Algebra a teorie čísel

In: Magdalena Hykšová (author): Karel Rychlík (1885–1968). (Czech). Praha: Prometheus, 2003. pp. 61–121.

Persistent URL: http://dml.cz/dmlcz/401157

2 ALGEBRA A TEORIE ČÍSEL

2.1 ZÁSADNÍ PRÁCE KARLA RYCHLÍKA

2.1.1 Historický úvod

2.1.2 ***g*-adická čísla** ..... **[R11], [R12], [R17], [R21]**

2.1.3 Teorie ohodnocení ..... **[R14], [R22]**

2.1.4 Teorie algebraických čísel, abstraktní algebra ..... **[R15], [R16], [R23], [R24], [R26], [R31], [R32], [R33], [R39], [R40]**

2.1.5 Teorie determinantů ..... **[R38], [R43]**

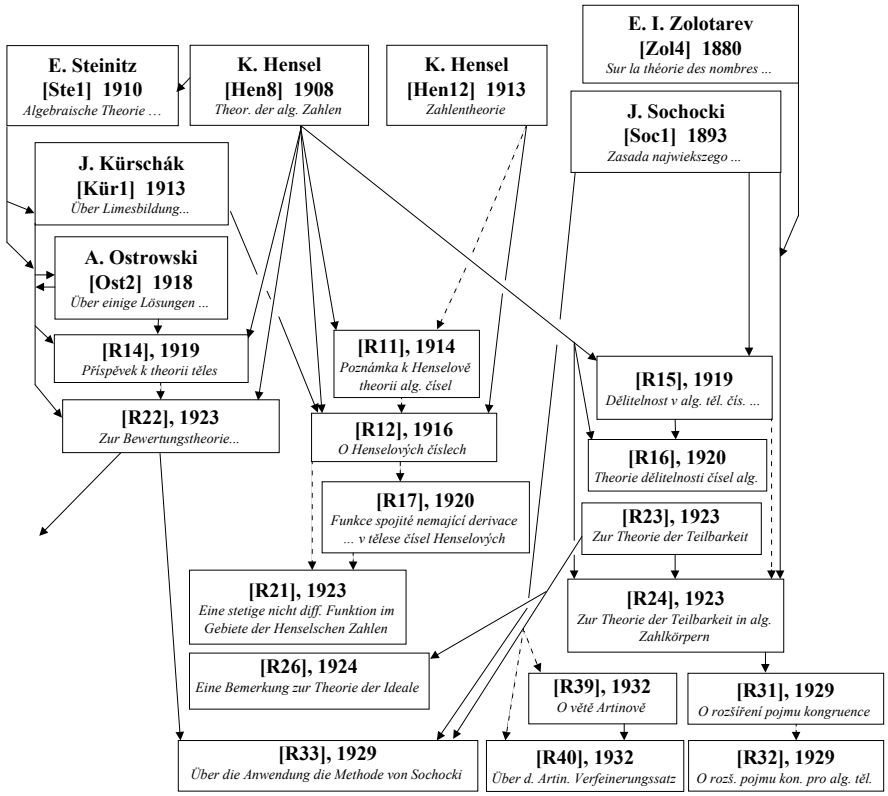
2.2 OSTATNÍ PRÁCE

2.2.1 Grupy substitucí ..... **[R2], [R3]**

2.2.2 Teorie forem ..... **[R4], [R7]**

2.3 ZÁVĚR

2.1 ZÁSADNÍ PRÁCE KARLA RYCHLÍKA



Obr. 2.1 Přehled vzájemných vazeb a nejdůležitějších citací

2.1.1 Historický úvod

Než přikročíme k diskusi Rychlíkových nejdůležitějších prací, podívejme se krátce na některé momenty vývoje algebraické teorie čísel. Jak je patrné z obr. 2.1, podstatná část Rychlíkových publikací zahrnutých do jednotlivých oddílů kapitoly 2.1 bezprostředně navazuje na práce Kurta Hensela. Dokonce lze říci, že Rychlík používal pojmy a výsledky Henselovy teorie do takové míry, že je téměř nemožné přehledně popsat a zhodnotit jeho práce bez podrobnějšího popisu příslušných prací Henselových. Pro ilustraci a pro uvedení do problematiky je na začátku této kapitoly zařazen krátký exkurs do teorie algebraických čísel v devatenáctém století. Aby bylo patrné, jak se daná disciplina postupně vyvíjela, a aby vyniklo přesné, stručné a jasné pojetí Rychlíkových prací, je v textu do určité míry použita tehdejší terminologie a zachováno či alespoň naznačeno původní pojetí definic a tvrzení.[1]

Počátky

V první polovině 19. století zobecnil Carl Friedrich Gauss (1777 – 1855) pojem celého čísla tím, že jej převedl (v dnešní terminologii) z oboru integrity [2] celých čísel $\mathbb{Z}$ do oboru integrity $\mathbb{Z}[i]$ tvořeného čísly

$$a + bi\,, \quad a, b \in \mathbb{Z}, \tag{2.1}$$

kde i je kořen polynomu $x^2 + 1$, která byla později nazvána *Gaussova celá čísla*; Gauss o nich hovořil jako o *celých komplexních číslech* (*numeros integros complexos*).

Podobnou myšlenku lze nalézt již u Leonharda Eulera (1707 – 1783), který při důkazu velké Fermatovy věty pro $n = 3$ v práci [Eul1] z roku 1770 pracoval s výrazy tvaru $m + n\sqrt{-3}$, kde $m, n \in \mathbb{Z}$, pro něž užíval i pojmů *prvočinitel, nesoudělná čísla* apod; využíval také zákona jednoznačného rozkladu v prvočinitele a jeho důsledků, ovšem bez ověření.[3]

Gauss zavedl čísla (2.1) v souvislosti se studiem bikvadratického zákona reciprocity v druhé části práce *Theoria residuorum biquadraticorum* [Gau2] z roku 1832. Ukázal, že množina čísel tvaru (2.1) je uzavřená na sčítání, odčítání a násobení a že je možné zde vybudovat aritmetiku analogickou aritmetice v $\mathbb{Z}$.

[1] Ještě Henselovy práce tvoří souvislý text, kde se prolínají definice, tvrzení a komentáře; pro přehlednost a kvůli odkazům jsou v našem popisu základní definice a tvrzení odděleny a očíslovány. Míra přesnosti však byla ponechána beze změny; čtenář nechť má na paměti, že se přenesl o století zpět, kdy byly na přesnost kladeny podstatně nižší nároky než dnes.

[2] Pro lepší názornost budeme používat pojmy *okruh*, *obor integrity*, *těleso* apod. i v souvislosti s pracemi, které vznikly v době, kdy tyto pojmy ještě nebyly zavedeny. Rovněž budeme užívat obvyklého označení číselných oborů $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, i když pochází až z pozdější doby (autoři, o nichž zde budeme hovořit, používali buď slovní vyjádření, nebo symboly, které budou uvedeny v poznámkách).

[3] V knize [Edw2], str. 39–54, je popsán korektní důkaz sestrojený na základě Eulerovy myšlenky použité ovšem v jiné souvislosti.

Jednotkami (*unitatibus*) Gauss nazval čísla $1,\ -1,\ i,\ -i$. *Asociovaná* (*socios* nebo *numeros associatos*) jsou taková čísla, která lze jedno z druhého získat vynásobením jednotkou. *Konjugovaná* (*coniunctum*) jsou čísla, která se na sebe navzájem převedou záměnou i za $-i$ (tj. čísla komplexně sdružená). *Normu* (*norma*) čísla $a + bi$ Gauss definuje jako součin $(a + bi)(a - bi)$. *Pročinitel* (*numerus primus*) je takové číslo tvaru (2.1), které nemůže být vyjádřeno jako součin dvou čísel, z nichž žádné není jednotka.[4]

Gauss zavedl a studoval další aritmetické pojmy; dokázal, že každé číslo tvaru (2.1) lze vyjádřit jednoznačně (až na asociovanost) jako součin prvočinitelů, podal důkaz malé Fermatovy věty a dalších tvrzení; v závěru pak zformuloval, ale nedokázal *bikvadratický zákon reciprocity*.[5]

Na Gaussovy myšlenky navázal Carl Gustav Jacob Jacobi (1804 až 1852). V roce 1839 bylo otištěno jeho pojednání [Jac2], kde jsou studovány vyšší zákony reciprocity, a to řádu 5, 8 a 12. Důkaz bikvadratického zákona reciprocity podal Jacobi ve svých přednáškách o teorii čísel, které konal ve školním roce 1836/37 na univerzitě v Královci. Poprvé však byl tento důkaz publikován až v práci *Lois de réciprocité* [Eis2] Ferdinanda Gottholda Max. Eisensteina (1823 – 1852) z roku 1844. Eisenstein také publikoval důkaz kubického zákona reciprocity, a to v pojednání [Eis1] z téhož roku; v souvislosti s kubickým zákonem reciprocity se Eisenstein i Jacobi zabývali aritmetikou v okruhu $\mathbb{Z}[\rho]$, kde $\rho^3 = 1,\ \rho \neq 1$.

Dalším krokem ve vývoji aritmetiky celých algebraických čísel bylo studium algebraických jednotek. Jejich teorii popsal Peter Gustav Lejeune Dirichlet (1805 – 1859) v práci *Zur Theorie der complexen Einheiten* [Dir2] z roku 1846. Poznamenejme, že Dirichlet pracoval s výrazy

$$\varphi(\alpha_i) = b_0 + b_1\alpha_i + \cdots + b_{n-1}\alpha_i^{n-1}, \qquad b_0, b_1, \ldots, b_{n-1} \in \mathbb{Z}, \tag{2.2}$$

kde α_i, $i = 1, \ldots, n$, je kořen polynomu

$$F(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n\,, \qquad a_1, a_2, \ldots, a_n \in \mathbb{Z}, \tag{2.3}$$

který je ireducibilní nad $\mathbb{Q}$; souhrn všech $\varphi(\alpha_i)$ tvaru (2.2) budeme pro pevné

[4] [Gau2], str. 103 (v přetisku v [Gau3]).

Uvědomme si, že složené celé číslo ze $\mathbb{Z}$ zůstává složené i v $\mathbb{Z}[i]$, avšak prvočísla ze $\mathbb{Z}$ mohou být v $\mathbb{Z}[i]$ složená, např. $2 = (1+i)(1-i)$, $5 = (1+2i)(1-2i)$ apod. Skutečnost, že číslo 2 je v $\mathbb{Z}[i]$ složené, poněkud zkomplikovala zobecnění pojmů sudého a lichého čísla. Gaussova celá čísla jsou rozdělena na *lichá* (*impar*), tj. ta, která nejsou dělitelná číslem $1 + i$ (tedy z čísel a, b je jedno sudé a jedno liché), *polosudá* (*semipar*), tj. ta, která jsou dělitelná číslem $1 + i$, ale ne číslem 2 (čísla a, b jsou obě lichá), a *sudá* (*par*), tj. ta, která jsou dělitelná číslem 2 (čísla a, b jsou obě sudá). Lze ukázat, že ze čtyř navzájem asociovaných lichých čísel je právě jedno *primární* (*primarius*), tj. číslo tvaru (2.1), kde $a + bi \equiv 1 \pmod{2 + 2i}$.

[5] Uveďme zde jeho znění v pozdějším, přehlednějším tvaru (viz např. [Die1], str. 183).
Věta (Bikvadratický zákon reciprocity). Pro libovolné liché primární prvočinitele $\alpha, \beta \in \mathbb{Z}[i]$ je

$$\left(\frac{\alpha}{\beta}\right)_4 = (-1)^{(N(\alpha)-1)(N(\beta)-1)/16} \left(\frac{\beta}{\alpha}\right)_4,$$

kde $\left(\frac{\alpha}{\beta}\right)_4$ značí hodnotu i^λ, $\lambda \in \{0, 1, 2, 3\}$, pro kterou platí: $\alpha^{(N(\beta)-1)/4} \equiv i^\lambda \pmod{m}$.

i značit obvyklým symbolem $\mathbb{Z}[\alpha_i]$. *Jednotkou* (*complexe Einheit*) Dirichlet rozuměl prvek $\varphi(\alpha_i) \in \mathbb{Z}[\alpha_i]$, pro který je $\varphi(\alpha_1)\varphi(\alpha_2)\dots\varphi(\alpha_n) = 1$.

Jak jsme viděli výše, jedním z podnětů pro budování teorie dělitelnosti algebraických čísel byl důkaz zákona reciprocity vyššího řádu. Dalším stimulem byla snaha dokázat *velkou Fermatovu větu*, tj. tvrzení, že rovnice

$$x^n + y^n = z^n \tag{2.4}$$

nemá pro $n > 2$ řešení v $\mathbb{Z}$ (a tedy ani v $\mathbb{Q}$), pro něž $xyz \neq 0$. V první polovině devatenáctého století dokázali některé speciální případy této věty Sophie Germain (1776–1831), C. F. Gauss, Adrien Marie Legendre (1752 až 1833), P. G. L. Dirichlet a Gabriel Lamé (1795–1870). Na tomto místě jen připomeňme, že z neřešitelnosti rovnice (2.4) plyne neřešitelnost rovnice $x^{mn} + y^{mn} = z^{mn}$ pro libovolné kladné celé číslo m. Proto k důkazu velké Fermatovy věty pro všechna $n > 2$ stačí dokázat, že platí pro $n = 4$ a pro všechna lichá prvočísla. Do konce roku 1839 byly vyřešeny případy $n = 3$, 4, 5, 7,[6] z toho nejobtížnější byl důkaz pro $n = 7$, který podal G. Lamé v práci [Lam1]. Zbývala tedy všechna lichá prvočísla kromě 3, 5 a 7.

1. března 1847 přednášel Lamé v pařížské akademii o svém „obecném důkazu“ velké Fermatovy věty pro libovolné prvočíslo $n > 2$. Základní myšlenka spočívala v rozkladu $x^n + y^n$ na součin lineárních faktorů pomocí komplexního čísla α, kde $\alpha^n = 1,\ \alpha \neq 1$:[7]

$$x^n + y^n = (x + y)(x + \alpha y)(x + \alpha^2 y)\dots(x + \alpha^{n-1} y)\,.$$

Jsou-li x, y taková, že čísla

$$x + y,\ x + \alpha y,\ \dots,\ x + \alpha^{n-1} y \tag{2.5}$$

jsou po dvou nesoudělná, pak rovnice (2.4) implikuje, že každé z čísel (2.5) je v $\mathbb{Z}[\alpha]$ n-tou mocninou. Odtud se pak dojde ke sporu pomocí metody nekonečného sestupu. Mají-li některá dvě z čísel (2.5) největšího společného dělitele $m > 1$, pak m je největším společným dělitelem všech čísel (2.5).[8] Čísla

$$(x + y)/m,\ (x + \alpha y)/m,\ \dots,\ (x + \alpha^{n-1} y)/m$$

jsou potom nesoudělná a použije se na ně argument z předchozího případu.[9]

Joseph Liouville však ihned poukázal na to, že předložený důkaz závisí na jednoznačnosti rozkladu prvků okruhu $\mathbb{Z}[\alpha]$ na součin prvočinitelů, která zatím nebyla dokázána.[10] Gabriel Lamé a Augustin Louis Cauchy (1789–1857) se

[6] Dříve než případ $n = 7$ byl vyřešen případ $n = 14$; důkaz podal Dirichlet v práci [Dir1].

[7] Zřejmě platí: $X^n - 1 = (X - 1)(X - \alpha)(X - \alpha^2)\dots(X - \alpha^{n-1})$; položme $X = -x/y$.

[8] Dělí-li nějaké celé číslo d čísla $x + \alpha^j y$ a $x + \alpha^{j+k} y$, pak dělí i jejich rozdíl $\alpha^j y - \alpha^{j+k} y$; d však dělí i číslo $x + \alpha^{j+2k} y = (x + \alpha^{j+k}) - \alpha^k(\alpha^j y - \alpha^{j+k} y)$, podobně $x + \alpha^{j+3k} y$ atd. Číslo d je tedy dělitelem čísel $x + \alpha^{j+ik} y$ pro všechna celá kladná i. Odtud (n je prvočíslo, k není násobkem n) d je společným dělitelem všech čísel (2.5).

[9] Podle [Edw1], str. 220–223; [Edw2], str. 76–77.

[10] Uvědomme si, že jednoznačnost je nezbytná k důkazu tvrzení, že nesoudělná čísla (2.5), jejichž součin je n-tou mocninou, jsou sama n-tými mocninami.

pak v následujících týdnech pokoušeli o odstranění uvedené mezery v důkazu; Liouville si naopak v té době poznamenal do zápisníku příklad

$$13.13 = 169 = (4 + 3\sqrt{-17})(4 - 3\sqrt{-17})$$

ukazující neplatnost jednoznačné faktorizace pro $\mathbb{Z}[\alpha]$, kde $\alpha^2 = -17$.[11]

Dne 24. května 1847 Liouville přečetl na jednání akademie dopis od Ernsta Eduarda Kummera (1810 – 1893), který měl celou diskusi ukončit. Kummer totiž Liouvillemu napsal, že jeho připomínka k jednoznačné faktorizaci byla zcela oprávněná a přiložil kopii pojednání [Kum2], které publikoval již roku 1844 – ovšem na málo známém místě – a ve kterém dokázal, že jednoznačná faktorizace pro celá cyklotomická čísla (viz dále) obecně neplatí. Dodal však, že je přesto možné pro tato čísla vybudovat rozumnou aritmetiku zavedením jistých nových veličin, tzv. *ideálních komplexních čísel*, což publikoval ve formě resumé v roce 1846 v pojednáních berlínské akademie [Kum4]; práce obsahující úplnou teorii byla právě chystána k tisku v *Crelleově časopise* [Kum5]. Liouville Kummerův článek [Kum2] otiskl spolu se zmíněným dopisem [Kum7] v časopise *Journal de mathématiques pures et appliquées*.

Kummerova teorie ideálních čísel

Kummer studoval okruh celých cyklotomických čísel $\mathbb{Z}[\alpha]$, kde α je kořen polynomu

$$x^{\lambda-1} + x^{\lambda-2} + \cdots + x + 1 = (x - \alpha)(x - \alpha^2)\dots(x - \alpha^{\lambda-1}), \tag{2.6}$$

λ je prvočíslo (tj. $\alpha^\lambda = 1$, $\alpha \neq 1$). Ukázal, že ireducibilní prvek okruhu $\mathbb{Z}[\alpha]$ nemusí být zároveň prvočinitelem v dnešním smyslu;[12] aby tento problém odstranil, rozšířil okruh $\mathbb{Z}[\alpha]$ o jistá „ideální čísla“, takže každý takový „nevhodný“ prvek je možné rozložit na součin prvočinitelů. Dále Kummer ukázal, že každý „reálný nebo ideální“ prvočinitel libovolného celého cyklotomického čísla je dělitelem nějakého prvočísla $p \in \mathbb{Z}$. To znamená, že k nalezení všech prvočinitelů v $\mathbb{Z}[\alpha]$ stačí uvažovat rozklady prvočísel ze $\mathbb{Z}$. Pro $p = m\lambda + 1$ se rozklad provádí v rámci okruhu $\mathbb{Z}[\alpha]$, v obecném případě Kummer pracuje s *Gaussovými periodami*, které již dříve studoval v pojednání [Kum3] z roku 1846.[13]

Velmi zjednodušeně lze říci, že v Kummerově teorii se pro každé prvočíslo p uvažuje rozklad

$$\begin{aligned} x^{\lambda-1} + \cdots + x + 1 = (x - \alpha)(x - \alpha^2)\dots(x - \alpha^{\lambda-1}) \equiv \\ \equiv V_0(x)V_1(x)\dots V_{e-1}(x) \pmod{p}, \end{aligned} \tag{2.7}$$

[11] Události z jara roku 1847 jsou podrobně popsány např. v [Edw1], str. 220–223; [Edw2], str. 76–79.

[12] Připomeňme, že *ireducibilním prvkem* se nazývá prvek, který nemá jiný než triviální rozklad, *prvočinitelem* se nazývá prvek s tou vlastností, že je-li jím dělitelný součin dvou čísel, pak je jím dělitelný alespoň jeden z činitelů; v obou případech se předpokládá, že daný prvek není jednotkou.

[13] Poznamenejme, že tyto periody definoval C. F. Gauss v práci [Gau1] z roku 1801. V Kummerově pojetí jsou pro dané prvočíslo p Gaussovy periody η_i zavedeny následujícím způsobem. Nechť $f \in \mathbb{Z}$ je nejmenší kladné celé číslo, pro něž $p^f \equiv 1 \pmod{\lambda}$; z malé Fermatovy věty plyne, že $\lambda - 1 = e.f$, $e \in \mathbb{Z}$. Nechť dále γ značí tzv. *primitivní kořen modulo* λ, tj. $\gamma^{\lambda-1} \equiv 1 \pmod{\lambda}$, $\gamma^n \not\equiv 1 \pmod{\lambda}$ pro $0 < n < \lambda - 1$ (mocniny čísla γ tedy proběhnou

kde $V_i(x) \in \mathbb{Z}[x]$ jsou polynomy tvaru $x^f + v_1 x^{f-1} + \cdots + v_f$,[14] které jsou ireducibilní v $\mathbb{Z}[x]$ vzhledem k modulu p, přičemž

$$V_i(x) \equiv (x - \alpha^{\gamma^i})(x - \alpha^{\gamma^{e+i}}) \dots (x - \alpha^{\gamma^{(f-1)e+i}}) \pmod{p}.$$

Každému faktoru $V_i(x)$, či každé Gaussově periodě η_i pak určitým způsobem odpovídá jeden prvočinitel $\mathfrak{p}_i$ prvočísla p (reálný nebo ideální), takže

$$p = \mathfrak{p}_1 \, \mathfrak{p}_2 \, \dots \, \mathfrak{p}_{e-1}.$$

Na základě své teorie Kummer podal důkaz velké Fermatovy věty pro všechny exponenty λ, které jsou regulárními prvočísly, a to v pracích [Kum6] z roku 1847 a [Kum11] z roku 1850.[15] Původní teorie – a tedy i uvedený důkaz velké Fermatovy věty – však ještě obsahovala jistý nedostatek, který byl odstraněn až v pojednání [Kum14] z roku 1857.[16] Téhož roku byly otištěny články [Kum15] a [Kum16] věnované znovu velké Fermatově větě, které byly založeny již na správné teorii. Zákonu reciprocity Kummer věnoval pojednání [Kum8] z roku 1850 a dále pojednání [Kum17] až [Kum20] z let 1858 – 86; zformuloval a dokázal jej pro exponenty, které jsou regulárními prvočísly.

Obecný případ

Kummer vytvořil aritmetiku pro celá cyklotomická čísla. K tomu, že nepokračoval dál a nezobecnil svou teorii na obecný případ, pravděpodobně přispělo (kromě toho, že pro své vlastní účely obecnou teorii nepotřeboval) i to, že na zobecnění pracoval jeho žák Leopold Kronecker (1823 – 1891). V pojednání [Kum19] z roku 1859 Kummer dokonce odkazuje na *práci pana Kroneckera, která se brzy objeví, v níž je teorie nejobecnějších komplexních čísel úplně a nanejvýš jednoduše rozvinuta.*[17] Bohužel, zmiňovaná práce nevyšla. Kronecker publikoval svou teorii až v roce 1882 [Kro2].[18] V Kroneckerových stopách

---

všechny nekongruentní zbytky modulo λ). Gaussovými periodami Kummer rozumí součty

$$\begin{array}{lcl}
\eta_0 & = & \alpha + \alpha^{\gamma^e} + \alpha^{\gamma^{2e}} + \cdots + \alpha^{\gamma^{(f-1)e}}, \\
\eta_1 & = & \alpha^{\gamma} + \alpha^{\gamma^{e+1}} + \alpha^{\gamma^{2e+1}} + \cdots + \alpha^{\gamma^{(f-1)e+1}}, \\
\eta_2 & = & \alpha^{\gamma^2} + \alpha^{\gamma^{e+2}} + \alpha^{\gamma^{2e+2}} + \cdots + \alpha^{\gamma^{(f-1)e+2}}, \\
& \cdots & \\
\eta_{e-1} & = & \alpha^{\gamma^{e-1}} + \alpha^{\gamma^{2e-1}} + \alpha^{\gamma^{3e-1}} + \cdots + \alpha^{\gamma^{fe-1}}.
\end{array}$$

[14] Při označení z poznámky 13.

[15] Jednu z ekvivalentních podmínek charakterizujících *regulární prvočísla* lze vyjádřit tak, že se λ nevyskytuje v čitateli prvních $(\lambda - 3)/2$ Bernoulliho koeficientů, které se obvykle definují jako koeficienty B_n v rozvoji $x(1 - e^x)^{-1} = 1 - x/2 + \sum_{n=1}^{\infty} B_n x^n/(2n)!$.

Poznamenejme, že jediná prvočísla menší než 100, která nejsou regulární, jsou 37, 59 a 67. V roce 1915 dokázal Jensen, že existuje nekonečně mnoho neregulárních prvočísel. Není však známo, zda existuje také nekonečně mnoho regulárních prvočísel.

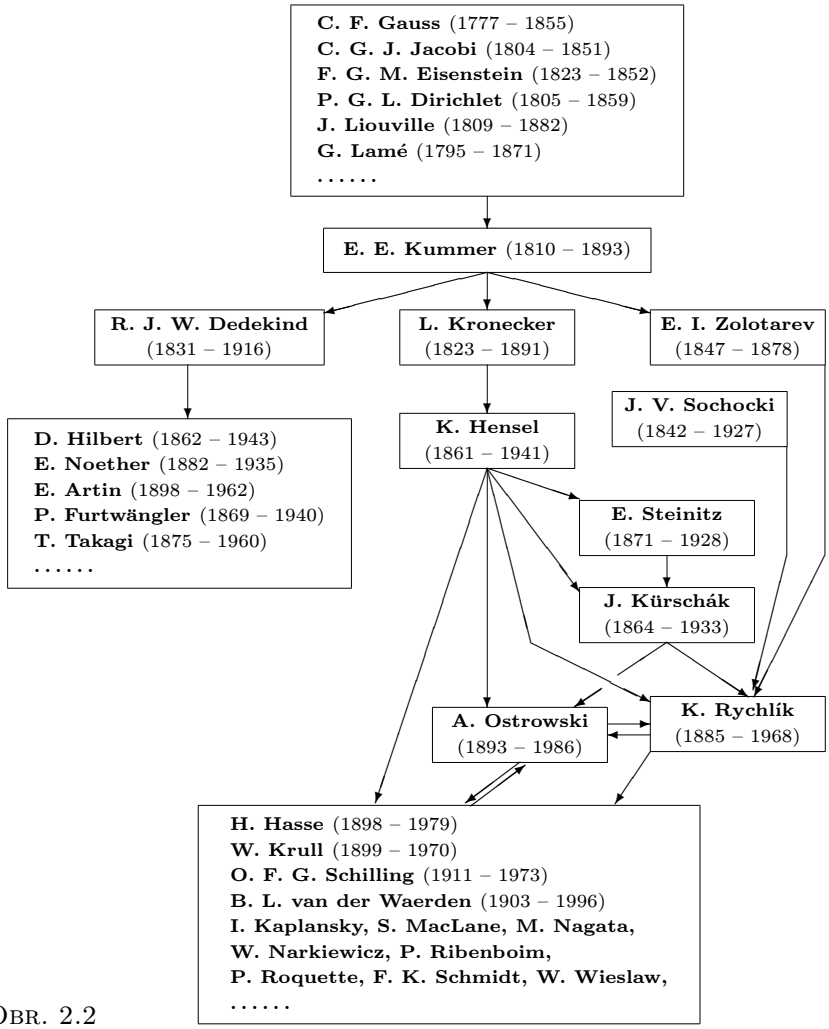
[16] Srov. [Edw1], str. 228–231; [Edw3], str. 328.

[17] [Kum19], str. 57, v přetisku str. 739.

[18] Někdy se můžeme setkat s tím, že je udán rok 1881; práce byla totiž otištěna na začátku roku 1882, avšak jako „oficiální datum publikace“ je udáno 10. září 1881, den padesátého výročí doktorátu Kroneckerova učitele a přítele E. E. Kummera; práce nese podtitul *Festschrift zu Herrn E. E. Kummers Doctor–Jubiläum, 10. September 1881.*

pokračoval jeho žák Kurt Hensel (1861 – 1941), jehož žákem byl Helmut Hasse (1898 – 1979), ale také Alexander Ostrowski (1893 – 1986) či Abraham Halevy Fraenkel (1891 – 1965).

Jiným způsobem vyřešil obecný případ Richard Julius Wilhelm Dedekind (1831 – 1916), který svou teorii popsal nejprve roku 1871 v *Dodatku X* ke druhému vydání Dirichletovy knihy *Vorlesungen über Zahlentheorie* [Dir3], později v *Dodatku XI* ke třetímu (1879) a čtvrtému (1894) vydání této knihy.



Obr. 2.2

Obrázek 2.2 zobrazuje hlavní vlivy ve vývoji teorie algebraických čísel. Jeho účelem je především ukázat, kam lze zařadit práce Karla Rychlíka; nejsou zde tedy znázorněny všechny existující vazby, neboť tím by se smysl obrázku zastřel. Schéma se snaží zachytit dva hlavní směry, *teorii ideálů* představovanou

R. Dedekindem a jeho následovníky a *teorii divisorů* představovanou L. Kroneckerem a dalšími matematiky, mezi nimiž je i Karel Rychlík. Oba přístupy jsou stručně zhodnoceny v předmluvě Hasseho knihy [Has3]:

K teorii algebraických čísel existují dva podstatně různé přístupy, přes teorii divisorů a přes teorii ideálů. První je založen na aritmetickém zkoumání Kummera a Kroneckera, stejně jako na funkcionálně-teoretické metodě Weierstrassově, rozvinut byl na přelomu století Henselem a potom byl podložen Steinitzovou obecnou teorií těles a obecnou teorií ohodnocení Kürschákа, Ostrowského aj.

Druhý byl vytvořen o něco dříve Dedekindem, vystavěn Hilbertem a potom prohlouben obecnou teorií ideálů E. Noetherové, Artina aj.

Nejprve se zdálo, že teorie ideálů je lepší než teorie divisorů; nejen proto, že vede k cíli rychleji a s menší námahou, ale také pro svou užitečnost v hlubším studiu teorie čísel. Furtwänglerovi a Takagimu se na této bázi podařilo vybudovat základy velkolepé konstrukce teorie těles tříd zahrnující obecný zákon reciprocity pro algebraická čísla, zatímco na Henselově straně nebyl takový pokrok zaznamenán. Nicméně později se ukázalo, nejprve v teorii kvadratických forem, později především v teorii hyperkomplexních čísel (algeber), že teorie divisorů či teorie ohodnocení je nejen schopna vyjádřit strukturální zákony aritmetiky jednodušeji a přirozeněji tím, že umožňuje přenesení dobře známých souvislostí mezi lokálními a globálními vztahy z teorie funkcí do aritmetiky, ale dokonce že skutečný význam teorie těles tříd a obecného zákona reciprocity pro algebraická čísla je odhalen pouze tímto přístupem. Misky vah se tedy nyní naklánějí ve prospěch teorie divisorů.[19]

Třetím matematikem, kterého lze považovat za zakladatele obecné teorie, je Egor Ivanovič Zolotarev (1847 – 1878), jehož pojednání [Zol2] vyšlo roku 1874, [Zol3] roku 1877 a dva roky po jeho smrti pak byla otištěna práce [Zol4]. Uvedené Zolotarevovy práce jsou poměrně málo známé a neměly příliš velký vliv na další vývoj. „Západní“ autoři často hovoří jako o zakladatelích jen o Kroneckerovi a Dedekindovi.[20] Zolotarevova teorie je však zajímavá mimo jiné tím, že rozvíjí přímo Kummerův postup a má velmi blízko k pozdějším pracím Kurta Hensela, který zavedl p-adická čísla (nicméně i Hensel cituje

[19] [Has3], str. IV.

[20] Například H. M. Edwards se v práci [Edw3] zmiňuje o Zolotarevovi pouze v poznámce pod čarou na str. 322, a to následujícím způsobem:

Někteří autoři z nedávné doby uvedli ruského matematika Egora Ivanoviče Zolotareva (1847 – 1878) jako jednoho ze zakladatelů teorie ideálů. Nicméně Zolotarevova práce byla zpracována poté, co byla publikována práce Dedekindova, a zdá se, že neměla žádný vliv na vývoj teorie.

Podobně píše i L. Corry v [Cor1] poznámce pod čarou na str. 120. N. Bourbaki v [Bou1] (v překladu str. 100) zmiňuje Zolotarevovu teorii v souvislosti s prvními pokusy R. Dedekinda, avšak již ji nepovažuje za zajímavou. J. Dieudonné v knize [Die1] Zolotarevovu práci [Zol4] pouze uvádí v seznamu literatury k danému tématu, H. Weyl se v práci [Wey1] o Zolotarevovi nezmiňuje vůbec, stejně tak D. Hilbert v přehledu [Hil1] aj.

Naopak v ruské knize [K-J1] jsou uvedené Zolotarevovy práce podrobně diskutovány (str. 107–116), na rozdíl od práce Kroneckerovy, o níž je zde jen krátká zmínka (str. 132–133). W. Narkiewicz v [Nar1] v historické poznámce na str. 119 uvádí Zolotarevovu teorii jako třetí a rovnocennou metodu a cituje bibliografii jejích výkladů, např. [Čbo1], [Čbo2], [Čbo3] aj.

jen Dedekinda a Kroneckera); tato cesta později vyústila v „lokální algebru“. Navíc byla Zolotarevova teorie uveřejněna dříve, než teorie Kroneckerova. Na Zolotarevovo pojednání [Zol4] z roku 1880 pak bezprostředně navázal Karel Rychlík.

Každý ze tří uvedených matematiků postupoval odlišnou cestou. Všichni však dali stejnou odpověď na otázku, jaké prvky daného algebraického tělesa $\mathbb{Q}(\alpha)$ je rozumné pokládat za celé. Místo prvků okruhu $\mathbb{Z}[\alpha]$, jak tomu bylo dříve, uvažovali jako *celá* taková čísla z tělesa $\mathbb{Q}(\alpha)$, která jsou kořeny nějakého monického polynomu tvaru (2.3) s celočíselnými koeficienty.

Popis celého historického vývoje překračuje rámec tohoto úvodu. Podívejme se však ještě alespoň na práce Kurta Hensela, jejichž výsledky budeme nezbytně potřebovat v částech 2.1.2 – 2.1.4 při diskusi prací Karla Rychlíka.

Kurt Hensel

Kurt Hensel se intenzivně zabýval teorií algebraických funkcí. Ze všech jeho prací věnovaných této problematice zde uveďme „klasickou“ knihu [Hen4] z roku 1902, kterou napsal společně s G. Landsbergem. Jméno Kurta Hensela je dodnes známé zejména v souvislosti se zavedením p-adických čísel; tento pojem se objevil poprvé v pojednání *Über eine neue Begründung der Theorie der algebraischen Zahlen* [Hen1] z roku 1899, kterému předcházela řada prací, ve kterých se již Henselova teorie formovala a na kterých je zřetelný vliv Leopolda Kroneckera. Z dalších Henselových publikací zde jmenujme [Hen2], [Hen3], [Hen5]–[Hen7] z let 1901–1907. Výsledky své práce na poli teorie algebraických čísel Hensel shrnul v dodnes velmi často citované monografii *Theorie der algebraischen Zahlen I* [Hen8] z roku 1908.[21] V roce 1913 vyšla monografie *Zahlentheorie* [Hen12] věnovaná obecněji okruhům g-adických čísel pro složené číslo g. Poslední dvě citované knihy jsou pro naše potřeby nejdůležitější, neboť na ně navázal Karel Rychlík ve svých nejvýznamnějších pracích. V dalším se proto budeme věnovat výhradně jim. Je však třeba zdůraznit, že Hensel se teorií algebraických čísel zabýval i později. V souvislosti s Karlem Rychlíkem připomeňme ještě Henselův článek *Über die Grundlagen einer neuen Theorie der quadratischen Zahlkörper* [Hen13] z roku 1914, který Rychlík zmiňuje ve své práci [R11].

V úvodu knihy [Hen8] Hensel rozebírá motivaci, která ho přivedla k předložené teorii:

Mezi oběma největšími a nejdůležitějšími disciplinami moderní matematiky, teorií funkcí a teorií čísel, existuje co do výsledků podivuhodná a dalekosáhlá analogie, v jejich metodách je však veliký rozdíl; a již předem můžeme říci, že srovnání obou disciplin podle použitelnosti a účinnosti jejich metod dopadne velmi výrazně ve prospěch analýzy . . . [22]

Od svého prvního přemítání o otázkách vyšší teorie čísel věřím, že metody teorie funkcí musí být upotřebitelné i v tomto oboru a že na tomto základě může

[21] Zůstalo jen u prvního dílu.
[22] [Hen8], str. 1.

být teorie algebraických čísel vybudována v mnoha směrech jednodušeji ...[23]

Ilustrujme Henselovy myšlenky následujícím příkladem, v němž budeme pro polynom $F(x) = x^3 - x^2 - 2x - 8$ uvažovat rozklady modulo 2^k, $k \in \mathbb{N}$:[24]

$$\begin{aligned} F(x) &\equiv x^2(x+1) \pmod 2 \\ &\equiv x(x-2)(x+1) \pmod{2^2}, \quad \text{resp.} \pmod{2^3} \\ &\equiv (x+4)(x+2)(x+9) = (x+2^2)(x+2)(x+1+2^3) \pmod{2^4} \\ &\equiv (x+12)(x+10)(x+9) = (x+2^2+2^3)(x+2+2^3)(x+1+2^3) \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \pmod{2^5} \\ &\ldots\ldots \\ &\equiv (x+172)(x+170)(x+169) = (x+2^2+2^3+2^5+2^7)\cdot \\ &\qquad\qquad \cdot(x+2+2^3+2^5+2^7)(x+1+2^3+2^5+2^7) \pmod{2^8} \\ &\ldots\ldots \end{aligned}$$

Půjde o to, že vždy existuje právě jedno celé číslo $\delta \geq 1$ (v našem případě $\delta = 3$; obecně číslo, pro něž lze diskriminant daného polynomu vyjádřit ve tvaru $D(F(x)) = p^\delta E$, kde $E \in \mathbb{Z}$, E není dělitelné prvočíslem p; viz větu 8, str. 76) s touto vlastností: pro $r \geq \delta + 1$ je rozklad

$$F(x) \equiv f_1(x) \ldots f_k(x) \pmod{p^r}, \quad f_i(x) \text{ ireducibilní nad } \mathbb{Q} \text{ modulo } p^r,$$

analogický rozkladu

$$F(x) \equiv \overline{f}_1(x) \ldots \overline{f}_k(x) \pmod{p^{\delta+1}}, \quad \overline{f}_i(x) \text{ ireducibilní nad } \mathbb{Q} \text{ modulo } p^{\delta+1},$$

přičemž jednotlivé koeficienty v $f_i(x)$ jsou „pokračováním“ odpovídajících koeficientů v $\overline{f}_i(x)$ v tom smyslu, že je lze vyjádřit ve tvaru

$$\pm(a_0 + a_1 p + \cdots + a_m p^m), \quad 0 \leq a_i \leq p-1,$$

a při přechodu k vyšším exponentům r se pouze přidávají další členy na konec tohoto rozvoje. To pak vede k uvažování polynomů, jejichž koeficienty jsou formální součty $\pm\sum_{i=0}^{\infty} a_i p^i, 0 \leq a_i \leq p-1$, čili *p-adická čísla*; prvočíslo p se potom v tělese $\mathbb{Q}(\alpha)$, kde $F(x)$ je minimální polynom pro α, rozloží v *prvodivisory*, z nichž každý odpovídá jednomu faktoru $f_i(x)$, tedy $p \sim \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_g^{e_g}$.

Rozbor Henselových monografií začneme mladší z nich, knihou *Zahlentheorie* [Hen12], a to z toho důvodu, že je zde vybudován obecně okruh g-adických čísel pro složené přirozené číslo g, zatímco pro potřeby teorie algebraických čísel v [Hen8] Hensel zavedl pouze těleso čísel p-adických, kde p je prvočíslo; postup je přitom velmi podobný. Až se budeme věnovat pracím Karla Rychlíka, budeme potřebovat právě postup z [Hen12] v souvislosti se zavedením g-adických čísel a výsledky z [Hen8] z teorie algebraických čísel.

[23] [Hen8], str. IV.

[24] Příklad pochází od R. Dedekinda, který jej uvedl v roce 1878 pro ilustraci obtíží, které nastanou při snaze o zobecnění Kummerovy teorie cyklotomických čísel a kvůli kterým nakonec Kummerovu cestu opustil a položil základy teorie ideálů.

Zahlentheorie [Hen12] (1913)

V úvodu knihy [Hen12] Hensel definuje základní struktury jako *těleso* (axiomaticky, v dnešním slova smyslu), *modul* (v dnešní terminologii aditivní grupa), *grupa* (multiplikativní grupa) a *okruh* (komutativní okruh). Definuje také *okruh vytvořený* (*komponierte*) *z těles* $K,\ K'$ (direktní součet) jako množinu

$$R(K,K') = \{(a,a'),\ a\ \in K,\ a' \in K'\}$$

se součtem a součinem po složkách a dokazuje, že je to skutečně okruh. Potom se obrací k tělesu racionálních čísel $\mathbb{Q}$ a zavádí pojem *dělitelnosti v oboru* g.

Definice 1 (Dělitelnost v oboru g). Nechť $g > 1$ je libovolné, pevně dané celé číslo. Racionální číslo $A = m/n$, kde m, n jsou celá nesoudělná čísla, se nazývá *celé v oboru* g nebo *modulo* g *celé* (*für den Bereich von* g *ganz* nebo *modulo* g *ganz*), jsou-li čísla n a g nesoudělná; jinak se číslo A nazývá *lomené* (*gebrochen*) *v oboru* g. *Jednotkou* (*Einheit*) *v oboru* g se nazývá racionální číslo E takové, že E i $1/E$ jsou čísla celá v oboru g. Racionální číslo A je *v oboru* g *dělitelné* (*teilbar*) racionálním číslem B, je-li číslo A/B celé v oboru g. Racionální čísla A, B se nazývají *kongruentní* (*kongruent*) *modulo* g^ρ, kde ρ je libovolné (i záporné) celé číslo, je-li jejich rozdíl $A - B$ dělitelný g^ρ; pro kongruenci se užívá zápis $A \equiv B \pmod{g^\rho}$.

Hensel ukazuje, že každé racionální číslo $A \in \mathbb{Q}$ lze právě jedním způsobem rozvinout v *g-adickou řadu* tvaru (2.8) s modulo g redukovanými koeficienty, tj. $a_i \in \{0, 1, \ldots, g-1\}$.[25] Rovnost racionálního čísla A a jeho g-adického rozvoje je přitom definována tak, že pro libovolnou kladnou mocninu g^{r+1} platí:

$$A \equiv a_n g^n + a_{n+1} g^{n+1} + \cdots + a_r g^r \pmod{g^{r+1}}.$$

Z těchto úvah pak vychází následující definice g-adického čísla.

Definice 2 (g-adická čísla). *g-adickým číslem* se nazývá každá řada

$$A = a_n g^n + a_{n+1} g^{n+1} + \cdots, \quad n \in \mathbb{Z}, \tag{2.8}$$

kde koeficienty a_i jsou libovolná racionální čísla celá v oboru g.

[25] Každé číslo celé v oboru g je zřejmě kongruentní s právě jedním modulo g redukovaným číslem a_0, proto $A = a_0 + gA_1$, kde A_1 je celé v oboru g; analogicky $A_1 = a_1 + gA_2$, …, $A_\rho = a_\rho + gA_{\rho+1}$, kde a_i jsou jednoznačně určená čísla z množiny $\{0, 1, \ldots, g-1\}$, A_i jsou čísla celá v oboru g. Po dosazení lze psát: $A = a_0 + a_1 g + a_2 g^2 + \cdots + a_\rho g^\rho + A_{\rho+1} g^{\rho+1}$. Proces může pokračovat libovolně dlouho, tj. pro libovolné ρ.

Není-li racionální číslo A celé v oboru g, lze je vyjádřit ve tvaru $A = B/g^\nu$, kde B je celé v oboru g, $\nu > 0$, a platí: $A = a_{-\nu} g^{-\nu} + \cdots + a_{-1} g^{-1} + a_0 + a_1 g + \cdots + a_\rho g^\rho + A_{\rho+1} g^{\rho+1}$.

Příklad. Pro ilustraci ukažme některé rozvoje:

$$\begin{aligned}
5673 &= 3,76500\ldots = 3,765\ (10) && (5673 = 3 + 7.10 + 6.10^2 + 5.10^3)\\
-3 &= 7,999\ldots\ (10) && (-3 = 7 + 10.(-1); 1 = 9 + 10.(-1),\ \ldots)\\
\tfrac{172}{5} &= \tfrac{344}{10} = 4,43\ (10) && (344 = 4 + 4.10 + 3.10^2)\\
\tfrac{2}{3} &= 4,333\ldots\ (10) && (\tfrac{2}{3} = 4 + (-\tfrac{1}{3}).10;\ -\tfrac{1}{3} = 3 + (-\tfrac{1}{3}).10,\ \ldots)
\end{aligned}$$

g-adická čísla lze rozdělit takto:

$$\left\langle \begin{array}{l} \textit{redukovaná } (a_i \in \{0,1,\ldots,\ g-1\}) \quad \left\langle \begin{array}{l} \textit{celá } (n \geq 0) \\ \textit{lomená } (n < 0) \end{array} \right. \\ \\ \textit{neredukovaná } (a_i - \text{libovolná racionální čísla celá v oboru } g) \end{array} \right. \tag{2.9}$$

Pro tyto nové objekty Hensel dále definuje rovnost a početní operace.[26]

Definice 3. *k-tou aproximací* (*k-ten Näherungswert*) g-adického čísla (2.8) se nazývá racionální číslo $A^{(k)} = a_n g^n + a_{n+1} g^{n+1} + \ \cdots \ + a_k g^k$. Dvě g-adická čísla A, A' se nazývají *kongruentní modulo* g^{k+1}, je-li $A^{(k)} \equiv A'^{(k)} \pmod{g^{k+1}}$; g-adická čísla A, A' se nazývají *rovnými,* jsou-li kongruentní pro každou mocninu základu g.

Hensel dokazuje, že právě definovaná rovnost je reflexivní, symetrická a tranzitivní relace; dále ukazuje, že dvě redukovaná g-adická čísla jsou si rovna, právě když jsou identická, a že každé g-adické číslo je rovno právě jednomu číslu redukovanému.[27]

Definice 4. *Součtem* $A + B$, resp. *součinem* AB dvou libovolných g-adických čísel A, B budeme rozumět číslo C, resp. D s touto vlastností: pro každé k' existuje k tak, že pro k-tou a vyšší aproximace je

$$\begin{array}{rcccll} C^{(k)} & = & (A+B)^{(k)} & \equiv & A^{(k)} + B^{(k)} & (\text{mod } g^{k'}), \\ D^{(k)} & = & (AB)^{(k)} & \equiv & A^{(k)} B^{(k)} & (\text{mod } g^{k'}). \end{array}$$

Věta 1. Množina g-adických čísel $\mathbb{Q}_g$ spolu s právě definovanými operacemi tvoří komutativní okruh.[28]

V další části se Hensel zabývá vztahy mezi g-adickými čísly o různých základech. Začíná úvahami, které ukazují, že každé g-adické číslo lze považovat za g^k-adické ($k > 0$) a naopak;[29] obecněji lze každé g-adické číslo vyjádřit jako číslo g'-adické a naopak, obsahují-li základy g, g' stejná prvočísla (případně v různých mocninách).[30] Tyto úvahy, které manipulují s nekonečnými součty, potom Hensel zpřesňuje na základě následující definice.

[26] V definici rovnosti a početních operací, stejně jako v pozdější definici rovnosti v oboru g', se Hensel pro jednoduchost omezuje na g-adická čísla tvaru (2.8), kde $n = 0$, takže uvažuje $k \in \mathbb{Z}$, $k \geq 0$. Podotýká však, že všechny pojmy a tvrzení lze snadno přenést na okruh všech g-adických čísel.

[27] To umožňuje dodefinovat pojem celého čísla i pro čísla neredukovaná: neredukované g-adické číslo B se nazývá *celé*, je-li celé to redukované g-adické číslo, jemuž je B rovno.

[28] Hensel psal $R(g)$, my se však budeme držet obvyklého označení $\mathbb{Q}_g$.

[29] Uvažujme libovolné, pro jednoduchost celé g-adické číslo $A = a_0 + a_1 g + a_2 g^2 + \cdots$. Toto číslo můžeme vyjádřit pomocí aproximací takto:

$$A = A^{(k-1)} + (A^{(2k-1)} - A^{(k-1)}) + (A^{(3k-1)} - A^{(2k-1)}) + \cdots = (a_0 + a_1 g + \cdots + a_{k-1} g^{k-1}) +$$

$$+ (a_k + a_{k+1} g + \cdots + a_{2k-1} g^{k-1}) g^k + (a_{2k} + a_{2k+1} g + \cdots + a_{3k-1} g^{k-1}) g^{2k} + \cdots \ .$$

[30] Pak existuje nejnižší mocnina g^k, která je dělitelná g', podobně existuje nejnižší mocnina $g'^{k'}$ dělitelná g.

Definice 5. Uvažujme g-adické číslo A a g'-adické číslo A'. Řekneme, že čísla A, A' jsou si *rovna v oboru* g', značíme $A = A'$ (g'), jestliže pro každé l existuje k tak, že $A^{(k)} \equiv A'^{(k)} \pmod{g'^l}$; analogicky se definuje *rovnost v oboru g*.

Potom se Hensel postupně dostává k důkazu tvrzení, které s využitím dnešního značení můžeme zapsat takto:

Věta 2. Pro libovolná prvočísla $p, q, \ldots, r$ a přirozená čísla $k, l, \ldots, m$ platí:

$$\mathbb{Q}_{p^k q^l \ldots r^m} = \mathbb{Q}_{pq\ldots r}. \tag{2.10}$$

Z dalších Henselových výsledků zde uveďme věty o tzv. aditivním a multiplikativním normálním tvaru.

Věta 3 (Aditivní normální tvar). Nechť $g > 1$ je libovolné celé číslo, nechť $p, q, \ldots, r$ jsou všichni navzájem různí kladní prvočinitelé čísla g. Potom lze každé g-adické číslo A vyjádřit právě jedním způsobem v *aditivním normálním tvaru* (*additive Normalform*):

$$A = A_p + A_q + \cdots + A_r \quad (g), \tag{2.11}$$

kde g-adická čísla $A_p, A_q, \ldots, A_r$ jsou jednoznačně určena vztahy

$$\begin{array}{llll} A_p = A\ (p), & A_p = 0\ (q), & \ldots, & A_p = 0\ (r), \\ A_q = 0\ (p), & A_q = A\ (q), & \ldots, & A_q = 0\ (r), \\ \multicolumn{4}{c}{\dotfill} \\ A_r = 0\ (p), & A_r = 0\ (q), & \ldots, & A_r = A\ (r), \end{array}$$

a nazývají se *p-komponenta, q-komponenta, ..., r-komponenta čísla A*. Pro libovolná čísla $\alpha_p \in \mathbb{Q}_p$, $\alpha_q \in \mathbb{Q}_q$, ..., $\alpha_r \in \mathbb{Q}_r$ naopak existuje právě jedno g-adické číslo $A \in \mathbb{Q}_g$, jehož příslušnými komponentami jsou $\alpha_p, \alpha_q, \ldots, \alpha_r$.

K tomu Hensel poznamenává, že součet a součin dvou g-adických čísel A, B vyjádřených v aditivním normálním tvaru probíhá „po komponentách“, tj. $(A + B)_p = A_p + B_p$, $(AB)_p = A_p B_p$, atd.

Dnešními slovy můžeme větu 3 vyjádřit tak, že okruh $\mathbb{Q}_g$ je direktním součtem

$$\mathbb{Q}_g = \mathbb{Q}_p \oplus \mathbb{Q}_q \oplus \cdots \oplus \mathbb{Q}_r, \quad \text{kde } g = p^k q^l \ldots r^m. \tag{2.12}$$

Z aditivního normálního tvaru lze snadno odvodit tzv. *multiplikativní normální tvar*:

Věta 4 (Multiplikativní normální tvar). Každé g-adické číslo A lze vyjádřit právě jedním způsobem v *multiplikativním normálním tvaru* (*multiplicative Normalform*):

$$A = \mathfrak{A}_p \mathfrak{A}_q \ldots \mathfrak{A}_r \quad (g), \tag{2.13}$$

kde $\mathfrak{A}_p, \mathfrak{A}_q, \ldots, \mathfrak{A}_r$ jsou g-adická čísla jednoznačně určená rovnicemi

$$\begin{array}{llll} \mathfrak{A}_p = A\ (p), & \mathfrak{A}_p = 1\ (q), & \ldots, & \mathfrak{A}_p = 1\ (r), \\ \mathfrak{A}_q = 1\ (p), & \mathfrak{A}_q = A\ (q), & \ldots, & \mathfrak{A}_q = 1\ (r), \\ \multicolumn{4}{c}{\dotfill} \\ \mathfrak{A}_r = 1\ (p), & \mathfrak{A}_r = 1\ (q), & \ldots, & \mathfrak{A}_r = A\ (r). \end{array}$$

Analogicky s předcházející větou Hensel poznamenává, že pro součin dvou g-adických čísel A, B platí: $(\mathfrak{AB})_p = \mathfrak{A}_p\mathfrak{B}_p$, stejně pro ostatní faktory.

Pro další úvahy je důležitá následující věta.

Věta 5. Je-li p prvočíslo, pak okruh p-adických čísel $\mathbb{Q}_p$ je tělesem. Je-li g složené, existují v okruhu $\mathbb{Q}_g$ netriviální dělitelé nuly.

Potom Hensel vyšetřuje těleso $\mathbb{Q}_p$,[31] kde p je prvočíslo. Kvůli pozdějším odkazům zde uveďme několik pojmů. Libovolné nenulové číslo $A \in \mathbb{Q}_p$ lze právě jedním způsobem vyjádřit ve tvaru

$$A = p^a E, \tag{2.14}$$

kde E je tzv. *p-adická jednotka*, tj. p-adické číslo tvaru

$$E = e_0 + e_1 p + e_2 p^2 + \cdots, \quad \text{kde} \quad (e_0, p) = 1. \tag{2.15}$$

Číslo a se nazývá *řád* (*Ordnungszahl*) čísla A, číslo

$$|A|_p = p^a \tag{2.16}$$

se nazývá *absolutní hodnota* (*absoluten Betrag*) *čísla A v oboru p.*[32]

Další partie Henselovy monografie jsou věnovány základům analýzy, algebry a teorie čísel v tělese p-adických čísel a především pak teorii čísel v okruhu čísel g-adických.

Theorie der algebraischen Zahlen [Hen8] (1908)

V knize *Theorie der algebraischen Zahlen* [Hen8] je nejprve vybudováno těleso p-adických čísel $\mathbb{Q}_p$, kde p je prvočíslo, a to podobným způsobem jako v monografii *Zahlentheorie* [Hen12]. Vztah těles $\mathbb{Q}_p$ a $\mathbb{Q}$ popisuje následující věta.

Věta 6. Číslo $A \in \mathbb{Q}_p$ v redukovaném tvaru je v oboru p rovno nějakému racionálnímu číslu právě tehdy, když je periodické.

Potom Hensel studuje polynomy s p-adickými koeficienty:[33]

$$f(x) = A_0 x^n + A_1 x^{n-1} + \cdots + A_n, \quad A_i \in \mathbb{Q}_p. \tag{2.17}$$

Uveďme zde přehledně základní Henselovy definice a věty, které budeme později potřebovat.

Definice 6. Polynom $f(x)$ tvaru (2.17) se nazývá *celočíselný* (*ganzzahlig*) *v oboru p*, jsou-li všechny koeficienty A_i celá p-adická čísla. Celočíselný polynom $f(x)$ se nazývá *primitivní,* jestliže nejsou všechny koeficienty A_i dělitelné p.

Hensel ukazuje, že každý polynom $f(x)$ lze právě jedním způsobem vyjádřit ve tvaru $f(x) = p^\delta f_0(x)$, kde $f_0(x)$ je primitivní polynom, tzv. *primitivní funkce* polynomu $f(x)$; p^δ se nazývá *číselný dělitel* (*Zahlenteiler*) *polynomu* $f(x)$.

[31] Hensel jej značil symbolem $K(p)$.

[32] Hensel psal pouze $|A|$; protože $\mathbb{Q}_p$ bylo pevně zvolené, nemohlo dojít k nedorozumění.

[33] Hensel používal pojmu *celá racionální funkce.*

DEFINICE 7. Polynom $f^{(k)}(x)$, který vznikne z polynomu (2.17) nahrazením koeficientů A_i jejich k-tými aproximacemi $A_i^{(k)}$, se nazývá *k-tou aproximací polynomu* $f(x)$. Polynomy $f(x)$ a $\overline{f}(x)$ se nazývají *kongruentní modulo* p^{k+1}, je-li $A_i \equiv \overline{A}_i \pmod{p^{k+1}}$ pro všechna $i \in \{0, 1, \ldots, n\}$. Polynomy *jsou si rovny v oboru* p, jsou-li kongruentní pro každou mocninu prvočísla p; píše se

$$f(x) = \overline{f}(x) \quad (p). \tag{2.18}$$

VĚTA 7. Libovolný polynom $f(x)$ lze v $\mathbb{Q}_p[x]$ právě jedním způsobem rozložit na součin ireducibilních p-adických faktorů.

V dalším se Hensel pro jednoduchost omezuje na tzv. *primární* (*primär*) polynomy $F(x)$, což jsou polynomy tvaru (2.17) s celými koeficienty, které jsou primitivní a jejichž vedoucí koeficient A_0 je mocninou prvočísla p, tj. $A_0 = p^\alpha$.

Důležitou roli zde hraje následující věta (srov. str. 71).

VĚTA 8. Je-li δ řád diskriminantu polynomu $F(x)$,[34] neboli $D(F(x)) = p^\delta E$, kde E je p-adická jednotka, pak se $F(x)$ rozpadá na faktory nižšího stupně, právě když se rozpadá δ-tá aproximace $F^{(\delta)}(x)$ modulo $p^{\delta+1}$:

$$F^{(\delta)}(x) \equiv \overline{f}(x)\overline{g}(x) \pmod{p^{\delta+1}}. \tag{2.19}$$

Rozkladu (2.19) přitom jednoznačně odpovídá rozklad $F(x) = f(x)g(x)$ (p), kde $\overline{f}(x), \overline{g}(x)$ jsou aproximacemi polynomů $f(x), g(x)$.

Odtud pak Hensel odvozuje kritéria rozložitelnosti polynomů.

VĚTA 9 (HENSELOVO LEMMA). Je-li pro nějaké $r \in \mathbb{Z}$

$$F(x) \equiv f_0(x)g_0(x) \pmod{p^{r+1}}, \quad r+1 \geq 2\rho, \tag{2.20}$$

kde 2ρ je řád druhé mocniny resultantu $R(f_0(x), g_0(x))$,[35] pak se polynom $F(x)$ rozloží na součin p-adických faktorů $f(x), g(x)$,

$$F(x) = f(x)g(x) \quad (p),$$

[34] *Diskriminant* $D(F(x))$ *polynomu* $F(x)$ je definován jako *resultant* $R(F(x), F'(x))$ polynomu $F(x)$ a jeho derivace $F'(x)$. *Resultantem* (*Resultante*) dvojice polynomů

$$f(x) = A_0x^\mu + A_1x^{\mu-1} + \cdots + A_\mu, \quad g(x) = B_0x^\nu + B_1x^{\nu-1} + \cdots + B_\nu$$

se rozumí determinant matice řádu $\mu + \nu$:

$$R(f,g) = \left|\begin{array}{cccccccccc} A_0 & A_1 & \ldots\ldots\ldots\ldots & & A_\mu & 0 & \ldots\ldots & 0 \\ 0 & A_0 & A_1 & \ldots\ldots\ldots\ldots & & A_\mu & \ldots\ldots & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \ldots & 0 & A_0 & A_1 & \ldots\ldots\ldots\ldots & A_\mu \\ B_0 & B_1 & \ldots\ldots\ldots\ldots & & B_\nu & 0 & \ldots\ldots\ldots\ldots & 0 \\ 0 & B_0 & B_1 & \ldots\ldots\ldots\ldots & & B_\nu & 0 & \ldots\ldots & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \ldots\ldots & 0 & B_0 & B_1 & \ldots\ldots\ldots\ldots & B_\nu \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} \nu \text{ řádků} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} \mu \text{ řádků} \end{array}$$

Srov. též pozn. 41.

[35] Tj. $R^2(f_0(x), g_0(x)) = (p^\rho)^2 E$, kde $E \in \mathbb{Q}_p$ je jednotka.

jejichž stupně jsou rovny stupňům polynomů $f_0(x), g_0(x)$ a jejichž $(r-\rho)$-tými aproximacemi jsou $f_0(x), g_0(x)$.

Speciálním případem Henselova lemmatu je následující věta (někdy označovaná rovněž jako Henselovo lemma, podobně jako některé další modifikace), kterou lze použít v případě, že jeden z faktorů má být lineární, např. $f(x) = x - \xi$, tj. v případě, že hledáme podmínku, kdy má polynom $F(x)$ p-adický kořen $x = \xi$.

Věta 10. *Můžeme-li určit celé kladné číslo ξ_0, takže podíl $F(\xi_0)/(F'(\xi_0))^2$ má kladný řád, pak má rovnice $F(x) = 0$ p-adický kořen $x = \xi$, jehož aproximace je rovna ξ_0 a který lze vypočítat s libovolnou předem danou přesností.*[36]

Z věty 9 plyne rovněž následující tvrzení.

Věta 11. Je-li $f(x)$ celočíselný primitivní ireducibilní polynom tvaru (2.17), kde koeficient A_0, resp. A_n je dělitelný p, pak jsou všechny vnitřní koeficienty $A_1, A_2, \ldots, A_{n-1}$ dělitelné p a A_n, resp. A_0 je jednotkou.

Těleso algebraických čísel $\mathbf{Q}(\alpha)$

Pro úplnost zde nejprve ve stručnosti uveďme způsob zavedení „obyčejných“ algebraických čísel v Henselově teorii.

Definice 8 (Algebraická čísla). *Algebraickým číslem* se nazývá takové číslo,[37] které je kořenem nějakého polynomu tvaru

$$F(x) = x^n + B_1 x^{n-1} + \cdots + B_n, \quad B_i \in \mathbb{Q}\,. \tag{2.21}$$

Věta 12. Mezi všemi polynomy (2.21), jimž dané algebraické číslo vyhovuje, existuje takový, jehož stupeň je nejnižší možný:

$$f(x) = x^\lambda + a_1 x^{\lambda-1} + \cdots + a_\lambda = (x-\alpha_1)\ldots(x-\alpha_\lambda), \quad a_i \in \mathbb{Q}\,. \tag{2.22}$$

Tento polynom je určen jednoznačně a je ireducibilní nad $\mathbb{Q}$.[38]

Definice 9. Nechť α značí libovolný kořen polynomu (2.22); α se nazývá *algebraické číslo λ-tého stupně*, čísla $\alpha_1, \alpha_2, \ldots, \alpha_\lambda$ se nazývají *algebraická čísla konjugovaná s α.*

Definice 10 (Dělitelnost algebraických čísel). Algebraické číslo α se nazývá *celým algebraickým číslem*, je-li kořenem nějakého polynomu tvaru (2.21) s koeficienty v $\mathbb{Z}$. Algebraické číslo α je *dělitelné* algebraickým číslem β, je-li podíl α/β celé algebraické číslo. Algebraická čísla α, β se nazývají *asociovaná*,[39] píše se $\alpha \sim \beta$, jestliže α je dělitelné číslem β a naopak. *Jednotkou* se nazývá celé algebraické číslo ε, jehož převrácená hodnota $1/\varepsilon$ je opět celé algebraické číslo.

Definice 11 (Těleso algebraických čísel $\mathbb{Q}(\alpha)$). *Tělesem vytvořeným z α* (*Durch α konstituierte Zahlkörper*) se nazývá souhrn *všech čísel, která*

[36] [Hen8], str. 71.
[37] Tím Hensel všude automaticky rozumí komplexní číslo.
[38] Polynom (2.22) se obvykle nazývá *minimální polynom α nad $\mathbb{Q}$*.
[39] Hensel psal *ekvivalentní*; pro přehlednost budeme používat obvyklý výraz *asociovaná*.

vzniknou z α čtyřmi operacemi, sčítáním, odčítáním, násobením a dělením, tj. souhrn všech racionálních funkcí α

$$\beta = \varphi(\alpha) = \frac{g(\alpha)}{h(\alpha)}$$

s racionálními koeficienty.[40]

Množinu všech celých algebraických čísel daného tělesa $\mathbb{Q}(\alpha)$ zde budeme značit symbolem $\mathfrak{D}$.

DEFINICE 12. Nechť $\beta = \varphi(\alpha)$ je číslo z tělesa $\mathbb{Q}(\alpha)$, kde α je kořen polynomu (2.22). Čísla $\beta_i = \varphi(\alpha_i)$, $i = 1, 2, \ldots, \lambda$, se nazývají *čísla konjugovaná s β*. *Norma čísla β* je definovaná jako racionální číslo $N(\beta) = \beta_1\beta_2 \ldots \beta_\lambda$.

VĚTA 13. Každé číslo $\beta = \varphi(\alpha)$ je spolu se svými konjugovanými čísly kořenem polynomu stupně λ,

$$g(y) = (y - \beta_1) \ldots (y - \beta_\lambda) = y^\lambda + b_1 y^{\lambda-1} + \cdots + b_\lambda, \quad b_i \in \mathbb{Q}, \tag{2.23}$$

který je první nebo vyšší mocninou ireducibilního polynomu nad $\mathbb{Q}$.

DEFINICE 13. *Bází tělesa* $\mathbb{Q}(\alpha)$ se nazývá libovolný systém $(\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(\lambda)})$ čísel z tělesa $\mathbb{Q}(\alpha)$, pro který platí:

$$d(\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(\lambda)}) = \begin{vmatrix} {\beta_1}^{(1)} & {\beta_1}^{(2)} & \ldots & {\beta_1}^{(\lambda)} \\ {\beta_2}^{(1)} & {\beta_2}^{(2)} & \ldots & {\beta_2}^{(\lambda)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ {\beta_\lambda}^{(1)} & {\beta_\lambda}^{(2)} & \ldots & {\beta_\lambda}^{(\lambda)} \end{vmatrix}^2 \neq 0, \tag{2.24}$$

kde ${\beta_1}^{(i)}, \ldots, {\beta_\lambda}^{(i)}$ jsou čísla konjugovaná s $\beta^{(i)}$, $i = 1, 2, \ldots, \lambda$. Racionální číslo $d(\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(\lambda)})$ se nazývá *diskriminant systému* $(\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(\lambda)})$.[41]

VĚTA 14. Každé $\gamma \in \mathbb{Q}(\alpha)$ lze právě jedním způsobem vyjádřit ve tvaru

$$\gamma = v_1\beta^{(1)} + v_2\beta^{(2)} + \cdots + v_\lambda\beta^{(\lambda)}, \quad v_i \in \mathbb{Q}, \tag{2.25}$$

kde $(\beta^{(1)}, \beta^{(2)}, \ldots, \beta^{(\lambda)})$ je báze tělesa $\mathbb{Q}(\alpha)$.[42]

---

[40] [Hen8], str. 102; používáme zde $\mathbb{Q}$, $\mathbb{Q}(\alpha)$ místo Henselova značení K, $K(\alpha)$.

[41] Hensel ukazuje, že bází tělesa $\mathbb{Q}(\alpha)$ je například systém $(1, \alpha, \ldots, \alpha^{\lambda-1})$ nebo $(1, \beta, \ldots, \beta^{\lambda-1})$, kde β je tzv. *primitivní číslo* tělesa $\mathbb{Q}(\alpha)$, tj. číslo tělesa $\mathbb{Q}(\alpha)$, pro které jsou všechna s ním konjugovaná čísla $\beta_1, \beta_2, \ldots, \beta_\lambda$ navzájem různá. Polynom (2.23) je v tomto případě ireducibilní nad $\mathbb{Q}$. K tomu poznamenejme, že podle definice 13 je diskriminant $d(\beta) = d(1, \beta, \ldots, \beta^{\lambda-1})$ druhou mocninou tzv. *Vandermondeova determinantu*,

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \beta_1 & \beta_2 & \ldots & \beta_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ {\beta_1}^{\lambda-1} & {\beta_2}^{\lambda-1} & \ldots & {\beta_n}^{\lambda-1} \end{vmatrix}^2 = \prod_{i<k} (\beta_i - \beta_k)^2 = (-1)^{\frac{\lambda(\lambda-1)}{2}} D(g(y)) = (-1)^{\frac{\lambda(\lambda-1)}{2}} R(g(y), g'(y)),$$

a od *diskriminantu polynomu $g(y)$* definovaného v pozn. 34 se tedy liší nejvýše znaménkem.

[42] Uvědomme si, že každé nadtěleso K tělesa $\mathbb{Q}$ (hovoří se též o *rozšíření* $K/\mathbb{Q}$) je vektorovým prostorem nad $\mathbb{Q}$; vztah (2.25) je tedy obvykle součástí *definice* báze, z níž se pak pro algebraické rozšíření odvodí platnost vztahu (2.24).

Definice 14. *Fundamentálním systémem* (*Fundamentalsystem*) *tělesa* $\mathbb{Q}(\alpha)$ se nazývá každá jeho báze $(\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(\lambda)})$, $\gamma^{(i)} \in \mathfrak{D}$, pomocí které lze všechna celá algebraická čísla tělesa $\mathbb{Q}(\alpha)$, tj. všechna čísla $\delta \in \mathfrak{D}$, vyjádřit ve tvaru

$$\delta = u_1\gamma^{(1)} + u_2\gamma^{(2)} + \cdots + u_\lambda\gamma^{(\lambda)}, \quad u_i \in \mathbb{Z}. \tag{2.26}$$

Věta 15. Systém celých algebraických čísel $(\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(\lambda)})$ je fundamentální, právě když jeho diskriminant má nejmenší možnou nenulovou absolutní hodnotu.[43]

V dalším bude p libovolné, pevně zvolené prvočíslo. Nejprve uvedeme zobecnění pojmů definovaných výše pro racionální čísla.

Definice 15 (Dělitelnost algebraických čísel v oboru p). Algebraické číslo β se nazývá *celé v oboru* p, je-li kořenem alespoň jednoho polynomu tvaru (2.21), kde všechny koeficienty $B_i \in \mathbb{Q}$ jsou celé v oboru p; β se nazývá *absolutně celé*, jsou-li všechny koeficienty $B_i \in \mathbb{Z}$. Algebraické číslo α je *v oboru* p *dělitelné* algebraickým číslem β, je-li podíl $\gamma = \alpha/\beta$ celé algebraické číslo v oboru p; α, β se nazývají *kongruentní modulo* p^δ, je-li rozdíl $\alpha - \beta$ dělitelný číslem p^δ (v obyčejném smyslu).

Definice 16. Uvažujme libovolné těleso $\mathbb{Q}(\alpha)$; souhrn všech čísel tohoto tělesa, která jsou celá v oboru p, označme symbolem $\mathfrak{D}_{(p)}$.[44] *Fundamentálním systémem v oboru* p *tělesa* $\mathbb{Q}(\alpha)$ se nazývá báze $(\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(\lambda)})$, $\gamma^{(i)} \in \mathfrak{D}_{(p)}$, pomocí níž lze každé algebraické číslo $\delta \in \mathfrak{D}_{(p)}$ vyjádřit ve tvaru (2.26).

Věta 16. Každý systém $(\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(\lambda)})$, $\gamma^{(i)} \in \mathfrak{D}_{(p)}$, jehož diskriminant není dělitelný prvočíslem p, je fundamentálním systémem v oboru p. Každý fundamentální systém (absolutní) je fundamentálním systémem v oboru libovolného prvočísla p.

Dále bude α pevně dané algebraické číslo stupně λ, $(\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(\lambda)})$ fundamentální systém v oboru p příslušného algebraického tělesa $\mathbb{Q}(\alpha)$.

Definice 17. *Modulo* p *redukovaným celým číslem tělesa* $\mathbb{Q}(\alpha)$ se nazývá celé číslo

$$e_1\gamma^{(1)} + e_2\gamma^{(2)} + \cdots + e_\lambda\gamma^{(\lambda)}, \ e_i \in \{0, 1, \ldots, p-1\}. \tag{2.27}$$

Věta 17. Pro každé algebraické číslo $\beta \in \mathbb{Q}(\alpha)$ a každé celé číslo $\nu \in \mathbb{Z}$ je splněna kongruence

$$\beta \equiv \varepsilon^{(r)}p^r + \varepsilon^{(r+1)}p^{r+1} + \cdots + \varepsilon^{(\nu)}p^\nu \pmod{p^{\nu+1}}, \tag{2.28}$$

kde $\varepsilon^{(i)}$ jsou jednoznačně určená modulo p redukovaná čísla z $\mathbb{Q}(\alpha)$; zřejmě $r \geq 0$, právě když $\beta \in \mathfrak{D}_{(p)}$.[45]

[43] Na základě této věty se v literatuře říká fundamentálnímu systému také *minimální báze*.

[44] Hensel nepoužíval žádný zvláštní symbol, jen slovní vyjádření.

[45] K důkazu této věty si stačí uvědomit, že každé algebraické číslo $\beta \in \mathbb{Q}(\alpha)$ lze vyjádřit pomocí fundamentálního systému ve tvaru (2.26), kde koeficienty jsou však nyní racionální čísla. Každý z těchto racionálních koeficientů pak lze vyjádřit periodickým p-adickým rozvojem

$$u_i = e_i{}^{(r)}p^r + e_i{}^{(r+1)}p^{r+1} + \cdots \ (p); \quad i = 1, 2, \ldots, \lambda, \ e_i{}^{(j)} = 0, 1, \ldots, p-1.$$

Okruh, resp. těleso p-adických algebraických čísel $\mathbf{Q}_p(\alpha)$

Předchozí věta a její důkaz vedou k rozšíření tělesa algebraických čísel $\mathbb{Q}(\alpha)$ na okruh tzv. *p-adických algebraických čísel* $\mathbb{Q}_p(\alpha)$.[46] Je proveden stejný obrat jako při přechodu od tělesa racionálních čísel $\mathbb{Q}$, jehož prvky lze vyjádřit pomocí periodických rozvojů $e_r p^r + e_{r+1}p^{r+1} + \cdots$ s modulo p redukovanými racionálními koeficienty, k tělesu p-adických čísel $\mathbb{Q}_p$ jako systému všech, tedy i neperiodických rozvojů.

Definice 18 (Okruh p-adických algebraických čísel $\mathbb{Q}_p(\alpha)$). *Souhrnem p-adických algebraických čísel tělesa* $\mathbb{Q}(\alpha)$ se rozumí množina všech veličin tvaru

$$\varepsilon^{(r)}p^r + \varepsilon^{(r+1)}p^{r+1} + \cdots \,, \tag{2.29}$$

kde $\varepsilon^{(i)}$ jsou libovolná modulo p redukovaná čísla z tělesa $\mathbb{Q}(\alpha)$.[47]

Zcela analogicky jako při budování tělesa $\mathbb{Q}_p$ jsou pro p-adická algebraická čísla definovány pojmy *k-té aproximace, kongruence, rovnosti, součtu* a *součinu* (pomocí aproximací); p-adické algebraické číslo se nazývá *celé,* je-li v rozvoji (2.29) $r \geq 0$, v opačném případě se nazývá *lomené.*

Každé p-adické algebraické číslo $\beta \in \mathbb{Q}_p(\alpha)$ lze dále vyjádřit pomocí fundamentálního systému $(\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(\lambda)})$ tělesa $\mathbb{Q}(\alpha)$:

$$\beta = v_1\gamma^{(1)} + v_2\gamma^{(2)} + \cdots + v_\lambda\gamma^{(\lambda)}, \quad v_i \in \mathbb{Q}_p\,. \tag{2.30}$$

Zřejmě je β celé, právě když jsou všechny koeficienty v_i celá p-adická čísla. Vzhledem k tomu, že algebraická čísla $\gamma^{(i)}$ jsou racionálními funkcemi čísla α, lze také každé $\beta \in \mathbb{Q}_p(\alpha)$ vyjádřit ve tvaru

$$\beta = \varphi(\alpha) \quad (p), \tag{2.31}$$

kde φ je racionální funkce s koeficienty v $\mathbb{Q}_p$. Naopak je každá racionální funkce (2.31) p-adickým algebraickým číslem ve smyslu definice 18.

Předpoklad 1. Pro další úvahy je učiněn předpoklad, že polynom (2.22) pro α je ireducibilní nejen nad $\mathbb{Q}$, ale i nad $\mathbb{Q}_p$.

Za tohoto předpokladu Hensel dokazuje, že $\mathbb{Q}_p(\alpha)$ je tělesem, v němž navíc platí obdoba věty 13 (těleso $\mathbb{Q}$ se pouze nahradí tělesem $\mathbb{Q}_p$). Rovněž dokazuje, že koeficienty b_i v polynomu (2.23) pro β jsou celá p-adická čísla, neboli β je *algebraicky celé*, právě když koeficienty v_i ve vyjádření (2.30) jsou celá p-adická čísla.

Dále Hensel studuje dělitelnost v tělese $\mathbb{Q}_p(\alpha)$ založenou na výše uvedeném pojmu celého p-adického algebraického čísla (analogicky s definicí 10). Tyto

Po dosazení do (2.26) a přerovnání (přitom bychom měli pracovat s aproximacemi; Hensel však na tomto místě hovoří přímo o řadách) dostaneme periodický rozvoj s jednoznačně určenými modulo p redukovanými algebraickými koeficienty $\beta = \varepsilon^{(r)}p^r + \varepsilon^{(r+1)}p^{r+1} + \cdots$, resp. dokazovanou kongruenci. Lze ukázat, že naopak každý takový periodický rozvoj určuje právě jedno algebraické číslo z tělesa $\mathbb{Q}(\alpha)$.

[46] Hensel používal označení $K(p, \alpha)$.

[47] Obecně je $\mathbb{Q}_p(\alpha)$ (spolu s dále zavedeným součtem a součinem) okruhem.

úvahy se přitom zjednoduší zavedením normy $N(\beta) = \beta_1\beta_2 \dots \beta_\lambda \in \mathbb{Q}_p$;[48] Hensel kromě jiného dokazuje, že $\beta \in \mathbb{Q}_p(\alpha)$ je celé, právě když jeho norma $N(\beta)$ je celé p-adické číslo.

Definice 19. *Prvočinitelem oboru* $\mathbb{Q}_p(\alpha)$ nazveme takové číslo $\pi \in \mathbb{Q}_p(\alpha)$ (a všechna s ním asociovaná), jehož norma $N(\pi) = p^f E$, kde $E \in \mathbb{Q}_p$ je p -adická jednotka, má nejnižší možný kladný *řád* f.

Věta 18. Nechť π je prvočinitel oboru $\mathbb{Q}_p(\alpha)$. Každé $\beta \in \mathbb{Q}_p(\alpha)$ lze právě jedním způsobem vyjádřit ve tvaru $\beta = \varepsilon\pi^\rho$, kde ε je jednotka v $\mathbb{Q}_p(\alpha)$, $\rho \in \mathbb{Z}$; ρ se nazývá *řádem* čísla β.

Hensel dokazuje, že výše definovaný prvočinitel má skutečně vlastnost prvočinitele (srov. pozn. 12). Rovněž ukazuje, že prvočinitele π daného oboru $\mathbb{Q}_p(\alpha)$ je vždy možné nalézt konečným počtem kroků, a to tak, že π je absolutně celé algebraické číslo tělesa $\mathbb{Q}(\alpha)$, tedy $\pi \in \mathfrak{D}$.

Divisory

V tělese $\mathbb{Q}_p(\alpha)$ existuje nekonečně mnoho prvočinitelů $\pi, \pi', \dots$, všichni jsou však asociovaní a z hlediska dělitelnosti jsou proto zcela rovnocenní. Aby se nemuselo hovořit o různých, ale asociovaných provočinitelích, je tělesu $\mathbb{Q}_p(\alpha)$ přiřazen jediný tzv. *prvodivisor* (*Primdivisor, Primteiler*) $\mathfrak{p}$ a definuje se dělitelnost mocninou prvodivisoru.[49]

Definice 20 (Dělitelnost prvodivisorem v $\mathbb{Q}_p(\alpha)$). Číslo $\beta \in \mathbb{Q}_p(\alpha)$ je *přesně dělitelné* (*genau teilbar*) mocninou $\mathfrak{p}^\rho$, jestliže řád čísla β je roven ρ. Obecněji řekneme, že β je *dělitelné* mocninou $\mathfrak{p}^{\rho_0}$, jestliže pro řád ρ čísla β platí: $\rho \geq \rho_0$.[50] Čísla β, β' se nazývají *kongruentní modulo* $\mathfrak{p}^{\rho_0}$, je-li rozdíl $\beta - \beta'$ dělitelný $\mathfrak{p}^{\rho_0}$; píše se $\beta \equiv \beta' (\mathrm{mod}\, \mathfrak{p}^{\rho_0})$.

Hensel dále definuje *normu prvodivisoru* $\mathfrak{p}$ jako mocninu p^f, pro kterou platí: $N(\pi) = p^f E$, kde E je p-adická jednotka; pro mocninu prvodivisoru Hensel klade $N(\mathfrak{p}^\rho) = (N(\mathfrak{p}))^\rho = p^{\rho f}$. Exponent f se nazývá *stupeň* (*Grad*) prvodivisoru $\mathfrak{p}$; je-li prvočíslo p přesně dělitelné $\mathfrak{p}^e$, pak se e nazývá *řád* prvodivisoru $\mathfrak{p}$.[51]

Následující úvahy se omezují na původní těleso $\mathbb{Q}(\alpha)$. Hensel dokazuje:

Věta 19. Je-li $\pi \in \mathbb{Q}(\alpha)$ prvočinitelem oboru $\mathbb{Q}_p(\alpha)$, potom jsou všechna konjugovaná čísla $\pi_1, \dots, \pi_\lambda$ v konjugovaných tělesech $\mathbb{Q}(\alpha_1), \dots, \mathbb{Q}(\alpha_\lambda)$, kde α značí libovolné z čísel α_i, prvočiniteli. Všechna mají týž řád e a týž stupeň f. Je-li řád čísla $\beta \in \mathbb{Q}(\alpha)$ roven ρ, pak týž řád mají všechna konjugovaná čísla $\beta_1, \dots, \beta_\lambda$. Tvoří-li $(\varepsilon^{(0)}, \varepsilon^{(1)}, \dots, \varepsilon^{(\sigma-1)})$ úplný systém modulo π nekongruentních celých čísel tělesa $\mathbb{Q}(\alpha)$, potom konjugovaná čísla $(\varepsilon_i{}^{(0)}, \varepsilon_i{}^{(1)}, \dots, \varepsilon_i{}^{(\sigma-1)})$ tvoří úplný systém modulo π_i nekongruentních celých čísel tělesa $\mathbb{Q}(\alpha_i)$.[52]

[48] Libovolné $\beta \in \mathbb{Q}_p(\alpha)$ je kořenem polynomu (2.23) s p-adickými koeficienty, nebo též polynomu $G(y) = B_0 y^\lambda + B_1 y^{\lambda-1} + \dots + B_\lambda \ \ (p)$, kde koeficienty B_i jsou celá p-adická čísla. Po roznásobení a porovnání odtud dostaneme vztah $N(\beta) = \beta_1\beta_2 \dots \beta_\lambda = (-1)^\lambda \cdot B_\lambda / B_0$.

[49] Dnešní čtenář si může představit prvodivisor jako třídu ekvivalence.

[50] Tj. pro libovolného prvočinitele $\pi \in \mathbb{Q}_p(\alpha)$ je β dělitelné mocninou π^{ρ_0}.

[51] Hensel dokazuje, že pro součin řádu e a stupně f prvodivisoru $\mathfrak{p}$ je $ef = \lambda$, kde λ značí stupeň tělesa $\mathbb{Q}_p(\alpha)$.

[52] V tomto smyslu se také říká, že tělesa $\mathbb{Q}(\alpha_i)$ či kořeny α_i tvoří jeden cyklus.

Je-li $e = 1$, pak $\pi_1 = \cdots = \pi_\lambda = p$, neboli p zůstává prvočinitelem ve všech konjugovaných tělesech $\mathbb{Q}(\alpha_i)$; Hensel dokazuje, že je to právě tehdy, když p není dělitelem diskriminantu těles $\mathbb{Q}(\alpha_i)$. Obecně je $p = \varepsilon_i \pi_i^e$, kde ε_i je jednotka; tento vztah se také označuje symbolem $\pi_i \sim p^{1/e}$.

Všem λ konjugovaným prvočinitelům, čili prvodivisorům všech λ konjugovaných těles Hensel nyní přiřadí týž *prvodivisor* $\mathfrak{p}$ a analogicky s definicí 20 definuje dělitelnost algebraických čísel mocninou prvodivisoru $\mathfrak{p}$.

Definice 21 (Dělitelnost prvodivisorem v $\mathbb{Q}(\alpha)$). Číslo $\beta \in \mathbb{Q}(\alpha)$ je *přesně dělitelné* mocninou $\mathfrak{p}^\rho$, jestliže každé z konjugovaných čísel $\beta_i \in \mathbb{Q}(\alpha_i)$ má řád ρ; číslo β je *dělitelné* $\mathfrak{p}^{\rho_0}$, jestliže pro řád ρ každého z konjugovaných čísel β_i platí: $\rho \geq \rho_0$. Čísla $\beta, \beta' \in \mathbb{Q}(\alpha)$ se nazývají *kongruentní modulo* $\mathfrak{p}^{\rho_0}$, je-li rozdíl $\beta - \beta'$ dělitelný $\mathfrak{p}^{\rho_0}$; čísla β, β' *jsou si rovna v oboru* $\mathfrak{p}$, píše se $\beta = \beta'$ $(\mathfrak{p})$, jsou-li kongruentní pro každou mocninu prvodivisoru $\mathfrak{p}$.

Hensel ukazuje, že libovolná konjugovaná čísla $\beta_1, \ldots, \beta_\lambda$ lze rozvinout v konjugované řady

$$\beta_i = \sum_{\nu=\rho}^{\infty} \varepsilon_i^{(\nu)} \pi_i^\nu \quad (\mathfrak{p}), \quad i = 1, 2, \ldots, \lambda, \tag{2.32}$$

kde $\pi_i \in \mathbb{Q}(\alpha_i)$ je prvočinitel, $\varepsilon_i^{(\nu)}$ jsou prvky úplného systému modulo p redukovaných, navzájem modulo $\mathfrak{p}$ nekongruentních celých čísel tělesa $\mathbb{Q}(\alpha_i)$.

Zatím se předpokládalo (str. 80), že minimální polynom $f(x)$ pro α (2.22) je ireducibilní nejen nad $\mathbb{Q}$, ale i nad $\mathbb{Q}_p$. Za tohoto předpokladu bylo vytvořeno těleso $\mathbb{Q}_p(\alpha)$ jako algebraické rozšíření tělesa $\mathbb{Q}_p$ stupně $\lambda = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Hensel ukázal, že čísla z $\mathbb{Q}_p(\alpha)$ se řídí stejnými zákony jako p-adická čísla z $\mathbb{Q}_p$, nahradí-li se prvočíslo p prvočinitelem π, nebo – což je totéž – prvodivisorem $\mathfrak{p}$. Dnes bychom řekli, že těleso $\mathbb{Q}_p(\alpha)$ je úplným uzávěrem tělesa $K = \mathbb{Q}(\alpha)$; značí se proto také jako $K_\mathfrak{p}$.[53] Podstatné je, že přechodem od K do $K_\mathfrak{p}$ se získají zcela jednoduché zákony dělitelnosti.

Hensel ukazuje, že v případě, kdy se polynom $f(x)$ rozloží v $\mathbb{Q}_p[x]$ na součin ireducibilních faktorů

$$f(x) = f_1(x) f_2(x) \ldots f_k(x) \quad (p), \quad f_i(x) \in \mathbb{Q}_p[x], \tag{2.33}$$

odpovídá každému faktoru $f_i(x)$ stupně λ_i ve smyslu věty 19 jednak cyklus λ_i těles $\mathbb{Q}_p(\alpha_j)$ konjugovaných nad $\mathbb{Q}_p$,[54] kde $[\mathbb{Q}_p(\alpha_j) : \mathbb{Q}_p] = \lambda_i$, jednak příslušný prvodivisor $\mathfrak{p}_i$ zastupující ekvivalentní prvočinitele π_j v tělesech i-tého cyklu. Prvočíslu p tak odpovídá celkem k různých prvodivisorů $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$.

Analogicky s definicí 21 se zavádí dělitelnost prvodivisorem $\mathfrak{p}_i$ – místo všech čísel konjugovaných nad $\mathbb{Q}$ se však uvažují pouze odpovídající čísla z i-tého cyklu, tedy čísla navzájem konjugovaná nad $\mathbb{Q}_p$.[55] Je-li algebraické číslo γ

[53] Lze dokázat, že konečné algebraické rozšíření úplného tělesa je úplné.

[54] I v pozdějším smyslu, že mezi nimi existuje isomorfismus zachovávající $\mathbb{Q}_p$; α_j jsou nyní jistá p-adická algebraická čísla.

[55] Jinak řečeno, pro dané algebraické číslo $\gamma \in \mathbb{Q}(\alpha)$ se uvažují jeho obrazy v isomorfismech určených přiřazeními $\alpha \mapsto \alpha_j$, kde α_j jsou kořeny polynomu $f_i(x)$.

přesně dělitelné mocninami $\mathfrak{p}_1^\rho, \mathfrak{p}_1^\sigma, \ldots, \mathfrak{p}_k^\tau$, pak se řekne, že je přesně dělitelné *součinem* $\mathfrak{p}_1^\rho \mathfrak{p}_1^\sigma \ldots \mathfrak{p}_k^\tau$, a píše se $\gamma \sim \mathfrak{p}_1^\rho \mathfrak{p}_1^\sigma \ldots \mathfrak{p}_k^\tau$.

Věta 20. Algebraické číslo $\gamma \in \mathbb{Q}(\alpha)$ je celé, právě když neobsahuje žádný prvodivisor pro žádné prvočíslo v záporné mocnině, neboli právě tehdy, když jeho rozvoj (2.32) má pro každý prvodivisor $\mathfrak{p}$ nezáporný řád ρ.[56]

Věta 21 (Fundamentalsatz). Každé algebraické číslo $\gamma \in \mathbb{Q}(\alpha)$ je dělitelné pouze konečným počtem prvodivisorů v nenulové mocnině.

Uvažujme libovolné $\gamma \in \mathbb{Q}(\alpha)$. Jsou-li $\mathfrak{p}^h, \mathfrak{r}^k, \ldots, \mathfrak{t}^m$ nenulové mocniny všech navzájem různých provodivisorů, jimiž je γ přesně dělitelné (mohou náležet různým prvočíslům nebo jen jednomu), pak se říká, že γ je přesně dělitelné součinem $\mathfrak{d} = \mathfrak{p}^h \mathfrak{r}^k \ldots \mathfrak{t}^m$, a píše se $\gamma \sim \mathfrak{d}$; součin $\mathfrak{d}$ se nazývá *algebraickým divisorem příslušným ke* γ.

Věta 22. Ke každému $\gamma \in \mathbb{Q}(\alpha)$ přísluší právě jeden algebraický divisor, který je celý (tj. neobsahuje žádný prvodivisor v záporné mocnině), resp. lomený (v opačném případě), právě když je toto číslo algebraické celé, resp. lomené.

Obecně *divisorem* Hensel rozumí jakýkoli součin mocnin prvodivisorů

$$\mathfrak{d} = \mathfrak{p}^{h'} \mathfrak{r}^{k'} \ldots \mathfrak{t}^{m'} \tag{2.34}$$

daného tělesa; pro divisor nemusí vždy existovat odpovídající algebraické číslo $\gamma \in \mathbb{Q}(\alpha)$.

Od uvedených pojmů se potom odvíjí další teorie. Její základní myšlenka tedy spočívá v tom, že se pro dané těleso $K = \mathbb{Q}(\alpha)$ „globální úvahy“ v algebraickém rozšíření $K/\mathbb{Q}$ nahradí pro každý prvodivisor $\mathfrak{p}$ „lokálními úvahami“ v rozšíření $K_\mathfrak{p}/\mathbb{Q}_p$, kde jsou aritmetické zákonitosti zcela triviální. Potom se lokální úvahy spojí vhodným způsobem dohromady do globálního závěru, tak jako například ve větě 20, kterou bychom mohli vyjádřit také takto: $\mathfrak{D} = \cap_\mathfrak{p} \mathfrak{D}_\mathfrak{p}$, kde $\mathfrak{D}_\mathfrak{p}$ značí celá čísla tělesa $K_\mathfrak{p}$ a $\mathfrak{p}$ probíhá všechny prvodivisory.

Na závěr poznamenejme, že Wolfgang Krull (1899 – 1970) zavedl v práci [Kru4] z roku 1938 pojem *lokálního okruhu* jako komutativního okruhu R s jednotkovým prvkem, který je noetherovský[57] a který má jen jeden maximální ideál. V tomto smyslu Hensel studoval první příklad lokálních okruhů – okruh $\mathfrak{D}_\mathfrak{p}$. Má-li R jistý konečný počet maximálních ideálů, nazývá se *semilokální*; tento pojem definoval C. Chevalley v práci [Che1] z roku 1943. První příklad semilokálních okruhů studoval již E. I. Zolotarev – okruh $\mathfrak{D}_{(p)}$.

[56] V souvislosti s touto větou Hensel připomíná analogii s teorií funkcí, kde se dokazuje věta, podle které je racionální nebo algebraická funkce jedné proměnné celá, právě když její rozvoj v okolí libovolného konečného bodu má nezáporný řád, neboli funkce nemá žádný (konečný) pól.

[57] Tj. rostoucí řetězec různých ideálů v R je nutně konečný; to je ekvivalentní s tím, že každý ideál v R je konečně generovaný.

2.1.2 *g*-adická čísla

Dvě z Rychlíkových prací jsou věnovány vlastnímu pojmu g-adických čísel zavedenému Kurtem Henselem na sklonku devatenáctého století (viz 2.1.1). Další dvojice článků zařazená do této části se zabývá spojitými nediferencovatelnými funkcemi v tělesech p-adických čísel, kde p je prvočíslo, a obecněji i v jejich algebraických rozšířeních konečného stupně a v okruzích g-adických čísel pro složené číslo g.

Poznámka k Henselově theorii algebraických čísel **[R11] (1914)**

Článek je příspěvkem ve sborníku z *V. sjezdu českých přírodozpytcův a lékařů*, který se konal v Praze roku 1914; Rychlík na sjezdu přednesl stejnojmenný referát. Cílem práce je zobecnění aditivního normálního tvaru (2.11), který pro g-adická čísla uvažoval Kurt Hensel, na tělesa čísel algebraických. Rychlík zmiňuje Henselovu práci [Hen13] otištěnou téhož roku, kde je toto zobecnění provedeno pro kvadratická tělesa. Rychlíkův článek je velice stručný, jedná se spíše o výtah z přednášky než o úplný výklad.

Rychlík uvažuje těleso algebraických čísel $\mathbb{Q}(\alpha)$ stupně n nad $\mathbb{Q}$,[58] tj. α je kořenem ireducibilního polynomu tvaru (2.22), kde $\lambda = n$. Na základě podobných úvah, jakých použil Hensel v případě prvočíselného modulu $g = p$ v práci [Hen8], Rychlík dospívá k definici *okruhu g-adických algebraických čísel tělesa* $\mathbb{Q}(\alpha)$, který zde budeme značit symbolem $\mathbb{Q}_g(\alpha)$,[59] jako souhrnu všech veličin tvaru

$$\varepsilon^{(r)} g^r + \varepsilon^{(r+1)} g^{r+1} + \cdots, \tag{2.35}$$

kde $\varepsilon^{(i)}$ jsou čísla z tělesa $\mathbb{Q}(\alpha)$ redukovaná modulo g, tedy čísla tvaru (2.27), kde $e_i \in \{0, 1, \ldots, g-1\}$. Rozšíření z $\mathbb{Q}(\alpha)$ na $\mathbb{Q}_g(\alpha)$ opět umožňuje kongruence (2.28), kde se místo p položí g. Rychlík poznamenává, že $\mathbb{Q}_g(\alpha)$ je tělesem, je-li $g = p$ prvočíslo a polynom (2.22) je ireducibilní nad $\mathbb{Q}_p$.

Pro okruhy g-adických algebraických čísel dále platí obdoba vztahu (2.10):

$$\mathbb{Q}_{p^k q^l \ldots r^m}(\alpha) = \mathbb{Q}_{pq\ldots r}(\alpha). \tag{2.36}$$

Rychlík připomíná, že každé g-adické algebraické číslo $\beta \in \mathbb{Q}_g(\alpha)$ lze vyjádřit pomocí báze $(1, \alpha, \ldots, \alpha^{n-1})$ tělesa $\mathbb{Q}(\alpha)$ ve tvaru

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_{n-1}\alpha^{n-1}, \quad b_i \in \mathbb{Q}_g. \tag{2.37}$$

Vyjádří-li se koeficienty b_i v aditivním normálním tvaru (2.11), pak

$$\beta = \beta_p + \beta_q + \cdots + \beta_r \quad (g), \tag{2.38}$$

[58] Rychlík je značil stejně jako Hensel symbolem $K(\alpha)$.
[59] Rychlík psal $R(g, \alpha)$ analogicky s Henselovým označením $K(p, \alpha)$.

kde $\beta_p \in \mathbb{Q}_p,\ \beta_q \in \mathbb{Q}_q,\ \ldots,\ \beta_r \in \mathbb{Q}_r$, a platí:

$$\begin{array}{llll} \beta_p = \beta\ (p), & \beta_p = 0\ (q), & \ldots, & \beta_p = 0\ (r), \\ \beta_q = 0\ (p), & \beta_q = \beta\ (q), & \ldots, & \beta_q = 0\ (r), \\ \multicolumn{4}{c}{\dotfill} \\ \beta_r = 0\ (p), & \beta_r = 0\ (q), & \ldots, & \beta_r = \beta\ (r), \end{array}$$

Dnešními slovy, okruh $\mathbb{Q}_g(\alpha)$ je direktním součtem okruhů $\mathbb{Q}_p(\alpha), \ldots, \mathbb{Q}_r(\alpha)$:

$$\mathbb{Q}_g(\alpha) = \mathbb{Q}_p(\alpha) \oplus \mathbb{Q}_q(\alpha) \oplus \cdots \oplus \mathbb{Q}_r(\alpha).$$

Nechť se dále minimální polynom pro α rozloží v okruhu $\mathbb{Q}_p[x]$ na součin (2.33), každému faktoru $f_i(x)$ nechť je přiřazen prvodivisor $\mathfrak{p}_i$.[60] Je-li $\alpha^{(j)}$ jeden z kořenů polynomu $f_i(x)$ a $\beta = \varphi(\alpha)$, pak se $\varphi(\alpha^{(j)})$ nazývá *hodnotou čísla* β *v oboru divisoru* $\mathfrak{p}_j$ a značí se symbolem $\beta_{\mathfrak{p}_j}$. Číslo β pak lze vyjádřit v aditivním normálním tvaru

$$\beta = \beta_{\mathfrak{p}_1} + \beta_{\mathfrak{p}_2} + \cdots + \beta_{\mathfrak{p}_k} \quad (p), \tag{2.39}$$

kde

$$\begin{array}{llll} \beta_{\mathfrak{p}_1} = \beta\ (\mathfrak{p}_1), & \beta_{\mathfrak{p}_1} = 0\ (\mathfrak{p}_2), & \ldots, & \beta_{\mathfrak{p}_1} = 0\ (\mathfrak{p}_k), \\ \beta_{\mathfrak{p}_2} = 0\ (\mathfrak{p}_1), & \beta_{\mathfrak{p}_2} = \beta\ (\mathfrak{p}_2), & \ldots, & \beta_{\mathfrak{p}_2} = 0\ (\mathfrak{p}_k), \\ \multicolumn{4}{c}{\dotfill} \\ \beta_{\mathfrak{p}_k} = 0\ (\mathfrak{p}_1), & \beta_{\mathfrak{p}_k} = 0\ (\mathfrak{p}_2), & \ldots, & \beta_{\mathfrak{p}_k} = \beta\ (\mathfrak{p}_k). \end{array}$$

Jinak řečeno, okruh $\mathbb{Q}_p(\alpha)$ je direktním součtem těles $\mathbb{Q}_{\mathfrak{p}_i}(\alpha)$:

$$\mathbb{Q}_p(\alpha) = \mathbb{Q}_{\mathfrak{p}_1}(\alpha) \oplus \mathbb{Q}_{\mathfrak{p}_2}(\alpha) \oplus \cdots \oplus \mathbb{Q}_{\mathfrak{p}_k}(\alpha).$$

O Henselových číslech **[R12] (1916)**

Práce je věnována zavedení a vlastnostem okruhu g-adických čísel $\mathbb{Q}_g$. Rychlík cituje Henselovy knihy [Hen8] a [Hen12] a Steinitzovu práci [Ste1]. Zatímco Hensel se vydal po cestě analogické budování tělesa reálných čísel pomocí dekadických rozvojů, jejíž exaktní vyjádření je poměrně pracné, Rychlík vyšel podobně jako Cantor z pojmu fundamentální posloupnosti a limity. Předností tohoto postupu je například to, že přímo z definice je vidět, že okruh g-adických čísel závisí pouze na prvočinitelích obsažených v g, nikoli na jejich mocninách (srov. (2.10)).

Jak uvidíme v úvodu části 2.1.3, myšlenka vybudování *tělesa* p-adických čísel pro prvočíslo p pomocí fundamentálních posloupností pochází od Józsefa Kürsch//áka, který zavedl pojem *ohodnocení*. Rychlík však zobecňuje pojem limity trochu jiným způsobem, bližším Henselovi; navíc se podrobně věnuje

[60] Rychlík psal y_i místo zde užitého $\mathfrak{p}_i$. Jinak však používal stejné značení jako Hensel; v případě divisorů se mohlo jednat o problém se sazbou některých symbolů ve sborníku. Na tomto místě bychom také měli poznamenat, že Rychlíkův článek obsahuje několik tiskových chyb, které však čtenář podle souvislostí snadno opraví.

okruhu g-adických čísel pro složené číslo g. Příslušné Kürschákovo pojednání [Kür2] z roku 1913 cituje až v doslovu ke svému článku. Je tedy možné, že na myšlenku zobecnění Cantorovy teorie pro vybudování okruhu g-adických čísel přišel nezávisle na Kürschákovi.[61]

Zdržme se nejprve u tohoto doslovu. Rychlík v něm zobecňuje Kürschákův postup pro případ složeného čísla g. Libovolný okruh R „ohodnocuje“ pomocí zobrazení $\|\cdot\|$ okruhu R do množiny nezáporných reálných čísel, které splňuje následující podmínky:

$$\forall a \in R,\ a \neq 0: \quad \|a\| > 0; \quad \|0\| = 0, \tag{PO1}$$

$$\forall a \in R: \quad \|1 + a\| \leq 1 + \|a\|, \tag{PO2}$$

$$\forall a, b \in R: \quad \|a \cdot b\| \leq \|a\| \cdot \|b\|, \tag{PO3}$$

$$\exists a \in R: \quad \|a\| \neq 0, 1. \tag{PO4}$$

Toto zobrazení se později začalo nazývat *pseudo-ohodnocením* (*Pseudobewertung*). Je zajímavé, avšak prakticky neznámé, že Rychlík tento pojem definoval – i když nepoužil uvedený název – o dvacet let dříve, než vyšel Mahlerův článek [Mah1], který je obvykle považován za práci, kde bylo pseudo-ohodnocení poprvé zavedeno.[62]

Rychlík poznamenává, použijeme-li dnešní terminologii, že je-li v daném okruhu definováno pseudo-ohodnocení, je možné zavést pojem limity a fundamentální posloupnosti a okruh rozšířit na jeho úplný uzávěr. Speciálně okruh g-adických čísel je úplným uzávěrem tělesa racionálních čísel, položí-li se $R = \mathbb{Q}$, $\|a\| = e^{-\rho}$, kde a je libovolné nenulové racionální číslo zapsané ve tvaru $a = g^{\rho}\bar{a}$, $\bar{a}$ je číslo celé v oboru g nedělitelné g.

Vraťme se nyní k vlastnímu článku. Rychlík nejprve definuje pojmy celé číslo, relace dělitelnosti, jednotka, asociovanost (ozn. $a \sim b\ (g)$)[63] a kongruence v oboru g, a to stejným způsobem jako Hensel v práci [Hen12]. Navíc zde zavádí relaci *uspořádání*: $a < b\ (g)$, právě když a je dělitelné b, ale není s ním asociované.[64] Rychlík studuje vlastnosti výše uvedených pojmů, potom se obrací k posloupnostem racionálních čísel $a_1, a_2, \ldots, a_n, \ldots$. Definuje pojmy *limita posloupnosti v oboru g* a *fundamentální posloupnost v oboru g*:

Definice 22 (Limita posloupnosti v oboru g). *Posloupnost ta má v oboru g za limitu číslo racionálné a,*

$$\lim_{n=\infty} a_n = a\ (g),$$

[61] V roce 1909 Rychlík přednášel v Jednotě na téma *O algebraických číslech podle Hensela*, což svědčí o tom, že přinejmenším tehdy se Henselovou teorií již zabýval – řádné zavedení ústředního pojmu je pak prvořadým problémem. Připomeňme také téma *Analogie theorie algebraických čísel a algebraických funkcí o jedné proměnné*, které Rychlík nabídl k přednášce na zkoušku ve své žádosti o habilitaci podané roku 1910 (viz str. 30).

[62] Na konci svého dalšího článku [Mah2] Mahler sám poznamenává, že se pseudo-ohodnocení objevilo již v Deuringově práci [Deu1] z roku 1935 (pro hyperkomplexní systémy), což však zjistil až poté, co předchozí článek [Mah1] vyšel.

[63] Rychlík používal stejně jako Hensel výraz *ekvivalence*.

[64] Uvědomme si, že vztah $a < b\ (g)$ odpovídá inkluzi $\mathbb{Z}_{(g)}\, a \subset \mathbb{Z}_{(g)}\, b$, kde symbol $\mathbb{Z}_{(g)}$ značí množinu čísel celých v oboru g.

je-li možno ke každému racionálnému číslu d nalézti celé číslo kladné N, takové, že pro každé $n \geq N$ bude $a_n - a < d$ (g).[65]

Definice 23 (Posloupnost fundamentální v oboru g). *Posloupnost $a_1, a_2, \ldots, a_n, \ldots$ splňující podmínku, že pro každé racionálné číslo d lze nalézti takové celé číslo kladné N, že pro $n \geq N$ a libovolné kladné k bude $a_{n+k} - a_n < d$, nazveme* fundamentální *v oboru g.*[66]

Rychlík dokazuje řadu vět analogických s obvyklými větami o posloupnostech v reálném oboru. Dále ukazuje, že každá posloupnost, která má v oboru g za limitu racionální číslo, je také fundamentální v oboru g, ale ne naopak. V tomto okamžiku už Rychlík může definovat g-adická čísla:

Definice 24. *Ke každé posloupnosti racionálných čísel* fundamentální *v oboru g, která nemá za limitu číslo racionálné, přiřadíme nové číslo a to nazveme její limitou. Limity posloupností konvergentních v oboru g nazveme pak čísly g-adickými. Jsou tedy v oboru čísel g-adických zahrnuta čísla racionálná ...*

Nepřiřadíme však ke každé posloupnosti fundamentální *v oboru g jinou limitu, nýbrž dvěma posloupnostem konvergentním v oboru g,*

$$a_1, a_2, \ldots a_n, \ldots, \quad b_1, b_2, \ldots b_n \ldots,$$

přiřadíme rovná čísla g-adická jako limitu

$$A = B \ (g), \quad A = \lim_{n=\infty} a_n \ (g), \ B = \lim_{n=\infty} b_n \ (g),$$

je-li

$$\lim_{n=\infty} (a_n - b_n) = 0 \ (g).$$

Tak definována rovnost čísel g-adických; a to je přípustno, poněvadž vztah uvedený je reflexivní, symmetrický, transitivní.[67]

Početní operace se definují zcela přirozeným způsobem: pro $A = \lim a_n \ (g)$, $B = \lim b_n \ (g)$ se položí $A \pm B = \lim (a_n \pm b_n) \ (g)$, $AB = \lim (a_n b_n) \ (g)$; korektnost je rovněž dokázána.

Snadno se ukáže, že množina g-adických čísel $\mathbb{Q}_g$ vybavená uvedenými operacemi tvoří okruh. Je-li $g = p$ (nebo, což je totéž, $g = p^k$), kde p je prvočíslo, pak je $\mathbb{Q}_g$ tělesem. Poslední tvrzení vůbec není triviální. Rychlík dokazuje, že v takovém případě je každé nenulové g-adické číslo *pravidelné*, tj. členy posloupnosti, která jej určuje, jsou od jistého indexu asociované s týmž racionálním číslem. Přitom pro pravidelné g-adické číslo $A = \lim a_n \ (g)$ je posloupnost $1/a_1, 1/a_2, \ldots, 1/a_n, \ldots$ fundamentální a má za limitu opět pravidelné g-adické číslo, které se označí jako $1/A$ a které je inverzním prvkem k A.

---

[65] [R12], str. 3; např. $\lim g^n = 0 \ (g)$.

[66] [R12], str. 5; Rychlík psal *konvergentní* – to se však dnes používá v jiném významu, proto se budeme držet označení *fundamentální.*

Rychlík ukázal, že v oboru g stačí ke konvergenci splnění uvedené podmínky pro $k = 1$: $a_{n+k} - a_n = (a_{n+k} - a_{n+k-1}) + (a_{n+k-1} - a_{n+k}) + \ldots + (a_{n+1} - a_n)$; pokud d dělí každý se sčítanců vpravo, dělí i rozdíl $a_{n+k} - a_n$, tedy $a_{n+k} - a_n < d \ (g)$.

[67] [R12], str. 5–6; povšimněme si, že citovaný text odpovídá definici pomocí tříd ekvivalence.

Je-li však g dělitelné alespoň dvěma různými prvočiniteli, existují v $\mathbb{Q}_g$ netriviální dělitelé nuly a g-adická čísla tvoří pouze okruh. Je-li nyní P dělitelem čísla g, můžeme definovat *P-adickou hodnotu g-adického čísla* $A = \lim a_n\ (g)$ jako limitu $A_p = \lim a_n\ (P)$.

Další Rychlíkovy úvahy směřují k rozkladu okruhu g-adických čísel na tělesa čísel p-adických, q-adických, ..., r-adických ve smyslu dnešního direktního součtu (2.12). Je dokázána věta o jednoznačném vyjádření g-adického čísla v aditivním normálním tvaru (2.11). Následuje věta o úplnosti okruhu g-adických čísel:

Věta 23. *Každá posloupnost čísel g-adických,* fundamentální *v oboru g, má v oboru čísel g-adických limitu.*[68]

Nakonec Rychlík uvažuje nekonečné řady v okruhu $\mathbb{Q}_g$. Nutnou i postačující podmínkou konvergence je, že členy řady mají v oboru g nulovou limitu. Proto jsou řady tvaru (2.8), pomocí nichž definoval g-adická čísla Hensel, konvergentní v oboru g. Rychlík pak dokazuje, že každé g-adické číslo lze znázornit právě jedním způsobem redukovaným g-adickým rozvojem (viz (2.9)).

Konečně Rychlík ukazuje, že opravdu existují g-adická čísla, která nejsou racionální. Jejich existence plyne buď z tvrzení, že racionálním číslům přísluší periodické rozvoje, anebo z úvah o mohutnostech; racionální čísla tvoří spočetnou množinu, zatímco množina čísel g-adických má mohutnost kontinua. Můžeme totiž vytvořit vzájemně jednoznačné zobrazení, v němž g-adickému číslu

$$a_\rho g^\rho + a_{\rho+1} g^{\rho+1} + \cdots$$

odpovídá reálné číslo

$$a_\rho g^{-\rho} + a_{\rho+1} g^{-\rho-1} + \cdots .$$

Spojité nediferencovatelné funkce v $\mathbf{Q}_p$ [R17], 1920; [R21], 1922

O dvojici Rychlíkových článků ***Funkce spojité nemající derivace pro žádnou hodnotu proměnné v tělese čísel Henselových*** [R17] a ***Eine stetige nicht differenzierbare Funktion im Gebiete der Henselschen Zahlen*** [R21], které svým obsahem spadají spíše do matematické analýzy, je pojednáno v části 3.2.3 (str. 140). Zde jen poznamenejme, že se jedná o jedny z prvních publikovaných prací studujících p-adické spojité funkce. Jistou elementární p-adickou analýzu lze nalézt již v Henselově knize *Zahlentheorie* [Hen12], více však byla rozvíjena až později; viz např. články L. G. Šnirelmana [Sni1] z roku 1938, J. Dieudonného [Die1] z roku 1944 či J. de Groota [Gro1] z roku 1956.[69]

[68] [R12], str. 12.

[69] Podrobnější bibliografie je uvedena v článku W. Więsława [Wie1].

2.1.3 Teorie ohodnocení

Pojem *ohodnocení* (*Bewertung*)[70] jako zobecnění absolutní hodnoty v $\mathbb{R}$ či $\mathbb{C}$ zavedl do teorie těles József Kürschák (1864 – 1933), a to nejprve v přednášce *Über Limesbildung und allgemeine Körpertheorie* pronesené v srpnu roku 1912 na *5. mezinárodním sjezdu matematiků* v Cambridge a otištěné o rok později jako [Kür1], detailně pak ve stejnojmenném pojednání [Kür2] z roku 1913:

Definice 25 (Ohodnocení). Zobrazení $\|\cdot\|$ tělesa K do množiny nezáporných reálných čísel se nazývá *ohodnocením*, jestliže platí:[71]

$$\forall a \in K,\ a \neq 0: \quad \|a\| > 0; \quad \|0\| = 0, \tag{O1}$$

$$\forall a \in K: \quad \|1 + a\| \leq 1 + \|a\|, \tag{O2}$$

$$\forall a, b \in K: \quad \|a \cdot b\| = \|a\| \cdot \|b\|, \tag{O3}$$

$$\exists a \in K: \quad \|a\| \neq 0, 1. \tag{O4}$$

Těleso K, na kterém je definované ohodnocení, se nazývá *ohodnocené těleso*.

Jako speciální případ Kürschák uvažuje p-adická ohodnocení definovaná na $\mathbb{Q}$ následujícím způsobem. Nechť p je prvočíslo; každé $a \in \mathbb{Q}$, $a \neq 0$, lze vyjádřit ve tvaru $a = p^\alpha u/v$, kde $u, v, \alpha \in \mathbb{Z}$, čísla u, v jsou nesoudělná s p. Položíme-li

$$\|a\| = \mathrm{e}^{-\alpha} \ \text{ pro } \ a \neq 0, \quad \|0\| = 0, \tag{2.40}$$

pak je toto zobrazení ohodnocením. Místo podmínky (O2) lze dokázat silnější tvrzení: pro libovolná $a, b \in \mathbb{Q}$ platí tzv. *ultrametrická nerovnost*[72]

$$\|a + b\| \leq \max(\|a\|, \|b\|). \tag{O2'}$$

Ohodnocení, kde místo (O2) platí (O2'), se brzy začalo nazývat *nearchimedovské*;[73] jinak se nazývá *archimedovské* (např. „obyčejná“ absolutní hodnota v $\mathbb{R}$). K terminologii ještě poznamenejme, že pro archimedovské ohodnocení vždy existuje alespoň jedno přirozené číslo n_0, pro které je $\|n_0\| > 1$; odtud se pak odvodí, že pro libovolné prvky $a, b \in K,\ a \neq 0$, existuje takové $n \in \mathbb{N}$, že $\|na\| > \|b\|$,[74] což odpovídá *Archimédovu* či *Eudoxovu–Archimédovu axiomu*.[75] Pro nearchimedovské ohodnocení je naopak $\|n\| \leq 1$ pro všechna $n \in \mathbb{N}$ a následně $\|na\| = \|n\| \cdot \|a\| \leq \|a\|$.

[70] V angličtině se používá ekvivalent *valuation*. Dnes se zobrazení z definice 25 obvykle nazývá *absolutní hodnotou* (*absolute value*) a termín *ohodnocení* se ponechává pro označení exponenciálního či obecněji Krullova ohodnocení – viz str. 90.

[71] Podmínkou (O4) se vyloučí triviální případ, kdy $\|a\| = 1$ pro všechna $a \in K,\ a \neq 0$.

[72] V pozdější terminologii.

[73] V Kürschákově práci se tento výraz ještě neobjevuje, brzy se však stal obvyklým (alespoň od Ostrowského článku [Ost2] z roku 1918).

[74] Použili jsme obvyklý zápis, kde na značí pro $n \in \mathbb{N}$, $a \in K$ součet $a + a + \cdots + a$ o n sčítancích. Speciálně n_0 značí $n_0 \cdot 1$, kde 1 je jednotkový prvek tělesa K.

[75] *Pravíme, že k sobě mají poměr veličiny, které násobeny jsouce mohou býti jedna druhé větší.* Viz Eukleides, *Základy*, JČM, Praha, 1907 (přeložil František Servít); citát str. 69.

Uvědomme si, že jakmile máme k dispozici „velikost“ prvků tělesa K, můžeme měřit i jejich „vzdálenosti“, neboli zavést *metriku* na K danou vztahem $\rho(a,b) = \|a-b\|$.[76] Metrika pak umožňuje definici otevřených a uzavřených množin a tedy studium *topologie* v K.[77]

K definici pojmu ohodnocení dodejme, že Alexander Ostrowski uvažoval pro nearchimedovská ohodnocení *řád* prvku $a \in K$ jako reálné číslo[78]

$$v(a) = -\ln\|a\|, \quad \text{tj.} \quad \|a\| = e^{-v(a)}, \tag{2.42}$$

a odvodil jeho vlastnosti, které odpovídají pozdějšímu pojmu *exponenciálního ohodnocení*. To se obvykle definuje jako zobrazení $v : K \to \mathbb{R} \cup \{\infty\}$ splňující následující podmínky:

$$\forall a \in K,\ a \neq 0: \quad v(a) < \infty; \quad v(0) = \infty, \tag{EO1}$$

$$\forall a, b \in K: \quad v(a+b) \geq \min\left(v(a), v(b)\right), \tag{EO2}$$

$$\forall a, b \in K: \quad v(ab) = v(a) + v(b), \tag{EO3}$$

$$\exists a \in K: \quad v(a) \neq 0, \infty. \tag{EO4}$$

Vztahem (2.42) je zřejmě dána vzájemně jednoznačná korespondence mezi uvedeným exponenciálním ohodnocením a nearchimedovským ohodnocením v Kürschákově smyslu. Wolfgang Krull pak v práci [Kru2] pojem ohodnocení zobecnil tím, že uvažoval surjektivní zobrazení $v : K \to G \cup \{\infty\}$, kde G je libovolná úplně uspořádaná aditivní Abelova grupa[79] a zobrazení v splňuje podmínky (EO1) – (EO4) pro exponenciální ohodnocení.

Vraťme se nyní ke Kürschákovu článku [Kür2] a k ohodnocení ve smyslu původní definice 25. Cílem Kürschákova pojednání je důkaz následující věty:

Věta 24 (Základní věta teorie ohodnocení). Každé ohodnocené těleso K lze rozšířit na úplné[80] algebraicky uzavřené těleso s ohodnocením, které je rozšířením ohodnocení v K.

[76] Takto určené zobrazení $\rho : K \times K \to \mathbb{R},\ K \neq \emptyset$ splňuje následující podmínky:
1) $\forall a, b \in K:\ \rho(a,b) \geq 0;\ \rho(a,b) = 0 \Leftrightarrow a = b$, 2) $\forall a, b \in K:\ \rho(a,b) = \rho(b,a)$,
3) $\forall a, b, c \in K:\ \rho(a,b) \leq \rho(a,c) + \rho(c,b)$.
Dvojice (K, ρ) tedy představuje *metrický prostor*. V tomto smyslu definoval *metriku* (*écart*) M. Fréchet v práci [Fre1] z roku 1906, kterou Kürschák ve svém článku cituje.
Platí-li pro ohodnocení ultrametrická nerovnost (O2'), pak je $\rho(a,b) \leq \max(\rho(a,c), \rho(c,b))$; dvojice (K, ρ) se v takovém případě nazývá *ultrametrický prostor*.

[77] Poznamenejme, že ultrametrické prostory mají některé zajímavé vlastnosti; například všechny trojúhelníky jsou rovnostranné, každý bod b ležící v okolí bodu a o poloměru r, tj. $b \in U(a,r) = \{c \in K; \rho(c,a) < r\}$, je středem tohoto okolí, množina $U(a,r)$ je zároveň otevřená i uzavřená, každá dvě okolí $U(a,r)$, $U(b,s)$ jsou buď disjunktní, anebo je jedno obsaženo ve druhém atd. Ve snadno přístupné formě jsou topologické vlastnosti ultrametrických prostorů popsány v knize [Gou1], str. 31–36.

[78] V této podobě je definice obsažena v práci [Ost4], bez znaménka minus již v [Ost2].

[79] O úplném uspořádání $\leq$ se předpokládá, že je kompatibilní se sčítáním prvků grupy G, tj. pro libovolné $\gamma, \gamma', \delta \in G$ platí implikace: $\gamma < \gamma' \Rightarrow \gamma + \delta \leq \gamma' + \delta$.

[80] Kürschák používal označení *perfektní* (*perfect*) ve smyslu dnešního vyjádření *úplný* (*komplett* či *vollständig*). Poznamenejme, že v tomto významu se slovo *perfect* v němčině standardně používalo až do počátku třicátých let dvacátého století (český ekvivalent *perfektní* používal také Karel Rychlík) a teprve později bylo nahrazeno výrazem *komplett* či *vollständig* ve shodě s obvyklým anglickým termínem *complete* (*úplný*), aby se zabránilo

Důkaz věty probíhá v několika krocích. Nejprve Kürschák řeší otázku zúplnění ohodnoceného tělesa. K tomu účelu zobecňuje Cantorovu konstrukci tělesa reálných čísel pomocí fundamentálních posloupností a buduje nejmenší úplné rozšíření K' daného tělesa K, tzv. *derivované těleso tělesa* K (*derivierte Körper von* K), v dnešní terminologii *úplný uzávěr tělesa* K, sestávající z prvků původního tělesa K a („ideálních“) limit všech fundamentálních posloupností v K.[81] Kürschák ukazuje, že není obtížné rozšířit ohodnocení $\|\cdot\|$ daného tělesa K na jeho úplný uzávěr; ohodnocení limity posloupnosti $\{a_n\},\ a_n \in K$, se definuje jako limita posloupnosti reálných čísel $\{\|a_n\|\}$.

Speciálním případem je nyní těleso p-adických čísel $\mathbb{Q}_p$, které je úplným uzávěrem tělesa racionálních čísel $\mathbb{Q}$ opatřeného p-adickým ohodnocením (2.40).[82]

Potom se Kürschák zabývá otázkou algebraického uzávěru úplného tělesa K' získaného v prvním kroku. Zde odkazuje na Steinitzovo pojednání [Ste1], ve kterém je dokázáno, že každé těleso K' lze rozšířit na těleso L, které je algebraické nad K' a které je algebraicky uzavřené.[83] Nakonec s využitím úvah, které použil Karl Weierstrass v práci [Wei1] k novému důkazu tvrzení, že těleso komplexních čísel je algebraicky uzavřené, Kürschák dokazuje, že úplný uzávěr algebraicky uzavřeného ohodnoceného tělesa je algebraicky uzavřené těleso.

V uvedeném druhém kroku je ovšem třeba rozšířit ohodnocení úplného tělesa K' na jeho algebraické rozšíření L. Nechť α je kořen nějakého monického polynomu

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \quad a_i \in K' \quad (a_n = \pm N\alpha), \tag{2.43}$$

který je ireducibilní v $K'[x]$. Položíme-li rozumný požadavek, aby všechny kořeny polynomu (2.43) měly stejné ohodnocení, pak lze snadno ukázat, že ohodnocení prvku α musí být[84]

$$\|\alpha\| = \|a_n\|^{\frac{1}{n}}. \tag{2.44}$$

Je však třeba dokázat, že jsou splněny podmínky (O1) – (O4) z definice 25. Platnost podmínek (O1) a (O4) je zřejmá; platnost podmínky (O3) Kürschák dokázal bez dalších předpokladů rovněž poměrně snadno (i když poněkud pracně

možným nedorozuměním – v angličtině totiž *perfect field* označuje těleso, které nemá ryze inseparabilní algebraické rozšíření (německý ekvivalent tohoto pojmu je *vollkommen*); srov. [Roq1], str. 293.

[81] Posloupnost $\{a_n\}$ Kürschák nazývá *fundamentální*, jestliže pro každé $\varepsilon > 0$ existuje $N \in \mathbb{N}$ tak, že pro každé $n > N$ a pro každé $k > 0$, platí: $\|a_n - a_{n+k}\| < \varepsilon$. Limita je definována obdobně – tedy obvyklým způsobem.

[82] Kromě různých tvrzení o ohodnocení v tělese $\mathbb{Q}_p$ Kürschák dokazuje, že každé nenulové $A \in \mathbb{Q}_p$ lze vyjádřit právě jedním způsobem ve tvaru (2.14). Ohodnocení prvku A je pak dané vztahem, který je obdobou Henselovy *absolutní hodnoty v oboru* p (2.16): $\|A\| = e^{-a}$.

Jak Kürschák sám uvádí, byl inspirován Henselovou knihou *Theorie der algebraischen Zahlen* [Hen8]. Právě popsaným způsobem, který je analogický Cantorovu zavedení reálných čísel, dal Henselově teorii p-adických (algebraických) čísel pevné základy. V té době se totiž objevovaly pochybnosti o tom, zda tato čísla opravdu existují – když jsou definovány pomocí mocninných rozvojů, které v obvyklém smyslu nekonvergují.

[83] Připomeňme, že těleso L se nazývá *algebraické nad* K', jestliže každý prvek $\alpha \in L$ je kořenem nějakého polynomu $f(x) \in K'[x]$. Těleso L se nazývá *algebraicky uzavřené*, jestliže každý polynom z $L[x]$ stupně aspoň 1 lze v $L[x]$ rozložit na součin lineárních faktorů.

[84] Plyne ze vztahu $x^n + a_1 x^{n-1} + \cdots + a_n = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$, tj. $a_n = (-1)^n \alpha_1 \alpha_2 \ldots \alpha_n$, a z třetí vlastnosti ohodnocení (O3).

– viz [Kür2], str. 245–247). Důkaz, že je splněna i podmínka (O2), je výrazně obtížnější. Kürschák k němu využívá Hadamardovy výsledky z [Had1] týkající se mocninných řad v $\mathbb{C}$, které zobecňuje na libovolné úplné ohodnocené těleso K', a dokazuje, že pro ireducibilní polynom $f(x)$ tvaru (2.43) je poloměr konvergence řady

$$\frac{1}{f(x)} = c_0 x^{-1} + c_1 x^{-2} + c_2 x^{-3} + \cdots \tag{2.45}$$

roven $l = \|a_n\|^{\frac{1}{n}} = \|\alpha\|$. Protože $1 + \alpha$ je kořenem polynomu $f(x - 1)$, je trojúhelníková nerovnost $\|1+\alpha\| \leq 1+\|\alpha\|$ ekvivalentní s nerovností $l' \leq 1+l$, kde l, resp. l' je poloměr konvergence rozvoje $1/f(x)$, resp. $1/f(x-1)$.

Tato část celého důkazu je poměrně dlouhá a pracná, navíc překračuje rámec algebry. V úvodu své práce však Kürschák poznamenává, že ve všech případech, kdy platí ultrametrická nerovnost (O2'), tj. pro nearchimedovská ohodnocení, je možné zobecnit Henselovu větu 11:

Věta 25. Nechť $\|\cdot\|$ je nearchimedovské ohodnocení definované na úplném tělese K'. Je-li polynom $f(x)$ tvaru (2.43) ireducibilní a $\|a_n\| \leq 1$, pak je také $\|a_i\| \leq 1$ pro všechny koeficienty a_i, $1 \leq i \leq n-1$.

Kürschák ukazuje, že je pak snadné odvodit trojúhelníkovou nerovnost (O2) pro algebraické rozšíření.[85] Větu 25 však nedokazuje a obrací se k zobecnění Hadamardových vět, které platí pro všechna ohodnocení, tedy i archimedovská.

V roce 1918 dokázal ve svém článku [Ost2] Alexander Ostrowski, že každé těleso K s archimedovským ohodnocením $\|\cdot\|$ je isomorfní s jistým podtělesem $\overline{K}$ tělesa komplexních čísel $\mathbb{C}$ takovým způsobem, že pro každé $a \in K$ a odpovídající $\overline{a} \in \overline{K}$ je $\|a\| = |\overline{a}|^{\rho}$, kde $|\cdot|$ je „obyčejná“ absolutní hodnota na $\mathbb{C}$, $0 < \rho < 1$, ρ nezávisí na a.[86] Jinými slovy, pro archimedovská ohodnocení jsou až na isomorfismus jedinými úplnými tělesy tělesa $\mathbb{R}$ a $\mathbb{C}$, kde je problém ohodnocení triviální. Proto je možné omezit veškeré úvahy pouze na nearchimedovská ohodnocení a použít zobecněné Henselovo lemma.

A právě toto do detailů vypracoval Karel Rychlík v článcích [R14] a [R22] otištěných v letech 1919 a 1923. Tím, že dokázal základní větu teorie ohodnocení bez použití matematické analýzy, postavil tuto teorii na ryze algebraické základy.

Příspěvek k theorii těles [R14] (1919)

Na první pohled a z dnešního hlediska vypadá Rychlíkova práce věnovaná teorii ohodnocení snad až triviálně. Rychlík v podstatě sleduje příslušné výsledky podané v Henselově knize [Hen8] a převádí je z tělesa $\mathbb{Q}_p$ do libovolného nearchimedovsky ohodnoceného tělesa. Do značné míry užívá Henselových formulací vět a jeho idejí důkazů. Kdokoli si proto dnes může pomyslet, že to,

[85] Nechť α je kořen ireducibilního polynomu (2.43), $\|a_n\| \leq 1$. Číslo $1 + \alpha$ je pak kořenem polynomu $f(x-1) = x^n + b_1 x^{n-1} + \cdots + b_n$, kde $b_n = (-1)^n + a_1(-1)^{n-1} + \cdots + a_n$. Platí-li věta 25, pak je $\|b_n\| \leq 1$ a tedy $\|1+\alpha\| = \|b_n\|^{\frac{1}{n}} \leq 1$. V případě, že $\|\alpha\| > 1$, neboli $\|a_n\| > 1$, by se přechodem k převrácené hodnotě ukázalo, že $\|1+\alpha\| \leq \|\alpha\|$.

[86] Připomeňme, že ohodnocení splňující uvedenou podmínku se nazývají *ekvivalentní*.

co je náplní Rychlíkovy práce [R14], muselo napadnout každého, kdo se teorií ohodnocení zabýval.

Takový pohled by však byl poněkud zjednodušující a podceňující. Uvědomme si, že v samotných počátcích nebylo matematiků věnujících se teorii ohodnocení mnoho – k výraznějšímu rozvoji došlo až později, zejména ve třicátých letech dvacátého století. A Rychlík byl první, kdo uvedené úvahy podrobně vypracoval a publikoval. Uvědomme si také skutečnost, že abstraktní algebra byla tehdy teprve v zárodku; přenesení Henselových výsledků do obecného ohodnoceného tělesa proto nebylo tak triviální, jak se může zdát nám, kteří jsme se s ní seznámili již jako s ucelenou teorií a neodlučitelnou součástí matematiky. Při přechodu k obecnému tělesu bylo navíc přece jen třeba překonat jisté odlišnosti.

Článek [R14] svědčí i o tom, že Rychlík sledoval soudobou světovou matematickou literaturu, měl výborný přehled o nejnovějším stavu teorie, odhadl, které výsledky budou mít podstatný vliv na další vývoj, dokázal těchto výsledků využít, případně je vhodně upravit či zobecnit, aplikovat je na stávající teorii a spojit přitom dohromady výsledky různých autorů do jednoho logického celku. Rovněž si můžeme povšimnout Rychlíkovy rychlé reakce – Ostrowského práce [Ost2] vyšla roku 1918, Rychlíkův článek [R14] byl publikován hned v následujícím roce.

Podívejme se nyní ve stručnosti na hlavní výsledky Rychlíkovy práce.

Nechť K je těleso s nearchimedovským ohodnocením $\|\cdot\|$. Rychlík používá následující terminologii. Prvek $a \in K$, pro který je $\|a\| \leq 1$, se nazývá *celým prvkem v* K; je-li $\|a\| = 1$, nazývá se prvek *a jednotkou*. Rychlík ukazuje, že celá čísla v K tvoří obor integrity J. Prvek $a \in K$ je *dělitelný* nenulovým prvkem $b \in K$, je-li $a/b \in J$, tj. $\|a\| \leq \|b\|$; *asociovanými* se nazývají prvky $a, b \in K$, kde prvek a je dělitelný prvkem b a naopak, tj. $\|a\| = \|b\|$. Rychlík zmiňuje existenci největšího společného dělitele, resp. nejmenšího společného násobku prvků $a_1, \ldots, a_n \in K$, pro které platí: $\|(a_1, \ldots, a_n)\| = \max(\|a_1\|, \ldots, \|a_n\|)$, resp. $\|[a_1, \ldots, a_n]\| = \min(\|a_1\|, \ldots, \|a_n\|)$.

Uvažujme celé prvky, které nejsou jednotkami, tj. prvky, jejichž ohodnocení je menší než 1. Jestliže mezi nimi existuje prvek p s největším ohodnocením, pak každý prvek $a \in K$ lze psát ve tvaru $a = ep^r$, kde $r \in \mathbb{Z}$, e je jednotka. Rychlík ukazuje, že p má vlastnost prvočinitele; těleso K se pak nazývá *tělesem s prvočinitelem*.[87]

Pro celý prvek $m \in K$, který není jednotkou, tj. $\|m\| < 1$, označuje kongruence $a \equiv 0 \pmod{m}^*$ vztah $\|a\| < \|m\|$; $a \equiv b \pmod{m}^*$ znamená $a - b \equiv 0 \pmod{m}^*$. Kongruencí polynomů se rozumí kongruence odpovídajících si koeficientů.

Po detailní přípravě zahrnující řadu pomocných tvrzení Rychlík odvozuje větu, která se později začala označovat jako *Hensel–Rychlíkovo lemma* (vedle

[87] Rychlík používá výraz *prvoprvek*. V pozdějších pracích však i on užívá obvyklý termín *prvočinitel*.

Připomeňme, že v případě *exponenciálního* či *aditivního ohodnocení*, kdy se od hodnoty $\|a\|$ přejde k $v(a) = -\log\|a\|$, odpovídá uvedené podmínce to, že existuje prvek s nejmenší kladnou hodnotou; obor hodnot ohodnocení v pak nemá žádný konečný hromadný bod a z toho důvodu se v nazývá *diskrétním ohodnocením*. Viz např. [Has3].

jiných variant) a která je analogií Henselovy věty 9.

Věta 26 (Hensel–Rychlíkovo lemma). Nechť $f(x)$ je polynom s celými koeficienty z úplného ohodnoceného tělesa K. Platí-li kongruence

$$f(x) \equiv g_0(x)h_0(x) \pmod{r^2}^*, \tag{2.46}$$

kde $g_0(x)$, $h_0(x)$ jsou polynomy s celými koeficienty stupně alespoň jedna a $r \neq 0$ je jejich resultant, pak [88]

$$f(x) = g(x)h(x), \tag{2.47}$$

kde $g(x)$, resp. $h(x)$ jsou polynomy s celými koeficienty týchž stupňů jako $g_0(x)$, resp. $h_0(x)$, a platí:

$$g(x) \equiv g_0(x) \pmod{r^2}^*, \qquad h(x) \equiv h_0(x) \pmod{r^2}^*. \tag{2.48}$$

Navíc je $\|R(g,h)\| = \|R(g_0,h_0)\|$.

Analogicky s Henselovým postupem (viz větu 10) Rychlík uvažuje následující speciální případ věty 26, o kterém se rovněž někdy hovoří jako o *Hensel–Rychlíkově lemmatu*:

Věta 27. Nechť $f(x)$ je polynom s celými koeficienty z úplného ohodnoceného tělesa K. Je-li možné nalézt $\xi_0 \in K$ tak, že

$$\|f(\xi_0)\| < \|f'(\xi_0)\|^2, \tag{2.49}$$

pak má rovnice $f(x) = 0$ v tělese K kořen ξ, pro který platí:

$$\xi \equiv \xi_0 \pmod{1}^*. \tag{2.50}$$

Jiným důsledkem věty 26 je zobecnění Henselovy věty 11, které bez důkazu zmínil J. Kürschák – viz větu 25.

Jak bylo naznačeno na str. 92, na základě tohoto tvrzení je možné dokázat základní větu teorie ohodnocení, tj. větu 24, ryze algebraicky, bez použití mocninných řad, což také Rychlík podrobně provádí.

Zur Bewertungstheorie der algebraischen Körper [R22] (1923)

Čtyři roky poté, co byl v *Časopise pro pěstování mathematiky a fysiky* otištěn Rychlíkův článek [R14], byla v *Crelleově časopise* publikována jeho německá verze [R22] s prakticky stejným obsahem. Oproti [R14] jsou zde pouze některé drobné změny ve formulacích či v dílčích krocích v důkazech (například místo explicitního vyslovení důsledku věty je důkaz jistého dílčího tvrzení veden

[88] Ve větě by měl být navíc ještě jeden předpoklad, aby byla obecně platná: vedoucí koeficient polynomu $f(x)$ je *roven* součinu vedoucích koeficientů polynomů $g_0(x)$ a $h_0(x)$, ne pouze kongruentní. Na pravé straně vztahu (2.47) by se jinak objevila jistá jednotka. Připomeňme, že Hensel se v této souvislosti omezil na primární polynomy (zde str. 76), pro které je uvedená podmínka vždy splněna – tuto drobnou odlišnost Rychlík patrně přehlédl. Viz např. [Ost4], str. 275; [Roq1], str. 12.

přímo, u některých tvrzení je místo rozepsání důkazu jen odkaz na literaturu, kde byl již proveden), podrobnější citace literatury apod. Nejsou tu však navíc žádná tvrzení, která by v původní verzi chyběla, postup a uspořádání obou prací se v zásadě shodují.

Zatímco česky psaná práce [R14] zůstala bez povšimnutí stranou dalšího vývoje, její německá varianta [R22] již našla širokou odezvu za hranicemi Československa a stala se prací často citovanou, známou prakticky všem významným matematikům, kteří se teorií ohodnocení zabývali či zabývají. A často zůstává Rychlíkovo jméno spojeno se zobecněním Henselova lemmatu, i když není článek [R22] přímo citován; tak je tomu například v Kaplanského pojednání [Kap1] z roku 1942, v Eršovově článku [Ers1] z roku 1980, v článku [E-M1] I. Efrata a M. Jardena z roku 1990 či v Ribenboimově knize [Rib2] z roku 1998.

Výslovně Rychlíkovu práci [R22] citují například R. Böffgen a M. A. Reichert ([B-R1], 1987), H. Hasse ([Has1], 1926; [H-S1], 1933), A. N. Kochubei ([Koc1], 1998), W. Krull ([Kru1], 1930; [Kru2], 1932), M. Nagata ([Nag1], 1953), W. Narkiewicz ([Nar1], 1974), A. Ostrowski ([Ost3], 1933; [Ost4], 1935), P. Ribenboim ([Rib1], 1985), P. Roquette ([Roq1], 1999), O. F. G. Schilling ([Sch1], 1950), F. K. Schmidt ([H-S1], 1933; [Scm1], 1933), W. Więsław ([Wie2], 1988) a další. Rychlíkova rychlá reakce, o které jsme se zmínili v úvodu této kapitoly, však zůstala skryta v českém ČPMF. Článek [R22] zůstal zároveň jedinou Rychlíkovou algebraickou prací, které se ve světě dostalo větší pozornosti.

2.1.4 Teorie algebraických čísel, abstraktní algebra

Práce zahrnuté do této skupiny byly publikovány v českých časopisech, česky nebo německy, a ve světě zůstaly téměř neznámé. Jsou však velmi zajímavé a ukazují Rychlíkův přístup k vědecké práci. Články se vyznačují jednak velmi aktuálním obsahem, jednak přímočarostí, stručností, zároveň však výstižností a korektností. Některé myšlenky, které jsou v nich obsažené, lze navíc nalézt v pozdějších – nezávislých – pracích jiných matematiků (např. H. Hasse [Has3], H. Prüfer [Prü1]).

Dělitelnost v algebraických tělesech číselných vzhledem k racionálnému prvočíslu **[R15] (1919)**

Článek je přípravou na práci [R16] věnovanou teorii dělitelnosti v tělesech algebraických čísel. Je zde citována poměrně málo známá polsky psaná práce [Soc1] J. Sochockého z roku 1893 a Henselova kniha [Hen8] z roku 1908. Rychlík studuje relaci dělitelnosti vzhledem k prvočíslu p v tělesech algebraických čísel konečného stupně nad $\mathbb{Q}$ (viz Henselovu definici 15; Rychlík místo „v oboru p“ používá vyjádření „vzhledem k p“) a dokazuje, že pro libovolné dva prvky α, β daného tělesa K existuje jejich největší společný dělitel $\delta \in K$, který může být

navíc vyjádřen ve tvaru $\delta = \alpha\mu + \beta\nu$ pro nějaké prvky $\mu, \nu \in K$, které jsou celé vzhledem k p.

Rychlík ukazuje, že není nutné předpokládat, že stupeň tělesa K je konečný. Pro danou dvojici $\alpha, \beta \in K$ totiž stačí uvažovat podtěleso tělesa K, jehož stupeň je již konečný a které obsahuje čísla α, β; takové podtěleso vždy existuje – např. těleso vytvořené adjunkcí prvků α, β k tělesu racionálních čísel $\mathbb{Q}$.

Pro těleso K *konečného stupně* n nad $\mathbb{Q}$ pak Rychlík dokazuje, že libovolné číslo $\alpha \in K$, které je celé vzhledem k p, lze rozložit na součin konečného počtu prvočinitelů vzhledem k p a že tento rozklad je v podstatě jednoznačný. *Prvočinitel vzhledem k p* je přitom definován jako prvek $\pi \in K$, který je ireducibilní vzhledem k p, tj. jeho jedinými děliteli jsou jednotky a čísla s ním asociovaná vzhledem k p, přičemž se ukáže, že tento prvek má vlastnost prvočinitele.

V závěru Rychlík dokazuje, že celkový počet g navzájem neasociovaných prvočinitelů vzhledem k p z tělesa K je konečný, $g \leq n$.

Stejné výsledky (s výjimkou poznámky o tělese nekonečného stupně) jsou obsaženy již v uvedeném Sochockého pojednání [Soc1]. Rychlíkův postup je však celkově jednodušší, přímočařejší a přehlednější než postup Sochockého, čemuž výrazně napomohlo využití Henselovy terminologie.

Theorie dělitelnosti čísel algebraických [R16] (1920)

Tento článek, předložený k tisku již v roce 1919, využívá výsledků odvozených v práci [R15]. Rychlík zde buduje teorii dělitelnosti pro algebraická čísla založenou na pojmu *divisor*. Cituje Henselovu knihu [Hen8], jeho přístup je však poněkud odlišný. Hensel uvažoval jisté algebraické těleso konečného stupně nad $\mathbb{Q}$, pro něj definoval *prvodivisory* a na základě rozkladu v provodivisory pak zavedl *divisory*, které jsou tak fixované na dané těleso. Oproti tomu Rychlíkův pojem divisoru, stejně jako z něj vyvozené pojmy celého čísla, dělitelnosti či asociovanosti, nezávisí na konkrétním uvažovaném tělese a je tedy možné například srovnávat divisory z různých těles; definici lze navíc použít i pro tělesa nekonečného stupně nad $\mathbb{Q}$. Jak Rychlík sám poznamenává v pozdější práci [R24], v tom také spočívá přednost teorie divisorů před teorií ideálů.

Je třeba zdůraznit, že Rychlíkova cesta k pojmu divisor je opět přímočará, přehledná a zcela v duchu „moderní“ abstraktní algebry, která se v té době jinak teprve formovala.

Rychlík postupuje v následujících krocích. Nejprve uvažuje komutativní multiplikativní grupu A všech nenulových algebraických čísel nad $\mathbb{Q}$ a její podgrupu J tvořenou jednotkami vzhledem k prvočíslu p. *Divisory vzhledem k p* nazývá prvky (komutativní) faktorové grupy A/J,[89] tedy třídy obsahující algebraická čísla navzájem asociovaná vzhledem k p; jednotkový prvek odpovídá algebraickým jednotkám vzhledem k p. Je-li algebraické číslo α prvkem třídy $\mathfrak{a}$, pak se řekne, že je *právě dělitelné divisorem* $\mathfrak{a}$ a píše se $\alpha \sim \mathfrak{a}\ (p)$; rovněž se používá vyjádření, že divisor $\mathfrak{a}$ *odpovídá* číslu α. Divisory odpovídající algebraickým číslům, která jsou celá vzhledem k p, se nazývají *celými vzhledem k p*.

[89] Rychlík ji nazývá grupou *komplementární*.

V dalším se Rychlík omezuje na libovolné, pevně zvolené těleso K. Divisory vzhledem k p odpovídající prvkům tělesa K se nazývají *divisory vzhledem k p z tělesa K*. Tyto divisory tvoří komutativní grupu, která je isomorfní s faktorovou grupou A'/J', kde A' značí grupu nenulových algebraických čísel z tělesa K a J' grupu jednotek vzhledem k p z tělesa K.

Grupu divisorů vzhledem k souhrnu jistých prvočísel $p, q, \ldots, r, \ldots$ (může jich být konečný nebo nekonečný počet) Rychlík definuje, řečeno v dnešní terminologii, jako vnější direktní součin výše definovaných grup divisorů vzhledem k prvočíslům $p, q, \ldots, r, \ldots$:

DEFINICE 26 (DIVISORY). *Buďtež* $\mathfrak{a}, \mathfrak{a}', \ldots; \mathfrak{b}, \mathfrak{b}', \ldots; \ldots; \mathfrak{c}, \mathfrak{c}', \ldots; \ldots$ *divisory patřící resp. k* $p, q, \ldots, r, \ldots$. *Nechť značí* $\mathfrak{ab}\ldots\mathfrak{c}\ldots$ `divisor patřící k souhrnu` $p, q, \ldots, r, \ldots$; $\mathfrak{a}, \mathfrak{b}, \ldots, \mathfrak{c}, \ldots$ *nazveme* `komponenty` *tohoto divisoru patřící resp. k* $p, q, \ldots, r, \ldots$. *Budeme předpokládati, že v případě nekonečného počtu prvočísel* $p, q, \ldots, r, \ldots$ *jen konečný počet komponent je různý od prvku jednotkového* $1_p, 1_q, \ldots, 1_r, \ldots$ *příslušné grupy.*

I budeme definovati pro divisory $\mathfrak{ab}\ldots\mathfrak{c}\ldots$, $\mathfrak{a}'\mathfrak{b}'\ldots\mathfrak{c}'\ldots$ *patřící k souhrnu* $p, q, \ldots, r, \ldots$ *rovnost*

$$\mathfrak{ab}\ldots\mathfrak{c}\ldots = \mathfrak{a}'\mathfrak{b}'\ldots\mathfrak{c}'\ldots, \qquad \textit{je-li} \quad \mathfrak{a} = \mathfrak{a}', \mathfrak{b} = \mathfrak{b}', \ldots \mathfrak{c} = \mathfrak{c}', \ldots,$$

násobení

$$(\mathfrak{ab}\ldots\mathfrak{c}\ldots)(\mathfrak{a}'\mathfrak{b}'\ldots\mathfrak{c}'\ldots) = (\mathfrak{aa}')(\mathfrak{bb}')\ldots(\mathfrak{cc}')\ldots,$$

dále

$$(\mathfrak{ab}\ldots\mathfrak{c}\ldots)^{-1} = \mathfrak{a}^{-1}\mathfrak{b}^{-1}\ldots\mathfrak{c}^{-1}\ldots \ .$$

Pak je patrně

$$\mathfrak{ab}\ldots\mathfrak{c}\ldots = (\mathfrak{a}1_q\ldots1_r\ldots)(1_p\mathfrak{b}\ldots1_r\ldots)\ldots(1_p1_q\ldots\mathfrak{c}\ldots)\ldots \ .$$

Kde nebude možný omyl, označíme $\mathfrak{a}1_q\ldots1_r\ldots$ *prostě* $\mathfrak{a}$ *atd. Takto bychom mohli postupovat pro libovolný souhrn prvočísel racionálných* $p, q, \ldots, r, \ldots$. *Budeme však uvažovati divisory vzhledem k soustavě všech prvočísel racionálných a ty nazveme prostě* `divisory`.[90]

Celým divisorem se nazývá divisor, jehož všechny komponenty jsou celé. Pak je možné pro divisory zavést relaci dělitelnosti a pojem *největšího společného dělitele*, kterého lze určit po komponentách.

Pro algebraické číslo α, pro které platí: $\alpha \sim \mathfrak{a}\ (p)$, $\alpha \sim \mathfrak{b}\ (q)$, ..., je mezi divisory $\mathfrak{a}, \mathfrak{b}, \ldots$ jen konečný počet nejednotek. Proto může být číslu α přiřazen jistý divisor $\alpha \sim (\mathfrak{ab}\ldots)$. Divisory, jejichž komponenty náležejí tělesu K, se nazývají *divisory tělesa K*. Mezi nimi existují tzv. *hlavní divisory*, které odpovídají číslům tělesa K. Rychlík ukazuje, že největší společný dělitel divisorů tělesa K je opět divisor tělesa K, ale největší společný dělitel dvou hlavních divisorů nemusí být hlavní.

Nechť je stupeň tělesa K konečný. Podle [R15] existuje konečný počet navzájem různých *prvodivisorů vzhledem k* p, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_g$, z nichž každý odpovídá

[90] [R16], str. 2–3.

třídě navzájem asociovaných prvočinitelů vzhledem k p. Každý divisor vzhledem k p z tělesa K lze potom jednoznačně vyjádřit ve tvaru

$$\mathfrak{a} = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\dots\mathfrak{p}_g^{k_g}\,, \qquad k_1, k_2, \dots, k_g \in \mathbb{Z}; \tag{2.51}$$

pro celé divisory bude zřejmě $k_1 \geq 0, \dots, k_g \geq 0$.

Každému prvodivisoru vzhledem k p odpovídá prvodivisor vzhledem k systému všech prvočísel, který se bude značit stejně (p je vzhledem ke všem ostatním prvočíslům jednotkou). Nyní je možné libovolný divisor jednoznačně rozložit na součin prvodivisorů; k tomu postačí rozložit jeho komponenty. Podobně, po komponentách, lze rozložit libovolné algebraické číslo $\alpha \in K$. To není jednotkou pouze vzhledem ke konečnému počtu prvočísel $p, q, \dots, r$. Značí-li $\mathfrak{p}, \mathfrak{q}, \dots, \mathfrak{r}$ navzájem různé prvodivisory, které dělí uvedená prvočísla, pak lze α vyjádřit právě jedním způsobem ve tvaru

$$\alpha \sim \mathfrak{p}^k\mathfrak{q}^l\dots\mathfrak{r}^m\,, \qquad k, l, \dots, m \in \mathbb{Z}. \tag{2.52}$$

Rychlík ukazuje, že α je celé, právě když je $k \geq 0$, $l \geq 0$, …, $m \geq 0$ (viz Henselovu větu 22 na str. 83).

Popsané pojmy a jejich vlastnosti jsou základem pro další vyšetřování. V závěru Rychlík dokazuje, že pro daný divisor $\mathfrak{d}$ tvoří všechna čísla z tělesa K, která jsou dělitelná divisorem $\mathfrak{d}$, ideál $I(\mathfrak{d})$,[91] a také naopak, pro každý ideál I existuje právě jeden divisor $\mathfrak{d}$, pro který je $I = J(\mathfrak{d})$. Rychlík pak ukazuje, jak lze tvrzení o rozkladu divisorů přenést na ideály daného tělesa K.

Poznamenejme, že pomocí faktorové grupy zavádí divisory v případě libovolného tělesa s diskrétním ohodnocením (viz pozn. 87) také například Helmut Hasse v knize [Has3]; Rychlíkovu práci [R16] však Hasse necituje. Přímo je článek [R16] citován v Narkiewiczově knize [Nar1], avšak s poznámkou, že autorovi nebyl dostupný.

Zur Theorie der Teilbarkeit [R23] (1923)

V poměrně rozsáhlém německy psaném pojednání [R23] Rychlík zavádí pojem *pologrupy* a buduje teorii dělitelnosti v její podílové grupě. *Komutativní grupu* definuje obvyklým způsobem jako množinu G opatřenou binární operací (používá multiplikativní značení) splňující asociativní a komutativní zákon a dále podmínku, že pro všechna $a, b \in G$ má rovnice $ax = b$ právě jeden kořen x.

Komutativní pologrupou (*kommutative Halbgruppe*) Rychlík nazývá množinu H s binární operací splňující asociativní a komutativní zákon a dvojici

[91] Označme symbolem $\mathfrak{D}$ množinu všech celých algebraických čísel tělesa K. Řečeno v pozdější terminologii, Rychlík zavádí pojem *ideál* jako konečně generovaný $\mathfrak{D}$-modul obsažený v K, neboli jako tzv. *lomený ideál* (*gebrochen Ideal, fractional ideal*; srov. např. [Wae1], [Jan1]). Rychlík podává dvě definice ideálu, o kterých dokazuje, že jsou ekvivalentní:

1. Pro daný konečný počet čísel $\alpha_1, \alpha_2, \dots, \alpha_m \in K$, která nejsou všechna nulová, se *ideálem* tělesa K nazývá množina $I = \{\lambda_1\alpha_1 + \lambda_2\alpha_2 + \dots + \lambda_m\alpha_m\,;\ \lambda_1, \dots\ \lambda_m \in \mathfrak{D}\}$.

2. Ideál je podmnožina $I \subseteq K$ té vlastnosti, že pro libovolná $\alpha, \beta \in I$, $\lambda \in \mathfrak{D}$, je $\alpha + \beta \in I$, $\lambda\alpha \in I$ a existuje $g \in \mathbb{Z}$ takové, že $gI \subseteq \mathfrak{D}$.

podmínek:

$$\forall a, b, b' \in H : \ ab = ab' \Rightarrow b = b'; \qquad \exists 1 \in H \ \forall a \in H : \ a1 = a.$$

Dnes bychom tedy hovořili o komutativní pologrupě s jednotkovým prvkem a krácením.[92]

V dalším bude H vždy značit komutativní pologrupu ve výše uvedeném smyslu a G její podílovou grupu, která je definovaná jako grupa obsahující H, přičemž každý prvek z G lze vyjádřit jako podíl dvou prvků z H.[93] Prvky pologrupy H se nazývají *celými prvky grupy* G. Prvek $a \in G$ se nazývá *dělitelný* prvkem $b \in G$, je-li $a/b \in H$; $e \in H$ se nazývá *jednotkou*, je-li rovněž $1/e \in H$; $a, b \in H$ jsou *asociované*, $a \sim b$, je-li a dělitelné b a naopak.

Povšimněme si, že Rychlík definuje dělitelnost nejen pro celé prvky, ale pro všechny prvky podílové grupy G. Podobně definuje *největšího společného dělitele* v H i v G, ozn. $(a, b, \ldots, c)_H$, resp. $(a, b, \ldots, c)_G$,[94] a ukazuje, že pokud největší společný dělitel v G (H) existuje, pak je určen v podstatě jednoznačně. Rovněž uvádí vzájemný vztah obou pojmů: pro celé prvky $a, b, \ldots, c$ grupy G je jejich největší společný dělitel v G (pokud existuje) zároveň jejich největším společným dělitelem v H; opak obecně neplatí. Rychlík však ukazuje, že je-li splněna podmínka označená jako (NSD), platí i opačná implikace.

Axiom (NSD). Každá dvojice prvků $a, b \in H$ má největšího společného dělitele v H.

Přitom dokazuje, že z podmínky (NSD) plyne existence největšího společného dělitele v G pro libovolný konečný počet prvků z G.

Ve své práci Rychlík studuje aritmetiku založenou na výše uvedených pojmech, a to jednak obecně, jednak za předpokladu, že je splněna podmínka (NSD) – v tom případě ukazuje výraznou analogii s aritmetikou v $\mathbb{Q}$. Kromě největšího společného dělitele studuje nejmenší společný násobek daných prvků v G a H a zabývá se jeho vztahem k největšímu společnému děliteli a dalšími jeho vlastnostmi. Rovněž vyšetřuje pojmy *prvočinitel* a *ireducibilní prvek* a jejich vlastnosti a vzájemné vztahy za různých podmínek. Ukazuje například, že každý prvočinitel je ireducibilní, ale obecně ne naopak; je-li však splněna podmínka (NSD), pak je každý ireducibilní prvek také prvočinitelem.

[92] Rychlík zde neuvádí žádný odkaz, ale pojem *pologrupy* byl definován již v Dicksonově článku [Dic2] z roku 1905 jako množina G opatřená binární (multiplikativní) operací, kde platí asociativní zákon a pro všechna $a, x, y \in G$ každá z rovností $ax = ay$, $xa = ya$ implikuje $x = y$. Účel Dicksonovy definice byl však jiný než teorie dělitelnosti. Práce [Dic2] byla otištěna hned za jiným Dicksonovým článkem [Dic1], který byl věnován definici grupy a tělesa pomocí systému nezávislých axiomů a který Rychlík zmínil ve své přednášce *O algebraických tělesech* konané roku 1918 v Jednotě českých matematiků a fyziků; lze se tedy domnívat, že si povšiml i uvedeného následujícího článku [Dic2].

[93] Automaticky se přitom předpokládá, že operace na pologrupě H je zúžením operace na grupě G.

[94] Definice je podána v obvyklém smyslu; pro úplnost ji zde však uveďme, aby byl patrný rozdíl mezi oběma pojmy.

Definice. Nechť jsou dány prvky $a, b, \ldots, c \in G$ (resp. H). Prvek $d \in G$ (H) se nazývá jejich *největším společným dělitelem v* G (H), jsou-li splněny následující podmínky:

1. Všechny prvky $a, b, \ldots, c$ jsou dělitelné d;
2. Jsou-li všechny prvky $a, b, \ldots, c$ dělitelné prvkem $n \in G$ (H), pak n dělí d.

Analogie s aritmetikou racionálních čísel je velmi těsná, je-li kromě podmínky (NSD) splněna ještě podmínka následující, kterou bychom dnes nazvali *existence ireducibilních rozkladů*:

Axiom (E). V grupě G existují celé prvky, které nejsou jednotkami a které lze vyjádřit jako součin konečného počtu ireducibilních prvků.

Kromě tvrzení a jejich důkazů v obecné rovině Rychlík ve své práci podává řadu příkladů a možností využití zavedených pojmů.

Pro ilustraci zde uveďme příklad, v němž uvažuje jako pologrupu H množinu všech celých kladných čísel různých od 2 spolu s operací násobení; podílovou grupou je multiplikativní grupa všech racionálních čísel, $G = \mathbb{Q}$. Rychlík dokazuje, že v tomto případě je splněna podmínka (E), ale ne (NSD).[95] Je-li dále p prvočíslo, pak p a $2p$ jsou nerozložitelné prvky, ale ne prvočinitelé: $8p = 4.2p = 8.p$.

V jiném příkladu Rychlík uvažuje algebraické těleso K konečného stupně nad $\mathbb{Q}$. Nenulová celá algebraická čísla z K tvoří multiplikativní pologrupu H, její podílovou grupou G je grupa všech nenulových prvků tělesa K. Opět zde platí podmínka (E), ale obecně neplatí (NSD). Označí-li se však jako $\mathfrak{H}$ pologrupa celých ideálů v K a jako $\mathfrak{G}$ grupa všech ideálů v K, pak je $\mathfrak{G}$ podílovou grupou pologrupy $\mathfrak{H}$ a kromě podmínky (E) zde platí i (NSD), neboli každý konečně generovaný ideál v K je hlavní.

V závěru Rychlík aplikuje své výsledky na libovolný obor integrity I a jeho podílové těleso K (klade $H = I$, $G = K$ a uvažuje operaci násobení). Navíc se zde zabývá následující podmínkou:[96]

Axiom (A). Pro libovolné prvky $a, b \in K$ existuje jejich největší společný dělitel v K, který lze vyjádřit ve tvaru $d = ax + by$ pro nějaké $x, y \in I$.

Snadno se ukáže, že z platnosti podmínky (A) plyne platnost podmínky (NSD), ale ne naopak. Jako protipříklad zde slouží těleso racionálních funkcí $K = \mathbb{Q}(x)$ a obor integrity polynomů s racionálními koeficienty $I = \mathbb{Q}[x]$. Je-li p prvočíslo, pak $(p, x)_K = 1$, ale pro žádné prvky $k, l \in I$ není $kx + lp = 1$.

Konečně Rychlík zavádí v tělese K *míru* (*Maß*) jako zobrazení K do množiny nezáporných racionálních čísel, které splňuje následující podmínky:

(M1) $M(a) = 0$, právě když $a = 0$; jinak je $M(a) > 0$. Pro $a \in I$ je $M(a) \in \mathbb{Z}$.

(M2) $M(ab) = M(a) \cdot M(b)$

(M3) Pro $a \in K \setminus I$ existují prvky $k, l \in I$ takové, že $0 < M(ka + l) < 1$.

Rychlík dokazuje, že prvek $e \in K$ je jednotkou, právě když je celý, $e \in I$, a $M(e) = 1$. Dále dokazuje, že v tělese K lze sestrojit míru, právě když jsou splněny podmínky (A) a (E).

[95] Jak Rychlík poznamenává, $(12, 24)_H$ neexistuje, neboť společnými děliteli čísel 12 a 24 jsou 1, 3 a 4. Největší společný dělitel $(3, 6)_H$ existuje a je roven 1, $(3, 6)_G$ však neexistuje (jiným společným dělitelem je číslo 4/3).

[96] Uvědomme si, že výše jsme měli jen jednu operaci.

Pro ilustraci je v článku uvedeno několik příkladů těles opatřených mírou:

1. $K = \mathbb{Q}\ \ I = \mathbb{Z},\ M(a) = |a|$.
2. K je kvadratické těleso nebo těleso vzniklé adjunkcí 3., 4. či 5. odmocniny z jedné k tělesu racionálních čísel, I je množina celých algebraických čísel tohoto tělesa, $M(a) = |N(a)|$.
3. K je těleso racionálních funkcí $\mathfrak{K}(x)$, kde je $\mathfrak{K}$ libovolné těleso a x transcendentní prvek vzhledem ke $\mathfrak{K}$, I je okruh polynomů $\mathfrak{K}[x]$. Každý nenulový prvek $a \in K$ lze vyjádřit jako podíl dvou nenulových polynomů: $a = f(x)/h(x)$, kde $\operatorname{st} f = m$, $\operatorname{st} h = n$; rozdíl $m - n$ nezávisí na volbě polynomů f, h. Míra je definována vztahem $M(a) = g^{m-n}$ pro $a \neq 0$, $M(0) = 0$, kde $g > 1$ je libovolně zvolené celé číslo.
4. K je libovolné těleso, na němž je definováno nearchimedovské ohodnocení $\|\cdot\|$,[97] $I = \{a \in K;\ \|a\| \leq 1\}$, $M(a) = \|a\|$.

Zbývá poznamenat, že některé úvahy z Rychlíkovy práce [R23] lze nalézt v Prüferově článku [Prü1] z roku 1932, kde je mimo jiné studována dělitelnost v podílovém tělese oboru integrity.

Zur Theorie der Teilbarkeit in alg. Zahlkörpern [R24] (1923)

V článku [R24] se Rychlík vrací k teorii dělitelnosti algebraických čísel založené na pojmu *divisor*. I když zde přímo necituje své dřívější česky psané práce [R15] a [R16] na stejné téma, rozvíjí myšlenky v nich obsažené. Opět cituje Sochockého článek [Soc1], navíc uvádí Zolotarevovo *téměř zapomenuté pojednání* [Zol4]. Ve srovnání s příslušnými českými pracemi je tato podrobnější a přístup je poněkud odlišný, využívající výsledků článku [R23].

Označme symbolem $\vee$ množinu všech přirozených prvočísel, $\wedge$ prázdnou množinu, $P = \{p_1, p_2, \ldots\} \subseteq \vee$, $\overline{P} = \vee \setminus P$. Čísla tvaru $p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$, kde $p_i \in P,\ k_i \in \mathbb{Z}$ a $P \neq \wedge$, se nazývají *vyjádřitelná v P* (*in P darstellbar*). Každé kladné racionální číslo je podle této definice vyjádřitelné v $\vee$, pouze číslo 1 se považuje za vyjádřitelné v $\wedge$.

Každé $a \in \mathbb{Q},\ a \neq 0$, může být vyjádřeno ve tvaru

$$a = |a|_P \,.\, |a|_{\overline{P}} \,.\, \operatorname{sgn} a, \tag{2.53}$$

kde $|a|_P$, resp. $|a|_{\overline{P}}$, je vyjádřitelné v P, resp. v $\overline{P}$; pro $a = 0$ se položí $|0|_P = 0$. Číslo $|a|_P$ se nazývá *absolutní hodnotou a vzhledem k P* (*in Bezug auf P*). V případě jednoprvkové množiny $P = \{p\}$ se místo a_P píše a_p. *Racionální číslo* a se nazývá *celé vzhledem k P*, je-li $|a|_P \in \mathbb{Z}$. *Algebraické číslo* α se nazývá *celé vzhledem P*, je-li kořenem polynomu tvaru (2.22), kde koeficienty jsou celé vzhledem k P.[98]

[97] Na tomto místě Rychlík cituje Kürschákův článek [Kür2] a své vlastní práce [R14] a [R22].

[98] Je-li P neprázdná konečná množina, pak Rychlík poznamenává, že pojem *celého čísla vzhledem k P* odpovídá pojmu *celý v oboru g* zavedenému Kurtem Henselem v [Hen12] (viz definici 1), kde g je libovolné celé číslo dělitelné právě všemi prvočísly obsaženými v množině P.

Rychlík odvozuje řadu tvrzení o algebraických číslech celých vzhledem k P. V jednom z nich například dokazuje, že je-li $P \neq \wedge$, pak libovolné algebraické číslo α je celé vzhledem k P, právě když je celé vzhledem ke všem prvočíslům obsaženým v P.

Celá algebraická čísla vzhledem k P tvoří obor integrity,[99] jehož podílovým tělesem je těleso všech algebraických čísel nad $\mathbb{Q}$. Mohou se sem tedy přenést výsledky odvozené v předchozí práci [R23].

Podobným způsobem jako v [R15], tentokrát však s využitím pojmů studovaných v [R23], Rychlík dokazuje existenci největšího společného dělitele vzhledem ke konečné neprázdné množině P; pro těleso K konečného stupně $\mathbb{Q}$ pak dokazuje, že existuje konečný počet v podstatě různých (až na asociovanost vzhledem k P) prvočinitelů vzhledem k P.

Pojem *divisor* Rychlík v této práci zavádí následujícím způsobem. Uvažujme systém $\{\alpha; P\}$ sestávající z algebraického čísla α a množiny P, která může být i prázdná. Pro $\alpha \neq 0$ se algebraické číslo A_p nazývá *komponentou vzhledem k p systému* $\{\alpha; P\}$, je-li

$$\begin{cases} A_p \sim \alpha & \text{vzhledem k } p \quad \text{pro } p \in P, \\ A_p \sim 1 & \text{vzhledem k } p \quad \text{pro } p \notin P. \end{cases}$$

Komponenty systému $\{0; P\}$ jsou definovány jako 0.

Systémy $\{\alpha; P\}$ a $\{\beta; Q\}$ se nazývají *asociované*, je-li $A_p \sim B_p$ pro všechna prvočísla p. Relace „asociovaný s“ je ekvivalence, což umožňuje definovat *divisory* jako *nové prvky přiřazené třídám navzájem asociovaných prvků.* Divisor přiřazený třídě obsahující systém $\{\alpha; P\}$ se značí symbolem $(\alpha)_P$, komponenta A_p, která je určena v podstatě jednoznačně vzhledem k p, se nazývá *číselnou komponentou* (*Zahlenkomponente*) *divisoru* $(\alpha)_P$ *vzhledem k p.*

Nechť K je algebraické těleso nad $\mathbb{Q}$. Divisor $\mathfrak{a}$, který je možné vyjádřit jako $\mathfrak{a} = (\alpha)_P$, $\alpha \in K$, se nazývá *divisorem tělesa* K. Jeho komponenty mohou být zvoleny v K. Divisor $(\alpha)_R$, kde $\alpha \neq 0$ a R je množina všech prvočísel, vzhledem ke kterým α není jednotkou (Rychlík ukazuje, že množina R je konečná), se značí symbolem (α) a nazývá se *hlavní divisor* (*Hauptdivisor*). Je-li $\alpha \in K$, pak se (α) nazývá *hlavní divisor tělesa* K.[100]

Nechť $\mathfrak{a}$ je libovolný divisor. Číselná komponenta A_p tohoto divisoru je určena v podstatě jednoznačně vzhledem k p; divisor $\mathfrak{a}_p = (A_p)_p$, je proto určen jednoznačně a nazývá se *divisor-komponentou* (*Divisorenkomponente*) *divisoru* $\mathfrak{a}$. Zřejmě je $\mathfrak{b} = \mathfrak{a}$, právě když $\mathfrak{a}_p = \mathfrak{b}_p$ pro všechna prvočísla p. *Součin* a *podíl* divisorů jsou definovány pomocí číselných komponent, stejně tak pojem *celého divisoru.* Rychlík pak dospívá k vyjádření libovolného divisoru ve tvaru

$$\mathfrak{a} = \prod_p \mathfrak{a}_p, \tag{2.54}$$

[99] Pro $P = \wedge$ je zřejmě tento obor integrity totožný s tělesem všech algebraických čísel nad $\mathbb{Q}$.

[100] Jak Rychlík poznamenává, pro $K = \mathbb{Q}$ jsou všechny divisory hlavní.

kde součin se bere přes všechna prvočísla, přičemž pro každý divisor je $\mathfrak{a}_p \neq (1)$ jen pro konečný počet prvočísel p. Připomeňme si způsob zavedení divisorů v článku [R16].

Na tomto základě je stavěna teorie dělitelnosti pro divisory; pro algebraická čísla je dělitelnost převedena na dělitelnost odpovídajících divisorů (α).

Jedním z výsledků Rychlíkovy práce je důkaz existence a jednoznačnosti *největšího společného dělitele* pro libovolný konečný počet divisorů. Rychlík rovněž dokazuje, že každý divisor tělesa K může být vyjádřen jako největší společný dělitel čísel z tohoto tělesa (speciálně pak dvou čísel, z nichž jedno je prvkem tělesa K a jedno racionální). Poznamenejme, že tímto způsobem, tj. jako největší společné dělitele, zavedl divisory Leopold Kronecker [Kro2].

Rychlík zkoumá další vlastnosti relace dělitelnosti divisorů, přičemž opět využívá výsledků své práce [R23] (všechny divisory daného tělesa K tvoří grupu, která je podílovou grupou pologrupy celých divisorů tělesa K), a podobně jako v článku [R16] se zde zabývá vzájemným vztahem divisorů a ideálů. Závěr práce je pak věnován aplikaci obecné teorie na případ kvadratických těles nad $\mathbb{Q}$.

Eine Bemerkung zur Theorie der Ideale [R26] (1924)

V článku [R26] Rychlík upravuje definici pojmu *ideál* tak, aby nebyl závislý na konkrétním uvažovaném algebraickém tělese nad $\mathbb{Q}$ a bylo tak možné srovnávat ideály různých těles; na této definici pak staví aritmetiku pro algebraická čísla. Vychází přitom ze své práce [R23] věnované teorii dělitelnosti v obecnější rovině. V souvislosti s klasickou teorií ideálů cituje knihy A. Châteleta [Châ1], E. Landaua [Lan1] a E. Heckeho [Hec1].

Nechť algebraické těleso K nad $\mathbb{Q}$ je podtělesem algebraického tělesa L nad $\mathbb{Q}$ a nechť jsou pevně zvoleny prvky $\alpha_1, \ldots, \alpha_k \in K$, $k \geq 1$. Označme symbolem $\mathfrak{D}_L$ obor integrity celých algebraických čísel obsažených v tělese L.[101] Rychlík definuje *ideál* I_K^L jako množinu

$$\mathfrak{a} = \{\alpha_1, \ldots, \alpha_k\}_K^L = \{\mu_1\alpha_1 + \cdots + \mu_k\alpha_k, \quad \mu_1, \ldots, \mu_k \in \mathfrak{D}_L\} \tag{2.55}$$

a buduje teorii ideálů založenou na této definici.

Jedním z výsledků, které Rychlík ve svém článku podává, je důkaz tvrzení, že nenulové ideály I_K^L tvoří grupu, která je podílovou grupou pologrupy tvořené nenulovými celými ideály I_K^L, přičemž ideál (2.55) se nazývá *celý*, jsou-li $\alpha_1, \ldots, \alpha_k$ celá algebraická čísla.[102] To umožňuje přenesení výsledků práce [R23] na tento konkrétní případ. Rychlík dokazuje existenci a jednoznačnost největšího společného dělitele pro libovolnou dvojici ideálů I_K^L.[103] Je-li stupeň tělesa K konečný, pak ukazuje, že kromě podmínky (NSD) platí i podmínka (E).

[101] Tento symbol zde používáme pro přehlednost, v Rychlíkově práci se neobjevuje.

[102] Součin dvou ideálů I_K^L, $\mathfrak{a} = \{\alpha_1, \ldots, \alpha_k\}_K^L$ a $\mathfrak{b} = \{\beta_1, \ldots, \beta_l\}_K^L$, je definován jako ideál

$$\mathfrak{ab} = \{\alpha_1\beta_1, \ldots, \alpha_k\beta_1, \alpha_1\beta_2, \ldots, \alpha_k\beta_2, \ldots, \alpha_1\beta_l, \ldots, \alpha_k\beta_l\}_K^L;$$

korektnost této definice je dokázána. Zřejmě je $\{1\}_K^L\,\mathfrak{a} = \mathfrak{a}$.

[103] Největší společný dělitel ideálů $\mathfrak{a}, \mathfrak{b}$ je ideál $\mathfrak{d} = (\mathfrak{a}, \mathfrak{b}) = \{\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l\}_K^L$.

K porovnání ideálů v různých tělesech stačí jako těleso L uvažovat těleso A všech algebraických čísel nad $\mathbb{Q}$ a využít ekvivalence

$$\{\alpha_1,\dots,\alpha_k\}_K^L = \{\beta_1,\dots,\beta_l\}_K^L \;\Leftrightarrow\; \{\alpha_1,\dots,\alpha_k\}_K^K = \{\beta_1,\dots,\beta_l\}_K^K . \qquad (2.56)$$

Ideály I_K^A se pak nazývají jednoduše *ideály z* K.

O rozšíření pojmu kongruence [R31] (1929)

Rychlík se nejprve věnuje výkladu pojmů souvisejících s dělitelností vzhledem k množině prvočísel P, a to stejným způsobem jako v článku [R24] (viz str. 101), který ovšem přímo necituje. Přitom se omezuje jen na speciální případ tělesa racionálních čísel $\mathbb{Q}$; ukazuje, že racionální čísla, která jsou celá vzhledem k P, tvoří obor integrity, jehož podílovým tělesem je $\mathbb{Q}$. Pak definuje následující pojem.

Definice 27. Nechť $m \in \mathbb{Q}$ je celé číslo vzhledem k P. Čísla $a, b \in \mathbb{Q}$, která jsou celá vzhledem k P a pro která je rozdíl $a - b$ dělitelný číslem m vzhledem k P, se nazývají *kongruentní* mod m *vzhledem k* P, což se vyjádří zápisem

$$a \equiv b \pmod{m; P}. \qquad (2.57)$$

Rychlík ukazuje, že právě definovaná relace je ekvivalencí. Pro třídy této ekvivalence pak uvažuje operace součtu a součinu, které jsou korektně definované obvyklým způsobem prostřednictvím reprezentantů, a dokazuje, že tvoří okruh $O(m; P)$. Označme symbolem $O(m)$ okruh tříd zbytků (mod m). Zřejmě je $O(m) = O(m; \vee)$. Obecně Rychlík dokazuje, že okruh $O(m; P)$ je isomorfní s okruhem $O(m)$.

O rozšíření pojmu kongruence pro alg. tělesa číselná [R32] (1929)

V tomto článku publikovaném v *Rozpravách* Rychlík zobecňuje úvahy podané ve výše diskutované práci [R31], jež byla otištěna téhož roku v ČPMF, na případ algebraických čísel. Ani práce [R31], ani [R24] tu však není přímo ocitována.

Nyní Rychlík místo tělesa $\mathbb{Q}$ uvažuje libovolné algebraické těleso K konečného stupně n nad $\mathbb{Q}$ a místo systému P jistých racionálních prvočísel p_i uvažuje systém $\mathfrak{P}$ jistých prvoideálů $\mathfrak{p}_i$. Pro algebraické číslo $\alpha \in K$ uvažujme hlavní ideál (α); je-li tento ideál celý vzhledem k $\mathfrak{P}$, pak se i samotné α nazývá *číslem celým vzhledem k* $\mathfrak{P}$. Rychlík ukazuje, že algebraická čísla tělesa K, která jsou celá vzhledem k $\mathfrak{P}$, tvoří obor integrity, jehož podílovým tělesem je K. Pak zobecňuje definici 27:

Definice 28. Nechť $\mathfrak{m}$ je ideál z tělesa K celý vzhledem k $\mathfrak{P}$. Algebraická čísla $\alpha, \beta \in K$, která jsou celá vzhledem k $\mathfrak{P}$ a pro která je rozdíl $\alpha - \beta$ dělitelný ideálem $\mathfrak{m}$ vzhledem k $\mathfrak{P}$, se nazývají *kongruentní* mod m *vzhledem k* $\mathfrak{P}$, což se zapíše jako

$$\alpha \equiv \beta \pmod{\mathfrak{m}; \mathfrak{P}}. \qquad (2.58)$$

Opět se jedná o ekvivalenci; třídy zbytků (mod $\mathfrak{m};\mathfrak{P}$) tvoří při operacích definovaných pomocí reprezentantů okruh $O(\mathfrak{m};\mathfrak{P})$. Označme symbolem $O(\mathfrak{m})$ okruh tříd zbytků (mod $\mathfrak{m}$). Zřejmě je $O(\mathfrak{m}) = O(\mathfrak{m},\vee)$. Obecně Rychlík dokazuje analogicky s předchozí prací, že okruh $O(\mathfrak{m};\mathfrak{P})$ je isomorfní s okruhem $O(\mathfrak{m})$.

Über die Anwendung der Methode von Sochocki ... [R33] (1929)

Sochockého pojednání [Soc1] již bylo zmiňováno v souvislosti s Rychlíkovými články [R15], [R16] a [R24]. Sochocki dokázal existenci největšího společného dělitele pro libovolnou dvojici prvků z oboru integrity tvořeného prvky konečného algebraického rozšíření tělesa racionálních čísel $\mathbb{Q}$, které jsou celé vzhledem k p; jinými slovy, každý ideál v tomto oboru integrity je hlavní. Totéž pak jednodušším způsobem dokázal Rychlík v článku [R15]; v práci [R33] je v této souvislosti citován pouze uvedený článek J. V. Sochockého.

S využitím výsledků své dřívější práce [R23] o teorii dělitelnosti Rychlík v příspěvku [R33] zobecňuje tvrzení o existenci největšího společného dělitele na případ konečného algebraického rozšíření libovolného ohodnoceného tělesa s prvočinitelem (viz str. 93). Přitom cituje německou verzi [R22] svého pojednání o teorii ohodnocení.

O větě Artinově [R39], [R40] (1932)

Dvojice článků [R39] a [R40] z roku 1932 věnovaných Artinově větě sestává z české a nepatrně zkrácené německé verze téže práce. Rychlík cituje druhý díl van der Waerdenovy knihy *Moderne Algebra* [Wae1] z roku 1931, kde je podán výklad teorie ideálů v oborech integrity. V poznámce pod čarou na straně 107, v souvislosti s ideály v oborech, kde neplatí podmínka konečnosti rostoucích řetězců ideálů („Teilerkettensatz“), van der Waerden cituje Artinův „Verfeinerungssatz“.[104] Rychlík přímo necituje svou práci *Zur Theorie der Teilbarkeit* [R23], rozvíjí však úvahy, které jsou v ní obsažené a Artinovu větu dokazuje pro komutativní grupu, v níž je zavedena dělitelnost založená na pojmu pologrupy.

Nechť $\mathfrak{H}$ je pologrupa a $\mathfrak{G}$ její podílová grupa. Předpokládejme, že je splněna podmínka (NSD) (viz str. 99). Indukcí a na základě dvou pomocných tvrzení Rychlík dokazuje:

Věta 28 (Artin). Je-li $a_1a_2\dots a_r \sim b_1b_2\dots b_s$, kde $a_1,\dots,a_r,b_1,\dots,b_s \in \mathfrak{H}$, pak je možné každého činitele rozložit na součin faktorů v $\mathfrak{H}$,

$$a_i \sim a_1^{(i)}a_2^{(i)}\dots a_{r_i}^{(i)}, \quad b_j \sim b_1^{(j)}b_2^{(j)}\dots a_{s_j}^{(j)},$$

[104] Uvažujme obor integrity R, který je celistvě uzavřený, tj. každý prvek jeho podílového tělesa, který je celý nad R, již leží v R. *Kvazirovnost* dvou ideálů $\mathfrak{a}$, $\mathfrak{b}$ oboru R je definována vztahem $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$; tato relace je ekvivalencí a používá se pro ni označení $\mathfrak{a} \sim \mathfrak{b}$.

Zmíněná Artinova věta tvrdí, že jsou-li dány dva rozklady ideálu $\mathfrak{a}$,

$$\mathfrak{a} \sim \mathfrak{b}_1\mathfrak{b}_2\dots\mathfrak{b}_m \sim \mathfrak{c}_1\mathfrak{c}_2\dots\mathfrak{c}_n,$$

pak je možné faktory dále rozložit, takže až na pořadí a kvazirovnost budou oba součiny obsahovat shodné činitele.

takže množiny

$$\{a_k^{(i)},\ i=1,\dots,r,\ k=1,\dots,r_i\},\quad \{b_l^{(j)},\ j=1,2,\dots,s,\ l=1,2,\dots,s_j\}$$

obsahují až na asociovanost shodné prvky.

Dodejme, že dne 26. listopadu 1931, tedy již v roce vydání uvedeného druhého dílu van der Waerdenovy knihy [Wae1], Rychlík přednesl v Jednotě přednášku *O větě Artinově* se stejným obsahem jako dvojice článků [R39] a [R40].

2.1.5 Teorie determinantů

Dvě krátké Rychlíkovy práce jsou věnovány determinantům a obě se zabývají zobecněním nějakého jednoduchého postupu, který selhává pro tělesa charakteristiky 2, právě na tento případ. První z této dvojice, německy psaná práce *Eine Bemerkung zur Determinantentheorie* [R38], byla otištěna roku 1931 v Crelleově časopise a ve světě nezůstala zcela bez povšimnutí; uvádí ji například O. Haupt ve třetím vydání své knihy *Einführung in die Algebra I* [Hau1] z roku 1956. Druhá práce, *Determinanty v tělesech libovolné charakteristiky* [R43], byla napsaná česky a vyšla o tři roky později v ČPMF. Rozhodně však stojí za zmínku, neboť obsahuje definici determinantu v dnes zcela standardní podobě – viz například Procházkovu *Algebru* [Pro1].

Eine Bemerkung zur Determinantentheorie **[R38] (1931)**

První článek z diskutované dvojice je věnován důkazu tvrzení, že determinant matice $A \in K^{n\times n}$, $n>1$, která má shodné dva řádky nebo sloupce, je pro libovolné těleso K nulový. Není-li charakteristika tělesa K rovna 2, pak je důkaz zcela jednoduchý.[105] Rychlík cituje Hasseho knihu [Has2], kde je s využitím Laplaceovy věty podán jednotný (ale již ne tak jednoduchý) obecný důkaz platný pro všechna tělesa.

Ve svém článku Rychlík ukazuje, že i pro tělesa charakteristiky 2 lze provést velice jednoduchý důkaz, a to následujícím způsobem. Uvažujme determinant matice $X=(x_{ij})$ jako polynom nad $\mathbb{Z}$ v proměnných x_{ij}. Má-li matice X^* dva shodné řádky (sloupce), pak v okruhu, který vznikne ze $\mathbb{Z}$ adjunkcí prvků matice X^*, je $|X^*|=0$; tedy také $|X^*|\equiv 0 \pmod 2$. Odtud plyne, že $|X^*|=0$ v okruhu, který vznikne z prvotělesa tělesa K adjunkcí prvků matice X^*, a tím i v okruhu, který vznikne stejnou adjunkcí z tělesa K. Má-li matice A nad tělesem K dva shodné řádky (sloupce), pak se determinant $|A|$ získá z determinantu $|X^*|$ dosazením prvků matice A za prvky matice X^*, takže je $|A|=0$.

[105] Základem je tvrzení, že záměna dvou řádků (sloupců) způsobí změnu znaménka determinantu; zaměníme-li dva řádky (sloupce), které jsou shodné, pak $|A|=-|A|$, tj. $|A|+|A|=2|A|=0$.

Determinanty v tělesech libovolné charakteristiky [R43] (1934)

Článek [R43] představuje zároveň příspěvek na *Druhém sjezdu matematiků zemí slovanských*, který se konal roku 1934 v Praze. Rychlík navazuje na Petrovu práci *O definici determinantu* [Pet1], která byla otištěna v ČPMF v roce 1931 a ve které je podána definice determinantu jako alternující m-lineární formy m-árních proměnných $x^{(i)} = (x_1^{(i)}, x_2^{(i)}, \dots, x_m^{(i)})$, kde koeficient u součinu $x_1^{(1)} x_2^{(2)} \dots x_m^{(m)}$ je roven 1.[106] Přitom m-lineární forma n-árních proměnných,

$$F(x^{(1)}, x^{(2)}, \dots, x^{(m)}) = \sum_{\substack{i_1, i_2, \dots, i_m \\ =1,2,\dots,n}} a_{i_1 i_2 \dots i_m} x_{i_1}^{(1)} x_{i_2}^{(2)} \dots x_{i_m}^{(m)}, \qquad (2.59)$$

se nazývá *alternující*, jestliže se při záměně $x^{(i)}$ a $x^{(i+1)}$ vynásobí číslem (-1).

Petr ukazuje, že na základě této definice lze zcela jednoduše odvodit základní věty o determinantech nad tělesem reálných, popř. komplexních čísel.[107] Je zřejmé, že stejným způsobem lze postupovat v případě libovolného tělesa, jehož charakteristika je různá od 2.

Rychlík ve své práci [R43] modifikuje definici alternující formy tak, aby se definice determinantu ve výše uvedeném smyslu mohla použít i pro tělesa charakteristiky 2: m-lineární forma n-árních proměnných tvaru (2.59) se nazývá *alternující*, jestliže platí: $F(x^{(1)}, \dots, x^{(m)}) = 0$, kdykoli je $x^{(i)} = x^{(j)}$ pro nějaká dvě různá čísla i, j.

Rychlík ukazuje, že tato definice je pro tělesa, jejichž charakteristika je různá od 2, ekvivalentní s definicí Petrovou. Pro tělesa charakteristiky 2 by se však k Petrově definici musela přidat ještě jedna podmínka, totiž že ve formě (2.59) je $a_{i_1 i_2 \dots i_m} = 0$, kdykoli jsou alespoň dva z indexů $i_1, i_2, \dots, i_m$ sobě rovny.

Determinant konkrétní matice $(\, a_i^{(j)} \,)$, $a_i^{(j)} \in K$, se pak získá dosazením. Podobně jako je tomu v Petrově článku [Pet1], Rychlík pomocí uvedené definice snadno odvozuje obvyklé věty pro determinanty matic, jejichž prvky jsou proměnné $x_i^{(j)}$, a dosazením pak pro determinanty matic s prvky z tělesa K. V závěru Rychlík poznamenává, že je také možné postupovat podobným způsobem, jako to ukázal v práci [R38] (viz výše), kdy se využijí přímo věty pro determinanty nad tělesem reálných nebo komplexních čísel.

---

[106] Představme si symbolický zápis

$$\left| (\, x_i^{(j)} \,) \right| = \begin{vmatrix} x_1^{(1)} & x_1^{(2)} & \dots & x_1^{(m)} \\ x_2^{(1)} & x_2^{(2)} & \dots & x_2^{(m)} \\ \dots & \dots & \dots & \dots \\ x_m^{(1)} & x_m^{(2)} & \dots & x_m^{(m)} \end{vmatrix}.$$

V úvodu své práce Petr zdůrazňuje, že si rozhodně neklade nároky na originalitu, jen chce čtenáře ČPMF seznámit s touto definicí, na kterou zatím nikde v literatuře nenarazil. Poznamenejme však, že podobným způsobem definoval pojem determinantu již K. Weierstrass – viz [Bec1], str. 211.

[107] Petr přímo neuvádí, z jakého tělesa jsou koeficienty uvažovaných forem, automaticky však s nimi pracuje jako s reálnými, popř. komplexními čísly.

2.2 OSTATNÍ PRÁCE

2.2.1 Grupy substitucí

Galoisova teorie těles

Připomeňme nejprve některé pojmy a výsledky Galoisovy teorie těles, jak se s nimi pracuje v posledním období.[108]

Především všechna tělesa (jistě komutativní) jsou zde charakteristiky *nula*, takže algebraická rozšíření budou vždy automaticky *separabilní* (minimální polynomy algebraických prvků mají pouze jednoduché kořeny). Je-li K podtěleso tělesa L (neboli, když L je rozšíření tělesa K), pak píšeme jednoduše $K \leq L$ a podobně, když H je podgrupa grupy G, pak také to zapíšeme symbolicky $H \leq G$. Znak $[L : K]$ představuje *stupeň* tělesa L nad K a obdobně $[G : H]$ značí *index* podgrupy H v grupě G. Rozšíření L tělesa K se nazývá *normální nad* K, jestliže každý ireducibilní polynom $g(x) \in K[x]$, který má v L alespoň jeden kořen, se v $L[x]$ už rozkládá na kořenové činitele.

Máme-li tělesa $K \leq L$, pak grupa všech K-automorfismů tělesa L[109] se značí $\Gamma(L|K)$ a nazývá se *Galoisovou grupou* tělesa L nad K. O tělese L se říká, že je *Galoisovým rozšířením* tělesa K, je-li L separabilní rozšíření tělesa K (tedy v našem případě algebraické), je-li L zároveň normální nad K a $|\Gamma(L|K)| = n < \infty$. V takovém případě již existuje *primitivní prvek* $\vartheta \in L$ pro těleso L nad K, tedy takový prvek, že $L = K(\vartheta) = K[\vartheta]$.

Polynom $F(x) \in K[x]$ nejmenšího stupně (s vedoucím koeficientem $1 \in K$) takový, že $F(\vartheta) = 0$, je tzv. *minimální polynom* prvku ϑ nad K. Polynom $F(x)$ je v $K[x]$ ireducibilní; je-li n jeho stupeň, pak vzhledem ke vztahu $L = K[\vartheta]$ máme

$$L : K = n = |\Gamma(L|K)|.$$

Pro dvojici těles $K \leq L$ nastává právě popsaná situace (Galoisovo rozšíření), jestliže L je rozkladové nadtěleso nějakého polynomu $f(x) \in K[x]$ stupně

[108] Za poznámky k této úvodní části autorka děkuje prof. RNDr. L. Procházkovi, DrSc.

[109] Tj. grupa všech automorfismů π tělesa L, kde $\pi(\alpha) = \alpha$ pro každé $\alpha \in K$. Prvky Galoisovy grupy $\Gamma(L|K)$ se ve starší literatuře nazývají také *substituce Galoisovy grupy.*

alespoň 1 nad K. V takovém případě se ireducibilní polynom $F(x) \in K[x]$ nazývá *Galoisovou resolventou* polynomu $f(x)$.[110]

Mějme tělesa $K \leq L$, nechť L je Galoisovo rozšíření tělesa K. Potom platí následující tvrzení:

Tvrzení 1. (i) Jestliže T je mezitěleso, $K \leq T \leq L$, pak pro grupy je

$$H = \Gamma(L|T) \leq \Gamma(L|K) = G;$$

současně pro stupeň těles $[T : K]$ a index grup $[G : H]$ platí rovnost

$$[T : K] = [G : H].$$

(ii) Při označení z (i) je podgrupa H normální v G právě tehdy, když mezitěleso T je normální nad K. V případě normality pak platí grupový isomorfismus

$$\Gamma(L|K)/\Gamma(L|T) = G/H \cong \Gamma(T|K).$$

Jako důsledek dostáváme:

(iii) Každému řetězci mezitěles

$$K = T_0 \leq T_1 \leq \cdots \leq T_{n-1} \leq T_n = L \tag{2.60}$$

odpovídá jednoznačně řetězec podgrup grupy $G = \Gamma(L|K)$:

$$\underline{1} = H_n \leq H_{n-1} \leq \cdots \leq H_1 \leq H_0 = G, \tag{2.61}$$

kde $H_i = \Gamma(L|T_i)$, $i = 0, 1, \ldots, n$. Obráceně, každému řetězci (2.61) podgrup grupy G přísluší jednoznačně řetězec mezitěles (2.60), kde klademe

$$T_i = \{x \mid x \in L,\ \tau(x) = x \text{ pro všechna } \tau \in H_i\}, \qquad i = 0, 1, \ldots, n.$$

Přitom vztah $H_{i+1} \trianglelefteq H_i$ $(0 \leq i < n)$, nastává právě tehdy, když těleso T_{i+1} je normální nad T_i.

(iv) Grupa $G = \Gamma(L|K)$ je řešitelná právě tehdy, když existuje řetězec mezitěles tvaru (2.60) takový, že každé těleso T_{i+1} je normální nad T_i a stupeň $[T_{i+1} : T_i]$ je prvočíslo.

Nyní uvedeme důležitou definici.

Definice 1. Nechť K je těleso.

(i) Rozšíření L tělesa K se nazývá *radikálové*, existuje-li konečný řetězec mezitěles (2.60) takový, že

$$T_{i+1} = T_i(\alpha_i) = T_i[\alpha_i], \qquad i = 0, 1, \ldots, n-1,$$

kde α_i je kořenem binomického polynomu $g_i = x^{r_i} - a_i \in T_i[x]$, který je ireducibilní v $T_i[x]$.

[110] Ještě připomeňme, že když L je Galoisovým rozšířením tělesa K a T je mezitěleso, tedy $K \leq T \leq L$, pak pro každé $\tau \in \Gamma(L|K)$ se mezitělesa T a $\tau(T)$ mezi K, L nazývají *konjugovaná nad* K.

(ii) Polynom $f \in K[x]$ stupně alespoň 1 se nazývá *algebraicky řešitelný nad tělesem* K, existuje-li radikálové rozšíření L tělesa K takové, že v $L[x]$ se f rozkládá na kořenové činitele.

Nyní už lze zformulovat stěžejní výsledek o algebraické řešitelnosti polynomů (neboli algebraické řešitelnosti jimi určených algebraických rovnic).

Věta 1. Nechť L je rozkladové nadtěleso polynomu $f \in K[x]$ nad tělesem K, kde st $f \geq 1$. Potom polynom f je algebraicky řešitelný nad K právě tehdy, když Galoisova grupa $G = \Gamma(L|K)$ je řešitelná.

Je-li T jakékoli těleso (charakteristiky 0) a je-li $f(x) \in T[x]$ polynom stupně $n \geq 1$, pak se f nazývá *algebraicky řešitelný* (neříká se nad čím), když je algebraicky řešitelný nad tělesem, které vzniklo adjunkcí koeficientů polynomu f k prvotělesu tělesa T. Na základě zmíněných výsledků lze dokázat:

Pro každé přirozené číslo $n \geq 5$ existují polynomy v $\mathbb{C}[x]$ stupně n, které nejsou algebraicky řešitelné.

O resolventách se dvěma parametry [R2] (1908)

Polynom

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \,, \tag{2.62}$$

kde koeficienty a_i jsou algebraicky nezávislé nad výchozím tělesem K, se nazývá *obecný polynom stupně* n. Lze dokázat, že obecný polynom (2.62) je separabilní,[111] jeho Galoisovou grupou vzhledem k tělesu $K(a_1, \ldots, a_n)$ je symetrická grupa S_n a stupeň rozkladového nadtělesa je $n!$.[112]

Leopold Kronecker vyslovil ve své práci [Kro1] z roku 1861 bez důkazu větu, kterou při výše uvedeném označení můžeme zformulovat tak, že pro obecný polynom pátého stupně tvaru (2.62) není možné nalézt resolventu $F(x, z)$ o jednom parametru z, kde $z \in K(a_1, \ldots, a_n, \sqrt{\Delta})$, Δ značí diskriminant polynomu $f(x)$ (viz pozn. 34) a koeficienty v F jsou prvky tělesa K; stupeň resolventy se předpokládá větší než 1. Větu dokázal v roce 1877 Felix Klein [Kle1], o deset let později pak poněkud jednodušší důkaz podal Paul Gordan [Gor1].[113]

Karel Rychlík ve své práci [R2] uvedenou větu zobecnil na tvrzení, že pro obecný polynom (2.62) stupně alespoň 6 není možné nalézt resolventu

[111] V jeho rozkladu $f(x) = (x - \xi_1) \ldots (x - \xi_n)$ v rozkladovém nadtělese jsou tedy všechny kořeny ξ_i navzájem různé.

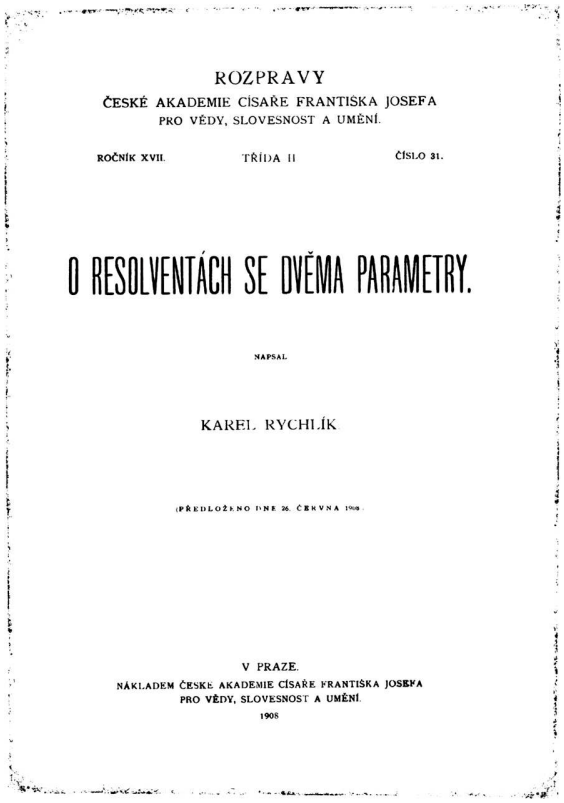
[112] Připomeňme, že *Galoisovou grupou polynomu* $f(x)$ se rozumí grupa permutací P_S přiřazených různým „substitucím“ S Galoisovy grupy rozkladového nadtělesa daného polynomu nad tělesem $K(a_1, \ldots, a_n)$:

$$P_S = \begin{pmatrix} \xi_1 & \xi_2 & \ldots & \xi_n \\ \xi_1^S & \xi_2^S & \ldots & \xi_n^S \end{pmatrix},$$

kde ξ_i^S značí obraz kořene ξ_i v substituci S.

[113] Znovu je důkaz popsán také v druhém díle Weberovy učebnice *Lehrbuch der Algebra* [Web2] z roku 1896.

$F(x, z_1, z_2)$ o dvou parametrech (ve výše uvedeném smyslu).[114] Kleinův i Gordanův důkaz byl založen na větě o racionálních křivkách, kterou roku 1875 dokázal J. Lüroth v práci [Lür1]. Rychlík Lürothovy výsledky zobecnil na racionální funkce dvou proměnných, tj. na racionální plochy, a aplikoval je na větu o resolventě o dvou parametrech.



ROZPRAVY
ČESKÉ AKADEMIE CÍSAŘE FRANTIŠKA JOSEFA
PRO VĚDY, SLOVESNOST A UMĚNÍ.

ROČNÍK XVII. TŘÍDA II ČÍSLO 31.

O RESOLVENTÁCH SE DVĚMA PARAMETRY.

NAPSAL

KAREL RYCHLÍK

(PŘEDLOŽENO DNE 26. ČERVNA 1908.)

V PRAZE.
NÁKLADEM ČESKÉ AKADEMIE CÍSAŘE FRANTIŠKA JOSEFA
PRO VĚDY, SLOVESNOST A UMĚNÍ.
1908

Obr. 2.3 Titulní list separátu Rychlíkovy práce [R2]

O Grupě řádu 360 [R3] (1908)

Část Rychlíkovy disertační práce *O grupách ternárních substitucí holoedricky isomorfních s alternujícími a symmetrickými grupami permutací* byla ještě před obhajobou otištěna v ČPMF, a to pod názvem *O grupě řádu 360* [R3]. V posudku z 23. 12. 1908, který vypracoval Karel Petr a podepsal navíc Jan Sobotka, je Rychlíkova disertace hodnocena takto:

V předložené práci odvozuje p. K. Rychlík nejprve základní věty vzahující se ku grupám substitucí lineárních vůbec. Potom obrací se ku substitucím ternár-

[114] V obou případech se také používá formulace ... *aniž by se zavedly akcessorické iracionality.*

ním a vyšetřuje nejprve, které jsou možné ternární grupy isomorfní se symmetrickými resp. alternujícími gruppami. Konečně vyhledává systémy kompletní invariantů a resolventy při jednotlivých gruppách.

Výklad vyniká velmi přehledným a jasným sestavením, na četných místech dociluje p. kand. podstatných zjednodušení. Část vztahující se ku grupě $\mathfrak{G}_{\frac{1}{2}.6!}$ *podána jest na základě samostatného bádání p. autora a byla uveřejněna tiskem v „Časopise pro pěstování math. a fys.“*

P. Kandidát osvědčuje svojí prací obzvláštní způsobilosti a nadání ku vědeckému bádání mathematickému a lze ji se zřetelem k účelu, za kterým byla p. kandidátu zadána, označiti jako výbornou v každém ohledu.[115]

2.2.2 Teorie forem

Příspěvek k theorii forem I, II **[R4] (1910); [R7] (1911)**

Rychlíkovu habilitační práci tvořila dvojice článků *Příspěvek k theorii forem* [R4] a *Příspěvek k theorii forem II* [R7], které byly publikovány v letech 1910 a 1911 v Rozpravách. Obsah i kritické zhodnocení výborně vystihne citát z posudku habilitační komise, který sepsal její referent Karel Petr a podepsali ještě Jan Sobotka a František Koláček.

Práce habilitační ... skládá se ze dvou částí. Nejprve zabývá se výkladem nauky o souhrnech jednočlenů, kterouž poprvé Delassus (r. 1896) systematicky pěstoval, a snaží se některé věty a výsledky Delassusovy v zjednodušené formě podati. To zejmena se mu podařilo při důkazu věty o kořenech soustavy rovnic tvořené lineárním systémem kanonickým. Důkaz věty, že lineární systém forem odvozený z lineárního systému kanonického jest opět kanonický, jest neúplný a tudíž nesprávný; věta tato však není pro ostatní vyšetřování habilitační práce podstatné důležitosti. Na druhém místě podány jsou v habilitační práci některé applikace. První použití činí na důkaz fundamentální věty Hilbertovy z theorie forem, která se jeví jako zcela jednoduchý důsledek. Větu Hilbertovu pomocí souhrnu jednočlenů dokázal již dříve Gordan, důkazy Rychlíkův a Gordanův jsou však jiného rázu a jsou na sobě nezávisly. Druhé použití týká se důkazu věty Hilbertovy o modulech, že, mizí-li forma pro všechny hodnoty proměnných, které annullují všechny formy daného modulu, jest jisté kladné celé ρ *takové, že* ρ*-tá mocnina té formy přináleží tomu modulu.*[116]

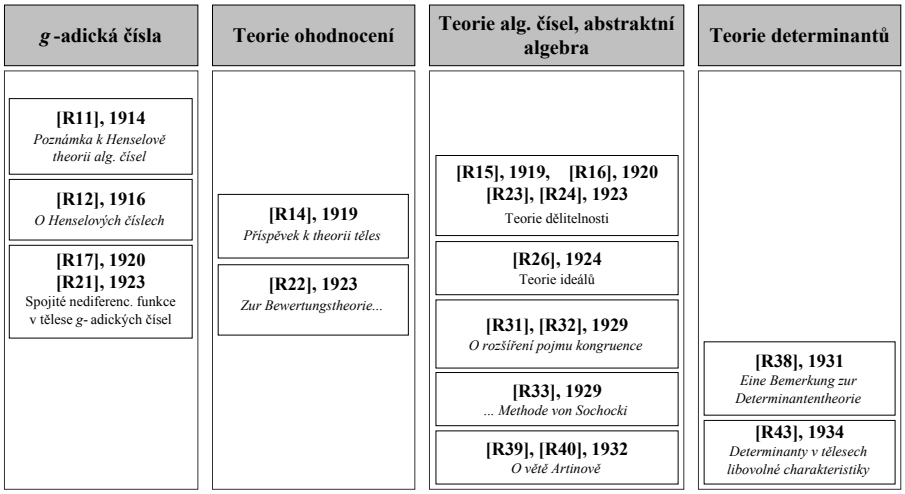
Kromě vlastní habilitační práce jsou v posudku hodnoceny i další Rychlíkovy publikace, a to *Poznámky k theorii interpolace* [R1] z roku 1907, *O grupě řádu 360* [R3] a *O resolventách se dvěma parametry* [R2] z roku 1908. Zmíněny jsou i popularizační články [R5], [R6] a [R8].

[115] Archiv UK, fond FF, Disertační posudky za rok 1908.

[116] Archiv UK, fond FF, Osobní složka Karla Rychlíka. Další podrobnosti související s habilitací jsou uvedeny v části 1.3, str. 30.

2.3 ZÁVĚR

Jak jsme viděli v části 2.1, nejdůležitější matematické práce Karla Rychlíka patří do oblasti algebry a teorie čísel a byly publikovány v letech 1914–1934; pro přehlednost zde byly rozčleněny do čtyř tematických skupin.



Obr. 2.4 Tematické rozdělení zásadních Rychlíkových prací z algebry a teorie čísel

Hlavní zdroje a vnitřní vazby mezi uvažovanými Rychlíkovými publikacemi jsou znázorněny na obr. 2.1, kde jsou plnou čarou vyznačeny explicitní citace, čárkovaně pak zřejmé, avšak ne přímo citované vlivy. Práce věnované determinantům, které tvoří čtvrtou skupinu, stojí poněkud stranou a ve schematu proto nejsou zobrazeny.

Zvlášť byly vyčleněny práce z let 1908–1911 věnované grupám substitucí a teorii forem, které se řadí spíše do „staré“ algebry konce devatenáctého a začátku dvacátého století a s pracemi z následujícího období přímo nesouvisejí – viz část 2.2.

K vytvoření představy o tom, kam lze Rychlíkovy zásadní práce zařadit v širším kontextu, slouží obr. 2.2 zachycující nejvýraznější vlivy (určené především na základě citací) ve vývoji teorie algebraických čísel. Jak již bylo zmíněno, nejsou zde zobrazeny všechny existující vazby, ale jen ty, které znázorňují hlavní vývojové proudy a bezprostřední souvislosti s Rychlíkovými pracemi.

Porovnáme-li oba zmíněné grafy, můžeme si povšimnout, že šipka vedoucí na obr. 2.2 od jména Karla Rychlíka ke jménům A. Ostrowského, H. Hasseho, W. Krulla aj. vychází vlastně z jediné publikace, totiž z německy psaného článku *Zur Bewertungstheorie der algebraischen Körper* [R22] z roku 1923 věnovaného teorii ohodnocení. Zopakujme, že tuto práci citují mj. R. Böffgen a M. A. Reichert ([B-R1], 1987), H. Hasse ([Has1], 1926; [H-S1], 1933), A. N. Kochubei ([Koc1], 1998), W. Krull ([Kru1], 1930; [Kru2], 1932), M. Nagata ([Nag1], 1953), W. Narkiewicz ([Nar1], 1974), A. Ostrowski ([Ost3], 1933; [Ost4], 1935), P. Ribenboim ([Rib1], 1985), P. Roquette ([Roq1], 1999), O. F. G. Schilling ([Sch1], 1950), F. K. Schmidt ([H-S1], 1933; [Scm1], 1933), W. Więsław ([Wie2], 1988) a další. V části 2.1.3 jsme přitom viděli, že stejné výsledky byly obsaženy již v českém článku *Příspěvek k theorii těles* [R14] z roku 1919, který si ovšem neslovanští matematici jen těžko mohli přečíst.

Přínos a zajímavé aspekty ostatních prací byly diskutovány na příslušných místech této kapitoly, stručné celkové hodnocení je podáno v části 1.2. Na tomto místě již jen zdůrazněme, že články zahrnuté do části 2.1 dokládají Rychlíkův hluboký zájem o danou problematiku, soustavné rozsáhlé a podrobné studium starší i nejnovější literatury, výborný „postřeh“, rychlou reakci, schopnost aplikovat nové výsledky a využít je k zobecnění či ke zjednodušení a zpřehlednění. Práce jsou psány na svou dobu velice „moderním“ způsobem – co možná nejstručněji, přitom však výstižně, korektně, s podrobnými citacemi zdrojů, v aktuální terminologii. Od samého počátku, kdy se začala formovat „moderní abstraktní“ čili axiomatická algebra, Rychlík odhadl její přínos a používal i spoluvytvářel její metody a pojmy; je škoda, že příslušné práce otištěné převážně v českých časopisech zaznamenaly ve světě jen minimální ohlas.

Zanedbatelný však rozhodně nebyl vliv na mladou generaci matematiků; jak se o Rychlíkovi vyjádřil jeho student na univerzitě a pozdější asistent na technice Vladimír Kořínek, *... byl ve svých přednáškách na univerzitě prvním průkopníkem této nové abstraktní algebry* (viz str. 31).

Literatura

[B-R1] Böffgen, R.; Reichert, M. A., *Computing the decomposition of primes p and p-adic absolute values in semisimple algebras over* $\mathbb{Q}$, Journal of symbolic computation **4**(1987), 3–10.

[Cau1] Cauchy, A. L., *Cours d'Analyse*, Paris, 1821.

[Châ1] Châtelet, A., *Leçons sur la théorie des nombres*, Gauthier-Villars, Paris, 1913.

[Che1] Chevalley, C., *On the Theory of Local Rings*, Math. Ann. **44**(1943), 690–708.

[Čeb1] Čebyšev, P. L., *Sur l'intégration de la différentielle*

$$\frac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}\,\mathrm{d}x,$$

Bulletin de l'Académie des sciences de St. Pétersbourg **3**(1861), 1–12; ruský překlad: *Ob integrovanii differenciala ...*, in: *Polnoje sobranie sočinenij P. L. Čebyševa, tom II, Matematičeskij analiz*, Izdateľstvo Akademii nauk SSSR, Moskva - Leningrad, 1947, 345–356 [přeložil A. M. Ljapinov].

[Ded1] Dedekind, R., *Gesammelte mathematische Werke I–III*, Vieweg, Braunschweig, 1932.

[Deu1] Deuring, M., *Algebren*, Springer Verlag, Berlin, 1935.

[Dic1] Dickson, L. E., *Definitions of a Group and a Field by Independent Postulates*, Trans. AMS **6**(1905), 198–204.

[Dic2] Dickson, L. E., *On Semi-groups and the General Isomorphism Between Finite Groups*, Trans. AMS **6**(1905), 205–208.

[Die1] Dieudonné, J., *Sur les fonctions continues p-adiques*, Bull. sci. **68**(1944), 79–95.

[Dir1] Dirichlet, P. G. L., *Démonstration du théorème de Fermat pour le cas des 14ièmes pussances*, Crelle **9**(1832), 390–393.

[Dir2] Dirichlet, P. G. L., *Zur Theorie der complexen Einheiten*, Berichte über die Verhandlungen der Königl. Preußischen Akademie der Wissenschaften Berlin (1846), 103–107.

[Dir3] Dirichlet, P. G. L., *Vorlesungen über Zahlentheorie*, Braunschweig, 1863; 2. vyd. 1871; 3. vyd. 1879; 4. vyd. 1894; editoval a doplnil R. Dedekind [odkazy v textu jsou na 4. vydání].

[E-M1] Efrat, I.; Jarden, M., *Free pseudo p-adically closed fields of finite corank*, Journal of Algebra **133**(1990), 132–150.

[Eis1] Eisenstein, G., *Beweis der Reciprocitätsgesetze für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzen Zahlen*, Crelle **27**(1844), 289–322.

[Eis2] Eisenstein, G., *Lois de réciprocité*, Crelle **28**(1844), 53–67.

[Ers1] Eršov, J. L., *Multiply valued fields*, Doklady akademii nauk SSSR **253**(1980), 274–277.

[Eul1] Euler, L., *Vollständige Anleitung zur Algebra*, St. Petersburg, 1770; přetisk: *Leonhardi Euleri Opera omnia, Series 1. Opera mathematica, vol. 1*, B. G. Teubner, Leipzig-Berlin, 1911 [vydal H. Weber, poznámkami opatřil J. L. Lagrange].

[Fra1] Fraenkel, A., *Axiomatische Begründung von Hensels p-adischen Zahlen*, Crelle **141**(1912), 43–76.

[Fra2] Fraenkel, A., *Lebenskreise. Aus den Erinnerungen eines Jüdischen Mathematikers*, Deutsche-Verlags-Anstalt, Stuttgart, 1967.

[Fre1] Fréchet, M., *Sur quelques points du calcul fonctionel*, Rendiconti del Circ. Mat. di Palermo **22**(1906).

[Gau1] Gauss, C. F., *Disquisitiones Arithmeticae*, Leipzig, 1801.

[Gau2] Gauss, C. F., *Theoria residuorum biquadraticorum. Commentatio prima*, Com. Soc. Reg. Sci. Gott. **6**(1828), 9–12*; rovněž v [Gau3], 65–91; *Commentatio secunda*, **7**(1832), 13–19*; rovněž v [Gau3], 93–148.

[Gau3] Gauss, C. F., *Werke*, Band II, Königlichen Gesellschaft der Wissenschaften zu Göttingen, Göttingen, 1876.

[Gor1] Gordan, P., *Ueber biquadratische Gleichungen*, Math. Ann. **29**(1887), 318–326.

[Gro1] Groot, J. de, *Non-Archimedean metrics in topology*, Proceedings of the AMS **7**(1956), 948–953.

[Had1] Hadamard, J., *Essai sur l'étude des functions données par leur développement de Taylor*, Jour. de Math. **(4)VIII**(1892), 101–186.

[Has1] Hasse, H., *Über die Einzigkeit der beiden Fundamentalsätze der elementaren Zahlentheorie*, Crelle **155**(1926), 199–220.

[Has2] Hasse, H., *Höhere Algebra I*, Sammlung Göschen, Berlin, 1926.

[Has3] Hasse, H., *Zahlentheorie*, Akademie-Verlag, Berlin, 1949; 2. vyd. 1963, 3. vyd. 1969; anglický překlad *Number Theory*, Akademie-Verlag, Berlin, 1979.

[Has4] Hasse, H., *Kurt Hensels entscheidender Anstoß zur Entdeckung des Lokal–Global Prinzips*, Crelle **209**(1960), 3–4.

[H-S1] Hasse, H.; Schmidt, F. K., *Die Struktur diskret bewerteter Körper*, Crelle **170**(1933), 4–63.

[Hau1] Haupt, O., *Einführung in die Algebra I, II*, Akademische Verlagsgesellschaft, Leipzig, 1929; 3. vyd. 1956.

[Hec1] Hecke, E., *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademische Verlagsgesellschaft, Leipzig, 1923.

[Hen1] Hensel, K., *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Jahr. DMV **6**(1899), 83–88.

[Hen2] Hensel, K., *Über die Entwickelung der algebraischen Zahlen in Potenzreihen*, Math. Ann. **55**(1901), 301–336.

[Hen3] Hensel, K., *Über analytische Funktionen und algebraische Zahlen*, Ber. Math. Ges. Ber. **1**(1902), 29–32.

[Hen4] Hensel, K.; Landsberg, G., *Theorie der algebraischen Funktionen einer Variabeln und ihre Anwendung auf algebraische Kurven und Abelsche Integrale*, B. G. Teubner, Leipzig, 1902.

[Hen5] Hensel, K., *Neue Grundlagen der Arithmetik*, Crelle **127**(1904), 51–84.

[Hen6] Hensel, K., *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Crelle **128**(1905), 1–32.

[Hen7] Hensel, K., *Ueber die arithmetischen Eigenschaften der Zahlen*, Jahr. DMV **16**(1907), 299–319, 388–393, 473–496.

[Hen8] Hensel, K., *Theorie der algebraischen Zahlen I*, B. G. Teubner, Leipzig, 1908.

[Hen9] Hensel, K., *Über die zu einer algebraischen Gleichung gehörigen Auflösungskörper*, Crelle **136**(1909), 183–209.

[Hen10] Hensel, K., *Gedächtnisrede auf Ernst Eduard Kummer*, in *Festschrift zur Feier des 100. Geburtstages Eduard Kummers*, B. G. Teubner, Berlin-Leipzig, 1910, 1–37; přetisk v [Kum21], 33–69.

[Hen11] Hensel, K., *E. E. Kummer und der grosse Fermatsche Satz*, Marburger Akademische Reden (1910), č. 23.

[Hen12] Hensel, K., *Zahlentheorie*, G. J. Göschen, Berlin-Leipzig, 1913.

[Hen13] Hensel, K., *Über die Grundlagen einer neuen Theorie der quadratischen Zahlkörper*, Crelle **144**(1914), 57–70.

[Hen14] Hensel, K., *Eine Neue Theorie der algebraischen Zahlen*, Math. Zeit. **2**(1918), 433–452.

[Hil1] Hilbert, D., *Die Theorie der algebraischen Zahlkörper* (*Zahlbericht*), Jahr. DMV **4**(1897), 175–546.

[Jac1] Jacobi, C. G. J., *Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie*, Monatsber. Berlin (1837), 127–136; rovněž v Crelle **30** (1846), 166–182.

[Jac2] Jacobi, C. G. J., *Über die complexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind*, Monatsber. Berlin (1839), 86–91; přetisk v Crelle **19**(1839), 314–318; francouzský překlad v Jour. de Math. **8**(1843), 268–272.

[Kap1] Kaplansky, I., *Maximal Fields with Valuations*, Duke Math. Journal **9**(1942), 303–321.

[Kle1] Klein, F., *Weitere Untersuchungen über das Ikosaeder II und III*, Math. Ann. **12**(1877), 503–560.

[Kle2] Klein, F., *Vorlesungen über das Ikosaeder und die Auflösung von Gleichungen vom fünften Grade*, Leipzig, 1884.

[Koc1] Kochubei, A. N., *Harmonic oscillator in characteristic p*, Letters in mathematical physics **45**(1998), 11–20.

[Kro1] Kronecker, L., *Ueber Gleichungen fünften Grades*, Crelle **59**(1861), 306–310.

[Kro2] Kronecker, L., *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, Crelle **92**(1882), 1–122.

[Kro3] Kronecker, L., *De unitatibus complexis. Dissertatio inauguralis arithmetica*, Crelle **93**(1882), 1–52 [disertační práce z roku 1845].

[Kru1] Krull, W., *Idealtheorie in unendlichen algebraischen Zahlkörpern II*, Math. Zeit. **31**(1930), 527–557.

[Kru2] Krull, W., *Allgemeine Bewertungstheorie*, Crelle **167**(1932), 160–196.

[Kru3] Krull, W., *Idealtheorie*, Springer Verlag, Berlin, 1935.

[Kru4] Krull, W., *Dimensionstheorie in Stellenringen*, Crelle **179**(1938), 204–226.

[Kum1] Kummer, E. E., *De aequatione $x^{2\lambda}+y^{2\lambda} = z^{2\lambda}$ per numeros integros resolvenda*, Crelle **17**(1837), 203–209; přetisk v [Kum21], 135–141.

[Kum2] Kummer, E. E., *De numeris complexis, qui radicibus unitatis et numeris integris realibus constant*, Gratulationsschrift der Univ. Breslau zur Jubelfeier der Univ. Königsberg (Academiae Albertinae Regiomontanae secularia tertia celebranti gratulatur Academia Vratislaviensis), 1844, 28 stran, přetisk in: Jour. de Math. **12**(1847), 185–212; [Kum21], 165–192.

[Kum3] Kummer, E. E., *Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen*, Crelle **30**(1846), 107–116; [Kum21], 193–202.

[Kum4] Kummer, E. E., *Zur Theorie der complexen Zahlen*, Monatsber. Berlin (1846), 87–96; přetisk v Crelle **35**(1847), 319–326; [Kum21], 203–210.

[Kum5] Kummer, E. E., *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren*, Crelle **35**(1847), 327–367; [Kum21], 211–251.

[Kum6] Kummer, E. E., *Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ für eine unendliche Anzahl Primzahlen λ*, Monatsber. Berlin (1847), 132–141, 306–319; [Kum21], 274–297.

[Kum7] Kummer, E. E., *Extrait d'une lettre de M. Kummer à M. Liouville*, Jour. de Math. **12**(1847), 136; [Kum21], 298.

[Kum8] KUMMER, E. E., *Allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste*, Monatsber. Berlin (1850), 154–165; [Kum21], 345–357.

[Kum9] KUMMER, E. E., *Bestimmung der Anzahl nicht äquivalenter Classen für die aus λten Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben*, Crelle **40**(1850), 93–116; [Kum21], 299–322.

[Kum10] KUMMER, E. E., *Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus λten Wurzeln der Einheit gebildeten complexen Zahlen*, Crelle **40**(1850), 117–129; [Kum21], 323–335.

[Kum11] KUMMER, E. E., *Allgemeiner Beweis des Fermat'schen Satzes, daß die Gleichung* $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ *durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten* λ*, welche ungerade Primzahlen sind und in den Zählern der ersten* $\frac{1}{2}(\lambda - 3)$ *Bernoulli'schen Zahlen als Factoren nicht vorkommen*, Crelle **40**(1850), 130–138; [Kum21], 336–344.

[Kum12] KUMMER, E. E., *Mémoire sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers*, Jour. de Math. **16**(1851), 377–498; [Kum21], 363–484.

[Kum13] KUMMER, E. E., *Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist*, Math. Abhand. Akad. Berlin (1856), 1–47; [Kum21], 583–629.

[Kum14] KUMMER, E. E., *Über die Gaussischen Perioden der Kreistheilung entsprechenden Congruenzwurzeln*, Crelle **53**(1857), 142–148 [datováno 5. 6. 1856].

[Kum15] KUMMER, E. E., *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen, für den Fall, daß die Klassenanzahl durch* λ *theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Monatsber. Berlin (1857), 275–282; [Kum21], 631–638 [jedná se o výtah z pojednání [Kum16]].

[Kum16] KUMMER, E. E., *Einige Sätze über die aus den Wurzeln der Gleichung* $\alpha^\lambda = 1$ *gebildeten complexen Zahlen, für den Fall, daß die Klassenanzahl durch* λ *theilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*, Math. Abhand. Akad. Berlin (1857), 41–74 [datováno 4. 5. 1857]; [Kum21], 639–672.

[Kum17] KUMMER, E. E., *Über die allgemeinen Reciprocitätsgesetze der Potenzreste*, Monatsber. Berlin (1858), 158–171; [Kum21], 673–687.

[Kum18] KUMMER, E. E., *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, Crelle **56**(1859), 270–279; [Kum21], 688–697.

[Kum19] KUMMER, E. E., *Über die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*, Math. Abhand. Akad. Berlin (1859), 19–159; [Kum21], 699–839.

[Kum20] KUMMER, E. E., *Zwei neue Beweise der allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*, Math. Abhand. Akad. Berlin (1861), 81–122; Crelle **100**(1886), 10–50; [Kum21], 842–882.

[Kum21] KUMMER, E. E., *Collected Papers*, Springer Verlag, Berlin-Heidelberg-New York, 1975.

[Kür1] KÜRSCHÁK, J., *Über Limesbildung und allgemeine Körpertheorie*, in: *Proceedings of the Fifth International Congress of Mathematicians (Cambridge, 22.–28. 8. 1912)*, E. W.Hobson a A. E. H. Love, ed., Vol. 1, Cambridge University Press, Cambridge, 1913, 285–289.

[Kür2] KÜRSCHÁK, J., *Über Limesbildung und allgemeine Körpertheorie*, Crelle **142**(1913), 211–253.

[Lam1] LAMÉ, G., *Mémoire sur le dernier théorème de Fermat*, Comptes rendus **9**(1839), 45–46; rovněž v Jour. de Math. **5**(1840), 195–211; Mém. présentés divers savants Acad. sci. de l'Institut de France **8**(1843), 421–437.

[Lam2] LAMÉ, G., *Démonstration générale du théorème de Fermat sur l'impossibilité, en nombres entiers, de l'equation* $x^n + y^n = z^n$, Comptes rendus **24**(1847), 310–315.

[Lan1] LANDAU, E., *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, B. G. Teubner, Leipzig, 1918.

[Lür1] LÜROTH, J., *Beweis eines Satzes über rationale Curven*, Math. Ann. **9**(1875), 163–165.

[Mah1] MAHLER, K., *Über Pseudobewertungen I*, Acta Math. **66**(1936), 79–119.

[Mah2] MAHLER, K., *Über Pseudobewertungen II (Die Pseudobewertungen eines endlichen algebraischen Zahlkoerpers)*, Acta Math. **67**(1936), 51–80.

[Mah3] MAHLER, K., *Über Pseudobewertungen III*, Acta Math. **67**(1936), 283–328.

[Mah4] MAHLER, K., *Introduction to p-adic Numbers and Their Functions*, University Press, Cambridge, 1973.

[Nag1] NAGATA, M., *On the Theory of Henselian Rings*, Nagoya Math. Journal **5**, February (1953), 45–57.

[Ost1] OSTROWSKI, A., *Über einige Fragen der allgemeinen Körpertheorie*, Crelle **143**(1913), 255–284.

[Ost2] OSTROWSKI, A., *Über einige Lösungen der Funktionalgleichung* $\varphi(x).\varphi(y) = \varphi(xy)$, Acta Math. **41**(1918), 271–284.

[Ost3] OSTROWSKI, A., *Algebraische Funktionen von Dirichletschen Reihen*, Math. Zeit. **37**(1933), 98–133.

[Ost4] OSTROWSKI, A., *Untersuchungen zur arithmetischen Theorie der Körper (Die Theorie der Teilbarkeit in allgemeinen Körpern)*, Math. Zeit. **39**(1935), 269–404.

[Pet1] PETR, K., *O definici determinantu*, ČPMF **60**(1931), 201–213.

[Prü1] PRÜFER, H., *Untersuchungen über Teilbarkeitseigenschaften in Körpern*, Crelle **168**(1932), 1–38.

[Sch1] SCHILLING, O. F. G., *The Theory of Valuations*, AMS, New York, 1950.

[Scm1] SCHMIDT, F. K., *Mehrfach perfekte Körper*, Math. Ann. **108**(1933), 95–153.

[Soc1] SOCHOCKI, J., *Zasada największego wspólnego dzielnika w zastowaniu do teoryi podzielności liczb algebraicznych*, Prace matematyczne-fyz. **4** (1893), 95–153.

[Ste1] STEINITZ, E., *Algebraische Theorie der Körper*, Crelle **137**(1910), 167–309.

[Sni1] ŠNIRELMAN, L. G., *O funkcijach v normirovannych algebraičeski zamknutych polach*, Izvestija AN - Serija mat. **5/6**(1938), 487–498.

[Wae1] WAERDEN, B. L. VAN DER, *Moderne Algebra I, II*, Springer Verlag, Berlin, 1930, 1931.

[Web1] WEBER, H., *Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie*, Math. Ann. **43**(1893), 521–549.

[Web2] WEBER, H., *Lehrbuch der Algebra I, II*, Vieweg, Braunschweig, 1. vyd. 1895, 1896; 2. vyd. 1898, 1899.

[Wei1] WEIERSTRASS, K., *Neuer Beweiß des Satzes, daß jede ganze rationale Funktion dargestellt werden kann als ein Produkt aus linearen Funktionen derselben Veränderlichen*, Berichte über die Verhandlungen der Königl. Preußischen Akademie der Wissenschaften Berlin (1891), 1085–1101.

[Zol1] ZOLOTAREV, E. I., *Sur la méthode d'intégration de m. Tchébychev*, Math. Ann. **5**(1872), 560–581.

[Zol2] Zolotarev, E. I., *Théorie des nombres entiers complexes, avec une application au calcul intégral*, Petrohrad, 1874.

[Zol3] Zolotarev, E. I., *Sur les nombres complexes*, Bull. de St. Pétersb. V (1877).

[Zol4] Zolotarev, E. I., *Sur la théorie des nombres complexes*, Jour. de Math. (3^e série) **6**(1880), 51–84, 129–166.

Práce o tématu

[Bec1] Bečvář, J., *Soustavy lineárních rovnic a determinanty*, in: *Světonázorová výchova v matematice*, JČSMF, Praha, 1987, 187–217.

[Bel1] Bell, E. T., *The Developement of Mathematics*, McGraw-Hill, New York, 1940.

[Bou1] Bourbaki, N., *Éléments d'Histoire des Mathématiques*, Hermann, Paris, 1969; anglický překlad: *Elements of the History of Mathematics*, Springer Verlag, Berlin-Heidelberg-New York, 1994.

[Cas1] Cassels, J. W. S., *Local Fields*, Springer Verlag, Berlin-Heidelberg-New York, 1986.

[Cor1] Corry, L., *Modern Algebra and the Rise of Mathematical Structures*, Birkhäuser, Basel-Boston-Berlin, 1996.

[Čbo1] Čebotarev, N. G., *Ob osnovanii teorii idealov (po Zolotarevu)*, Izvestia fiz. mat. obščestva, Kazaň, **25**(1925), 1–14.

[Čbo2] Čebotarev, N. G., *The Foundations of the Ideal Theory of Zolotarev*, American Math. Monthly, **37**(1930), 117–118.

[Čbo3] Čebotarev, N. G., *Ob osnovanii teorii idealov*, Uspechi matematičeskich nauk **2**(1947), 52–67.

[Dic1] Dickson, L. E., *History of the Theory of Numbers*, vol. 2, Stechert, New York, 1934.

[Die1] Dieudonné, J., *Abrégé d'histoire des mathématiques 1700–1900*, Hermann, Paris, 1978; německý překlad *Geschichte der Mathematik 1700–1900*, Vieweg, Braunschweig, 1985.

[Edw1] Edwards, H. M., *The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes*, Archive **14**(1974/75), 219–236.

[Edw2] Edwards, H. M., *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*, Springer Verlag, Berlin-Heidelberg-New York, 1977.

[Edw3] Edwards, H. M., *The Genesis of Ideal Theory*, Archive **23**(1980), 321–378.

[Edw4] Edwards, H. M.; Neumann, O.; Purkert, W., *Dedekind's „Bunte Bemerkungen" zu Kroneckers „Grundzüge"*, Archive **27**(1982), 50–85.

[Edw5] Edwards, H. M., *Divisor Theory*, Birkhäuser, Boston, 1990.

[Eic1] Eichler, M., *Einführung in die Theorie der algebraischen Zahlen und Funktionen*, Birkhäuser, Basel, 1963; anglický překlad: Academic Press, New York, 1966.

[End1] Endler, O., *Valuation Theory*, Springer Verlag, Berlin-Heidelberg-New York, 1972.

[Fla1] Flanders, H., *The Meaning of the Form Calculus in Classical Ideal Theory*, Trans. AMS, **95**(1960), 92–100.

[F-T1] Fröhlich, A.; Taylor, M. J., *Algebraic Number Theory*, Cambridge University Press, Cambridge, 1991.

[Gou1] Gouvêa, F. Q., *p-adic Numbers. An Introduction*, Springer Verlag, Berlin-Heidelberg, 1993.

[Jan1] Janusz, G. J., *Algebraic Number Fields*, Academic Press, USA, 1973; 2. vyd. AMS, 1996 [odkazy v textu jsou na 2. vydání].

[Kli1] Kline, M., *Mathematical Thought from Ancient to Modern Times*, Oxford University Press, New York, 1972.

[Koc1] Kochendörffer, R., *Einführung in die Algebra*, Deutscher Verlag der Wissenschaften, Berlin, 1955; 2. vyd. 1966.

[K-J1] Kolmogorov, A. N.; Juškevič, A. P., ed., *Matematika XIX veka: Matematičeskaja logika, algebra, teorija čisel, teorija verojatnostej*, Izdatelstvo Nauka, Moskva, 1978; anglický překlad: *Mathematics of the 19th Century: mathematical logic, number theory, probability theory*, Birkhäuser, Basel, 1992.

[Kra1] Kraemer, P., *Zákon reciprocity v teorii čísel*, in: *Člověk–Umění–Matematika*, Prometheus, Praha, 1990, 179–186.

[Nar1] Narkiewicz, W., *Elementary and Analytic Theory of Algebraic Numbers*, Pastwowe wydawnictwo naukowe, Warszawa, 1974.

[Neu1] Neumann, O., *Über die Anstöße zu Kummers Schöpfung der "Idealen Complexen Zahlen"*, in: *Mathematical Perspectives, Essays on Mathematics and Its Historical Development*, Academic Press, New York-London-Toronto-Sydney-San Francisco, 1981 [J. W. Dauben, ed.], 179–199.

[Ono1] Ono, T., *An Introduction to Algebraic Number Theory*, Plenum Press, New York, 1990.

[Pro1] Procházka, L. a kol., *Algebra*, Academia, Praha, 1990.

[Rib1] Ribenboim, P., *Equivalent Forms of Hensel's Lemma*, Expositiones Mathematicae **3**(1985), 3–24.

[Rib2] Ribenboim, P., *The Theory of Classical Valuations*, Springer Verlag, New York-Berlin-Heidelberg, 1998.

[Rib3] Ribenboim, P., *Fermat's Last Theorem for Amateurs*, Springer Verlag, New York-Berlin-Heidelberg, 1999.

[Roq1] Roquette, P., *On the History of Valuation Theory. Part I*, in: *Valuation Theory and its applications*, vol. I, Fields Institute Communications, 2002, 291–355 [F. V. Kuhlmann; S. Kuhlmann; M. Marshall, ed.; rukopis je k dispozici na internetové adrese: *http://www.rzuser.uni-heidelberg.de/~ci3/manu.html*].

[Ser1] Serre, J. P., *Local Fields*, Springer Verlag, Berlin-Heidelberg-New York, 1979.

[Wey1] Weyl, H., *Algebraic Theory of Numbers*, Princeton Univ. Press, Princeton, 1940.

[Wie1] Więsław, W., *Analiza niearchimedesowska i ciała liczb p-adycznych*, Roczniki polskiego towarystwa matematycznego, Seria II: Wiadomości matematyczne **9**(1970), 221–234.

[Wie2] Więsław, W., *Topological Fields*, Marcel Dekker, New York, 1988.