jako modul nad $\mathbb{Z}[G]$ je tedy S' generován prvky θ, γ a $\frac{1}{2}N_k$. Z rovností

$$\begin{aligned}
\sigma\theta &= \theta & \tau\theta &= (2, 2, 1, 1)\\
\sigma\gamma &= \frac{1}{3}(2, 1, 2, 1) & \tau\gamma &= \gamma
\end{aligned}$$

snadno odvodíme, že jako abelovskou grupu lze $S = S' \cap \mathbb{Z}[G]$ generovat např. prvky $(1, 1, 1, 1), (1, 1, 0, 0), (1, 0, 1, 0)$. Vidíme, že rozšířený Stickelbergerův ideál obsahuje normu a je mnohem větší než původní Stickelbergerův ideál. Z tohoto příkladu však také vidíme, že Stickelbergerův ideál nemusí obsahovat všechny anihilátory grupy tříd ideálů. Okruh celých algebraických čísel tělesa $\mathbb{Q}(\sqrt{-3}, \sqrt{-7})$ je totiž okruhem hlavních ideálů, jak se lze přesvědčit např. pomocí softwarového produktu PARI/GP. Jeho grupa tříd ideálů je tedy triviální a libovolný prvek grupového okruhu $\mathbb{Z}[G]$ ji anihiluje.

Rejstřík

Literatura

[1] J. A. Beachy and W. D. Blair: Abstract Algebra, Waveland Press, Illinois, 1996.

[2] D. A. Cox: Primes of the form $x^2 + ny^2$, John Wiley & Sons, 1989.

[3] K. Ireland and M. Rosen: A Classical Introduction to Modern Number Theory, Springer Verlag, N.Y., 1990.

[4] R. Kučera: On the Stickelberger Ideal and Circular Units of a Compositum of Quadratic Fields, J. Number Theory 56 (1996), 139-166.

[5] F. Lemmermeyer: Reciprocity Laws: From Euler to Eisenstein, Springer Verlag, 2000.

[6] B. Neradílek: Galoisova teorie (Diplomová práce), Masarykova univerzita v Brně, 2000.

[7] J. Rosický: Algebra: Grupy a okruhy, Masarykova univerzita v Brně, 2000.

[8] W. Sinnott: Stickelberger Ideal and Circular Units of an Abelian Field, Inv. Math. 62 (1980), 181-234.

[9] L. C. Washington: Introduction to Cyclotomic Fields, Springer Verlag, N.Y., 1996.