Časopis pro pěstování mathematiky a fysiky

Karel Rychlík

Příspěvek k theorii těles

Časopis pro pěstování mathematiky a fysiky, Vol. 48 (1919), No. 3-4, 145--165

Persistent URL: http://dml.cz/dmlcz/121292

Příspěvek k theorii těles.

Dr. **Karel Rychlík.**

Úvod. Těleso, ohodnocení, limita, posloupnost konvergentní, těleso ohodnocené perfektní. Vytčení základního úkolu: Ohodnocení prvků algebraických vzhledem k tělesu ohodnocenému.

§ 1. Obecná theorie těles zabývá se pojmem *tělesa* jako soustavy prvků se dvěma početními úkony, sčítáním a násobením, které splňují zákon associativní a kommutativní, jsou spojeny zákonem distributivním a připouštějí inversní úkony, odčítání a dělení, jednoznačné a, až na dělení nullou, vždy proveditelné.*) Jsou tedy tělesa obory, v nichž pro počítání platí pravidla známá z počátků algebry.

Dále možno sevšeobecniti pojem absolutní hodnoty a na tomto základě i limity a konvergence.

Nazveme *ohodnocením***) číslo reálné $\|a\|$, přiřaděné každému prvku a z tělesa K, tak že jsou splněny podmínky:

I. $\|0\| = 0$ *a při* $a \neq 0$ *je* $\|a\| > 0$,

II. $\|ab\| = \|a\| \cdot \|b\|$,

III. $\|1 + a\| \leqq 1 + \|a\|$,

a konečně, nechceme li přihlížeti k triviálnímu případu, kdy $\|0\| = 0$, $\|a\| = 1$ pro každý jiný prvek $(a \neq 0)$ z tělesa,

IV. *v tělese je aspoň jeden prvek takový, že pro něj* $\|a\| \neq 1$.

Těleso, v němž takovéto přiřadění provedeno, nazveme *ohodnoceným*.

---

*) Viz Weber, Math. Ann. 43. str. 521 a Steinitz, Crelles Journ. 137. str. 167. Výsledky této práce v násl. předpokládám a terminologii tam zavedenou užívám.

**) Bewertung; viz Kürschák, Crelles Journ. 142, 1913, § 1—23.

Z II. plyne, klademe-li $\frac{a}{b}$ místo a, že 1.) $\left\|\frac{a}{b}\right\| = \frac{\|a\|}{\|b\|}$ pro $b \neq 0$. Dále dostaneme ze II., pro $b = 1$, že 2.) $\|1\| = 1$ a pro $a = b = -1$, že 3.) $\|-1\| = 1$ a tedy 4.) $\|-a\| = \|a\|$.

Z II. a III. pak plyne $\|a+b\| \leqq \|a\| + \|b\|$.

Speciální případ ohodnocení, tak zvané *ohodnocení nearchimedické,* dostaneme, je-li místo III. splněna podmínka:

III′ *pro* $\|a\| \leqq 1$ *je* $\|1+a\| \leqq 1$.

Z II. a III′ dostaneme pak, klademe-li b/a místo a,

5.) $\|a+b\| \leqq \mathrm{Max}\,(\|a\|,\ \|b\|)$, z toho pak

6.) $\|a+b+c+\ldots\| \leqq \mathrm{Max}\,(\|a\|,\ \|b\|,\ \|c\|,\ldots)$

a pro celé číslo kladné n,

7.) $\|n\| \leqq 1$.

Je-li však $\|a\| \neq \|b\|$, platí místo 5.) přesněji 5′.) $\|a+b\| = \mathrm{Max}\,(\|a\|,\ \|b\|)$. Dejme tomu, že 8.) $\|a\| > \|b\|$. Dle 5.) je 9.) $\|a+b\| \leqq \|a\|$. Avšak, klademe-li do 5.), $a+b$ místo a, $-b$ místo b, dostaneme 10) $\|a\| \leqq \mathrm{Max}\,(\|a+b\|,\ \|b\|)$. Není možno, aby $\|b\| \leqq \|a+b\|$, ježto by pak z poslední nerovnosti 10.) plynulo $\|a\| \leqq \|b\|$ proti předpokladu 8.). Musí tedy býti $\|b\| < \|a+b\|$, pak plyne z 10.) $\|a\| \leqq \|a+b\|$, což zároveň s 9.) poskytuje, j. b. d. $\|a+b\| = \|a\|$.

§ 2. V tělese ohodnoceném lze definovati *limitu posloupnosti a posloupnost konvergentní* právě tak, jako je to obvyklé v Cantor-Mérayově theorii čísel irracionálných.

Posloupnost prvků $a_1, a_2, \ldots a_n \ldots$ z tělesa K má za limitu prvek a z K, $a = \lim\limits_{n=\infty} a_n$, je-li možno přiřaditi k libovolně malému (reálnému) číslu kladnému ε takové celé číslo kladné N, že pro všechna $n > N$ platí $\|a_n - a\| < \varepsilon$.*)

Posloupnost prvků $a_1, a_2, \ldots a_n, \ldots$ z tělesa K je konvergentní, je-li možno přiřaditi ke každému libovolně malému číslu kladnému ε takové číslo kladné N, že platí $\|a_{n+k} - a_n\| < \varepsilon$. pro všechna $n > N$ a pro všechna celá čísla kladná k.

V tělesech nearchimedických nastane zjednodušení. Při podmínce konvergence stačí, aby byla splněna pro $k = 1$; po-

*) t. j. $\lim\limits_{n=\infty} \|a_n - a\| = 0$, značí-li $\lim$ limitu v obyčejném slova smyslu pro číslo reálné.

sloupnost je konvergentní, je-li možno k libovolně malému číslu kladnému ε určiti takové celé číslo kladné N, že $\|a_{n+1}-a_n\|<\varepsilon$ pro $n>N$, nebo-li, ke konvergenci posloupnosti stačí, aby $\lim_{n=\infty} a_{n+1}-a_n)=0$.*)

Je-li totiž $\|a_{n+1}-a_n\|<\varepsilon$ pro $n>N$, je

$$\|a_{n+k}-a_n\|=\|(a_{n+k}-a_{n+k-1})+\ldots+(a_{n+1}-a^n)\|$$
$$\leqq \mathrm{Max}\,(\|a_{n+k}-a_{n+k-1}\|,\ldots\|a_{n+1}-a_n\|)<\varepsilon.$$

Aby posloupnost měla limitu, musí býti nutně konvergentní. Opak však vždy neplatí. Nazveme-li tělesa, v nichž má každá konvergentní posloupnost limitu, *perfektními*, eksistují skutečně tělesa neperfektní. Možno však v tělese neperfektním přiřaditi každé posloupnosti konvergentní nový prvek jako limitu, pro tyto prvky definovati rovnost, sčítání, odčítání, násobení a dělení, takže tvoří těleso K', *derivované těleso* tělesa K, tělesu K nadřaděné. Je-li K těleso perfektní, je těleso derivované K' totožno s K. Lze pak ukázati, že pro každé těleso K je těleso derivované, K', perfektní, t. j. $K''=(K')'=K'$.

§ 3. Uveďme příklady na ohodnocení těles.

Těleso čísel racionálných, reálných, Gaussovo těleso (tvořené čísly kompleksními $a+ib$, kdež a, b jsou čísla racionálná), těleso čísel kompleksních lze ohodnotiti pomocí absolutní hodnoty. Těleso čísel racionálných a těleso Gaussovo nejsou perfektní; derivováním vznikne těleso čísel reálných a těleso čísel kompleksních, kterážto tělesa jsou perfektní.

Nearchimedická ohodnocení tělesa čísel racionálných dostaneme takto: Každé číslo racionálné lze psáti ve tvaru $a=p^r u/v$, kdež p je prvočíslo, u, v čísla celá nedělitelná p, r číslo celé. Položme $\|a\|=c^r$, $0<c<1$.**) Těleso derivované je těleso Henschlových čísel p-adických.***)

*) t. j. $\lim_{n=\infty}\|a_{n+1}-a_n\|=0$.

Z toho lse snadno odvoditi další důsledky: Ke konvergenci nekonečné řady stačí již, aby její členy měly za limitu nullu. Součet nekonečné řady se nezmění, provedeme-li libovolné přemístění jejích členů.

**) Tato ohodnocení a pak svrchu uvedená pomocí absolutní hodnoty jsou jedině možná ohodnocení tělesa čísel racionálných; viz Ostrowski, Acta mathem. 41, 1917, str. 271.

***) Důkaz viz Kürschák, l. c. § 19—23.

§ 4. Můžeme si nyní položiti otázku: *Lze algebraické rozšíření ohodnoceného tělesa K tak ohodnotiti, aby ohodnocení původního tělesa K zůstalo zachováno?* Každý prvek nadřaděného tělesa algebraického je kořenem jediné rovnice algebraické s koeficienty z původního tělesa a v něm nerozložitelné. Nazveme ji *definující rovnicí* onoho prvku. Budeme požadovati, aby *prvky definované toutéž rovnicí měly stejné ohodnocení.* I je pak patrno, že prvek α definovaný rovnicí $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, je-li úloha daná vůbec řešitelná, musí býti takto ohodnocen: $\|\alpha\| = \|a_n\|^{\frac{1}{n}}$ Jsou však splněny podmínky II. a III.? Důkaz, že splněna podmínka II., je snadný. Aby podmínka III. vůbec mohla býti splněna, dlužno o tělese ohodnoceném K předpokládati, že je perfektní.

Kürschák užívá pak k tomu důkazu theorie potenčních řad a vět Hadamardových. Klade však otázku, zda by snad pro tělesa nearchimedická nebylo možno provésti důkaz snadněji methodou podobnou oné, které používá Hensel *) pro algebraické rozšíření tělesa čísel p-adických. O to se pokouším v tomto pojednání. Stačí však také úplně, zabývati se pouze případem ohodnocení nearchimedického. Ostrowski totiž ukázal, že těleso K, pro něž definováno ohodnocení, které není nearchimedické, je nutně isomorfní s jistým podtělesem $\bar{K}$ tělesa čísel kompleksních a jestliže prvku a z K odpovídá prvek $\bar{a}$ z $\bar{K}$, je $\|a\| = |\bar{a}|^{\varrho}$, $0 < \varrho < 1$. Pro taková tělesa však můžeme problém ohodnocení pokládati za rozřešený.

Prvky celé, dělitelnost, kongruence v tělese ohodnoceném.

§ 5. Uvažujme těleso ohodnocené **) K. Prvky, jichž ohodnocení je $\leqq 1$, tvoří obor celistvosti J: je-li totiž $\|a\| \leqq 1$, $\|b\| \leqq 1$ je též $\|a \pm b\| \leqq$ Max $(\|a\|, \|b\|) \leqq 1$, $\|ab\| = \|a\| \cdot \|b\| \leqq 1$.

Každý prvek z tělesa K je podílem dvou prvků z J; dokonce, nepatří-li do J, tak že má ohodnocení > 1, patří jistě jeho převratná hodnota do J. Prvky z J nazveme *celými*

*) Hensel, Theorie d. algebr. Zahlen.

**) nearchimedicky. V dalším budu uvažovati pouze ohodnocení nearchimedická.

prvky z K. 1.) Je patrno, že z prvků a a $1/a$ je aspoň jeden celý. 2.) Jsou-li oba celé, což nastane u prvků, jichž ohodnocení je 1, nazveme prvek takový *jednotkou*. Také můžeme zavésti pojem *dělitelnosti*. 3.) Prvek a je dělitelný prvkem $b\,(\neq o)$, je-li jich podíl a/b prvek celý. Ihned je patrna platnost vět: 4.) Je-li prvek a dělitelný prvkem b, prvek b prvkem c, je prvek a dělitelný prvkem c. 5.) Je-li prvek a dělitelný prvkem d, prvek k celý, je též ak dělitelno d. 6.) Jsou-li prvky a, b dělitelny d, je též $a \pm b$ dělitelno d. 7.) Je-li prvek a dělitelný b a též prvek b dělitelný a, nazveme *prvky* a, b spolu *associovanými*. 8.) Dva prvky jsou spolu associované tehdy a jen tehdy, mají-li rovná ohodnocení. 9.) Jednotky jsou prvky associované s 1. 10.) Podíl dvou prvků spolu associovaných je jednotka. 11.) Pro prvky $a, b, c, \ldots$ eksistuje vždy prvek, jich *největší společná míra* $(a, b, c, \ldots)$, té vlastnosti, že každý společný dělitel prvků $a, b, c, \ldots$ je dělitelem tohoto prvku $(a, b, c, \ldots)$. Pro tento prvek je $\|(a, b, c, \ldots)\| = \mathrm{Max}\,(\|a\|, \|b\|, \|, \|c\|, \ldots)$. 12. Podobně eksistuje prvek, *nejmenší společný násobek* $[a, b, c, \ldots]$ prvků $a, b, c, \ldots$, který má tu vlastnost, že všechny prvky dělitelné jak a, tak b, tak $c \ldots$ jsou dělitelny $[a, b, c, \ldots]$. Pro ten je $\|[a, b, c \ldots]\| = \mathrm{Min}\,(\|a\|, \|b\|, \|c\|, \ldots)$.

§ 6. Uvažujme v tělese ohodnoceném K prvky celé nejednotkové: jich ohodnocení je < 1. Je-li mezi nimi prvek p, který má největší ohodnocení, lze všechny prvky z tělesa K vyjádřiti ve tvaru ep^r, kdež e je jednotka a r racionálné celé číslo. Pro prvky celé je pak $r \leq 0$, pro jednotky $r = 0$. Důkaz: Hlavní hodnoty $\log \|a\|$, $\log \|p\|$ $(\neq 0)$ jsou čísla reálná. I lze klásti $\log \|a\| = r \log \|p\| + s$, kdež r je číslo celé a $0 \leq s < \log \|p\|$. I bude $\|a\| = \|p\|^r e^s$, $1 \leq e^s < \|p\|$. Položme $a = p^r c$. Pak bude $1 \leq \|c\| < \|p\|$. Nutně pak musí býti $\|c\| = 1$, poněvadž prvek p má míti mezi prvky s ohodnocením < 1, ohodnocení největší. Tím tvrzení dokázáno.

Prvek p má tu vlastnost, že, je-li jím dělitelný součin ab, je jím pak dělitelný aspoň jeden z činitelů a, b. Proto ho nazveme *prvoprvkem* a těleso, v němž se prvek takový vyskytuje, nazveme *tělesem s prvoprvkem*.

§ 7. Zaveďme nyní pro prvky celé z tělesa ohodnoceného K pojem *kongruence*. Budiž m prvek celý nejednotkový, $\|m\| < 1$. Pak $a \equiv 0 \pmod{m}$ je-li a dělitelno m, t. j. $\|a\| \leqq \|m\|$. $a \equiv b \pmod{m}$ znamená, že $a - b \equiv 0 \pmod{m}$. I. Snadno lze ukázati, že takto zavedená kongruence je vztah reflexivní ($a \equiv a \pmod{m}$), symetrický (z $a \equiv b \pmod{m}$ plyne $b \equiv a \pmod{m}$), transitivní (z $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ plyne $a \equiv c \pmod{m}$). I lze prvky celé z tělesa K rozděliti na třídy spolu kongruentních mod m. II. Je-li $a \equiv b \pmod{m}$, je též $a \equiv b \pmod{m'}$, kdež m' je dělitel m : $\|m\| < \|m'\|$. III. Dále plyne z kongruencí $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, že α) $a \pm c \equiv b \pm d \pmod{m}$, β) $ac \equiv bd \pmod{m}$. γ) Z kongruence $ae \equiv be \pmod{m}$ plyne $a \equiv b \pmod{m}$, je-li e prvek jednotkový. Na základě toho lze pro třídy mod m definovati sčítání, odčítání a násobení.*)

Můžeme však uvažovati ještě *jiný druh kongruencí*. Budiž m prvek celý: $\|m\| \leqq 1$. I budeme definovati: $a \equiv 0 \pmod{m}^*$, je-li $\|a\| < \|m\|$. $a \equiv b \pmod{m}^*$, je-li $a - b \equiv 0 \pmod{m}^*$. I* Je ihned patrno, že i tato kongruence je vztah reflexivní a symmetrický; je to však též vztah transitivní: z $a \equiv b$, $b \equiv c \pmod{m}^*$, t. j. $\|a - b\| < \|m\|$, $\|b - c\| < \|m\|$, plyne $\|a - c\| = \|(a-b) + (b-c)\| \leqq \text{Max}\,(\|a-b\|, \|b-c\|) < \|m\|$, tedy $a \equiv c \pmod{m}^*$. Zase je možno provésti rozdělení na třídy $\pmod{m}$.* II* Je-li $a \equiv b \pmod{m}^*$ je též $a \equiv b \pmod{m'}^*$, kdež m' je dělitel m, $\|m\| \leqq \|m'\|$. III* Z kongruencí $a \equiv b \pmod{m}^*$, $c \equiv d \pmod{m}^*$, plyne α) $a \pm c \equiv b \pm d \pmod{m}^*$, β) $ac \equiv bd \pmod{m}^*$.

Důkaz: $a \equiv b \pmod{m}^*$, $c \equiv d \pmod{m}^*$ znamená, že $\|a - b\| < \|m\|$, $\|c - d\| < \|m\|$. Pak je $\|a \pm c - (b \pm d)\| = \|(a-b) \pm (c-d)\| \leqq \text{Max}\,(\|a-b\|, \|c-d\|) < \|m\|$

t. j. $a \pm c \equiv b \pm d \pmod{m^*}$

$\|ac - bd\| = \|(a-b)\,d + (c-d)\,b + (a-b)\,(c-d)\| \leqq \text{Max}\,(\|a-b\|\,\|d\|, \|c-d\|\,\|b\|, \|a-b\|\,\|c-d\|) < \|m\|$

*) Třídy ty pak tvoří okruh; v něm jsou dělitelé nully prvky celé nejednotkové, prvky pravidelné jsou jednotky.

Kongruenci lze definovati pro všechny prvky z tělesa ohodnoceného K. Pak platí I., II., III. α) γ), III. β) neplatí; místo toho lze tvrditi: Je-li $a \equiv b \pmod{m}$, k prvek celý, je $ak \equiv bk \pmod{m}$. Třídy mod m tvoří pak modul.

tak že skutečně $ac \equiv bd$ (mod m)*. γ) Konečně plyne z kongruence $ac \equiv be$ (mod m)*, kdež e je jednotka, že $a \equiv b$ (mod m)*. Na základě toho lze snadno pro třídy (mod m)* definovati sčítání, odčítání a násobení.

Snadno lze ukázati, že *třídy* (*mod* 1)* *tvoří těleso.* Aby tomu tak bylo, nutno dokázati, že kongruence $ax \equiv b$ (mod 1)* má jediné řešení (mod 1)*, není-li $a \equiv 0$ (mod 1)*. Z této podmínky totiž plyne, že a je jednotka, takže z III*γ) plyne existence řešení $x \equiv b/a$ (mod 1)*. Důkaz, že je to řešení jediné (mod 1)* je pak již zcela snadný.*)

Pro těleso ohodnocené s prvoprvkem p je kongruence (mod p^r)* totožná s kongruencí (mod p^{r+1}) a speciálně kongruence (mod 1)* totožná s kongruencí (mod p). Tvoří tedy třídy (mod p) těleso.

Mnohočleny s koeficienty z tělesa ohodnoceného. Několik vět o resultantu a diskriminantu.

§ 8. Budeme uvažovati mnohočleny v proměnné x s koefficienty z tělesa ohodnoceného K: $f(x) = a_0 x^\mu + a_1 x^{\mu-1} + \ldots + a_\mu$. Takový mnohočlen s koefficienty celými bude *primitivní*, budou-li míti koefficienty za největší společnou míru jednotku, což nastane tehdy a jen tehdy, je-li jeden z nich jednotkou. Libovolný mnohočlen lze pak psáti ve tvaru $f(x) = df_0(x)$, kdež d je největší společná míra koefficientů a $f_0(x)$ mnohočlen primitivní. Aby pak měl mnohočlen celé koefficienty je nutno a postačí, aby d bylo celé, $\|d\| \leqq 1$.

Nazveme dva *mnohočleny* s celými koefficienty *kongruentní* (identicky) (mod m) a (mod m)*, platí-li tatáž kongruence pro příslušné jejich koefficienty.

Mnohočlen s celými koefficienty $f_0(x)$ je primitivní tehdy a jen tehdy, není-li $\equiv 0$ (mod 1)*, tak že lze pak psáti $f_0(x) \equiv f_0^*(x)$ (mod m)*, $f_0^*(x) = a_0^* x^\lambda + a_1^* x^{\lambda-1} + \ldots + a_\lambda^*$, $a_0^* \neq 0$. Je-li $g_0(x)$ jiný primitivní mnohočlen, tak že $g_0(x) \equiv$

) Není-li m jednotka, tvoří třídy (mod m) pouze okruh; dělitelé nully jsou prvky celé nejednotkové, prvky pravidelné jsou jednotky. Také kongruenci (mod m)* lze definovati pro všechny prvky z tělesa ohodnoceného K. Zase platí I*), II*), III* α) γ) a místo III* β): Je-li $a \equiv b$ (mod m)*, k prvek celý, je $ak \equiv bk$ (mod m). Třídy (mod m)* tvoří pak modul.

$\equiv g_0^*(x) \pmod{1}^*, g_0^*(x) = b_0^* x^\mu + b_1^* x^{\mu-1} + \ldots + a^{\mu *}, b_0^* \neq 0$, bude platiti pro součin $f_0(x) g_0(x) \equiv f_0^*(x) g_0^*(x) \equiv a_0^* b_0^* x^{\mu+\nu} + \ldots$, $a_0^* b_0^* \neq 0$, tak že to je primitivní mnohočlen. Platí tedy věta: *Součin dvou primitivních mnohočlenů z tělesa ohodnoceného je zase mnohočlen primitivní v K.*

Dále platí věta:

Je-li primitivní mnohočlen rozložitelný v tělese ohodnoceném K, dá se rozložiti na činitele primitivní v K.

Důkaz stačí provésti pro případ, že primitivní mnohočlen $f_0(x)$ se rozpadá na dva činitele z K, $f_0(x) = g(x) h(x)$. I lze psáti $g(x) = a g_0(x)$, $h(x) = b h_0(x)$, kdež $g_0(x)$, $h_0(x)$ jsou mnohočleny primitivní. Pak $f_0(x) = a b g_0(x) h_0(x)$. Součin $g_0(x) h_0(x)$ je mnohočlen primitivní. Je tedy součin ab nutně jednotkou a tím věta dokázána.

Mnohočlen tvaru $x^\mu + a_1 x^{\mu-1} + \ldots + a_\mu$, kdež koefficienty $a_1, a_2 \ldots a_\mu$ jsou celé, je jistě primitivní. Z předcházející věty pak plyne, že, je-li takový mnohočlen rozložitelný, dá se jistě rozložiti na činitele podobného tvaru, u nichž tedy koefficient u nejvyšší mocniny x je 1, ostatní koefficienty jsou prvky celé.

§ 9. Uvedeme několik vět o *resultantu* a *diskriminantu.*

Pro mnohočleny z libovolného tělesa $g(x) = a_0 x^\mu + a_1 x^{\mu-1} + \ldots + a_\mu$, $h(x) = b_0 x^\nu + b_1 x^{\nu-1} + \ldots + b_\nu$ definujeme resultant pomocí determinantu

$$R(g, h) = \begin{vmatrix} a_0, & a_1, & \ldots & a_\mu, & 0, & \ldots & 0 \\ 0, & a_0, & a_1, & \ldots & a_\mu, & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & \ldots & 0, & a_0, & a_1, \ldots & a_\mu \\ b_0, & b_1, & \ldots & b_\nu, & 0, & \ldots & 0 \\ 0, & b_0, & b_1, & \ldots & b_\nu, & \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & \ldots & 0, & b_0, & b_1, \ldots & b_\nu \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} (\nu \text{ řádek}) \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} (\mu \text{ řádek}) \end{matrix}$$

$R(g, h) = 0$ je pak nutná a postačující podmínka, aby mnohočleny g, h měly největší společnou míru stupně $\geqq 1$. I platí rovnice:

$$R(x - \xi, h(x)) = h(\xi)$$
$$R(g, h) = (-1)^{\mu\nu} R(h, g)$$
$$R(g_1 g_2, h) = R(g_1, h) R(g_2, h).$$

Lze je dokázati transformacemi determinantů.

Jednodušeji však možno provésti důkaz, uvažujeme-li vhodné algebraické rozšíření tělesa koefficientů.

Platí-li pro $g(x)$ a $h(x)$ rozklad v kořenové činitele $g(x) = a_0(x-\xi_1)(x-\xi_2)\dots(x-\xi_\mu)$, $h(x) = b_0(x-\eta_1)(x-\eta_2)\dots(x-\eta_\nu)$ je pak

$$R(g,h) = a_0^\nu b_0^\mu \prod_{i=1}^{\mu}\prod_{k=1}^{\nu}(\xi_i - \eta_k) = a_0^\nu \prod_{i=1}^{\mu} h(\xi_i) = (-1)^{\mu\nu} b_0^\mu \prod_{k=1}^{\nu} f(\eta_k).$$

Diskriminant je resultant mnohočlenu $f(x)$ a jeho derivace $f'(x)$, $D(f) = R(f, f')$. $D(f) = 0$ je nutná a postačující podmínka, aby mnohočlen $f(x)$ měl mnohonásobné kořeny. Je-li $f(x) = g(x)h(x)$, kdež $g(x)$ je stupeň μ, $h(x)$ stupně ν, je $D(f) = (-1)^{\mu\nu} D(g) D(h) (R(g,h))^2$.

Pro $f(x) = a_0(x-\xi_1)\dots(x-\xi_n)$ je

$$D(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{2\mu-1}(\xi_1-\xi_2)^2(\xi_1-\xi_2)^2\dots(\xi_1-\xi_\mu)^2\dots(\xi_{n-1}-\xi_n)^2.$$

§ 10. Buďtež $g(x) = a_0 x^\mu + a_1 x^{\mu-1} + \dots + a_\mu$, $h(x) = b_0 x^\nu + b_1 x^{\nu-1} + \dots b_\nu$ dva nesoudělné mnohočleny s koefficienty z tělesa K. Resultant $r = R(g, h)$ je různý od nully. Budiž $F(x) = c_0 x^{\mu+\nu-1} + c_1 x^{\mu+\nu-2} + \dots + c_{\mu+\nu-1}$ mnohočlen s koefficienty z K. Pak lze určiti a sice jednoznačně, mnohočleny $g_1(x)$, $h_1(x)$ stupně $\mu - 1$ a $\nu - 1$

$$g_1(x) = a'_0 x^{\mu-1} + a'_1 x^{\mu-2} + \dots + a'_{\mu-1},$$
$$h_1(x) = b'_0 x^{\nu-1} + b'_1 x^{\nu-2} + \dots + b'_{\nu-1},$$

tak že $F(x) = g(x)h_1(x) + h(x)g_1(x)$. Proveďme na pravé straně násobení a srovnejme koefficienty μ stejných mocnin x. Dostaneme $\mu + \nu$ rovnic lineárních

$$\begin{aligned} a_0 b_0 \qquad\quad & + b_0 a_0' & = c_0 \\ a_1 b'_0 + a_0 b_1 & + b_1 a'_0 + b_0 a'_1 & = c_1, \end{aligned}$$

jichž determinant je právě resultant $R(g, h)$, tedy $\neq 0$. Předpokládejme nyní, že koefficienty a_i, b_k, c_c jsou celé prvky z tělesa ohodnoceného. Z oněch lineárních rovnic jsou koefficienty a'_i, b'_k určeny jako zlomky o společném jmenovateli $R(g, h) = r$ a čitatelích vyjádřených jako lineární, homogenní funkce $c_0, c_1, \dots c_{\mu+\nu-1}$ s celými koefficienty. Je-li $F(x) = \varrho F_0(x)$, kdež $F_0(x)$ je primitivní mnohočlen, jsou a'_i, b'_k jistě dělitelny aspoň ϱ/r. V případě, že ϱ/r je celé, tedy $\|\varrho\| \leqq \|r\|$. mají mnohočleny $f_1(x)$, $g_1(x)$ celé koefficienty. I platí věta:

Jsou li $g(x)$, $h(x)$ mnohočleny s celými koefficienty z ohodnoceného tělesa stupně μ a ν, nesoudělné, tak že jich resultant $r \neq 0$, lze libovolný mnohočlen stupně nižšího než $\mu+\nu$, $F(x) = \varrho F_0(x)$, kdež $F_0(x)$ je mnohočlen primitivní, $\|\varrho\| \leqq \|r\|$, znázorniti jednoznačně ve tvaru $F(x) = g(x)h_1(x) + h(x)g_1(x)$, při čemž stupně mnohočlenů $g_1(x)$ a $h_1(x)$ jsou resp. menší než μ a ν a jich koefficienty celé a dělitelny aspoň ϱ/r.

Jako speciální případ této věty uveďme:

Jsou-li $g(x)$, $h(x)$ mnohočleny s celými koefficienty z tělesa ohodnoceného K, stupně μ a ν, jichž resultant je jednotka, pak lze každý mnohočlen $F(x)$ stupně menšího než $\mu+\nu$ s celými koefficienty znázorniti ve tvaru $F(x) = g(x)h_1(x) + h(x)g_1(x)$, kdež mnohočleny $h_1(x)$ a $g_1(x)$ mají celé koefficienty a stupně resp. menší než μ a ν.

Rozklad mnohočlenů v tělese ohodnoceném perfektním.

§ 11. *Platí-li pro mnohočlen $f(x)$ s celými koefficienty z tělesa ohodnoceného perfektního K kongruence 1.) $f(x) \equiv g_0(x)h_0(x) \pmod{r^2}^*$, kdež $g_0(x)$ a $h_0(x)$ jsou mnohočleny s celými koefficienty z K stupně $\geqq 1$ a $r \neq 0$ jich resultant, je též 2.) $f(x) = g(x)h(x)$, kdež $g(x)$ a $h(x)$ jsou mnohočleny s celými koefficienty z K stejného stupně jako $g_0(x)$ resp. $h_0(x)$ a platí 3.) $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x) \pmod{r}^*$. Mimo to je $\|R(g,h)\| = \|R(g_0,h_0)\|$.*

Z kongruence 1.) plyne eksistence takového m, jehož ohodnocení je <1, že 4.) $f(x) \equiv g_0(x)h_0(x) \pmod{mr^2}$. Při tom $\|R(g_0,h_0)\| = \|r\|$. Dokážeme si nejprvé, že na základě toho lze určiti mnohočleny $g_1(x)$, $h_1(x)$ stejného stupně jako $g_0(x)$ resp. $h_0(x)$, tak že 5.) $f(x) \equiv g_1(x)h_1(x) \pmod{m^2r^2}$, 6.) $g_1(x) \equiv g_0(x)$, $h_1(x) \equiv h_0(x) \pmod{mr}$ a pro resultant $R(g_1,h_1)$ platí $\|R(g_1,h_1)\| = \|r\|$.

Položme 7.) $g_1(x) = g_0(x) + m\bar{g}_1(x)$, $h_1(x) = h_0(x) + m\bar{h}_1(x)$. Aby platila kongruence 5.), musí býti

$$8.)\ \frac{f(x) - g_0(x)h_0(x)}{m} \equiv \bar{h}_1(x)g_0(x) + \bar{g}_1(x)h_0(x) + m\bar{g}_1(x)\bar{h}_1(x)$$

(mod mr^2). Dle věty z § 10. lze určiti jednoznačně mnohočleny $\overline{g}_1(x)$, $\overline{h}_1(x)$, tak že

$$9.)\quad \frac{f(x)-g_0(x)h_0(x)}{m} \equiv \overline{h}_1(x)\,g_0(x)+\overline{g}_1(x)\,h_0(x).$$

Označme ϱ největší společnou míru koefficientů mnohočlenu na levé straně v 9.). Ze 4.) plyne, že $\|\varrho\| \leqq \|r^2\|$. Mnohočleny $\overline{g}_1(x)$, $\overline{h}_1(x)$ budou stupňů resp. menších než stupně mnohočlenů $g_0(x)$, $h_0(x)$. Jejich koefficienty budou celé a budou míti ohodnocení $\leqq \|\varrho/r\| \leqq \|r\|$. Bude tedy 10.) $\overline{g}_1(x) \equiv \overline{h}_1(x) \equiv 0$ (mod r), $\overline{g}_1(x)\overline{h}_1(x) \equiv 0$ (mod r^2). I plyne z platnosti rovnice 9.), že $\overline{g}_1(x)$ a $\overline{h}_1(x)$ splňují kongruenci 8.). Pak je také splněna kongruence 5.). $g_1(x)$, $h_1(x)$ mají stejný stupeň jako resp. $g_0(x)$ a $h_0(x)$. Ze 7.) a 10.) plyne pak platnost 6.). Z 6.) plyne, že $R(g_1, h_1) \equiv R(g_0, h_0)$ (mod mr) a ježto $\|R(g_0, h_0)\| = \|r\|$, je též $\|R(g_1, h_1)\| = \|r\|$.

Podobně dokážeme dále eksistenci mnohočlenů $g_2(x)$, $h_2(x)$ stejného stupně jako $g_1(x)$, $h_1(x)$, tak že $f(x) \equiv g_2(x)\,h_2(x)$ (mod $m^4 r^2$), $g_2(x) \equiv g_1(x)$, $h_2(x) \equiv h_1(x)$ (mod $m^2 r$), $\|R(g_2, h_2)\| = \|r\|$ a konečně 11.) $f(x) \equiv g_k(x)\,h_k(x)$ (mod $m^{2k} r^2$), 12.) $g_k(x) \equiv g_{k-1}(x)$, $h_k(x) \equiv h_{k-1}(x)$ (mod $m^{2k-1} r$), $\|R(g_k, h_k)\| = \|r\|$. Z 12.) plyne, že posloupnosti mnohočlenů $g_0(x), g_1(x), \ldots$, $h_0(x), h_1(x), \ldots$, v nichž v každé mají všechny stejný stupeň, konvergují resp. k limitám $g(x)$, $h(x)$ $g(x)$ bude mnohočlen stejného stupně jako $g_0(x)$, podobně bude $h(x)$ stejného stupně s $h_0(x)$ a na základě 12.) $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x)$ (mod r)*, $\|R(g, h)\| = \|r\|$. Z 11.) pak plyne, že $f(x) = g(x)\,h(x)$. Tím věta dokázána.

§ 12. *Budiž $f(x)$ mnohočlen s celými koefficienty z ohodnoceného perfektního tělesa K. Je-li $D(f(x)) = D \neq 0$, rozpadá se $f(x)$ jen tehdy v činitele nižšího stupně v K, rozpadne-li se $f(x)$ (mod D)* a sice každému rozkladu 1.) $f(x) \equiv g_0(x)\,h_0(x)$ (mod D)* bude odpovídati jednoznačný rozklad $f(x)$ v činiteli 2.) $f(x) = g(x)\,h(x)$, tak že 3.) $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x)$ (mod 1)*.*

Z kongruence 1.) plyne dle § 9., že $D(f) = D \equiv \pm D(g_0)\,D(h_0)\,(R^2(g_0, h_0))^2$ (mod D)*, a odtud $\|D\| = \|D(g_0)\| \cdot \|D(h_0)\|\;\|R(g_0, h_0)\|^2$, ježto pak $\|D(g_0)\| \leqq 1$,

$\|D(h_0)\| \leq 1$, bude $\|D\| \leq \|r^2\|$, kdež kladeno $\|R(g_0, h_0)\| = \|r\|$. Plyne tedy z kongruence 1.), že též $f(x) \equiv g_0(x) h_0(x)$ (mod r^2). Užijme věty z předešlého § J obdržíme rozklad $f(x) = g(x) h(x)$; $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x)$ (mod r)* a tedy tím spíše $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x)$ (mod 1)*.

§ 13. Uveďme speciální případ věty z § 11.

Budiž $f(x)$ mnohočlen s celými koefficienty z tělesa ohodnoceného perfektního K. Je-li možno určiti ξ_0 v tělese K, tak že 1.) $\|f(\xi_0)\| < \|f'(\xi_0)\|^2$, má rovnice $f(x) = 0$ kořen ξ v tělese K takový, že 2.) $\xi \equiv \xi_0$ (mod 1).*

Položme 3.) $f(\xi_0) = m$. Pak platí kongruence 4.) $f(x) \equiv f(x) - f(\xi_0) \equiv (x - \xi_0) g_0(x)$ (mod m). Dle § 9. jest však 5.) $r = R(x - \xi_0, g_0(x)) = g_0(\xi_0)$. Rozkladu $f(x) \equiv (x - \xi_0) g_0(x)$ (mod m) bude dle § 11. odpovídati rozklad $f(x)$ na činitele $(x - \xi) g(x)$, takový, že $\xi \equiv \xi_0$ (mod 1)*, bude-li $\|m\| < \|r^2\|$. To však možno snadno dokázati. Ze 4.) plyne, s použitím 5.), $f'(\xi_0) \equiv g_0(\xi_0) \equiv r$ (mod m) a ježto dle 1.) a 3.) $\|m\| < \|f'(\xi_0)\|^2$ je $\|f'(\xi_0)\| = \|r\|$. Je tedy jistě $\|m\| < \|r^2\|$.

Další věty o mnohočlenech z tělesa ohodnoceného perfektního. Mnohočleny Eisensteinovy.

§ 14. Z věty v § 11. plyne jako důsledek věta:

Je-li $f(x)$ mnohočlen s celými koefficienty z tělesa ohodnoceného perfektního K, plyne z rozkladu $f(x) \equiv g_0(x) h_0(x)$ (mod 1), kdež $g_0(x)$, $h_0(x)$ značí mnohočleny s celými koefficienty z K stupně ≥ 1 spolu nesoudělné (mod 1)* (jich resultant je pak jednotka), rozklad $f(x) = g(x) h(x)$, kdež $g(x)$, $h(x)$ jsou mnohočleny s celými koefficienty stejného stupně jako $g_0(x)$ resp. $h_0(x)$, pro něž $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x)$ (mod 1)*.*

Z věty této plyne dále:

Mnohočlen s celými koefficienty z tělesa ohodnoceného perfektního K je jistě rozložitelný, rozpadá-li se (mod 1) v různé činitele. Nerozložitelný mnohočlen z K je tedy (mod 1)* buď zase nerozložitelný nebo mocninou nerozložitelného mnohočlenu (mod 1)*.*

Rozpadá-li se $f(x)$ v různé činitele (mod 1)*, lze znázorniti $f(x)$ jako součin $g_0(x) h_0(x)$ dvou mnohočlenů, které nemají společných činitelů (mod 1)*, neboť mnohonásobného činitele lze připojiti celého buď k $f_0(x)$ nebo ke $g_0(x)$. I je $f(x) \equiv g_0(x)\, h_0(x)$ (mod 1)*, $g_0(x)$, $h_0(x)$ jsou nesoudělné (mod 1)*, je tedy dle věty předešlé $f(x) = g(x)\, h(x)$ j. b. d.

§ 15. Na základě věty v čele § 14. dokažme větu pro následující velmi důležitou:

Je-li $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ *primitivní mnohočlen z tělesa ohodnoceného perfektního K, buď nerozložitelný neb mocnina mnohočlenu nerozložitelného, a je-li jeden z krajních koefficientů celý nejednotkový, jsou i všechny vnitřní koefficienty celé nejednotkové (druhý krajní koefficient je pak jednotka).*

Při důkazu této věty budeme předpokládati, že je prostý člen celý nejednotkový, $\|a_n\| < 1$. Kdyby totiž $\|a_0\| < 1$, uvažovali bychom místo $f(x)$ mnohočlen

$$x^n f(1/x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0,$$

který je rovněž buď nerozložitelný neb mocninou mnohočlenu nerozložitelného a u něhož je ohodnocení prostého členu < 1. Nechť tedy jest již $\|a_n\| < 1$. Dejme tomu, že by neměly vnitřní koefficienty ohodnocení vesměs < 1. Budiž a_r v řadě $a_1, a_2, \ldots a_{n-1}$ poslední s ohodnocením 1, tedy $\|a_r\| = 1$, $1 \leqq r \leqq n-1$. I bude $f(x) \equiv a_0 x^n + a_1 x^{n-1} + \ldots + a_r x^{n-r} \equiv (a_0 x^r + \ldots + a_r)\, x^{n-r}$ (mod 1)*, t. j. $f(x) \equiv g_0(x) h(x)$ (mod 1)*, kdež $g_0(x) = a_0 x^r + \ldots + a_r$, $h_0(x) = x^{n-r}$. Největší společná míra $(g_0(x), x^{n-r})$ (mod 1)* je dělitelem nejv. spol. míry $(g_0{}^{n-r}, x^{n-r}) \equiv (g_0, x)^{n-r}$ (mod 1)*. Avšak nejv. spol. míra $(g_0, x) \equiv (a_0, x) \equiv 1$ (mod 1)*, tak že mnohočleny $g_0(x)$, $h_0(x)$ jsou nesoudělné (mod 1)*. Z tohoto rozkladu by dle věty na začátku § 14. plynulo, že $f(x) = g(x) h(x)$, kdež by pro $g(x)$ stupně r platila kongruence $g(x) \equiv g_0(x)$ (mod 1)* a pro $h(x)$ stupně $n-r$ podobně $h(x) \equiv h_0(x)$ (mod 1)*. Rozpadal by se tedy mnohočlen $f(x)$ ve dva různé činitele, což je proti předpokladu.

§ 16. Budiž $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ primitivní mnohočlen z tělesa ohodnoceného, jehož koefficienty jsou celé nejednotkové, až na a_0, což je jednotka : $\|a_0\| = 1$, $\|a_1\|$, $\|a_2\|$, $\ldots \|a_n\| < 1$. Takový mnohočlen nazveme *mnohočlenem Eisensteinovým.* I lze větu z předešlého § vysloviti takto:

Nerozložitelný primitivní mnohočlen z tělesa ohodnoceného perfektního, jehož prostý člen není jednotka, je nutně mnohočlen Eisensteinův.

Dokážeme si několik vět o mnohočlenech Eisensteinových z tělesa ohodnoceného (nemusí býti perfektní!).

Rozpadá-li se mnohočlen Eisensteinův z tělesa ohodnoceného, jsou jednotliví činitelé zase mnohočleny Eisensteinovy.

Nechť je $f(x) = g(x)\, h(x)$, při čemž lze předpokládati o mnohočlenech $g(x)$, $h(x)$, že mají celé koefficienty (§ 8.). Uvažujme rovnost tu (mod 1)*. I bude $a_0 x^n \equiv (b_0 x^\mu + \ldots + b_\varrho x^{\mu-\varrho})(c_0 x^\nu + \ldots + c_\sigma x^{\nu-\sigma})$ (mod 1)*, při čemž b_ϱ, c_σ jsou jednotky. To však je jen tehdy možno, když $\varrho = 0$, $\sigma = 0$. Tím věta dokázána.

Pro těleso ohodnocené prvoprvkem má mnohočlen Eisensteinův tvar $f(x) = a_0 x^n + a'_1 p x^{n-1} + \ldots + a'_n p$. Rozpadá-li se na k činitelů, je v těch činitelích každý prostý člen dělitelný aspoň p, tedy jich součin aspoň p^k a ježto tento součin je roven prostému členu v $f(x)$, dostáváme větu:

Eisensteinův mnohočlen s prostým členem dělitelným právě p^k může se rozpadnouti nanejvýš v k činitelů nižšího stupně.

Speciálním případem jest pak věta, analogická s větou Eisensteinovou pro těleso čísel racionálných:

Primitivní mnohočlen tvaru $a_0 x^n + p a'_1 x^{n-1} + \ldots + p a'_n$, při čemž prostý člen není dělitelný vyšší mocninou p než první, je nerozložitelný.

Prvky celé algebraické vzhledem k tělesu ohodnocenému.

§ 17. Prvek α nazveme *algebraickým celým prvkem* vzhledem k ohodnocenému tělesu K, hoví-li aspoň jedné rovnici $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ s koefficienty celými z K. I lze ihned dokázati větu: *Prvek algebraický celý vzhledem ke K, patřící do K, je celý prvek z K.* Budiž α algebraický celý prvek vzhledem ke K, hovící rovnici $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ s celými koefficienty z K. Dejme tomu, že by prvek α byl lomený prvek z K, tedy $\|\alpha\| > 1$. Položme $1/\alpha = \beta$. I bylo by $\|\beta\| < 1$ a β by hovělo rovnici $1 + a_1 \beta + a_2 \beta^2 + \ldots + a_n = 0$, což je nemožno, ježto by odtud plynulo $1 \equiv 0$ (mod 1)*.

Uvedeme několik vět, jichž důkaz je zcela podobný důkazu obdobných vět o číslech celých algebraických.*)

Jsou-li α, β prvky celé algebraické vzhledem ke K, platí totéž i o jich součtu $\alpha + \beta$, rozdílu $\alpha - \beta$ a součinu $\alpha\beta$. Prvky celé algebraické vzhledem ke K tvoří obor celistvosti.

Každý lomený prvek algebraický dá se znázorniti jako podíl dvou celých prvků algebraických (za jmenovatele lze dokonce zvoliti prvek z K.

Při definici prvku celého algebraického vzhledem ke K stačilo věděti, že jedna z nekonečně mnoho rovnic z K, jíž prvek ten hoví, má 1 za koefficient u nejvyšší mocniny x a ostatní koefficienty celé z K. Lze však dokázati větu:

Prvek α je tehdy a jen tehdy celý algebraický, má-li jeho definující rovnice v K u nejvyšší mocniny x koefficient 1 a všechny ostatní koefficienty celé.

Konečně uveďme větu:

Kořeny rovnice $x^m + \alpha_1 x^{m-1} + \ldots + \alpha_m = 0$, jejíž koefficienty jsou celé prvky algebraické z K, jsou celé prvky algebraické vzhledem ke K.

Nyní můžeme na prvky celé algebraické přenésti některé z definic a vět z § 5.

Jsou-li oba prvky ε a $1/\varepsilon$ celé, nazveme ε *algebreickým prvkem jednotkovým* (vzhledem ku K). Pojem *dělitelnosti* lze zase definovati pomocí 3.), platí pak věty 4.), 5.), 6.); *prvky associované* pomocí 7.), platí pak 9.), 10.).

Snadno lze nahlédnouti, že rovnice definující v K algebraický prvek jednotkový má u nejvyšší mocniny x koefficient 1, ostatní koefficienty celé a za prostý člen jednotku z K.

§ 18. Všimněme si nyní, jak se poměry utváří v případě, že těleso základní K je ohodnocené *perfektní*.

Tu platí věta:

Prvek α, jehož definující rovnice v tělese ohodnoceném perfektním je $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, je celý tehdy a jen tehdy, je-li prostý člen a_n celý prvek z K.

Je ihned patrno, že podmínka ta je nutná: má-li býti prvek α celý, musí býti prostý člen a_n celý. Dokažme si, že

*) Hensl l. c. Weber, Algebra II.

jest též postačující: z celistvosti a_n, $\|a_n\| \leqq 1$ plyne celistvost ostatních koefficientů. Dejme tomu, že by se vyskytly koefficienty necelé, jichž ohodnocení tedy > 1. Budiž a ten z nich, pro který $\|a\| = Max\,(\|a_1\|, \|a_2\|, \ldots \|a_n\|)$. I bude jistě $\|a\| > 1$, $\|1/a\| < 1$. Mnohočlen $\frac{1}{a}x^n + \frac{a_1}{a}x^{n-1} + \ldots + \frac{a_n}{a}$ je jistě primitivní, poněvadž má celé koefficienty, z nichž jeden jistě (a to vnitřní) je jednotkový prvek. Je to tedy mnohočlen nerozložitelný, primitivní a krajní koefficient $\|1/a\| < 1$. Jeden z vnitřních koefficientů je jednotka, což odporuje větě z § 15. Musí tedy býti nutně koefficienty $a_1, a_2, \ldots a_{n-1}$ celé, j. b. d.

Pro prvek algebraický jednotkový je a_n jednotkou z K, $\|a_n\| = 1$; pro prvek celý algebraický nejednotkový je $\|a_n\| < 1$ a dle věty z § 15. je též $\|a_1\| < 1$, $\|a_r\| < 1, \ldots \|a_{n-1}\| < 1$.

Ohodnocení prvků algebraických vzhledem k tělesu ohodnocenému.

§ 19. Budeme se nyní zabývati ohodnocením prvků algebraických vzhledem k tělesu ohodnocenému K. Tak dostaneme ohodnocení všech algebraických rozšíření tělesa K i algebraického rozšíření tělesa K algebraicky uzavřeného.

Je-li prvek α definován v K nerozložitelnou rovnicí $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ a mají-li všechny kořeny její míti totéž ohodnocení, musíme zvoliti $\|\alpha\| = \|a_n\|^{\frac{1}{n}}$, má-li býti splněna podmínka II. $\|\alpha\beta\| = \|\alpha\|\,\|\beta\|$. Nevíme však, zda, položíme-li $\|\alpha\| = \|a_n\|^{\frac{1}{n}}$, vůbec dostaneme ohodnocení, totiž budou-li splněny podmínky I.—IV. z § 1. Co se týče podmínek I. a IV., splněny budou. Jak tomu bude s podmínkami II. $\|\alpha\beta\| = \|\ \|\alpha\| . \|\beta\|$, III′ $\|1 + \alpha\| \leqq 1$ pro $\|\alpha\| < 1$.

§ 20. *Podmínka II. je splněna, i když nečiníme o tělese ohodnoceném K předpoklad, že je perfektní.* Nejprvé to dokážeme pro případ, že prvky α a β jsou prvního druhu vzhledem ke K.*)

Uvažujme těleso $L = K(\alpha, \beta)$. To bude zase prvního druhu a jednoduché: bude v něm existovati primitivní prvek

*) t. j. nerozložitelné rovnice, jimiž jsou prvky ty definovány, mají jednoduché kořeny.

ϑ, takže $L = K(\alpha, \beta) = K(\vartheta)$. Prvek ϑ je v K definován nerozložitelnou rovnicí s jednoduchými kořeny stupně r; ostatní její kořeny označme $\vartheta_1, \vartheta_2, \ldots \vartheta_{r-1}$. Libovolný prvek δ tělesa L dá se vyjádřiti jako racionální funkce ϑ s koefficienty z K, $\delta = \varphi(\vartheta)$. Sdružené hodnoty jsou pak $\delta = \varphi(\vartheta_1), \ldots \delta_{r-1} = \varphi(\vartheta_{r-1})$, jich součin $\delta, \delta_1, \delta_2 \ldots \delta_{2-1} = N(\delta)$ je norma prvku δ. δ vyhovuje rovnici $N(x-\delta) = 0$, jejíž levá strana je mnohočlen nerozložitelný neb mocnina mnohočlenu nerozložitelného. Snadno nahlédneme, že $\|\delta\| = \|N(\delta)\|^{\frac{1}{r}}$. Je-li mnohočlen $N(x-\delta)$ nerozložitelný, je to přímo patrné, je-li to mocnina mnohočlenu nerozložitelného $(x^\mu + d_1 x^{\mu-1} + \ldots + d_\mu)^\nu$, $\mu\nu = r$, je $\|\delta\| = \|d_\mu\|^{\frac{1}{\mu}} = \|d_\mu^\nu\|^{\frac{1}{r}} = \|N(\delta)\|^{\frac{1}{r}}$. I je ihned patrno, že $N(\alpha\beta) = N(\alpha)\, N(\beta)$ a tedy též $\|N(\alpha\beta)\|^{\frac{1}{r}} = \|N(\alpha)\|^{\frac{1}{r}} \|N(\beta)\|^{\frac{1}{r}}$, t. j. $\|\alpha\beta\| = \|\alpha\|\ \|\beta\|$.

§ 21. Nyní si všimněme případu, kdy prvky α a β nejsou oba prvého druhu. Případ ten může nastati pouze tehdy, když charakteristika tělesa K je různá od nully (je to pak jisté prvočíslo l).

Nechť prvek α hoví v K rovnici nerozložitelné $f(x) = 0$; pak lze určiti celé číslo $r \leqq 0$ tak, že $f(x)$ je racionálná funkce v x^{l^r}, nikoliv však v $x^{l^{r+1}}$, t. j. $f(x) = g(x^{l^r})$. $g(x)$ je mnohočlen nerozložitelný s jednoduchými kořeny. Jeho kořen $\bar{\alpha} = \alpha^{l^r}$ je tedy prvního druhu. r nazývá se eksponentem prvku α. Je-li

$$f(x) = g(x^{l^r}) = x^{nl^r} + a_1 x^{(n-1)l^r} + \ldots + a_n,$$

je
$$\|\alpha\| = \|a_n\|^{\frac{1}{nl^r}}, \quad \|\bar{\alpha}\| = \|a_n\|^{\frac{1}{n}},$$

a tedy
$$\|\alpha\| = \|\bar{\alpha}\|^{\frac{1}{l^r}}.$$

Buďtež nyní r, s, t eksponenty prvků $\alpha, \beta, \gamma = \alpha\beta$, tak že $\bar{\alpha} = \alpha^{l^r}$, $\bar{s} = s^{l^s}$, $\bar{\gamma} = \gamma^{l^t}$ jsou prvního druhu. Z $\gamma = \alpha\beta$ plyne, umocníme-li p^{r+s+t}, $\bar{\gamma}^{l^{r+s}} = \bar{\alpha}^{l^{s+t}} \bar{\beta}^{l^{r+t}}$; ježto pro prvky $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ prvního druhu II platí,

je
$$\|\bar{\gamma}\|^{l^{r+s}} = \|\bar{\alpha}^{l^{s+t}} \bar{\beta}^{l^{r+t}}\| = \|\bar{\alpha}\|^{l^{s+t}}\ \|\bar{\beta}\|^{l^{r+t}},$$

a tedy $\|\bar{\gamma}\|^{\frac{1}{l^t}} = \|\bar{\alpha}\|^{\frac{1}{l^r}} \|\bar{\beta}\|^{\frac{1}{l^s}}$, odtud pak $\|\gamma\| = \|\alpha\| . \|\beta\|$.

§ 22. *Aby platila podmínka III', musíme o tělese ohodnoceném K učiniti předpoklad, že je perfektní.*

Je-li prvek α v K definován rovnicí nerozložitelnou $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0$, plyne z $\|\alpha\| \leqq 1$, t. j. $\|a_n\|^{\frac{1}{n}} \leqq 1$, že $\|a_n\| \leqq 1$, tak že a_n je celý prvek z K a dle § 18. je pak též α celý prvek, prvky z K, $a_1, a_2, \ldots a_n$, jsou též celé, tak že 1.) $\|a_1\| \leqq 1$, $\|a_n\| \leqq 1, \ldots \|a_n\| \leqq 1$. Prvek $1 + \alpha$ je definován rovnicí $f(x-1) = 0$,

tak že $$\|1+\alpha\| = \|f(-1)\|^{\frac{1}{n}}.$$

Avšak $f(-1) = (-1)^n + a_1(-1)^{n-1} + \ldots + a_n$, tak že z 1.) plyne $\|f(-1)\| \leqq 1$, a tedy též $\|1+\alpha\| \leqq 1$.

Zároveň vidíme, že *v tělese ohodnoceném perfektním jsou prvky celé algebraické zase charakterisovány tím, že jich ohodnocení je $\leqq 1$, jednotky mají ohodnocení 1.*

Ukážeme na příkladě nutnost předpokladu, že těleso ohodnocené K je perfektní.

Uvažujme rovnici $x^2 - 2_x + 3 = 0$ v tělese racionálných čísel R ohodnoceném způsobem Henselovým, tak že za $\|3\|$ zvolíme libovolné číslo reálné mezi 0 a 1 (§ 3). Rovnice ta je nerozložitelná v R (vidíme hned, že neplatí věta z § 15). Kořeny její $1 \pm \sqrt{-2}$ dostaly by oba ohodnocení $\sqrt{\|3\|} < 1$. 2 je jednotka v tělese R, t. j. $\|2\| = 1$. Jest však $2 = (1 + \sqrt{-2}) + (1 - \sqrt{-2})$. Kdyby platila podmínka III', musilo by býti $\|2\| \leqq \|1 + \sqrt{-2}\| = \|1 - \sqrt{-2}\| = \sqrt{\|3\|}$ tedy $\|2\| < 1$, což vede ke sporu. Také by neplatila věta z § 18 a věta, že k tomu, aby byl prvek algebraický celý, je nutno a postačí, aby jeho ohodnocení bylo $\leqq 1$. Stačí uvažovati

$$\frac{1 + \sqrt{-2}}{1 - \sqrt{-2}} = \frac{-1 + 2\sqrt{-2}}{3}.$$

Ohodnocení tohoto prvku je 1 a není to prvek celý, ježto je kořenem rovnice nerozložitelné v R: $x^2 + \frac{2}{3} x + 1 = 0$. Těleso perfektní R' je těleso Henselových čísel 3-adických. V tom je rovnice $x^2 - 2_x + 3 = 0$ rozložitelná, což plyne z § 12. Diskriminant rovnice té je totiž -2, $\|-2\| = 1$. Uvažujeme-li ji mod 3, rozpadá se $x(x-2) \equiv 0$ (mod 3), tak že se rozpadá též v R' a je $1+\sqrt{-2} \equiv 2$, $1-\sqrt{-2} \equiv 0 \pmod 3$. Je tedy

$$\|1+\sqrt{-2}\| = 1, \quad \|1-\sqrt{-2}\| = \|3\|.$$

§ 23. *Je-li K těleso ohodnocené perfektní s prvoprvkem p, eksistuje též prvoprvek v každém konečném algebraickém rozšíření L tělesa K.*

Budiž n stupeň konečného algebraického rozšíření L. Každý prvek z L hoví v K nerozložitelné rovnici, jejíž stupeň je dělitelem n. Ohodnocení prvků z L budou tedy míti tvar $\|p\|^{\frac{k}{n}}$, kdež k je celé číslo; pro prvky celé nejednotkové bude k celé číslo kladné. Je tedy jistě mezi celými prvky nejednotkovými prvek π s největším ohodnocením a ten bude v L prvoprvkem. Nechť je $\|\pi\| = \|p\|^{\frac{f}{n}}$, f celé číslo kladné. Všechny prvky z L dají se vyjádřiti ve tvaru $\varepsilon\pi^r$, kdež ε je jednotka z L, r číslo celé; pro prvky celé je $r \geqq 0$.

Je tedy též $p = \varepsilon\pi^e$, $\|p\| = \|\pi\|^e$,

$$\|\pi\| = \|p\|^{\frac{1}{e}} = \|p\|^{\frac{f}{n}}, \text{ tak že } ef = n.$$

§ 24. Snažíce se ohodnotiti algebraické rozšíření perfektního tělesa ohodnoceného K položili jsme předem podmínku, že, hoví-li prvek α algebraický vzhledem ku K nerozložitelné rovnici 1.) $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0$ mají míti všechny kořeny této rovnice rovné ohodnocení $\|a_n\|^{\frac{1}{n}}$ a ukázali, že jest to možné. Koefficienty rovnice 1.) nerozložitelné v tělese ohodnoceném perfektním K musí proto hověti jistým podmínkám, které si odvodíme. Označme její kořeny $\alpha_2 = \alpha_1$ $\alpha_2, \alpha_3, \ldots \alpha_n$. I bude lze položiti 2.) $\|\alpha_1\| = \|\alpha_2\| = \ldots \|\alpha_n\| = \|a_n\|^{\frac{1}{n}}$. Koefficienty rovnice 1.) dají se vyjádřiti jako elementární symmetrické funkce kořenů $a_i = \pm \Sigma \alpha_1, \alpha_2 \ldots \alpha_i$. Z 2.) pak bude plynouti

3.) $\|a_i\| \leqq \|a_n\|^{\frac{i}{n}}$ $(i = 1, 2, \ldots n)$.

Ohodnocení koefficientů rovnice nerozložitelné v tělese perfektním ohodnoceném musí tedy hověti nerovnostem 3.).

Položíme si otázku, zda by bylo možno ohodnotiti algebraické rozšíření L tělesa ohodnoceného perfektního K tak, aby ohodnocení tělesa K zůstalo zachováno, že by však prvek α z L, definovaný v K nerozložitelnou rovnicí 1.) $(n > 1)$, měl ohodnocení $\|\alpha\| \neq \|a_n\|^{\frac{1}{n}}$.

Dejme tomu, že by bylo $||\alpha|| > ||a_n||^{\frac{1}{n}}$. Z 3.) by plynulo $||\alpha^n|| > ||a_1 \alpha^{n-1}||$, $||\alpha^n|| > ||a_2 \alpha^{n-2}||, \dots ||\alpha^n|| > ||a_n||$.

Bylo by tedy $||f(\alpha)|| = ||\alpha^n|| > ||a_n|| > 0$, t. j. $f(\alpha) \neq 0$, což by odporovalo předpokladu, že α je kořen 1.).

Stejně není možno, aby

$$||\alpha|| < ||a_n||^{\frac{1}{n}}; \text{ pak by } ||1/\alpha|| > ||1/a_n||^{\frac{1}{n}};$$

$1/a_n$ by byl prostý člen rovnice v K nerozložitelné $x^n f(1/x) = 0$, jíž hoví $1/\alpha$. Musí býti tedy nutně $||\alpha|| = ||a_n||^{\frac{1}{n}}$. I platí věta:

Chceme-li ohodnotiti algebraické rozšíření L tělesa perfektního ohodnoceného K, tak aby ohodnocení tělesa K zůstalo zachováno, lze to učiniti tím způsobem, že prvku α z L definovanému v K nerozložitelnou rovnicí 1.) dáme ohodnocení $||\alpha|| = ||a_n||^{\frac{1}{n}}$. Jinak to však ani učiniti není možno.

Těleso ohodnocené perfektní algebraicky uzavřené.

§ 25. Dokážeme nyní, že *derivované těleso K' tělesa K algebraicky uzavřeného, ohodnoceného, je zase algebraicky uzavřené.* K tomu cíli dlužno dokázati, že každý mnohočlen $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$ s koefficienty z K', rozpadá se v K' v lineární činitele.

Budeme se nejprve zabývati případem, kdy diskriminant $D(f(x)) = D \neq 0$.

I lze stanoviti v tělese K prvky $A_1, A_2, \dots A_n$, tak že

$$||a_1 - A_1|| < ||D||, ||a_2 - A_2|| < ||D||, \dots ||a_n - A_n|| < ||D||.$$

Položíme-li $F(x) = x^n + A_1 x^{n-1} + \dots + A_n$, bude $F(x) \equiv f(x)$ (mod D)*. Dále bude $D(F) \equiv D$ (mod D)*, t. j. $||D(F)|| = ||D||$. Užijme věty z § 12. Rozkladu $f(x)$ (mod D)* bude odpovídati rozklad v tělese ohodnoceném perfektním K'. Avšak $F(x)$ je mnohočlen z tělesa algebraicky uzavřeného K, rozpadá se tedy v K v lineární činitele, $F(x) = (x - \Xi_1)(x - \Xi_2) \dots (x - \Xi_n)$. I bude též $f(x) \equiv (x - \Xi_1)(x - \Xi_2) \dots (x - \Xi_n)$ (mod D)* a z § 12, bude plynouti, že v K' platí rozklad $f(x) = (x - \xi_1)(x - \xi_2) \dots (x - \xi_n)$, $\xi^1 \equiv \Xi_1, \dots \xi_n \equiv \Xi_n$ (mod 1).*

Je-li diskriminant $D(f(x)) = 0$, má $f(x)$ mnohonásobné kořeny. Položme $f(x) = f_1(x) (f_2(x))^2 (f_3(x))^3 \dots$, kdež $f_1(x), f_2(x), \dots$ mají jednoduché kořeny a tedy diskrimant $\neq 0$. Je-li charakte-

…istika tělesa K' rovna 0, patří každý z mnohočlenů $f_m(x)$ do K'; zrovna tak tomu je při charakteristice l (l prvočíslo), není-li m dělitelno l. V těchto případech lze ihned užíti výsledku předešlého. Je-li charakteristika tělesa K' rovna l, $\lambda = l^f$ nejvyšší mocnina l obsažená v m, patří $(f_m(x))^\lambda$ do K'. Jsou-li však v K' λ-té odmocniny koefficientů mnohočlenu $f_m(x)$, bude již $f_m(x)$ patřiti do K'. Bude tedy věta i v tomto případě, s použitím výsledku předešlého, dokázána, dokážeme-li, že jakákoliv rovnice tvaru $x^{l^f} - C = 0$, kdež C je z K', je v K' řešitelná (má tam pak jediný kořen). C lze znázorniti jako limitu posloupnosti $c_1, c_2, \dots c_n, \dots$ z K. Rovnice $x^{l^f} - c_n = 0$ jest řešitelná v K vzhledem k tomu, že těleso K je algebraicky uzavřené. Má pak jediný kořen, který označme γ_n. Ukažme, že posloupnost $\gamma_1, \gamma_2, \dots \gamma_n \dots$ konverguje a její limita γ, patřící jistě do K', je kořenem rovnice $x^{l^f} - C = 0$. Jest totiž $\lim\limits_{n=\infty} (\gamma_{n+1} - \gamma_n)^{l^f} = \lim\limits_{n=\infty} (\gamma_{n+1}^{l^f} - \gamma_n^{l^f}) = \lim\limits_{n=\infty} (c_{n+1} - c_n) = 0$, tedy též $\lim\limits_{n=\infty} (\gamma_{n+1} - \gamma_n) = 0$, čímž konvergence posloupnosti $\gamma_1, \gamma_2, \dots$ dokázána. Pro její limitu γ platí: $\lim\limits_{n=\infty} (\gamma^{l^f} - c) = \lim\limits_{n=\infty} (\gamma^{l^f} - c_n) = \lim\limits_{n=\infty} (\gamma^{l^f} - \gamma_n^{l^f}) = \lim\limits_{n=\infty} (\gamma - \gamma_n)^{l^f} = 0$. Tím tvrzení dokázáno.

§ 26. Ukažme konečně, *že možno každé ohodnocené těleso K rozšířiti na těleso perfektní, algebraicky uzavřené, ohodnocené.*

Těleso ohodnocené K lze rozšířiti nejprvé na těleso perfektní ohodnocené tím, že utvoříme těleso derivované K'. To můžeme rozšířiti na algebraicky uzavřené ohodnocené těleso $\overline{K}$. Utvořme derivované těleso $\overline{K}'$ tohoto tělesa algebraicky uzavřeného ohodnoceného. Dle věty z předešlého § bude zase algebraicky uzavřené. Vyhovuje tedy $\overline{K}'$ všem podmínkám současně: je to těleso ohodnocené perfektní algebraicky uzavřené.*)

---

*) Zvolíme-li za K těleso čísel racionálných ohodnocené pomocí absolutní hodnoty, je K' těleso čísel reálných. Algebraicky uzavřené ohodnocené těleso $\overline{K}$ dostaneme připojením $i = \sqrt{-1}$. $\overline{K}$ je těleso čísel komplexních a to je již perfektní, $\overline{K}' = \overline{K}$. Tomu tak vždy není. Ostrowski ukázal (Crelles Journ 143, 147), že, zvolíme-li za K těleso čísel racionálných ohodnocených způsobem Henselovým, tak že K' je těleso Henselových čísel p-adických racionálných, $\overline{K}$ těleso Henselových čísel algebraických, eksistují posloupnosti takovýchto čísel konvergentní, které nemají za limitu Henselovo číslo algebraické, tak že jistě $\overline{K}' \neq \overline{K}$.