Časopis pro pěstování matematiky a fysiky

Karel Petr

O basi celých čísel v obecných tělesech algebraických

Časopis pro pěstování matematiky a fysiky, Vol. 64 (1935), No. 5, 62--72

Persistent URL: http://dml.cz/dmlcz/121256

O basi celých čísel v obecných tělesech algebraických.

Karel Petr, Praha.

V teorii algebraických těles číselných se naskýtá často jedna velmi závažná okolnost. Máme tam velikou řadu obecných vět, chceme-li však tyto obecné věty skutečně použíti, neposkytuje nám teorie ta prostředky použití to provésti, po případě jenom takové prostředky, že — nehledíc k nejjednodušším případům — lze úkol ten vykonati po veliké námaze nepřiměřené tomu úkolu. Že tento stav není pro pokrok vědy prospěšný a že nasvědčuje tomu, že jsme ještě nedospěli k nejjednoduššímu pojetí té teorie, pokládám za jasné. Z té příčiny jsem si předsevzal, některé úkoly, jež teorie alg. čísel nám předkládá, vyšetřovati. Tak před krátkým časem jsem odvodil přesné kriterium pro rozložitelnost mnohočlenů s celistvými součiniteli podle modulu prvočíselného p a odvodil věty, jak rozklad ten provésti (není-li prvočíslo p dělitelem diskriminantu). Dnes hodlám se zabývati konstrukcí base pro celá čísla tělesa $K(\Theta)$, kde Θ jest algebraické číslo celé splňující rovnici

$$f(\Theta) = 0,$$

při čemž

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

$a_1, a_2, \ldots, a_n$ jsou čísla racionální celá. Mnohočlen $f(x)$ budiž v tělese K čísel racionálních ireducibilní.

V následujícím značí vždy malá latinská písmena, pokud nezastupují označení funkce resp. polynomu, celá racionální čísla. Obdobně řecká písmena jsou obecně čísla algebraická. Mnohočleny jsou vyznačovány pomocí znaků P, Q, R, S, avšak také pomocí znaků φ, ψ, Ψ, f, g. Význam ostatních symbolů jest vždy úplně vytčen na příslušném místě.

I.

Pod basí čísel celých tělesa $K(\Theta)$ vyrozumíváme n čísel (celých) $\omega_1, \omega_2, \ldots, \omega_n$ takových, že všecka čísla celá toho tělesa dostáváme ve tvaru

$$b_1\omega_1 + b_2\omega_2 + \ldots + b_n\omega_n,$$

dosazujeme-li za $b_1, b_2, \ldots, b_n$ po řadě všecka čísla celá racionální. Každé číslo celé tělesa dostaneme tak pouze jedenkrát.

O basi platí nejprve věty:

I. **Věta prvá.** Basi lze dáti vždy tvar

$$\omega_k = \frac{\varphi_{k-1}(\Theta)}{d_{k-1}}, \quad k = 1, 2, 3, \ldots, n,$$

při čemž jednak

$$\varphi_k(x) = x^k + c_{k1}x^{k-1} + \ldots + c_{kk}, \quad \varphi_0(x) = 1,$$

c_{kj} (pro $k = 1, 2, \ldots, n-1$, $j = 1, 2, \ldots, k$) jsou čísla celá racionální; jednak $d_1, d_2, \ldots, d_{n-1}$ jsou čísla celá racionální kladná a taková, že d_k jest dělitelno d_{k-1} (pro $k = 2, 3, \ldots, n-1$), takže lze klásti

$$d_k = c_1 c_2 \ldots c_k,$$

c_k číslo celé racionální kladné.

Důkaz této věty jest snadný a netřeba se jím zdržovati.

Při větě druhé jest třeba opustiti obor daný tělesem $K(\Theta)$; bude třeba přibrati vedle čísla Θ ještě čísla konjugovaná $\Theta_1, \Theta_2, \ldots, \Theta_{n-1}$.

Budiž dále $P(x, x_1, \ldots, x_{n-1})$ mnohočlen v $x, x_1, \ldots, x_{n-1}$ se součiniteli celistvými racionálními. Sestrojíme všecka čísla různá, vznikající z $P(\Theta, \Theta_1, \ldots, \Theta_{n-1})$, když na tento výraz provedeme všecky permutace symetrické grupy (permutující prvky $\Theta, \Theta_1, \ldots, \Theta_{n-1}$). Je-li těch různých čísel r, hoví $P(\Theta, \Theta_1, \ldots, \Theta_{n-1})$ rovnici stupně r-tého tvaru

$$P^r + l_1 P^{r-1} + \ldots + l_r = 0,$$

kde l_k jsou čísla celá racionální. Jsou-li $p^{i_1}, p^{i_2}, \ldots, p^{i_r}$ nejvyšší mocniny prvočísla p dělící po řadě součinitele $l_1, l_2, \ldots, l_r$ a značíme-li nejmenší z r čísel

$$\frac{i_1}{1}, \frac{i_2}{2}, \ldots, \frac{i_r}{r}$$

α, budeme říkati, že $P(\Theta, \Theta_1, \ldots, \Theta_{n-1})$ jest dělitelno p^α (a ovšem každou mocninou $p^{\alpha'}$, kde $0 \leqq \alpha' < \alpha$).

Jestliže $P(\Theta, \Theta_1, \ldots, \Theta_{n-1})$ jest dělitelno mocninami různých prvočísel $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots$, pak budeme též říkati, že jest dělitelno jejich součinem $p_1^{\alpha_1} p_2^{\alpha_2} \ldots$

Lze snadno dokázati větu: Je-li $P(\Theta, \Theta_1, \ldots, \Theta_{n-1})$ dělitelno $p_1^{\alpha_1} p_2^{\alpha_2} \ldots$, pak symetrická funkce všech čísel vznikajících permutacemi z $P(\Theta, \Theta_1, \ldots, \Theta_{n-1})$ (v počtu $n!$) váhy w jest dělitelna aspoň $p_1^{\nu_1} p_2^{\nu_2} \ldots$, kde celá čísla $\nu_1, \nu_2, \ldots$ jsou dána nerovninami

$$w\alpha_1 \leqq \nu_1 < w\alpha_1 + 1, \; w\alpha_2 \leqq \nu_2 < w\alpha_2 + 1, \ldots$$

Toto předeslavše můžeme vysloviti **větu II:** Celá čísla $d_1, d_2, \ldots, d_{n-1}$ jsou taková, že výraz $\Delta(\Theta_1, \Theta_2, \ldots, \Theta_k)$ jest dělitelný součinem $d_1 d_2 \ldots d_{k-1}$. Při tom jest $\Delta(\Theta_1, \Theta_2, \ldots, \Theta_k)$ nejjednodušší alternující funkce čísel $\Theta_1, \Theta_2, \ldots, \Theta_k$ daná vztahem

$$\Delta(\Theta_1, \Theta_2, \ldots, \Theta_k) =$$
$$= (\Theta_1 - \Theta_2)(\Theta_1 - \Theta_3) \ldots (\Theta_1 - \Theta_k)(\Theta_2 - \Theta_3) \ldots (\Theta_{k-1} - \Theta_k).$$

Z věty této následuje jako snadný důsledek: Největší společná míra determinantů r-tého stupně symetrické matice

$$\left\{\begin{array}{cccc} s_0, & s_1, & s_2, & \ldots, s_{n-1} \\ s_1, & s_2, & s_3, & \ldots, s_n \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ s_{n-1}, & s_n, & s_{n+1}, & \ldots, s_{2n+2} \end{array}\right\} = \{S\}$$

jest dělitelna $d_1^2 d_2^2 \ldots d_{k-1}^2$ pro $k = 2, 3, \ldots, n$. Tu jest

$$s_k = \Theta^k + \Theta_1^k + \ldots + \Theta_{n-1}^k$$

a determinant stupně n-tého jest, jak známo, diskriminant rovnice $f(x) = 0$.

Důkaz věty II. leží nasnadě. Naznačíme jej pro $k = 3$. K tomu cíli stačí uvažovati determinant

$$\begin{vmatrix} 1, & \frac{\varphi_1(\Theta)}{d_1}, & \frac{\varphi_2(\Theta)}{d_2} \\ 1, & \frac{\varphi_1(\Theta_1)}{d_1}, & \frac{\varphi_2(\Theta_1)}{d_2} \\ 1, & \frac{\varphi_1(\Theta_2)}{d_1}, & \frac{\varphi_2(\Theta_2)}{d_2} \end{vmatrix}$$

Determinant jest patrně číslo celé v tělese $K(\Theta, \Theta_1, \Theta_2)$. Jest však rovný

$$\frac{\Delta(\Theta, \Theta_1, \Theta_2)}{d_1 d_2};$$

jelikož pak toto číslo jest celé v tělese $K(\Theta, \Theta_1, \Theta_2)$ a ovšem také všecka čísla permutacemi z něho vznikající jsou čísla celá, jest tvrzení na podkladě definice učiněné jasné.

Větou II. jest obor možných čísel pro $d_1, d_2, \ldots, d_{n-1}$ značně omezen. Tak na př. nemají-li determinanty stupně $n - 1$ z matice $\{S\}$ společné míry aneb je-li největší společná míra těch determinantů dělitelna jenom prvými mocninami různých prvočísel, pak $d_1 = d_2 = \ldots = d_{n-2} = 1$. Je-li nadto $|S| = \pm d^2 . g$, kde g jest dělitelno rovněž jenom prvými mocninami prvočísel, pak d_{n-1} jest dělitelem čísla d.

Vedle těchto dvou vět budeme užívati ještě **větu III:** Jestliže ω jest číslo celé tělesa $K(\Theta)$, pak $f'(\Theta) . \omega$ dá se vyjádřiti ve tvaru

$$f'(\Theta) . \omega = b_0 + b_1\Theta + b_2\Theta^2 + \ldots + b_{n-1}\Theta^{n-1};$$

$b_0, b_1, \ldots, b_{n-1}$ čísla celá racionální.

Důkaz jest snadný.

Jest patrno, že každý polynom v Θ s celočíselnými součiniteli lze psáti ve tvaru

$$b'_0 + b'_1 d_1 \varphi_1(\Theta) + b'_2 d_2 \varphi_2(\Theta) + \ldots + b'_{n-1} d_{n-1} \varphi_{n-1}(\Theta).$$

kde b'_k jsou čísla celá.

Konečně uvádím bez důkazu **větu IV.** Budiž p kterékoliv prvočíslo dělící c_k. Pro $f(x)$ jest, jak známo, platný rozklad

$$f(x) \equiv \psi_1(x)^{v_1} \psi_2(x)^{v_2} \ldots \psi_s(x)^{v_s}, \pmod{p},$$

kde

$$\psi_i(x) = x^{n_i} + a_1^{(i)} x^{n_i - 1} + \ldots + a_{n_i}^{(i)}$$

jest mnohočlen ireducibilní mod p a kde $\psi_i(x)$ s různým indexem jsou mod p různé polynomy. Pak jest

$$\varphi_k(x) \equiv \psi_1(x)^{v'_1} \psi_2(x)^{v'_2} \ldots \psi_s(x)^{v'_s} \pmod{p},$$

kde $\quad 1 \leqq v'_i \leqq v_i$ a $n_1 v'_1 + n_2 v'_2 + \ldots + n_s v'_s = k.$

II.

Pro $\varphi_{n-1}(x), \varphi_{n-2}(x), \ldots, \varphi_1(x)$ jsou platny zajímavé vztahy, jež jest rovněž užitečno odvoditi. Utvořme výraz

$$(x - b_1)\, \varphi_{n-1}(x) - f(x);$$

v tomto výraze vymizí n-tá mocnina x, celé číslo b_1 můžeme pak voliti tak, aby i $(n-1)$-vá mocnina x vymizela. Bude pak výraz ten stupně $n-2$. Dosadíme-li v něm Θ za x, vznikne číslo tělesa $K(\Theta)$ dělitelné d_{n-1}; avšak mnohočlen stupně $n-2$ v Θ s celistvými součiniteli jest v nejkrajnějším případě dělitelný číslem celým racionálním, jež jest rovno součinu čísla d_{n-2} a největší společné míry součinitelů. Jsou tedy všecky součinitele uvažovaného výrazu dělitelny $c_{n-1} = d_{n-1}/d_{n-2}$. Lze tedy psáti

$$(x - b_1)\, \varphi_{n-1}(x) = c_{n-1}\, \psi_{n-2}(x) + f(x) \qquad (m)$$

a tvrditi, že shoda

$$f(x) \equiv 0 \pmod{c_{n-1}}$$

má jeden kořen $x = b_1$. Při tom jest $b_1 = c_{n-1,1} - a_1$.

Uvažujme dále součin

$$f'(\Theta)\, \frac{\varphi_{n-1}(\Theta)}{d_{n-1}},$$

součin tento lze upraviti na mnohočlen $(n-1)$-vého stupně v A, který má podle věty III. celočíselné součinitele. Můžeme tudíž psáti

$$f'(\Theta)\, \varphi_{n-1}(\Theta) = d_{n-1}\, \Psi_{n-1}(\Theta).$$

Avšak upravíme-li $f'(x)$ na tvar $(x - b_1)\, P_{n-2}(x) + a'_{n-1}$, kde $a'_{n-1} = f'(b_1)$, a užijeme-li vztahu (m), máme — po snadné úpravě —

$$f'(\Theta)\, \varphi_{n-1}(\Theta) = a'_{n-1}\, \varphi_{n-1}(\Theta) + c_{n-1}\, \overline{\Psi_{n-1}}(\Theta).$$

Porovnáme-li v obou výsledcích součinitele při Θ^{n-1}, vidíme ihned, že $a'_{n-1} = f'(b_1)$ jest dělitelno c_{n-1}, t. j. že $f'(b_1) \equiv 0 \pmod{c_{n-1}}$, a mají tudíž obě shody

$$f(x) \equiv 0, \; f'(x) \equiv 0 \pmod{c_{n-1}}$$

společný kořen $x = b_1$.

Uvažujme nyní obecněji $\varphi_r(x)$. Jestliže $P_{n-r}(x) = x^{n-r} + b_1 x^{n-r-1} + b_2 x^{n-r-2} + \ldots + b_{n-r}$, pak v rozdílu

$$P_{n-r}(x)\, \varphi_n(x) - f(x),$$

kterýž jest polynom stupně $n - 1$, lze voliti součinitele $b_1, b_2, \ldots, b_{n-r}$ tak, aby vymizely koeficienty při mocninách x stupňů $n - 1$, $n - 2, \ldots, r$. Tím se rozdíl redukuje na mnohočlen stupně $r - 1$ a ten, jelikož, dělen byv d_r, dává pro $x = \Theta$ celé alg. číslo, má součinitele vesměs dělitelny c_r. Tak dospíváme ke vztahu

$$P_{n-r}(x)\, \varphi_r(x) = c_r\, Q_{r-1}(x) + f(x). \qquad (+)$$

Dále, jelikož součin

$$\frac{\varphi_r(x)}{d_r}\, f'(x)$$

dává pro $x = \Theta$ polynom stupně $n - 1$ v Θ s celočíselnými součiniteli, jest

$$\varphi_r(x)\, f'(x) = d_r\, Q_{n-1}^{(1)}(x) + f(x)\, Q_{r-1}^{(2)}(x).$$

Pro $f'(x)$ lze psáti

$$f'(x) = P_{n-r}(x)\, Q_{r-1}^{(3)}(x) + Q_{n-r-1}^{(4)}(x).$$

Dosazením z rovnice poslední do předcházející a použitím $(+)$ máme

$$c_r\, Q_{r-1}(x)\, Q_{r-1}^{(3)}(x) + \varphi_r(x)\, Q_{n-r-1}^{(4)}(x) = d_r\, Q_{n-1}^{(1)}(x) + f(x)\, \overline{Q}(x).$$

Z této identity jest nejprve patrno, že součinitele v mnohočlenu $\overline{Q}$ jsou vesměs dělitelny číslem c_r (v případě, že $r - 1 < \frac{1}{2}n$, jsou dokonce rovny nule). Avšak pak ihned následuje, že i součinitele v $Q_{n-r-1}^{(4)}(x)$ jsou vesměs dělitelny číslem c_r a tedy

$$f'(x) \equiv P_{n-r}(x)\, Q_{r-1}^{(3)}(x) \pmod{c_r}.$$

Máme tak větu: Polynom $\varphi_r(x)$ base sestrojené podle věty I. jest podle modulu c_r dělitelem polynomu $f(x)$. Podíl $P_{n-r}(x)$ vznikající při dělení podle modulu c_r mnohočlenu $f(x)$ mnohočlenem $\varphi_r(x)$ jest pak dělitelem derivace $f'(x)$ rovněž podle modulu c_r, takže $f(x)$, $f'(x)$ mají $P_{n-r}(x)$ podle modulu c_r za společný dělitel.

Věta tato má praktický význam jenom v případě, že $c_r > 1$; je-li $c_r = 1$, jest $d_r = d_{r-1}$ a v tomto případě můžeme voliti $\varphi_r(x)$ podle rovnice

$$\varphi_r(x) = x\, \varphi_{r-1}(x).$$

III.

Pomocí symetrických funkcí můžeme konstruovati mnohočleny v x, jež pro $x = \Theta$ jsou dělitelny celými čísly (děliteli diskriminantu), existují-li vůbec takové mnohočleny. Nejjednodušší takové výrazy jsou dány mnohočleny

$$\overline{Q}_k(x) = \Sigma \Delta(\Theta_1, \Theta_2, \ldots, \Theta_k)^2 (x - \Theta_1)(x - \Theta_2) \ldots (x - \Theta_k),$$
$$k = 1, 2, \ldots, n - 1,$$

kde součet vztahuje se na všecky kombinace k-té třídy z n konjugovaných kořenů $\Theta, \Theta_1, \ldots, \Theta_{n-1}$ základní rovnice. $\Theta_k(x)$ jest zpravidla*) mnohočlen k-tého stupně; jeho součinitelé jsou celá čísla racionální. Lze jej psáti očividně ve tvaru determinantním

$$Q_k(x) = \begin{vmatrix} s_0, & s_1, & s_2, & \ldots, & s_{k-1}, & 1 \\ s_1, & s_2, & s_3, & \ldots, & s_k, & x \\ s_2, & s_3, & s_4, & \ldots, & s_{k+1}, & x^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ s_k, & s_{k+1}, & s_{k+2}, & \ldots, & s_{2k-1}, & x^k \end{vmatrix}.$$

Největší společnou míru součinitelů toho mnohočlenu označíme m_k.

Výraz $\Delta(\Theta, \Theta_1, \ldots, \Theta_{n-1})$ jest odmocnina z diskriminantu dané rovnice pro Θ, označíme ji (tu odmocninu) Δ_n. Prvočísla v diskriminantu obsažená budeme nazývati diskriminantní prvočísla; budeme je značiti $p_1, p_2, \ldots$ Pak $\Delta(\Theta_1, \Theta_2, \ldots, \Theta_k)$ jest dělitelno součinem $p_1^{\alpha_1} p_2^{\alpha_2} \ldots$, kde α_1, α_2 jsou čísla racionální; jsou-li ta čísla již taková, že žádný výraz $p_1^{\alpha'_1} p_2^{\alpha'_2} \ldots$, kde aspoň jedno z čísel α'_i jest větší ($>$) než α_i, není dělitelem výrazu $\Delta(\Theta_1, \Theta_2, \ldots, \Theta_k)$, označíme $p_1^{\alpha_1} p_2^{\alpha_2} \ldots$ znakem Δ_k a nazveme Δ_k nejvyšším dělitelem výrazu $\Delta(\Theta_1, \Theta_2, \ldots, \Theta_k)$. Stejný nejvyšší dělitel má ovšem výraz vznikající z $\Delta(\Theta_1, \Theta_2, \ldots, \Theta_k)$, nahradíme-li $\Theta_1, \Theta_2, \ldots, \Theta_k$ jakoukoliv jinou kombinací k-té třídy z čísel $\Theta, \Theta_1, \ldots, \Theta_{n-1}$.

V důsledku učiněného označení můžeme tvrditi:

$$\overline{Q}_k(\Theta) = \Sigma \Delta(\Theta_1, \Theta_2, \ldots, \Theta_k)^2 (\Theta - \Theta_1)(\Theta - \Theta_2) \ldots (\Theta - \Theta_k)$$

jest dělitelno $\Delta_{k+1}\Delta_k$. Aneb, což jest totéž: Mnohočlen

$$\frac{1}{m_k} \overline{Q}_k(x) \qquad (p)$$

pro $x = \Theta$ jest číslo algebraické dělitelné $\frac{\Delta_{k+1}\Delta_k}{m'_k}$, kde m'_k dostaneme z m_k tím, že v m'_k potlačíme všecky prvočíselné faktory, jež

*) Ve zvláštních případech může býti nižšího stupně než k-tého a může býti i roven identicky nule.

nejsou v Δ_{k+1}, a u těch, jež jsou v Δ_{k+1} a jejichž exponent převyšuje exponent v součinu $\Delta_{k+1}\,\Delta_k$ snížíme ten exponent tak, aby se rovnal exponentu v tom součinu. Jelikož Δ_k^2 jest, jak patrno, dělitelem čísla m'_k, můžeme tvrditi, že mnohočlen (p) jest dělitelný číslem

$$\frac{1}{n_k}\,\frac{\Delta_{k+1}}{\Delta_k};$$

při tom jest n_k tvaru $p_1^{b_1}p_2^{b_2}\ldots$, kdež $p_1, p_2, \ldots$ jsou prvočísla, jejichž vhodné mocniny jsou činitele součinu dávajícího Δ_{k+1}.

Největší celočíselný dělitel tohoto výrazu jest ovšem též dělitelem mnohočlenu (p), v němž za x dosazeno Θ.

K mnohočlenům $\overline{\mathrm{Q}}_k(x)$ dospějeme ještě jinou cestou. Očividně jest

$$\overline{\mathrm{Q}}_k(\Theta)\,\mathrm{f}'(\Theta) = \mathrm{Q}_k(\Theta)\,(\Theta-\Theta_1)\,(\Theta-\Theta_2)\ldots(\Theta-\Theta_{n-1}) =$$
$$= \Sigma\Delta(\Theta,\Theta_1,\ldots,\Theta_k)^2\,(\Theta-\Theta_{k+1})\,(\Theta-\Theta_{k+2})\ldots(\Theta-\Theta_{n-1}).$$

Označíme-li tudíž

$$\overline{\mathrm{R}}_{n-k-1}(x) = \Sigma\Delta(\Theta,\Theta_1,\ldots,\Theta_k)\,(x-\Theta_{k+1})\,(x-\Theta_{k+2})\ldots(x-\Theta_{n-1})$$

kde v součtu za $\Theta, \Theta_1, \ldots, \Theta_k$ jest dosazovati všecky kombinace $(k+1)$-vé třídy z $\Theta, \Theta_1, \ldots, \Theta_{n-1}$ a za $\Theta_{k+1}, \ldots, \Theta_{n-1}$ kombinaci doplňkovou, máme tento vztah mezi mnohočlenem $\overline{\mathrm{Q}}_k(x)$ a mnohočlenem stupně $n-k-1$ označeném $\overline{\mathrm{R}}_{n-k-1}(x)$

$$\overline{\mathrm{Q}}_k(\Theta)\,\mathrm{f}'(\Theta) = \overline{\mathrm{R}}_{n-k-1}(\Theta),$$

ze kteréhož následuje ihned identita

$$\overline{\mathrm{Q}}_k(x)\,\mathrm{f}'(x) - \overline{\mathrm{P}}_{k-1}(x)\,\mathrm{f}(x) = \overline{\mathrm{R}}_{n-k-1}(x), \qquad (q)$$

v níž $\overline{\mathrm{P}}_{k-1}(x)$ jest polynom stupně $k-1$ v x jednoznačně určený a s koeficienty celočíselnými (stejně jako polynomy $\overline{\mathrm{Q}}_k$, $\overline{\mathrm{R}}_{n-k-1}$).

Polynomy, k nimž jsme tak dospěli, jsou polynomy, jež dostaneme též algoritmem Euklidovým provedeným na $\mathrm{f}(x)$, $\mathrm{f}'(x)$. Při dělení $\mathrm{f}(x)$ mnohočlenem $\mathrm{f}'(x)$ obdržíme zpravidla zbytek v x stupně $n-2$, při druhém dělení pak zpravidla zbytek stupně $n-3$ atd. až při posledním dělení [$(n-1)$-vém] dostáváme zbytek stupně nultého. Může se však státi ve výjimečných případech, že stupně zbytků budou při postupných děleních podle algoritmu Euklidova nižší a že pak těch dělení resp. zbytků bude méně než $n-1$. Tento výjimečný případ předpokladem vyloučíme a budeme uvažovati jenom obecný případ, jež nazveme normální případ.

Označíme koeficient nejvyšší mocniny x v $\overline{\mathrm{R}}_{n-k}(x)$ předběžně $\overline{r}_{n-k}$. Polynom $\mathrm{f}'(x)$ značiti budeme též $\overline{\mathrm{R}}_{n-1}(x)$; jest tedy $\overline{r}_{n-1} = n$. Abychom získali přesně mnohočleny $\overline{\mathrm{R}}_{n-k}(x)$, jak svrchu byly

definovány, jest třeba prováděti algoritmus Euklidův podle předpisu daného rovnicemi

$$\begin{aligned}
\overline{r}_{n-1}^{\,2}\, \mathrm{f}(x) - \overline{\mathrm{S}}^{(1)}(x)\, \mathrm{f}'(x) &= -\overline{\mathrm{R}}_{n-2}(x),\\
\overline{r}_{n-2}^{\,2}\, \mathrm{f}'(x) - \overline{\mathrm{S}}^{(2)}(x)\, \overline{\mathrm{R}}_{n-2}(x) &= -\overline{r}_{n-1}^{\,2}\, \overline{\mathrm{R}}_{n-3}(x),\\
\overline{r}_{n-3}^{\,2}\, \overline{\mathrm{R}}_{n-2}(x) - \overline{\mathrm{S}}^{(3)}(x)\, \overline{\mathrm{R}}_{n-3}(x) &= -\overline{r}_{n-2}^{\,2}\, \overline{\mathrm{R}}_{n-4}(x),\\
&\cdots\cdots\cdots\cdots\\
\overline{r}_1^{\,2}\overline{\mathrm{R}}_2(x) - \overline{\mathrm{S}}^{(n-1)}(x)\, \overline{\mathrm{R}}_1(x) &= -\overline{r}_2^{\,2}\, \overline{\mathrm{R}}_0(x).
\end{aligned}$$

Postupem tímto bychom získali pro $\overline{\mathrm{R}}_k(x)$ celistvé součinitele i v případě, že by $a_1, a_2, \ldots, a_n$ byla neurčitá čísla (nezávisle proměnná).*)

$\mathrm{R}_0(x)$ jest diskriminant daný determinantem

$$\overline{\mathrm{R}}_0(x) = \begin{vmatrix} s_0, & s_1, \ldots, & s_{n-1} \\ s_1, & s_2, \ldots, & s_n \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ s_{n-1}, & s_n, \ldots, & s_{2n-2} \end{vmatrix} = \Delta(\Theta, \Theta_1, \ldots, \Theta_{n-1})^2.$$

Naznačené dělení ještě lze poněkud zjednodušiti. Součinitele v jednotlivých zbytcích mohou míti společnou míru různou od 1. Mají-li na př. součinitele v $\overline{\mathrm{R}}_{n-2}(x)$ společnou míru m, pak kdybychom dělení prováděli naznačeným způsobem, byly by součinitele v $\overline{\mathrm{R}}_{n-3}$, $\overline{\mathrm{R}}_{n-4}, \ldots, \overline{\mathrm{R}}_0$ dělitelny po řadě čísly $m^2, m^3, \ldots, m^{n-1}$. A obdobně se to má i při jiných zbytcích. Majíce tuto okolnost na mysli, můžeme největší společnou míru, než provádíme dělení, napřed krácením odstraniti a prováděti postupná dělení podle tohoto předpisu:

$$\begin{aligned}
r_{n-1}^{\,2}\, \mathrm{f}(x) - \mathrm{S}^{(1)}(x)\, \mathrm{R}_{n-1}(x) &= -e_1\, \mathrm{R}_{n-2}(x),\\
r_{n-2}^{\,2}\, \mathrm{R}_{n-1}(x) - \mathrm{S}^{(2)}(x)\, \mathrm{R}_{n-2}(x) &= -r_{n-1}^{\,2} e_2\, \mathrm{R}_{n-3}(x),\\
r_{n-3}^{\,2}\, \mathrm{R}_{n-2}(x) - \mathrm{S}^{(3)}(x)\, \mathrm{R}_{n-3}(x) &= -r_{n-2}^{\,2} e_3\, \mathrm{R}_{n-4}(x),\\
&\cdots\cdots\cdots\cdots\\
r_1^{\,2}\, \mathrm{R}_2(x) - \mathrm{S}^{(n-1)}(x)\, \mathrm{R}_1(x) &= -r_2^{\,2} e_{n-1}.
\end{aligned} \qquad (\mathrm{I})$$

V něm jsou $\mathrm{R}_k(x)$ již mnohočleny mající za součinitele čísla celá bez společné míry, r_k pak značí součinitel při nejvyšší mocnině proměnné x. Mezi $\overline{\mathrm{R}}_k(x)$ a $\mathrm{R}_k(x)$ jsou pak tyto vztahy:

$$\begin{aligned}
\mathrm{f}'(x) &= e_0\, \mathrm{R}_{n-1}(x),\ \overline{\mathrm{R}}_{n-2}(x) = e_0^{\,2} e_1\, \mathrm{R}_{n-2}(x),\\
\overline{\mathrm{R}}_{n-3}(x) &= e_0^{\,3} e_1^{\,2} e_2\, \mathrm{R}_{n-3}(x),\ \overline{\mathrm{R}}_{n-4}(x) = e_0^{\,4} e_1^{\,3} e_2^{\,2} e_3\, \mathrm{R}_{n-4}(x), \ldots
\end{aligned}$$

Diskriminant pak jest rovný $e_0^{\,n} e_1^{\,n-1} e_2^{\,n-2} \ldots e_{n-2}^{\,2} e_{n-1}$; za $\mathrm{R}_0(x)$ klademe 1, $\mathrm{R}_0(x) = 1$.

*) V tomto případě by součinitele $\overline{\mathrm{R}}_k(x)$ byly mnohočleny v $a_1, a_2, \ldots$ s celočíselnými koeficienty.

Eliminací dostáváme z rovnic (I) rovnice tvaru

$$Q_k(x)\, R_{n-1}(x) - P_{k-1}(x)\, f(x) = e_1 e_2 \ldots e_k\, R_{n-k-1}(x);$$
$$k = 1, 2, \ldots, n-1. \qquad \text{(II)}$$

Porovnáme-li rovnici poslední s rovnicí (q), vidíme, že

$$\overline{Q}_k(x) = e_0^k e_1^{k-1} \ldots e_{k-1}\, Q_k(x).$$

Dosadíme-li dále do rovnice (II) za x číslo Θ, máme

$$Q_k(\Theta)\, R_{n-1}(\Theta) = e_1 e_2 \ldots e_k\, R_{n-k-1}(\Theta). \qquad \text{(II')}$$

Formule (I) a (II) jsou pro konstrukci base velmi užitečny; již okolnost, že algoritmus (I) nám dává diskriminant — číslo pro konstrukci base nezbytné a pro studium tělesa $K(\Theta)$ potřebné — to potvrzuje. Čísla $e_1, e_2, \ldots$ nás pak orientují o různých možnostech pro $d_1, d_2, \ldots, d_{n-1}$. Jest totiž, jak z odst. I. ihned vysvítá,

$$(d_1 d_2 \ldots d_k)^2 \text{ dělitelem součinu } e_0^{k+1} e_1^{k} \ldots e_{k-1}^{2} e_k$$

pro $k = 1, 2, \ldots, n-1$; z těchto $n-1$ podmínek vychází konečný počet systémů možných pro čísla $d_1, d_2, \ldots, d_{n-1}$; při tom ovšem musí pro $d_1, d_2, \ldots$ býti splněny ještě jisté podmínky, zejména pak podmínka, že d_k jest dělitelno součinem $d_1^{r_1} d_2^{r_2} d_3^{r_3} \ldots$, kde čísla celá $r_1, r_2, \ldots$ hoví rovnici $r_1 + 2r_2 + 3r_3 + \ldots \leqq k$.

Avšak to není jediný užitek, který nám poskytuje algoritmus Euklidův. Mnohočleny $Q_k(x)$ jsou v úzkém vztahu k polynomům base $\varphi_k(x)$; ve většině případů nám $Q_k(x)$ tyto polynomy bezprostředně (anebo aspoň po snadném počtu) dávají. Objasním to aspoň na jednom jednoduchém případě. Nechť jest

$$e_0 = 1,\ e_1 = 1,\ e_2 = 1, \ldots, e_{n-2} = 1,\ e_{n-1} = d^2 f.$$

kde d, f jsou celá racionální čísla, f pak nemá žádný dělitel, jenž by byl kvadrátem celého rac. čísla. Pak jest $d_1 = 1$, $d_2 = 1, \ldots, d_{n-2} = 1$. Jmenovatel d_{n-1} jest pak dělitelem čísla d. Rovnici (II') pro $k = n-1$ lze psáti ve tvaru

$$Q_{n-1}(\Theta)\, f'(\Theta) = d^2 f.$$

Není-li společná míra součinitelů v mnohočlenu $Q_{n-1}(x)$ soudělna s d, nemá i součinitel při x^{n-1} v tom mnohočlenu společnou míru s d. Jelikož pak podle poslední rovnice číslo algebraické

$$\frac{Q_{n-1}(\Theta)}{d}$$

jest celé algebraické číslo, jest mnohočlen $\varphi_{n-1}(x)$ daný vztahem

$$\varphi_{n-1}(x) = r\, Q_{n-1}(x) + d\, T_{n-1}(x)$$

polynomem base. Při tom jest r číslo celé a $T_{n-1}(x)$ celočíselný polynom stupně $n-1$, obojí vázané pouze podmínkou, aby

součinitel při x^{n-1} ve $\varphi_{n-1}(x)$ byl rovný 1. Podmínka ta jest jistě splnitelna, není-li součinitel při x^{n-1} ve $Q_{n-1}(x)$ soudělný s d (jakž předpokládáme). Ostatní mnohočleny base v uvažovaném případě jsou 1, x, $x^2, \ldots, x^{n-2}$.

IV.

Ve složitějších případech jest možno daný úkol — sestrojiti basi k danému tělesu algebraickému — rozložiti na jednodušší.

Nejprve lze — obsahují-li jmenovatele $d_1, d_2, \ldots, d_{n-1}$ různé prvočinitele $p_1, p_2, \ldots$ — provésti rozklad toho úkolu tím, že uvažujeme basi vzhledem k jednotlivým prvočinitelům.

Pod basi tělesa $K(\Theta)$ vzhledem k prvočíslu p budeme vyrozumívati n čísel celých tvaru

$$\frac{b_0 + b_1\Theta + \ldots + b_{n-1}\Theta^{n-1}}{p^r},$$

— označme je $\overline{\omega}_1, \overline{\omega}_2, \ldots, \overline{\omega}_n$ —, tak že každé celé číslo $\overline{\omega}$ toho tvaru se dá vyjádřiti vztahem

$$\overline{\omega} = f_1\overline{\omega}_1 + f_2\overline{\omega}_2 + \ldots + f_n\overline{\omega}_n.$$

I v tomto případě lze $\overline{\omega}_k$ voliti tak, že jest

$$\overline{\omega}_k = \frac{\overline{\varphi}_{k-1}(\Theta)}{p^{r_{n-1}}}, \quad k = 1, 2, \ldots, n,$$

kde

$$\overline{\varphi}_k(x) = x^k + \overline{c}_{k1}x^{k-1} + \ldots + c_{kk}, \quad \overline{\varphi}_0(x) = 1$$

a jsou platny s náležitou obměnou věty odstavců I. a II. pro tyto mnohočleny $\overline{\varphi}_k(x)$.

Dále jest patrno, že známe-li base algebraického tělesa vzhledem ke všem prvočíslům dělícím jmenovatele d_k, $k = 1, 2, \ldots, n - 1$, dovedeme pomocí snadných operací aritmetických sestrojiti mnohočleny $\varphi_k(x)$ v obecné basi tělesa.

Avšak to není jediný rozklad zjednodušující náš úkol. I úkol sestrojiti basi vzhledem k prvočíslu p dá se dále (zpravidla) rozkladem zjednodušiti. Jestliže p jest dělitelem některých jmenovatelů d_k, pak podle modulu p jest platný tento rozklad (viz v I. větu IV.)

$$f(x) \equiv \psi_1(x)^{v_1}\,\psi_2(x)^{v_2} \ldots \psi_s(x)^{v_s} \pmod{p},$$

kde $\psi_1(x)$, $\psi_2(x), \ldots$ jsou mod p ireducibilní mnohočleny stupňů $n_1, n_2, \ldots$ a různé podle mod p. Je-li m číslo celé rac. větší než exponent nejvyšší mocniny prvočísla p obsažené v diskriminantu mnohočlenu $f(x)$, pak v důsledku uvedeného rozkladu jest platný další rozklad (ať jest m jakkoliv veliké)

$$f(x) \equiv P_1(x) \,.\, P_2(x) \ldots P_s(x) \pmod{p^m}.$$

Při tom jest při určitém m

$$P_i(x) = \psi_i(x)^{v_i} + p\, Q_i(x),$$

$Q_i(x)$ mnohočlen stupně $< n_i v_i$. Resultanty dvou polynomů $P_i(x)$, $P_j(x)$ při $i \neq j$ nejsou dělitelny p. A tu stačí sestrojiti base tělesa $K(\vartheta_i)$, kde $P_i(\vartheta_i) = 0$, vzhledem k prvočíslu p, abychom dospěli k basi tělesa $K(\Theta)$ daného vzhledem k p.

Jsou-li totiž výrazy pro basi tělesa $K(\vartheta_1)$ vzhledem k p*)

$$1, \frac{\psi_1(x)}{p^{q_1}}, \quad \frac{\psi_2(x)}{p^{q_2}}, \ldots, \frac{\psi_{m_1-1}(x)}{p^{q_{m_1-1}}}, \quad m_1 = n_1 v_1,$$

a dále výrazy pro basi tělesa $K(\vartheta_2)$

$$1, \frac{\psi'_1(x_1)}{p^{s_1}}, \quad \frac{\psi'_2(x)}{p^{s_2}}, \ldots, m_2 = n_2 v_2.$$

pak nejprve

$$0 \leqq q_1 \leqq q_2 \leqq q_3 \leqq \ldots \leqq q_{m_1-1}, \quad 0 \leqq s_1 \leqq s_2 \leqq \ldots \leqq s_{m_2-1}.$$

Srovnáme-li čísla q_i, s_i v jednu řadu podle velikosti, která bude na př.

$$0 \leqq q_1 < q_2 < s_1 < s_2 < q_3 < s_3 < q_4 < \ldots < q_{m_2-1},$$

pak výrazy pro basi vzhledem k p tělesa $K(\vartheta')$, kde $g(\vartheta') = 0$ a

$$g(\vartheta') \equiv P_1(x)\, P_2(x) \pmod{p^m},$$

budou očividně dány výrazy

$$1, x, \frac{\psi_1(x)\,\psi'_1(x)}{p^{q_1}}, \frac{\psi_2(x)\,\psi'_1(x)}{p^{q_2}}, \frac{\psi_3(x)\,\psi'_1(x)}{p^{s_1}}, \frac{\psi_3(x)\,\psi'_2(x)}{p^{s_2}},$$

$$\frac{\psi_3(x)\,\psi'_3(x)}{p^{q_3}}, \frac{\psi_4(x)\,\psi'_3(x)}{p^{s_3}}, \frac{\psi_4(x)\,\psi'_4(x)}{p^{s_4}}, \ldots, \frac{P_1(x)\,\psi'_{m_2-1}(x)}{p^{s_{m_2-1}}}.$$

a obdobně i v případě, kdy levá strana rovnice určující číslo ϑ' se rozpadá na libovolný počet činitelů.

Avšak i pro konstrukci base těles $K(\vartheta_i)$ lze, jestliže $P_i(x)$ podle modulu p^m jest reducibilní, odvoditi podobné rozklady a některé další věty, o nichž však tu nehodlám se šířiti, jelikož bych nemohl pohodlně k rozkladům těm dojíti bez zavedení imaginárních čísel Galoisových a výklad příslušný by tím velice vzrostl.

---

*) Prvních n_1 členů se redukuje ostatně na $1, x, x^2, \ldots, x^{n_1-1}$ a i v následujících členech se periodicky opětují obdobná zjednodušení.