

# Pokroky matematiky, fyziky a astronomie

---

D. K. Faddějev

O devátém Hilbertově problému

*Pokroky matematiky, fyziky a astronomie*, Vol. 18 (1973), No. 2, 90--96

Persistent URL: <http://dml.cz/dmlcz/138509>

## Terms of use:

© Jednota českých matematiků a fyziků, 1973

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

# Hilbertovy problémy

---

Ve své přednášce „Matematické problémy“ v Paříži r. 1900 se zabývá D. Hilbert také speciálními problémy z teorie čísel. Jeden z nich je devátý problém týkající se zákona reciprocity. O tomto problému uvádí D. Hilbert toto:

## „9. Důkaz nejobecnějšího zákona reciprocity v libovolném číselném tělese

Je třeba dokázat zákon reciprocity pro zbytky stupně  $l$  v libovolném číselném tělese, kde  $l$  je liché prvočíslo nebo mocnina čísla 2 nebo mocnina lichého prvočísla. Stanovení tohoto zákona a také základní prostředky pro jeho dokázání se myslím určí, jestliže se odpovídajícím způsobem zobecní moje teorie těles kořenů  $l$ -tého stupně z jedničky\*) a moje teorie týkající se kvadratického tělesa.\*\*)

Ve sborníku *Problemy Gil'berta*, Moskva 1969, iz. „Nauka“ je uveřejněn k tomuto problému následující článek D. K. Faddějeva.\*\*\*)

---

## O devátém Hilbertově problému

*D. K. Faddějev*

### 1°. Gaussův zákon reciprocity

Nejjednodušším projevem zákona reciprocity je následující fakt, který byl znám již P. Fermatovi. Mezi prvočísly, která dělí čísla  $z^2 + 1$  ( $z$  celé č.), se vyskytují všechna prvočísla tvaru  $4k + 1$  a žádné prvočíslo tvaru  $4k + 3$  ( $k$  celé č.). Např.  $2^2 + 1 = 5$ ;  $8^2 + 1 = 5 \cdot 13$ ;  $4^2 + 1 = 17$ ;  $12^2 + 1 = 5 \cdot 29$  atd. Jinými slovy: kongruence  $z^2 + 1 \equiv 0 \pmod{p}$  pro prvočíselný modul  $p$  je řešitelná, právě když  $p = 2$  nebo  $p \equiv 1 \pmod{4}$ . Tento fakt se zobecní takto: Jestliže celé číslo  $a$  není čtvercem celého čísla, pak prvočísel-

---

\*) *Über die Theorie der algebraischen Zahlkörper*, Jahresber. Dtsch. Math.-Ver. 4 (1897) (uveřejněno v *Gesamm. Abh. I*, No 7).

\*\*) *Math. Ann.* 51 (1899). 1–127 v *Nachr. Ges. Wiss. Göttingen*, 1898, 370–399 (nebo viz *Gesamm. Abh. I*, No 9, 10, mimoto srovnej s doktorskou disertací G. RÜCKLE, Göttingen, 1901, D. V. No 13).

\*\*\*) Čtvrtý odstavec článku je zkrácen překladatelem.

ní dělitelé čísel  $z^2 - a$  mimo 2 a dělitelů čísla  $a$  leží přesně v polovině primitivních zbytkových tříd podle modulu  $4a$  (tj. aritmetických posloupností  $4ak + b$ ,  $0 < b < 4a$ ,  $b$  nesoudělné s  $4a$ ). Charakteristika zbytkových tříd obsahujících prvočíselné dělitele čísel  $z^2 - a$  tvoří základní obsah Gaussova zákona reciprocity.

Uvedeme pojmy a označení pro formulaci tohoto zákona. Celé číslo  $a$  se nazývá kvadratickým zbytkem podle prvočíselného modulu  $p \neq 2$ , jestliže  $a$  není dělitelno  $p$  a kongruence  $x^2 - a \equiv 0 \pmod{p}$  je řešitelná. Jestliže kongruence  $x^2 - a \equiv 0 \pmod{p}$  nemá řešení, nazývá se číslo  $a$  kvadratickým nezbytkem. Podle „malé Fermatovy věty“ pro libovolné celé číslo  $a$  nedělitelné  $p$  platí kongruence  $a^{p-1} \equiv 1 \pmod{p}$ , odkud  $(a^{(p-1)/2} - 1) \cdot (a^{(p-1)/2} + 1) \equiv 0 \pmod{p}$  a tedy  $a^{(p-1)/2} \equiv 1 \pmod{p}$  nebo  $a^{(p-1)/2} \equiv -1 \pmod{p}$ .

Ukazuje se, a to tvoří obsah tak zvaného Eulerova kritéria, že první kongruence platí, jestliže  $a$  je kvadratický zbytek; druhá kongruence platí, jestliže  $a$  je kvadratický nezbytek. Vlastnosti kvadratických zbytků a nezbytků se dají vhodně formalizovat pomocí Legendreova symbolu  $(a/p)^*$ , který je funkcí prvočísel  $p$  a celých čísel  $a$  nedělitelných  $p$  s hodnotami  $+1$  nebo  $-1$  podle toho, zda číslo  $a$  je kvadratickým zbytkem nebo nezbytkem podle modulu  $p$ . Nejjednodušší vlastnosti kvadratických zbytků a nezbytků jsou dány formulemi:

1.  $(a/p) = (a_1/p)$ , jestliže  $a \equiv a_1 \pmod{p}$ ,  
tedy  $(a/p)$  jako funkce  $a$  při pevném  $p$  má periodu  $p$ .
2.  $(a/p) \equiv a^{(p-1)/2} \pmod{p}$  (Eulerovo kritérium).
3.  $(a_1 a_2/p) = (a_1/p) (a_2/p)$ . Tato vlastnost značí, že součin dvou kvadratických zbytků nebo nezbytků je zbytek a součin zbytku s nezbytkem je nezbytek.

Vyšetřování chování symbolu  $(a/p)$  jako funkce proměnné  $p$  při pevném  $a$  představuje otázku ekvivalentní s otázkou popsání všech prvočíselných dělitelů čísla  $z^2 - a$ . Odpověď je dána Gaussovým zákonem reciprocity. Skládá se ze základní formulace a dvou doplňků:

1. Jestliže  $p$  a  $q$  jsou různá lichá prvočísla, pak  $p$  podle modulu  $q$  a  $q$  podle modulu  $p$  budou současně kvadratickými zbytky nebo nezbytky, jestliže je aspoň jedno z těchto prvočísel kongruentní s  $+1$  podle modulu 4. Jestliže obě tato prvočísla jsou kongruentní s  $-1 \pmod{4}$ , pak jedno z nich je zbytkem podle druhého a druhé nezbytkem podle prvního.

Pomocí Legendreova symbolu se to píše takto:

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2} \left(\frac{p}{q}\right).$$

2.  $(-1/p) = (-1)^{(p-1)/2}$ . Tato formule vyjadřuje, že  $-1$  je kvadratický zbytek pro  $p \equiv 1 \pmod{4}$  a nezbytek pro  $p \equiv -1 \pmod{4}$ .
3.  $(2/p) = (-1)^{(p^2-1)/8}$ . Tato formule udává, že 2 je kvadratický zbytek pro  $p \equiv \pm 1 \pmod{8}$  a nezbytek pro  $p \equiv \pm 3 \pmod{8}$ .

\*) Tento symbol zavedl A. G. LEGENDRE r. 1808. — Pozn. redakce sborníku *Problémy Gil'berta*.

Ukážeme, jak zákon reciprocity řeší úlohu o hodnotách  $(a/p)$  při pevném  $a$ . Bez újmy na obecnosti můžeme předpokládat, že  $a$  není dělitelno žádným čtvercem  $\neq 1$ . Nechť  $a = (-1)^\alpha 2^\beta q_1 \dots q_k$ , kde  $\alpha = 0,1$ ;  $\beta = 0,1$ ;  $q_1, \dots, q_k$  různá lichá prvočísla. Pak

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^\alpha \left(\frac{2}{p}\right)^\beta \left(\frac{q_1}{p}\right) \dots \left(\frac{q_k}{p}\right).$$

Hodnota prvního činitele (pro  $\alpha = 1$ ) závisí na třídě čísla  $p$  podle modulu 4, druhého (pro  $\beta = 1$ ) na třídě čísla  $p$  podle modulu 8. Následující činitel  $(q_i/p)$  v důsledku rovnice

$$\left(\frac{q_i}{p}\right) = \left(\frac{p}{q_i}\right) (-1)^{(q_i-1)/2 \cdot (p-1)/2}$$

závisí na třídě čísla  $p$  podle modulu  $4q_i$ . Jestliže tedy budeme znát zbytkovou třídu, do které náleží  $p$  podle modulu  $4 \cdot 2^\beta \cdot q_1 \dots q_k = 4|a|$ , budeme znát hodnotu každého činitele a hodnotu symbolu  $(a/p)$ . Např.

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{5}{p}\right) = (-1)^{(p-1)/2} \left(\frac{p}{5}\right),$$

odkud snadno dostáváme, že  $(-5/p) = +1$  pro  $p \equiv 1, 3, 7, 9 \pmod{20}$  a  $(-5/p) = -1$  pro  $p \equiv 11, 13, 17, 19 \pmod{20}$ .

Gauss oprávněně přikládal velký význam jím dokázanému zákonu reciprocity a podal několik jeho důkazů, založených na zcela různých ideách ([1]).

Pro mnohé cíle, zejména pro další zobecnění, ukazuje se vhodná trochu obecnější forma zákona reciprocity spjatá s Jacobiho symbolem. Jacobiho symbol  $(a/b)$  se definuje pro kladné liché číslo  $b$  a pro celé číslo  $a$  nesoudělné s  $b$ . Jestliže  $b = q_1^{\alpha_1} \dots q_k^{\alpha_k}$  je kanonický rozklad čísla  $b$ , pak definujeme

$$\left(\frac{a}{b}\right) = \left(\frac{a}{q_1}\right)^{\alpha_1} \dots \left(\frac{a}{q_k}\right)^{\alpha_k}.$$

Jacobiho symbol je multiplikativní vzhledem k čitateli i jmenovateli:

$$\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right) \left(\frac{a_2}{b}\right) \quad \text{a} \quad \left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right) \left(\frac{a}{b_2}\right).$$

Zákon reciprocity zformulovaný termíny Jacobiho symbolu se neliší formou od zákona reciprocity v termínech Legendreova symbolu a je dán třemi vzorci:

$$\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}; \quad \left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}; \quad \left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{(a-1)/2 \cdot (b-1)/2}$$

(pro lichá, kladná, nesoudělná čísla  $a, b$ ).

## 2°. Zobecnění zákona reciprocity

Pojem kvadratického zbytku se dá přirozeným způsobem zobecnit. Celé číslo  $a$  nedělitelné prvočíslem  $p$  se nazývá zbytkem stupně  $n$  podle modulu  $p$  ( $n$  je přirozené číslo  $> 1$ ), jestliže kongruence  $x^n \equiv a \pmod{p}$  má řešení. Rozumné zobecnění zákona reciprocity na zbytky stupně  $n$  se ukazuje možné při přechodu od aritmetiky celých racionálních čísel k teorii algebraických čísel. Aritmetika celých čísel nadtělesa konečného stupně tělesa racionálních čísel  $Q$  se v základě podobá aritmetice celých racionálních čísel až na dva důležité rozdíly. Za prvé: okruh celých algebraických čísel nějakého konečného rozšíření tělesa racionálních čísel má nekonečně mnoho jednotek, tj. celých čísel, jejichž inverze je též celé algebraické číslo (s výjimkou imaginárních kvadratických těles). To vynucuje v otázkách teorie dělitelnosti „slepovat“ čísla lišící se násobky jednotek do jednoho objektu – „hlavního dělitele“. Za druhé: aby byla zachována v platnosti věta o jednoznačnosti rozkladu na ireducibilní faktory, je nutno vnořit množinu všech hlavních dělitelů do větší množiny všech dělitelů („ideálních čísel“). Ukazuje se, že počet tříd dělitelů je konečný, jestliže sjednotíme do tříd dělitele, kteří se liší násobkem hlavního dělitele.\*) Třídy zbytků podle prvodělitele  $p$  vytvářejí konečné těleso, které je konečným rozšířením tělesa zbytkových tříd podle prvočíselného modulu  $p$ , kde prvodělitel  $p$  dělí  $p$ . Stupeň  $f$  tohoto rozšíření se nazývá stupněm (neboli řádem) prvodělitele  $p$ . Počet  $p^f$  tříd zbytků se nazývá formou  $p$  a značí se  $N(p)$ , tedy  $N(p) = p^f$ . Platí analogické tvrzení k Fermatově větě:  $a^{N(p)-1} \equiv 1 \pmod{p}$ , kde  $a$  je celé algebraické číslo daného nadtělesa nedělitelné  $p$ .

Při zobecnění zákona reciprocity na zbytky stupně  $n$  je nutno předpokládat, že uvedené nadtěleso obsahuje primitivní  $n$ -tou odmocninu z jedné. Za tohoto předpokladu je pro prvodělitele  $p$  ( $p$  nedělí  $n$ )  $N(p) \equiv 1 \pmod{n}$ . Analogický pojem k Legendreovu symbolu se definuje pomocí kongruence  $(a/p) = \zeta^k \equiv a^{(N(p)-1)/n} \pmod{p}$ .

Symbol analogický k symbolu Jacobiho se definuje formulí

$$\left(\frac{a}{b}\right) = \prod \left(\frac{a}{p_i}\right)^{m_i},$$

kde  $(b) = \prod p_i^{m_i}$ ;  $a, b$  jsou celá čísla,  $b$  je nesoudělné s číslem  $a \cdot n$ .

\*) Přesně řečeno jde o homomorfismus  $h$  multiplikativní pologrupy  $R'$  příslušného okruhu  $R$  celých algebraických čísel do nějaké komutativní pologrupy  $\mathfrak{D}$  s jednoznačným rozkladem na ireducibilní faktory, která má jedinou jednotku, a to jedničku. Tento homomorfismus  $h$  splňuje tyto axiomy:

$$1^\circ r_1, r_2 \in R' \Rightarrow \frac{h(r_1)}{\mathfrak{D}} / \frac{h(r_2)}{\mathfrak{D}} \equiv \frac{r_1}{R} / \frac{r_2}{R};$$

$$2^\circ \mathfrak{d} \in \mathfrak{D}, r_1, r_2 \in R', r_1 + r_2 \neq 0_R, \frac{\mathfrak{d}}{\mathfrak{D}} / \frac{h(r_1)}{\mathfrak{D}}, \frac{\mathfrak{d}}{\mathfrak{D}} / \frac{h(r_2)}{\mathfrak{D}} \Rightarrow \frac{\mathfrak{d}}{\mathfrak{D}} / \frac{h(r_1 + r_2)}{\mathfrak{D}};$$

$$3^\circ \mathfrak{d}_1, \mathfrak{d}_2 \in \mathfrak{D}, \{r \in R' : \frac{\mathfrak{d}_1}{\mathfrak{D}} / \frac{h(r)}{\mathfrak{D}}\} = \{r \in R' : \frac{\mathfrak{d}_2}{\mathfrak{D}} / \frac{h(r)}{\mathfrak{D}}\} \Rightarrow \mathfrak{d}_1 = \mathfrak{d}_2.$$

Prvky z  $\mathfrak{D}$  se nazývají dělitelé, prvek z  $\mathfrak{D}$  tvaru  $h(r)$ , kde  $r \in R'$ , se nazývá hlavní dělitel  $h$ , ireducibilní prvek z  $\mathfrak{D}$  se nazývá prvodělitel. Dá se ukázat, že pologrupa  $\mathfrak{D}$  je izomorfní s pologrupou ideálů okruhu  $R$ , přičemž hlavním dělitelům odpovídají hlavní ideály a prvodělitelům odpovídají prvoideály. Třídy dělitelů se definují stejně jako třídy ideálů. Podrobnější výklad této teorie je uveden v knize S. J. BOREVIČE a J. R. ŠAFAREVIČE: *Teorija čísel*, Moskva 1964. (Pozn. překl.)

Zákon reciprocity pro  $n = 4$  v tělese  $Q(i)$  byl dán ještě GAUSSEM ([2]) a pro  $n = 3$  v tělese  $Q(e^{2\pi i/3})$  – EISENSTEINEM ([3]). Eisensteinovi ([4]) též náleží zákon reciprocity pro prvočíselné  $n$  v tělese  $Q(e^{2\pi i/n})$  pro dvojici čísel, z nichž jedno je racionální. Obecný zákon reciprocity pro prvočíselný stupeň  $n$  v tělese  $Q(e^{2\pi i/n})$  byl dán KUMMEREM ([5]).

Kummerova formule zní:

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{l^1(\alpha)l^{n-1}(\beta) - l^2(\alpha)l^{n-2}(\beta) + \dots - l^{n-1}(\alpha)l^1(\beta)}.$$

Zde  $\alpha, \beta$  jsou celá čísla tělesa  $Q(e^{2\pi i/n})$ ,

$$\alpha \equiv \beta \equiv 1 \pmod{(\zeta - 1)}, \quad l^i(\alpha) = \left[ \frac{d^i \lg f(e^\alpha)}{dv^i} \right]_{v=0},$$

kde  $f(t)$  je polynom stupně  $n-1$  takový, že  $\alpha = f(\zeta), f(1) = 1$ .

Kummer dokázal zákon reciprocity pro případ regulárního prvočísla  $n$  (tj. počet tříd dělitelů tělesa  $Q(\zeta)$  není dělitelný číslem  $n$ ), TAKAGI ([6]) dokázal tento zákon bez předpokladu regularity prvočísla  $n$ .

### 3°. Hilbertova teorie

Pravá strana Gaussova a Kummerova zákona reciprocity závisí jen na zbytcích podle modulu 4 čísel  $a, b$  (pro Gaussův zákon) a na zbytcích podle modulu  $(\zeta - 1)^n$  čísel  $\alpha, \beta$  (pro Kummerův zákon). Vlastnosti čísel, které závisí jen na třídách kongruencí, jež tato čísla obsahují, podle modulu dostatečně velkého stupně prvočinitele  $p$ , se nazývají lokálními vzhledem k tomuto děliteli. Tímto způsobem má pravá strana Gaussova a Kummerova zákona reciprocity lokální charakter vzhledem k prvočíselným dělitelům čísla  $n$ .

Hilbert má zásluhu na vybudování teorie, která vysvětluje tuto skutečnost. Samým Hilbertem tato teorie nebyla vybudována v úplné obecnosti (pro regulární kruhové těleso ([7]) a pro  $n = 2$  ([8]) pro komplexní těleso algebraických čísel, které má lichý počet tříd (dělitelů). Při formulaci devátého problému Hilbert vyjadřuje naději, že jeho řešení se dostane rozvojem této jeho teorie.

Stručně vyložíme Hilbertovu teorii a její užití pro Gaussův zákon reciprocity. Pro každé prvočíslu  $p$  a celá čísla  $a, b$  zavedeme „symbol normovaného zbytku“  $(a, b/p)$  s hodnotami  $+1$  a  $-1$  podle toho, zda kongruence  $x^2 - ay^2 \equiv b \pmod{p^k}$  má pro libovolné  $k$  řešení nebo ne. Symbol  $(a, b/p)$  závisí na lokálním chování čísel  $a, b$  vzhledem k  $p$ . Z definice je zřejmé, že

$$\left(\frac{a, b}{p}\right) = \left(\frac{b, a}{p}\right), \quad \left(\frac{a, b_1 b_2}{p}\right) = \left(\frac{a, b_1}{p}\right) \left(\frac{a, b_2}{p}\right) \quad \text{a} \quad \left(\frac{a, -a}{p}\right) = 1.$$

Z podrobnější analýzy plyne, že pro liché prvočíslu  $p$ , které nedělí  $a, b$ , je  $(a, b/p) = 1$ .

Dále pro lichá čísla  $a, b$  je

$$\left(\frac{a, b}{2}\right) = (-1)^{(a-1)/2 \cdot (b-1)/2}; \quad \left(\frac{a, b}{2}\right) = (-1)^{(a^2-1)/8}.$$

Proto symbol  $(a, b/p)$  pro pevná  $a, b$  nabývá hodnoty  $+1$  pro všechna prvočísla  $p$  s eventuální výjimkou  $p = 2$  nebo prvočísla  $p$ , které dělí  $a$  nebo  $b$ .

Pro lichá kladná  $a, b$  je

$$\prod_{p/a} \left(\frac{a, b}{p}\right) = \left(\frac{b}{a}\right); \quad \prod_{p/b} \left(\frac{a, b}{p}\right) = \left(\frac{a}{b}\right),$$

takže zákon reciprocit v termínech Jacobiho symbolu přejde v tvar

$$(*) \quad \prod_p \left(\frac{a, b}{p}\right) = 1.$$

Tato formule zůstane v platnosti pro libovolná celá čísla  $a, b$ , z nichž je aspoň jedno kladné. Kromě toho je ekvivalentní zákonu reciprocit ještě s doplňujícími formulemi. Při jejím rozšíření na libovolná čísla  $a, b$  je nutno přidat k levé straně jeden faktor

$$\left(\frac{a, b}{p_\infty}\right) = (-1)^{(\operatorname{sgn} a - 1)/2 \cdot (\operatorname{sgn} b - 1)/2},$$

který závisí jen na znaménkách čísel  $a, b$ .

Tímto způsobem v souladu s plánem načrtnutým Hilbertem bylo třeba dát náležitou definici symbolu normovaného zbytku  $(a, b/p)$  pro libovolné  $n$  a libovolné těleso obsahující kořen  $n$ -tého stupně z 1, stanovit formulí (\*) pro zkonstruovaný symbol a udát explicitní formule pro výpočet hodnot symbolu.

Tím sám tento plán předvídal princip, v současné době často používaný, rozdělení problému na dvě části – lokální a globální. Zde první část se skládá z definice a vyšetřování symbolu  $(a, b/p)$ , druhá ze stanovení formule (\*).

Rozvinutí teorie tělesa tříd (TAKAGI [9], HASSE [10]), stanovení Artinova zákona reciprocit (ARTIN [11]) a systematické užívání metody vnoření tělesa algebraických čísel do úplně lokálních těles (zúplnění tělesa algebraických čísel vzhledem k archimedovským a nearchimedovským metrikám) (HASSE) realizovaly Hilbertův plán, avšak bez stanovení explicitních formulí pro symbol normovaných zbytků. Za nejdokonalejší v této etapě (HASSE [12]) je třeba považovat definici symbolu  $(a, b/p)$  pomocí invariantu algebry  $k(A, B)$  s multiplikační tabulkou  $A^n = a, B^n = b, BA = AB\zeta$ , kde  $\zeta$  je primitivní kořen  $n$ -tého stupně z 1. Tato definice je ekvivalentní současnější definici v termínech teorie kohomologií v grupách. Při této definici se ukázalo, že formule (\*) platí bez jakýchkoli omezení.

Tyto způsoby definice symbolu  $(a, b/p)$  však nedávají explicitní formule pro výpočet jeho hodnot, takže Hilbertův problém o explicitní formě zákona reciprocit ve tvaru typu Gaussových a Kummerových formulí zůstává otevřený.

#### 4°. Šafarevičův zákon reciprocity

Pro vytvoření explicitních formulí pro zákon reciprocity mocninových zbytků stupně  $n$  stačí se omezit na případ  $n = p^k$ , ( $p$  prvočíslo) a udat explicitní formuli  $(a, b/p)$  pro prvo-dělitele  $p$ , které dělí  $p$ . Taková formule byla sestavena I. R. ŠAFAREVIČEM v r. 1948 ([13]) a publikována v článcích [14] a [15].

Pro  $n = p^k$  pro libovolné  $k$  byly podány důkazy Šafarevičovy formule A. I. LAPINEM ([16]) přímo z definice Šafarevičova symbolu s M. KNESEREM ([17]) použitím vlastností symbolu normovaného zbytku, A. I. Lapin ([18]), ([19]) realizoval také zdůvodnění teorie tělesa tříd na základě Šafarevičova zákona reciprocity.

#### Literatura

- [1] GAUSS C. F., *Disquisitiones arithmeticae*, Werke 1, Göttingen, 1870.
- [2] GAUSS C. F., *Theorie residuorum biquadraticorum, commentatio prima et secunda*, Werke 2, Göttingen, 1863, 65 a 93.
- [3] EISENSTEIN G., *Beweis des Reziprozitätsgesetzes für die Kubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen*, J. Math. 27 (1844).
- [4] EISENSTEIN G., *Bewies der allgemeinsten Reziprozitätsgesetze zwischen reellen und komplexen Zahlen*, Ber. K. Akad. Wiss., Berlin, 1850.
- [5] KUMMER E., *Ueber allgemeine Reziprozitätsgesetze für beliebig hohe Potenzseste*, Ber. K. Akad. Wiss., Berlin, 1850.
- [6] TAKAGI T., *On the law reciprocity in the cyclotomic corpus*, Proc. of the Phys.-math. Soc. of Japan, 1922.
- [7] HILBERT D., *Die Theorie der algebraischen Zahlkörper*, Jahresber. Dtsch. Math.-Ver. 4 (1897).
- [8] HILBERT D., *Über die Theorie der relativquadratischen Zahlkörper*, Jahresber. Dtsch. Math.-Ver. 6 (1899).
- [9] TAKAGI T., *Über eine Theorie des relativ-Abelschen Zahlkörper*, J. Coll. Science, Tokyo, 41, 9 (1920).
- [10] HASSE H., *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresber. Dtsch. Math.-Ver. 35 (1926); 36 (1927); 39 (1930).
- [11] ARTIN E., *Beweis des allgemeinen Reziprozitätsgesetzes*, Abh. Math. Semin. Hamburg. Univ. 5 (1928).
- [12] HASSE H., *Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper*, Math. Ann. 107 (1935), 731—760.
- [13] ŠAFAREVIČ I. R., *Obščij zakon vzaimnosti*, UMN 3, No 3 (25) (1948), str. 165.
- [14] ŠAFAREVIČ I. R., *Obščij zakon vzaimnosti*, DAN SSSR 64 (1949), 25—28.
- [15] ŠAFAREVIČ I. R., *Obščij zakon vzaimnosti*, Matem. sb. 26 (1950), 113—146.
- [16] LAPIN A. I., *Teorija symvola Šafareviča*, IAN SSSR, ser. matem., 17 (1953), 31—50.
- [17] KNESER M., *Zum expliziten Reziprozitätsgesetz von Šafarevič*, Math. Nachr. 6, No 2 (1951), 89—96.
- [18] LAPIN A. I., *K teoriji symvola Šafareviča*, IAN SSSR, ser. matem., 18 (1954), 145—158.
- [19] LAPIN A. I., *Obščij zakon vzaimnosti i novoe obosnovanie teorii polej klassov*, IAN SSSR, ser. matem. 18 (1954), 335—378.

Přeložil L. Skula