Math-Net.Ru

Общероссийский математический портал

Ю. Л. Ершов, Расширения Любина–Тейта (элементарный подход), *Изв. РАН. Сер. матем.*, 2007, том 71, выпуск 6, 3–28

DOI: <https://doi.org/10.4213/im728>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.81.137.203

26 апреля 2023 г., 08:50:36

УДК 510.53+512.52

Ю. Л. Ершов

Расширения Любина–Тейта (элементарный подход)

Дано элементарное доказательство того, что расширение Любина–Тейта $L \geq K$ является абелевым расширением с группой Галуа, изоморфной $U_K/N_{L/K}(U_L)$, для произвольных полей K , имеющих гензелево кольцо дискретного нормирования с конечным полем вычетов. Термин “элементарность” означает лишь алгебраичность доказательств (отсутствие использования трансцендентных методов [1, с. 327, 332]).

Библиография: 9 наименований.

Пусть K – поле, O_K – гензелево кольцо дискретного нормирования поля K , π – простой элемент из O_K (т. е. $\pi O_K = \mathfrak{m}(O_K)$ – единственный максимальный идеал кольца O_K), $k \rightleftharpoons O_K/\pi O_K$ – конечное поле вычетов, имеющее $q = p^f$ элементов, где p – характеристика поля k , $f \in \omega^+ = \{1, 2, \dots\}$, и v – нормирование поля K , определенное кольцом нормирования O_K .

Поскольку кольцо O_K гензелево, то для любого алгебраического расширения $L \geq K$ поля K на L существует единственное нормирование (которое так же будем обозначать через v), продолжающее v . Кольцом этого нормирования будет целое замыкание O_L кольца O_K в L . Мультипликативная группа U_K обратимых элементов кольца O_K состоит из всех элементов $a \in K^\times$ таких, что $v(a) = 0$. Поле K содержит первообразный корень ξ из единицы степени $q - 1$, и множество $A \rightleftharpoons \{0, \xi, \xi^2, \dots, \xi^{q-1} = 1\} \subseteq O_K$ образует мультипликативный базис представителей поля k . Обозначим через $U_K^{(n)}$ множество элементов $a \in K$ таких, что $v(a - 1) \geq nv(\pi)$, $n \in \omega^+$. Нетрудно видеть, что $U_K^{(n)}$ является подгруппой группы U_K , $U_K = \langle \xi \rangle \times U_K^{(1)}$, а факторгруппа $U_K^{(n)}/U_K^{(n+1)}$ изоморфна аддитивной группе поля $k \simeq C_p^f$, т. е. прямой сумме f циклических групп простого порядка p .

Образ элемента $a \in O_K$ в k будем обозначать $\bar{a} = a + \pi O_K$; относительно π любой элемент ε из $U_K^{(n)}$ однозначно представим в виде $\varepsilon = 1 + \alpha\pi^n + a\pi^{n+1}$, где $\alpha \in A$, $a \in O_K$. Определим отображение $\varphi: U_K^{(n)} \rightarrow k$ следующим образом: $\varphi(\varepsilon) \rightleftharpoons \bar{a}$. Нетрудно проверить, что φ – эпиморфизм мультипликативной группы $U_K^{(n)}$ на аддитивную группу $\langle k, + \rangle$ с ядром $U_K^{(n+1)}$. Отсюда следует, что порядок факторгруппы $U_K/U_K^{(n)}$ равен $(q - 1)q^{n-1}$, $n \in \omega^+$.

На кольце многочленов $O_K[x]$ определена еще одна операция – суперпозиция:

$$f \circ g = a_0 g^n + a_1 g^{n-1} + \dots + a_{n-1} g + a_n,$$

для многочленов $f = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$, $g \in O_K[x]$.

Для $M, m \in \omega$ пусть $I_{M,m} \rightleftharpoons (\pi^{M+1}, x^{m+1})$ – идеал кольца $O_K[x]$, порожденный элементами π^{M+1} и x^{m+1} , а отношение $f \equiv_m^M g$ на многочленах $f, g \in O_K[x]$

означает, что $f - g \in I_{M,m}$. Отношение $f \equiv_m g$ означает, что $f \equiv_m^M g$ для всех $M \in \omega$; аналогично определяется отношение $\equiv^M$.

Если

$$f = \sum_{i=0}^n a_i x^i, \quad g = \sum_{i=0}^n b_i x^i$$

– многочлены из $O_K[x]$, то

$$\begin{aligned} f &\equiv_m^M g \Leftrightarrow v(a_i - b_i) > Mv(\pi) \quad \forall i \leq m, \\ I_M &\equiv \pi^{M+1} O_K[x], \quad I_m \equiv x^{m+1} O_K[x], \\ f &\equiv^M g \Leftrightarrow f - g \in I_M, \quad f \equiv_m g \Leftrightarrow f - g \in I_m. \end{aligned}$$

Без труда проверяется, что отношения $\equiv_m^M, \equiv_m, \equiv^M$ являются отношениями конгруэнтности относительно операций $+$, $\cdot$ и $\circ$.

ЛЕММА 1. Пусть $f, g, f', g' \in O_K[x]$, $f \equiv_m^M f'$, $g \equiv_m^M g'$. Тогда $f + g \equiv_m^M f' + g'$, $f \cdot g \equiv_m^M f' \cdot g'$ и $f \circ g \equiv_m^M f' \circ g'$.

Многочленом Любина–Тейта (ЛТ-многочленом) относительно простого элемента π назовем всякий многочлен $f(x) = x^q + a_1 x^{q-1} + \dots + a_{q-2} x^2 + \pi x \in O_K[x]$ такой, что $a_1, \dots, a_{q-2} \in \pi O_K$.

Для ЛТ-многочлена f полагаем

$$f^{(0)} \equiv x, \quad f^{(n+1)} \equiv f \circ (f^{(n)}), \quad n \in \omega$$

(в частности, $f^{(1)} = f \circ f^{(0)} = f$),

$$F_n \equiv f^{(n)} (f^{(n-1)})^{-1} = (f^{(n-1)})^{q-1} + a_1 (f^{(n-1)})^{q-2} + \dots + a_{q-2} f^{(n-1)} + \pi, \quad n \in \omega^+.$$

Нетрудно видеть (проверка индукцией по n), что F_n является многочленом Эйзенштейна над K (см. [1]–[3]) степени $(q-1)q^{n-1}$. Обозначим через $L_{f,n}$ расширение поля K , полученное присоединением корня $\alpha_{f,n}$ многочлена F_n (в некотором алгебраическом замыкании $\bar{K}$ поля K) к K . Тогда $L_{f,n}$ – вполне разветвленное расширение поля K и $[L_{f,n} : K] = (q-1)q^{n-1}$.

Заметим, что $f(\alpha_{f,n+1})$ является корнем многочлена F_n , т.е. можно считать, что $\alpha_{f,n} = f(\alpha_{f,n+1})$.

Оказывается, что расширение $L_{f,n} \supseteq K$, которое назовем *расширением Любина–Тейта степени n* , является абелевым и не зависит от f , т.е. если g – другой ЛТ-многочлен, то $L_{f,n} = L_{g,n}$.

Рассмотрим сначала “простейший” ЛТ-многочлен $f(x) \equiv x^q + \pi x$ и вместо обозначения $L_{f,n}$ будем использовать обозначение L_n .

ТЕОРЕМА 1. Поле L_n является абелевым вполне разветвленным расширением поля K , и $G(L_n/K) \simeq U_K/U_K^{(n)}$.

Данная теорема была доказана в исходной работе [4] и с тех пор ни одно изложение локальной теории полей классов не обходится без использования этой теоремы. Однако, как отмечает Ю. Нейкирх [1, с. 327, 332], в известных доказательствах этой теоремы используются трансцендентные методы. Он высказывает надежду найти чисто алгебраическое доказательство. В настоящей работе предлагается именно такое доказательство.

В приложении рассматриваются произвольные гензелевы нормированные поля; в частности, установлена теорема П2, гарантирующая существование корня многочлена в гензелевом поле при условиях, которые (часто) более оптимальны, чем условия теоремы Гензеля–Рихлика.

В доказательстве теоремы 1 будем использовать теорему П2 и более детальную информацию о многочленах $[u]_m = [u]_{f,f}^m$ из леммы Любина–Тейта (см. ниже).

Для применения теоремы П2 необходимо вычислить элементы

$$\varkappa_{F_n} = \max\{v(\alpha - \beta) \mid F_n(\alpha) = F_n(\beta) = 0, \alpha \neq \beta, \alpha, \beta \in K^{\text{sep}}\},$$

$$\Delta_{F_n} = \max\{vF'_n(\alpha) \mid F_n(\alpha) = 0, \alpha \in K^{\text{sep}}\}, \quad \varepsilon_{F_n} = \varkappa_{F_n} + \Delta_{F_n}.$$

ПРЕДЛОЖЕНИЕ 1. *Имеют место равенства*

$$\varkappa_{F_n} = \frac{1}{q-1}v(\pi), \quad \Delta_{F_n} = \left(n - \frac{1}{q-1}\right)v(\pi), \quad \varepsilon_{F_n} = nv(\pi).$$

ДОКАЗАТЕЛЬСТВО. Пусть α – корень многочлена F_n , $\alpha = \alpha_{f,n}$. Так как F_n – многочлен Эйзенштейна степени $(q-1)q^{n-1}$, то $v(\alpha) = \frac{1}{(q-1)q^{n-1}}v(\pi)$.

Вычислим норму $v(F'_n(\alpha))$ производной многочлена F_n в α . Имеем

$$F'_n = ((f^{(n-1)})^{q-1} + \pi)' = (q-1)(f^{(n-1)})^{q-2}f'(f^{(n-2)}) \dots f'(f)f',$$

$$f' = (x^q + \pi x)' = qx^{q-1} + \pi.$$

Поскольку $v(q) \geq v(p) \geq v(\pi)$, то для любого $\beta \in L_n$ такого, что $v(\beta) > 0$, имеем

$$vf'(\beta) = v(q\beta^{q-1} + \pi) = v(\pi),$$

так как $v(q\beta^{q-1}) > v(q) \geq v(\pi)$. Отсюда получаем

$$v(F'_n(\alpha)) = (q-2)v(f^{(n-2)}(\alpha)) + (n-1)v(\pi).$$

Далее, для $i \in \omega^+$ и $\beta \in L_n$ если $0 < v(\beta) < \frac{1}{q^i}v(\pi)$, то $v(f^{(i)}(\beta)) = q^i v(\beta)$. Действительно, $f^{(i)}(x)$ представим в виде $x^{q^i} + \pi x Q_i(x)$ для подходящего многочлена $Q_i(x) \in O_K[x]$. Тогда $v(\pi \beta Q_i(\beta)) > v(\pi) > q^i v(\beta) = v(\beta^{q^i})$ и, следовательно, $v(f^{(i)}(\beta)) = q^i v(\beta)$. Отсюда

$$v(F'_n(\alpha)) = (q-2)v(f^{(n-2)}(\alpha)) + (n-1)v(\pi),$$

$$v(F'_n(\alpha)) = \frac{q-2}{q-1}v(\pi) + (n-1)v(\pi) = \left(n - \frac{1}{q-1}\right)v(\pi) < nv(\pi).$$

Таким образом, $v(F'_n(\alpha))$ не зависит от α , и, следовательно,

$$\Delta_{F_n} = \left(n - \frac{1}{q-1}\right)v(\pi).$$

Доказательство того, что $\varkappa_{F_n} = \frac{1}{q-1}v(\pi)$, будем проводить индукцией по n .

Пусть $n = 1$, $F_1 = x^{q-1} + \pi$. Если $\alpha \neq \beta$ и $F_1(\alpha) = F_1(\beta) = 0$, то $\alpha = \xi\beta$ для $\xi \neq 1$ такого, что $\xi^{q-1} = 1$. Тогда $v(1 - \xi) = 0$ и $v(\alpha - \beta) = v(\alpha(1 - \xi)) = v(\alpha) = \frac{1}{q-1}v(\pi)$. Отсюда $\varkappa_{F_1} = \frac{1}{q-1}v(\pi)$.

Пусть $n > 1$.

ЛЕММА 2. Пусть $F_n(\alpha) = F_n(\beta) = 0$, $\alpha \neq \beta$. Тогда для $\alpha_0 \Rightarrow f(\alpha) = \alpha^q + \pi\alpha$ и $\beta_0 \Rightarrow f(\beta) = \beta^q + \pi\beta$ имеем $F_{n-1}(\alpha_0) = F_{n-1}(\beta_0) = 0$ и $v(\alpha_0 - \beta_0) > v(\alpha - \beta)$.

ДОКАЗАТЕЛЬСТВО. Полагаем $\gamma \Rightarrow \beta\alpha^{-1}$; так как $v(\alpha) = v(\beta)$, то $v(\gamma) = 0$ и $v(1 - \gamma) \geq 0$. Имеем

$$\begin{aligned}\alpha_0 - \beta_0 &= (\alpha^q - \beta^q) + \pi(\alpha - \beta) = \alpha^q(1 - \gamma^q) + \pi\alpha(1 - \gamma), \\ v(\alpha^q(1 - \gamma^q)) &= qv(\alpha) + v(1 - \gamma^q) = qv(\alpha) + v(1 - \gamma) + v(1 + \gamma + \dots + \gamma^{q-1}) \\ &\geq qv(\alpha) + v(1 - \gamma) = (q - 1)v(\alpha) + v(\alpha) + v(1 - \gamma) \\ &= (q - 1)v(\alpha) + v(\alpha - \beta) > v(\alpha - \beta), \\ v(\pi(\alpha - \beta)) &= v(\pi) + v(\alpha - \beta) > v(\alpha - \beta).\end{aligned}$$

Следовательно,

$$v(\alpha_0 - \beta_0) \geq \min\{v(\alpha^q - \beta^q), v(\pi(\alpha - \beta))\} > v(\alpha - \beta).$$

Лемма доказана.

Пусть $F_n(\alpha) = F_n(\beta) = 0$, $\alpha \neq \beta$, и предположим, что $v(\alpha - \beta) \geq \frac{1}{q-1}v(\pi)$. Тогда по лемме 2

$$v(\alpha_0 - \beta_0) > \frac{1}{q-1}v(\pi) = \varkappa_{F_{n-1}}$$

(последнее равенство выполнено по индуктивному предположению). Но это может быть только при условии $\alpha_0 = \beta_0$. Если $\alpha_0 = \beta_0$, то $\alpha^q - \beta^q = \pi(\beta - \alpha)$. Полагаем $\gamma \Rightarrow \beta\alpha^{-1}$, $\varepsilon \Rightarrow 1 - \gamma$, $\gamma = 1 - \varepsilon$; имеем

$$\gamma^q = (1 - \varepsilon)^q = 1 + \pi\varepsilon a \pm \varepsilon^q$$

для подходящего $a \in O_K$. Рассмотрим два возможных случая.

Случай 1: $v(\varepsilon^q) \geq v(\pi\varepsilon)$. Тогда $v(1 - \gamma^q) \geq v(\pi\varepsilon)$; но должно быть выполнено равенство $v(\alpha^q - \beta^q) = v(\pi(\beta - \alpha))$. Имеем

$$\begin{aligned}v(\alpha^q - \beta^q) &= v(\alpha^q(1 - \gamma^q)) = qv(\alpha) + v(1 - \gamma^q) \geq (q - 1)v(\alpha) + v(\alpha) + v(\pi\varepsilon) \\ &> v(\alpha) + v(\pi\varepsilon) = v(\alpha\pi\varepsilon) = v(\pi\alpha(1 - \gamma)) = v(\pi(\alpha - \beta)) = v(\pi(\beta - \alpha)).\end{aligned}$$

Противоречие. Этот случай невозможен.

Случай 2: $v(\varepsilon^q) < v(\pi\varepsilon)$. Тогда $v(1 - \gamma^q) = v(\varepsilon^q) = qv(\varepsilon)$ и равенство $v(\alpha^q - \beta^q) = v(\pi(\beta - \alpha))$ влечет

$$\begin{aligned}v(\alpha^q - \beta^q) &= v(\alpha^q(1 - \gamma^q)) = qv(\alpha) + qv(\varepsilon) = v(\pi) + v(\alpha) + v(\varepsilon), \\ (q - 1)(v(\alpha) + v(\varepsilon)) &= v(\pi), \quad v(\alpha) + v(\varepsilon) = \frac{1}{q-1}v(\pi);\end{aligned}$$

так как $v(\alpha) + v(\varepsilon) = v(\alpha - \beta)$, имеем $v(\alpha - \beta) = \frac{1}{q-1}v(\pi)$.

Для завершения доказательства предложения заметим, что существуют $\alpha \neq \beta$ такие, что $F_n(\alpha) = F_n(\beta) = 0$ и $f(\alpha) = f(\beta)$. Однако это следует из того, что многочлен F_n имеет $(q - 1)q^{n-1}$ корней, а многочлен F_{n-1} имеет только $(q - 1)q^{n-2}$ корней.

Сформулируем теперь лемму Любина–Тейта.

ЛЕММА 3 [4]. Пусть $g = x^q + b_1x^{q-1} + \dots + b_{q-2}x^2 + \pi x$, $h = x^q + c_1x^{q-1} + \dots + c_{q-2}x^2 + \pi x \in O_K[x]$ – LT-многочлены, $b_1, \dots, b_{q-2}, c_1, \dots, c_{q-2} \in \pi O_K$. Тогда для любых $d \in O_K$ и $m \in \omega^+$ существует единственный многочлен $[d]_{g,h}^m = d_1x + d_2x^2 + \dots + d_mx^m \in xO_K[x]$ степени не более m такой, что $d_1 = d$ и $g \circ [d]_{g,h}^m \equiv_m [d]_{g,h}^m \circ h$.

Доказательство этой леммы часто повторяется (см. [1]–[3]) и поэтому в настоящей работе не приводится. Основные моменты этого доказательства воспроизводятся ниже, в доказательстве предложения 2.

Лемму Любина–Тейта можно сформулировать и в терминах рядов.

Для любого $d \in O_K$ существует единственный ряд $[d]_{g,h} = d_1x + d_2x^2 + \dots \in xO_K[[x]]$ такой, что $d_1 = d$ и $g \circ [d]_{g,h} = [d]_{g,h} \circ h$.

Заметим, что операция суперпозиции определена корректно и на рядах из кольца $xO_K[[x]]$.

Если h_0 , h_1 и h_2 – LT-многочлены, $d_0, d_1 \in O_K$, то $[d_0]_{h_0, h_1} \circ [d_1]_{h_1, h_2} = [d_0d_1]_{h_0, h_2}$; действительно,

$$h_0 \circ [d_0]_{h_0, h_1} \circ [d_1]_{h_1, h_2} = [d_0]_{h_0, h_1} \circ h_1 \circ [d_1]_{h_1, h_2} = [d_0]_{h_0, h_1} \circ [d_1]_{h_1, h_2} \circ h_2;$$

ряд $[d_0]_{h_0, h_1} \circ [d_1]_{h_1, h_2}$ имеет элемент d_0d_1 коэффициентом при x . Тогда единственность влечет равенство

$$[d_0d_1]_{h_0, h_2} = [d_0]_{h_0, h_1} \circ [d_1]_{h_1, h_2}. \quad (1)$$

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. Пусть $m \equiv (n+1)(q-1)q^{n-1}$, $\alpha \equiv \alpha_{f,n}$. Для любого $u \in U_K$ пусть $[u]_m$ обозначает многочлен $[u]_{f,f}^m$ из леммы Любина–Тейта и пусть $\beta_u \equiv [u]_m(\alpha)$. Из того, что $u \in U_K$, легко следует равенство $v(\beta_u) = v(\alpha)$.

Проверим, что $v(F_n(\beta_u)) > nv(\pi) = \varepsilon_{F_n}$. Так как $f \circ [u]_m \equiv_m [u]_m \circ f$, то индукцией по i получаем, что $f^{(i)} \circ [u]_m \equiv_m [u]_m \circ f^{(i)}$ для любого $i \in \omega^+$. В частности, $f^{(n)} \circ [u]_m - [u]_m \circ f^{(n)} \in x^{m+1}O_K[x]$. Тогда

$$\begin{aligned} f^{(n)} \circ [u]_m(\alpha) - [u]_m \circ f^{(n)}(\alpha) &= f^{(n)}(\beta_u) \in \alpha^{m+1}O_K, \\ v(f^{(n)}(\beta_u)) &\geq (m+1)v(\alpha) = (n+1)(q-1)q^{n-1}v(\alpha) + v(\alpha) \\ &= (n+1)v(\pi) + v(\alpha) > (n+1)v(\pi). \end{aligned}$$

Заметим, что $v(f^{(n-1)}(\beta_u)) = q^{n-1}v(\beta_u)$. На самом деле для любых $\beta \in L_n$, $i \in \omega^+$ таких, что $0 < v(\beta) \leq q^{-i}v(\pi)$, справедливо $v(f^{(i)}(\beta)) = q^i v(\pi)$. Действительно, $f^{(i)}(x)$ представимо в виде $x^{q^i} + \pi x Q_i(x)$ для подходящего многочлена $Q_i(x) \in O_K[x]$. Тогда

$$v(\pi \beta Q_i(\beta)) \geq v(\pi \beta) > v(\pi) \geq q^i v(\beta) = v(\beta^{q^i})$$

и, следовательно, $v(f^{(i)}(\beta)) = q^i v(\beta)$. Так как

$$v(\beta_u) = v(\alpha) = \frac{1}{(q-1)q^{n-1}}v(\pi) \leq \frac{1}{q^{n-1}}v(\pi),$$

то

$$v(f^{(n-1)}(\beta_u)) = q^{n-1}v(\beta_u) = \frac{1}{q-1}v(\pi).$$

Из соотношений $v(f^{(n)}(\beta_u)) > (n+1)v(\pi)$, $v(f^{(n-1)}(\beta_u)) = \frac{1}{q-1}v(\pi)$ следует, что

$$v(F_n(\beta_u)) = v(f^{(n)}(\beta_u)) - v(f^{(n-1)}(\beta_u)) > nv(\pi) + \frac{q-2}{q-1}v(\pi) \geq nv(\pi).$$

По теореме П2 в L_n существует единственный элемент α_u такой, что $F_n(\alpha_u) = 0$ и $v(\beta_u - \alpha_u) = v(F_n(\beta_u)) - v(F'_n(\beta_u)) > \varkappa_{F_n}$. Таким образом определено отображение $u \mapsto \alpha_u$, $u \in U_K$, из множества U_K во множество корней многочлена F_n в L_n . Так как $L_n = K(\alpha) = K(\alpha_u)$, то для любого $u \in U$ существует K -автоморфизм σ_u поля L_n такой, что $\sigma_u(\alpha) = \alpha_u$. Из соотношения (1) при $h_0 = h_1 = h_2 = f$ получаем $[u_0]_m \circ [u_1]_m \equiv_m [u_0 u_1]_m$ и отсюда имеем $\sigma_{u_0} \sigma_{u_1} = \sigma_{u_0 u_1}$.

Итак, определен гомоморфизм $\sigma: U_K \rightarrow \text{Aut}_K L_n$. Далее будет установлено, что $\text{Ker } \sigma \leq U_K^{(n)}$; отсюда получим

$$(q-1)q^{n-1} = |U_K : U_K^{(n)}| \leq |U_K : \text{Ker } \sigma| \leq |\text{Aut}_K L_n| \leq (q-1)q^{n-1},$$

$$U_K^{(n)} = \text{Ker } \sigma, \quad |\text{Aut}_K L_n| = (q-1)q^{n-1} = [L_n : K].$$

Из последних соотношений следует, что L_n — абелево расширение поля K с группой Галуа $\text{Aut}_K L_n$, изоморфной группе $U_K/U_K^{(n)}$.

Для доказательства включения $\text{Ker } \sigma \leq U_K^{(n)}$ получим более детальную информацию о многочленах $[u]_m$.

ПРЕДЛОЖЕНИЕ 2. а) Для любых $a \in O_K$ и $m \geq 1$ существует единственный многочлен $[a]_m$ вида $ax + a_2 x^2 + \dots + a_m x^m$ степени не более m такой, что $f \circ [a]_m \equiv_m [a]_m \circ f$.

б) Если $a^q = a$, то $[a]_m = ax$ для всех $m \geq 1$.

с) Если $a^q \neq a$ и $v(a^q - a) = lv(\pi)$, $l \in \omega$ (заметим, что тогда $l > 0$), то $v(a_{q^i}) = (l-i)v(\pi)$ для $1 \leq i \leq l$ и $v(a_m) > v(a_{q^i})$ для $1 \leq i \leq l$, $1 < m < q^i$.

ДОКАЗАТЕЛЬСТВО. Проверим утверждение б). Пусть $a^q = a$; тогда

$$f \circ ax = (ax)^q + \pi ax = a^q x^q + \pi ax = ax^q + \pi ax = a(x^q + \pi x) = af(x) = ax \circ f.$$

Докажем утверждение а). Пусть $a^q \neq a$ и $v(a^q - a) = lv(\pi)$. Если $v(a) > 0$, то $v(a^q - a) = v(a) > 0$, $l > 0$; если $v(a) = 0$, то a представимо в виде $a = \alpha + \pi b$, $b \in O_K$, $\alpha \in A \setminus \{0\}$. Тогда $a^q = (\alpha + \pi b)^q = \alpha^q + \pi c$ для подходящего $c \in O_K$. Однако $\alpha^q = \alpha$, следовательно, $a^q - a = \alpha + \pi c - (\alpha + \pi b) = \pi(c - b)$, $c - b \in O_K$, и $v(a^q - a) > 0$.

Проверим, что $[a]_m = ax$ для $1 \leq m < q$. Действительно, имеем

$$f \circ ax = f(ax) = a^q x^q + \pi ax \equiv_m \pi ax,$$

$$ax \circ f = a(x^q + \pi x) = ax^q + \pi ax \equiv_m \pi ax.$$

Следовательно, $f \circ ax \equiv_m ax \circ f$ для $1 \leq m < q$.

Проверим, что $[a]_q = ax + a_q x^q$ для

$$a_q \rightleftharpoons \frac{a^q - a}{\pi^q - \pi}.$$

Заметим, что

$$\begin{aligned} v(\pi^q - \pi) &= v(\pi) + v(\pi^{q-1} - 1) = v(\pi), \\ v(a_q) &= v(a^q - a) - v(\pi^q - \pi) = lv(\pi) - v(\pi) = (l-1)v(\pi). \end{aligned}$$

Имеем

$$\begin{aligned} f \circ (ax + a_q x^q) &= (ax + a_q x^q)^q + \pi(ax + a_q x^q) \\ &\equiv_q a^q x^q + \pi ax + \pi a_q x^q = \pi ax + (a^q + \pi a_q) x^q, \\ (ax + a_q x^q) \circ f &= a(x^q + \pi x) + a_q (x^q + \pi x)^q \\ &\equiv_q ax^q + a\pi x + a_q \pi^q x^q = \pi ax + (a + \pi^q a_q) x^q. \end{aligned}$$

Если $f \circ (ax + a_q x^q) \equiv_q (ax + a_q x^q) \circ f$, то должно быть выполнено равенство $a^q + \pi a_q = a + \pi^q a_q$, следовательно,

$$a_q = \frac{a^q - a}{\pi^q - \pi}.$$

Рассмотрим общий случай. Пусть $m \geq q$ и многочлен $[a]_m = ax + a_2 x^2 + \dots + a_m x^m$, удовлетворяющий условию $f \circ [a]_m \equiv_m [a]_m \circ f$, уже (однозначно) определен. Будем искать $a_{m+1} \in O_K$ таким, чтобы было выполнено $f \circ [a]_{m+1} \equiv_{m+1} [a]_{m+1} \circ f$ для $[a]_{m+1} \rightleftharpoons [a]_m + a_{m+1} x^{m+1}$.

Имеем

$$\begin{aligned} f \circ [a]_{m+1} &= ([a]_m + a_{m+1} x^{m+1})^q + \pi([a]_m + a_{m+1} x^{m+1}) \\ &\equiv_{m+1} [a]_m^q + \pi[a]_m + \pi a_{m+1} x^{m+1}. \end{aligned}$$

Отметим следующий простой факт.

ЛЕММА 4. Пусть $b_1, \dots, b_n \in O_K$, $n > 1$. Тогда коэффициенты многочлена

$$(b_1 x + \dots + b_n x)^q - \sum_{i=1}^n b_i^q x^{qi}$$

принадлежат идеалу $p(b_2, \dots, b_n)$ кольца O_K .

ДОКАЗАТЕЛЬСТВО проводится индукцией по n с использованием того, что биномиальный коэффициент C_q^i , $0 < i < q$, делится на p .

Используя лемму 4, представим многочлен $[a]_m^q$ в виде

$$[a]_m^q = \sum_{i=1}^m a_i^q x^{qi} + \pi Q(x)$$

($a_1 \rightleftharpoons a$, π делит p), где многочлен

$$Q(x) = \sum_{j=1}^{qm-1} a'_j x^j$$

таков, что его коэффициенты a'_j не зависят от a_{m+1} и принадлежат идеалу $(a_2, \dots, a_m)$. Тогда коэффициент при x^{m+1} в многочлене $[a]_m^q + \pi[a]_m + \pi a_{m+1} x^{m+1}$ будет равен $\pi a'_{m+1} + \pi a_{m+1}$, если q не делит $m+1$, и равен $a_{m'}^q + \pi a'_{m+1} + \pi a_{m+1}$, если q делит $m+1$ и $m+1 = qt'$.

Далее,

$$\begin{aligned} [a]_{m+1} \circ f &= a(x^q + \pi x) + a_2(x^q + \pi x)^2 + \dots + a_m(x^q + \pi x)^m \\ &\quad + a_{m+1}(x^q + \pi x)^{m+1} \\ &\equiv_{m+1} \pi a x + a x^q + \sum_{j=2}^m a_j x^{qj} + \pi P(x) + a_{m+1} \pi^{m+1} x^{m+1}, \end{aligned}$$

где $\pi P(x) = \sum_{j=2}^m a_j (x^q + \pi x)^j - \sum_{j=2}^m a_j x^{qj}$.

Коэффициенты a''_j многочлена $P(x) = \sum_{j=1}^{qm} a''_j x^j$ не зависят от a_{m+1} и принадлежат идеалу $(a_2, \dots, a_m)$ кольца O_K . Коэффициент при x^{m+1} многочлена

$$\pi a x + a x^q + \sum_{j=2}^m a_j x^{qj} + \pi P(x) + a_{m+1} \pi^{m+1} x^{m+1}$$

равен $\pi a''_{m+1} + \pi^{m+1} a_{m+1}$, если q не делит $m+1$, и равен $a_{m'} + \pi a''_{m+1} + \pi^{m+1} a_{m+1}$, если q делит $m+1$ и $m+1 = qt'$.

Итак, должно выполняться или равенство

$$\pi a'_{m+1} + \pi a_{m+1} = \pi a''_{m+1} + \pi^{m+1} a_{m+1},$$

если q не делит $m+1$, и тогда

$$a_{m+1} = \frac{a'_{m+1} - a''_{m+1}}{\pi^m - 1},$$

или равенство

$$a_{m'}^q + \pi a'_{m+1} + \pi a_{m+1} = a_{m'} + \pi a''_{m+1} + \pi^{m+1} a_{m+1},$$

если q делит $m+1$ и $m+1 = qt'$, и тогда

$$a_{m+1} = \frac{(a_{m'}^q - a_{m'}) + \pi(a'_{m+1} - a''_{m+1})}{\pi(\pi^m - 1)}.$$

Поскольку $a_{m'}^q - a_{m'} \in \pi O_K$, то $a_{m+1} \in O_K$. Отсюда следует утверждение а) предложения.

Докажем утверждение с). В случае, когда q не делит $m+1$, имеем $a_{m+1} \in (a_2, \dots, a_m)$; так как $a'_{m+1}, a''_{m+1} \in (a_2, \dots, a_m)$, $(\pi^m - 1)^{-1} \in U_K$, то $v(a_{m+1}) \geq \min\{v(a_i) \mid 2 \leq i \leq m\}$.

Предположим, что для $i_0 < l$ и $q^{i_0} \leq m < q^{i_0+1}$ уже установлены следующие факты:

- (i) $v(a_{q^i}) = (l - i)v(\pi)$ для любого $1 \leq i \leq i_0$;
- (ii) $v(a_{m'}) > v(a_{q^i})$ для любого $m' < q^i$;
- (iii) $v(a_{m'}) \geq v(a_{q^{i_0}}) = (l - i_0)v(\pi) > l - (i_0 + 1)v(\pi)$ для любого $m' < m$.

Рассмотрим элемент a_{m+1} .

Случай 1: $m+1 \neq q^{i_0+1}$. Тогда $q^{i_0} < m+1 < q^{i_0+1}$.

а) q не делит $m+1$. Тогда, как замечено выше, $a_{m+1} \in (a_2, \dots, a_m)$ и $v(a_{m+1}) \geq \min\{v(a_i) \mid 2 \leq i \leq m\} = v(a_{q^{i_0}}) = (l - i_0)v(\pi)$ (по индуктивному предположению).

б) q делит $m+1$, $m+1 = qm'$. Тогда $q^{i_0-1} < m' < q^{i_0}$ и по индуктивному предположению имеем $v(a_{m'}) > v(a_{q^{i_0}})$ и

$$\begin{aligned} a_{m+1} &= \frac{(a_{m'}^q - a_{m'}) + \pi(a'_{m+1} - a''_{m+1})}{\pi(\pi^m - 1)} \\ &= (\pi^m - 1)^{-1}(\pi^{-1}(a_{m'}^q - a_{m'}) + (a'_{m+1} - a''_{m+1})), \\ a'_{m+1} - a''_{m+1} &\in (a_2, \dots, a_m), \end{aligned}$$

следовательно,

$$\begin{aligned} v(a'_{m+1} - a''_{m+1}) &\geq \min\{v(a_i) \mid 2 \leq i \leq m\} = v(a_{q^{i_0}}) = (l - i_0)v(\pi), \\ v(\pi^{-1}(a_{m'}^q - a_{m'})) &= v(a_{m'}) - v(\pi) \geq v(a_{q^{i_0}}) = (l - i_0)v(\pi). \end{aligned}$$

Итак,

$$v(a_{m+1}) \geq (l - i_0)v(\pi).$$

Случай 2: $m+1 = q^{i_0+1}$. Тогда

$$\begin{aligned} a_{m+1} = a_{q^{i_0+1}} &= \frac{(a_{q^{i_0}}^q - a_{q^{i_0}}) + \pi(a'_{q^{i_0+1}} - a''_{q^{i_0+1}})}{\pi(\pi^{q^{i_0+1}-1} - 1)}, \\ v(a_{q^{i_0}}) &= (l - i_0)v(\pi), \end{aligned}$$

отсюда имеем

$$v(a_{q^{i_0}}^q - a_{q^{i_0}}) = v(a_{q^{i_0}}) = (l - i_0)v(\pi), \quad a'_{q^{i_0+1}} - a''_{q^{i_0+1}} \in (a_2, \dots, a_{q^{i_0+1}-1}),$$

следовательно,

$$\begin{aligned} v(a'_{q^{i_0+1}} - a''_{q^{i_0+1}}) &\geq \min\{v(a_i) \mid 2 \leq i < q^{i_0+1}\} = (l - i_0)v(\pi), \\ v(\pi(a'_{q^{i_0+1}} - a''_{q^{i_0+1}})) &> (l - i_0)v(\pi). \end{aligned}$$

Итак,

$$\begin{aligned} v((a_{q^{i_0}}^q - a_{q^{i_0}}) + \pi(a'_{q^{i_0+1}} - a''_{q^{i_0+1}})) &= (l - i_0)v(\pi), \\ v(a_{q^{i_0+1}}) &= (l - i_0)v(\pi) - v(\pi) = (l - (i_0 + 1))v(\pi). \end{aligned}$$

Утверждение с), а следовательно, и все утверждения предложения доказаны.

Покажем теперь, что если $u \in U_K \setminus U_K^{(n)}$, то $\alpha_u \neq \alpha$. Из условия для u следует, что $v(u - 1) < nv(\pi)$. Оценим норму $v(\beta_u - \alpha)$ разности элементов β_u и α : $\beta_u - \alpha = (u-1)\alpha + u_2\alpha^2 + \dots + u_m\alpha^m$; если $v(u-1) = 0$, то $v(\beta_u - \alpha) = v(\alpha) < v(\pi)$, $v(\alpha_u - \alpha) = v(\alpha_u - \beta_u + \beta_u - \alpha) = v(\alpha)$ и $\alpha_u \neq \alpha$.

Пусть $v(u-1) > 0$, $v(u-1) = lv(\pi)$ для $0 < l < n$; тогда $v(u^q - u) = v(u-1) = lv(\pi)$. По предложению 2 имеем $v(u_{q^l}) = 0$ и $v(u_i) \geq v(\pi)$ для $0 < i < q^l$. Тогда

$$v(u_{q^l} \alpha^{q^l}) = \frac{q^l}{(q-1)q^{n-1}} v(\pi) < v(\pi), \quad v((u-1)\alpha) > v(\pi),$$

$$v(u_i \alpha^i) \geq v(\alpha^i) = \frac{i}{(q-1)q^{n-1}} v(\pi) > \frac{q^l}{(q-1)q^{n-1}} v(\pi)$$

для $q^l < i \leq m$. Отсюда

$$v(\beta_u - \alpha) = \frac{q^l}{(q-1)q^{n-1}} v(\pi) \leq \frac{1}{q-1} v(\pi),$$

так как $l \leq n-1$. Тогда $v(\alpha_u - \alpha) = v(\alpha_u - \beta_u + \beta_u - \alpha) = v(\beta - \alpha)$, так как $v(\beta_u - \alpha) > nv(\pi) \geq v(\pi) \geq \frac{1}{q-1} v(\pi) \geq v(\beta_u - \alpha)$. Отсюда имеем $v(\alpha_u - \alpha) = v(\beta_u - \alpha) \neq \omega$ и $\alpha_u \neq \alpha$. Теорема доказана.

В ходе доказательства теоремы 1 было установлено

СЛЕДСТВИЕ 1. Если $0 \leq l < n$, $u \in U_K^{(l)} \setminus U_K^{(l+1)}$ ($U_K^{(0)} = U_K$), то

$$v(\alpha - \sigma_u \alpha) = v(\alpha - \alpha_u) = q^l v(\alpha) = \frac{1}{(q-1)q^{n-l-1}} v(\pi).$$

Следствие 1 можно переформулировать, используя высшие группы ветвления.

Пусть $i \in \omega$, $G_i = \{\sigma \mid \sigma \in \text{Aut}_K L_n, v(\sigma a - a) > iv(a) \text{ для всех } a \in O_{L_n}\} = \{\sigma \mid \sigma \in \text{Aut}_K L_n, v(\sigma \alpha - \alpha) > iv(\alpha)\}$.

СЛЕДСТВИЕ 2. Для $0 \leq l < n$ имеем:

- а) $\sigma(U_K^{(l)}) = G_{q^l-1}$;
- б) $G_i = G_{q^l}$ для $q^l \leq i < q^{l+1}$.

ЗАМЕЧАНИЕ 1. На самом деле имеет место равенство

$$U_K^{(n)} = N_{L_n/K}(U_{L_n}).$$

Включение $U_K^{(n)} \leq N_{L_n/K}(U_{L_n})$ вытекает из следствия П1 (см. приложение), так как $U_K^{(n)} = U_K^{(\gamma^+)}$ для $\gamma = \varepsilon_{F_n} - v(\pi) = (n-1)v(\pi)$. Обратное включение было установлено элементарными средствами в работе [5, теорема 6.5]. Однако, как будет указано ниже, достаточное для этого неравенство $[L_n : K] \leq [U_K : N_{L_n/K}(U_{L_n})]$ вытекает из абстрактной теории полей классов [1] (см. предложение 6 ниже).

Докажем, что расширение Любина–Тейта не зависит от выбора ЛТ-многочлена.

ПРЕДЛОЖЕНИЕ 3. Пусть $g = x^q + a_1 x^{q-1} + \dots + a_{q-2} x^2 + \pi x$ – произвольный ЛТ-многочлен. Тогда $L_{g,n} = L_n$ для любого $n \in \omega^+$.

ДОКАЗАТЕЛЬСТВО. Достаточно установить, что $G_n = g^{(n)}(g^{(n-1)})^{-1}$ имеет корень в L_n (тогда $L_{g,n} \leq L_n$ и $[L_{g,n} : K] = (q-1)q^{n-1} = [L_n : K]$ влечет $L_{g,n} = L_n$).

Пусть $m \in \omega$ такое, что

$$\frac{m}{(q-1)q^{n-1}}v(\pi) > \max\{\varepsilon_{G_n}, \varepsilon_{F_n}\} + \frac{1}{q-1}v(\pi).$$

Пусть α – корень многочлена F_n . Рассмотрим многочлен $[1]_{g,f}^m$ и элемент $a = [1]_{g,f}^m(\alpha) \in L_n$. Имеем $g^{(n)} \circ [1]_{g,f}^m \equiv_m [1]_{g,f}^m \circ f^{(n)}$; тогда

$$g^{(n)}(a) = (g^{(n)} \circ [1]_{g,f}^m)(\alpha) = g^{(n)} \circ [1]_{g,f}^m(\alpha) - [1]_{g,f}^m \circ f^{(n)}(\alpha) \in \alpha^{m+1}O_{L_n}$$

и, следовательно,

$$v(g^{(n)}(a)) > mv(\alpha) = \frac{m}{(q-1)q^{n-1}}v(\pi) > \varepsilon_{G_n} + \frac{1}{q-1}v(\pi).$$

Аналогично, $g^{(n-1)}(a) - ([1]_{g,f}^m \circ f^{(n-1)})(\alpha) \in \alpha^{m+1}O_{L_n}$. Поскольку $F_n(\alpha) = (f^{(n-1)}(\alpha))^{q-1} + \pi = 0$, то

$$v(f^{(n-1)}(\alpha)) = \frac{1}{q-1}v(\pi), \quad [1]_{g,f}^m \circ f^{(n-1)}(\alpha) = f^{(n-1)}(\alpha) + f^{(n-1)}(\alpha)^2b$$

для подходящего $b \in O_{L_n}$. Следовательно,

$$v([1]_{g,f}^m \circ f^{(n-1)}(\alpha)) = v(f^{(n-1)}(\alpha)) = \frac{1}{q-1}v(\pi) < \frac{m}{(q-1)q^{n-1}}v(\pi);$$

отсюда $v(g^{(n-1)}(a)) = \frac{1}{q-1}v(\pi)$. Имеем

$$v(G_n(a)) = v(g^{(n)}(a)(g^{(n-1)}(a))^{-1}) = v(g^{(n)}(a)) - v(g^{(n-1)}(a)) > \varepsilon_{G_n}.$$

По теореме [П2](#) многочлен G_n имеет корень $\beta \in L_n$ такой, что $v(\beta - a) > \varkappa_{G_n}$. Итак, $L_{g,n} = K(\beta) = L_n$. Предложение доказано.

Опишем, как действует автоморфизм σ_u поля $L_n = L_{g,n}$, $u \in U_K$, определенный в доказательстве теоремы [1](#), на корни многочлена G_n .

Заметим, что $[u]_{g,g} = [1]_{g,f} \circ [u]_{f,f} \circ [1]_{f,g}$; действительно, полагая $\overline{[u]} \equiv [1]_{g,f} \circ [u]_{f,f} \circ [1]_{f,g}$, имеем

$$\begin{aligned} g \circ \overline{[u]} &= g \circ [1]_{g,f} \circ [u]_{f,f} \circ [1]_{f,g} = [1]_{g,f} \circ f \circ [u]_{f,f} \circ [1]_{f,g} \\ &= [1]_{g,f} \circ [u]_{f,f} \circ f \circ [1]_{f,g} = [1]_{g,f} \circ [u]_{f,f} \circ [1]_{f,g} \circ g = \overline{[u]} \circ g. \end{aligned}$$

Так как коэффициент при x в ряде $\overline{[u]}$ равен u , то из единственности следует $\overline{[u]} = [u]_{g,g}$.

Пусть α – корень многочлена F_n , $m \in \omega$ таково, что

$$mv(\alpha) = \frac{m}{(q-1)q^{n-1}}v(\pi) > \max\{\varepsilon_{G_n}, \varepsilon_{F_n}\} + \frac{1}{q-1}v(\pi),$$

и пусть β – единственный корень многочлена G_n такой, что $v(\beta - \bar{\beta}) > \varkappa_{G_n}$, где $\bar{\beta} \equiv [1]_{g,f}^m(\alpha)$. Заметим, что (из доказательства теоремы 1)

$$v(\sigma_u \alpha - [u]_{f,f}^m(\alpha)) > mv(\alpha) - \frac{1}{q-1}v(\pi) \geq \max\{\varepsilon_{G_n}, \varepsilon_{F_n}\}$$

для любого $u \in U_K$.

ПРЕДЛОЖЕНИЕ 4. Для любого $u \in U_K$ корень $\beta' \equiv \sigma_u \beta$ является единственным корнем многочлена G_n , удовлетворяющим условию

$$v(\beta' - [u]_{g,g}^m(\beta)) > \varkappa_{G_n}.$$

ДОКАЗАТЕЛЬСТВО. Заметим, что $v(\beta - \bar{\beta}) = v(\sigma_u(\beta - \bar{\beta})) = v(\sigma_u \beta - \sigma_u \bar{\beta}) > \varepsilon_{G_n}$. Далее, $\sigma_u \bar{\beta} = \sigma_u [1]_{g,f}^m(\alpha) = [1]_{g,f}^m(\sigma_u \alpha)$. Как было отмечено выше, $v(\sigma_u \alpha - [u]_{f,f}^m \alpha) > \varepsilon_{G_n}$; тогда

$$v([1]_{g,f}^m(\sigma_u \alpha) - [1]_{g,f}^m \circ [u]_{f,f}^m(\alpha)) > \varepsilon_{G_n}, \quad [1]_{g,f}^m \circ [u]_{f,f}^m \equiv^m [u]_{g,g}^m \circ [1]_{g,f}^m,$$

следовательно,

$$[u]_{g,g}^m \circ [1]_{g,f}^m(\alpha) = [u]_{g,g}^m(\bar{\beta}), \quad v([1]_{g,f}^m \circ [u]_{f,f}^m(\alpha) - [u]_{g,g}^m(\bar{\beta})) > mv(\alpha) \geq \varkappa_{G_n}.$$

Итак, имеем неравенства

$$\begin{aligned} v(\sigma_u \beta - \sigma_u \bar{\beta}) &> \varepsilon_{G_n} \geq \varkappa_{G_n}, \\ v(\sigma_u \bar{\beta} - [1]_{g,f}^m \circ [u]_{f,f}^m(\alpha)) &> \varepsilon_{G_n} \geq \varkappa_{G_n}, \\ v([1]_{g,f}^m \circ [u]_{f,f}^m(\alpha) - [u]_{g,g}^m(\bar{\beta})) &> \varkappa_{G_n}, \\ v(\beta - \bar{\beta}) &> \varkappa_{G_n}, \quad v([u]_{g,g}^m(\beta) - [u]_{g,g}^m(\bar{\beta})) > \varkappa_{G_n}. \end{aligned}$$

Отсюда $v(\sigma_u \beta - [u]_{g,g}^m(\beta)) > \varkappa_{G_n}$ и $\sigma_u \beta$ – единственный корень β' многочлена G_n такой, что $v(\beta' - [u]_{g,g}^m(\beta)) > \varkappa_{G_n}$.

До настоящего момента простой элемент $\pi \in O_K$ был фиксирован. Рассмотрим другой простой элемент $\bar{\pi} = \pi u$, $u \in U_K$. Расширение Любина–Тейта степени n , относящееся к простому π ($\bar{\pi}$), будем обозначать $L_{\pi,n}$ ($L_{\bar{\pi},n}$).

Изучим взаимоотношение расширений $L_{\pi,n}$ и $L_{\bar{\pi},n}$.

ПРЕДЛОЖЕНИЕ 5. Если $u \in U^{(n)}$, то $L_{\pi,n} = L_{\bar{\pi},n}$.

ДОКАЗАТЕЛЬСТВО. Пусть $f_\pi = x^q + \pi x$, $f_{\bar{\pi}} = x^q + \bar{\pi} x$; из условия, налагаемого на u , следует, что $f_\pi \equiv^n f_{\bar{\pi}}$. Действительно,

$$\begin{aligned} f_\pi - f_{\bar{\pi}} &= x^q + \pi x - x^q - \bar{\pi} x = \pi(1 - u)x, \\ v(\pi(1 - u)) &= v(\pi) + v(1 - u) \geq (n+1)v(\pi) > nv(\pi). \end{aligned}$$

Тогда

$$\begin{aligned} f_\pi^{(n-1)} &\equiv^n f_{\bar{\pi}}^{(n-1)}, \\ F_{\pi,n} &= (f_\pi^{(n-1)})^{q-1} + \pi \equiv^n (f_{\bar{\pi}}^{(n-1)})^{q-1} + \bar{\pi} = F_{\bar{\pi},n}. \end{aligned}$$

Пусть α – корень многочлена $F_{\pi,n}$; тогда

$$v(F_{\bar{\pi},n}(\alpha)) = v(F_{\bar{\pi},n}(\alpha) - F_{\pi,n}(\alpha)) > nv(\pi) = \varepsilon_{F_{\bar{\pi}}}.$$

Отсюда по теореме П2 в $L_{\pi,n} = K(\alpha)$ найдется корень многочлена $F_{\bar{\pi},n}$, следовательно, $L_{\bar{\pi},n} \leq L_{\pi,n}$ и, симметрично, $L_{\pi,n} \leq L_{\bar{\pi},n}$.

Если поле K полно относительно нормирования v , то K – классическое локальное поле и для него справедлива классическая локальная теория полей классов. В частности, для любого конечного расширения Галуа $L \geq K$ определен гомоморфизм взаимности $r_L: G(L/K) \rightarrow K^\times / N_{L/K}(L^\times)$, который индуцирует изоморфизм групп $G(L/K)^{\text{ab}} = G(L/K)/[G(L,K), G(L,K)]$ и $K^\times / N_{L/K}(L^\times)$. Это означает, что ядром гомоморфизма r_L является коммутант группы $G(L/K)$ и r_L является эпиморфизмом.

Однако абстрактная теория полей классов, предложенная Нейкирхом [1] (другие изложения этой теории см. в [6]–[8]), позволяет определять единообразно гомоморфизмы взаимности и в более общей ситуации. Так, если $\langle F, R \rangle$ – гензелево дискретно нормированное поле такое, что поле вычетов F_R совершенно, а его абсолютная группа Галуа $G(F_R)$ изоморфна группе $\widehat{\mathbb{Z}}$ (это имеет место в случае, например, когда F_R конечно), то для любого конечного расширения Галуа $F' \geq F$ определен гомоморфизм взаимности

$$r_{F'/F}: G(F'/F) \rightarrow F'^\times / N_{F'/F}(F'^\times),$$

ядром которого является коммутант группы $G(F'/F)$ (так что $r_{F'/F}$ индуцирует вложение $\bar{r}_{F'/F}: G(F'/F)^{\text{ab}} \rightarrow F'^\times / N_{F'/F}(F'^\times)$). Гомоморфизм $r_{F'/F}$ является изоморфизмом $G(F'/F)$ и $F'^\times / N_{F'/F}(F'^\times)$ в случае, когда F' – неразветвленное расширение F , и в общем случае если $I \leq G(F'/F)$ – группа инерции, то имеет место

$$r_{F'/F}(I) \leq U_F / N_{F'/F}(U_{F'}) \leq F'^\times / N_{F'/F}(F'^\times).$$

Здесь U_F ($U_{F'}$) – группа единиц кольца R (R' – кольцо нормирования поля F' , доминирующее R , $R' \cap F = R$).

Отображения взаимности обладают рядом хороших функторных свойств. Например, если $F \leq F'' \leq F'$, F' и F'' – конечные расширения Галуа, то коммутативна диаграмма

$$\begin{array}{ccc} G(F'/F) & \longrightarrow & G(F''/F) \\ r_{F'/F} \downarrow & & \downarrow r_{F''/F} \\ F'^\times / N_{F'/F}(F'^\times) & \longrightarrow & F''^\times / N_{F''/F}(F''^\times) \end{array} \quad (2)$$

где верхняя горизонтальная стрелка – эпиморфизм ограничения, а нижняя индуцирована включением

$$N_{F'/F}(F'^\times) = N_{F''/F} N_{F'/F''}(F'^\times) \leq N_{F''/F}(F''^\times).$$

Не давая точного определения и не указывая все свойства гомоморфизмов взаимности, получим ряд следствий из уже указанных свойств.

ПРЕДЛОЖЕНИЕ 6. *Имеет место равенство $N_{L_n/K}(U_{L_n}) = U_K^{(n)}$.*

ДОКАЗАТЕЛЬСТВО. Действительно, так как L_n – абелево вполне разветвленное расширение поля K , то гомоморфизм взаимности $r_{L_n/K}$ определяет вложение $G(L_n/K) \rightarrow U_K/N_{L_n/K}(U_{L_n})$, так как группа $G(L_n/K)$ абелева и совпадает со своей группой инерции. Отсюда получаем соотношения

$$(q-1)q^{n-1} = |G(L_n/K)| \leq |U_K/N_{L_n/K}(U_{L_n})|,$$

вместе с равенством $(q-1)q^{n-1} = |U_K/U_K^{(n)}|$ и включением $U_K^{(n)} \leq N_{L_n/K}(U_{L_n})$, отмеченным в замечании 1, получим равенство $N_{L_n/K}(U_{L_n}) = U_K^{(n)}$.

ПРЕДЛОЖЕНИЕ 7. *Пусть $M \geq K$ – вполне разветвленное конечное расширение Галуа поля K такое, что $N_{M/K}(U_M) \geq U_K^{(n)}$. Тогда $L_n M$ является неразветвленным расширением L_n .*

ДОКАЗАТЕЛЬСТВО. Пусть $G = G(L_n M/K)$, $G_0 = G(L_n/K)$, $G_1 = G(M/K)$. Гомоморфизмы ограничения $G \rightarrow G_0$, $G \rightarrow G_1$ индуцируют вложение группы G в прямое произведение $G_0 \times G_1$. Пусть I – подгруппа инерции группы G ; группы G_0 и G_1 совпадают со своими подгруппами инерции.

Из коммутативности диаграммы (2) и свойств гомоморфизма взаимности вытекает коммутативность диаграмм

$$\begin{array}{ccc} I & \longrightarrow & G_0 \\ \downarrow & & \downarrow \\ U_K/N_{L_n M/K}(U_{L_n M}) & \longrightarrow & U_K/N_{L_n/K}(U_{L_n}) \end{array} \quad (3)$$

$$\begin{array}{ccc} I & \longrightarrow & G_1 \\ \downarrow & & \downarrow \\ U_K/N_{L_n M/K}(U_{L_n M}) & \longrightarrow & U_K/N_{M/K}(U_M) \end{array} \quad (4)$$

Покажем, что гомоморфизм ограничения $p_0: I \rightarrow G_0$ является вложением. Предположим, что $\tau \in I$ и $p_0(\tau) = 1$; тогда диаграмма (3) показывает, что $r_{L_n M/K}(\tau) \in N_{L_n/K}(U_{L_n})$, однако $N_{L_n/K}(U_{L_n}) = U_K^{(n)} \leq N_{M/K}(U_M)$. Поэтому диаграмма (4) показывает, что $p_1(\tau) = 1$. Но $(p_0, p_1): G \rightarrow G_0 \times G_1$ является вложением и $I \leq G$, следовательно, $\tau = 1$ и p_0 является вложением. Отсюда $|I| \leq |G_0|$. Однако порядок группы инерции является индексом ветвления $e(L_n M/K)$ расширения $L_n M \geq K$, который не меньше индекса ветвления $e(L_n/K)$ расширения $L_n \geq K$, равного $|G_0|$. Отсюда $|I| = |G_0|$, и из мультипликативности индекса ветвления $e(L_n M/K) = e(L_n M/L_n)e(L_n/K)$ следует, что $e(L_n M/L_n) = 1$, т. е. расширение $L_n M \geq L_n$ не разветвлено.

СЛЕДСТВИЕ 3. *Пусть $u \in U_K$, $\bar{\pi} \equiv \pi u$. Тогда для любого $n \in \omega^+$ композит $L_{\pi, n} L_{\bar{\pi}, n}$ является неразветвленным расширением как $L_{\pi, n}$, так и $L_{\bar{\pi}, n}$.*

Важным следствием предложения 7 является описание наибольшего абелева расширения поля K . Пусть L_u – наибольшее неразветвленное расширение поля K ; тогда $G(L_u/K) \simeq \hat{\mathbb{Z}} = G(k)$ и L_u – абелево расширение поля K . Пусть

$L_\pi = \bigcup_{n \in \omega^+} L_{\pi,n}$ – объединение абелевых вполне разветвленных расширений $L_{\pi,n} \geq K$, $n \in \omega^+$, поля K . Тогда L_π – абелево расширение поля K , линейно разделенное с L_u , и

$$G(L_\pi/K) \simeq \varprojlim_{n \in \omega^+} U_K/U_K^{(n)}.$$

ТЕОРЕМА 2. *Композит $L_u L_\pi = L_u \otimes_K L_\pi$ является наибольшим абелевым расширением поля K , и*

$$G(L_u L_\pi/K) \simeq \widehat{\mathbb{Z}} \times \varprojlim_{n \in \omega^+} U_K/U_K^{(n)}.$$

ДОКАЗАТЕЛЬСТВО. Пусть $L \geq K$ – произвольное конечное абелево расширение поля K , $I \leq G(L/K)$ – группа инерции, $l = |I|$. Пусть $L_{u,l}$ – неразветвленное расширение поля K степени $l = [L_{u,l} : K]$. Тогда нетрудно проверить, что группа Галуа $G(L'/K)$ поля $L' = LL_{u,l}$ расщепляется:

$$G(L'/K) = \langle \varphi \rangle \times I,$$

где I – группа инерции, φ – автоморфизм Фробениуса. Пусть $L'' = (L')^{\langle \varphi \rangle}$; тогда L'' – абелево вполне разветвленное расширение поля K и $L' = L'' L_{u,l} \geq L$. Поэтому для доказательства включения $L \leq L_u L_\pi$ достаточно предположить, что L – вполне разветвленное расширение поля K .

ЛЕММА 5. *Для любого конечного сепарабельного расширения $L \geq K$ существует $n \in \omega^+$ такое, что $N_{L/K}(U_L) \geq U_K^{(n)}$.*

ДОКАЗАТЕЛЬСТВО. Лемма сразу вытекает из следствия П1 (см. приложение).

Возвращаемся к доказательству теоремы. Пусть L – конечное вполне разветвленное абелево расширение K . По лемме 5 существует $n \in \omega^+$ такое, что $N_{L/K}(U_L) \geq U_K^{(n)}$, но тогда по предложению 7 композит $LL_{\pi,n}$ является неразветвленным расширением $L_{\pi,n}$. Отсюда, как в начале доказательства, следует $L \leq LL_{\pi,n} \leq L_u L_{\pi,n} \leq L_u L_\pi$, что и требовалось получить. (Описание группы Галуа $G(L_u L_\pi/K)$ следует из рассуждений, проведенных перед теоремой.)

ЗАМЕЧАНИЕ 2. Из теоремы 2 и предложения 6 следует, что для поля K гомоморфизм взаимности индуцирует изоморфизм $G(L/K)^{\text{ab}} \xrightarrow{\sim} K^\times / N_{L/K}(L^\times)$ для любого конечного расширения Галуа $L \geq K$. Это известно для классических локальных полей, так как “классический” гомоморфизм взаимности совпадает с гомоморфизмом взаимности, определенным с помощью абстрактной теории полей классов [1]. Однако важно заметить, что в приведенном доказательстве не использовался тот факт, что поле L_u имеет кохомологическую размерность не более 1 (см. [1], [3], [8]).

Снова рассмотрим расширения $L_n = L_{\pi,n} \geq K$. Имеются изоморфизмы

$$\begin{aligned} \sigma: U_K/U_K^{(n)} &\xrightarrow{\sim} G_{L_n/K}, \\ r_{L_n/K}: G_{L_n/K} &\xrightarrow{\sim} U_K/N_{L_n/K}(U_{L_n}) \leq K^\times / N_{L_n/K}(L_n^\times) \end{aligned}$$

и равенство $U_K^{(n)} = N_{L_n/K}(U_{L_n})$. В каком отношении находятся эти изоморфизмы? Следующая теорема отвечает на этот вопрос.

ТЕОРЕМА 3. Для любого $u \in U_K$

$$r_{L_n/K}(\sigma_{u^{-1}}) = uN_{L_n/K}(L_n^\times).$$

ДОКАЗАТЕЛЬСТВО. Для доказательства теоремы необходимо знать, как определяется $r_{L_n/K}(\sigma)$ для $\sigma \in G(L_n/K)$. Не приводя общие определения из [1], [6], [7], укажем более конкретный путь. Пусть M – неразветвленное расширение поля K степени $(q-1)q^n$, и пусть φ – автоморфизм Фробениуса, т. е. такой K -автоморфизм M , что $\overline{\varphi a} = \overline{a^q}$ для $a \in O_M$, φ порождает группу $G(M/K) = \langle \varphi \rangle$. Композит $\overline{M} = ML_n$ является абелевым расширением поля K , и группа $G(\overline{M}/K)$ естественно изоморфна группе $\langle \varphi \rangle \times G(L_n/K)$. Элементом Фробениуса группы $G(ML_n/K)$ назовем всякий элемент вида $\varphi' = \varphi\tau$, $\tau \in G(L_n/K)$. Для всякого элемента Фробениуса $\varphi' = \varphi\tau$ поле $\overline{M}^{(\varphi')}$ является вполне разветвленным расширением поля K . Если α' – простой элемент кольца $O_{\overline{M}^{(\varphi')}}/K$, то $r_{\overline{M}/K}(\varphi') = N_{\overline{M}^{(\varphi')}/K}(\alpha')N_{\overline{M}/K}(\overline{M}^\times)$. Так как $r_{\overline{M}/K}$ – гомоморфизм, то $r_{\overline{M}/K}(\varphi') = r_{\overline{M}/K}(\varphi\tau) = r_{\overline{M}/K}(\varphi)r_{\overline{M}/K}(\tau)$; отсюда

$$r_{\overline{M}/K}(\tau) = N_{\overline{M}^{(\varphi')}/K}(\alpha')N_{\overline{M}^{(\varphi)}/K}(\alpha'^{-1})N_{\overline{M}/K}(\overline{M}^\times),$$

где $\alpha \in L_n$ – корень многочлена F_n , α – простой элемент кольца O_{L_n} и $L_n = \overline{M}^{(\varphi)}$. Поскольку $N_{\overline{M}^{(\varphi')}/K}(\alpha')$ и $N_{L_n/K}(\alpha) = \pm\pi$ являются простыми элементами кольца O_K , то

$$\begin{aligned} u &= N_{\overline{M}^{(\varphi')}/K}(\alpha')N_{L_n/K}(\alpha'^{-1}) \in U_K, \\ r_{L_n/K}(\tau) &= uN_{L_n/K}(U_{L_n}) \end{aligned}$$

(по определению). Таким образом, чтобы вычислить $r_{L_n/K}(\sigma_{u^{-1}})$, необходимо найти подходящий простой элемент α' поля $\overline{M}^{(\varphi\sigma_{u^{-1}})}$ и определить $N_{\overline{M}^{(\varphi\sigma_{u^{-1}})}/K}(\alpha')$. Сделаем это, проведя предварительные рассуждения.

ПРЕДЛОЖЕНИЕ 8. Для любого элемента $u \in U_K$ существует элемент $\varepsilon \in U_M$ такой, что $u\varepsilon^{\varphi-1} \in U_M^{(n+1)}$ и, следовательно, $v(\varepsilon^{\varphi-1} - u) \geq (n+1)v(\pi)$.

ДОКАЗАТЕЛЬСТВО. Докажем сначала две вспомогательные леммы.

ЛЕММА 6. Пусть поле F характеристики $p > 0$ имеет единственное сепарабельное расширение $F_n \geq F$ степени n для любого $n \in \omega^+$ и F содержит подполе F' из $q = p^l$, $l \in \omega^+$, элементов. Тогда для любого элемента a из F уравнение $x^q - x - a = 0$ имеет решение в поле F_q .

ДОКАЗАТЕЛЬСТВО. Пусть $\prod_{i < k} f_i(x)$ – разложение многочлена $f(x) = x^q - x - a$ на неприводимые множители над F . Пусть α_i – какой-нибудь корень многочлена f_i (в алгебраическом замыкании $\overline{F}$ поля F), $i < k$; тогда $\alpha_i + \varepsilon$, $\varepsilon \in F'$, – это все корни многочлена f , следовательно, $F(\alpha_0) = F(\alpha_1) = \dots = F(\alpha_{n-1})$. Однако $[F(\alpha_i) : F] = \deg f_i$ – степень f_i ; тогда $q = (q')^k$, где $q' = \deg f_0 = \dots = \deg f_{k-1}$, следовательно, q' делит q , $[F(\alpha_0) : F] = q'$ влечет, что $F(\alpha_0) = F_{q'} \leq F_q$.

ЛЕММА 7. Пусть $M \geq L > K$ – неразветвленное расширение, $K \leq L' < L$ – промежуточное поле такое, что $[L : L'] = q$. Тогда для любых $k > 0$, $u \in U_L^{(k)}$ найдется $v \in U_L^{(k)}$ такой, что $uv^{1-\varphi} \in U_L^{(k+1)}$, где φ – автоморфизм Фробениуса.

ДОКАЗАТЕЛЬСТВО. Если $v = 1 + \pi^k b \in U_L^{(k)}$, $b \in O_L$, то $v^{-1} \equiv 1 - \pi^k b \pmod{\pi^{k+1}}$ и $v^\varphi \equiv 1 + \pi^k b^q \pmod{\pi^{k+1}}$. Пусть $u = 1 + \pi^k a \in U_L^{(k)}$, $a \in O_L$. Найдем в O_L элемент b такой, что $b^q - b - a = 0$. Это можно сделать, используя лемму 6 и лемму Гензеля.

Полагаем $v \equiv 1 + b\pi^k$, $v \in U_L^{(k)}$; имеем

$$\begin{aligned} uv^{1-\varphi} &= (1 + \pi^k a)(1 + \pi^k b)((1 + \pi^k b)^\varphi)^{-1} \equiv (1 + \pi^k a)(1 + \pi^k b)(1 - \pi^k b^q) \\ &\equiv 1 + (a + b - b^q)\pi^k \equiv 1 \pmod{\pi^{k+1}}, \end{aligned}$$

т. е. $uv^{1-\varphi} \in U_L^{(k+1)}$.

Продолжим теперь доказательство предложения.

Существуют подполя $(K <)M^0$, $(K =)M_0 < M_1 < M_2 < \dots < M_n$ поля M такие, что $[M^0 : K] = q - 1$, $[M_i : K] = q^i$, $i = 0, 1, \dots, n$, следовательно, $[M_{i+1} : M_i] = q$, $0 \leq i < n$. Тогда $M = M^0 M_n$.

Элемент $u \in U_K$ представим в виде $u = u^0 u_0$, где $u^0 \in A$, $u_0 \in U_K^{(1)}$. Из условия для M^0 следует, что в мультипликативной группе представителей A^0 поля вычетов поля M^0 найдется элемент η такой, что $\eta^{q-1} = u^0$. Заметим, что $\eta^\varphi = \eta^q$, $\eta^{\varphi-1} = \eta^{q-1}$ и $u^0 \eta^{1-\varphi} = 1$.

Далее, используя лемму 7, находим элементы $u_k \in U_{M_k}^{(k)}$ такие, что $u_0 u_k^{1-\varphi} \in U_{M_k}^{(k+1)}$, $k < n$. Действительно, если найден $u_k \in U_{M_k}^{(k)}$, $k < n$, такой, что $u_0 u_k^{1-\varphi} \in U_{M_k}^{(k+1)}$, то в $U_{M_k}^{(k+1)}$ найдется элемент v_{k+1} такой, что $(u_0 u_k^{1-\varphi})v_{k+1}^{1-\varphi} \in U_{M_{k+1}}^{(k+2)}$. Тогда для $u_{k+1} \equiv u_k v_{k+1}$ имеем $u_0 u_{k+1}^{1-\varphi} = u_0 u_k^{1-\varphi} v_{k+1}^{1-\varphi} \in U_{M_{k+1}}^{(k+2)}$.

Полагаем теперь $\varepsilon \equiv \eta u_n$; тогда

$$u\varepsilon^{1-\varphi} = u^0 u_0 \eta^{1-q} u_n^{1-\varphi} = u_0 u_n^{1-\varphi} \in U_{M_n}^{(n+1)} \leq U_M^{(n+1)}.$$

Предложение доказано.

Пусть $u \in U_K$, $\bar{\pi} \equiv \pi u$, $\bar{f} \equiv x^q + \bar{\pi}x$; по предложению 8 существует элемент $\varepsilon \in U_M$ такой, что $v(\varepsilon^{\varphi-1} - u) \geq (n+1)v(\pi)$.

ПРЕДЛОЖЕНИЕ 9. Для любого $t \geq 1$ существует многочлен

$$\Theta_m(x) = \varepsilon_1 x + \dots + \varepsilon_m x^m \in xO_M[x]$$

степени не более t такой, что $\varepsilon_1 = \varepsilon$, $\varepsilon_i = 0$ для $1 < i < q$ и $\bar{f} \circ \Theta_m \equiv_m^n \Theta_m^\varphi \circ f$.

ДОКАЗАТЕЛЬСТВО проведем индукцией по t . Пусть $1 \leq t < q$, $\Theta_m(x) \equiv \varepsilon x$; тогда $\bar{f} \circ \Theta_m(x) = (\varepsilon x)^q + \bar{\pi} \varepsilon x \equiv_m \bar{\pi} \varepsilon x = \pi \varepsilon x \equiv_m^n \pi \varepsilon^\varphi x$, так как

$$\begin{aligned} v(u - \varepsilon^{\varphi-1}) &\geq (n+1)v(\pi), & v(u\varepsilon - \varepsilon^\varphi) &= v(u - \varepsilon^{\varphi-1}) \geq (n+1)v(\pi), \\ \Theta_m^\varphi(x) \circ f &= \varepsilon^\varphi(x^q - \pi x) \equiv_m^n \varepsilon^\varphi \pi x. \end{aligned}$$

Итак, $\bar{f} \circ \Theta_m(x) \equiv_m^n \Theta_m^\varphi \circ f$.

Пусть для $m \geq q - 1$ существует многочлен

$$\Theta_m(x) = \varepsilon x + \varepsilon_2 x^2 + \dots + \varepsilon_m x^m \in O_M[x],$$

удовлетворяющий условиям $\varepsilon_2 = \dots = \varepsilon_{q-1} = 0$ и $\bar{f} \circ \Theta_m \equiv_m^n \Theta_m^\varphi \circ f$. Будем искать $\Theta_{m+1}(x)$ в виде $\Theta_m(x) + \varepsilon_{m+1}x^{m+1}$.

Имеем

$$\begin{aligned} \bar{f} \circ \Theta_{m+1} &= \Theta_{m+1}^q + \bar{\pi} \Theta_{m+1} = (\Theta_m + \varepsilon_{m+1}x^{m+1})^q + \bar{\pi} \Theta_{m+1} \\ &\equiv_{m+1} \Theta_m^q + \bar{\pi} \Theta_{m+1}, \\ \Theta_m^q &= \left(\sum_{i=1}^m \varepsilon_i x^i \right)^q = \sum_{i=1}^m \varepsilon_i^q x^{qi} + \pi P_m(x, \bar{\varepsilon}), \end{aligned}$$

где

$$P_m(x, \bar{\varepsilon}) = \sum_{i=1}^{mq-1} \varepsilon_i' x^i \in xO_M[x, \varepsilon_1, \dots, \varepsilon_m]$$

(и коэффициенты $\varepsilon_i' = P_{m,i}(\varepsilon_1, \dots, \varepsilon_m)$ многочлена P_m не зависят от ε_{m+1}).

Тогда коэффициентом при x^{m+1} многочлена $\Theta_m^q + \pi \Theta_{m+1}$ будет $\pi \varepsilon_{m+1}' + \pi u \varepsilon_{m+1}$, если $m+1$ не делится на q , и $\varepsilon_{m+1}^q + \pi \varepsilon_{m+1}' + \pi u \varepsilon_{m+1}$, если $m+1$ делится на q и $m+1 = qm'$.

Далее,

$$\begin{aligned} \Theta_{m+1}^\varphi \circ f &= \Theta_m^\varphi \circ f + \varepsilon_{m+1}^\varphi f^{m+1} = \Theta_m^\varphi \circ f + \varepsilon_{m+1}^\varphi (x^q + \pi x)^{m+1} \\ &\equiv_{m+1} \Theta_m^\varphi \circ f + \varepsilon_{m+1}^\varphi \pi^{m+1} x^{m+1}, \\ \Theta_m^\varphi \circ f &= \sum_{i=1}^m \varepsilon_i^\varphi (x^q + \pi x)^i = \sum_{i=1}^m \varepsilon_i^\varphi x^{qi} + \pi Q_m(x, \bar{\varepsilon}^\varphi), \end{aligned}$$

где многочлен

$$\begin{aligned} Q_m(x, \bar{\varepsilon}^\varphi) &= \sum_{i=1}^{mq-1} \varepsilon_i'' x^i \in xO_M[x, \varepsilon_1^\varphi, \dots, \varepsilon_m^\varphi], \\ \varepsilon_i'' &= Q_{m,i}(\varepsilon_1^\varphi, \dots, \varepsilon_m^\varphi), \quad i < mq. \end{aligned}$$

Тогда коэффициентом при x^{m+1} многочлена $\Theta_m^\varphi \circ f + \pi^{m+1} \varepsilon_{m+1}^\varphi x^{m+1}$ будет $\pi \varepsilon_{m+1}'' + \pi^{m+1} \varepsilon_{m+1}^\varphi$, если q не делит $m+1$, и $\varepsilon_{m+1}^\varphi + \pi \varepsilon_{m+1}'' + \pi^{m+1} \varepsilon_{m+1}^\varphi$, если q делит $m+1$ и $m+1 = qm'$.

Итак, задача состоит в нахождении элемента $\varepsilon_{m+1} \in O_M$ такого, что

$$v(\pi \varepsilon_{m+1}' + \pi u \varepsilon_{m+1} - \pi \varepsilon_{m+1}'' - \pi^{m+1} \varepsilon_{m+1}^\varphi) \geq (n+1)v(\pi),$$

если q не делит $m+1$, и

$$v(\varepsilon_{m+1}^q + \pi \varepsilon_{m+1}' + \pi u \varepsilon_{m+1} - \varepsilon_{m+1}^\varphi - \pi \varepsilon_{m+1}'' - \pi^{m+1} \varepsilon_{m+1}^\varphi) \geq (n+1)v(\pi),$$

если q делит $m+1$ и $m+1 = qm'$.

Следует заметить, что $v(a^q - a^\varphi) \geq v(\pi)$ для любого элемента $a \in O_M$. Действительно, если $v(a) > 0$, то $v(a) \geq v(\pi)$, так как M – неразветвленное расширение поля K . Если же $v(a) = 0$, то $\bar{a}^\varphi = \bar{a}^q$ влечет $v(a^q - a^\varphi) > 0$ и $v(a^q - a^\varphi) \geq v(\pi)$, так как $a^\varphi - a^q \in O_M$.

Теперь установим лемму, из которой будет следовать существование искомого элемента ε_{m+1} .

ЛЕММА 8. Пусть $a, b \in O_M$, $v(a) > 0$ ($v(a) \geq v(\pi)$). Тогда для любого $l \in \omega$ существует элемент $c \in O_M$ такой, что $v(c - ac^\varphi - b) > lv(\pi)$.

ДОКАЗАТЕЛЬСТВО. Пусть $c_0 \equiv b$; тогда

$$v(c_0 - ac_0^\varphi - b) = v(ab^\varphi) = v(a) + v(b^\varphi) \geq v(\pi).$$

Если для $l \in \omega$ элемент $c_l \in O_M$ таков, что $v(c_l - ac_l^\varphi - b) > lv(\pi)$, то для $b_l \equiv c_l - ac_l^\varphi - b$ полагаем $c_{l+1} \equiv c_l - b_l$. Тогда

$$\begin{aligned} c_{l+1} - ac_{l+1}^\varphi - b &= c_l - b_l - a(c_l^\varphi - b_l^\varphi) - b = c_l - ac_l^\varphi - b - (b_l - ab_l^\varphi) \\ &= b_l - b_l + ab_l^\varphi = ab_l^\varphi, \\ v(ab_l^\varphi) &= v(a) + v(b_l) \geq v(b_l) + v(\pi); \end{aligned}$$

отсюда $v(c_{l+1} - ac_{l+1}^\varphi - b) > (l+1)v(\pi)$. Лемма доказана.

Завершаем доказательство предложения. Имеются два случая.

Случай 1: q не делит $m+1$. Полагая $a \equiv \pi^m$ и $b \equiv \varepsilon^\varphi(\varepsilon''_{m+1} - \varepsilon'_{m+1})$, находим по лемме 8 элемент $c \in O_M$ такой, что $v(c - ac^\varphi - b) \geq nv(\pi)$. Полагаем $\varepsilon_{m+1} \equiv \varepsilon^{-1}c$ и проверим, что

$$\begin{aligned} v(\pi\varepsilon'_{m+1} + \pi u\varepsilon_{m+1} - \pi\varepsilon''_{m+1} - \pi^{m+1}\varepsilon_{m+1}^\varphi) &\geq (n+1)v(\pi), \\ u\varepsilon_{m+1} - \pi^m\varepsilon_{m+1}^\varphi + (\varepsilon'_{m+1} - \varepsilon''_{m+1}) &= u\varepsilon^{-1}c - \pi^m(\varepsilon^{-1}c)^\varphi + (\varepsilon'_{m+1} - \varepsilon''_{m+1}) \\ &\equiv^{n-1} \varepsilon^{1-\varphi}\varepsilon^{-1}c - \varepsilon^{-\varphi}\pi^m c^\varphi + (\varepsilon'_{m+1} - \varepsilon''_{m+1}) \\ &= \varepsilon^{-\varphi}(c - \pi^m c^\varphi + \varepsilon^\varphi(\varepsilon'_{m+1} - \varepsilon''_{m+1})) = \varepsilon^{-\varphi}(c - ac^\varphi - b). \end{aligned}$$

Тогда

$$\begin{aligned} v(u\varepsilon_{m+1} - \pi^m\varepsilon_{m+1}^\varphi + (\varepsilon'_{m+1} - \varepsilon''_{m+1})) &\geq nv(\pi), \\ v(\pi\varepsilon'_{m+1} + \pi u\varepsilon_{m+1} - \pi\varepsilon''_{m+1} - \pi^{m+1}\varepsilon_{m+1}^\varphi) &\geq (n+1)v(\pi). \end{aligned}$$

Случай 2: q делит $m+1$ и $m+1 = qm'$. Полагаем $a \equiv \pi^m$ и $b \equiv \varepsilon^\varphi(\pi^{-1}(\varepsilon_{m'}^\varphi - \varepsilon_{m'}^q) + (\varepsilon''_{m+1} - \varepsilon'_{m+1}))$. Заметим, что $b \in O_M$. По лемме 8 находим элемент $c \in O_M$ такой, что $v(c - ac^\varphi - b) \geq (n+1)v(\pi)$. Полагаем $\varepsilon_{m+1} = \varepsilon^{-1}c$ и, как выше, проверяем, что

$$v(\varepsilon_{m'}^q + \pi\varepsilon'_{m+1} + \pi u\varepsilon_{m+1} - \varepsilon_{m'}^\varphi - \pi\varepsilon''_{m+1} - \pi^{m+1}\varepsilon_{m+1}^\varphi) \geq (n+1)v(\pi).$$

Предложение доказано.

Установим аналог свойства единственности для многочленов вида Θ_m из предложения 9.

ПРЕДЛОЖЕНИЕ 10. Пусть $m \geq q^n$,

$$\Theta(x) = \sum_{i=1}^m \varepsilon_i x^i, \quad \eta(x) = \sum_{i=1}^m \eta_i x^i \in xO_M[x],$$

$$\varepsilon_2 = \dots = \varepsilon_{q-1} = \eta_2 = \dots = \eta_{q-1} = 0$$

и выполнены сравнения $\bar{f} \circ \Theta \equiv_m^n \Theta^\varphi \circ f$, $\bar{f} \circ \eta \equiv_m^n \eta^\varphi \circ f$ и неравенство $v(\varepsilon_1 - \eta_1) \geq (n+1)v(\pi)$. Тогда $v(\varepsilon_i - \eta_i) \geq (n+1-k)v(\pi)$ для любых $k < n$ и $q^k \leq i \leq q^{k+1}$.

ДОКАЗАТЕЛЬСТВО. Для $1 \leq i < q$ заключение справедливо из условий предложения. Пусть для всех $i' \leq i < q^n$ утверждение справедливо и $1 \leq k < n$ таково, что $q^k \leq i < q^{k+1}$.

Случай 1: q не делит $i + 1$. Тогда из условий предложения (и доказательства предложения 9) вытекает, что

$$v(\varepsilon'_{i+1} + u\varepsilon_{i+1} - \varepsilon''_{i+1} - \pi^{i+1}\varepsilon_{i+1}^\varphi) \geq nv(\pi), \quad (5)$$

$$v(\eta'_{i+1} + u\eta_{i+1} - \eta''_{i+1} - \pi^{i+1}\eta_{i+1}^\varphi) \geq nv(\pi). \quad (6)$$

Поскольку

$$\varepsilon'_{i+1} = P_{i,i+1}(\varepsilon_1, \dots, \varepsilon_i), \quad \eta'_{i+1} = P_{i,i+1}(\eta_1, \dots, \eta_i),$$

то из индуктивного предположения имеем $v(\varepsilon'_{i+1} - \eta'_{i+1}) \geq (n + 1 - k)v(\pi)$; аналогично, $v(\varepsilon''_{i+1} - \eta''_{i+1}) \geq (n + 1 - k)v(\pi)$. Так как $k \geq 1$, то $n + 1 - k \leq n$ и из неравенств (5), (6) получаем

$$v(u(\varepsilon_{i+1} - \eta_{i+1}) - \pi^{i+1}(\varepsilon_{i+1}^\varphi - \eta_{i+1}^\varphi)) \geq (n + 1 - k)v(\pi).$$

Однако $v(\pi) > 0$, $v(\varepsilon_{i+1} - \eta_{i+1}) = v((\varepsilon_{i+1} - \eta_{i+1})^\varphi) = v(\varepsilon_{i+1}^\varphi - \eta_{i+1}^\varphi)$, следовательно,

$$v(\varepsilon_{i+1} - \eta_{i+1}) = v(u(\varepsilon_{i+1} - \eta_{i+1}) - \pi^{i+1}(\varepsilon_{i+1}^\varphi - \eta_{i+1}^\varphi)) \geq (n + 1 - k)v(\pi).$$

Случай 2: q делит $i + 1$ и $i + 1 = qi'$. Тогда $q^{k-1} < i' \leq q^k$. Из условий предложения следует, что

$$\begin{aligned} v(\varepsilon_{i'}^q + \pi\varepsilon'_{i+1} + \pi u\varepsilon_{i+1} - \varepsilon_{i'}^\varphi - \pi\varepsilon''_{i+1} - \pi^{i+1}\varepsilon_{i+1}^\varphi) &\geq (n + 1)v(\pi), \\ v(\eta_{i'}^q + \pi\eta'_{i+1} + \pi u\eta_{i+1} - \eta_{i'}^\varphi - \pi\eta''_{i+1} - \pi^{i+1}\eta_{i+1}^\varphi) &\geq (n + 1)v(\pi). \end{aligned}$$

Как выше, заметим, что

$$v(\varepsilon'_{i+1} - \eta'_{i+1}) \geq (n + 1 - k)v(\pi), \quad v(\varepsilon''_{i+1} - \eta''_{i+1}) \geq (n + 1 - k)v(\pi).$$

Поскольку $i' \geq q^k$, то $v(\varepsilon_{i'} - \eta_{i'}) \geq (n + 2 - k)v(\pi)$ и $v(\varepsilon_{i'}^q - \eta_{i'}^q) \geq (n + 2 - k)v(\pi)$, $v(\varepsilon_{i'}^\varphi - \eta_{i'}^\varphi) \geq (n + 2 - k)v(\pi)$. Как выше, заметим, что

$$v(\varepsilon'_{i+1} - \eta'_{i+1}) \geq (n + 1 - k)v(\pi) v(\varepsilon''_{i+1} - \eta''_{i+1}) \geq (n + 1 - k)v(\pi);$$

но тогда

$$v(\pi(\varepsilon'_{i+1} - \eta'_{i+1})) \geq (n + 2 - k)v(\pi), \quad v(\pi(\varepsilon''_{i+1} - \eta''_{i+1})) \geq (n + 2 - k)v(\pi).$$

Отсюда вытекает, что

$$v(\pi u(\varepsilon_{i+1} - \eta_{i+1}) - \pi^{i+1}(\varepsilon_{i+1} - \eta_{i+1})^\varphi) \geq (n + 2 - k)v(\pi)$$

и, следовательно, $v(\varepsilon_{i+1} - \eta_{i+1}) \geq (n + 1 - k)v(\pi)$. Предложение доказано.

Пусть $m \equiv nq^n$, $\Theta(x) \equiv \Theta_m(x)$ из предложения 9 и $\eta(x) \equiv \Theta^\varphi \circ [u^{-1}]_m$. Проверим, что $\bar{f} \circ \eta \equiv_m^n \eta^\varphi \circ f$. Имеем

$$\begin{aligned} \bar{f} \circ \eta &= \bar{f} \circ \Theta^\varphi \circ [u^{-1}]_m = (\bar{f} \circ \Theta \circ [u^{-1}]_m)^\varphi \equiv_m^n (\Theta^\varphi \circ f \circ [u^{-1}]_m)^\varphi \\ &\equiv_m (\Theta^\varphi \circ [u^{-1}]_m \circ f)^\varphi = (\eta \circ f)^\varphi = \eta^\varphi \circ f. \end{aligned}$$

Рассмотрим коэффициенты $\eta_1, \dots, \eta_{q-1}$ многочлена

$$\begin{aligned} \eta &= \Theta^\varphi \circ [u^{-1}]_m = \varepsilon^\varphi [u^{-1}]_m + \varepsilon_q^\varphi ([u^{-1}]_m)^q + \dots + \varepsilon_m^\varphi ([u^{-1}]_m)^m \\ &\equiv_{q-1} \varepsilon^\varphi [u^{-1}]_m \equiv_{q-1} \varepsilon^\varphi u^{-1} x. \end{aligned}$$

Отсюда $\eta_1 = \varepsilon^\varphi u^{-1}$, $\eta_2 = \dots = \eta_{q-1} = 0$. Далее, $\varepsilon^\varphi u^{-1} \equiv^n \varepsilon^\varphi \varepsilon^{1-\varphi} = \varepsilon$. Применяя предложение 10, получим

$$v(\varepsilon_i - \eta_i) \geq v(\pi), \quad i \leq q^n.$$

Пусть α – корень многочлена F_n и $\alpha' \equiv \Theta(\alpha)$. Тогда сравнение $\bar{f} \circ \Theta \equiv_m^n \Theta^\varphi \circ f$ влечет $v(\bar{F}_n(\alpha')) > nv(\pi)$; следовательно, существует единственный корень $\bar{\alpha}$ многочлена $\bar{F}_n$ такой, что

$$v(\bar{\alpha} - \alpha') > \varkappa_{F_n} = \frac{1}{q-1} v(\pi).$$

Покажем, что $\bar{\alpha}^{\varphi\sigma_{u^{-1}}} = \bar{\alpha}$. Рассмотрим элемент

$$(\alpha')^{\varphi\sigma_{u^{-1}}} = (\Theta(\alpha))^{\varphi\sigma_{u^{-1}}} = \Theta^\varphi(\alpha^{\sigma_{u^{-1}}}).$$

Имеем $v(\bar{\alpha}^{\varphi\sigma_{u^{-1}}} - (\alpha')^{\varphi\sigma_{u^{-1}}}) = v(\bar{\alpha} - \alpha') > \varkappa_{\bar{F}_n}$. Далее,

$$v(\alpha^{\sigma_{u^{-1}}} - [u^{-1}]_m(\alpha)) > \varkappa_{F_n} = \varkappa_{\bar{F}_n}, \quad v(\Theta^\varphi(\alpha^{\sigma_{u^{-1}}}) - \Theta^\varphi([u^{-1}]_m(\alpha))) > \varkappa_{\bar{F}_n}.$$

Однако $\Theta^\varphi(\alpha^{\sigma_{u^{-1}}}) = (\alpha')^{\varphi\sigma_{u^{-1}}}$, а $\Theta^\varphi([u^{-1}]_m(\alpha)) = \eta(\alpha)$, следовательно, имеем $v((\alpha')^{\varphi\sigma_{u^{-1}}} - \eta(\alpha)) > \varkappa_{\bar{F}_n}$.

Заметим теперь, что

$$v(\alpha' - \eta(\alpha)) = v(\Theta(\alpha) - \eta(\alpha)) > v(\pi) \geq \frac{1}{q-1} v(\pi) = \varkappa_{\bar{F}_n}.$$

Действительно, как было отмечено выше, по предложению 10 имеем $v(\varepsilon_i - \eta_i) \geq v(\pi)$ для $1 \leq i \leq q^n$, и тогда $v(\varepsilon_i \alpha^i - \eta_i \alpha^i) > v(\pi)$ для $i \leq q^n$. Для $i > q^n$ имеем

$$\begin{aligned} v(\varepsilon_i \alpha^i) &= v(\varepsilon_i) + iv(\alpha) \geq iv(\alpha) > \frac{q^n}{(q-1)q^{n-1}} v(\pi) \\ &= \frac{q}{q-1} v(\pi) > v(\pi); \end{aligned}$$

аналогично, $v(\eta_i \alpha^i) > v(\pi)$ для $i > q^n$.

Используя установленные выше неравенства, имеем

$$v(\bar{\alpha}^{\varphi\sigma_{u^{-1}}} - \bar{\alpha}) = v(\bar{\alpha}^{\varphi\sigma_{u^{-1}}} - (\alpha')^{\varphi\sigma_{u^{-1}}} + (\alpha')^{\varphi\sigma_{u^{-1}}} - \eta(\alpha) - \alpha' + \alpha' - \bar{\alpha}) > \varkappa_{F_n}.$$

Поскольку $\bar{\alpha}$ и $\bar{\alpha}^{\varphi\sigma_{u^{-1}}}$ – корни многочлена $\bar{F}_n$, то должно быть $\bar{\alpha} = \bar{\alpha}^{\varphi\sigma_{u^{-1}}}$.

Заметим, что

$$N_{L_n M/M}(\alpha) = N_{L_n/K}(\alpha) = (-1)^{(q-1)q^{n-1}} \pi,$$

$$N_{L_n M/M}(\bar{\alpha}) = N_{L_n/K}(\bar{\alpha}) = N_{L_{\bar{\pi},n}/K}(\bar{\alpha}) = (-1)^{(q-1)q^{n-1}} \bar{\pi} = (-1)^{(q-1)q^{n-1}} \pi u.$$

Тогда $N_{L_n M/M}(\bar{\alpha}\alpha^{-1}) = u$. Учитывая рассуждения, проведенные в начале доказательства теоремы 3, получим $r_{L_n/K}(\sigma_{u^{-1}}) = u N_{L_n/K}(L_n^\times)$, что и завершает доказательство теоремы.

В заключение рассмотрим классический пример, когда $K = \mathbb{Q}_p$ – поле p -адических чисел. Если ξ_n – первообразный корень из единицы степени p^n , $n \in \omega^+$, то $\mathbb{Q}_p(\xi_n)$ – расширение Любина–Тейта L_n поля $\mathbb{Q}_p$. Действительно, полагая $\alpha \rightleftharpoons \xi_n - 1$, видим, что α является корнем многочлена $((x+1)^{p^n} - 1)((x+1)^{p^{n-1}} - 1)^{-1}$, причем многочлен $g(x) = (x+1)^p - 1$ является многочленом Любина–Тейта. Пусть u – целое положительное число, не делящееся на p . Пусть $[u] \rightleftharpoons (x+1)^u - 1$; проверим, что $g \circ [u] = [u] \circ g$. Действительно,

$$g \circ [u] = ([u] + 1)^p - 1 = (x+1)^{pu} - 1,$$

$$[u] \circ g = (g + 1)^u - 1 = ((x+1)^p - 1 + 1)^u - 1 = (x+1)^{pu} - 1.$$

Тогда по предложению 4 имеем равенство

$$\sigma_u(\alpha - 1) = \sigma_u(\xi_n) = [u](\alpha) + 1 = (\alpha + 1)^u - 1 + 1 = \xi_n^u.$$

Таким образом, элементарными средствами установлена классическая

ТЕОРЕМА 4. *Имеем*

$$r_{L_n/Q}^{-1}(u^{-1})(\xi_n) = \sigma_u(\xi_n) = \xi_n^u \quad \text{для } u \in \omega^+, \quad p \nmid u.$$

Из того, что для любого поля K , удовлетворяющего условиям, сформулированным в начале статьи, наибольшее неразветвленное расширение $L_u > K$ порождается корнями из единицы (степеней, взаимно простых с p), из рассуждений, проведенных выше для $K = \mathbb{Q}_p$, и из теоремы 2 следует

ТЕОРЕМА 5 (Кронекер–Вебер). *Наибольшее абелево расширение поля $\mathbb{Q}_p$ порождается корнями из единицы.*

Приложение

В настоящем приложении будут установлены некоторые общие факты о гензелевых нормированных полях, которые имеют и самостоятельный интерес. Определение и простейшие свойства нормированных полей можно найти в книге [9].

Пусть $\mathbb{F} = \langle F, R \rangle$ – гензелево нормированное поле, $\bar{\mathbb{F}} = \langle \bar{F}, \bar{R} \rangle \geq \mathbb{F}$ – алгебраически замкнутое алгебраическое расширение. Через v будем обозначать нормирование, определенное кольцом нормирования $\bar{R}$; $\Gamma_R, \Gamma_{\bar{R}}, \Gamma_R \leq \Gamma_{\bar{R}}$, – группы нормирования нормированных полей $\mathbb{F}$ и $\bar{\mathbb{F}}$ соответственно. Одно из эквивалентных свойств гензелевости следующее:

(*) для любого $\alpha \in \overline{F}$ и любого F -автоморфизма σ поля $\overline{F}$ имеет место равенство $v(\alpha) = v(\sigma\alpha)$.

Основным новым наблюдением является

ПРЕДЛОЖЕНИЕ П1. Пусть $f \in F[x]$ – унитарный многочлен, $a \in F$ и $\alpha \in \overline{F}$ – корень многочлена f , наиболее близкий к a , т.е. $v(a - \alpha) = \max\{v(a - \alpha') \mid f(\alpha') = 0, \alpha' \in \overline{F}\}$. Тогда:

а) имеют место неравенства $v(f(a)) \leq v(a - \alpha) + v(f'(a))$ и $v(f(a)) \leq v(a - \alpha) + v(f'(\alpha))$;

б) если α – единственный корень, т.е. $f'(\alpha) \neq 0$, при этом $f(\alpha') = 0, \alpha \neq \alpha'$, влечет неравенство $v(a - \alpha) > v(a - \alpha')$, то $\alpha \in F$ и имеют место равенства $v(f(a)) = v(a - \alpha) + v(f'(a))$ и $v(f'(a)) = v(f'(\alpha))$.

Пусть $f = \prod_{i < n} (x - \alpha_i)$, $\alpha_0 = \alpha$, $\alpha_1, \dots, \alpha_{n-1} \in \overline{F}$. Тогда

$$v(f(a)) = v\left(\prod_{i < n} (a - \alpha_i)\right) = \sum_{i < n} v(a - \alpha_i) = v(a - \alpha_0) + \gamma,$$

где

$$\gamma = \sum_{i=1}^{n-1} v(a - \alpha_i).$$

ЛЕММА П1. Для любого i , $1 \leq i < n$, выполнено $v(a - \alpha_i) \leq v(\alpha_0 - \alpha_i)$.

ДОКАЗАТЕЛЬСТВО. Имеем

$$v(a - \alpha_i) = v(a - \alpha_0 + \alpha_0 - \alpha_i) \geq \min\{v(a - \alpha_0), v(\alpha_0 - \alpha_i)\}.$$

Если $v(\alpha_0 - \alpha_i) < v(a - \alpha_0)$, то $v(a - \alpha_i) = v(\alpha_0 - \alpha_i)$. Если же $v(\alpha_0 - \alpha_i) \geq v(a - \alpha_0)$, то $v(a - \alpha_i) \geq v(a - \alpha_0)$ и $v(a - \alpha_i) \leq v(a - \alpha_0)$ по выбору $\alpha = \alpha_0$. Следовательно, $v(a - \alpha_i) = v(a - \alpha_0) \leq v(\alpha_0 - \alpha_i)$.

Из леммы П1 следует, что

$$\begin{aligned} \gamma &\leq \sum_{i=1}^{n-1} v(\alpha_0 - \alpha_i) = v(f'(\alpha_0)), \\ v(f(a)) &\leq v(a - \alpha_0) + v(f'(\alpha_0)). \end{aligned}$$

Заметим, что если $v(a - \alpha_0) > v(a - \alpha_i)$ для некоторого i , $1 \leq i < n$, то из доказательства леммы П1 видно, что $v(a - \alpha_i) = v(\alpha_0 - \alpha_i)$. Если $v(a - \alpha_0) > v(a - \alpha_i)$ для всех i , $1 \leq i < n$, то $v(f'(\alpha_0)) = \gamma$ и $v(f(a)) = v(a - \alpha_0) + v(f'(\alpha_0))$.

Далее,

$$f'(x) = \sum_{i < n} \prod_{j \neq i} (x - \alpha_j), \quad f'(a) = \sum_{i < n} \prod_{j \neq i} (a - \alpha_j).$$

Заметим, что для $i = 0$

$$v\left(\prod_{j \neq 0} (a - \alpha_j)\right) = \sum_{j=1}^{n-1} v(a - \alpha_j) = \gamma,$$

для $i > 0$ имеем

$$\begin{aligned} v\left(\prod_{j \neq i} (a - \alpha_j)\right) &= v(a - \alpha_0) + \sum_{j \neq i} v(a - \alpha_j) + v(a - \alpha_i) - v(a - \alpha_i) \\ &= \gamma + (v(a - \alpha_0) - v(a - \alpha_i)) \geq \gamma, \end{aligned}$$

так как $v(a - \alpha_0) \geq v(a - \alpha_i)$ по выбору $\alpha_0 = \alpha$. Тогда

$$v(f'(a)) \geq \min_i v\left(\prod_{j \neq i} (a - \alpha_j)\right) = \gamma.$$

Если же $v(a - \alpha_0) > v(a - \alpha_i)$ для $1 \leq i < n$, то

$$v\left(\prod_{j \neq i} (a - \alpha_j)\right) > \gamma,$$

и тогда $v(f'(a)) = \gamma$.

Остается проверить, что $\alpha_0 \in F$. Имеем $f'(\alpha_0) \neq 0$, и корень α_0 сепарабелен над F . Если $\alpha_0 \notin F$, то существует F -автоморфизм σ поля $\overline{F}$ такой, что $\alpha_0 \neq \sigma(\alpha_0)$. Однако $f(\sigma(\alpha_0)) = \sigma f(\alpha_0) = 0$, следовательно, $\sigma(\alpha_0) = \alpha_i$ для некоторого i , $1 \leq i < n$. Так как $\mathbb{F}$ гензелево, то $v(a - \alpha_0) = v(\sigma(a - \alpha_0)) = v(a - \sigma(\alpha_0)) = v(a - \alpha_i)$, что приводит к противоречию с предположением $v(a - \alpha_0) > v(a - \alpha_i)$ для всех i , $1 \leq i < n$. Предложение доказано.

Покажем, что следующие теорема и лемма являются легкими следствиями предложения П1.

ТЕОРЕМА П1 (Гензель–Рихлик). Пусть $f \in R[x]$ – унитарный многочлен, $a \in R$ и $v(f(a)) > 2v(f'(a))$. Тогда в R существует (единственный) корень α многочлена f такой, что

$$v(a - \alpha) = v(f(a)) - v(f'(a)) > v(f'(a)) \geq 0.$$

ДОКАЗАТЕЛЬСТВО. Пусть α – такой корень, как в условии предложения П1. Тогда имеем неравенства

$$\begin{aligned} 2v(f'(a)) &< v(f(a)) \leq v(a - \alpha) + v(f'(a)), \\ v(a - \alpha) &\geq v(f(a)) - v(f'(a)) > 2v(f'(a)) - v(f'(a)) = v(f'(a)). \end{aligned}$$

Проверим, что α – единственный корень с условием $v(a - \alpha) > v(f'(a))$. Используем обозначения $\alpha_0 = \alpha$ из доказательства предложения П1 и предположим, что для некоторого α_i , $1 \leq i < n$, выполнено

$$v(a - \alpha_i) > v(f'(a)) \geq \gamma = \sum_{j=1}^{n-1} v(a - \alpha_j).$$

Однако $a, \alpha_0, \dots, \alpha_{n-1} \in \overline{R}$, следовательно, $v(a - \alpha_j) \geq 0$ для всех $j < n$. Тогда $v(a - \alpha_i) > \gamma \geq v(a - \alpha_i)$. Противоречие. Итак, $\alpha = \alpha_0$ – единственный корень многочлена f с условием $v(a - \alpha) > v(f'(a))$. Тогда (по предложению П1, b))

$$v(f(a)) = v(a - \alpha) + v(f'(a)), \quad v(a - \alpha) = v(f(a)) - v(f'(a)).$$

ЛЕММА П2 (Краснер). Пусть $a, \alpha \in \bar{F}$, α сепарабелен над $F(a)$ и $v(a - \alpha) > v(\alpha - \sigma(\alpha))$ для любого $F(a)$ -автоморфизма σ , не тривиального на $F(a, \alpha)$. Тогда $\alpha \in F(a)$.

ДОКАЗАТЕЛЬСТВО. Пусть f – минимальный многочлен для α над $F(a)$. Из условия леммы следует, что

$$v(a - \alpha) = v(a - \sigma(\alpha) + \sigma(\alpha) - \alpha) = v(\sigma(\alpha) - \alpha) < v(a - \alpha),$$

т.е. для f , a и α выполнены условия предложения П1, б) (с полем $F(a)$ вместо F). Тогда $\alpha \in F(a)$.

Для удобства применений предложения П1 введем в рассмотрение три элемента группы $\Gamma_{\bar{R}}$, связанных с многочленом $f \in \bar{F}[x]$ без кратных корней:

$$\begin{aligned} \varkappa_f &\equiv \max\{v(\alpha - \alpha') \mid f(\alpha) = f(\alpha') = 0, \alpha \neq \alpha' \in \bar{F}\}, \\ \Delta_f &\equiv \max\{v(f'(\alpha)) \mid f(\alpha) = 0, \alpha \in \bar{F}\}, \\ \varepsilon_f &\equiv \varkappa_f + \Delta_f. \end{aligned}$$

Тогда справедлива

ТЕОРЕМА П2. Пусть $f \in F[x]$ – унитарный многочлен без кратных корней и $a \in F$ такой, что $v(f(a)) > \varepsilon_f$. Тогда в F существует (единственный) корень α многочлена f такой, что

$$v(a - \alpha) = v(f(a)) - v(f'(a)) > \varkappa_f.$$

ДОКАЗАТЕЛЬСТВО. Пусть $\alpha \in \bar{F}$ такой, как в условиях предложения П1. Тогда по этому предположению $v(f(a)) \leq v(a - \alpha) + v(f'(\alpha))$, $\varepsilon_f < v(f(a)) \leq v(a - \alpha) + \Delta_f$, $v(a - \alpha) > \varkappa_f$. Отсюда

$$v(a - \alpha') = v(a - \alpha + \alpha - \alpha') = v(\alpha - \alpha') < v(a - \alpha)$$

(так как $v(\alpha - \alpha') \leq \varkappa_f$ для любого корня $\alpha' \neq \alpha$ многочлена f). Но тогда по утверждению б) предложения П1 имеем $\alpha \in F$ и $v(a - \alpha) = v(f(a)) - v(f'(a))$.

ЗАМЕЧАНИЕ П1. Если унитарный многочлен без кратных корней имеет коэффициенты в R , то $\Delta_f \leq (n - 1)\varkappa_f$ и $\varepsilon_f \leq v(\delta_f)$, где δ_f – дискриминант многочлена f .

Укажем одно из следствий теоремы П2. Пусть $F(\alpha) \geq F$ – сепарабельное расширение F , f – минимальный многочлен для α над F , $\gamma \equiv \varepsilon_f - v(N_{F(\alpha)/F}(\alpha))$, $U^{(\gamma^+)} \equiv \{u \mid u \in F^\times, v(1 - u) > \gamma\}$.

СЛЕДСТВИЕ П1. Имеет место включение $U^{(\gamma^+)} \leq N_{F(\alpha)/F}(F(\alpha)^\times)$.

ДОКАЗАТЕЛЬСТВО. Пусть $u \in U^{(\gamma^+)}$, $f = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in F[x]$, $g \equiv x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_nu$, и пусть β – корень многочлена g в $\bar{F}$. Тогда

$$v(f(\beta)) = v(f(\beta) - g(\beta)) = v(a_n - a_nu) = v(a_n) + v(1 - u) > \varepsilon_f,$$

так как $v(a_n) = v(N_{F(\alpha)/F}(\alpha))$. Следовательно, по теореме П2 в $F(\beta)$ существует корень α' многочлена f . Можно считать, что $\alpha' = \alpha$; тогда $F(\alpha) \leq F(\beta)$,

$n = [F(\alpha) : F] \leq [F(\beta) : F] \leq n$, следовательно, $F(\alpha) = F(\beta)$, g – неприводимый многочлен, $a_n u = (-1)^n N_{F(\alpha)/F}(\beta)$, $a_n = (-1)^n N_{F(\alpha)/F}(\alpha)$, и тогда $u = N_{F(\alpha)/F}(\beta \alpha^{-1}) \in N_{F(\alpha)/F}(F(\alpha)^\times)$.

Список литературы

1. J. Neukirch, *Algebraic number theory*, Grundlehren Math. Wiss., **322**, Springer, Berlin, 1999.
2. Дж. Касселс, А. Фрелих (ред.), *Алгебраическая теория чисел*, Мир, М., 1969; пер. с англ.: J. W. S. Cassels, A. Frohlich (eds.), *Algebraic number theory*, Academic Press, London; Thompson, Washington, 1967.
3. К. Ивасава, *Локальная теория полей классов*, Мир, М., 1983.
4. J. Lubin, J. Tate, “Formal complex multiplication in local fields”, *Ann. of Math.* (2), **81**:2 (1965), 380–387.
5. M. Hazewinkel, “Local class field theory is easy”, *Adv. Math.*, **18**:2 (1975), 148–181.
6. Ю.Л. Ершов, “Абстрактная теория полей классов (финитарный подход)”, *Матем. сб.*, **194**:2 (2003), 37–60; англ. пер.: Yu. L. Ershov, “Abstract class field theory (a finitary approach)”, *Sb. Math.*, **194**:2 (2003), 199–223.
7. Ю.Л. Ершов, “Абстрактная теория полей классов (форматирование модулей)”, *Сиб. электр. матем. изв.*, **1** (2004), 1–23; англ. пер.: Yu. L. Ershov, “Abstract class field theory (module formatting)”, *Siberian Advances in Mathematics*, **18**:4 (2006), 21–49.
8. Ю.Л. Ершов, “Локальная теория полей классов”, *Алгебра и анализ*, **15**:6 (2003), 35–47; англ. пер.: Yu. L. Ershov, “Local class field theory”, *St. Petersburg Math. J.*, **15**:6 (2004), 837–846.
9. Ю.Л. Ершов, *Кратно нормированные поля*, Научная книга, Новосибирск, 2000.

Ю.Л. ЕРШОВ (Yu. L. Ershov)
Институт математики им. С.Л. Соболева СО РАН,
Новосибирск
E-mail: ershov@math.nsc.ru

Поступило в редакцию
20.12.2005