Алгебра и логика, 50, № 6 (2011), 701—706

УДК 512.623.4

ОБОБЩЕНИЯ ЛЕММЫ ГЕНЗЕЛЯ И МЕТОД БЛИЖАЙШЕГО КОРНЯ*)

Ю. Л. ЕРШОВ

Лемма Гензеля и её различные модификации, такие, напр., как теорема Гензеля–Рихлика (см. [1]), являются важными средствами исследования проблем существования корней многочленов нормированных полей. В последнее время появился ряд работ [2, 3], в которых указаны дальнейшие расширения леммы Гензеля. В настоящей работе будет показано, что метод, предложенный в работах автора [4, 5], может быть использован и для более простого получения результатов из [3].

Все необходимые сведения о (гензелевых) нормированных полях см. в [1, гл. 1].

Пусть $\mathbb{F} = \langle F, R\rangle$ — нормированное поле, $\tilde{F}$ — алгебраическое замыкание поля F; $\tilde{R}$ — кольцо нормирования поля $\tilde{F}$, доминирующее R ($\tilde{R} \cap F = R$); $\tilde{\mathbb{F}} \rightleftharpoons \langle \tilde{F}, \tilde{R}\rangle \geq \mathbb{F}$ — расширение нормированных полей; $\mathbb{H}_R(F) = \langle H_R(F), H(R)\rangle$ $(\leq \tilde{\mathbb{F}})$ — гензелизация нормированного поля $\mathbb{F}$.

Пусть $\mathbb{F}' \geq \tilde{\mathbb{F}}$ — некоторое расширение нормированных полей, $\mathbb{F}' = \langle F', R'\rangle$. Через v будем всюду ниже обозначать $v_{R'}$, а через $\tilde{v}$ будем обозначать $v_{\tilde{R}}$; $f \in F[x]$ — унитарный многочлен, $a \in F'$. Обозначим через $\mu_f(a)$ один из корней многочлена f в поле $\tilde{F}$, такой что $v_{R'}(a-\mu_f(a)) \geq v_{R'}(a-\alpha)$ для любого корня α многочлена f в $\tilde{F}$. Назовём $\mu_f(a)$ *ближайшим* к элементу корнем многочлена. Элемент $v_{R'}(a-\mu_f(a))$ группы $\Gamma_{R'}$ обозначим через $\varepsilon_f(a)$.

ЗАМЕЧАНИЕ. Ближайших к a корней может быть несколько, но $\varepsilon_f(a)$ определено однозначно.

*)Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект № 11-01-00688-а.

ОСНОВНАЯ ЛЕММА. *Для любого корня α многочлена f справедливо равенство $v(a-\alpha)=\min\{\varepsilon_f, v(\mu_f(a)-\alpha)\}$.*

Действительно, $v(a-\alpha)=v(a-\mu_f(a)+\mu_f(a)-\alpha)$. Если $v(a-\mu_f(a))\neq$ $\neq v(\mu_f(a)-\alpha)$, то $v(a-\alpha)=\min\{v(a-\mu_f(a)), v(\mu_f(a)-\alpha)\}=\min\{\varepsilon_f,$ $v(\mu_f(a)-\alpha)\}$, т. к. $v(a-\mu_f(a))=\varepsilon_f$. Если $v(\mu_f(a)-\alpha)=v(a-\mu_f(a))=\varepsilon_f$, то $v(a-\alpha)\geq\varepsilon_f$; но $\varepsilon_f=v(a-\mu_f(a))\geq v(a-\alpha)$ (по определению $\mu_f(a)$), следовательно, в этом случае $v(a-\alpha)=\varepsilon_f=\min\{\varepsilon_f, v(\mu_f(a)-\alpha)\}$. □

Для любых нормирования $v: F'\to\Gamma'\cup\{\omega\}$ некоторого поля F' и $\gamma'\in\Gamma'$ через $v_{\gamma'}$ обозначим отображение из F' в Γ', такое что $v_{\gamma'}(a')\rightleftharpoons$ $\rightleftharpoons\min\{\gamma', v(a')\}$. Тогда основную лемму можно переформулировать так:

для любого корня α многочлена f справедливо равенство $v(a-\alpha)=$ $=v_{\varepsilon_f}(\mu_f(a)-\alpha)$.

Основная лемма является ключевым элементом доказательства следующего предложения.

ПРЕДЛОЖЕНИЕ [4, предлож. П1]. *Пусть $f\in F[x]$ — унитарный многочлен, $a\in F$, тогда*

a) имеют место неравенства $vf(a)\leq v(a-\mu_f(a))+vf'(\mu_f(a))$, $v(f(a))\leq v(a-\mu_f(a))+vf'(a)$;

b) если $\mu_f(a)$ единственный, т. е. $f'(\mu_f(a))\neq 0$ и $v(a-\alpha')<v(a-$ $-\mu_f(a))$ для любого корня α' многочлена f, отличного от $\mu(a)$, то $\alpha\in$ $\in H_R(F)$ и имеют место равенства $vf(a)=v(a-\mu_f(a))+vf'(a)$, $vf'(a)=$ $=vf'(\mu_f(a))$.

Пусть $f\in R[x]$ — унитарный многочлен, $\alpha\in\tilde F$ — корень многочлена f. Полагаем

$$\varkappa_{f,\alpha}\rightleftharpoons\begin{cases}\omega, \text{ если } f'(\alpha)=0 \text{ (т. е. } \alpha - \text{ кратный корень } f),\\ \max\{v(\alpha-\alpha')\mid \alpha'\in\tilde F, f(\alpha')=0, \alpha'\neq\alpha\}, \text{ если } f'(\alpha)\neq 0;\end{cases}$$

$\sigma_{f,\alpha}\rightleftharpoons\varkappa_{f,\alpha}+vf'(\alpha)$, $\varkappa_f\rightleftharpoons\max\{\varkappa_{f,\alpha}\mid\alpha\in\tilde F, f(\alpha)=0\}$; $\sigma_f\rightleftharpoons\max\{\sigma_{f,\alpha}\mid$ $\alpha\in\tilde F, f(\alpha)=0\}$. Константа σ_f называется *сепарантом* многочлена f, [2].

Из предложения вытекает следующий вариант леммы Гензеля (см. [5]).

ТЕОРЕМА. *Пусть $\mathbb{F}$ гензелево, $f \in F[x]$ — унитарный сепарабельный многочлен, $a \in F$ и $vf(a) > \sigma_f$. Тогда существует единственный корень α многочлена f, такой что $\alpha \in F$ и $v(a-\alpha) = vf(\alpha) - vf'(\alpha) > \varkappa_{f,\alpha}$.*

ЗАМЕЧАНИЕ. Если $\mathbb{F}$ — гензелево, а унитарный многочлен f неприводим над F, то для любых корней α, α' многочлена f справедливы равенства $\varkappa_{f,\alpha} = \varkappa_{f,\alpha'} = \varkappa_f$ и $\sigma_{f,\alpha} = \sigma_{f,\alpha'} = \sigma_f$.

Для любых многочлена

$$g = \prod_{i \leqslant n} (x - \beta_i) \in F'[x], \quad \beta_i \in F', \quad i \leqslant n,$$

и элемента $b \in F'$ *функция Бринка* $B_{g,b} : \Gamma' \to \Gamma'$ определяется правилом

$$B_{g,b}(\gamma) \rightleftharpoons \sum_{i \leqslant n} v_\gamma(b - \beta_i).$$

Справедливо такое важное следствие основной леммы.

СЛЕДСТВИЕ 1. *Для любых унитарного многочлена $f \in F[x]$ и элемента $a \in F'$ справедливо равенство*

$$vf(a) = B_{f,\mu_f(a)}(\varepsilon_f(a)).$$

СЛЕДСТВИЕ 2. *Если $\mathbb{F}$ гензелево, унитарный многочлен $f \in F[x]$ неприводим, для $a \in F$ справедливо $\varepsilon_f(a) \geq \varkappa_f (\varepsilon_f(a) = \varkappa_f)$, то $vf(a) \geq \geq \sigma_f (vf(a) = \sigma_f)$.*

Действительно,

$$f(a) = (a - \mu_f(a)) \cdot \prod_{\substack{f(\alpha)=0 \\ \alpha \neq \mu_f(a)}} (a - \alpha)$$

и

$$vf(a) = v(a - \mu_f(a)) + \sum_{\substack{f(\alpha)=0 \\ \alpha \neq \mu_f(a)}} v(a - \alpha);$$

с другой стороны, $v(a-\alpha) = v_{\varepsilon_f}(\mu_f(a) - \alpha) = v(\mu_f(a) - \alpha)$, т. к. $\varepsilon_f \geq \varkappa_f \geq \geq v(\mu_f(a) - \alpha)$ и

$$\sum_{\substack{f(\alpha)=0 \\ \alpha \neq \mu_f(a)}} v(a - \alpha) = \sum_{\substack{f(\alpha)=0 \\ \alpha \neq \mu_f(a)}} v(\mu_f(a) - \alpha) = vf'(\mu_f(a)).$$

Имеем $vf(a) = v(a - \mu_f(a)) + vf'(\mu_f(a)) = \varepsilon_f(a) + vf'(\mu_f(a)) \geq \geq \varkappa_{f,\mu_f(a)} + vf'(\mu_f(a)) = \sigma_{f,\mu_f(a)} = \sigma_f$. $\square$

Из определения функции Бринка $B_{f,a}$ легко следуют такие её свойства:

i) *функция* $B_{f,a}$ *монотонна*;

ii) *если* a *является корнем многочлена* f, *то* $B_{f,a}$ *строго монотонна.*

Действительно, пусть

$$f = \prod_{i<n}(x - \alpha_i), \quad \gamma_0 \leq \gamma_1 \in \Gamma_{R'}.$$

Тогда $v_{\gamma_0}(a - \alpha_i) = \min\{\gamma_0, v(a - \alpha_i)\} \leq \min\{\gamma_1, v(a - \alpha_i)\} = v_{\gamma_1}(a - \alpha_i)$ и

$$B_{f,a}(\gamma_0) = \sum_{i \leqslant n} v_{\gamma_0}(a - \alpha_i) \leq \sum v_{\gamma_1}(a - \alpha_i) = B_{f,a}(\gamma_1).$$

Если же $a = \alpha_{i_0}$ для некоторого i_0 и $\gamma_0 < \gamma_1$, то $v_{\gamma_0}(a - \alpha_{i_0}) = \gamma_0 < \gamma_1 = = v_{\gamma_1}(a - \alpha_{i_0})$.

ТЕОРЕМА 1. *Пусть* $f \in F[x]$ — *унитарный многочлен,* $a_0, a_1 \in \tilde{F}$, *тогда* $vf(a_0) \geq vf(a_1)$ $(vf(a_0) > vf(a_1))$ *влечёт* $\varepsilon_f(a_0) \geq \varepsilon_f(a_1)$ $(\varepsilon_f(a_0) > > \varepsilon_f(a_1))$ *в любом из следующих случаев*:

i) $\mu_f(a_0) = \mu_f(a_1)$;

ii) *многочлен* f *неприводим, а нормированное поле* $\mathbb{F}$ *является гензелевым.*

Пусть $\mu_f(a_0) = \mu_1(a_1)$; по следствию 1 имеем $vf(a_0) = = B_{f,\mu_f(a_0)}(\varepsilon_f(a_0))$, $vf(a_1) = B_{f,\mu_f(a_1)}(\varepsilon_f(a_1))$. В этом случае заключение теоремы следует из отмеченных выше свойств монотонности функции Бринка.

Пусть $\mathbb{F}$ гензелево и f неприводим. Поскольку $\mu_f(a_0)$ и $\mu_f(a_1)$ являются корнями многочлена f, существует F-автоморфизм σ поля $\tilde{F}$, такой что $\sigma\mu_f(a_0) = \mu_f(a_1)$. В силу определений можно считать, что $\mu_f(\sigma(a_0)) = \sigma\mu_f(a_0)$. Тогда $\sigma(a_0)$ и a_1 удовлетворяет условию „i“, следовательно, $vf(\sigma(a_0)) \geq vf(a_1)$ $(vf(\sigma(a_0)) > vf(a_1))$ влечёт $\varepsilon_f(a_0) \geq \geq \varepsilon_f(a_1)$ $(\varepsilon_f(a_0) > \varepsilon_1(a_1))$.

Остаётся заметить: поле $\mathbb{F}$ гензелево, поэтому $vf(\sigma a_0) = v\sigma f(a_0) = = vf(a_0)$ и $\varepsilon_f(\sigma a_0) = \varepsilon_f(a_0)$. $\square$

Алгебра и логика, 53, № 6 (2014), 704—709

УДК 512.623.4

СЕПАРАНТ ПРОИЗВОЛЬНОГО МНОГОЧЛЕНА*)

Ю. Л. ЕРШОВ

Все необходимые определения и сведения о нормированных полях содержатся в книге [1].

Пусть $\mathbb{F} = \langle F, R\rangle$ — нормированное поле, $\mathbb{F}_0 = \langle F_0, R_0\rangle \geqslant \mathbb{F}$ — алгебраически замкнутое нормированное расширение.

Пусть $f = x^n + a_1x^{n-1} + \ldots + a_n$ — унитарный многочлен над F ($f \in F[x]$), $f = \prod\limits_{i<n}(x - \alpha_i)$ — разложение f над F_0 на линейные множители. В работе [2] было определено понятие сепаранта многочлена f в случае, когда f не имеет кратных корней. Понятие сепаранта оказалось весьма полезным для обобщений леммы Гензеля [2–5]. В настоящей работе предлагается обобщение этого понятия и на случай, когда многочлен может иметь кратные корни. Это позволяет расширить лемму Гензеля и на этот случай.

Пусть $\alpha \in \{\alpha_0, \ldots, \alpha_{n-1}\}$ — корень многочлена f. *Локальной* (в α) *константой Краснера* будем называть следующий элемент группы Γ_{R_0}:

$$\varkappa_{f,\alpha} = \max\{v_{R_0}(\alpha - \alpha_i) \mid i < n,\, \alpha_i \neq \alpha\}.$$

Пусть $k_{f,\alpha}$ — кратность корня α многочлена f (т. е. $(x-\alpha)^{k_{f,\alpha}} \mid f$, но $(x-\alpha)^{k_{f,\alpha}+1} \nmid f$). Полагаем

$$\delta_\alpha(f) = \prod_{i<n,\, \alpha_i\neq\alpha}(\alpha - \alpha_i).$$

*)Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект № 15-01-05114а.

Если $k_{f,\alpha} = 1$ (т. е. α — простой корень f), то $\delta_\alpha(f) = f'(\alpha)$.

Локальным (в α) *сепарантом* многочлена f назовём элемент

$$\sigma_{f,\alpha} = k_{f,\alpha}\varkappa_{f,\alpha} + v_{R_0}\delta_\alpha(f).$$

ЗАМЕЧАНИЕ 1. Справедливо равенство

$$\sigma_{f,\alpha} = B_{f,\alpha}(\varkappa_{f,\alpha}),$$

где $B_{f,\alpha}$ — функция Бринка, определенная, напр., в [5, 6].

Действительно, $B_{f,\alpha}(\gamma) = \sum\limits_{i<n} v_\gamma(\alpha - \alpha_i)$, где $v_\gamma(\alpha) \rightleftharpoons \min\{v_{R_0}(\alpha), \gamma\}$. Имеем $v_{\varkappa_{f,\alpha}}(\alpha - \alpha_i) = \varkappa_{f,\alpha}$, если $\alpha_i = \alpha$, и $v_{\varkappa_{f,\alpha}}(\alpha - \alpha_i) = v_{R_0}(\alpha - \alpha_i)$, если $\alpha_i \neq \alpha$, т. к. $v_{R_0}(\alpha - \alpha_i) \leqslant \varkappa_{f,\alpha}$ и

$$B_{f,\alpha}(\varkappa_{f,\alpha}) = k_{f,\alpha}\varkappa_{f,\alpha} + \sum_{i<n,\, \alpha_i\neq\alpha} v_{R_0}(\alpha - \alpha_i) = k_{f,\alpha}\varkappa_{f,\alpha} + v_{R_0}\delta_\alpha(f) = \sigma_{f,\alpha}.$$

Сепарантом многочлена f будем называть элемент

$$\sigma_f = \max\{\sigma_{f,\alpha_i} \mid i < n\}.$$

ЗАМЕЧАНИЕ 2. Если $\mathbb{F}$ гензелев, а многочлен f неприводим над F, то для любых корней $\alpha, \alpha' \in \tilde{F}$ многочлена F имеет место $\varkappa_{f,\alpha} = \varkappa_{f,\alpha'}, \sigma_{f,\alpha} = \sigma_{f,\alpha'}$ и $\varkappa_f = \varkappa_{f,\alpha}$, $\sigma_f = \sigma_{f,\alpha}$.

Пусть $a \in F_0$; *ближайшим* к a корнем многочлена f назовём $\alpha \in \{\alpha_0, \ldots, \alpha_{n-1}\}$, такой что

$$v_{R_0}(a - \alpha) = \max\{v_{R_0}(a - \alpha_i) \mid i < n\}.$$

Укажем на связь константы Краснера с этим понятием.

ПРЕДЛОЖЕНИЕ 1. *Пусть $a \in F_0$, α — корень многочлена f. Если $v_{R_0}(a - \alpha) > \varkappa_{f,\alpha}$, то α — единственный ближайший к a корень многочлена f.*

Действительно, предположим, что $v_{R_0}(a - \alpha_i) \geqslant v_{R_0}(a - \alpha)$ для некоторого $i < n$, такого что $\alpha_i \neq \alpha$. Оценим норму разности $\alpha - \alpha_i$: $v_{R_0}(\alpha - \alpha_i) = v_{R_0}(\alpha - a + a - \alpha_i) \geqslant \min\{v_{R_0}(a - \alpha), v_{R_0}(a - \alpha_i)\} = v_{R_0}(a - \alpha) >$

$> \varkappa_{f,\alpha} = \max\{v_{R_0}(a-\alpha_i) \mid j < n,\ \alpha_i \neq \alpha\}$. Полученное противоречие завершает доказательство предложения. □

Укажем справедливость следующей формы известной леммы Краснера.

ПРЕДЛОЖЕНИЕ 2 [7, теор. 4.1.7]. *Пусть $a \in F_0$, α — корень многочлена f, такой что $v_{R_0}(a-\alpha) > \varkappa_{f,\alpha}$. Тогда α является чисто несепарабельным над гензелизацией $H_{R_1}(F(a))$ поля $F(a)$ в $\mathbb{F}_0$, где $R_1 = R_0 \cap F(a))$.*

Основным результатом работы является

ТЕОРЕМА 1. *Пусть $a \in F_0$, α — ближайший к a корень f. Тогда*

1) $v_{R_0}(a-\alpha) \geqslant \frac{1}{k_{f,\alpha}}(v_{R_0}f(a) - v_{R_0}\delta_\alpha(f))$;

2) *если $v_{R_0}(a-\alpha) > \varkappa_{f,\alpha}$, то $v_{R_0}f(a) = k_{f,\alpha}v(a-\alpha) + v_{R_0}\delta_\alpha(f)$.*

ДОКАЗАТЕЛЬСТВО. 1) Имеем

$$\begin{aligned} v_{R_0}f(a) &= v_{R_0}\left(\prod_{i<n}(a-\alpha_i)\right) \\ &= v_{R_0}\left(\prod_{i<n,\,\alpha_i=\alpha}(a-\alpha_i)\right) + v_{R_0}\left(\prod_{i<n,\,\alpha_i\neq\alpha}(a-\alpha_i)\right) \\ &= k_{f,\alpha}v_{R_0}(a-\alpha) + v_{R_0}\left(\prod_{i<n,\,\alpha_i\neq\alpha}(a-\alpha)\right). \end{aligned}$$

ЛЕММА 1. *Если $\alpha_i \neq \alpha$, то $v_{R_0}(a-\alpha_i) \leqslant v_{R_0}(\alpha-\alpha_i)$.*

Действительно,

$$v_{R_0}(\alpha-\alpha_i) = v_{R_0}(\alpha-a+a-\alpha_i) \geqslant \min\{v_{R_0}(a-\alpha), v_{R_0}(a-\alpha_i)\} = v_{R_0}(a-\alpha_i)$$

(напомним, что α — ближайший к a корень). □

Тогда

$$v_{R_0}\left(\prod_{i<n,\,\alpha_i\neq\alpha}(a-\alpha_i)\right) \leqslant v_{R_0}\left(\prod_{i<n,\,\alpha_i\neq\alpha}(\alpha-\alpha_i)\right) = v_{R_0}\delta_\alpha(f).$$

Итак, $v_{R_0}(f(a)) \leqslant k_{f,\alpha}v_{R_0}(a-\alpha) + v_{R_0}\delta_\alpha(f)$ и

$$v_{R_0}(a-\alpha) \geqslant \frac{1}{k_{f,\alpha}}(v_{R_0}f(a) - v_{R_0}\delta_\alpha(f)).$$

Алгебра и логика, 54, № 2 (2015), 236—242

DOI: 10.17377/alglog.2015.54.206 УДК 512.623.4

КАК НАХОДИТЬ (ВЫЧИСЛЯТЬ) СЕПАРАНТ*)

Ю. Л. ЕРШОВ

Для произвольного (унитарного) многочлена f над нормированным полем $\mathbb{F} = \langle F, R\rangle$ (все необходимые сведения и обозначения о нормированных полях см. в [1]) в [2] был определён сепарант σ_f этого многочлена как элемент группы нормирования Γ_{R_0} для любого алгебраически замкнутого расширения $\mathbb{F}_0 = \langle F_0, R_0\rangle \geqslant \mathbb{F}$ следующим образом.

Пусть $f = \prod\limits_{i<n}(x-\alpha_i)$ — разложение f над F_0 на линейные множители; для $i < n$ локальная (в α_i) константа Краснера $\varkappa_{f,\alpha_i}$ определяется по правилу

$$\varkappa_{f,\alpha_i} \rightleftharpoons \max\{v_{R_0}(\alpha_i - \alpha_j) \mid j < n, \alpha_j \neq \alpha_i\}.$$

Полагая

$$\delta_{\alpha_i}(f) \rightleftharpoons \prod_{\substack{j<n\\(\alpha_j\neq\alpha_i)}} (\alpha_i - \alpha_j),$$

определяем локальный (в α_i) сепарант

$$\sigma_{f,\alpha_i} \rightleftharpoons k_{f,\alpha_i}\varkappa_{f,\alpha_i} + v_{R_0}\delta_{\alpha_i}(f),$$

где k_{f,α_i} — кратность корня α_i многочлена f.

Наконец, сепарант σ_f определим как $\max\limits_{i<n}\sigma_{f,\alpha_i}$.

Сепарант используется для получения следующего обобщения леммы Гензеля.

*)Настоящая работа выполнена во время пребывания автора в университете Сан-Пауло (Бразилия). Автор выражает свою благодарность И. П. Шестакову и фонду FAPESP, grant 2014/23645-0, за возможность этой поездки.

ТЕОРЕМА 1 [2, след. 2]**.** *Для $a \in F_0$, если $v_{R_0} f(a) > \sigma_f$, существует (единственное) α_i, $i < n$, такое что $v_{R_0}(a - \alpha_i) > \varkappa_{f,\alpha_i}$.*

Как показано в [2, след. 3], константа σ_f в условиях теоремы 1 не улучшаема.

Следующая теорема является хорошей версией теоремы о непрерывности корней многочленов для случая многочленов с кратными корнями.

ТЕОРЕМА 2 [2, теор. 3]**.** *Пусть $f, g \in R[x]$ — унитарные многочлены одной и той же степени n,*

$$f = \prod_{i<n} (x - \alpha_i) \ -$$

разложение f на линейные множители над F_0. Если $v_{R_0}(f - g) > \sigma_f$, то существует разложение

$$g = \prod_{i<n} (x - \beta_i),$$

такое что $v_{R_0}(\alpha_i - \beta_i) > \sigma_{f,\alpha_i}$, $i < n$.

В ряде работ [2–6] были найдены сепаранты многочленов для некоторых важных (интересных) классов многочленов.

Используя понятия конструктивной [7] или (эквивалентно) вычислимой [7, 8] модели, нетрудно понять, что в случае, когда поле $\mathbb{F}_0$ конструктивно, само определение сепаранта σ_f даёт способ его вычисления (по многочлену f эффективно находятся (перебором) его корни $\alpha_0, \ldots, \alpha_{n-1}$ и т. д.).

В настоящей работе будет указан более алгебраический способ нахождения сепаранта.

Рассмотрим сначала случай, когда многочлен f не имеет кратных корней. В этом случае

$$\delta_{\alpha_i}(f) = f'(\alpha_i), \ k_{f,\alpha_i} = 1, \ i < n.$$

Рассмотрим многочлен

$$\Sigma_f \rightleftharpoons \prod_{\substack{i<n \\ j<n}} (x - (\alpha_i - \alpha_j) f'(\alpha_i)).$$

Нетрудно понять, что справедливо следующее

ЗАМЕЧАНИЕ 1. Сепарант σ_f равен максимуму норм не нулевых корней многочлена Σ_f.

Действительно, если $\alpha_j \neq \alpha_i$, то $v_{R_0}(\alpha_j - \alpha_i) \leqslant \varkappa_{f,\alpha_i}$ и

$$\begin{aligned} v_{R_0}((\alpha_i - \alpha_j)f'(\alpha_i)) &= v_{R_0}(\alpha_i - \alpha_j) + v_{R_0} f'(\alpha_i) \\ &\leqslant \varkappa_{f,\alpha_i} + v_{R_0}\delta_{\alpha_i}(f) = \sigma_{f,\alpha_i}. \end{aligned}$$

Если же $\sigma_f = \sigma_{f,\alpha_i}$ и $j < n$ таково, что $v_{R_0}(\alpha_i - \alpha_j) = \varkappa_{f,\alpha_i}$, то

$$v_{R_0}((\alpha_i - \alpha_j)f'(\alpha_i)) = \varkappa_{f,\alpha_i} + v_{R_0} f'(\alpha_i) = \sigma_{f,\alpha_i} = \sigma_f. \ \square$$

Коэффициенты многочлена Σ_f являются симметрическими функциями от α_i, $i < n$, поэтому $\Sigma_f \in F[x]$. Нахождение коэффициентов Σ_f может быть осуществлено с помощью результантов (см. [8]). Рассмотрим результанты

$$\mathrm{Res}_y(f(y), x - (y - z)f'(y)) = \prod_{i<n}(x - (\alpha_i - z)f'(\alpha_i))$$

и

$$\mathrm{Res}_z\left(f(z), \prod_{i<n}(x - (\alpha_i - z)f'(\alpha_i)\right) = \prod_{j<n}\prod_{i<n}(x - (\alpha_i - \alpha_j)f'(\alpha_i)) = Z_f.$$

В [9, теор. 1] показано, как можно эффективно найти нормы всех корней многочлена Z_f. Вычисление результантов (напр., с помощью матрицы Сильвестра, см. [8]) эффективно, поэтому можно считать, что проблема нахождения сепаранта многочлена без кратных корней решается эффективно.

Обратимся теперь к общему случаю. Нам понадобится следующее алгебраическое наблюдение.

ЛЕММА 1. *Пусть F совершенно, $l \leq n$ таково, что $\alpha_0, \ldots, \alpha_{l-1}$ — это все различные корни многочлена f, $k \leq n$,*

$$f_k \rightleftharpoons \prod_{\substack{i<l \\ k_{f,\alpha_i}=k}} (x - \alpha_i).$$

ДОКЛАДЫ АКАДЕМИИ НАУК, 2007, том 417, № 5, с. 1–3

МАТЕМАТИКА

УДК 512.52

ТЕОРЕМА О НОРМАХ КОРНЕЙ И КОЭФФИЦИЕНТОВ

© 2007 г. Академик Ю. Л. Ершов

Поступило 15.08.2007 г.

В работе автора [1] была установлена полезная лемма (воспроизведенная в книге [2, лемма 1.2.3], лемма о нормах корней и коэффициентов), показывающая, что знание норм коэффициентов многочлена над нормированным полем дает важную информацию о нормах корней этого многочлена. Оказывается (теорема 1), что знание норм коэффициентов дает полную информацию о нормах коней. Теорема 2 показывает "непрерывность" этой зависимости.

Пусть $\mathbb{F} = \langle F, R\rangle$ – нормированное поле,

$$f = \prod_{i<n}(x-\alpha_i) = x^n + a_1x^{n-1} + \ldots + a_n \in F[x]$$

есть унитарный многочлен над F (имеющий все корни в F). Предположим, что корни $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ многочлена f занумерованы так, что $v_R(\alpha_0) \le \le v_R(\alpha_1) \le \ldots \le v_R(\alpha_{n-1})$. Пусть $k_0 \rightleftharpoons 0 < k_1 < \ldots < < k_s \rightleftharpoons n$ таковы, что для любого $0 \le i < s$ справедливо $v_R(\alpha_{k_i}) = \ldots = v_R(\alpha_{k_{i+1}-1})$ и $v_R(\alpha_{k_i})(=v_R(\alpha_{k_{i+1}-1})) < < v_R(\alpha_{k_{i+1}})$; полагаем $\gamma_i \rightleftharpoons v_R(\alpha_{k_i})$, $i < s$; $\gamma_0 < \gamma_1 < \ldots < < \gamma_{s-1}$.

Т е о р е м а 1. *Имеют место следующие соотношения*:

1) $\gamma_0 = \min\left\{\frac{1}{k}v_R(a_k) \mid 1 \le k \le n\right\}$,

$$k_1 = \max\left\{k \,\middle|\, \frac{1}{k}v_R(a_k) = \gamma_0,\ 1 \le k \le n\right\};$$

2) *для* $1 \le i < s$

$$\gamma_i = \min\left\{\frac{1}{k-k_i}v_R(a_k a_{k_{i-1}}^{-1}) \,\middle|\, k_i < k \le n\right\},$$

$$k_{i+1} = \max\left\{k \,\middle|\, \frac{1}{k-k_i}v_R(a_k a_{k_{i-1}}^{-1}) = \gamma_i,\ k_i < k \le n\right\};$$

3) *для* $i < s$

$$v_R(a_{k_i}) = \sum_{j<i}(k_{j+1}-k_j)\gamma_j.$$

Соотношение 3) легко вытекает из 1) и 2).

Таким образом, по теореме 1 числа s; ($k_0 = 0$), $k_1, \ldots, k_{s-1}$ ($k_s = n$) и элементы $\gamma_0, \gamma_1, \ldots, \gamma_{s-1} \in \Gamma_R$ однозначно определены нормами $v_R(a_1)$, $v_R(a_2)$, $\ldots$, $v_R(a_n)$ коэффициентов многочлена f. Чтобы определить норму $v_R(\alpha_i)$ i-го корня многочлена f, нужно найти $t < s$ такое, что $k_t \le i < k_{t+1}$; тогда $v_R(\alpha_i) = \gamma_t$.

Теорема легко вытекает из следующей леммы, дающей более подробную информацию о соотношениях между нормами коэффициентов $v_R(a_1)$, $v_R(a_2)$, $\ldots$, $v_R(a_n)$.

Л е м м а 1. *Справедливы следующие соотношения*:

1) $v_R(a_{k_1}) = k_1\gamma_0$; $\frac{1}{k}v_R(a_k) \le \frac{1}{k_1}v_R(a_{k_1}) = \gamma_0$ *для всех* $1 \le k \le n$; $\frac{1}{k}v_R(a_k) > \gamma_0$ *для всех* $k_1 < k \le n$;

2) *для* $1 \le i \le s$

$$v_R(a_{k_{i+1}}) = k_1\gamma_0 + (k_2-k_1)\gamma_1 + \ldots + (k_{i+1}-k_i)\gamma_i = \sum_{j\le i}(k_{j+1}-k_j)\gamma_j;$$

$$\frac{1}{k-k_i}v_R(a_k a_{k_i}^{-1}) \ge \frac{1}{k_{i+1}-k_i}v_R(a_{k_{i+1}}a_{k_i}^{-1}) = \gamma_i$$

для всех $k_i < k \le n$;

$$\frac{1}{k-k_i}v_R(a_k a_{k_i}^{-1}) > \gamma_i \quad \textit{для всех} \quad k_{i+1} < k \le n.$$

Институт математики им. С.Л. Соболева Сибирского отделения Российской Академии наук, Новосибирск

Сибирский математический журнал
Ноябрь—декабрь, 2006. Том 47, № 6

УДК 512.623.4

ТЕОРЕМЫ О НЕПРЕРЫВНОСТИ КОРНЕЙ МНОГОЧЛЕНОВ В НОРМИРОВАННЫХ ПОЛЯХ

Ю. Л. Ершов

Аннотация: В литературе по нормированным полям известен ряд теорем, которые носят название теорем о непрерывности корней. Цель настоящей работы — дать улучшение констант δ для известных трех теорем, формулируемых на языке ε, δ. Доказательства базируются на основном предложении, установленном в работе автора [1].

Ключевые слова: нормированные поля, непрерывность корней.

Основные определения и необходимые свойства нормированных полей можно найти в гл. 1 книги [2].

Пусть $\mathbb{F} = \langle F, R\rangle$ — нормированное поле, $\widetilde{\mathbb{F}} = \langle \widetilde{F}, \widetilde{R}\rangle \geq \mathbb{F}$ — расширение такое, что $\widetilde{F}$ — алгебраическое замыкание F. В дальнейшем для нормирования $v_{\widetilde{R}}$ и группы нормирования $\Gamma_{\widetilde{R}}$ будут использоваться упрощенные обозначения v и Γ соответственно.

Нормирование v расширяется до нормирования (обозначаемого также через v) поля рациональных функций $\widetilde{F}(x)$ так: $vf \rightleftharpoons \min\{v(a_i) \mid i \leq n\}$ для многочлена $f = a_0x^n + \dots + a_n \in \widetilde{F}[x]$ и $v(fg^{-1}) \rightleftharpoons vf - vg$ для рациональной функции fg^{-1}; $f, g \in \widetilde{F}[x]$, $g \neq 0$.

Через $H(\mathbb{F}) = \langle H_R(F), H(R)\rangle$ обозначается гензелизация поля $\mathbb{F}$; $\mathbb{F} \leq H(\mathbb{F}) \leq \widetilde{\mathbb{F}}$. Поле $\mathbb{F}$ гензелево тогда и только тогда, когда $\mathbb{F} = H(\mathbb{F})$.

В литературе по нормированным полям известен ряд теорем, которые носят название теорем о непрерывности корней (такие, как предложение 1.3.7 в [2], теорема 2.4.7 в [3], теорема 7.4.9 в [4], теорема 2 в [5]). Цель настоящей работы — дать улучшение констант δ для первых трех утверждений, формулируемых на языке ε, δ. Интересная теорема 2 в [5] имеет другой вид и здесь не рассматривается.

В основе доказательств лежит следующее предложение, установленное автором в [1].

Основное предложение. *Пусть $f \in F[x]$ — унитарный многочлен, $a \in F$ и $\alpha \in \widetilde{F}$ — корень многочлена f, наиболее близкий к a, т. е.*

$$v(a - \alpha) = \max\{v(a - \alpha') \mid f(\alpha') = 0,\ \alpha' \in \widetilde{F}\}.$$

Тогда

(a) *имеют место неравенства*

$$vf(a) \leq v(a - \alpha) + vf'(a), \quad vf(a) \leq v(a - \alpha) + vf'(\alpha);$$

(б) *если α единственный, т. е. $f'(\alpha) \neq 0$ и $v(a-\alpha) > v(a-\alpha')$ для любого $\alpha' \neq \alpha \in \widetilde{F}$ такого, что $f(\alpha') = 0$, то $\alpha \in H_R(F)$ и имеют место равенства $vf(a) = v(a-\alpha) + vf'(a)$ и $vf'(a) = vf'(\alpha)$.*

Пусть $f \in F[x]$ — унитарный многочлен, $\alpha \in \widetilde{F}$ и $f(\alpha) = 0$. Полагаем

$$\varkappa_{f,\alpha} \rightleftharpoons \begin{cases} \omega, & \text{если } f'(\alpha) = 0 \text{ (т. е. } \alpha \text{ — кратный корень } f); \\ \max\{v(\alpha - \alpha') \mid \alpha' \in \widetilde{F},\ f(\alpha') = 0,\ \alpha \neq \alpha'\}, & \text{если } f'(\alpha) \neq 0; \end{cases}$$

$$\sigma_{f,\alpha} \rightleftharpoons \varkappa_{f,\alpha} + vf'(\alpha); \quad \varkappa_f \rightleftharpoons \max\{\varkappa_{f,\alpha} \mid \alpha \in \widetilde{F},\ f(\alpha) = 0\};$$

$$\sigma_f \rightleftharpoons \max\{\sigma_{f,\alpha} \mid \alpha \in \widetilde{F},\ f(\alpha) = 0\}; \quad \Delta_f \rightleftharpoons \max\{vf'(\alpha) \mid \alpha \in \widetilde{F}, f(\alpha) = 0\}$$

(константа σ_f введена в работе [5] и названа там *сепарантом* многочлена f).

Заметим, что имеют место эквивалентности

$$\varkappa_f \neq \omega \Leftrightarrow \sigma_f \neq \omega \Leftrightarrow \Delta_f \neq \omega \Leftrightarrow f \text{ — сепарабельный многочлен.}$$

Укажем два следствия основного предложения.

Следствие 1. *Пусть $f \in F[x]$ — унитарный многочлен, $a \in F$ и $\alpha \in \widetilde{F}$, как в условии основного предложения. Если $vf(a) > \sigma_{f,\alpha}$, то имеет место случай (б) основного предложения и $v(a-\alpha) = vf(a) - vf'(a) > \sigma_{f,\alpha} - vf'(a) = \sigma_{f,\alpha} - vf'(\alpha) = \varkappa_{f,\alpha}$ ($\geq v(\alpha - \alpha')$, $\alpha \neq \alpha' \in \widetilde{F}$, $f(\alpha') = 0$).*

Из условий следует, что $\sigma_{f,\alpha} \neq \omega$ (тогда и $\varkappa_{f,\alpha} \neq \omega$). Предположим, что α не единственный. Тогда существует $\alpha \neq \alpha' \in \widetilde{F}$ такой, что $f(\alpha') = 0$ и $v(a-\alpha') = v(a-\alpha)$. Из последнего равенства вытекает, что $v(\alpha-\alpha') = v(\alpha - a + a - \alpha') \geq v(a-\alpha)$. Далее, $v(\alpha - \alpha') \leq \varkappa_{f,\alpha}$, и заключение п. (а) предложения дает неравенство $vf(a) \leq v(a-\alpha') + vf'(\alpha)$. Имеем

$$vf(a) > \sigma_{f,\alpha} = \varkappa_{f,\alpha} + vf'(\alpha) \geq v(\alpha - \alpha') + vf'(\alpha) \geq v(a-\alpha) + vf'(\alpha).$$

Отсюда $v(a-\alpha) + vf'(\alpha) \leq \sigma_{f,\alpha} < vf(a) \leq v(a-\alpha) + vf'(\alpha)$; противоречие. □

Следствие 2 (лемма Краснера). *Пусть $\mathbb{F}$ гензелево, $f \in F[x]$ — унитарный многочлен, $a, \alpha \in \widetilde{F}$, $f(\alpha) = 0$ и $v(a-\alpha) > \varkappa_{f,\alpha}$. Тогда $\alpha \in F(a)$.*

Действительно, рассматривая гензелево поле $F(a)$ вместо F, видим, как выше, что для корня α многочлена $f \in F(a)[x]$ имеет место заключение (б) основного предложения. □

Еще одно следствие сформулируем как отдельную теорему.

Теорема 1. *Пусть $\mathbb{F}$ гензелево, $f \in F[x]$ — унитарный сепарабельный многочлен, $a \in F$ и $vf(a) > \sigma_f$. Тогда существует единственный корень α многочлена f такой, что $\alpha \in F$ и*

$$v(a-\alpha) = vf(a) - vf'(a) > \varkappa_{f,\alpha} \quad (\geq v(\alpha - \alpha'),\ \alpha \neq \alpha' \in \widetilde{F},\ f(\alpha') = 0).$$

Пусть $\alpha \in \widetilde{F}$, как в основном предложении; тогда $vf(a) > \sigma_f \geq \sigma_{f,\alpha}$ и следствие 1 показывает, что имеет место случай (б) основного предложения. Тогда $\alpha \in H_R(F) = F$ и $v(a-\alpha) = vf(a) - vf'(a)$. □

Приступим к теоремам о непрерывности корней. Сначала рассмотрим случай унитарных сепарабельных многочленов с коэффициентами из R.

Теорема 2. *Пусть $f, g \in R[x]$ — унитарные многочлены одной и той же степени n, f сепарабелен и $f = \prod\limits_{i<n}(x-\alpha_i)$ — разложение f над $\widetilde{F}$ ($\alpha_i \in \widetilde{R}$, $i < n$). Если $v(f-g) > \sigma_f$, то g сепарабелен, $\varkappa_f = \varkappa_g$, $\sigma_g = \sigma_f$, $\Delta_g = \Delta_f$; существует (единственная) нумерация $\beta_0, \dots, \beta_{n-1}$ всех корней многочлена g такая, что $\varkappa_{g,\beta_i} = \varkappa_{f,\alpha_i}$, $\sigma_{g,\beta_i} = \sigma_{f,\beta_i}$, $v(\beta_i - \alpha_i) > \varkappa_{f,\alpha_i}$ для всех $i < n$.*

Из условия $f \in R[x]$ следует, что $v(f(\gamma) - g(\gamma)) > \sigma_f$, $v(f'(\gamma) - g'(\gamma)) > \sigma_f$ для любого $\gamma \in \widetilde{R}$. Кроме того, для любого $\alpha \in \widetilde{F}(\widetilde{R})$ такого, что $f(\alpha) = 0$, имеем $vf'(\alpha) \le \sigma_{f,\alpha}$ $(= \varkappa_{f,\alpha} + vf'(\alpha)) \le \sigma_f$; следовательно, $v(g'(\alpha) - f'(\alpha)) > \sigma_f$ влечет, что $vg'(\alpha) = vf'(\alpha)$.

Для α_i ($i < n$) выберем (произвольный) ближайший корень β_i многочлена g. Тогда по основному предложению имеет место неравенство $vg(\alpha_i) \le v(\alpha_i - \beta_i) + vg'(\alpha_i)$. Далее, $vg(\alpha_i) = v(g(\alpha_i) - f(\alpha_i)) > \sigma_f \ge \sigma_{f,\alpha_i} = \varkappa_{f,\alpha_i} + vf'(\alpha_i)$; по отмеченному выше $vg'(\alpha_i) = vf'(\alpha_i)$. Следовательно, $v(\alpha_i - \beta_i) > \varkappa_{f,\alpha_i}$. Пусть $j \ne i$ и β — (произвольный) корень многочлена g такой, что $v(\alpha_j - \beta) > \varkappa_{f,\alpha_j}$ (такой β существует по доказанному выше). Покажем, что $v(\beta_i - \beta) = v(\alpha_i - \alpha_j)$. Имеем

$$v(\beta_i - \beta) = v((\beta_i - \alpha_i) + (\alpha_i - \alpha_j) + (\alpha_j - \beta)); \quad v(\alpha_i - \alpha_j) \le \varkappa_{f,\alpha_i}, \varkappa_{f,\alpha_j};$$

$$v(\beta_i - \alpha_i) > \varkappa_{f,\alpha_i}, \quad v(\alpha_j - \beta) > \varkappa_{f,\alpha_j};$$

тогда $v(\beta_i - \beta) = v(\alpha_i - \alpha_j)$. Отсюда следует, что отображение $\alpha_i \mapsto \beta_i$, $i < n$, разнозначно и корень β_i многочлена g единственный ближайший к α_i, $i < n$. Значит, g сепарабелен,

$$g = \prod_{i<n}(x - \beta_i), \quad \varkappa_{g,\beta_i} = \varkappa_{f,\alpha_i}, \quad vf'(\alpha_i) = vg'(\beta_i),$$

$$\sigma_{g,\beta_i} = \sigma_{f,\alpha_i},\ i < n; \quad \varkappa_g = \varkappa_f, \quad \sigma_g = \sigma_f, \quad \Delta_g = \Delta_f. \quad \square$$

Следствие. *В условиях (и обозначениях) теоремы при условии, что $\mathbb{F}$ гензелево, имеют место равенства $F(\alpha_i) = F(\beta_i)$, $i < n$.*

Это вытекает из следствия 2 основного предложения и неравенств

$$v(\alpha_i - \beta_i) > \varkappa_{f,\alpha_i} (= \varkappa_{g,\beta_i}), \quad i < n. \quad \square$$

Замечание 1. Предложение 1.3.7 в [2] утверждает заключение следствия в предположении, что $v(f-g) > v\delta_f^2$, где δ_f — дискриминант f. Но условие $v(f-g) > \sigma_f$, вообще говоря, заметно слабее, так как $\sigma_f \le v\delta_f \le 2v\delta_f = v\delta_f^2$.

Действительно, не уменьшая общности, предположим, что $\sigma_f = \sigma_{f,\alpha_0}$ $(= vf'(\alpha_0) + \varkappa_{f,\alpha_0})$, а $\varkappa_{f,\alpha_0} = \max\{v(\alpha_0 - \alpha_i) \mid i > 0\} = v(\alpha_0 - \alpha_1)$. Имеем

$$\pm\delta_f = \prod_{i<n} f'(\alpha_i) = f'(\alpha_0) \cdot (\alpha_1 - \alpha_0) \cdot \prod_{i>1}(\alpha_1 - \alpha_i) \cdot \prod_{j>2} f'(\alpha_j),$$

тогда

$$v(\delta_f) \ge vf'(\alpha_0) + v(\alpha_1 - \alpha_0) = \sigma_f,$$

так как $\alpha_0, \dots, \alpha_{n-1} \in \widetilde{R}$.

Замечание 2. Теорема 2 была доказана автором к константой $\varkappa_f + \Delta_f$ вместо σ_f $(\le \varkappa_f + \Delta_f)$. Независимо Бринк [5] установил ее с константой σ_f. Однако предложенное автором доказательство (изложенное выше) справедливо и для σ_f и существенно проще доказательства этой теоремы в [5].

Теорема 3. *Пусть $f, g \in R[x]$ — унитарные многочлены одной и той же степени n, f сепарабелен и $f = \prod_{i<n}(x-\alpha_i)$ — разложение f над $\widetilde{F}$. Пусть $\varepsilon \geq \varkappa_f$ и $\delta \rightleftharpoons \varepsilon + \Delta_f$. Если $v(f-g) > \delta$, то g сепарабелен и существует (единственная) нумерация $\beta_0, \dots, \beta_{n-1}$ всех корней многочлена g такая, что $v(\alpha_i - \beta_i) > \varepsilon$, $i < n$.*

Так как $\varepsilon \geq \varkappa_f$, то $\delta \geq \varkappa_f + \Delta_f \geq \sigma_f$. По теореме 2 g сепарабелен и существует нумерация $\beta_0, \dots, \beta_{n-1}$ всех корней многочлена g такая, что $v(\alpha_i - \beta_i) > \varkappa_{f,\alpha_i}$, $i < n$. При доказательстве теоремы 2 было фактически установлено, что имеют место равенства $vf(\beta_i) = v(\alpha_i - \beta_i) + vf'(\alpha_i)$, $i < n$ (заключение (б) основного предложения). Кроме того,

$$vf(\beta_i) = v(f(\beta_i) - g(\beta_i)) > \delta = \varepsilon + \Delta_f \geq \varepsilon + vf'(\alpha_i).$$

Отсюда $v(\alpha_i - \beta_i) > \varepsilon$. $\square$

Обратимся теперь к случаю произвольного унитарного сепарабельного многочлена $f \in F[x]$. Пусть

$$\gamma_f \rightleftharpoons \min\{v(\alpha) \mid \alpha \in \widetilde{F},\ f(\alpha) = 0\}, \quad \gamma_f^* \rightleftharpoons \min\{0, \gamma_f\}\ (\gamma_f^* \leq 0);$$
$$\varkappa_f^* \rightleftharpoons \varkappa_f - (n-1)\gamma_f^*; \quad \sigma_f^* \rightleftharpoons \sigma_f - (n-1)\gamma_f^*.$$

Теорема 4. *Пусть $f, g \in F[x]$ — унитарные многочлены одной и той же степени n, f сепарабелен и $f = \prod_{i<n}(x-\alpha_i)$ — разложение f над $\widetilde{F}$. Если $v(f-g) > \sigma_f^*$, то g сепарабелен, $\varkappa_g = \varkappa_f$, $\sigma_g = \sigma_f$, $\Delta_g = \Delta_f$ и существует (единственная) нумерация $\beta_0, \dots, \beta_{n-1}$ всех корней многочлена g такая, что $\varkappa_{g,\beta_i} = \varkappa_{f,\alpha_i}$, $\sigma_{g,\beta_i} = \sigma_{f,\alpha_i}$ и $v(\alpha_i - \beta_i) > \varkappa_{f,\alpha_i}$, $i < n$.*

Для α_i $(i < n)$ выберем (произвольный) ближайший корень β_i многочлена g. Тогда по основному предложению имеет место неравенство

$$vg(\alpha_i) \leq v(\alpha_i - \beta_i) + vg'(\alpha_i).$$

Оценим $vg(\alpha_i)$. Имеем

$$vg(\alpha_i) = v(g(\alpha_i) - f(\alpha_i)) = v\left(\sum_{j=1}^{n}(b_j - a_j)\alpha_i^{n-j}\right)$$
$$\geq \min\{v(b_j - a_j) + (n-j)v\alpha_i \mid 0 < j \leq n\},$$
$$v(b_j - a_j) > \sigma_f^*, \quad v\alpha_i \geq \gamma_f^*, \quad (n-j)v\alpha_i \geq (n-j)\gamma_f^* \geq (n-1)\gamma_f^*.$$

Отсюда

$$vg(\alpha_i) > \sigma_f^* + (n-1)\gamma_f^* = \sigma_f - (n-1)\gamma_f^* + (n-1)\gamma_f^* = \sigma_f.$$

Оценим $vg'(\alpha_i)$. Имеем

$$v(g'(\alpha_i) - f'(\alpha_i)) = v\left(\sum_{j=1}^{n-1}(n-j)(b_j - a_j)\alpha_i^{n-j-1}\right)$$
$$\geq \min\{v(b_j - a_j) + (n-j-1)v(\alpha_i) \mid 0 < j < n\} > \sigma_f^* + (n-2)\gamma_f^* = \sigma_f - \gamma_f^*;$$
$$\sigma_f \geq \sigma_{f,\alpha_i} = \varkappa_{f,\alpha_i} + vf'(\alpha_i); \quad \varkappa_{f,\alpha_i} = \max\{v(\alpha_i - \alpha_j) \mid j \neq i\} \geq \gamma_f^*.$$

Тогда $\sigma_f - \gamma_f^* \geq vf'(\alpha_i) + \gamma_f^* - \gamma_f^* = vf'(\alpha_i)$ и $v(g'(\alpha_i) - f'(\alpha_i)) > \sigma_f - \gamma_f^* \geq vf'(\alpha_i)$. Отсюда следует, что $vg'(\alpha_i) = vf'(\alpha_i)$.

Используя полученные оценки, приходим к соотношению

$$\sigma_f < vg(\alpha_i) \leq v(\beta_i - \alpha_i) + vg'(\alpha_i) \quad (= vf'(\alpha_i));$$
$$v(\beta_i - \alpha_i) > \sigma_f - vf'(\alpha_i) \geq \sigma_{f,\alpha_i} - vf'(\alpha_i) = \varkappa_{f,\alpha_i} + vf'(\alpha_i) - vf'(\alpha_i) = \varkappa_{f,\alpha_i}.$$

Итак, $v(\beta_i - \alpha_i) > \varkappa_{f,\alpha_i}$.

Далее рассуждаем, как в доказательстве теоремы 2. $\square$

3378_1

УДК 512.623.4

О МНОГОЧЛЕНАХ БРАУНА. II

Ю. Л. Ершов

Аннотация. Усилены результаты предыдущих работ автора, а также установлено, что любой неприводимый многочлен над гензелевым нормированным полем является многочленом Брауна.

DOI 10.33048/smzh.2060.01.001

Ключевые слова: Прошу составить список.

Все необходимые сведения о нормированных полях можно найти в [1, гл. 1].

Настоящая статья продолжает серию работ автора [2–4].

Пусть $\mathbb{F} = \langle F, R\rangle$ — нормированное поле, $\widetilde{F}$ — алгебраическое замыкание F, $\widetilde{R}$ — кольцо нормирования поля $\widetilde{F}$ такое, что $\widetilde{R} \cap F = R$ (т. е. $\mathbb{F} \leq \widetilde{F} = \langle \widetilde{F}, \widetilde{R}\rangle$).

Пусть $g \in R[x]$ — унитарный многочлен такой, что его образ $\bar{g}$ в $F_R[x]$ является неприводимым многочленом над полем вычетов F_R кольца нормирования R; пусть $\lambda > 0, \lambda \in \Gamma_{\widetilde{R}}$ и $e > 0$ целое. Многочлен $f \in R[x]$ назовем *многочленом Брауна* (типа (g, e, λ)), если выполнены следующие условия для g-разложения $f = \sum\limits_{i<n} f_i g^i$ $(f_i \in R[x]$ — многочлен степени, меньшей, чем степень δg многочлена $g)$:

(1) $v_x f_e = 0$, $v_x f_0 = e\lambda$,

(2) $v_x f_i \geq (e-i)\lambda$ для $i < 0 < e$.

Здесь v_x — гауссово нормирование поля $F(x)$, продолжающее нормирование v_R $(v_x h = \min\{v_R(a_i) \mid i \leq \delta h\}$ для $h = \sum a_i x^i \in F[x])$.

Замечание. Если f — многочлен Брауна типа (g, e, λ), то число e однозначно определяется следующими условиями:

$$\bar{g}^e \mid \bar{f} \ (\bar{g} \text{ делит } \bar{f}) \quad \text{и} \quad \bar{g}^{e+1} \nmid \bar{f} \ (\bar{g}^{e+1} \text{ не делит } \bar{f}).$$

Как и в [4], будет использоваться нормирование w поля $F[x]$, продолжающее нормирование v_R поля F, которое определяется так:

$$wh = \min\{v_x h_i + i\lambda \mid i \leq \delta h\}$$

для любого многочлена $h \in F[x]$ и его g-разложения $h = \sum\limits_{i<\delta h} h_i g_i$.

Предложение 1. *Многочлен $f \in R[x]$ является многочленом Брауна типа (g, e, λ) тогда и только тогда, когда выполнены следующие условия:*

(1) $v_x f_0 = e\lambda$, $v_x f_e = 0$,

Работа выполнена при поддержке программы фундаментальных научных исследований СО РАН № I.1.1 (проект № 0314–2019–0003).

(2) $wf = e\lambda$.

Доказательство. Пусть f является многочленом Брауна типа (g, e, λ). Условие (1) предложения совпадает с условием (1) определения многочлена Брауна.

Если $0 < i < e$, то $v_x f_i \geq (e-i)\lambda, v_x f_i + i\lambda \geq e\lambda$; если $i > e$, то $v_x f_i + i\lambda \geq i\lambda > e\lambda$. Отсюда следует, что $e\lambda = \min\{v_x f_i + i\lambda \mid i < \delta f\} = wf$.

Обратно, если $wf = e\lambda$, то $e\lambda = \min\{v_x f_i + i\lambda \mid i < \delta f\}$ влечет, что $e\lambda \leq v_f f_i + i\lambda,\ v_f f_i \geq (e-i)\lambda$ для любого i.

Вместе с условием (1) получаем, что f является многочленом Брауна типа (g, e, λ). $\square$

Предложение 2. *Пусть $f, h \in R[x]$ являются многочленами Брауна типа (g, e_0, λ) и (g, e_1, λ) соответственно. Тогда многочлен $f \cdot h$ является многочленом Брауна типа $(g, e_0 + e_1, \lambda)$.*

Доказательство. Пусть

$$f = \sum_{i<\delta f} f_i g^i, \quad h = \sum_{i<\delta h} h_i g^i,$$

$$fh = \sum_{i<\delta(fh)} F_i g^i \text{ — } g\text{-разложения многочленов } f, h \text{ и } fh.$$

Имеем $w(fh) = w(f) + w(h) = e_0\lambda + e_1\lambda = (e_0 + e_1)\lambda$.

Лемма 1. *Пусть $f, h \in R[x], r(f)$ — остаток от деления f на $g, r(h)$ — остаток от деления h на g и $r(fh)$ — остаток от деления fh на g. Тогда $v_x(r(fh)) = v_x r(f) + v_x r(h)$.*

Доказательство. Заметим, что $r(fh)$ является остатком от деления $r(f) \cdot r(h)$ на g, так что можно ограничиться рассмотрением случая, когда $f = r(f)$ и $h = r(h)$, т. е. когда степени многочленов f и h меньше степени многочлена g.

Итак, пусть степени многочленов f и h меньше степени многочлена g и $fh = d \cdot g + r, d, r \in R[x]$ — g-разложение многочлена fh. Заметим, что $r = r(f \cdot h)$. В доказательстве будет использоваться нормирование w, определенное выше.

Из предположений о степенях многочленов f и h следует, что $wf = v_x f$, $wh = v_x h$. Имеем

$$v_x f = \min\Big\{v(a_i) \mid f = \sum a_i x^i\Big\}, \quad v_x h = \min\Big\{v(b_i) \mid h = \sum b_i x^i\Big\}.$$

Пусть $a, b \in R[x]$ таковы, что $v_x f = v(a), v_x(h) = v(b)$. Полагаем $\bar{f} \rightleftharpoons a^{-1} f$, $\bar{h} = b^{-1} h$, тогда $\bar{f}, \bar{h} \in R[x]$, $v_x(\bar{f}) = v_x(\bar{h}) = 0$. Если $\bar{f} = \bar{d}g + \bar{r}$, $\bar{d}, \bar{r} \in R[x]$ — g-разложение $\bar{f}\bar{h}$, то нетрудно видеть, что $\bar{d} = (ab)^{-1} d$, $\bar{r} = (ab)^{-1} r$.

Имеем

$$0 = v_x \bar{f} + v_x \bar{g} = w\bar{f} + w\bar{g} = w(\bar{f}\bar{g}) = \min\{v_x \bar{d} + \lambda, v_x \bar{r}\} = v_x \bar{r},$$

так как $v_x \bar{d} + \lambda \geq \lambda > 0$,

$$0 = v_x(\bar{r}) = v_x((ab)^{-1} r) = v_x(r) - v_x(ab) : v_x(r)$$
$$= v_x(ab) = v_x(a) + v_x(b) = v_x f + v_x g. \quad \square$$

Из леммы 1 получаем, что

$$v_x(F_0) = v_x(h_0) + v_x(h_1) = e_0\lambda + e_1\lambda = (e_0 + e_1)\lambda.$$

Установим лемму, достаточную для завершения доказательства.

Лемма 2. *Пусть $g, f \in R[x]$, g унитарен, $\bar{g}$ неприводим над F_R, $\bar{g}^e \mid \bar{f}$, $\bar{g}^{e+1} \nmid \bar{f}$. Если $f = \sum f_i g^i$ — g-разложение f, то $\bar{f}_e \neq 0$ $(v_x f_e = 0)$, $\bar{f}_i = 0$ для $i < e$.*

Доказательство. Действительно, $\sum \bar{f}_i \bar{g}^i$ — $\bar{g}$-разложение $\bar{f}$. Отсюда сразу следует заключение леммы.

Для доказательства предложения достаточно заметить, что $\bar{g}^{e_0+e_1} \mid \overline{fh}(= \bar{f} \cdot \bar{h})$ и $\bar{g}^{e_0+e_1+1} \nmid \overline{fh}$. Тогда $\overline{F}_{e_0+e_1} \neq 0$ и $v_x(F_{e_0+e_1}) = 0$. □

Для формулировки следующего предложения необходимо расширить класс многочленов Брауна на случай $e = 0$.

Определение. Пусть $g \in R[x]$ — унитарный многочлен такой, что $\bar{g} \in R[x]$ неприводим над $F_D, \lambda > 0 \in \Gamma_{\bar{R}}$. Многочлен $f \in R[x]$ назовем *многочленом Брауна типа* $(g, 0, \lambda)$, если $\bar{g} \nmid \bar{f}$.

Заметим, что f — многочлен Брауна типа $(g, 0, \lambda)$ тогда и только тогда, когда $v_x f_0 = 0$.

Нетрудно проверить, что предложение 2 остается справедливым и для случаев, когда $e_0 = 0$ и (или) $e_1 = 0$.

Предложение 3. *Пусть $f \in R[x]$ — многочлен Брауна типа (g, e, λ) и $f = h_0 \cdot h_1$, $h_0, h_1 \in R[x]$. Тогда существуют натуральные e_0 и e_1 такие, что $e = e_0 + e_1$, h_i является многочленом Брауна типа (g, e_i, λ), $i = 0, 1$.*

Доказательство. Пусть e_i — натуральное число такое, что $\bar{g}^{e_0} \mid \bar{h}_1$, $\bar{g}^{e_i+1} \nmid \bar{h}_i$, $i = 0, 1$. Ясно, что $e = e_0 + e_1$.

Лемма 3. *Пусть $f \in R[x]$ и $\bar{g}^e \mid \bar{f}, \bar{g}^{e+1} \nmid \bar{f}$. Тогда $wf \leq e\lambda$.*

Доказательство. Действительно, пусть $f = \sum f_i g^i$, g — разложение f. Если $\bar{g}^e \mid \bar{f}$, $\bar{g}^{e+1} \nmid \bar{f}$, то $\bar{f}_e \neq 0$, $v_x f_e = 0$ и тогда $w(f) \leq e\lambda + v_x f_e = e\lambda$. □

Из леммы следует, что $w(h_i) \leq e_i\lambda, i = 0, 1$. Тогда

$$e\lambda = (e_0 + e_1)\lambda = w(f) = w(h_0 h_1) = w(h_0) + w(h_1) \leq e_0 + e_1\lambda = (e_0 + e_1)\lambda.$$

Отсюда вытекает, что $w(h_i) = e_i\lambda$, $i = 0, 1$.

Итак, установлено, что $wh_i = e_i\lambda$.

Для завершения доказательства будем применять предложение 1. Пусть

$$h_i = \sum h_{ij} g^j, \; i = 0, 1, \text{ — } g\text{-разложения многочленов } h_0 \text{ и } h_1.$$

Достаточно установить, что $v_x h_{i0} = e_i\lambda$ и $v_x h_{ie_i} = 0$, $i = 0, 1$. Из доказанного равенства $wh_i = e_i\lambda$ получаем, что $v_x h_{i0} \geq e_0\lambda$ (так как $wh_i = \min\{v_x h_{ij} + j\lambda\}$). Из леммы 1 следует, что

$$e\lambda = (e_0 + e_1)\lambda = v_x h_{00} + v_x h_{1,0} \geq e_0 + e_1\lambda = (e_0 + e_1)\lambda,$$

отсюда $v_x h_{i0} = e_i\lambda$, $i = 0, 1$.

Из того, что $\bar{g}^{e_i} \mid \bar{h}_i$, $\bar{g}^{e_i+1} \nmid \bar{h}_i$, и леммы 2 вытекает, что $v_x h_{ie_i} = 0$. Тем самым установлено, что h_i является многочленом Брауна типа (g, e_i, λ), $i = 0, 1$. □

В заключение докажем теорему, которая показывает, что многочленов Брауна не так уж мало.

Теорема. *Пусть $\mathbb{F} = \langle F, R\rangle$ — гензелево нормированное поле и $f \in R[x]$ — унитарный многочлен, неприводимый над F. Тогда f является многочленом Брауна типа (g, e, λ), $e > 0$, для подходящих g, e и λ.*

Доказательство. Рассмотрим образ $\bar{f}$ многочлена f в $F_R[x]$. Так как $\mathbb{F}$ гензелево, то $\bar{f}$ не может быть представлено в виде произведения взаимно простых многочленов. Но тогда существуют многочлен $\tilde{g} \in F_R[x]$, неприводимый над F_R, и натуральное $e > 0$ такие, что $\bar{f} = \tilde{g}^e$.

Пусть $g \in R[x]$ — унитарный многочлен такой, что $\bar{g} = \tilde{g}$ и $g \neq f$, если $e = 1$. Заметим, что неприводимость $\tilde{g}$ над F_R влечет неприводимость g над F.

Пусть $r \in R[x]$ — остаток от деления f на g и $\lambda \rightleftharpoons \frac{1}{e}v_x(r)$. Докажем, что f является многочленом Брауна типа (g, e, λ). Пусть

$$f = \sum f_i g^i \text{ — } g\text{-разложение } f.$$

Так как $r = f_0$, то $v_x(f_0) = e\lambda$. Пусть $\alpha, \theta \in F$ такие, что α — корень многочлена g, θ — корень многочлена f и

$$\tilde{v}(\alpha - \theta) = \max\{v(\alpha' - \theta')\} \mid g(\alpha') = 0, f(\theta') = 0\}.$$

Полагаем $\delta \rightleftharpoons \tilde{v}(\alpha - \theta)$. Для дальнейшего будем пользоваться нормированием $w' = w_{\alpha,\delta}$ поля $\widetilde{F}$, определенным по минимальной паре (α, δ) (см. [5]). Нормирование w' на $\widetilde{F}[x]$ определяется так: если $h = \sum c_i(x - \alpha)^i$, $\cancel{i} \in \widetilde{F}$, то $w'h = \min\{\tilde{v}(c_i) + i\delta\}$. Установим следующие соотношения: c_i

1. $w'(g) = \tilde{v}g(\theta)$. Пусть

$$g = \prod(x - \alpha_i), \quad w'(x - \alpha_i) = w'((x - \alpha) + (\alpha - \alpha_i)) = \min\{\delta, \tilde{v}(\alpha - \alpha_i)\}.$$

Далее, $\tilde{v}(\theta - \alpha_i) = \tilde{v}((\theta - \alpha) + (\alpha - \alpha_i))$. Если $\tilde{v}(\alpha - \alpha_i) < \delta = v(\theta - \alpha)$, то $\tilde{v}(\theta - \alpha_i) = \tilde{v}(\alpha - \alpha_i) = w'(x - \alpha_i)$; если $\tilde{v}(\alpha - \alpha_i) \geq \delta$, то $\tilde{v}(\theta - \alpha) + (\alpha - \alpha_i) \geq \delta$ и $\tilde{v}((\theta - \alpha_i)) \leq \delta$, следовательно, $\tilde{v}(\theta - \alpha_i) = \delta = v(\alpha - \alpha_i) = w'(x - \alpha_i)$; если $\tilde{v}(\alpha - \alpha_i) > \delta$, то $\tilde{v}(\theta - \alpha_i) = \delta = w'(x - \alpha)$. Тем самым

$$w'g(x) = \sum w'(x - \alpha_i) = \sum \tilde{v}(\theta - \alpha_i) = \tilde{v}g(\theta).$$

2. $w'f = \tilde{v}f(\alpha)$. Пусть

$$f = \prod(x - \theta_i), \quad w'f = \sum w'(x - \theta_i).$$

Тогда

$$w'(x - \theta_i) = w'((x - \alpha) + (\alpha - \theta_i)) = \min\{\delta, \tilde{v}(\alpha - \theta_i)\} = \tilde{v}(\alpha - \theta_i),$$

так как $\tilde{v}(\alpha - \theta_i) \leq \tilde{v}(\alpha - \theta) = \cancel{0}\,\delta$. δ

Итак,

$$w'f = \sum w(x - \theta_i) = \sum \tilde{v}(\alpha - \theta_i) = \tilde{v}f(\alpha).$$

3. $\tilde{v}f(\alpha) = v_x f_0$. Действительно,

$$f(\alpha) = \sum f_i(\alpha)g(\alpha)^i = f_0(\alpha), \quad \text{так как } g(\alpha) = 0.$$

Стало быть, $\tilde{v}f(\alpha) = \tilde{v}f_0(\alpha)$, но $\tilde{v}f_0(\alpha) = v_x f_0(x)$, поскольку нетрудно проверить, что для любого многочлена $h \in R[x]$, степень которого меньше степени g, справедливо равенство $\tilde{v}h(\alpha) = v_x h$.