Acta Universitatis Carolinae. Mathematica

Ivan Friš

O basích celých čísel v obecných tělesech algebraiských

Acta Universitatis Carolinae. Mathematica, Vol. 1 (1960), No. 3, 67--122

Persistent URL: http://dml.cz/dmlcz/142120

1960 Acta Universitatis Carolinae — Mathematica no. 3, pag. 67—122.

O BASÍCH CELÝCH ČÍSEL V OBECNÝCH TĚLESECH ALGEBRAICKÝCH

О БАЗИСАХ ЦЕЛЫХ ЧИСЕЛ В ОБЩИХ АЛГЕБРАИЧЕСКИХ ПОЛЯХ

ÜBER DIE BASEN GANZER ZAHLEN IN ALLGEMEINEN ALGEBRAISCHEN KÖRPERN

Ivan Friš

(Došlo 13. ledna 1960)

Prof. Karel Petr vyslovil v práci [1] bez důkazu řadu vět o basích celých čísel v obecných algebraických tělesech, pomocí nichž lze numericky vypočítat tyto base. Na podnět akademika Vladimíra Kořínka se autor tohoto článku pokusil doplnit chybějící důkazy tím že přenesl některé věty z teorie algebraických číselných těles na jisté okruhy. Touto metodou se podařilo dokázat všechny uvedené věty s výjimkou dvou, jejichž znění bylo třeba opravit. Mimo to obsahuje práce ještě některé další nové výsledky.

ZÁKLADNÍ DEFINICE

K bude značit těleso racionálních čísel,

J obor integrity celých racionálních čísel.

$K[x]$ resp. $J[x]$ je obor integrity polynomů jedné neurčité x nad K resp. nad J.

$J'[x]$ je pak ta podmnožina $J[x]$ polynomů, jejichž vedoucí koeficient je rovný jedné.

K_f označuje okruh $K[x]/\{f(x)\}$, podílový okruh $K[x]$ podle hlavního ideálu vytvořeného polynomem $f(x)$. O polynomu $f(x)$ budeme předpokládat vždy, že $f(x) \in J'[x]$ a počínaje paragrafem 2 ještě navíc, že $f(x)$ má pouze jednoduché kořeny.

Δ_f nechť označuje diskriminant polynomu $f(x)$ a

$Exp_q a$ značí nejvyšší mocninu prvočísla q, která dělí a:

$$q^{Exp_q a} \mid a, \quad q^{Exp_q a+1} \nmid a.$$

§1. *Definice* K_f.

K_f je komutativní okruh obecně s děliteli nuly.

Df. 1.

Písmenem Θ (nebo přesněji Θ_f) označme třídu, která obsahuje prvek x. Prvku Θ budeme říkat generátor K_f.
V K_f existuje množina prvků isomorfní s K. Tuto množinu pro jednoduchost s K ztotožníme. Je tedy $K_f \supset K$.

Platí

$$f(\Theta) = 0; \quad v(\Theta) = v'(\Theta) \Leftrightarrow f(x)/v(x) - v'(x) \text{ ap.}$$

Každý prvek $z \in K_f$ dá se jednoznačně psát ve tvaru

$$z = a_0 + a_1\Theta + \ldots + a_k\Theta^k, \; a_i \in K, \; k < n.$$

Převedeme-li všechna racionální čísla na společného jmenovatele, lze psát

$$z = \frac{a_0 + a_1\Theta + \ldots + a_{n-1}\Theta^{n-1}}{d},$$

přičemž $\quad a_i \in J; \; (a_0, \ldots, a_{n-1}) = 1, \; d \in J, \; 0 < d.$

Závěrem lze říci, že každý prvek $z \in K_f$ lze jednoznačně psát ve tvaru $z = \frac{\varphi(\Theta)}{d}$; $\varphi(t) \in J[t]$, $d \in J$, $0 < d$, φ je primitivní.

K_f je algebra hodnosti n nad K, proto každý prvek $z \in K_f$ je kořenem nějakého polynomu nejmenšího stupně z $K[t]$ s vedoucím koeficientem rovným 1. Označme tento polynom $\boldsymbol{P}_z(t)$. Zřejmě platí

$$Q(t) \in K[t], \; Q(z) = 0 \Rightarrow \boldsymbol{P}_z(t)/Q(t).$$

V obecném případě, tj. pro f reducibilní, není minimum polynom nutně ireducibilní.

V 1,1.

Buď $f_1(x) = f_2(x).f_3(x)$; $f_i(x) \in J'[x]$ $(i = 1, 2, 3)$; $(f_2(x); f_3(x)) = 1$.

Potom platí

$$K_{f_1} \cong K_{f_2} \dotplus K_{f_3}.$$

Důkaz:

Buďte Θ_i generátory K_{f_i}. Najděme polynomy $k(x), h(x)$, že

$$(1) \; f_2(x)h(x) + f_3(x)k(x) = 1.$$

Pro každé dva polynomy $\varphi(x)$, $\psi(x) \in K[x]$ definujme zobrazení ι_1, ι_2 vztahy

$$\iota_1\varphi(\Theta_1) = [\varphi(\Theta_2),\ \varphi(\Theta_3)],$$
$$\iota_2[\varphi(\Theta_2);\ \psi(\Theta_3)] = \varphi(\Theta_1)f_3(\Theta_1)k(\Theta_1) + \psi(\Theta_1)f_2(\Theta_1)k(\Theta_1).$$

ι_1 je zřejmě homomorfismus. Spočteme

$$\iota_1\iota_2[\varphi(\Theta_2);\ \psi(\Theta_3)] = \iota_1(\varphi(\Theta_1)f_3(\Theta_3)k(\Theta_1) + \psi(\Theta_1)f_2(\Theta_1)k(\Theta_1)) =$$
$$= [\varphi(\Theta_2)f_3(\Theta_2)k(\Theta_2);\quad \psi(\Theta_3)f_2(\Theta_3)k(\Theta_3)] = [\varphi(\Theta_2);\quad \psi(\Theta_3)],$$

neboť $$f_2(\Theta_2) = f_3(\Theta_3) = 0$$

a dosazení Θ_2 resp. Θ_3 do (1) dá $f_3(\Theta_2)k(\Theta_2) = f_2(\Theta_3)h(\Theta_3) = 1$. Stejně $\iota_2\iota_1 z = z$ pro každé $z \in K_{f_1}$.
Je tedy $\iota_1\iota_2$ identita na $K_{f_1} + K_{f_2}$ a stejně $\iota_2\iota_1$ je identické na K_{f_1}. Obě zobrazení proto jsou navzájem inversní a jsou isomorfismy.

Analogicky platí

Je-li $f_1(x) = \prod_{i=2}^{n} f_i(x)$ a pro každé $2 \leqslant i \neq j \leqslant n$ je $(f_i(x);\ f_j(x)) = 1$,

pak taky $$K_{f_1} = \sum_{i=2}^{n}{}_d\, K_{f_i}.$$

Důkaz se provede indukcí.

Df. 2.

Isomorfismy sestrojené ve větě 1,1 budu vždy značit písmeny ι_1, ι_2.

§2. *Celá čísla.*

Df. 3.

Buď $f(x) \in J'[x]$. Polynom $f(x)$ měj jen jednoduché kořeny. Označme I_f množinu těch prvků $z \in K_f$, jejichž minimální polynom má celočíselné koeficienty a vedoucí koeficient rovný 1.

Tedy
$$J_f = \mathop{\mathscr{E}}_{\nu}(y \in K_f,\ \ \boldsymbol{P}_\nu(t) \in J'[t]).$$

Prvky $z \in J_f$ nazýváme celé prvky.

V 2,1.

Prvek $z \in J_f$ je celý právě tehdy, je-li kořenem nějakého, ne nutně minimálního polynomu $Q(t)$:
$$Q(z) = 0,\quad Q(t) \in J'[x].$$

Důkaz plyne ihned z Gaussovy věty o primitivních polynomech.

V 2,2.

Buď $f(x) = f_1(x)f_2(x)$, oba polynomy nesoudělné a s jednoduchými kořeny. Označme $\iota_1 z = [z_1, z_2]$. Pak platí
$$z \in J_f \Leftrightarrow z_1 \in J_{f_1},\ z_2 \in J_{f_2}.$$

Důkaz:

1. Nechť $z \in J_f$. Pak $\boldsymbol{P}_z(t) \in J'[t]$.

V okruhu $J_{f_1} + J_{f_2}$ platí

$$[\boldsymbol{P}_z(z_1), \boldsymbol{P}_z(z_2)] = \boldsymbol{P}_z([z_1, z_2]) = \boldsymbol{P}_z(\iota_1 z) = \iota_1 \boldsymbol{P}_z(z) = \iota_1 0 = [0; 0];$$

tedy $\boldsymbol{P}_z(z_1) = \boldsymbol{P}_z(z_2) = 0$, tedy $z_1 \leq J_{f_1}$, $z_2 \leq J_{f_2}$.

2. Buď $z_1 \in J_{f_1}$, $z_2 \in J_{f_2}$. Položme $P(t) = \boldsymbol{P}_{z_1}(t)\boldsymbol{P}_{z_2}(t)$. Je zřejmě $P(t) \in J'[t]$.

V okruhu J_f platí

$$P(z) = P(\iota_2[z_1, z_2]) = \iota_2 P([z_1, z_2]) = \iota_2[P(z_1), P(z_2)] = \iota_2[0, 0] = 0.$$

A opět podle věty 2,1 je $z \in J_f$.
Poznamenejme, že věta 2,2 nám umožňuje dokázat, že J_f je okruh i v případě, že f je reducibilní.
Dále budeme vždy o polynomech $f(x)$, pro něž tvoříme K_f, předpokládat, že mají jednoduché kořeny.

§3. *Přidružené vektory.*

Označme A_n direktní součet n sčítanců

$$A_n = A \dotplus \ldots \dotplus A,$$

kde A je těleso všech algebraických (komplexních) čísel.
Buď $f(x) \in J'[x]$ a buď Θ generátor K_f.
Buď $\varphi(x) \in K[x]$ a konečně buďte $\vartheta_1, \vartheta_2, \ldots \vartheta_n$ kořeny rovnice $f(x) = 0$ v tělese A.

V 3,1

Zobrazení $\varkappa$ definované rovnicí

$$\varkappa\varphi(\Theta) = \{\varphi(\vartheta_1), \varphi(\vartheta_2), \ldots, \varphi(\vartheta_n)\}$$

je isomorfismus K_f do A_n.

Důkaz:

$\varphi(\Theta)$ je ovšem obecný prvek $\in K_f$.

Buďte φ, ψ dva libovolné polynomy. Je zřejmě

$$\varkappa(\varphi(\Theta) + \psi(\Theta)) = \varkappa\varphi(\Theta) + \varkappa\psi(\Theta)$$
$$\varkappa(\varphi(\Theta).\psi(\Theta)) = \varkappa\varphi(\Theta).\varkappa\psi(\Theta).$$

Nechť platí

$\varkappa\varphi(\Theta) = \varkappa\psi(\Theta)$, tj. podle definice zobrazení $\varphi(\vartheta_i) = \psi(\vartheta_i)$ pro každé $1 \leqslant i \leqslant n$. Pišme $(\varphi(x) - \psi(x)) = h(x).f(x) + g(x)$, kde stupeň $g(x) < n$. Dosazení ϑ_i za x dá $g(\vartheta_i) = 0$ pro každé $i \leqslant n$. Ovšem nenulový polynom stupně menšího než n nemůže míti n různých kořenů (po-

znamenávám pro úplnost, že od §2 stále bereme f bez vícenásobných kořenů). Je $g(x) = 0$, a tedy $f(x)/\psi(x) - \varphi(x)$, neboli dle poznámky za Df1

$$\varphi(\Theta) = \psi(\Theta).$$

Tedy zobrazení je prosté.

Df 4

Buď $z \in K_f$ a nechť $z = \varphi(\Theta)$. Prvek $\varkappa z = \{\varphi(\vartheta_1), \ldots, \varphi(\vartheta_n)\}$ nazveme vektorem přidruženým k prvku z.

V 3,2

Buď $f(x) = g(x).h(x)$, f, g nesoudělné. Je pak

$$K_f = K_g + K_h.$$

Je-li $u \in K_g, v \in K_h$, a označíme-li $\iota_2[u, v] = z$, pak o přidružených vektorech k prvkům u, v

$$\{\omega_1, \ldots, \omega_n\}, \quad \{\varphi_1, \ldots, \varphi_m\}$$

platí

$$\varkappa z = \{\omega_1, \omega_2, \ldots, \omega_n, \varphi_1, \varphi_2, \ldots, \varphi_m\}$$

nebo případně jsou čísla ω_i, φ_j jinak uspořádána.

Důkaz:

Označme $\vartheta_1, \ldots, \vartheta_n$ kořeny polynomu $g(x)$, $\vartheta_{n+1}, \ldots, \vartheta_{n+m}$ kořeny polynomu $h(x)$.

Jsou tedy

$$\vartheta_1, \vartheta_2, \ldots, \vartheta_{n+m} \text{ kořeny } f(x).$$

Označme $z = \varphi(\Theta)$, $u = \psi(\Omega)$, $v = X(\Phi)$. Je
$\omega_i = \psi(\vartheta_i)$ pro $1 \leqslant i \leqslant n$,
$\varphi_i = X(\vartheta_{i+n})$ pro $1 \leqslant i \leqslant m$ (po vhodném přečíslování ϑ_i).

Dále je z věty 1,1

$\varphi(x) = g(x)k(x)X(x) + h(x).l(x)\psi(x)$ pro k, l takové, že $k(x)g(x) + h(x)l(x) = 1$.

Je tedy

$\varkappa z = [\ldots, g(\vartheta_i)k(\vartheta_i)X(\vartheta_i) + h(\vartheta_i)l(\vartheta_i)\psi(\vartheta_i), \ldots]$. Buď nejprve $1 \leqslant i \leqslant n$. Je $g(\vartheta_i) = 0$ a $k(\vartheta_i)g(\vartheta_i) + h(\vartheta_i)l(\vartheta_i) = 1$, tj. $h(\vartheta_i)l(\vartheta_i) = 1$, neboli $g(\vartheta_i)k(\vartheta_i)X(\vartheta_i) + h(\vartheta_i)l(\vartheta_i)\psi(\vartheta_i) = \psi(\vartheta_i) = \omega_i$ a stejně pro $n + 1 \leqslant i \leqslant m + n$

$$g(\vartheta_i)k(\vartheta_i)X(\vartheta_i) + h(\vartheta_i)l(\vartheta_i)\psi(\vartheta_i) = X(\vartheta_i) = \varphi_{i-n}, \text{ což dá větu.}$$

Vektor $\varkappa z$ ve skutečnosti nezávisí na prvku Θ, nýbrž pouze na prvku z.

Df 5

Buď $z \in K_f$, $z = \varphi(\Theta)$. Položme

$$P'_\varphi(t) = P'_\varphi(t; x_1, \ldots, x_n) = \prod_{i=1}^{n} (t - \varphi(x_i)) \in K[t; x_1, \ldots, x_n].$$

Buď σ nějaká permutace prvků $x_1, \ldots, x_n$. Je zřejmě

$P'_\varphi(t; \sigma x_1, \sigma x_2, \ldots, \sigma x_n) = P'_\varphi(t; x_1, \ldots, x_n)$, a tedy podle věty o symetrických funkcích platí

$P'_\varphi(t; x_1, \ldots, x_m) = P''_\varphi(t; \alpha_1, \ldots, \alpha_n)$; kde jsme označili

$\alpha_i = (-1)^i \Sigma x_1 x_2 \ldots x_i$ i-tou elementární symetrickou funkci.

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

položme konečně

$$P_z(t) = P''_\varphi(t; a_1, a_2, \ldots, a_n).$$

V 3,3

$$P_z(z) = 0.$$

Důkaz:

$$\text{Je } P'_\varphi(z; x_1, \ldots, x_n) = \prod_{i=1}^{n} (\varphi(\Theta) - \varphi(x_i)) =$$

$$= \prod_{i=1}^{n} [(\Theta^k - x_i^k) + f_1(\Theta^{k-1} - x_i^{k-i}) + \ldots] = \prod_{i=1}^{n} (\Theta - x_i)\, \zeta_i(\Theta, x_i) =$$

$$= (\Theta - x_1)(\Theta - x_2) \ldots (\Theta - x_n)\, \zeta(\Theta, x_1, \ldots, x_n) =$$

$$= (\Theta^n + \alpha_1 \Theta^{n-1} + \ldots + \alpha_n)\, \zeta'(\Theta, \alpha_1, \ldots, \alpha_n).$$

Tedy $P''_\varphi(z, a_1, \ldots, a_n) = 0$, neboť $f(\Theta) = 0$.

V 3,4

Buď $z \in K_f$, pak

(1) $\quad P_z(t) = (t - \zeta_1)(t - \zeta_2) \ldots (t - \zeta_n)$, kde $\{\zeta_1, \zeta_2, \ldots, \zeta_n\} = \varkappa z$.

Důkaz:

Je $\zeta_i = \varphi(\vartheta_i)$, je-li $z = \varphi(\Theta)$, poněvadž $f(\vartheta_i) = 0$. Dokážeme jako v předcházející větě $P_z(\zeta_i) = 0$. Rozklad (1) je rozklad v A a je jediný.

V 3,5

Označme pro $z \in K_f$

$\varkappa z = \{z_1, z_2, \ldots, z_n\}$. Platí

$z \in J_f$, právě když všechna z_i $(1 \leqslant i \leqslant n)$ jsou celá algebraická čísla.

Důkaz:

1. Buď $z \in J_f$. Existuje polynom $P(t) \in J'[t]$, že $P(z) = 0$. Je však $P(z_i) = 0$, neboť zobrazení $z \to z_i$ je homomorfismus.

2. Jsou-li z_i celá algebraická, je $P(t) = (t - z_1)(t - z_2) \ldots (t - z_n) \in J'[t]$, ale podle V 3,4 je $P(z) = 0$.

Z toho speciálně plyne:

V 3,6

$P_z(t) \in J'[t]$, právě když $z \in J_f$.

§4. *Diskriminant.*

Df 6

Buďte $\omega_1, \omega_2, \ldots, \omega_n \in K_f$ libovolné prvky. Buď $\{\omega_i^{(1)}, \omega_i^{(2)}, \ldots, \omega_i^{(n)}\}$ přidružený vektor k ω_i. Položme

$$D(\omega) = D(\omega_1, \ldots, \omega_n) = \begin{vmatrix} \omega_1^{(1)} \omega_2^{(1)} \ldots \omega_n^{(1)} \\ \omega_1^{(2)} \omega_2^{(2)} \ldots \omega_n^{(2)} \\ \ldots\ldots\ldots\ldots \\ \omega_1^{(n)} \omega_2^{(n)} \ldots \omega_n^{(n)} \end{vmatrix}^2.$$

Číslo $D(\omega) \in A$ zveme diskriminantem n-tice ω.

Df 7

Je-li $\omega_1', \omega_2', \ldots, \omega_n'$ jiná n-tice a platí-li

1. $\omega_i' = \sum_{k=1}^{n} c_{ik}\omega_k$, $c_{ik} \in K$, pak matici

$$\begin{Vmatrix} c_{11} c_{12} \ldots c_{1n} \\ c_{21} c_{22} \ldots c_{2n} \\ \ldots\ldots\ldots\ldots \\ c_{n1} c_{n2} \ldots c_{nn} \end{Vmatrix}$$

označíme $\boldsymbol{D}(\omega', \omega)$ a nazveme maticí přechodu.
Její determinant označený $D(\omega', \omega)$ pak nazveme determinantem přechodu.

V 4,1

Platí

$D(\omega') = D^2(\omega', \omega)\, D(\omega)$ pro ty n-tice, pro něž platí (1).

Důkaz:

Platí-li $\omega_i' = \Sigma c_{ik}\,\omega_k$, pak z vlastnosti isomorfismu $\varkappa$ je

$$[\ldots, \omega_i'^{(j)}, \ldots] = \Sigma c_{ik}[\ldots, \omega_k^{(j)}, \ldots] = [\ldots, \Sigma c_{ik}\,\omega_k^{(j)}, \ldots],$$

tedy $\omega_i'^{(j)} = \Sigma c_{ik}\omega_k^{(j)}$, a proto

$$\begin{vmatrix} \omega_1'^{(1)} \ldots \omega_n'^{(1)} \\ \ldots\ldots\ldots \\ \omega_1'^{(n)} \ldots \omega_n'^{(n)} \end{vmatrix} = \begin{vmatrix} \sum_k c_{1k}\,\omega_k^{(1)} \ldots \sum_k c_{nk}\,\omega_k^{(1)} \\ \ldots\ldots\ldots\ldots\ldots \\ \sum_k c_{1k}\,\omega_k^{(n)} \ldots \sum_k c_{nk}\,\omega_k^{(n)} \end{vmatrix} = \begin{vmatrix} c_{11} \ldots c_{1n} \\ \ldots\ldots\ldots \\ c_{n1} \ldots c_{nn} \end{vmatrix} \cdot \begin{vmatrix} \omega_1^{(1)} \ldots \omega_n^{(1)} \\ \ldots\ldots\ldots \\ \omega_1^{(n)} \ldots \omega_n^{(n)} \end{vmatrix}$$

Věta pomocná

Buď Θ generátor J_f. Je

$$D(1, \Theta, \Theta^2, \ldots, \Theta^{n-1}) = \Delta_f.$$

Skutečně je $D(\omega)$, jak byl definován, čtverec Vandermondova determinantu a ten je, jak je známo, právě roven diskriminantu polynomu $f(x)$.

V 4,2

Buď $\omega_i = \dfrac{\varphi_i(\Theta)}{d_i}$, $\varphi_i(x) \in J[x]$, $d_i \in J$. Pak je

1. $D(\omega) = \dfrac{a^2}{d_1^2 \ldots d_n^2}\Delta_f$, při čemž $a \in J$. Tedy speciálně
2. $D(\omega) \in K$ pro každou n-tici $\omega_1, \ldots, \omega_n \in K_f$.
3. Jsou-li všechna $\omega_i \in J_f$, je
$$D(\omega) \in J.$$
4. $D(\omega) \neq 0$ právě tehdy, jsou-li prvky ω_i lineárně nezávislé nad K.

Důkaz:

1. Buď $\varphi_i(x) = \sum_{j=1}^{n} c_{ij}x_j^{-1}$, $c_{ij} \in J$. Zvolme $\langle\omega'\rangle = \langle 1, \Theta, \ldots, \Theta^{n-1}\rangle$.

Je podle 4,1 a pomocné věty

$D(\omega) = D^2(\omega, \omega')\,D(\omega')$ a zřejmě

$$D(\omega, \omega') = \begin{vmatrix} \frac{c_{11}}{d_1} & \frac{c_{12}}{d_1} & \ldots & \frac{c_{1n}}{d_1} \\ \ldots\ldots\ldots\ldots & & & \\ \frac{c_{n1}}{d_n} & \frac{c_{n2}}{d_n} & \ldots & \frac{c_{nn}}{d_n} \end{vmatrix} = \frac{\begin{vmatrix} c_{11} \ldots c_{1n} \\ \ldots\ldots\ldots \\ c_{n1} \ldots c_{nn} \end{vmatrix}}{d_1 \ldots d_n}$$

Je ovšem $(c_{ik}) \in J$. Označíme-li $(c_{ik}) = a$, je 1. dokázáno.

3. $\omega_i \in J_f \Rightarrow \omega_i^{(j)}$ je celé algebraické a $D(\omega)$ je celistvý polynom v $\omega_i^{(j)}$.
4. Je-li ω lineárně nezávislý, existuje $D(\omega', \omega)$ a je z pomocné věty $\Delta_f = D(\omega') = D^2(\omega', \omega).D(\omega)$, a poněvadž f je dle předpokladu bez vícenásobných kořenů, je $\Delta_f \neq 0$, tedy i $D(\omega)$.

Df 8

1. Buď $\langle \omega_1, \ldots, \omega_n \rangle = \langle \omega \rangle$ nějaká n-tice prvků $\in K_f$.

   Množinu všech prvků $z \in K_f$ tvaru

   $z = \sum_{i=1}^{n} \lambda_i \omega_i$, kde $\lambda_1, \ldots, \lambda_n$ jsou libovolná čísla $\in J$, označme $[\omega]$,

   n-tici $\langle \omega \rangle$ říkejme base $[\omega]$.
2. Buď $\langle \omega' \rangle$ druhá taková n-tice, pak definujme

   $\langle \omega' \rangle \sim \langle \omega \rangle$, je-li $[\omega] = [\omega']$, a říkáme, že $\langle \omega' \rangle$ je ekvivalentní $\langle \omega \rangle$.
3. $\langle \omega' \rangle > \langle \omega \rangle$, je-li $[\omega'] \supset [\omega]$ a říkáme, že $\langle \omega' \rangle$ je jemnější $\langle \omega \rangle$.

Poznámka.

Je zřejmě $[\omega]$ modul nad J s basí $\omega_1, \ldots, \omega_n$.

V 4,3

Platí

1. $\langle \omega \rangle \sim \langle \omega' \rangle \Rightarrow D(\omega) = D(\omega')$
2. $\langle \omega \rangle > \langle \omega' \rangle \Rightarrow D(\omega) / D(\omega')$, přičemž dělitelnost se rozumí ve smyslu dělitelnosti racionálních čísel.

Důkaz:

Dokážeme nejdříve 2. Je-li $\langle \omega \rangle > \langle \omega' \rangle$, tedy pro každé $1 \leqslant i \leqslant n$ $\omega_i' \in [\omega]$, tedy podle def. $\omega_i' = \sum_{j=1}^{n} c_{ij} \omega_j$ pro nějaká vhodná $c_{ij} \in J$.

Avšak V 4,1 dá

(1) $D(\omega') = D^2(\omega', \omega).D(\omega)$, a poněvadž $D(\omega', \omega) = (c_{ij}) \in J$, 2. platí. Dokážeme nyní 1. Je-li $\langle \omega' \rangle \sim \langle \omega \rangle$, je $\langle \omega \rangle > \langle \omega' \rangle$ i $\langle \omega' \rangle > \langle \omega \rangle$, jsou tedy $D(\omega)$ a $D(\omega')$ asociovány; protože však $D^2(\omega', \omega) > 0$, dává (1) rovnost.

Příklad.

Buď $f(x) = x^2 - 2$. Vyšetřujme K_f.

Označme $\sqrt{2}$ generátor K_f a označme

$$\langle \omega \rangle = \langle 2, \sqrt{2} \rangle$$
$$\langle \omega' \rangle = \langle 1, 2\sqrt{2} \rangle$$

Spočteme $D(\omega) = 32 = D(\omega')$, avšak snadno nahlédneme, že

$$1 \notin [\omega].$$

Tento příklad ukazuje, že implikace ve větě 4,3 nelze obecně obrátit.

Platí však

V 4,4

Buď $D(\omega) = D(\omega')$ a současně $\langle\omega\rangle > \langle\omega'\rangle$. Potom již

$$\langle\omega\rangle \sim \langle\omega'\rangle.$$

Nebo, což je totéž

Buď $\langle\omega\rangle \gtrdot \langle\omega'\rangle$, potom $D(\omega) \mid D(\omega')$ a $D(\omega) < D(\omega')$.

Důkaz:

Pišme $\omega_i' = \Sigma c_{ij}\omega_j$, $c_{ij} \in J$. Je podle předchozího $D^2(\omega', \omega) = 1$, neboli $D(\omega', \omega) = \pm 1$. Avšak v tomto případě má matice $\boldsymbol{D}(\omega', \omega)$ inversní v J a tedy, označíme-li

$$\boldsymbol{D}^{-1}(\omega', \omega) = (d_{ik}), \text{ je } d_{ik} \in J \text{ a}$$
$$\omega_k = \Sigma d_{ki}\omega_i, \text{ čili } \langle\omega\rangle < \langle\omega'\rangle.$$

Věta 4,3 ukazuje, že číslo $D(\omega)$ závisí vlastně na modulu $[\omega]$ a ne pouze na jeho basi $\langle\omega\rangle$. Skutečně, zavedeme-li si jinou basi, vytvářející týž modul, je $\langle\omega\rangle \sim \langle\omega'\rangle$ a tedy $D(\omega) = D(\omega')$. To nás přivádí k definici

Df 9

Buď R podmodul nad J, $R \supset K_f$ a buď $\langle\omega\rangle$ jeho base (pokud existuje). Položme $\boldsymbol{D}(R) = D(\omega)$ a nazvěme číslo $\boldsymbol{D}(R)$ diskriminantem R.
Věta 4,3 pak zní

V 4,3b

$$R \supset S \Rightarrow \boldsymbol{D}(R) \mid \boldsymbol{D}(S).$$

Existují ovšem v K_f podmoduly, které nemají basi a tedy ani diskriminant. Není těžké ukázat, že například K_f sám je takový modul. Poznamenejme, že kdybychom chtěli každému modulu přiřadit diskriminant, musely by okruhy bez basí mít $\boldsymbol{D}(R) = 0$.
Naším dalším úkolem bude ukázat, že J_f má basi.

§5. Base J_f.

Df 10

Buď $M \supset K$ nějaký modul nad J. Nechť existuje číslo $d \in J$ tak, že pro každé $z \in M$, $z = \frac{\varphi(\Theta)}{a}$, $\varphi(x)$ primitivní polynom $\in J[x]$, $a \in J$, platí normalisační podmínka

$$a \mid d.$$

Potom modul M nazýváme ohraničený modul nebo krátce o-modul a píšeme $M \subset\subset K_f$. Číslo d nazvěme hranicí M.

V 5,1

Nutná a postačující podmínka, aby modul měl basi, je, aby byl o-modulem.

Důkaz:

1. Postačitelnost.

a) Buď Δ hranice M. Pak každý prvek $z \in M$ lze psát jednoznačně

$$(1) \qquad z = \frac{b_1 + b_2\Theta + \ldots + b_n\Theta^{n-1}}{\Delta}, \; b_i \in J, \; 1 \leqslant i \leqslant n.$$

b) Pro každé $0 \leqslant i \leqslant n$ značme M_i modul všech prvků $z \in M$ takových, že jsou (racionální) lineární kombinací pouze $1, \Theta, \ldots, \Theta^{i-1}$, tedy platí-li (1), je

$$z \in M_i \Leftrightarrow b_{i+1} = b_{i+2} = \ldots = b_{n-1} = 0.$$

Dále je

$$\{0\} = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_{n-1} \subseteq M_n = M.$$

c) Označme ω_i ten prvek $\in M_i$ (resp. jeden z těch prvků), $(i \geqslant 1)$, který má u Θ^{i-1} nejmenší kladný koeficient. V případě, že $M_{i-1} = M_i$ a takový prvek neexistuje, položíme $\omega_i = 0$.

Je $\omega_1, \ldots, \omega_n$ basí M.

d) Lema.

Buď $z \in M_i$, potom existuje celé číslo $\lambda_i \in J$ tak, že

$$(2) \qquad z - \lambda_i\omega_i \in M_{i-1}.$$

Rozeznávejme dva případy:

$\alpha)$ $z \in M_{i-1}$. Pak položme $\lambda = 0$ a (2) platí.

$\beta)$ $z \notin M_{i-1}$. Pak ale $\omega_i \neq 0$ a v (1) je i $b_i \neq 0$.

Pišme

$$\omega_i = \frac{1}{\Delta}(e_{i-1,i-1} + e_{i-1,i-2}\,\Theta + \ldots + e_{i-1,0}\,\Theta^{i-1}).$$

A dále pišme

$$b_i = \lambda_i e_{i-1,0} + \mu, \; 0 \leqslant \mu < e_{i-1,0}.$$

Je $z - \lambda_i\omega_i \in M_i$. Jeho koeficient u Θ^{i-1} je $\frac{\mu}{\Delta}$ a je $0 \leqslant \frac{\mu}{\Delta} < \frac{e_{i-1,0}}{\Delta}$; tedy podle definice ω_i platí $\mu = 0$, neboli $z - \lambda_i\omega_i \in M_{i-1}$, což je tvrzení pomocné věty.

e) Můžeme nyní ovšem najít číslo λ_{i-1} tak, že $(z - \lambda_i\omega_i) - \lambda_{i-1}\omega_{i-1} \in M_{i-2}$ a tak dále, až $z - \lambda_i\omega_i - \lambda_{i-1}\omega_{i-1} - \ldots - \lambda_1\omega_1 \in M_0$, neboli $z = \lambda_1\omega_1 + \ldots + \lambda_i\omega_i$, kterážto relace ukazuje, že $\omega_1, \omega_2, \ldots, \omega_i$ je base M_i.

Stačí nyní položit $i = n$.

2. Nutnost.

Buď $\omega_1, \ldots, \omega_n$ base M. Buď $\omega_i = \frac{\varphi_{i-1}(\Theta)}{d_{i-1}}$ a buď Δ nejmenší společný násobek $d_0, d_1, \ldots, d_{n-1}$,
$\Delta = [d_0, \ldots, d_{n-1}]$. Zřejmě je Δ hranicí M.

Poznámka.

Je vidět, že vypustíme-li z n-tice $\omega_1, \ldots, \omega_n$ nulové členy a ponecháme ostatní $\omega_{i_1}, \ldots, \omega_{i_k}$, bude opět $M = [\omega_{i_1}, \ldots, \omega_{i_k}]$. Tedy modul M má hodnost n, právě když jsou všechna $\omega_i \neq 0$.

V 5,2

Buď $f(x) = 0$ polynom s jednoduchými kořeny. Potom modul $J_f \subset K_f$ je omezený.
Jeho hranicí je diskriminant Δ_f.

Důkaz:

Buď Θ generátor J_f a buď $\{\vartheta_1, \ldots, \vartheta_n\}$ přidružený vektor. Buď $z \in J_f$ a $\{z_1, \ldots, z_n\}$ přidružený vektor. Lze psát

$$(1) \qquad z = \frac{b_1 + b_2\Theta + \ldots + b_n\Theta^{n-1}}{b},$$

kde čísla $b_1, b_2, \ldots, b_n$ jsou nesoudělná s b. Podle V 3,1 je pak

$$(2) \qquad z_j = \frac{1}{b}(b_1 + b_2\vartheta_j + \ldots + b_n\vartheta_j^{n-1}) \text{ pro } j = 1, 2, \ldots, n.$$

Ze soustavy (2) můžeme čísla $\frac{b_i}{b}$ vypočítat.

Je (v tělese algebraických čísel):

$$(3) \qquad \frac{b_i}{b} = \frac{\sqrt{\Delta_f}}{\Delta_f} \begin{vmatrix} 1 & \vartheta_1 & \ldots & \vartheta_1^{i-2} & z_1 & \vartheta_1^{i} & \ldots & \vartheta_1^{n-1} \\ 1 & \vartheta_2 & \ldots & \vartheta_2^{i-2} & z_2 & \vartheta_2^{i} & \ldots & \vartheta_2^{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \vartheta_n & \ldots & \vartheta_n^{i-2} & z_n & \vartheta_n^{i} & \ldots & \vartheta_n^{n-1} \end{vmatrix}$$

neboť $$\sqrt{\Delta_f} = \frac{\Delta_f}{\sqrt{\Delta_f}} = \begin{vmatrix} 1 & \vartheta_1 & \ldots & \vartheta_1^{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \vartheta_n & \ldots & \vartheta_n^{n-1} \end{vmatrix}$$

je determinantem soustavy.

Z rovnice (3) však plyne, že $\frac{b_i}{b} \Delta_f$ je celé algebraické, tedy celé racionální číslo. Tj. $b / b_i \Delta_f$ pro každé i, neboli $b/\Delta_f (b_1, \ldots, b_n)$, avšak b je nesoudělné s $(b_1, \ldots, b_n)$, tedy b/Δ_f, což jsme chtěli dokázat.
Je tedy přímým důsledkem vět 5,1 a 5,2

V 5,3

J_f má basi.

V 5,4

Buď $f(x) = g(x).h(x)$, $(g, h) = 1$. Potom

$$\boldsymbol{D}(J_f) = \boldsymbol{D}(J_g).\boldsymbol{D}(J_h).$$

Důkaz:

Buď $\langle \omega \rangle$ base J_g, $\langle \varphi \rangle$ base J_h, a buďte n, m stupně postupně g, h. Označme

$$\psi_i = \iota_2 [\omega_i; 0] \qquad \text{pro } 1 \leqslant i \leqslant n,$$
$$\psi_i = \iota_2 [0; \varphi_{i-1}] \qquad \text{pro } n + 1 \leqslant i \leqslant n + m.$$

Potom je $\langle \psi \rangle$ base J_f.
Je podle V 2,2 ψ_i celé.
Je-li $z \in J_f$ a označíme-li $\iota_1 z = [z_1, z_2]$, jsou z_1, z_2 podle téže věty celé.

Tedy

$$z_1 = \sum_{i=1}^{n} \lambda_i \omega_i \qquad z_2 = \sum_{i=1}^{m} \lambda_{i+n} \varphi_i. \quad \text{Je však}$$

$$z = \iota_2[z_1, z_2] = \iota_2[\Sigma \lambda_i \omega_i; \Sigma \lambda_{i+n} \varphi_i] = \iota_2[\Sigma \lambda_i \omega_i; 0] + \iota_2 [0; \Sigma \lambda_{i+n} \varphi_i] =$$
$$= \iota_2 \Sigma \lambda_i [\omega_i; 0] + \iota_2 \Sigma \lambda_{i+n} [0; \varphi_i] = \Sigma \lambda_i \iota_2 [\omega_i, 0] + \Sigma \lambda_{i+n} \iota_2 [0, \varphi_i] =$$
$$= \sum_{1}^{n} \lambda_i \psi_i + \sum_{1}^{m} \lambda_{i+n} \psi_{i+n} = \sum_{1}^{n+m} \lambda_i \psi_i .$$

Podle věty 3,2, označíme-li přidružené vektory

$$\varkappa \omega_i = \{\omega_i^{(1)}, \ldots, \omega_i^{(n)}\},$$
$$\varkappa \varphi_i = \{\varphi_i^{(1)}, \ldots, \varphi_i^{(m)}\},$$

je

$$\varkappa \psi_i = \begin{cases} \{\omega_i^{(1)}, \ldots, \omega_i^{(n)}, 0, \ldots, 0\} & i \leqslant n \\ \{0, \ldots, 0, \varphi_{i-n}^{(1)}, \ldots, \varphi_{i-n}^{(m)}\} & i > n \end{cases} \quad \text{pro} \quad .$$

Spočtěme

$$\boldsymbol{D}(J_f) = D(\psi) = \begin{vmatrix} \omega_1^{(1)} \omega_1^{(2)} \dots \omega_1^{(n)} & 0 & 0 & \dots 0 \\ \omega_2^{(1)} \omega_2^{(2)} \dots \omega_2^{(n)} & 0 & 0 & \dots 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots & & & \\ \omega_n^{(1)} \omega_n^{(2)} \dots \omega_n^{(n)} & 0 & 0 & \dots 0 \\ 0 \quad 0 \quad \dots 0 & \varphi_1^{(1)} & \varphi_1^{(2)} & \dots \varphi_1^{(m)} \\ 0 \quad 0 \quad \dots 0 & \varphi_2^{(1)} & \varphi_{(2)}^{2} & \dots \varphi_2^{(m)} \\ \dots\dots\dots\dots\dots\dots\dots\dots & & & \\ 0 \quad 0 \quad \dots 0 & \varphi_m^{(1)} & \varphi_m^{(2)} & \dots \varphi_m^{(m)} \end{vmatrix} =$$

$$= \begin{vmatrix} \omega_1^{(1)} \dots \omega_1^{(n)} \\ \dots\dots\dots \\ \omega_n^{(1)} \dots \omega_n^{(n)} \end{vmatrix} \cdot \begin{vmatrix} \varphi_1^{(1)} \dots \varphi_1^{(m)} \\ \dots\dots\dots \\ \varphi_m^{(1)} \dots \varphi_m^{(m)} \end{vmatrix} = D(\omega).D(\varphi) = \boldsymbol{D}(J_g).\boldsymbol{D}(J_h).$$

Protože okruh J_f je nejdůležitější ze všech podmodulů K_f, uvedu speciální důsledek věty 4,4 jako větu.

V 5,5

Buď $\langle\omega\rangle$ base $M \subset\subset K_f$ a buďte ω_i celé prvky. Je-li $\boldsymbol{D}(M) = \boldsymbol{D}(J_f)$, je již $\langle\omega\rangle$ basí J_f.

§6. Θ-base.

Base, kterou jsme sestrojili podle věty 5,1 pro J_f, bude mít některé zajímavé vlastnosti, které jsou pro další důležité. Zachováme-li značení V 5,1, totiž

$\langle\omega\rangle = \langle\omega_1, \dots, \omega_n\rangle$ base J_f,

$\omega_i = \frac{1}{\Delta_f}(e_{i-1,i-1} + e_{i-1,i-2}\Theta + \dots e_{i-1,0}\Theta^{i-1})$, pak platí, jak za chvíli dokážeme

(1_1) $e_{i,0}/e_{i,k}$ pro $0 \leqslant i \leqslant n-1$, $0 \leqslant k \leqslant i$,

(1_2) $e_{i,0}/\Delta_f$ pro $0 \leqslant i \leqslant n-1$. Lze tedy po vhodném krácení psát

$$\omega_1 = 1$$

$$\omega_2 = \frac{\Theta + c_{11}}{d_1}$$

$$\omega_3 = \frac{\Theta^2 + c_{21}\Theta + c_{22}}{d_2}$$

. . . . .

$$\omega_n = \frac{\Theta^{n-1} + c_{n-1,1}\Theta^{n-2} + \ldots + c_{n-1,n-1}}{d_{n-1}}.$$

Basi tohoto tvaru budeme říkat Θ-base. Tedy definujme.

Df 10

Buď $M \subset\subset K_f$ a buď $\langle\omega\rangle$ base M. Buď $\omega_i = \frac{\varphi_{i-1}(\Theta)}{d_{i-1}}$, $\varphi_{i-1}(x)$ primitivní polynom. Je-li navíc

1. $\varphi_i(x) \in J'[x]$,
2. stupeň $\varphi_i(x)$ je i,

pak $\langle\omega\rangle$ nazýváme Θ-basí, a modul M Θ-modulem. Přesněji, neboť M má různé base, $M \subset\subset K_f$ je Θ-modul, existuje-li v M base, která je Θ-basí.

1. Již z definice je jasné, že je-li M Θ-modul, pak pro $0 \leqslant i \leqslant n-1$ je

   (1) $\qquad \Theta^i \in M$, tedy $[1, \Theta, \ldots, \Theta^{n-1}] \subseteq M$.

2. Také je jasné, že Θ-moduly mají hodnost n, tedy jejich base je lineárně nezávislá a moduly M_i z věty 5,1 jsou proto všechny různé.

Podmínka (1) [a z ní vyplývající podmínka (2)] však není postačující pro to, aby M měl Θ-basi.
Tak například není těžké ukázat, že je-li Θ generátor J_f, kde f je libovolný polynom druhého stupně s $\Delta_f \neq 0$ a zvolíme-li

$$M = \left[\frac{1}{2}; \frac{2\Theta + 1}{4}\right], \text{ pak } M \text{ nemá } \Theta\text{-basi, ač obsahuje 1 i } \Theta.$$

Platí však

V 6,1

Nechť $[1, \Theta, \ldots, \Theta^{n-1}] \subset M \subset\subset K_f$ a nechť M je okruh. Pak M má Θ-basi (M můžeme nazývat Θ-okruhem).

Důkaz:

Ukážeme, že base sestrojená ve větě 5,1 je v našem případě Θ-basí.

1. Jak jsme již poznamenali nahoře, je $M_{i-1} \subset M_i$, a tedy $\omega_i \neq 0$. Lema d) ve větě 5,1 neříká v tomto případě nic jiného než to, že značíme-li

   (1) $z \in M_i$, $z = \frac{1}{\Delta}(b_1 + \ldots + b_i\Theta^{i-1})$, $\omega_i = \frac{1}{\Delta}(e_{i-1,i-1} + \ldots + e_{i-1,0}\Theta^{i-1})$,

   potom $b_i = \lambda_i e_{i-1,0}$; tedy že Δ . nejvyšší koeficient u libovolného prvku $z \in M_i$ je dělitelný $e_{i-1,0}$.

2. Je $\Theta \in M$, $\omega_{i-1} \in M$, M okruh $\Rightarrow \omega_{i-1}\Theta \in M$. Tento prvek je stupně i v Θ, a proto $\omega_{i-1}\Theta \in M_{i+1}$. Koeficient u Θ^i je $\frac{e_{i-2,0}}{\Delta}$, tedy

   (2) $\qquad e_{i-1,0} \,/\, e_{i-2,0}$.

3. Je $\Theta^i \in M_{i+1}$, tedy existují čísla

$$\lambda_{i,1}; \lambda_{i,2}; \ldots, \lambda_{i,i}; d_i, \text{ že } \Theta^k = \lambda_{i,1}\omega_1 + \ldots + \lambda_{i,i}\omega_i + d_i\omega_{i+1}.$$

Porovnáním koeficientů u Θ^i je

$$1 = \frac{d_i e_{i,0}}{\Delta}, \text{ tedy}$$

$$d_i e_{i,0} = \Delta, \text{ což je } (1_2). \tag{3}$$

4. Indukcí podle i dokážeme

$$e_{i,0} / e_{i,k} \text{ pro } 0 \leqslant i \leqslant n - 1,\ 0 \leqslant k \leqslant i. \tag{4}$$

Buď $i = 0$. (4) se redukuje na $e_{0,0}/e_{0,k}$, což je triviální. Nechť (4) platí pro $i = 0, 1, \ldots, e$.

(5) Označme $$\frac{\Delta}{e_{i,0}} = d_i; \quad \frac{e_{i,k}}{e_{i,0}} = c_{i,k}$$

pro $0 \leqslant i \leqslant e$, $0 \leqslant k \leqslant i$. Z (3) a z indukčního předpokladu plyne, že čísla $d_k, c_{i,k} \in J$. (2) dává $\dfrac{\Delta}{d_{i-1}} \Big| \dfrac{\Delta}{d_{i-2}}$.

neboli d_{i-2} / d_{i-1}. Je tedy

$$d_0 / d_1 / \ldots / d_e. \tag{6}$$

Dosaďme (5) do vzorce pro ω_i z (1):

$$\begin{aligned} \omega_1 &= \frac{1}{d_0} \\ \omega_2 &= \frac{\Theta + c_{11}}{d_1} \\ &\cdots\cdots \\ \omega_e &= \frac{\Theta^{e-1} + c_{e-1,1}\Theta^{e-2} + \ldots + c_{e-1,e-1}}{d_{e-1}} \end{aligned} \tag{7}$$

Z tohoto vyjádření speciálně plyne, že, je-li

$$\omega = \frac{c_1\Theta^{e-1} + \ldots + c_e}{c} \in M_e,$$

je vzhledem k (6) $\omega . d_{e-1}$ polynom s celistvými koeficienty v Θ, to jest

$$\frac{d_{e-1} . c_k}{c} \in J \text{ pro } 1 \leqslant k \leqslant l. \tag{8}$$

Označme

$$\omega = \frac{e_{e-1,0}}{e_{e,0}}\omega_{e+1} - \Theta\omega_e =$$

$$= \frac{\left(\frac{e_{e-1,0}}{e_{e,0}} e_{e,0} - \frac{\Delta}{d_{e-1}}\right)\Theta^e + \ldots + \left(\frac{e_{e-1,0}}{e_{e,0}} e_{e,k} - \frac{\Delta_f}{d_{e-1}} c_{e-1,k}\right)\Theta^{e-k} + \ldots}{\Delta}.$$

Je $$\frac{e_{e-1,0}}{e_{0,0}} e_{e,0} - \frac{\Delta}{d_{e-1}} = e_{e-1,0} - \frac{\Delta}{d_{e-1}} = 0,$$

tedy $\omega \in M_e$, a proto podle (8)

$$\lambda_k = \frac{\frac{e_{e-1,0}}{e_{e,0}} e_{e,k} - \frac{\Delta}{d_{e-1,k}} c_{e-1,k}}{\Delta} \cdot d_{e-1} \in J.$$

Upravme jej

$$\lambda_k = e_{e,k} \frac{e_{e-1,0}}{e_{e,0}} \frac{d_{e-1}}{\Delta} - c_{e-1,k}$$

Využijeme vztahu $\frac{1}{e_{e-1,0}} = \frac{d_{e-1}}{\Delta}$ a dostaneme $\lambda_k + c_{e-1,k} = \frac{e_{e,k}}{e_{e,0}} \in J$.
Tím jsme dokázali (4).

Tedy rovnice (5), (7) platí pro $0 \leqslant i \leqslant n - 1$, což je odvození věty.

Poznamenejme, že předpoklad, že M je okruh, lze nahradit zřejmě předpokladem, že $\omega_k \Theta \in M$ pro každé k.
Ani v tomto případě nestane se tato podmínka nutnou pro to, aby M byl Θ-modul.

V 6,2

J_f má Θ-basi.

V 6,3

Buď M Θ-modul a $\langle\omega\rangle$ jeho Θ-base. Buď $\omega_i = \frac{\varphi_{i-1}(\Theta)}{d_{i-1}}$, potom je

$$\boldsymbol{D}(M) = \frac{\Delta_f}{d_1^2 d_2^2 \ldots d_{n-1}^2}.$$

Důkaz plyne z věty 4,2, neboť označíme-li $\langle\omega'\rangle = \langle 1, \Theta, \ldots, \Theta^{n-1}\rangle$, je

$$D(\omega, \omega') = \begin{vmatrix} 1 & 0 & \ldots & 0 \\ \frac{c_{11}}{d_1} & \frac{1}{d_1} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ \frac{c_{n-1,n-1}}{d_{n-1}} & \frac{c_{n-1,n-2}}{d_{n-1}} & \ldots & \frac{1}{d_{n-1}} \end{vmatrix} = \frac{1}{d_1} \cdot \frac{1}{d_2} \ldots \frac{1}{d_{n-1}}.$$

Již tato věta ukazuje výhody Θ-base oproti obecným basím, neboť je vidět, že jmenovatelé prvků Θ-base jsou nejmenší možní; v basi mohou být větší.

V 6,4

Buď M Θ-modul a $\langle\omega\rangle$ jeho Θ-base. Buď $\omega_i = \frac{\varphi_{i-1}(\Theta)}{d_{i-1}}$.
Buď $\psi(x) \in J'[x]$ polynom stupně $i - 1$ a nechť

$$\omega' = \frac{\psi(\Theta)}{d_{i-1}} \in M;$$

potom je již $\langle\omega_1, \ldots, \omega_{i-1}, \omega_i', \omega_{i+1}, \ldots, \omega_n\rangle$ Θ-base, neboť má stejný diskriminant jako má $\langle\omega\rangle$ (viz V 4,4).
Tedy opět věta, která neplatí pro obecné base. Ukazuje, že lze zaměnit prvek base libovolným jiným, jen když patří do modulu a je dělitelný stejným číslem. Přesto je Θ-base, jak za chvíli ukážeme, v jistém smyslu někdy jediná.

V 6,5

Buď M Θ-modul, $\langle \ldots \omega_i = \frac{\varphi_{i-1}(\Theta)}{d_{i-1}} \ldots\rangle$ jeho Θ-base a $\langle\omega'\rangle =$
$= \langle \ldots \frac{\varphi'_{i-1}(\Theta)}{d'_{i-1}} \ldots\rangle$ jiná Θ-base.
Pak platí $d_i = d_i'$ pro $i = 0, 1, \ldots, n - 1$.

Skutečně je

$$\omega_i' \in [\omega],$$

tedy $\omega_i' = \lambda_1\omega_1 + \ldots + \lambda_i\omega_i$; srovnání koeficientů u Θ^{i-1} dá

$$\frac{1}{d'_{i-1}} = \frac{\lambda_i}{d_{i-1}},$$

tedy d'_{i-1}/d_{i-1} a stejně naopak (je $d_i > 0$, $d_i' > 0$).
Předcházející věta ukazuje, že jmenovatelé d_i nezávisejí na volbě Θ-base, ale pouze na modulu M.

Značme proto

$$d_i(M) = d_i,$$

kde d_i mají význam jako v předcházející větě. Speciálně položme ještě

$$d_i(J_f) = d_i(f).$$

Věta pomocná

Buď R Θ-okruh. Pak platí

$$d_i(R) \mid d_{i+1}(R).$$

Důkaz plyne ze skutečnosti, že $\omega_i.\omega_2 \in R$ a lze tento člen vyjádřit jako lineární kombinaci $\omega_1, \omega_2, \ldots, \omega_{i+1}$. Porovnáním koeficientů dostaneme dokonce $d_{i-1}d_1/d_i$.

V 6,6. O jednoznačnosti.

Buď R Θ-okruh a buďte $\langle\omega\rangle$, $\langle\omega'\rangle$ dvě jeho Θ-base. Označme

$$\omega_i = \frac{\varphi_{i-1}(\Theta)}{d_{i-1}}, \quad \omega_i' = \frac{\varphi_{i-1}'(\Theta)}{d_{i-1}}.$$

Pak platí

$$\varphi_i(x) \equiv \varphi_i'(x) \left(\mathrm{mod}\ \frac{d_i}{d_{i-1}}\right).$$

Důkaz:

Existují čísla $\lambda_1, \ldots, \lambda_{i-1} \in J$, že

$$(1) \qquad \frac{\varphi_i(\Theta) - \varphi_i'(\Theta)}{d_i} = \sum_{j=0}^{i-1} \lambda_j \frac{\varphi_j'(\Theta)}{d_j}.$$

Stupně všech polynomů v rovnici (1) jsou menší než n, a proto můžeme od rovnosti v Θ přejít k rovnosti v x. Vynásobíme-li pak rovnici d_{i-1}, dostaneme $(\varphi_i(x) - \varphi_i'(x)) \cdot \frac{d_{i-1}}{d_i}$ je celistvý polynom. Odtud věta.

V 6,7

Buď $f(x) = g(x).h(x)$. Buď $\boldsymbol{R}(g, h)$ resolventa polynomů $h(x)$, $g(x)$. Je pak

$$d_1(g)d_2(g) \ldots d_{n-1}(g).|\boldsymbol{R}(g, h)|.d_1(h).d_2(h) \ldots d_{m-1}(h) = \\ = d_1(f)d_2(f) \ldots d_{n+m+1}(f).$$

Důkaz:

Vždy předpokládáme $f(x)$ s jednoduchými kořeny, tedy g, h jsou nesoudělná.

Věty 5,4 a 6,3 dávají

$$\frac{\Delta_f}{\ldots d_i^2(f) \ldots} = \boldsymbol{D}(J_f) = \boldsymbol{D}(J_h).\boldsymbol{D}(J_g) = \frac{\Delta_h}{\ldots d_i^2(h) \ldots} \cdot \frac{\Delta_g}{\ldots d_i^2(g) \ldots}.$$

Je však

$$\Delta_f = \Delta_g \boldsymbol{R}^2(g, h) \Delta_h,$$

jak se zjistí porovnáním kořenových vyjádření Δ, $\boldsymbol{R}$.

§7. Base vzhledem k prvočíslu.

Buďte $\langle\omega'\rangle$, $\langle\omega''\rangle$ dvě Θ-base postupně modulů K', $K'' \subset\subset K_f$.

Buď

$$(1) \qquad \omega_i' = \frac{\varphi_i'(\Theta)}{d_i'}$$
$$\omega_i'' = \frac{\varphi_i''(\Theta)}{d_i''}$$

Df 11

Je-li pro každé $1 \leqslant i \leqslant n$ $(d_i', d_i'') = 1$, říkáme, že obě base (lze říkat i oba moduly $[\omega]$, $[\omega']$) jsou nesoudělné.

V 7,1

Buďte K', K'' dva nesoudělné moduly. Buď K nejmenší modul, který oba obsahuje. Potom K má Θ-basi. Modulu K se říká nejmenší společné zjemnění K', K''.

Důkaz:

Podle definice nesoudělných modulů mají K', K'' Θ-basi; označme ji $\langle\omega'\rangle$, $\langle\omega''\rangle$ a nechť platí (1).
Označme e_i', e_i'' ta čísla, pro něž platí $e_i'd_i'' + e_i''d_i' = 1$; je e_i', $e_i'' \in J$ pro každé $1 \leqslant i \leqslant n$. Označme $e_i'\omega_i' + e_i''\omega_i'' = \omega_i$. Je $\omega_i \in K_f$. Spočteme

$$\omega_i = \frac{e_i'd_i''\varphi_i'(\Theta) + e_i''d_i'\varphi_i''(\Theta)}{d_i'd_i''}.$$

Píšeme-li $e_i'd_i''\varphi_i'(x) + e_i''d_i'\varphi_i''(x) = \varphi_i(x)$ a $d_i'd_i'' = d_i$, je

1. $\omega_i = \dfrac{\varphi_i(\Theta)}{d_i}$
2. $\varphi_i(x) \in J'[x]$
3. stupeň $\varphi_i(x) = i - 1$.

(2) Je tedy $\langle\omega\rangle$ Θ-basí nějakého modulu $\subset K$. Je však

$$e_i''(\varphi_i'(\Theta) - \varphi_i''(\Theta)) + d_i''\omega_i = \frac{e_i''d_i'\varphi_i' - e_i''d_i'\varphi_i'' + e_i'd_i''\varphi_i' + e_i''d_i'\varphi_i''}{d_i'} =$$

$$= (e_i''d_i' + e_i'd_i'')\frac{\varphi_i'(\Theta)}{d_i'} = \omega_i'$$

a podobně $e_i'(\varphi_i''(\Theta) - \varphi_i'(\Theta)) + d_i'\omega_i = \omega_i''$.
Poněvadž $\varphi_i'(\Theta) - \varphi_i''(\Theta)$ je celistvý polynom v Θ, leží zřejmě v K, K'', neboť oba moduly mají Θ-basi, a tedy $\omega_i' \in K$, $\omega_i'' \in K$; vzhledem k (2) je pak $[\omega] = K$.
Konstrukce ve větě 7,1 je poměrně jednoduchá a umožňuje tedy snadno sestrojit basi J_f. Jsou-li totiž $K_1, K_2, \ldots, K_n$ po dvou nesoudělné moduly, takové, že dohromady vytvářejí již celé J_f, máme ve větě numericky mnohem snazší prostředek ke konstrukci Θ-base J_f, než ve větě 6,1.
Celkem nejjednodušší nesoudělné moduly K_i jsou ty, jejichž base mají za jmenovatele prvočísla p_i, a to samozřejmě pokud možno v nejvyšší mocnině.
Je proto přirozené definovat

Df 12

Množinu všech čísel $z \in J_f$ tvaru

(1) $$z = \frac{b_1\Theta^{n-1} + b_2\Theta^{n-2} + \ldots + b_n}{p^q},$$

kde Θ je generátor J_f, p prvočíslo a q, b_1, b_2, ..., b_n jsou libovolná čísla celá, nazvěme $J_f^{(p)}$.

Je zřejmě $J_f^{(p)}$ okruh pro každé prvočíslo p. Poznamenejme, že přirozené zobecnění df 12 by bylo $J_f^{(p_1,p_2,\ldots,p_r)}$, kde bychom uvažovali čísla tvaru (1), ale jmenovatel by byl tvaru $p_1^{q_1}p_2^{q_2}\ldots p_r^{q_r}$ pro celá nezáporná $q_1, q_2 \ldots, q_r$.

V 7,2

$J_f^{(p)}$ má Θ-basi.

Důkaz plyne sice ihned z věty 6,1, ale uvedu jiný, neboť potřebuji pro větu 7,3 i metodu, jak basi vytvořit.

Buď $\omega_i' = \frac{\varphi_i(\Theta)}{d_{i-1}}$, buď $d_i = d_i' p^{q_i}$ a $p \nmid d_i'$. Je $\omega_i = \frac{\varphi_i(\Theta)}{p^{q_{i-1}}}$ base $J_f^{(p)}$.

Skutečně je ovšem $\varphi_i(x) \in J'[x]$ a stupeň $\varphi_i(x) = i - 1$. Dále je $\omega_i \in J_f^{(p)}$. Stačí tedy ukázat, že $[\omega] \subset J_f^{(p)}$.

Buď $z \in J_f^{(p)}$, $z = \frac{\varphi(\Theta)}{p^q}$. Je $z \in J_f$, tedy $z = \Sigma \lambda_i \omega_i'$. Je zp^q celistvý polynom v Θ, proto lze psát

$$z.p^q = \Sigma \mu_i \varphi_i(\Theta)$$

a z lineární nezávislosti $\varphi_i(\Theta)$ plyne

$$\frac{p^q \lambda_i}{d_{i-1}} = \mu_i, \text{ čili } d_{i-1}' p^{q_{i-1}}/\lambda_i p^q.$$

A protože $d_i' \neq 0$ (p), je i d_{i-1}'/λ_i a označíme-li $\frac{\lambda_i}{d_{i-1}'} = \nu_i \in J$, je

$$z = \sum \lambda_i \omega_i' = \sum \lambda_i \frac{\varphi_i(\Theta)}{d_{i-1}} = \sum \frac{\lambda_i}{d_{i-1}'} \frac{\varphi_i(\Theta)}{p^{q_{i-1}}} = \sum \nu_i \omega_i.$$

Poznámka:

Basi $J_f^{(p)}$ se v literatuře často říká base J_f vzhledem k p.

V 7,3

$$\boldsymbol{D}(J_f^{(p)}) = \frac{\Delta_f}{p^{Exp_p \frac{\Delta_f}{\boldsymbol{D}(J_f)}}}.$$

Důkaz:

Je-li $\boldsymbol{D}(J_f) = \frac{\Delta_f}{d.p^q}$, kde $p \nmid d$, je podle V 7,2

$$\frac{\Delta_f}{p^q} = \boldsymbol{D}(J_f^{(p)}).$$

V 7,4

Buďte p_i prvočísla dělící diskriminant f, Δ_f ($i = 1, 2, \ldots, r$). Potom moduly $J_f^{(p_1)}, J_f^{(p_2)}, \ldots, J_f^{(p_r)}$ vytvářejí J_f, čili postupnou aplikací věty 7,1 dostaneme basi J_f.

Důkaz:

Jsou-li K', K'' dva nesoudělné moduly a K jejich nejmenší společné zjemnění, pak zřejmě

$$\boldsymbol{D}(K').\boldsymbol{D}(K'') = \boldsymbol{D}(K)\Delta_f.$$

Je-li tedy $J_f^{(p_1,p_2,\ldots,p_k)} (k \leqslant r)$ zjemnění $J_f^{(p_1)}, \ldots, J_f^{(p_k)}$, je

$$\boldsymbol{D}_f(J_f^{(p_1,\ldots,p_k)}) = \frac{\Delta_f}{p_1^{i_1}p_2^{i_2}\ldots p_k^{i_k}},$$

přičemž každé prvočíslo se podle V 7,3 ve jmenovateli vyskytuje právě v té mocnině, v jaké se vyskytuje ve jmenovateli d, neboť $\boldsymbol{D}_f(J_f) = \frac{\Delta_f}{d}$.

Je ovšem d/Δ_f a odtud věta.

Poznamenejme, že nemusíme brát, jak uvidíme dále, všechna prvočísla dělící Δ_f. Například hned důkaz věty 6,7 ukazuje, že stačí brát ta prvočísla, jejichž čtverce dělí Δ_f. Větu 7,4 jsem jen proto uvedl v tomto paragrafu, abych ukázal význam „base vzhledem k p".

Dále si uvědomme, že $J_f^{(p)}$ opět charakterisuje jednoznačně $\boldsymbol{D}(J_f^{(p)})$ ve smyslu věty 4,4. Čísla $p^{q_1}, p^{q_2}, \ldots, p^{q_{n-1}}$ jsou opět jednoznačně určena $J_f^{(p)}$.

Definujme tedy opět

$$d_i^{(p)}(J_f) = d_i^{(p)}(f) = d_i(J_f^{(p)}) = p^{q_i}.$$

V 7,5

Buď $f(x) = g(x)h(x)$ a buďte $h(x)$, $g(x)$ nesoudělné modulo p. Pak je

$$d_1^{(p)}(f) \ldots d_{m+n-1}^{(p)}(f) = d_1^{(p)}(g) \ldots d_{n-1}^{(p)}(g)d_1^{(p)}(h) \ldots d_{m-1}^{(p)}(h).$$

Důkaz plyne z vět 6,7 a 7,3, uvědomíme-li si, že $p \nmid \boldsymbol{R}(g, h)$.

Důsledkem této věty je

V 7,6

Buďte $h(x)$, $g(x)$ nesoudělné mod p a $f(x) = g(x).h(x)$, potom

$$\boldsymbol{D}(J_f) = \frac{\Delta_f}{\left(d_1^{(p)}(g) \ldots d_{n-1}^{(p)}(g)d_1^{(p)}(h) \ldots d_{m-1}^{(p)}(h)\right)^2}.$$

Poznamenejme, že jsme ve větě 7,2 dokázali víc, než jsme vyslovili. Dokázali jsme nejen, že $J_f^{(p)}$ má basi, ale dokonce, že tuto basi získáme z Θ-base J_f tím, že ve jmenovatelích potlačíme všechna prvočísla kromě p. Této skutečnosti později využijeme.

§8. *Pomocné věty.*

Buďte $x_1, \ldots, x_n$ neurčité. Označme $\sum_{k=0}^{n} x_i^k = s_k$ a

$$\overset{k}{S}_{j} = \overset{k}{S}_{j_1 \ldots j_k}^{i_1 \ldots i_k} = \begin{vmatrix} s_{i_1+j_1} & s_{i_1+j_2} & \ldots & s_{i_1+j_k} \\ s_{i_2+j_1} & s_{i_2+j_2} & \ldots & s_{i_2+j_k} \\ \ldots\ldots\ldots\ldots\ldots & & & \\ s_{i_k+j_1} & s_{i_k+j_2} & \ldots & s_{i_k+j_k} \end{vmatrix}$$

pro $1 \leqslant k \leqslant n$, $0 \leqslant i_r \leqslant n-1$, $0 \leqslant j_r \leqslant n-1$.

Konečně

$$\Delta(x_1, \ldots, x_n) = (x_2 - x_1)(x_3 - x_1) \ldots (x_n - x_1).$$
$$(x_3 - x_2) \ldots (x_n - x_2).$$
$$\ldots\ldots\ldots$$
$$(x_n - x_{n-1}).$$

V 8,1

Existují polynomy s celistvými koeficienty $F_{i,j}(x_1, \ldots, x_k)$, tak, že platí

$$\overset{k}{S}_{j_1 \ldots j_k}^{i_1 \ldots i_k} = \sum \Delta^2(x_{e_1} \ldots x_{e_k})\, F_{i,j}(x_{e_1} \ldots x_{e_k}),$$

kde součet se bere přes všechny kombinace k-té třídy z 1, 2, ..., n.

Důkaz:

Platí následující věta (viz DICKSON: Modern algebraic theories, Chicago 1926, str. 49):

Buďte A, B dvě matice typu $n \times n$ nad J, nějakým tělesem. Buď $M_{e_1 \ldots e_m}^{k_1 \ldots k_m}$ m-řádkový minor součinu obou matic $A.B$. Pak platí

$$\operatorname{Det}\left(M_{e_1 \ldots e_m}^{k_1 \ldots k_m}\right) = \sum \operatorname{Det}\left(A_{i_1 \ldots i_m}^{k_1 \ldots k_m}\right) \operatorname{Det}\left(B_{e_1 \ldots e_m}^{i_1 \ldots i_m}\right),$$

kde součet je přes všech $\binom{n}{m}$ výběrů $i_1, \ldots, i_m$ z 1, 2, ..., n bez změny pořadí.

Použijme této věty. Je

$$\overset{0}{S}_{0\,1 \ldots n-1}^{0\,1 \ldots n-1} = \begin{vmatrix} s_0 & s_1 \ldots s_{n-1} \\ s_1 & s_2 \ldots s_n \\ \ldots\ldots\ldots\ldots & \\ s_{n-1} & s_n, \ldots s_{2n-2} \end{vmatrix} = \begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ & & & \\ & & & \\ 1 & x_n & \ldots & x_n^{n-1} \end{vmatrix}^2.$$

Je též S_j^k zřejmě minor determinantu S v obvyklém značení. Označme ještě na chvíli

$$\Delta(x_1, x_2, \ldots x_k; i_1, \ldots, i_k) = \begin{vmatrix} x_1^{i_1} x_1^{i_2} \ldots x_1^{i_k} \\ x_k^{i_1} x_k^{i_2} \ldots x_k^{i_k} \end{vmatrix}. \quad \text{Je tedy}$$

$$(1) \qquad S^k_{\substack{i_1 \ldots i_k \\ j_1 \ldots j_k}} = \sum \Delta(x_{e_1}, x_{e_2}, \ldots, x_{e_k}; i_1 \ldots, i_k)\, \Delta(x_{e_1}, \ldots, x_{e_k}; j_1, \ldots, j_k)$$

Je však (viz KOŘÍNEK: Základy algebry, Praha 1953, str. 282)

$\Delta(x_{e_1}, \ldots, x_{e_k})/\Delta(x_{e_1}, \ldots, x_{e_k}; i_1, \ldots, i_k)$ pro každé $0 \leqslant i_r \leqslant n-1$.

Je tedy v (1) možno z každého členu vytknout $\Delta^2(x_{e_1}, \ldots, x_{e_k})$.

V 8,2

Buď $\alpha \in J_f$, potom, píšeme-li

$$(2) \qquad f'(\Theta)\alpha = \sum_{i=0}^{n-1} b_i \Theta^i, \text{ jsou čísla } b_i \in J, \ (f'(x) \text{ je derivace } f(x)).$$

Důkaz:

Vzorec (2) rozhodně platí pro čísla $b_i \in K$. Buďte $\{\alpha_1, \ldots, \alpha_n\}, \{\vartheta_1, \ldots, \vartheta_n\}$ přidružené vektory k α, Θ. Pak podle V 4,1 platí

$$(3) \qquad f'(\vartheta_j)\alpha_j = \sum_{i=0}^{n-1} b_i \vartheta_j^i.$$

To je soustava rovnic pro b_i.
Cramerovo pravidlo dá

$$b_i = \frac{\begin{vmatrix} & \cdots & \\ 1\ \vartheta_j \ \ldots\ \vartheta_j^{i-1} f'(\vartheta_j)\alpha_j\ \vartheta_j^{i+1} \ldots\ \vartheta_j^{n-1} \\ & \cdots & \end{vmatrix}}{\begin{vmatrix} & \cdots & \\ 1\ \vartheta_j \ \ldots\ \vartheta_j^{i} \ldots\ \vartheta_j^{n-1} \\ & \cdots & \end{vmatrix}} =$$

$$(4) \qquad = \sum \pm \alpha_j f'(\vartheta_j) \cdot \frac{\begin{vmatrix} 1\ \vartheta_1 & \ldots\ \vartheta_1^{i-1}\ \vartheta_1^{i+1} \ldots\ \vartheta_1^{n-1} \\ & \cdots & \\ 1\ \vartheta_{j-1} & \ldots\ \vartheta_{j-1}^{i-1}\ \vartheta_{j-1}^{i+1} \ldots\ \vartheta_{j-1}^{n-1} \\ 1\ \vartheta_{j+1} & \ldots\ \vartheta_{j+1}^{i-1}\ \vartheta_{j+1}^{i+1} \ldots\ \vartheta_{j+1}^{n-1} \\ & \cdots & \\ 1\ \vartheta_n & \ldots\ \vartheta_n^{i-1}\ \vartheta_n^{i+1} \ldots\ \vartheta_n^{n-1} \end{vmatrix}}{\Delta(\vartheta_1, \ldots, \vartheta_n)} =$$

$$= \sum_{j=1}^{n} \pm \alpha_j F(\vartheta_1, \vartheta_2, \ldots, \vartheta_{j-1}, \vartheta_{j+1}, \ldots, \vartheta_n),$$

kde shodně s předcházející větou je $F(x_1, \ldots, x_{n-1})$ nějaká celá funkce. Z rovnice (4) je ovšem vidět, že b_i je celé algebraické číslo, a poněvadž je racionální, tedy je celé racionální.

V 8,3

Platí

$$\begin{vmatrix} 1 & x_1 & \ldots & x_1^{i-1} & x_1^{i+1} & \ldots & x_1^n \\ & & \ldots & & & & \\ 1 & x_n & \ldots & x_n^{i-1} & x_n^{i+1} & \ldots & x_n^n \end{vmatrix} = \sum x_1 \ldots x_{n-k} \begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ & & \ldots & \\ 1 & x_n & \ldots & x_n^{n-1} \end{vmatrix}.$$

Důkaz:

Je

$$\begin{vmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^{i-1} & x_0^i & x_0^{i+1} & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^{i-1} & x_1^i & x_1^{i+1} & \ldots & x_1^n \\ & & & \ldots & & & & & \\ 1 & x_n & x_n^2 & \ldots & x_n^{i-1} & x_n^i & x_n^{i+1} & & x_n^n \end{vmatrix} =$$

$$= \sum_{k=0}^{n} (-1)^k x_0^k \begin{vmatrix} 1 & x_1 & \ldots & x_1^{k-1} & x_1^{k+1} & \ldots & x_1^n \\ & & \ldots & & & & \\ 1 & x_n & \ldots & x_n^{k-1} & x_n^{k+1} & \ldots & x_n^n \end{vmatrix} = (x_1 - x_0)(x_2 - x_0) \ldots (x_n - x_0)$$
$$(x_2 - x_1) \ldots (x_n - x_1)$$
$$\ldots \ldots$$
$$(x_n - x_{n-1}) =$$

$$= (x_0 - x_1)(x_0 - x_2) \ldots (x_0 - x_n) \Delta(x_1, \ldots, x_n) . (-1)^n =$$

$$= (-1)^n \sum_{k=0}^{n} x_0^k \sum x_1 \ldots x_{n-k} (-1)^{n-k} . \Delta(x_1, \ldots, x_n) =$$

$$= \Delta(x_1, \ldots, x_n) \sum (-1)^k x^k \sum x_1 \ldots x_{n-k},$$

kde $\Sigma x_1 \ldots x_{n-k}$ je elementární symetrická funkce $n - k$-tého stupně neurčitých $x_1, \ldots, x_n$. Porovnáním koeficientů u stejných mocnin x_0 máme větu.

Dále budeme potřebovat jeden triviální důsledek tvrzení o částečném dělení.

Máme-li dva polynomy $h(x), k(x) \in J'[x]$ stupňů $r \geqslant s$, pak, jak známo, existují polynomy $r(x), e(x)$, pro něž

$$h(x) = k(x)e(x) + r(x),$$

přičemž stupeň $r(x) <$ stupeň $k(x) = s$.

Potřebuji však ještě ukázat, že $e(x) \in J'[x]$. Proto dokážeme

V 8,4

Buďte $h(x)$, $k(x) \in J'[x]$ polynomy stupňů $r \geqslant s$. Pak existuje polynom $e(x) \in J'[x]$ stupně $r - s$, že

$$h(x) - k(x)e(x)$$

je polynom stupně nejvýše $s - 1$.

Důkaz:

Pišme $h(x) = x^r + h_1x^{r-1} + \ldots + h_r$

$k(x) = x^s + k_1x^{s-1} + \ldots + k_s$ a položíme-li

$e(x) = x^{r-s} + e_1x^{r-s-1} + \ldots + e_{r-s}$, je

$$k(x)e(x) = x^s + x^{s-1}(e_1 + k_1) + \ldots + x\,(e_{r-s} + e_{r-s-1}k_1 + \ldots) + e_{r-s}k_s$$

Zvolíme-li čísla $e_1, e_2, \ldots, e_{r-s}$ tak, že

$$\begin{aligned} e_1 + k_1 &= h_1 \\ e_2 + e_1k_1 + k_2 &= h_2 \\ &\ldots \\ e_{r-s} + e_{r-s-1}k_1 + \ldots &= h_{r-s}, \end{aligned}$$

což lze, bude polynom $e(x)$ vyhovovat požadavkům věty.

Nepředpokládáme-li, že $k(x) \in J'[x]$, ale pouze $k(x) \in J[x]$, je podobně

$$k(x) = k_0x^s + \ldots + k_s, \quad e(x) = e_0x^{r-s} + \ldots + e_{r-s},$$

$$\begin{aligned} k(x)e(x) = k_0e_0x^s + x^{s-1}(k_0e_1 + k_1e_0) + x^{s-2}(k_0e_2 + k_1e_1 + k_2e_0) + \ldots + \\ + (k_0e_{r-s} + k_1e_{r-s-1} + \ldots) + \ldots + e_{r-s}k_s. \end{aligned}$$

Požadujeme-li opět, aby

$$\begin{aligned} k_0e_0 &= h_0 \\ k_0e_1 + k_1e_0 &= h_1 \\ &\ldots \\ k_0e_{r-s} + k_1e_{r-s-1} + \ldots &= h_{r-s}, \end{aligned} \tag{1}$$

lze rovnice pro e_i opět vždy vyřešit ($k_0 \neq 0$), ale čísla $e_0, e_1, \ldots, e_{r-s}$ nejsou nutně celá. Je-li však polynom $h(x)$ dělitelný k_0^{r-s+1}, je podle první rovnice (1) e_0 celé číslo dělitelné k_0^{r-s}, podle druhé je e_1 celé číslo dělitelné zřejmě k_0^{r-s-1} a tak dále, až z poslední rovnice dostanu, že e_{r-s} je celé číslo dělitelné $k_0^{r-s-(r-s)} = k_0^0$. Platí tedy

V 8,5

Buďte $h(x)$, $k(x) \in J[x]$ dva polynomy stupňů $r \geqslant s$. Označme k_0 koeficient u x^s v $k(x)$ a $q = r - s$. (Je $k_0 \neq 0$, $q \geqslant 0$.) Je-li $h(x)$ dělitelný k_0^{q+1}, pak polynomy $e(x)$ a $r(x)$, pro něž platí

(2) $h(x) = k(x)e(x) + r(x)$, stupeň $r(x) < s$, jsou prvky $J[x]$.

Důkaz:

$e(x) \in J[x]$ podle předchozího a $r(x) \in J[x]$ podle rovnice (2).

§9. *Podmínky pro* d_i.

V 9,1

Buď J_f okruh generovaný prvkem Θ a buď $\{\vartheta_1, \ldots, \vartheta_n\}$ přidružený vektor k Θ. Potom platí (zachováme-li značení §8)

$$d_1(f)d_2(f) \ldots d_{k-1}(f)/\Delta(\vartheta_{i_1}, \ldots, \vartheta_{i_k})$$

pro každou kombinaci čísel $i_1, i_2, \ldots, i_k$ z 1, 2, …, n. (Definici $d_i(f)$ viz za větou 6,5).

Důkaz:

Zaveďme determinant

$$D_k = \begin{vmatrix} \frac{\varphi_0(\vartheta_{i_1})}{d_0} & \frac{\varphi_1(\vartheta_{i_1})}{d_1} & \ldots & \frac{\varphi_{k-1}(\vartheta_{i_1})}{d_{k-1}} \\ \frac{\varphi_0(\vartheta_{i_2})}{d_0} & \frac{\varphi_1(\vartheta_{i_2})}{d_1} & \ldots & \frac{\varphi_{k-1}(\vartheta_{i_2})}{d_{k-1}} \\ & & \ldots & \\ \frac{\varphi_0(\vartheta_{i_k})}{d_0} & \frac{\varphi_1(\vartheta_{i_k})}{d_1} & \ldots & \frac{\varphi_{k-1}(\vartheta_{i_k})}{d_{k-1}} \end{vmatrix}.$$

Jeho prvky jsou celá algebraická čísla, tedy je i D_k celé algebraické číslo. Počítejme:

$$D_k = \begin{vmatrix} 1 & \frac{\vartheta_{i_1} + c_{11}}{d_1} & \frac{\vartheta_{i_1}^2 + c_{21}\vartheta_{i_1} + c_{22}}{d_2} & \ldots & \frac{\vartheta_{i_1}^{k-1} + c_{k-1,1}\vartheta_{i_1}^{k-2} + \ldots + c_{k-1,k-1}}{d_{k-1}} \\ & & & \ldots & \\ 1 & \frac{\vartheta_{i_k} + c_{11}}{d_1} & \frac{\vartheta_{i_k}^2 + c_{21}\vartheta_{i_k} + c_{22}}{d_2} & \ldots & \frac{\vartheta_{i_k}^{k-1} + c_{k-1,1}\vartheta_{i_k}^{k-2} + \ldots + c_{k-1,k-1}}{d_{k-1}} \end{vmatrix}$$

Vytkneme z druhého řádku $\frac{1}{d_1}$ a odečteme od něho první řádek násobený c_{11}:

$$D_k = \frac{1}{d_1} \begin{vmatrix} 1 & \vartheta_{i_1} & \frac{\vartheta_{i_1}^2 + c_{21}\vartheta_{i_1} + c_{22}}{d_2} & \ldots \\ & & \ldots & \\ 1 & \vartheta_{i_k} & \frac{\vartheta_{i_k}^2 + c_{21}\vartheta_{i_k} + c_{22}}{d_2} & \ldots \end{vmatrix}.$$

Z třetího sloupce vytkneme $\frac{1}{d_2}$ a odečteme (c_{22}.první sloupec + c_{21}. .druhý sloupec):

$$D_k = \frac{1}{d_1} \cdot \frac{1}{d_2} \begin{vmatrix} 1 & \vartheta_{i_1} & \vartheta_{i_1}^2 & \frac{\varphi_2(\vartheta_{i_1})}{d_3} & \dots \\ & & \dots & & \\ 1 & \vartheta_{i_k} & \vartheta_{i_k}^2 & \frac{\varphi_2(\vartheta_{i_k})}{d_3} & \dots \end{vmatrix}$$

a tak dále, až dostaneme

$$D_k = \frac{1}{d_1}\frac{1}{d_2} \dots \frac{1}{d_{k-1}} \begin{vmatrix} 1 & \vartheta_{i_1} & \dots & \vartheta_{i_1}^{k-1} \\ & & \dots & \\ 1 & \vartheta_{i_k} & \dots & \vartheta_{i_k}^{k-1} \end{vmatrix} = \frac{\Delta(\vartheta_{i_1}, \dots, \vartheta_{i_k})}{d_1 \dots d_{k-1}},$$

neboli $d_1 d_2 \dots d_{k-1} D_k = \Delta(\vartheta_{i_1}, \dots, \vartheta_{i_k})$, což jsme chtěli dokázat. Tato věta poskytuje tedy horní hranici pro velikost čísel d_i. Speciálně z ní plyne, že

$$(1)\, d_1 d_2 \dots d_{k-1} / (\Delta(\vartheta_1, \dots, \vartheta_k), \Delta(\vartheta_1, \dots, \vartheta_{k-1}, \vartheta_{k+1}), \dots, \Delta(\vartheta_{n-k+1}, \dots, \vartheta_n)),$$

totiž, že $d_1 \dots d_{k-1}$ dělí největšího společného dělitele všech čísel $\Delta(\vartheta_{i_1}, \dots, \vartheta_{i_k})$. Nebo, položíme-li δ_k největší celé racionální číslo takové, že $\frac{\Delta(\vartheta_{i_1}, \dots, \vartheta_{i_k})}{\delta_k}$ je celé algebraické číslo pro všechny kombinace i_j, platí

(2) $\qquad d_1 d_2 \dots d_{k-1}/\delta_k$, neboť čísla d_i jsou racionální.

Ale žádná takováto věta nemá velký praktický význam, neboť výpočet čísel $\Delta(\vartheta_{i_1}, \dots, \vartheta_{i_k})$, jejich největšího společného dělitele nebo čísla δ_k je numericky značně složitý, a to i pro polynomy nízkého stupně. Lze však odvodit praktičtější, ale patrně hrubší omezení. Z (2) plyne

(3) $\qquad d_1^2 \dots d_{k-1}^2/\delta_k^2.$

Použijeme nyní pomocné věty 8,1, v níž dosadíme za x_i ϑ_i. Protože platí

$\delta_i/\Delta(\vartheta_{i_1}, \dots, \vartheta_{i_k})$, je z V 8,1

$\delta_i^2/S^{i_1 \dots i_k}_{j_1 \dots j_k}$ pro všechna $i_1, \dots, i_n$. Tedy platí

V 9,2

Buď S matice $\begin{pmatrix} s_0 & s_1 & \dots & s_{n-1} \\ s_1 & s_2 & \dots & s_n \\ & \dots & & \\ s_{n-1} & s_n & \dots & s_{2n-2} \end{pmatrix}$, buď Δ_k největší společný dělitel všech minorů matice S řádu k. Potom platí

$$d_1^2 d_2^2 \dots d_{k-1}^2 / \Delta_k \text{ a specielně}$$
$$d_1^2 d_2^2 \dots d_{n-1}^2 / \Delta_n = \text{Det } S = \Delta_f .$$

Poznámka.

Nepodařilo se mi zjistit, kdy platí $\Delta_k = \delta_k^2$, tj., kdy věta 9,2 dává stejně silné omezení jako V 9,1. (Platí to např. tehdy, je-li $d_1 = d_2 = \dots = d_k = \Delta_{k+1} = 1$.) Avšak ani V 9,1 nedává přesnou hranici. Například

$$J_{x^2+2} \text{ má basi } \langle 1, \sqrt{2} \rangle, \text{ tj. } d_1 = 1,$$
ačkoliv $\quad \Delta(\vartheta_1, \vartheta_2) = (\sqrt{2} - (-\sqrt{2})) = 2\sqrt{2}$, tj. $\delta_1 = 2$.

Jsou-li však koeficienty rovnice spolu nesoudělné a nesoudělné s n!, pak alespoň pro $n = 2,3$ je odhad přesný, jak lze bez obtíží spočítat. (Pro n = 3 viz příklad dále.)

§10. *Další omezení.*

Označme

$$\overline{Q}_0(x) = 1$$
$$\overline{Q}_k(x) = \Sigma \Delta^2(\vartheta_1, \dots, \vartheta_k)\,(x - \vartheta_1) \dots (x - \vartheta_k) \quad k = 1,2, \dots, n.$$

Součet v definici se bere přes všechny kombinace z čísel $\vartheta_1, \dots, \vartheta_n$.

V 10,1

Platí

$$\overline{Q}_k(x) = \begin{vmatrix} s_0 & s_1 & \dots & s_{k-1} & 1 \\ s_1 & s_2 & \dots & s_k & x \\ & & \dots & & \\ s_k & s_{k+1} & \dots & s_{2k-1} & x^k \end{vmatrix}$$

Důkaz:

Rozvineme $\overline{Q}_k(x)$ podle posledního sloupce:

$$\overline{Q}_k(x) = x^k \begin{vmatrix} s_0 & \dots & s_{k-1} \\ & \dots & \\ s_{k-1} & \dots & s_{2k-2} \end{vmatrix} - \dots + (-1)^{i+k} x^i \begin{vmatrix} s_0 & s_1 & \dots & s_{k-1} \\ & & \dots & \\ s_{i-1} & s_i & \dots & s_{k+i-2} \\ s_{i+1} & s_{i+2} & \dots & s_{k+i} \\ & & \dots & \\ s_k & s_{k+1} & \dots & s_{2k-1} \end{vmatrix} \pm \dots =$$

$$= \sum_{j=0}^{k} (-1)^{j+k} x^j \sum_{i_1 \dots i_k} \begin{vmatrix} 1 & \vartheta_{i_1} & \dots & \vartheta_{i_1}^{k-1} \\ & & \dots & \\ 1 & \vartheta_{i_k} & \dots & \vartheta_{i_k}^{k-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & \vartheta_{i_1} & \dots & \vartheta_{i_1}^{j-1} & \vartheta_{i_1}^{j+1} & \dots & \vartheta_{i_1}^{k} \\ & & \dots & & & & \\ 1 & \vartheta_{i_k} & \dots & \vartheta_{i_k}^{j-1} & \vartheta_{i_k}^{j+1} & \dots & \vartheta_{i_k}^{k} \end{vmatrix},$$

kde součet se bere přes všechny kombinace $i_1, \dots, i_k$ z $1,2, \dots, n$ (srovnej s důkazem V 8,1). Druhý determinant je však rovný (viz V 8,3)

$$\begin{vmatrix} 1 & \vartheta_{i_1} & \dots & \vartheta_{i_1}^{k-1} \\ 1 & \vartheta_{i_k} & \dots & \vartheta_{i_k}^{k-1} \end{vmatrix} \cdot \sum \vartheta_{i_1} \dots \vartheta_{i_{k-j}},$$

tedy $$\overline{Q}(x) = \sum_{j=0}^{k} (-1)^{j+k} x^j \sum \vartheta_{i_1} \dots \vartheta_{i_{k-j}} \sum \Delta^2(\vartheta_{i_1} \dots \vartheta_{i_k}) =$$

$$= \sum \Delta^2(\vartheta_{i_1} \dots \vartheta_{i_k}) \sum_{j=0}^{k} (-1)^{j+k} x^j \sum \vartheta_{i_1} \dots \vartheta_{i_{k-j}} =$$

$$= \sum \Delta^2(\vartheta_{i_1}, \dots, \vartheta_{i_k}) (x - \vartheta_{i_1}) \dots (x - \vartheta_{i_k}).$$

Označme ještě

$$\overline{R}_{n-k}(x) = \sum \Delta^2(\vartheta_1, \dots, \vartheta_k) (x - \vartheta_{k+1}) \dots (x - \vartheta_n),$$

kde součet se bere přes všechny kombinace $k+1$ třídy z $\vartheta_1, \dots, \vartheta_n$ a přes doplňkovou kombinaci v druhém faktoru. Počítejme

$$\overline{Q}_k(\vartheta) f'(\vartheta) = \Sigma \Delta^2(\vartheta_1, \dots, \vartheta_k) (\vartheta - \vartheta_1) \dots (\vartheta - \vartheta_k) . (\vartheta - \vartheta_1) \dots (\vartheta - \vartheta_n) =$$
$$= \Sigma \Delta^2(\vartheta_1, \dots, \vartheta_k, \vartheta) (\vartheta - \vartheta_{k+1}) (\vartheta - \vartheta_{k+2}) \dots (\vartheta - \vartheta_n) = \overline{R}_{n-k-1}(\vartheta).$$

Máme proto (výraz je psán jen symbolicky, rozumí se, že v součtu nahoře i dole chybí výraz $(\vartheta - \vartheta)$):

V 10,2

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

kde $\overline{P}_k(x)$ je vhodný polynom stupně nejvýše k.
Pro praktický výpočet odvodíme větu

V 10,3

Platí

$$\overline{r}_{n-1}^2 f(x) - \overline{S}^{(1)}(x) f'(x) = - \overline{R}_{n-2}(x)$$
$$\overline{r}_{n-2}^2 f'(x) - \overline{S}^{(2)}(x) \overline{R}_{n-2}(x) = - \overline{r}_{n-1}^2 \overline{R}_{n-3}(x)$$
$$\dots \dots \dots$$

(1) $$\overline{r}_{n-k}^2\overline{R}_{n-k+1}(x) - \overline{S}^{(k)}(x)\overline{R}_{n-k}(x) = -\overline{r}_{n-k+1}^2\overline{R}_{n-k-1}(x)$$

$$\cdots\cdots\cdots$$

$$\overline{r}_1^2\overline{R}_2(x) - \overline{S}^{(n-1)}(x)\overline{R}_1(x) = -\overline{r}_2^2\overline{R}_0(x)$$

kde $\overline{S}^{(i)}(x)$ je jednoznačně určený polynom prvého stupně a $\overline{r}_k$ je koeficient u x^k v $\overline{R}_k(x)$, $\overline{r}_{n-1} = n$.

Poznámka.

Vzorce (1) jsou v podstatě Eukleidův algoritmus provedený na $f(x)$, $f'(x)$ (až na koeficient $\overline{r}_i^2$, což může být někdy nula) a dávají nám tedy možnost $\overline{R}_k(x)$ skutečně vypočítat.

Důkaz V 10,3.

Je, jak vyplývá z definice $\overline{R}_{n-k+1}$ pro $k = 0$,

$$\overline{R}_{n-1}(x) = f'(x) \text{ a položme ještě } \overline{R}_n(x) = f(x).$$

Pak věta 10,2 v této symbolice dá

(2) $$\overline{R}_{n-k-1}(x) = \overline{Q}_k(x)\overline{R}_{n-1}(x) - \overline{P}_{k-1}(x)\overline{R}_n(x).$$

Je postupně (argument x pro jednoduchost vynechávám):

$$\begin{aligned}
0 = \overline{R}_{n-1}[&\overline{P}_{i-1}(\overline{Q}_k\overline{Q}_j - \overline{Q}_j\overline{Q}_k) + \overline{P}_{j-1}(\overline{Q}_i\overline{Q}_k - \overline{Q}_k\overline{Q}_i) + \overline{P}_{k-1}(\overline{Q}_j\overline{Q}_i - \overline{Q}_i\overline{Q}_j)] + \\
&+ \overline{R}_n[\overline{Q}_i(\overline{P}_{k-1}\overline{P}_{j-1} - \overline{P}_{j-1}\overline{P}_{k-1}) + \overline{Q}_j(\overline{P}_{i-1}\overline{P}_{k-1} - \overline{P}_{k-1}\overline{P}_{i-1}) + \\
&+ \overline{Q}_k(\overline{P}_{i-1}\overline{P}_{j-1} - \overline{P}_{j-1}\overline{P}_{i-1})] = \\
&= (\overline{Q}_k\overline{R}_{n-1} - \overline{P}_{k-1}\overline{R}_n)(\overline{P}_{i-1}\overline{Q}_j - \overline{P}_{j-1}\overline{Q}_i) + \\
&+ (\overline{Q}_j\overline{R}_{n-1} - \overline{P}_{j-1}\overline{R}_n)(\overline{P}_{k-1}\overline{Q}_i - \overline{P}_{i-1}\overline{Q}_k) + \\
&+ (\overline{Q}_i\overline{R}_{n-1} - \overline{P}_{i-1}\overline{R}_n)(\overline{P}_{j-1}\overline{Q}_k - \overline{P}_{k-1}\overline{Q}_j) = \\
&= \overline{R}_{n-k-1}(\overline{P}_{i-1}\overline{Q}_j - \overline{P}_{j-1}\overline{Q}_i) + \overline{R}_{n-j-1}(\overline{P}_{k-1}\overline{Q}_i - \overline{Q}_k\overline{P}_{i-1}) + \\
&+ \overline{R}_{n-i-1}(\overline{P}_{j-1}\overline{Q}_k - \overline{Q}_j\overline{P}_{k-1}).
\end{aligned}$$

Dosaďme ještě

(3) $$\begin{aligned} j &= k - 1 \\ i &= k - 2. \end{aligned}$$ Je

(4) $$\begin{aligned}
&\overline{R}_{n-k+1}(\overline{P}_{k-2}\overline{Q}_k - \overline{P}_{k-1}\overline{Q}_{k-1}) + \overline{R}_{n-k}(\overline{P}_{k-1}\overline{Q}_{k-2} - \overline{P}_{k-3}\overline{Q}_k) = \\
&= -(\overline{P}_{k-3}\overline{Q}_{k-1} - \overline{P}_{k-2}\overline{Q}_{k-2})\overline{R}_{n-k-1}.
\end{aligned}$$

Dokážeme-li ještě, že

$$\overline{P}_{k-2}\overline{Q}_k - \overline{P}_{k-1}\overline{Q}_{k-1} = \overline{r}_{n-k}^2, \text{ dá (4) ihned větu.}$$

Podle (2) je

$$\begin{aligned}\overline{Q}_{i+1}\overline{R}_{n-1} - \overline{P}_i\overline{R}_n &= \overline{R}_{n-i-2}\\ \overline{Q}_{i+2}\overline{R}_{n-1} - \overline{P}_{i+1}\overline{R}_n &= \overline{R}_{n-i-3}.\end{aligned} \tag{5}$$

Buď zatím determinant soustavy různý od nuly. Pak je

$$\overline{R}_n = \frac{\begin{vmatrix}\overline{Q}_{i+1} & -\overline{R}_{n-i-2}\\ \overline{Q}_{i+2} & -\overline{R}_{n-i-3}\end{vmatrix}}{\begin{vmatrix}\overline{Q}_{i+1} & -\overline{P}_i\\ \overline{Q}_{i+2} & -\overline{P}_{i+1}\end{vmatrix}}. \tag{6}$$

Polynom v čitateli je stupně nejvýše n, proto je jmenovatel stupně 0 a čitatel stupně právě n. Označíme-li koeficienty u nejvyšší mocniny v $\overline{Q}_i$ resp. $\overline{P}_k$ $\overline{q}_i$ resp. $\overline{p}_k$, plyne z (6) porovnáním

$$\overline{r}_{n-i-2}\overline{q}_{i+2}(-\overline{Q}_{i+1}\overline{P}_{i+1} + \overline{P}_i\overline{Q}_{i+2})^{-1} = r_n.$$

Je ovšem $r_n = 1$, a z definice $\overline{R}_{n-k}$, $\overline{Q}_k$ plyne $\overline{r}_{n-k} = \overline{q}_k$, tedy

$$\overline{P}_i\overline{Q}_{i+2} - \overline{P}_{i+1}\overline{Q}_{i+1} = \overline{r}^2_{n-i-2}. \tag{7}$$

Je-li však determinant soustavy roven nule, pak je ovšem první rovnice (5) násobkem druhé ($R_n \neq 0$), tedy

$$R_{n-i-2} = dR_{n-i-3},$$

a tedy R_{n-i-2} je stupně $n - i - 3$, čili $\overline{r}_{n-i-2} = 0$ a rovnost (7) platí, neboť levá strana (7) je determinant soustavy). K důkazu věty je nyní třeba ukázat pouze, že $\overline{S}^{(i)}(x)$ je prvního stupně, to však plyne z rovnice (1) bezprostředně.

Algoritmus (1) je numericky snadno upotřebitelný. Jediná jeho větší nevýhoda je snad v tom, že koeficienty u polynomů se často dosti zvětšují. Tuto nesnáz možno odstranit. Položme

$$\overline{R}_{n-k}(x) = e_0^k e_1^{k-1} \ldots e_{k-1}R_{n-k}(x) \ (k = 1, 2, \ldots, n),$$

kde číslo $f_k = e_0^k \ldots e_{k-1}$ je největší společný dělitel koeficientů polynomu $\overline{R}_{n-k}$, takže R_{n-k} je primitivní polynom. Čísla f_k jsou tedy celá a $e_k = \frac{f_{k+1}f_{k-1}}{f_k^2}$ jsou obecně racionální (např. pro $f(x) = x^4 + 2x^2 + 2x + 2$ je $e_2 = \frac{1}{2}$).

Zaveďme ještě $r_{n-k} = \frac{\overline{r}_{n-k}}{f_k}$ je koeficient u $n - k$-té mocniny v R_{n-k}.

Je pak z (1)

$$r^2_{n-1}f(x) - S^{(1)}(x)R_{n-1}(x) = -e_1R_{n-2}(x) \tag{8}$$

. . . . . .

(8) $$r_{n-k}^2 R_{n-k+1}(x) - S^{(k)}(x)R_{n-k}(x) = -e_k r_{n-k+1}^2 R_{n-k-1}(x)$$

$$\cdots\cdots\cdots$$

$$r_1^2 R_2(x) - S^{(n-1)}(x)R_1(x) = -e_{n-1}r_2^2 R_0(x).$$

Zde je $R_0 = 1$ a $S^{(i)}(x)$ je vhodný polynom svázaný s $\overline{S}^{(i)}(x)$ vztahem $S^{(i)}(x) = \dfrac{\overline{S}^{(i)}(x)}{f_i f_{i-1}}$.

(8) je opět Eukleidův algoritmus (se stejnými výhradami jako předtím. Jsou totiž v případě $r_k = 0$ některé řádky ve schématu navíc proti obvyklému schématu Eukleidova algoritmu). Z věty 8,5 plyne, že koeficienty polynomu $S^{(k)}(x)$ a číslo $e_k r_{n-k-1}^2$ jsou čísla celá.

Ve větě 9,1 jsme zavedli číslo δ_k, které dělilo všechna $\Delta(\vartheta_{i_1}, \ldots, \vartheta_{i_k})$. Je, jak plyne okamžitě z definice $R_{n-k}(x)$,

$$\delta_k^2 / f_k.$$

Proto z věty 9,1 plyne

V 10,4

$$d_1^2 d_2^2 \ldots d_{k-1}^2 / f_k.$$

Dále platí

V 10,5

$$\Delta_f = f_n.$$

Důkaz:

Podle definice je $\overline{R}_0 = \Sigma\Delta^2(\vartheta_1, \ldots, \vartheta_n) = \Delta^2(\vartheta_1, \ldots, \vartheta_n) = \Delta_f$.

Vraťme se nyní k polynomům $\overline{Q}_k(x)$. Jest podle definice

$$\overline{Q}_k(x) = \Sigma\Delta^2(\vartheta_1, \ldots, \vartheta_k)(x - \vartheta_1) \ldots (x - \vartheta_k) \quad k = 1, \ldots, n.$$

Tedy protože $\delta_k / \Delta(\vartheta_1, \ldots, \vartheta_k)$, platí $\delta_k^2 / \overline{Q}_k(x)$ a dokonce ze stejného důvodu platí

(1) $$\delta_{k+1}\delta_k / \overline{Q}(\vartheta), \text{ kde } \vartheta \text{ je kterékoli } \vartheta_i.$$

Z toho ovšem plyne podle V 3,5, že

$$\frac{\overline{Q}_k(\Theta)}{\delta_k \delta_{k+1}} \in J_f.$$

Buď m_k největší společný dělitel koeficientů v $\overline{Q}_k(x)$ a označme

$$\frac{\overline{Q}_k(x)}{m_k} = Q'_k(x) \in J[x].$$

Buď m'_k číslo, které dostaneme z m_k tím, že v něm potlačíme všechny prvočíselné faktory, jež nejsou v $\delta_k\delta_{k+1}$ a snížíme exponent těch, které tam jsou, na exponent v tomto součinu. Položme ještě

$$\frac{\delta_{k+1}\delta_k}{m'_k} = n_k.$$

Je podle předešlého

(2) $\dfrac{Q'_k(\Theta)}{n_k}$ celé algebraické číslo.

Poslední formuli lze ještě trochu zlepšit. Označme na chvíli Δ_k největšího společného dělitele čísel $\Delta(\vartheta_{i_1}, \ldots, \vartheta_{i_k})$. Potom platí nejen (1), ale dokonce $\Delta_k \Delta_{k+1} / \overline{Q_k}(\vartheta)$. Položíme pak $\dfrac{\Delta_{k+1}\Delta_k}{m'_k} = n'_k$. Najdeme-li ještě n''_k největší celé racionální číslo, které dělí n'_k, lze (2) nahradit $\dfrac{Q'_k(\Theta)}{n'_k} \in J_f$, přičemž obecně n_k / n''_k, takže poslední vztah je o něco silnější. Ale ovšem prakticky sotva použitelný pro nesnadný výpočet Δ_k. Poznamenejme ještě, že číslo Δ_k je totožné s číslem Δ_k, jak je zavedl prof. Petr v kapitole III citovaného referátu. Petr vzal prvočísla $p_1, p_2, \ldots$ dělící diskriminant Δ_f. Pak hledal největší racionální číslo a_i, aby $p_i^{a_i} / \Delta(\vartheta_1, \ldots, \vartheta_k)$, načež položil $\Delta_k = p_1^{a_1} p_2^{a_2} \ldots$.
Tedy známe-li $\overline{Q_k}(x)$, známe nějaká, často netriviální, celá čísla z našeho okruhu. To nám dává zřejmě odhad pro velikost čísel d_k, a to odhad s druhé strany, než dává věta 10,4, neboť ukazuje, že d_i musí být alespoň tak velké, aby prvky

$$\frac{Q'_1(\Theta)}{n_1}, \frac{Q'_2(\Theta)}{n_2}, \ldots, \frac{Q'_{n-1}(\Theta)}{n_{n-1}}$$

ležely v modulu vytvořeném naší basí.

Z těchto omezení vychází konečný a zpravidla nepříliš značný počet systémů pro čísla $d_1, d_2, \ldots, d_n$. Kromě toho platí ještě další omezení, a to

V 10,6

Buďte r_i celá nezáporná taková, že $r_1 + 2r_2 + \ldots + ir_i \leqslant k$, pak

$$d_1^{r_1} \cdot d_2^{r_2} \ldots d_i^{r_i} \mid d_k .$$

Důkaz plyne z toho, že

$$\frac{\varphi_1^{r_1}(\Theta)}{d_1^{r_1}} \ldots \frac{\varphi_i^{r_i}(\Theta)}{d_i^{r_i}} \in J_f \text{ je polynom stupně} \leqslant k \text{ v } \Theta,$$

a proto ho lze napsat jako lineární kombinaci prvních k členů base:

$$\frac{\varphi_1^{r_1}(\Theta)}{d_1^{r_1}} \ldots \frac{\varphi_i^{r_i}(\Theta)}{d_i^{r_i}} = \sum_{i=1}^{k} \lambda_i \frac{\varphi_i(\Theta)}{d_i} .$$

Porovnání koeficientů u nejvyšší mocniny Θ^k dá

$$\frac{1}{d_1^{r_1} \ldots d_i^{r_i}} = \frac{\lambda_k}{d_k}, \text{ z čehož plyne tvrzení věty.}$$

Pro výpočet polynomu Q platí analogické formule jako pro výpočet R. Skutečně zjistili jsme již (V 10,2), že

$$\begin{aligned}\overline{R}_{n-k-2} &= \overline{Q}_{k+1}\overline{R}_{n-1} - \overline{P}_k\overline{R}_n\\ \overline{R}_{n-k-1} &= \overline{Q}_k\overline{R}_{n-1} - \overline{P}_{k-1}\overline{R}_n\\ \overline{R}_{n-k} &= \overline{Q}_{k-1}\overline{R}_{n-1} - \overline{P}_{k-2}\overline{R}_n.\end{aligned}$$

Vynásobme první rovnici $\overline{r}^2_{n-k}$, druhou $-\overline{S}^{(k+1)}$ a třetí $\overline{r}^2_{n-k-1}$. Sečtěme a dostaneme

$$\begin{aligned}&\overline{r}^2_{n-k}\overline{R}_{n-k-2} - \overline{S}^{(k+1)}\overline{R}_{n-k-1} + \overline{r}^2_{n-k-1}\overline{R}_{n-k} =\\ &= \overline{R}_{n-1}(\overline{r}^2_{n-k}\overline{Q}_{k+1} - \overline{S}^{(k+1)}\overline{Q}_k + \overline{r}^2_{n-k-1}\overline{Q}_{k-1}) +\\ &+ \overline{R}_n(\overline{r}^2_{n-k}\overline{P}_k + \overline{S}^{(k+1)}\overline{P}_{k-1} + \overline{r}^2_{n-k-1}\overline{P}_{k-2}).\end{aligned} \tag{2}$$

Levá strana se však podle (1) z V 10,3 rovná nule. Tedy

$$\overline{R}_{n-1}q_{k+1} = -\overline{R}_n p_k, \tag{3}$$

kde jsem pro jednoduchost polynomy v závorce u (2) označil q_{k+1} resp. p_k. Polynomy $\overline{R}_{n-1}$, $\overline{R}_n$ jsou nesoudělné, a proto (3) dává

$$\overline{R}_n/q_{k+1};$$

protože stupeň q_{k+1} je nejvýše $k+1$ a stupeň $\overline{R}_n$ je právě $n > k+1$, je $q_{k+1} = 0$ identicky a tedy

$$\overline{r}^2_{n-k-1}\overline{Q}_{k-1} - \overline{S}^{(k+1)}\overline{Q}_k = -\overline{r}^2_{n-k}\overline{Q}_{k+1} \text{ pro } k = 2, 3, \ldots, n-1. \tag{4}$$

Položíme-li $Q_{-1} = 0$, platí (4), jak lze spočítat i pro $k = 1$.

Polynomy $\frac{\overline{Q}_k(x)}{n_k}$ nám často poskytují dokonce basi J_f; obecně však lze říci pouze, že dávají jen basi nějakého podokruhu J_f. Bylo by důležité zjistit, kdy basi dávají. Domnívám se, že podmínka pro to záleží pouze v tom, jak velkým číslem jsou dělitelny koeficienty polynomu $\overline{Q}_k(x)$ a na jeho vedoucím členu. Příklad, který uvedl prof. Petr ve svém referátě [1] a příklad, který uvedu dál, tuto domněnku potvrzuje.

Velkého zjednodušení v našem příkladě se dosáhne, bude-li base tvaru $1, \Theta, \ldots$.

Všimněme si proto, že $\frac{\Theta}{\alpha} \in J_f$, právě když i-tý koeficient v $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ je dělitelný $\alpha^i : \alpha^i/a_i$. Nastane-li tento případ, snadno se z rovnice zjistí a substitucí $\frac{\Theta}{\alpha} = \Theta'$ se odstraní. Ale i pak se může stát, že $\frac{\Theta + a}{d} \in J_f$ pro nějaké a. Proto tento případ blíže vyšetřeme.

Každou rovnici můžeme celistvou lineární substitucí $(nx = y - a_1)$ převést na rovnici, jejíž koeficient u x^{n-1} je roven nule. Učiňme tak.

V 10,7 pomocná.

Buď $f(x) = x^n + a_2x^{n-2} \ldots + a_n$, $a \in J$. Buď $\frac{\Theta + a}{p} \in J_f$ pro nějaké celé číslo a a pro prvočíslo p. Pak je buď

(1) $\qquad p^i \mid a_i \quad i = 1, 2, \ldots, n$ nebo

(2) $\qquad p \mid n.$

Důkaz:

Nechť (1) neplatí, tedy podle předchozího $\frac{\Theta}{p} \notin J_f$. Označme $x + a = z$ a $g(z) = (z - a)^n + a_2(z - a)^{n-2} + \ldots + a_n$. Je-li Θ' generátor J_g, je zřejmě $\frac{\Theta'}{p} \in J_g$, a tedy p^i dělí i-tý koeficient u $g(x)$. Tedy speciálně druhý

$$p \mid na.$$

Ovšem $p \nmid a$, neboť z $\frac{\Theta + a}{p} \in J_f$ by pak plynulo $\frac{\Theta}{p} + \frac{a}{p} \in J_f$, tedy $\frac{\Theta}{p} \in J_f$, což jsme vyloučili.

Příklad.

Mějme rovnici třetího stupně $f(x) = x^3 + ax + b$. Označme součet k-tých mocnin kořenů s_k. Je

$$\begin{aligned} s_0 &= 3 \\ s_1 &= 0 \\ s_2 &= -2a \\ s_3 &= -3b \\ s_4 &= 2a^2 - 4a \quad \text{a tedy} \end{aligned}$$

$$\overline{Q}_1(x) = \begin{vmatrix} 3 & 1 \\ 0 & x \end{vmatrix} = 3x, \quad \overline{Q}_2(x) = \begin{vmatrix} 3 & 0 & 1 \\ 0 & -2a & x \\ -2a & -3b & x^2 \end{vmatrix} = -6ax^2 + 9bx - 4a^2.$$

Je podle tohoto paragrafu

$$\overline{\omega} = \frac{6a\Theta^2 - 9b\Theta + 4a^2}{\Delta_2\Delta_3} \in J_f.$$

Buď nyní p prvočíslo nedělící $6a$. Buď $q = Exp_p\Delta_2\Delta_3$. Pak, zavedeme-li

$$\omega = \frac{6a\Theta^2 - 9b\Theta + 4a^2}{p^q}, \text{ je } \langle 1, \Theta, \omega \rangle \text{ base } J_f^{(p)}.$$

Skutečně:

1. Podle pomocné věty 10,7 není žádné číslo tvaru $\frac{\Theta + \alpha}{p}$ celé.

2. Buď nyní $\langle 1, \Theta, \tilde{\omega}\rangle$ base $J_f^{(p)}$. Buď $\tilde{\omega} = \frac{\Theta^2 + \alpha\Theta + \beta}{p^s}$.

Dále platí podle 10,4, neboť $f_3 = \Delta_3^2$,

$$p^s \mid d_2 \mid \Delta_3, \text{ tedy } s \leqslant q.$$

Je také $\omega = \lambda_1 + \lambda_2\Theta + \lambda_3\tilde{\omega}$, z čehož srovnáním koeficientu u Θ^2:

$\frac{6a}{p^q} = \frac{\lambda_3}{p^s}$, tedy $6a = \lambda_3 p^{q-s}$, ale $p \nmid 6a$, proto $q = s$. Spočtěme

$$6a\tilde{\omega} - \omega = \frac{(6a\alpha + 9b)\Theta + (6a\beta - 4a^2)}{p^q} = \omega'. \tag{1}$$

Označme $0 \leqslant r$ nejvyšší mocninu p, která dělí $6a\alpha + 9b$. Buď zatím $r < q$. Je ovšem

$$\frac{(6a\alpha + 9b)\Theta + (6a\beta - 4a^2)}{p^r} \in J_f \text{ a tedy } \frac{(6a\alpha + 9b)}{p^r}\Theta + \frac{6a\beta - 4a^2}{p^r} \in J_f,$$

z čehož plyne $p^r \mid 6a\beta - 4a^2$. Označíme-li

$$\frac{6a\alpha + 9b}{p^r} = e_1 \in J, \quad \frac{6a\beta - 4a^2}{p^r} = e_2 \in J,$$

je $\omega' = \frac{e_1\Theta + e_2}{p^{q-r}} \in J_f$ a podle předpokladu je ještě $p \nmid e_1$, tedy $(p^{q-r}, e_1) = 1$. Nalezneme čísla x, y, aby $e_1 x + p^{q-r}y = 1$. Pak lze tvrdit, že $x\omega' + y\Theta = \frac{(xe_1 + p^{q-r}y)\Theta + xe_2}{p^{q-r}} = \frac{\Theta + xe_2}{p^{q-r}} \in J_f$, a tedy vzhledem k bodu 1, je $q = r$, neboli $p^q \mid 6a\alpha + 9b$ a $p^q \mid 6a\beta - 4a^2$. Je-li však $r \geqslant q$, máme hned $p^q \mid 6a\alpha + 9b$, a tedy z relace $\frac{6a\alpha + 9b}{p^q}\Theta + \frac{6a\beta - 4a^2}{p^q} \in J_f$ plyne opět, že $p^q \mid 6a\beta - 4a^2$.

Je tedy $\omega' = e_1\Theta + e_2$, a protože 1 i Θ leží v obou basích $\langle 1, \Theta, \omega\rangle$, $\langle 1, \Theta, \tilde{\omega}\rangle$, leží v obou i ω' a relace (1) dokazuje, že $\langle 1, \Theta, \omega\rangle \sim \langle 1, \Theta, \tilde{\omega}\rangle$. Známe-li však basi $\langle 1, \Theta, \omega\rangle$, sestrojíme snadno Θ-basi (vzhledem k p).

§11. *Podmínky pro $\varphi(x)$.*

Buď jako obvykle $f(x) = 0$ rovnice s jednoduchými kořeny, J_f okruh jí vytvořený a Θ jeho generátor.

Buď $\langle \omega^{(p)}\rangle = \langle \omega_1^{(p)}, \ldots, \omega_n^{(p)}\rangle$ Θ-base J_f vzhledem k prvočíslu p a $\langle \omega\rangle = \langle \omega_1, \ldots, \omega_n\rangle$ Θ-base J_f. Poslední budeme někdy pro jednoduchost značit $\langle \omega^{(0)}\rangle$.

Buď

$$(1)\quad \omega_k^{(p)} = \frac{\varphi_{k-1}^{(p)}(\Theta)}{p^{q_{k-1}}},\ \varphi_k^{(p)}(x) = \sum_{i=0}^{k} c_{k,i}^{(p)} x^i,\ c_{kk} = 1,\ k = 0, 1, \ldots, n-1.$$

Je-li $p = 0$, nutno ovšem první rovnici v (1) rozumět

$$\omega_k = \frac{\varphi_{k-1}(\Theta)}{d_{k-1}} = \frac{\varphi_{k-1}^{(0)}(\Theta)}{d_{k-1}}.$$

Toto označení zachováme po celý tento §.

V 11,1

Pro exponenty q_k platí

$$q_k + q_e \leqslant q_{k+e} \quad \text{pro} \quad k + e \leqslant n-1,$$

a analogicky $d_k d_e / d_{k+e}$ pro $k + e \leqslant n-1$.

Důkaz je důsledek věty 10,6.
Je tedy speciálně

$d_1/d_2 \ldots / d_{n-1}$ a $0 \leqslant q_1 \leqslant q_2 \leqslant \ldots \leqslant q_{n-1}$. Lze proto zavést $\frac{d_k}{d_{k-1}} = c_k \in J$ a psát

$$\begin{aligned} d_1 &= c_1 \\ d_2 &= c_1 c_2 \\ &\ldots\ldots\ldots \\ d_k &= c_1 c_2 \ldots c_k \\ &\ldots\ldots\ldots \\ d_{n-1} &= c_1 c_2 \ldots c_{n-1}. \end{aligned}$$

Platí ovšem ještě, jak se snadno zjistí, $c_1 c_2 \ldots c_e / c_{k+1} \ldots c_{k+e}$ pro každé k, e, $k + e \leqslant n-1$, ale to nás nebude tak zajímat.

V 11,2

Buď c_r přirozené číslo. Platí

1. $\varphi_r(x)/f(x) \pmod{c_r}$ a $\frac{f(x)}{\varphi_r(x)} / f'(x) \pmod{c}$,
2. $\varphi_r(x)/\varphi(x) \pmod{c_r}$ pro $1 \leqslant r \leqslant k \leqslant n-1$, $c_r \neq 1$.

Důkaz:

Podle pomocné věty 8,4 existuje polynom $P_{n-r}(x)$ stupně $n-r$, že $\chi(x) = f(x) - P_{n-r}(x)\varphi_r(x)$ je polynom stupně menšího než r. Je

$$P_{n-r}(\Theta)\frac{\varphi_r(\Theta)}{d_r} = \frac{f(\Theta) - P_{n-r}(\Theta)\varphi_r(\Theta)}{d_r} = \frac{\chi(\Theta)}{d_r} \in J_f,$$

a tedy $$\frac{\mathfrak{z}(\Theta)}{d_r} = \sum_{i=0}^{r-1} \lambda_i \omega_{i+1} = c_r \sum_{i=0}^{r-1} \lambda_i \frac{\varphi_i(\Theta)}{c_1 \dots c_i c_r}.$$

Vynásobením d_r

$$\mathfrak{z}(\Theta) = \left(\sum_{i=0}^{r-1} \lambda_i c_{i+1} \dots c_{r-1} \varphi_i(\Theta) \right) . c_r.$$

Je tedy každý koeficient u Θ^i napravo, tedy i nalevo dělitelný c_r, jinými slovy

(1_1) $$\mathfrak{z}(x) = f(x) - P_{n-r}(x)\varphi_r(x) \equiv 0 \ (c_r), \text{ tedy}$$

(1_2) $$\varphi_r(x) / f(x) \quad (c_r).$$

Tím je 1. dokázáno.
Podle V 8,2 je-li

$$\frac{\varphi_r(\Theta)}{d_r} f'(\Theta) = \sum_{0}^{n-1} b_i \Theta^i, \text{ je } b_i \in J.$$

Označme $\Sigma b_i \Theta^i = \psi_{n-1}(\Theta)$, pak

(2) $$f'(\Theta)\varphi_r(\Theta) = d_r \psi_{n-1}(\Theta), \text{ tedy (viz §1)}$$

(3) $$f'(x)\varphi_r(x) = f(x) Q^{(2)}_{r-1}(x) + d_r \psi_{n-1}(x).$$

Můžeme najít polynomy $Q^{(3)}_{r-1}(x)$, $Q^{(4)}_{n-r-1}(x)$ stupňů $r-1$, $n-r-1$ tak, že

(4) $$f'(x) = P_{n-r}(x) Q^{(3)}_{r-1}(x) + Q^{(4)}_{n-r-1}(x).$$

Dosaďme (4) do (3):

$$f'(x)\varphi_r(x) = P_{n-r}(x) Q^{(3)}_{r-1}(x)\varphi_r(x) + Q^{(4)}_{n-r-1}(x)\varphi_r(x) =$$
$$= f(x) Q^{(2)}_{r-1}(x) + d_r \psi_{n-1}(x).$$

Odtud použitím (1_1)

$$f(x) \left(Q^{(2)}_{r-1}(x) - Q^{(3)}_{r-1}(x) \right) \equiv Q^{(4)}_{n-r-1}(x)\varphi_r(x) \pmod{c_r}.$$

Protože polynom vpravo je stupně nejvýše $n-1$, kdežto $f(x)$ stupně n, je nutně

$$Q^{(2)}_{r-1} \equiv Q^{(3)}_{r-1}(x), \quad \text{tedy} \quad Q^{(4)}_{n-r-1}(x) \equiv 0 \quad (c_r),$$

neboť φ_r je nedělitel nuly mod c_r.
Všimnu-li si rovnice (4), mám

(5) $$f'(x) \equiv P_{n-r}(x) Q^{(3)}_{r-1}(x),$$

tedy $P_{n-r}(x)/f'(x)$ mod c_r, a to je právě (1_2), jak ukazuje (1_1).

Zbývá dokázat 2. Důkaz se povede analogicky jako u bodu 1., a proto ho provedu méně podrobně.

Lze psát $\varphi_k(x) - \varphi_r(x)p_{k-r}(x) = \chi(x)$ a je $\frac{\chi(\Theta)}{d_r} \in J_f$,

z čehož, neboť opět je stupeň $\chi(x) <$ stupeň $\varphi_r(x)$,

$$c_r/\chi(x), \text{ neboli } \varphi_k(x) \equiv \varphi_r(x)p_{k-r}(x) \pmod{c_r}.$$

Poznamenejme, že věta nic neříká, je-li $c_r = 1$. Pak ale lze, jak plyne z V 6,4, $\varphi_r(x)$ předefinovat

$$\varphi_r(x) = x.\varphi_{r-1}(x). \text{ Pak 2. platí.}$$

Nyní dokážeme analogii věty 11,2 pro basi vzhledem k prvočíslu. Buď tedy p prvočíslo a

$$\left\langle \ldots \frac{\varphi_i^{(p)}(\Theta)}{p^{q_i}} \ldots \right\rangle \ \Theta\text{-base } J_f^{(p)}.$$

Je ovšem (V 7,2 nebo V 6,6)

$$\left\langle \ldots \frac{\varphi_i(\Theta)}{p^{q_i}} \ldots \right\rangle \text{ také } \Theta\text{-base } J_f^{(p)}, \text{ a proto (V 6,6)}$$

$$\varphi_i(x) \equiv \varphi_i^{(p)}(x) \pmod{p^{q_i - q_{i-1}}}.$$

Je

p^{q_i} / d_i a $p^{q_{i+1}} \nmid d_i$, proto $p^{q_i - q_{i+1}} / c_i$, tedy

(5)
1. $f(x) \equiv \varphi_r(x)P_{n-r}(x) \equiv \varphi_r^{(p)}(x)P_{n-r}(x) \qquad (p^{q_r - q_{r-1}})$
2. $P_{n-r}(x) / f'(x) \qquad (p^{q_r - q_{r-1}})$
3. $\varphi_r^{(p)}(x) / \varphi_k^{(p)}(x) \qquad (p^{q_r - q_{r-1}}) \qquad (q_r > q_{r-1})$

V tomto případě je však výhodné psát větu ještě jinak.

V 11,3

Buď $f(x) \equiv w_1(x)^{v_1}.w_2(x)^{v_2} \ldots w_s(x)^{v_s}$ (p) rozklad polynomu $f(x)$ na modulo p ireducibilní faktory. Buďte $1 \leqslant r_1 < r_2 < \ldots < n$ ty indexy, pro něž $q_{r_i} > q_{r_i - 1}$. Pro tato r platí rozklad

$$\varphi_r^{(p)} \equiv w_1(x)^{q_{1,r}} \ldots w_s(x)^{q_{s,r}} \pmod{p},$$

přičemž platí $1 \leqslant q_{i,r_1} \leqslant q_{i,r_2} \leqslant \ldots \leqslant v_i$ pro všechna $1 \leqslant i \leqslant s$. Je-li kromě toho stupeň $w_i(x)$ rovný n_i, je ovšem

$$\Sigma n_i q_{i,r} = r.$$

Důkaz:

Věta je celkem jasná, je snad jen třeba ukázat $1 \leqslant q_{i,r_1}$.

Je totiž $f'(x) \equiv w_1(x)^{v_1-1} \ldots w_s(x)^{v_s-1} w_{s+1}(x)^{v_{s+1}} \ldots w_{s+h}(x)^{v_{s+h}}$

a $$P_{n-r}(x) = w_1^{v_1-q_{1,r}}(x) \ldots w_s^{v_s-q_{s,r}}(x).$$

a proto (5_2) dává

$$v_i - q_{i,r} \leqslant v_i - 1 \text{ pro } 1 \leqslant i \leqslant s, \text{ z čehož } 1 \leqslant q_{i,r}.$$

§12. *O prodloužení rozkladu.*

Věta 11,3 v minulém paragrafu značně omezila možnosti pro $\varphi^{(p)}(x)$. Tak například, je-li $f(x) \equiv w_1(x)^{v_1} \ldots w_s(x)^{v_s}$ (p), jsou první členy base vzhledem k p zřejmě

$$1, \Theta, \Theta^2, \ldots, \Theta^{t-1}, \frac{\varphi_i^{(p)}(\Theta)}{p^{q_s}}, \quad \text{kde } t = \sum_{i=0}^{s} n_i$$

a dokonce je $\varphi^{(p)}(x)$ buď x^t nebo je kongruentní s $w_1(x) \ldots w_s(x)$. Vzhledem k větě 11,2 je však V 9,3 trochu zeslabena. Abychom mohli větu 9,3 vyslovit obecněji, je třeba přejít od kongruencí modulo p ke kongruenci mod $p^{q_r-q_{r-1}}$. O tom pojednává následující věta.*)

V 12,1

Nechť

$$a(z) \equiv w_1(z)^{v_1} w_2(z)^{v_2} \ldots w_r(z)^{v_r} \pmod{p}$$

je rozklad nějakého polynomu $a(z)$ na modulo p ireducibilní faktory. Potom platí, ať b je jakkoli velké, také rozklad

$$a(z) \equiv P_1(z) P_2(z) \ldots P_r(z) \pmod{p^b},$$

kde $P_i(z)$ jsou vhodné polynomy takové, že

$P_i(z) \equiv w_i(z)^{v_i} \pmod{p}$, stupeň $P_i(z) =$ stupeň $w_i(z)^{v_i}$ a $P_i(z) \in J'[z]$.

Pak jsou polynomy $P_i(z)$ určeny jednoznačně mod p^b.

Důkaz:

Pišme $$a(z) = \prod_{i=1}^{r} w_i(z)^{v_i} + pV_1(z)$$

a položme

$$\xi_i(z) = w_1(z)^{v_1} \ldots w_{j-1}(z)^{v_{j-1}} w_{j+1}(z)^{v_{j+1}} \ldots w_r(z)^{v_r} \quad (i = 1, 2, \ldots, r).$$

*) Podle [2].

Polynomy $\xi_1(z), \ldots, \xi_r(z)$ jsou nesoudělné mod p, a proto existují celé polynomy $\eta_1'(z), \ldots, \eta_2'(z)$ tak, že platí

(1) $$\Sigma \eta_i'(z)\,\xi_i(z) \equiv 1 \ (p).$$

Položme ještě

$$\eta_i''(z) = \eta_i'(z) V_1(z) \qquad \text{a dostaneme}$$

(2) $$\Sigma \eta_i''(z)\xi_i(z) \equiv V_1(z) \ (p).$$

Přitom jest stupeň $V_1(z) <$ stupeň $a(z) = n = \sum_1^r v_i g_i$, kde jsme písmenem g_i označili stupeň $w_i(z)$.
Je možno nalézt polynomy $Q_1(z), \eta_{11}(z)$ tak, že $\eta_1''(z) = w_1(z)^{v_1} Q_1(z) + \eta_{11}(z)$, přičemž stupeň $\eta_{11}(z) < v_1 g_1$.
Položme $\eta_2''(z) = -w_2(z)^{v_2} Q_1(z) + \eta_{12}'(z)$ a dostaneme dosazením do (2)

(3) $$\eta_{11}(z)\xi_1(z) + \eta_{12}'(z)\xi_2(z) + \ldots + \eta_r(z)\xi_r(z) \equiv V_1(z) \ (p).$$

Je-li stupeň $\eta_{12}' > v_2 g_2 - 1$, položíme opět

$$\eta_{12}' = -w_2^{v_2} Q_2 + \eta_{12}, \text{ stupeň } \eta_{12} < v_2 g_2$$
$$\eta_{13}'' = -w_3^{v_3} Q_2 + \eta_{13}' \text{ a dosazení do (3) dá}$$

$$\eta_{11}(z)\xi_1(z) + \eta_{12}(z)\xi_2(z) + \eta_{13}'(z)\xi_3(z) + \eta_4'(z)\xi_4(z) + \ldots = \eta_r'\xi_r(z) \equiv V_1(z) \ (p),$$

kde stupně prvních dvou členů jsou již menší než $v_1 g_1$ resp. $v_2 g_2$. Postupujeme-li takto dále, dostaneme

$$\sum_1^{r-1} \eta_{1i}(z)\xi_i(z) + \eta_{1r}'(z)\xi_r(z) \equiv V_1(z) \ (p),$$

přičemž stupeň $\eta_{1i}(z) < v_i g_i$ pro $i = 1, 2, \ldots, r-1$. Jest ale stupeň $\xi_i(z) = n - v_i g_i$ a má tedy suma vlevo stupeň nejvýše $n - 1$; také $V_1(z)$ má stupeň nejvýše $n - 1$, proto má týž stupeň i poslední člen $\eta_{1r}'\xi_r$, tedy stupeň $\eta_{1r}'(z) < v_r g_r$ a položíme-li $\eta_{1r}' = \eta_{1r}$, je

(4) $$\sum_1^r \eta_{1i}(z)\xi_i(z) \equiv V_1(z) \ (p), \text{ stupeň } \eta_{1i} < v_i g_i.$$

Dosaďme tuto kongruenci do rozkladu $a(z)$:

$$a(z) \equiv w_1(z)^{v_1} \ldots w_r(z)^{v_r} + p\Sigma \eta_{1i}(z)\xi_i(z) \ (p^2), \text{ neboli}$$

(5) $$a(z) \equiv (w_1(z)^{v_1} + p\eta_{11}(z)) \ldots (w_r(z)^{v_r} + p\eta_{1r}(z)) \ (p^2).$$

Ukážeme, že polynomy η_{1i} jsou určeny jednoznačně (mod p). Buď tedy

(6_1) $$R_1(z) \ldots R_r(z) \equiv a(z) \ (p^2)$$

(6_2) $$R_i(z) \equiv w_i(z)^{v_i} \ (p)$$

(6_3) $$R_i(z) \in J'[z] \quad i = 1, 2, \ldots, r.$$

Polynom $R_i(z) - w_i^{v_i}(z)$ má podle (6_2) všechny koeficienty dělitelny prvočíslem p. Protože nejvyšší koeficient u obou polynomů je 1, plyne z toho, že jsou oba stejného stupně. Je proto polynom

$$\varepsilon_i(z) = \frac{R_i(z) - w_i^{v_i}(z)}{p} \text{ stupně} < v_i g_i \text{ s celými koeficienty.}$$

Protože $R_i(z) = w_i^{v_i}(z) + p\varepsilon_i(z)$, je

$$w_1(z)^{v_1} \ldots w_r(z)^{v_r} + p\Sigma\varepsilon_i(z)\xi_i(z) \equiv \Pi R_i(z) \equiv a(z) \equiv$$
$$\equiv w_1(z)^{v_1} \ldots w_r(z)^{v_r} + pV_1(z) \pmod{p^2},$$

z čehož $$\Sigma\varepsilon_i(z)\xi_i(z) \equiv V_1(z) \ (p).$$

Odečtením od (4) je $\Sigma(\eta_{1i}(z) - \varepsilon_i(z))\xi_i(z) \equiv 0 \ (p)$.

Protože však $w_i(z)^{v_i}$ dělí každé $\xi_j(z)$ kromě $\xi_i(z)$, s nímž je nesoudělné (mod p), je $w_i(z)^{v_i}/\eta_{12}(z) - \varepsilon_i(z)$ (mod p), z čehož plyne ihned $\eta_{1i}(z) - \varepsilon_i(z) \equiv 0 \ (p)$, neboť stupeň polynomu vpravo je menší než $w_i(z)^{v_i}$. Nechť nyní platí rozklad

$$(7) \quad a(z) \equiv \prod_{i=1}^{r} (w_i(z)^{v_i} + p\eta_{1i}(z) + p^2\eta_{2i}(z) + \ldots + p^{a-1}\eta_{a-1i}(z)) \pmod{p^a}$$

a nechť je stupeň $\eta_{ij}(z) < v_j g_j$ pro $1 \leqslant i \leqslant a - 1$, $1 \leqslant j \leqslant r$, a předpokládejme konečně, že označíme-li

$$w_i(z)^{v_i} + p\eta_{1i}(z) + \ldots + p^{a-1}\eta_{a-1i}(z) = P_i(z),$$

pak je již $P_i(z)$ určeno jednoznačně mod p^a.

Vezměme jako dříve již nalezené polynomy $\eta_i'(z)$, pro něž platí (1), a označme

$$(8) \quad a(z) - P_1(z)P_2(z) \ldots P_r(z) = p^a V_a(z)$$

Definujeme-li

$$\eta_i'''(z) = \eta_i'(z)V_a(z), \quad \text{platí}$$
$$(2') \quad \Sigma\eta_i'''(z)\xi_i(z) \equiv V_a(z) \pmod{p}.$$

Snížíme jako dřív stupeň u η''' pomocí vztahů $\eta_1''' = w_1(z)^{v_1}Q_1(z) + \eta_{a1}(z)$ apod., až dostaneme

$$(4') \quad \Sigma\eta_{ai}(z)\xi_i(z) \equiv V_a(z) \ (p), \text{ stupeň } \eta_{ai}(z) < v_1 g_i, \text{ a tedy}$$
$$(5') \quad a(z) \equiv \Pi(w_i(z)^{v_1} + p\eta_{1i}(z) + \ldots + p^a\eta_a(z)) \ (p^{a+1}).$$

Buď

$(6_1')$ $\quad a(z) \equiv R_1(z) \ldots R_r(z)\ (p^{a+1})$

$(6_2')$ $\quad R_i(z) \equiv w_i(z)^{v_i}\ (p)$

$(6_3')$ $\quad R_i(z) \in J'[z].$

Z $(6_1')$ plyne speciálně

$$a(z) \equiv R_1(z) \ldots R_r(z)\ (p^a),$$

a proto dává $(6_2')$ a $(6_3')$ a indukční předpoklad

$$R_i(z) \equiv P_i(z)\ (p^a), \text{ neboli, značíme-li } \frac{R_i(z) - P_i(z)}{p^a} = \varepsilon_i(z),$$

je $\varepsilon_i(z)$ celistvý polynom, o němž dá se stejně jako dřív ukázat, že je stupně menšího $v_i g_i$.

Je tedy $$R_i(z) = P_i(z) + p^a \varepsilon_i(z),$$

a tedy $$a(z) \equiv \Pi, R_i(z) \equiv \Pi P_i(z) + p^a \Sigma \varepsilon_i(z) \xi_i(z)\ (p^{a+1})$$

a z druhé strany

$$a(z) \equiv \Pi, (P_i(z) + p^a \eta_{a,i}(z)) \equiv \Pi P_i(z) + p^a \Sigma \eta_{a,i}(z) \xi_i(z).$$

Z těchto dvou rovnic již snadno ukážeme, že

$$\eta_{a,i}(z) \equiv \varepsilon_i(z)\ (p),$$

a tedy $$R_i(z) = P_i(z) + p^a \varepsilon_i(z) \equiv P_i(z) + p^a \varepsilon_i(z) \pmod{p^{a+1}},$$

což jsme chtěli ukázat.

Konstrukce prodloužení rozkladu vyložená ve větě 12,1 je numericky dosti namáhavá. Podám zde ještě jednu metodu, která je jednodušší hlavně v případech, kdy r je malé. Tato metoda mohla by též sloužit za důkaz věty 12,1.

Buď $a(z) \equiv w_1(z).w_2(z)\ (p)$, kde w_1, w_2 jsou sice nesoudělné (mod p), ne však nutně ireducibilní. Pišme

$$\begin{aligned} a(z) &= z^n + a_1 z^{n-1} + \ldots + a^n \\ w_1(z) &= z^m + v_1 z^{m-1} + \ldots + v_m \\ w_2(z) &= z^r + u_1 z^{r-1} + \ldots + u^r. \end{aligned}$$

Platí $m + r = n$, $b_k = \sum_{i=0}^{k} v_i u_{k-i} \equiv a_k\,(p)$, klademe-li $a_0 = v_0 = u_0 = 1$.

Pišme

$$\begin{aligned} P_1(z) &= z^m + (v_1 + p\lambda_1) z^{m-1} + \ldots + (v_m + p\lambda_m) \\ P_2(z) &= z^r + (u_1 + p\mu_1) z^{r-1} + \ldots + (u_r + p\mu_r), \end{aligned}$$

a počítejme

$$P_1(z) P_2(z) = z^n + z^{n-1}(u_1 + v_1 + p(\lambda_1 + \mu_1)) + \ldots +$$

$$+ z^{n-k}(u_k + u_{k-1}v_1 + v_k + p(\lambda_k + \lambda_{k-1}u_1 + \ldots + \mu_k + p^2(\ldots)) + \ldots +$$
$$+ v_m u_r + p(v_m\mu_r + u_r\lambda_m) + p^2(\lambda\mu).$$

(1) Je $$\frac{b_k - a_k}{p} = \nu_k \in J.$$

Lze tedy psát

$$P_1(z)P_2(z) \equiv z^{n-1}p(\nu_1 + \lambda_1 + \mu_1) + \ldots + pz^{n-k}(\nu_k + \lambda_k + u_1\lambda_{k-1} + \ldots +$$
$$+ u_{k-1}\lambda_1 + \ldots + \mu_1\nu_{k-1} + \ldots + \mu_{k-1}\nu_1 + \mu_k + \ldots +$$
$$+ p(\nu_m + \mu_r\nu_m + \lambda_m u_r) + a(z) \pmod{p^2}.$$

Zvolíme-li nyní čísla λ_i, μ_i tak, aby

(2) $$\nu_k + \lambda_k + u_1\lambda_{k-1} + \ldots + u_{k-1}\lambda_1 + \ldots + \mu_k \equiv 0 \ (p),$$

bude $$P_1(z)P_2(z) \equiv a(z) \bmod p^2.$$

Je však diskriminant soustavy rovný $\boldsymbol{R}(w_1,w_2)$, a tedy inkongruentní s nulou mod p. Soustava má řešení. Neřešme ji však pro ν_k určená rovnicí (1), ale považujme ν_k za neurčité. Po výpočtu teprve dosadíme a dostaneme tak rozklad mod p^2. Nahradíme získané koeficienty $v_i + p\lambda_i = v_i'$ za $v_i' + p^2\lambda_i'$ a sestavíme rovnice (2)′. Budou se od rovnice (2) lišit pouze pravými stranami a máme je tedy vypočtené. Můžeme postupovat tímto způsobem, jak daleko chceme.

Dostaneme tedy výsledkem

$$P_1^{(i)}(z)P_2^{(i)}(z) \equiv a(z) \pmod{p^i}.$$

Je podle konstrukce

$$w_1(z) \equiv P_1^{(i)}(z) \ (p) \quad \text{pro každé } i,$$
$$w_2(z) \equiv P_2^{(i)}(z) \ (p)$$

Je-li nyní $w_1(z)$ reducibilní modulo p, je

$$w_1(z) \equiv w_3(z)w_4(z) \ (p)$$

a tedy i $$w_3(z).w_4(z) \equiv P_1^{(i)}(z) \pmod{p}$$

a pokračujeme jako dřív, až dostaneme

$$P_3^{(i)}(z).P_4^{(i)}(z) \equiv P_1^{(i)}(z) \pmod{p^i},$$

tedy $$P_2^{(i)}(z)P_3^{(i)}(z)P_4^{(i)}(z) \equiv a(z) \ (p^i).$$

Poznamenejme, že tato metoda je pro velký počet ireducibilních faktorů w velmi zdlouhavá, ale nepříliš namáhavá. Mohli bychom nyní vyslovit větu 9,3 v silnější formě tak, že bychom kongruence mod p nahradili kongruencemi mod p^a pro nějaké vhodné a. Neuděláme to, protože později odvodíme ještě silnější věty. Všimneme si však hned jednoho důsledku věty 9,3.

Zvolme prvočíslo p a ptejme se, pro které polynomy $f_1(x)$, $f_2(x)$ mají J_{f_1}, J_{f_2} stejné base vzhledem k p, čímž rozumíme, že je-li $\left\langle \ldots \frac{\varphi_i(\Theta_1)}{p^{q_i}} \ldots \right\rangle$ base J_{f_1}, je $\left\langle \ldots \frac{\varphi_i(\Theta_2)}{p^{q_i}} \ldots \right\rangle$ base J_{f_2} a naopak. Je zřejmé, že k tomu je nutné, aby $f_1(x) \equiv f_2(x) \bmod p$.
(Příklad ukazuje, že tato podmínka není postačující: $x^2+1 \equiv x^2+3$ (2), ale první má basi $\langle 1, \Theta_1 \rangle$, druhá $\left\langle 1, \frac{1+\Theta_2}{2} \right\rangle$; ukáže se ale, že stačí již kongruence p^a, je-li a již dost velké.) Mají-li okruhy stejnou basi, můžeme ji hledat u toho, u něhož ji lze nalézt snadněji. To uděláme v příští kapitole.

III. ROZKLAD BASE

§13. *Stejné okruhy.*

Df 17

Buďte $f_1(x)$, $f_2(x) \in J'[x]$ dva polynomy stejného stupně n; J_{f_1}, J_{f_2} jim odpovídající okruhy a Θ_1, Θ_2 jejich generátory. Buď p prvočíslo a q přirozené číslo, $\varphi(x) \in J'[x]$. Nechť platí pro každý polynom φ stupně $< n$

$$(1) \qquad \frac{\varphi(\Theta_1)}{p^r} \in J_{f_1} \Rightarrow \frac{\varphi(\Theta_2)}{p^r} \in J_{f_2} \text{ pro každé } r \leqslant q.$$

Potom říkáme, že J_{f_1} je větší J_{f_2} vzhledem k p^q a píšeme

$$J_{f_1} > J_{f_2} (p^q).$$

Platí-li (1) pro každé r bez omezení, je přirozené psát

$$J_{f_1} > J_{f_2}(p^\infty) \quad \text{nebo prostě} \quad J_{f_1}^{(p)} > J_{f_2}^{(p)}.$$

Platí-li v (1) implikace též obráceně, je J_{f_1} stejné s J_{f_2} vzhledem k p^q a značíme

$$J_{f_1} \geqq J_{f_2} (p^q).$$

Poznamenejme, že je-li $\left\langle 1, \ldots, \frac{\varphi_{n-1}(\Theta_1)}{p^{q_{n-1}}} \right\rangle$ base $J_{f_1}^{(p)}$, pak je ovšem $J_{f_1} > J_{f_2} (p^{q_{n-1}})$ ekvivalentní s $J_{f_1} > J_{f_2} (p^\infty)$.

V 13,1

Nutná a postačující podmínka pro to, aby J_{f_1} a J_{f_2} měly stejné base vzhledem k p, je aby

$$J_{f_1} \geqq J_{f_2} (p^\infty).$$

Důkaz:

1. Nutnost je celkem jasná. Skutečně buďte

(1) $\left\langle \ldots, \frac{\varphi_i(\Theta_1)}{p^{a_i}} \ldots \right\rangle, \left\langle \ldots, \frac{\varphi_i(\Theta_2)}{p^{a_i}}, \ldots \right\rangle$ base J_{f_1} respektive J_{f_2}.

Buď $\frac{\varphi(\Theta_1)}{p^a} \in J_{f_1} \Rightarrow \frac{\varphi(\Theta_1)}{p^a} = \sum_0^{n-1} \lambda_i \frac{\varphi_i(\Theta_1)}{p^{a_i}}$. Je však $\sum \lambda_i \frac{\varphi_i(\Theta_2)}{p^a} = \frac{\varphi(\Theta_2)}{p^a} \in J_{f_2}$, tedy $J_{f_1} > J_{f_2}$ a stejně naopak.

2. Nechť nyní je $J_{f_1} \geqq J_{f_2}$ a nechť (1_1) je base J_{f_1}. Pak zřejmě pro každé $0 \leqslant i \leqslant n-1$ $\frac{\varphi_i(\Theta_2)}{p^{a_i}} \in J_{f_2}$. Buď s druhé strany $\frac{\varphi(\Theta_2)}{p^a} \in J_{f_2}$, stupeň $\varphi(x) < n$; pak ale $\frac{\varphi(\Theta_1)}{p^a} \in J_{f_1}$ a úvaha stejná jako v 1. ukáže, že $\frac{\varphi(\Theta_2)}{p^a} \in \left[\ldots \frac{\varphi_i(\Theta_2)}{p^{a_i}} \ldots \right]$, tedy $\left\langle \ldots \frac{\varphi_i(\Theta_2)}{p^{a_i}} \ldots \right\rangle$ je base.

V 13,2

Buď a přirozené číslo. Platí-li pro nějaké dva polynomy $f(x), g(x) \in J'[x]$ stejného stupně n kongruence

(1) $$f(x) \equiv g(x) \pmod{p^{an}},$$

pak je

(2) $$J_f \geqq J_g \ (p^a).$$

Důkaz:

Buď $z_2 = \frac{\varphi(\Theta_2)}{p^r}$, označme $z_1 = \frac{\varphi(\Theta_1)}{p^r}$. Buď $z_2 \in J_g^{(p)}$ a buď $r \leqslant a$. Spočteme $P_{z_1}(t)$ (viz df 5 v §3). Je, označíme-li

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n, \quad P_{p^r \cdot z_1}(t) = P'_\varphi(t, a_1, \ldots, a_n).$$

Je ovšem, je-li $g(x) = x^n + b_1 x^{n-1} + \ldots + b_n$, $P_{p^r \cdot z_2}(t) = P''_\varphi(t, b_1, \ldots, b_n)$. Avšak $b_i \equiv a_i \ (p^{an})$ $i = 1, 2, \ldots, n$, tedy

(3) $$P_{p^r \cdot z_1}(t) \equiv P_{p^r \cdot z_2}(t) \pmod{p^{an}}.$$

Protože je však $z_2 \in J_g^{(p)}$, je, zavedeme-li

$$P_{p^r z_i}(t) = t^n + \gamma_{i_1} t^{n-1} + \ldots + \gamma_{i_n} \ (i = 1, 2),$$

$$p^r / \gamma_{21}, \ p^{2r} / \gamma_{22}, \ \ldots, \ p^{nr} / \gamma_{2n},$$

a tedy vzhledem k (3) a $r \leqslant a$, je i

$$p^{ir} / \gamma_{1i} \quad i = 1, 2, \ldots, n, \quad \text{tedy} \quad z_1 \in J_f^{(p)}.$$

Ze symetrie předpokladů plyne i $z_1 \in J_f^{(p)} \Rightarrow z_2 \in J_g^{(p)}$.

V 13,3

Ve větě 13,2 není obecně možno snížit v kongruenci (1) exponent an u prvočísla p, aby platilo (2).

Důkaz:

Buď $f(x) = x^n + p^a a_1' x^{n-1} + p^{2a} a_2' x^{n-2} + \ldots + p^{na} a_n'$. Pak zřejmě $\frac{\Theta_1}{p^a} \in J_f$ a má-li platit (2), $\frac{\Theta_2}{p^a} \in J_g$, tedy koeficienty b_k polynomu $g(x)$ musí být dělitelny p^{ak}. Nestačí tedy $f(x) \equiv g(x) \pmod{p^{an-1}}$.

Poznámka 1:

Zároveň je vidět, že kongruence polynomů není vhodná relace pro tyto účely, neboť museli jsme vzít kongruenci podle tak vysoké mocniny prvočísla pouze kvůli poslednímu koeficientu.

Poznámka 2:

Prof. Petr uvádí mylně, že stačí vzít ve větě 13,2 kongruenci mod p^a (viz [1]).
Vraťme se opět k větě 13,2. Mějme pevně dán polynom $f(x)$ a volme pro různá a polynomy $g_a(x)$ tak, aby

$$f(x) \equiv g_a(x) \ (p^{an}).$$

Pak podle citované věty je speciálně $J_f > J_{g_a} \ (p^a)$. Budeme-li a zvětšovat, nastane jednou případ, že $\frac{\varphi(\Theta)}{p^a} \in J_f$ již pro žádný primitivní polynom stupně $< n$, a tedy pro toto a platí již

$$J_f > J_{g_a} \ (p^\infty) \text{ podle poznámky za větou 13,1.}$$

Věty 10,4 a 10,5 ukazují, že takové číslo a skutečně existuje, a že stačí položit

$$a > \left[\frac{Exp_p \Delta_f}{2}\right] = b.$$

(Lze také ukázat, že existují polynomy $f(x)$, pro něž je číslo b nejmenší takové, aby již $J_f > J_{g_b} \ (p^a) \Rightarrow J_f > J_{g_a} \ (p^\infty)$.
Tedy lze říci

Buď $a > b = \left[\frac{Exp_p \Delta_f}{2}\right]$, potom z $f(x) \equiv g(x) \ (p^{an})$ plyne $J_f > J_g \ (p^\infty)$. Chceme-li, aby bylo dokonce $J_f \gtrless J_g \ (p^\infty)$, stačí podle předešlého a ještě natolik zvětšit, aby platilo $a > c = \left[\frac{Exp_p \Delta_g}{2}\right]$. Tato nerovnost je však pro $n > 2$ již splněna automaticky. Všimněme si, že je-li $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$, je $\Delta f = \Sigma c_i a_1^{i_1} a_2^{i_2} \ldots a_n^{i_n}$, kde c_i jsou

nějaká celá čísla a součet se vede přes všecka $i_1, \ldots, i_n$, pro něž $\sum_{k=1}^{n} k i_k = n(n-1)$. Je tedy

$$n - 1 = \frac{i_1}{n} + \frac{2i_2}{n} + \ldots + i_n \leqslant i_1 + i_2 + \ldots + i_n.$$

Bude-li dále $g(x) = x^n + b_1 x^{n-1} + \ldots + b_n$, pak z $f(x) \equiv g(x)\ (p^a)$ plyne $a_i \equiv b_i\ (p^a)$, a tedy $\Delta_f \equiv \Delta_g\ (p^{(n-1)a})$ a je-li $n > 2$, je $\Delta_f \equiv \Delta_g\ (p^{2a})$. Je, jak bylo zvoleno, $p^{2b} | \Delta_f$, tedy $p^{2b} | \Delta_g$ a $p^{2b+2} \nmid \Delta_f$, tedy $p^{2b+2} \nmid \Delta_g$, neboť vzhledem k $a > b$ platí $2a \geqslant 2b + 2$. Tedy celkem lze říci, že $p^{2b} | \Delta g$, $p^{2(b+1)} \nmid \Delta g$, neboli $b = c$. Platí proto věta

V 13,4

Pro nějaký polynom $f(x) \in J'[x]$ stupně n a pro nějaké prvočíslo p položme

$$a = \left[\frac{Exp_p \Delta_f}{2}\right] + 1.$$

Buď $g(x) \in J'[x]$ druhý polynom takový, aby $g(x) \equiv f(x) \pmod{p^{na}}$, potom je

$$a = \left[\frac{Exp_p \Delta_g}{2}\right] + 1 \text{ a } J_f \geqslant J_g.$$

§14. *Base reducibilních okruhů.*

Buď $f(x) = g(x)h(x)$, kde f, g, h jsou stupňů n, n_1, n_2, a buďte g, h nesoudělné mod p. Dále buďte $\Theta_3, \Theta_1, \Theta_2$ resp. generátory okruhů J_f, J_g, J_h resp. Nechť jsou

$$\omega_{i+1}^{\prime(p)} = \omega_{i+1}^{\prime} = \frac{\varphi_i'(\Theta_1)}{p^{q_i}}\ 0 \leqslant i < n_1$$

Θ-base vzhledem k p okruhu J_g a

$$\omega_{i+1}^{\prime\prime(p)} = \omega_{i+1}^{\prime\prime} = \frac{\varphi_i''(\Theta_2)}{p^{s_i}}\ 0 \leqslant i < n_2\ \Theta\text{-base } J_h^{(p)}.$$

Pišme ještě $\varphi_{n_1}'(x) = g(x)$ a $\varphi_{n_2}''(x) = h(x)$.
Označme $r_{ij} = \min(q_i, s_j)$, kde $q_{n_1} = s_{n_2} = \infty$ (nebo, chceme-li, větší než q_{n_1-1}, resp. s_{n_2-1}). Dále označme

$$\omega_{i,j} = \frac{\varphi_i'(\Theta_3)\varphi_j''(\Theta_3)}{p^{r_{ij}}} \quad \begin{matrix} i = 0,1, \ldots, n_1 \\ j = 0, 1, \ldots, n_2,\ i + j \neq n \end{matrix}$$

(v posledním případě $i + j = n$ lze chápat ovšem $\omega_{n_1,n_2} = 0$.) Je

$$\omega_{ij} = \iota_2 [\omega_i' \varphi_j''(\Theta_1) p^{q_i - r_{ij}};\ \omega_j'' \varphi'(\Theta_2)\ p^{s_i - r_{ij}}].$$

Oba faktory v závorce jsou čísla celá, tedy podle V 2,2 je $\omega_{ij} \in J_f$.

Položme $r_k = \max_{i+j=k} r_{ij} = r_{k_1,k_2}$, kde k_1, k_2 jsou ty indexy, pro něž se maxima nabývá, to jest, pro něž $k_1 + k_2 = k$, $r_{k_1,k_2} = r_k$.

Položme ještě

$$\omega_{k_1 k_2} = \omega_{k+1} = \frac{\varphi'_{k_1}(\Theta)\varphi''_{k_2}(\Theta)}{p^{r_k}} = \frac{\varphi_k(\Theta)}{p^{r_k}},$$

kde jsme položili $\varphi_k(x) = \varphi'_{k_1}(x)\varphi'_{k_2}(x)$. Přitom platí $\omega_k \in J_f^{(p)}$ a

1. $\varphi_k(x) \in J'[x]$
2. stupeň $\varphi_k(x) = k$
3. $0 \leqslant r_1 \leqslant r_2 \leqslant \ldots \leqslant r_{n-1}$

Tedy $\langle \omega \rangle$ je Θ-basí vzhledem k p nějakého okruhu $K \subset J_f^{(p)}$. Spočtěme

$$\boldsymbol{D}(K) = D(\omega) = \frac{\Delta_f}{(p^{r_1}p^{r_2} \ldots p^{r_{n-1}})^2} \quad \text{jak plyne z V 6,3.}$$

Dokážeme nyní, že čísla

$$r_0, r_1, \ldots, r_{n-1} \tag{1}$$

dostaneme z čísel

$$q_0, q_1, \ldots, q_{n_1-1}, s_0, s_1, \ldots, s_{n_2-1} \tag{2}$$

tím, že tato uspořádáme podle velikosti (přičemž stejná tam dáme tolikrát, kolikrát se vyskytují v obou posloupnostech q i s). Nejprve pro technické zjednodušení dodefinujme

$$q_{-1} = s_{-1} = -1,$$

$q_{n_1+1} = q_{n_1+2} = \ldots = q_n = s_{n_2+1} = \ldots = s_n = \infty$ (nebo větší než q_{n_1-1} i s_{n_2-1}). Jakmile jsme toto určili, můžeme bez jakýchkoli omezení nalézt ke každému číslu r indexy $k_1 \geqslant -1$, $l_1 \leqslant n_1$, že platí

$$q_{k_1} < r < q_{l_1} \tag{3}$$

a indexy $k_2 \geqslant -1$, $l_2 \leqslant n_2$, pro něž analogicky

$$s_{k_2} < r < s_{l_2}. \tag{4}$$

Nyní můžeme dokázat

Lema.

1. Z nerovností $q_{k_1} < r$ a $s_{k_2} < r$ plyne $r_{k_1+k_2+1} < r$ a
2. z nerovností $r < q_{l_1}$ a $r < s_{l_2}$ plyne $r < r_{l_1+l_2}$.

Důkaz:

1. Nechť tedy

$$q_{k_1} < r \quad \text{a} \quad s_{k_2} < r, \tag{5}$$

pak pro $i = 0, 1, \ldots, k_1$ platí $q_i \leqslant q_{k_1} < r$, a tedy pro tato i $\min(q_i, s_{k_1+k_2+1-i}) < r$. Dále platí pro $i = k_1 + 1, k_1 + 2, \ldots, k_1 + k_2 + 1$, $s_{k_1+k_2+1-i} \leqslant s_{k_1+k_2+1-(k_1+1)} = s_{k_2} < r$, a tedy pro tato i $\min(q_i, s_{k_1+k_2+1-i}) < r$; čili nerovnost $\min(q_i, s_{k_1+k_2+1-i}) < r$ platí pro všechna $0 \leqslant i \leqslant k_1 + k_2 + 1$, a tedy podle definice

$$r_{k_1+k_2+1} = \max_{0 \leqslant i \leqslant k_1+k_2+1} \min(q_i, s_{k_1+k_2+1-i}) < r.$$

2. Nechť platí

(6) $$r < q_{l_1} \quad \text{a} \quad r < s_{l_2}.$$

Protože maximum z několika výrazů je alespoň tak veliké jako některý z nich, platí

$$r_{l_1+l_2} \geqslant \min(q_{l_1}, s_{l_2}) > r.$$

Tím je lema dokázáno.

Vraťme se ještě jednou k nerovnostem (3) a (4). Není-li r žádné číslo z posloupnosti (2), můžeme indexy k_1 a l_1 zvolit tak, že $l_1 = k_1 + 1$. Stejně pro index $l_2 = k_2 + 1$.
Tedy platí $(l_1 - k_1 - 1) + (l_2 - k_2 - 1) = 0$. V tomto případě lema tvrdí

$$r_{k_1+k_2+1} < r < r_{l_1+l_2} = r_{k_1+k_2+2},$$

tedy že r leží mezi dvěma sousedními členy v posloupnosti (1); jinými slovy, žádné číslo posloupnosti (1) nerovná se r.
Nyní obecně. Nechť ve (2) je právě a čísel rovných r. Pak indexy můžeme zvolit tak, že

(7) $$(l_1 - k_1 - 1) + (l_2 - k_2 - 1) = a.$$

Lema opět dá $r_{k_1+k_2+1} < r < r_{l_1+l_2} = r_{k_1+k_2+a+2}$ (použitím (7)).

Může tedy být nejvýše a čísel v posloupnosti (1) rovných r. Obě posloupnosti však mají $n = n_1 + n_2$ prvků, nemůže být tedy počet stejných čísel v posloupnosti (1) menší a je tedy stejný. První posloupnost vznikla tedy přerovnáním posloupnosti druhé. Protože (1) je monotonní, platí:
Posloupnost $r_0, r_1, \ldots, r_{n-1}$ *dostaneme z posloupnosti* $q_0, q_1, \ldots, q_{n_1-1}$, $s_0, s_1, \ldots, s_{n_2-1}$, *uspořádáme-li tato čísla podle velikosti s příslušnou násobností.*

A také platí

$$\sum_{i=0}^{n_1-1} q_i + \sum_{i=0}^{n_2-1} s_i = \sum_{i=0}^{n-1} r_i.$$

Označme $\Sigma p_i = \alpha$ a $\Sigma q_i = \beta$; je

$$D(K) = \frac{\Delta_f}{p^{2(\alpha+\beta)}}.$$

Je však podle V 7,6

$$\boldsymbol{D}(J_f^{(p)}) = \boldsymbol{D}(K),$$

tedy podle V 5,5 $J_f = K$.
Našli jsme tedy metodu, jak najít Θ-basi J_f, známe-li Θ-basi J_g a J_h, pro něž platí $f = g.h$. Větu vyslovíme trochu obecněji a spojíme ji ihned s větou 13,4.

Hlavní věta.

Buď $f(x) \in J'[x]$ polynom s jednoduchými kořeny. Buď p prvočíslo a nechť

$$p^{2\alpha_p} \mid \Delta_f, \quad p^{2(\alpha_p+1)} \nmid \Delta_f.$$

Položme $b > n\alpha_p$. Pak existuje právě jeden (ve smyslu věty 10,1) rozklad $f(x) \equiv P_1(x)P_2(x) \ldots P_s(x) \pmod{p^b}$, přičemž $P_i(x)$ jsou navzájem inkongruentní polynomy stupně n_i. Buďte

$$\left\langle \ldots, \omega_{j+1}^{(i)} = \frac{\varphi_j^{(i)}(\Theta_i)}{p^{q_j^{(i)}}} \ldots \right\rangle,$$

$j = 1, 2, \ldots, n_i$ base $J_{n_i}^{(p)}$ pro $i = 1, 2, \ldots, s$, přičemž Θ_i je generátor J_{p_i}. Položme $\varphi_{n_i}^{(i)}(x) = P_i(x)$ a $r_k = \max\limits_{\Sigma j_i = k} \min\limits_{0 \leqq i \leqq s} q_{j_i}^{(i)}$. Čísla $k_1, k_2, \ldots,$ k_s buďte taková, že $\sum\limits_1^s k_i = k$ a $r_k = \max q_{k_i}^{(i)}$. Buď Θ generátor J_f. Potom, položíme-li

$$\omega_{k+1} = \frac{\prod\limits_{i=1}^{s} \varphi_{k_i}^{(i)}(\Theta)}{p^{r_k}}, \quad k = 0, 1, \ldots, n-1, \text{ je } \langle \omega \rangle \text{ base } J_f^{(p)}.$$

Na závěr zbývá sestrojit base vzhledem k p okruhů J_{P_i}. Zde platí

Věta.

Buď $P(x) = w(x) + p\Theta(x)$, přičemž $w(x)$ je ireducibilní mod p. Buď stupeň $w(x)$ rovný m. Pak

$$\left\langle 1, \Theta, \Theta^2, \ldots, \Theta^{m-1}, \frac{\varphi_1(\Theta)}{p^{q_1}}, \Theta\,\frac{\varphi_1(\Theta)}{p^{q_1}}, \ldots, \right.$$

$$\left. \Theta^{m-1}\,\frac{\varphi_1(\Theta)}{p^{q_1}}, \frac{\varphi_2(\Theta)}{p^{q_2}}, \ldots, \Theta^{m-1}\,\frac{\varphi_{v-1}(\Theta)}{p^{q_{v-1}}} \right\rangle$$

je base $J_f^{(p)}$. Přitom zřejmě je $\varphi_i(x) \in J'[x]$ polynom stupně $m - i$.

Věta je důsledkem V 11,3.

Závěrem bych chtěl poděkovat akademiku Vladimíru Kořínkovi za jeho podněty a účinnou pomoc, kterou mi poskytl při mé práci na tomto článku.

ВЫВОДЫ

В настоящей работе, котороя исходит из работы [1], рассматриваются методы эффективного нумерического исчисления базисов целых чисел алгебраических полей.

Если мы обозначим буквой K поле рациональных чисел, буквой J область целостности целых рациональных чисел, то, как обычно разумеется, алгебраическое поле $K[\Theta]$ получится адюнкцией корня Θ уравнения

$$f(x) \equiv x^n + a_1 x^{n-1} + \ldots + a_n = 0, \ (a_i \in J).$$

Полезным оказалось изучать случай редуцибильных уравнений. В этом случае возникнет кольцо K_f, которое в дальнейшем называется кольцом алгебраических элементов. Можно доказать, что K_f является алгеброй ранга n над K и что существует элемент Θ, называемый генератором, такого вида, что каждый другой элемент из K_f возможно писать как полином над K в Θ.

Если ограничиться уравнениями только с простыми корнями, то можно определить в K_f подалгебру J_f так называемых целых элементов. Они имеют базис, это значит, что существуют целые элементы $\omega_1, \omega_2, \ldots, \omega_n$ такие, что любой целый элемент является их линейной комбинацией над J.

Можно ввести своеобразный базис, так называемый Θ-базис вида

$$\omega_1 = 1; \omega_2 = \frac{\Theta + e_{11}}{d_1} = \frac{\varphi_1(\Theta)}{d_1}, \omega_3 = \frac{\Theta^2 + e_{21}\Theta + e_{22}}{d_2} = \frac{\varphi_2(\Theta)}{d_2}, \ldots$$

Этот базис является в определенном смысле единственным. Далее можно ввести базис относительно простого числа и возможно доказать большинство теорем знакомых из теории алгебраических чисел. Оказывается даже, что почти все доказательства знакомые из теории алгебраических полей возможно перенести на алгебраические кольца. Необходимо только модифицировать понятие сопраженного числа. Это понятие непосредственно перенести нельзя.

Расширению наиболее важных теорем об этих кольцах посвящена глава I настоящей работы. Следующие главы носят уже нумерический характер. Во второй главе доказывается (теорема 9, 1), что знаменатели d_i Θ-базиса удовлетворяют соотношению

$$d_1 d_2 \ldots d_{k-1} / (\Theta_1 - \Theta_2)(\Theta_1 - \Theta_3) \ldots (\Theta_1 - \Theta_k)(\Theta_2 - \Theta_3) \ldots (\Theta_{k-1} - \Theta_k)$$

для $k = 1, 2, \ldots, n$, где Θ_i — числа сопраженные к Θ.

Далее согласно теоремы 9,2 $d_1^2 d_2^2 \ldots d_{k-1}^2$ делит каждый минор ранга k матрицы

$$\begin{Vmatrix} s_0 & s_1 & \ldots & s_{n-1} \\ s_1 & s_2 & \ldots & s_n \\ \cdot & \cdot & \cdot & \cdot \\ s_{n-1} & s_n & \ldots & s_{2n-2} \end{Vmatrix}$$

где s_i являются суммами i-тых степеней корней уравнения $f(x) = 0$. Обе теоремы очень важны для первоначальной прикладки при построении базиса.

В § 10 определены полиномы похожие на Ганкелевы полиномы. С их помощью можно во многих случаях получить базис.

Самым важным следует считать § 14, в котором доказана основная теорема

Пусть $$f(x) \equiv x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

полином с целыми коеффициентами и простыми корнями. Пусть p — простое число и α_p — такое число, что имеет место

$$p^{2\alpha_p} | \Delta_f, \quad p^{2(\alpha_p+1)} \nmid \Delta_f.$$

[Δ_f — дискриминант $f(x)$].

Если $b > n\alpha_p$, то существует следующее разложение полинома

$$f(x) \equiv P_1(x).P_2(x) \ldots P_s(x) \quad (p^b),$$

где $P_i(x)$ являются попарно простыми mod p целыми полиномами с ведущим коеффициентом равным 1.

Если выражения

$$\omega_j^i = \frac{\varphi_j^{(i)}(\Theta_i)}{p^{q_j^{(i)}}}, \; j = 1, 2, \ldots, n_i$$

являются базисами J_{P_i} относительно p для $i = 1, 2 \ldots, s$, то тогда выражения

$$\omega_k = \frac{\prod_{i=1}^{s} \varphi_{k_i}^{(i)}(\Theta)}{p^{r_k}}, \; k = 0, 1, \ldots, n-1,$$

где Θ — генератор J_f, $r_k = \max\limits_{\sum i_i = k} \min\limits_{0 \leqslant i \leqslant s} q_{j_i}^{(i)}$, являются базисом J_f.

ZUSAMMENFASSUNG

In der vorliegenden Arbeit, die sich der Arbeit [1] anknüpft werden Methoden zur effektiven numerischen Berechnung von Basen ganzer Zahlen algebraischer Körper angegeben.

Wir bezeichnen K den Körper der rationalen Zahlen, J den Integritätsbereich der ganzen rationalen Zahlen. Dann erhalten wir den algebraischen Körper $K[\Theta]$ wie üblich durch Adjunktion der Wurzel Θ der irreduziblen Gleichung

$$f(x) \equiv x^n + a_1 x^{n-1} + \ldots + a_n = 0, \; (a_i \in J).$$

Es zeigt sich als vorteilhaft, auch den Fall von reduziblen Gleichungen zu untersuchen. In diesem Falle entsteht der Ring K_f, der im weiteren Ring der algebraischen Elemente genannt wird.
Wenn wir uns auf Gleichungen mit ausschliesslich einfachen Wurzeln beschränken, ist es möglich, in K_f die Teilmenge J_f der sogenannten ganzen Elemente einzuführen. Man kann beweisen, dass ein Element Θ, ein sogenannter Generator existiert, solcherart, dass sich alle Elemente aus J_f als Polynome in Θ über K schreiben lassen. Diese Elemente bilden eine Algebra vom Range n über J und haben eine Basis, d. h. es existieren ganze Elemente $\omega_1, \omega_2, \ldots, \omega_n$, so dass jedes ganze Element eine ganzzahlige lineare Kombination dieser Elemente ist.
Es ist möglich, eine spezielle Basis, die sogenannte Θ-Basis der Form

$$\omega_1 = 1,\ \omega_2 = \frac{\Theta + e_{11}}{d_1} = \frac{\varphi_1(\Theta)}{d_1},\ \omega_3 = \frac{\Theta^2 + e_{21}\Theta + e_{22}}{d_2} = \frac{\varphi_2(\Theta)}{d_2}, \ldots$$

einzuführen, die in einem bestimmten Sinne die einzige ist. Weiter kann man eine Basis im Bezug auf eine Primzahl einführen und die Mehrzahl der Sätze beweisen, die aus der Theorie der algebraischen Zahlen bekannt sind. Es zeigt sich sogar, daß praktisch alle Beweise der Theorie der algebraischen Körper auf die algebraischen Ringe übertragbar sind; es ist nur nötig den Begriff der konjugierten Zahl zu modifizieren, der nicht unmittelbar übertragbar ist.
Mit der Entwicklung der wichtigsten Sätze über diese Ringe befaßt sich das Kapitel I.
In Kapitel II ist bewiesen (Satz 9,1), daß die Nenner d_i der Θ-Basis der Bedingung

$$d_1 d_2 \ldots d_{k-1} / (\Theta_1 - \Theta_2)(\Theta_1 - \Theta_3) \ldots (\Theta_1 - \Theta_k)(\Theta_2 - \Theta_3) \ldots (\Theta_{k-1} - \Theta_k),$$
$$k = 1, 2, \ldots, n$$

genügen, wo Θ_i zu Θ konjugierte Zahlen sind. Weiter behauptet Satz 9,2, daß $d_1^2 d_2^2 \ldots d_{k-1}^2$ jeden Minor vom Range k der Matrix

$$\begin{Vmatrix} s_0 & s_1 & \ldots & s_{n-1} \\ s_1 & s_2 & \ldots & s_n \\ \cdot & \cdot & \cdot & \cdot \\ s_{n-1} & s_n & \ldots & s_{2n-2} \end{Vmatrix}$$

teilt, wo s_i die Summen der n-ten Potenzen der Wurzeln der Gleichung $f(x) = 0$ sind. Beide Sätze sind für die Konstruktion der Basis von Wichtigkeit.
In §10 werden den Hankelschen Polynomen ähnliche Polynome eingeführt, die in vielen Fällen die Basis angeben. In § 11 werden die Sätze über

$$\varphi_i(x) / f(x) \mod \frac{d_i}{d_{i-1}}$$

verstärkt.

Die wichtigsten Ergebnisse sind im § 14 enthaltn wo der Hauptsatz bewiesen ist: Es sei $f(x) \equiv x^n + a_1 x^{n-1} + \ldots + a_n = 0$ ein ganzzahliges Polynom mit

lauter einfachen Wurzeln. Weiter sei p eine Primzahl und α_p eine solche Zahl, daß

$$p^{2\alpha_p} \mid \Delta_f, \quad p^{2(\alpha_p+1)} \nmid \Delta_f$$

(Δ_f ist der Diskriminant $f(x)$). Wenn $b > n\alpha_p$ besteht, so existiert eine Zerlegung $f(x) \equiv P_1(x)P_2(x) \ldots P_s(x)$ (p^b), wobei $P_i(x)$ inkongruente ganzzahlige Polynome mit dem ersten Koeffizient $= 1$ sind. Wenn

$$\omega_j^i = \frac{\varphi_j^{(i)}(\Theta_i)}{p^{q_j^{(i)}}}, \quad j = 1, 2, \ldots, n_i,$$

Basen von J_{P_i} in Beziehung zu p für $i = 1, 2, \ldots, s$ sind, so ist

$$\omega_k = \frac{\prod_{i=1}^{s} \varphi_{k_i}^{(i)}(\Theta)}{p^{r_k}}, \quad k = 0, 1, \ldots, n-1$$

eine Basis von J_f (wo Θ der Generator J_f ist und $r_k = \max_{\Sigma j_i = k} \min_{0 \leqslant i \leqslant s} q_{j_i}^{(i)}$).

LITERATURA

[1] KAREL PETR: O basi celých čísel v obecných tělesech algebraických. Časopis pro pěstování matematiky a fysiky, (část vědecká) *64* (1934—35), 62—72.
[2] W. E. H. BERWICK: Integral Bases, (Cambridge University Press 1927).
[3] DICKSON: Modern Algebraic Theories, (Chicago 1926).