Записки научных
семинаров ПОМИ
Том 394, 2011 г.

С. В. Востоков

КАНОНИЧЕСКИЙ БАЗИС ГЕНЗЕЛЯ–ШАФАРЕВИЧА В ПОЛНЫХ ДИСКРЕТНО-НОРМИРОВАННЫХ ПОЛЯХ

Введение

Курт Гензель, основоположник p-адических полей, в работе [4] нашел широкую систему образующих для группы главных единиц полного дискретно нормированного поля нулевой характеристики с совершенным полем вычетов характеристики $p > 0$. В 1950 г. И. Р. Шафаревич определил базис в группе главных единиц поля, содержащего все корни p^n-ых степеней из 1, который он назвал каноническим, и который определял разложение однозначно с точностью до p^n-ых степеней. Этот базис был основан на определении единиц с помощью функции Артина–Хассе

$$E(x) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \cdots\right).$$

В настоящей работе из произвольной системы образующих Гензеля мы выделяем образующие, которые образуют базис $\mathbb{Z}_p$ -модуля главных единиц (см. ниже теоремы 2, 4), а при наличии p^n-ых корней из 1 – базисом по модулю p^n-ых степеней, при этом доказательство существенно упрощает доказательство работы [1].

Далее в теореме 8 мы обобщаем полученный результат на полное дискретно нормированное поле с произвольным полем вычетов. В дальнейшем предполагается перенести полученные результаты на формальные модули.

Обозначения

K – полное дискретно нормированное поле нулевой характеристики,

---

Ключевые слова: полное дискретно нормированное поле, p-базис, образующие Гензеля, базис Шафаревича.

Работа выполнена при финансовой поддержке ФЦП Минобрнауки РФ номер 2010-1.1-111-128-033.

e – абсолютный индекс ветвления поля K,
O_K – кольцо целых поля K,
π – простой элемент в K,
$U_1 = 1 + (\pi)$ – группа главных единиц в K,
$\overline{K}$ – поле вычетов поля K, характеристики $p > 0$,
N – подполе инерции в K,
O_N – кольцо целых поля N,
$f = (N : \mathbb{Q}_p)$ для конечного поля вычетов $\overline{K}$,
θ_0 – элемент O_N, полученный из сравнения

$$-p \equiv \theta_0 \pi^e \mod \pi^{e+1},$$

ζ_n – первообразный корень степени p^n из 1.
Если $\zeta_n \in K$, $n \geq 1$ то

$$e_0 = \frac{e}{p^{\overline{n}-1}(p-1)} \not\equiv 0 \mod p, \quad \overline{n} \geq n.$$

Для совершенного поля вычетов $\overline{K}$ обозначим
$\mathfrak{R}$ – набор представителей Тейхмюллера поля вычетов $\overline{K}$ в K,
$v : K^* \mapsto \mathbb{Z}$ – показатель поля K,
$S_e = \left\{1 \leq s < \frac{pe}{p-1}, (p,s) = 1\right\}$.

§1. Полная система образующих ступеней фильтрации главных единиц

1. Базис поля вычетов

Пусть в случае конечного поля вычетов $\{\overline{\theta}_1, \ldots, \overline{\theta}_n\}$ – базис поля $\overline{K}$ над $\mathbb{F}_p$, и $\{\theta_1, \ldots, \theta_n\}$ – система представителей этого базиса в кольце O_K.

В случае совершенного поля вычетов $\overline{K}$ выберем в $\overline{K}$ какой-нибудь базис $\{\overline{\theta}_i, i \in I\}$, и пусть $\{\theta_i, i \in I\}$ – представители этого базиса в O_K.

Наконец, в случае несовершенного поля вычетов $\overline{K}$ возьмем p-базис.

Определение. *Элементы $\{t_r, r \in R\}$ образуют p-базис поля $\overline{K}$, если $\overline{K} = \overline{K}^p[\{\overline{t}_r\}]$ и $|\overline{K}^p[\overline{t}_1, \ldots, \overline{t}_n] : \overline{K}^p| = p^n, n \geq 1$ для любых попарно различных элементов $\overline{t}_1, \ldots, \overline{t}_n$.*

Заметим, что пустое множество является p-базисом тогда и только тогда, когда поле $\overline{K}$ – совершенно. Из определения p-базиса следует,

что $\overline{K} = \overline{K}^{p^n}[\{\overline{t}_r\}]$ для любого $n \geq 1$. (Подробнее см. [4, гл. II, 5,(5.3)] и [6, стр. 82]).

Введем следующие обозначения:

$\{t_r, r \in R\}$ – система представителей p-базиса $\{\overline{t}_r, r \in R\}$ в O_K,

$t_{(r)}^{(k)} = t_{r_1}^{k_1} \ldots t_{r_v}^{k_v}$, $k_i \in \mathbb{N}$, $r_i \in R$.

Будем писать для $t_{(r)}^{(k)}$:

$m \leq (k) \leq n$, если $m \leq k_i \leq n$ для всех i,

$p \not| (k)$, если $(p, k_i) = 1$ для всех i,

T_m – множество всех мономов $t_{(r)}^{(k)}$, для которых $1 \leq (k) \leq m$,

$T_0 := 1$,

$p \not| T_m$, если $t_{(r)}^{(k)} \not| p$ для всех мономов из T_m,

$\overline{\Theta} = \{\overline{\theta}_i, i \in I\}$ – базис поля $\overline{K}, \overline{K}$ – совершенное,

$\Theta = \{\theta_i, i \in I\}$ – система представителей базиса $\overline{\Theta}$ в O_K,

A – система представителей в O_K элементов поля вычетов $\overline{K}$.

Из определения p-базиса следует

$$\overline{K} = \overline{K}^{p^n} + \overline{K}^{p^n}[\overline{T_n}] = \bigoplus_{0 \leq i \leq n} \overline{K}^{p^n}[\overline{T_{n-i}^{p^i}}], \tag{1}$$

где $p \not| \overline{T}_{n-i}$, $0 \leq i \leq n-1$ в последней сумме.

Отсюда следует

$$A = A^{p^n} + A^{p^n}[T_n] = \sum_{0 \leq i \leq n} A^{p^n}[T_{n-i}^{p^i}], \tag{2}$$

где $p \not| \overline{T}_{n-i}$, $0 \leq i \leq n-1$ в последней сумме. Обозначим

$$B_i = A^{p^{\overline{n}}}[T_i^{p^{\overline{n}-i}}] - \theta_0 A^{p^{\overline{n}-1}}[T_i^{p^{\overline{n}-i-1}}], 0 \leq i \leq \overline{n}-1,$$
$$\epsilon(A[T^m]\pi^s) = \{\epsilon \equiv 1 + \alpha t_{(r)}^{(k)} \pi^s (\pi^{s+1})\},$$

где α пробегает A, а $t_{(r)}^{(k)}$ – все мономы T_m.

2. Формулы возведения в степень p

Пусть $\epsilon_s(\alpha) \equiv 1 + \alpha\pi^s \mod (\pi^{s+1})$, тогда

$$\epsilon_s(\alpha)^p \equiv 1 + \alpha^p \pi^{ps}(\pi^{ps+1}), \quad s < \frac{e}{p-1}, \tag{3a}$$

$$\epsilon_s(\alpha)^p \equiv 1 - \theta_0 \alpha \pi^{e+s}(\pi^{e+s+1}), \quad s > \frac{e}{p-1}, \tag{3b}$$

$$\epsilon_s(\alpha)^p \equiv 1 + (\alpha^p - \theta_0\alpha)\pi^{\frac{pe}{p-1}}(\pi^{\frac{pe}{p-1}+1}), \quad s = \frac{e}{p-1}, \tag{3c}$$

где $-p \equiv \theta_0 \pi^e \mod (\pi^{e+1})$.

3. Система представителей ступени $U_r \setminus U_{r+1}$

Случай $e \not\equiv 0 \mod (p-1)$**.** Пусть $s \in S_e$ и μ_s – такое число, что

$$\frac{e}{p-1} \le p^{\mu_s} s < \frac{pe}{p-1}. \tag{4}$$

а) Совершенное поле вычетов $\overline{K}$. Из формул (3) получаем

Лемма 1. а) *Базисом ступени* $U_{p^{\mu_s}} \setminus U_{p^{\mu_s}s+1}, 0 \le \mu \le \mu_s$ *является множество единиц*

$$\epsilon^{p^\mu}(\Theta\pi^s) = \epsilon(\Theta^{p^\mu}\pi^{p^\mu s}). \tag{5}$$

б) *Базисом ступени* $U_{p^{\mu_s}s+\mu e} \setminus U_{p^{\mu_s}s+\mu e+1}, 0 \le \mu \le \mu_s$ *является множество единиц*

$$\epsilon(\Theta\pi^s)^{p^{\mu_s+\mu}} = \epsilon(\theta_0^\mu \Theta^{p^{\mu_s}} \pi^{p^{\mu_s}s+\mu e}), \tag{6}$$

где $-p \equiv \theta_0\pi^e \pmod{\pi}^{e+1}$.

Замечание. В конечном случае поля $\overline{K}$ имеем

$$\Theta = \{\theta_1, \dots, \theta_f\}.$$

б) Несовершенное поле вычетов $\overline{K}$. Из формул (3) получаем

Лемма 2. *Полная система представителей ступени* $U_s \setminus U_{s+1}$, $s \in S_e$, *состоит из единиц*

$$\epsilon(A\pi^s), \tag{7}$$

а полной системой представителей ступени $U_{\mu e+s} \setminus U_{\mu e+s+1}$, $s \in S_e$, $s > \frac{e}{p-1}$, *будет множество единиц*

$$\epsilon(\theta^\mu A\pi^{s+\mu e}). \tag{8}$$

Лемма 3. а) *Полной системой представителей ступени* $U_{p^\mu s}\setminus U_{p^\mu s+1}$, $0 \le \mu \le \mu_s$, *является множество единиц*

$$\epsilon\left(\left(\sum_{0\le i\le m} A^{p^m}[T_i^{p^{m-i}}]\right)\pi^{p^m s}\right), \tag{9}$$

где $p \nmid T_i$.

б) *Полной системой представителей ступени* $U_{p^{\mu_s} s+\mu e}\setminus U_{p^{\mu_s} s+\mu e+1}$ *является множество единиц*

$$\epsilon\left(\left(\theta^\mu \sum_{0\le i\le \mu_s} A^{p^{m_s}}[T_i^{p^{m_s-i}}]\right)\pi^{p^{m_s} s+\mu e}\right), \tag{10}$$

где $p \nmid T_i$, $s \in S_e$.

Доказательство. Согласно лемме 2 множество единиц $\epsilon(A\pi^s)$ является полной системой представителей для ступени $U_s \setminus U_{s+1}$, $s \in S_e$. Тогда из формулы (3а) следует, что

$$\epsilon(A\pi^s)^p = \epsilon(A^p\pi^{ps}) \subset U_{p^s} \setminus U_{p^s+1}.$$

Используя равенство $A = A^p + A^p[T_1]$, $p \nmid T_i$ (см. (2)), получим полную систему представителей ступени $U_{ps} \setminus U_{ps+1}$:

$$\epsilon((A^p + A^p[T_1])\pi^{ps}), \quad p \nmid T_i.$$

Продолжим процесс, с использованием (3а) и (2) получим утверждение а) в лемме 3.

Утверждение б) получаем отсюда, применяя формулу (3с). □

Случай $e \equiv 0 \mod (p-1)$**.**

Пусть

$$e_0 = \frac{e}{p^{\overline{n}-1}(p-1)}, \quad e_0 \not\vdots\, p, \quad \overline{n} \ge 1 \tag{11}$$

Определим гомоморфизм

$$\psi : \overline{K} \to \overline{K}, \quad \overline{\epsilon} \mapsto \overline{\epsilon}^{p^{\overline{n}}} - \overline{\theta}_0\overline{\epsilon}^{p^{\overline{n}-1}}, \tag{12}$$

где $-p \equiv \theta_0\pi^e \mod (\pi^{e+1})$.

A) $\operatorname{Ker}\psi = (0)$

а) $\overline{K}$ – совершенное поле. Пусть $\Theta = \{\theta_i, i \in I\}$ – представители базиса $\{\overline{\theta}_i, i \in I\}$ в O_K, определим

$$\eta_i = \theta_i^{p^{\overline{n}}} - \theta_0 \theta_i^{p^{\overline{n}-1}}, \quad i \in I,$$

и обозначим

$$H = \{\eta_i, i \in I\}.$$

Лемма 4. *Если* $\operatorname{Ker}\psi = (0)$, *то* $\overline{H} = \{\overline{\eta}_i,\ i \in I\}$ *– базис* $\overline{K}$.

Доказательство. Пусть

$$\sum_{\alpha=1}^{k} a_\alpha \overline{\eta}_{i_\alpha} = 0,$$

тогда

$$\sum_{\alpha=1}^{k} ((a_\alpha \overline{\theta}_{i_\alpha})^{p^{\overline{n}}} - \theta_0 (a_\alpha \overline{\theta}_{i_\alpha})^{p^{\overline{n}-1}}) = 0.$$

Отсюда, обозначив $\overline{\beta} = \sum\limits_{\alpha=1}^{k} a_\alpha \overline{\theta}_{i_\alpha}$, получаем $\overline{\beta}^{p^{\overline{n}}} - \overline{\theta}_0 \overline{\beta}^{p^{\overline{n}-1}} = 0$, т.е. $\overline{\beta} \in \operatorname{Ker}\psi = 0$, а значит, $\sum\limits_{\alpha=1}^{k} a_\alpha \overline{\theta}_{i_\alpha} = 0$, и из линейной независимости системы $\Theta = \{\theta_i, i \in I\}$ следует $a_\alpha = 0$, $\alpha = 1, \ldots, k$. □

Предложение 1. *Пусть* $\overline{K}$ *– совершенное поле,*
$e \equiv 0 \mod (p-1)$, $\operatorname{Ker}\psi = (0)$. *Тогда*

а) Базисом ступени $U_{p^\mu s} \setminus U_{p^\mu s+1}$, $s \in S_e$, $0 \le \mu < \mu_s$, является множество единиц:

$$\epsilon(\Theta^{p^\mu} \pi^{p^\mu s}). \tag{13}$$

б) Базисом ступени $U_{p^\mu s+\mu e} \setminus U_{p^\mu s+\mu e+1}$, $s \in S_e$, $0 \le \mu < \mu_s$, является множество единиц:

$$\epsilon(\theta_0^\mu \Theta^{p^\mu} \pi^{p^{\mu_s} s+\mu e}). \tag{14}$$

в) Базисом ступени $U_{\frac{pe}{p-1}+\mu e} \setminus U_{\frac{pe}{p-1}+\mu e+1}$ является множество единиц:

$$\epsilon(\theta_0^\mu H \pi^{\frac{pe}{p-1}+\mu e}). \tag{15}$$

Доказательство. Первые два утверждения это лемма 1. Последнее утверждение следует из формул (3c) для ступени $p^{\overline{n}-1} e_0$ и леммы 4. □

б) $\overline{K}$ – несовершенное поле, $\operatorname{Ker}\psi = (0)$**.**

Предложение 2. а) *Полной системой представителей ступени* $U_{p^\mu s} \setminus U_{p^\mu s+1}$, $s \in S_e$, $0 \le \mu < \mu_s$, μ_s *из* (4), *является множество единиц*

$$\epsilon\left(\left(\sum_{i=0}^{\mu} A^{p^\mu}[T_i^{p^{\mu-i}}]\right)\pi^{p^\mu s}\right) \tag{16}$$

где $p \nmid T_i$, $0 \le i \le \mu, (T_0 = 1)$.

б) *Полной системой представителей ступени* $U_{p^{\mu_s} s+\mu e} \setminus U_{p^{\mu_s} s+\mu e+1}$, $s \in S_e$, $s \ne e_0$, *является множество единиц*

$$\epsilon\left(\left(\sum_{i=0}^{\mu_s} \theta_0^\mu A^{p^{\mu_s}}[T_i^{p^{\mu_s-i}}]\right)\pi^{p^{\mu_s} s+\mu e}\right), \tag{17}$$

где $p \nmid T_i$, $0 \le i \le \mu_s$, $(T_0 = 1)$.

в) *Полной системой представителей ступени* $U_{\frac{pe}{p-1}+\mu e} \setminus U_{\frac{pe}{p-1}+\mu e+1}$, $s \in S_e$, $s \ne e_0$, *является множество единиц*

$$\epsilon(\theta_0^\mu \mathfrak{B}\pi^{p^{\frac{pe}{p-1}+\mu e}}), \tag{18}$$

где $\mathfrak{B} = \sum\limits_{i=0}^{\overline{n}-1} \mathfrak{B}_i$, *а* $\mathfrak{B}_i = A^{p^{\overline{n}}}[T_i^{p^{\overline{n}-i}}] - \theta_0 A^{p^{\overline{n}-1}}[T_i^{p^{\overline{n}-i-1}}]$, $p \nmid T_i$, $0 \le i \le \overline{n}-1$, $(T_0 = 1)$.

Доказательство. Первые два утверждения проверены в лемме 3.

Для доказательства последнего утверждения надо взять полную систему представителей ступени с номером $p^{\overline{n}-1}e_0$ из (9), воспользоваться формулой (3c) и следующим наблюдением:

поскольку $\operatorname{Ker}\psi = 0$, и $A = \sum\limits_{i=0}^{\overline{n}-1} A^{\overline{n}}[T_i^{\overline{n}}]$ – полная система представителей поля $\overline{K}$ в кольце O_K, то $\mathfrak{B} = \sum\limits_{i=0}^{\overline{n}-1} \mathfrak{B}_i$ тоже будет полной системой представителей поля $\overline{K}$ в кольце O_K, т.е. $A \equiv \mathfrak{B} \mod (\pi)$. □

В) $\operatorname{Ker}\psi \ne (0)$

В этом случае поле K содержит все p-е корни из 1 (см., например, [5, глава 1, (5.7) и (6.3)]). Пусть ζ_n – первообразный корень максимальной степени p^n из 1 в поле K. Тогда $n \le \overline{n}$, где $e_0 = \frac{e}{(p-1)p^{\overline{n}-1}} \not\equiv 0 \mod (p)$.

а) $\overline{K}$ – совершенное поле, $\operatorname{Ker}\psi = (0)$. Так как $\zeta_1 \in K$, то $\operatorname{Ker}\psi$ имеет порядок p. Пусть

$$\eta_* \in O_K*, \quad \overline{\eta}_* \in \operatorname{Ker}\psi, \tag{19}$$

таким образом,

$$\eta_*^{p^{\overline{n}}} - \theta_0 \eta_*^{p^{\overline{n}-1}} \equiv 0 \mod (\pi)$$

и $\zeta_1 \equiv 1 + \overline{\eta}_*^{p^{\overline{n}}} \mod (\mathfrak{p}(\overline{K}))$, где $\mathfrak{p}(a) = \overline{a}^p - \overline{a}$, $\overline{a} \in \overline{K}$ (см. [5, глава 1, (6.3)]).

Пусть $H_0 = \{\eta_i, i \in I_0\}$ – система представителей в O_K базиса $\overline{K}/\operatorname{Ker}\psi$, т.е. дополнение $\overline{\eta}_*$ до базиса поля $\overline{K}$. Таким образом, $\overline{H_0} \cup \{\overline{\eta}_*\}$ – базис $\overline{K}$. Нетрудно видеть, что вычеты образов элементов η_i:

$$\{\overline{\psi(\eta_i)}, i \in I_0\} \subset \operatorname{Im}\psi \tag{20}$$

– линейно независимая система в $\overline{K}$ (см. лемму 4). Пусть $\Psi = \{\xi_j, j \in J\}$ – система представителей дополнения (20) до базиса $\overline{K}$, т.е. базис $\overline{K}/\operatorname{Im}\psi$. Таким образом, мы имеем три разных базиса поля $\overline{K}$ над $\mathbb{F}_p$:

$$\overline{\Theta} = \{\overline{\theta}_i, i \in I\}, \quad \overline{H}_0 \cup \{\overline{\eta}_*\} = \{\overline{\eta}_i, \overline{\eta}_*, i \in I_0\}. \tag{21}$$

$$\psi(\overline{H}_0) \cup \overline{\Psi} = \{\psi(\overline{\eta}_i), \overline{\xi}_j, i \in I_0, j \in J\}. \tag{22}$$

Отсюда и из формул (3) получаем

Предложение 3. а) *Пусть $s \in S_e$, $s \neq e_0$, μ_s из* (4). *Тогда базисом ступени*

$$U_{p^\mu s} \setminus U_{p^\mu s+1}, \quad 0 \le \mu < \mu_s,$$

и

$$U_{p^{\mu_s} s+\mu e} \setminus U_{p^{\mu_s} s+\mu e+1}$$

будут системы (14) *и* (15) *из предложения* 1.

б) *Пусть $s = e_0 \in S_e$. Тогда базисом ступени*

$$U_{p^\mu e_0} \setminus U_{p^\mu e_0+1}, \quad 0 \le \mu \le \overline{n},$$

будет система единиц

$$\epsilon(H^{p^\mu} \pi^{p^\mu e_0}).$$

в) *Для ступеней $U_{\frac{pe}{p-1}+\mu e} \setminus U_{\frac{pe}{p-1}+\mu e+1}$ базисом будут системы единиц*

$$\epsilon(\theta_0^\mu \mathfrak{B} \pi^{\frac{pe}{p-1}+\mu e}), \quad \mathfrak{B} = \Theta^{p^{\overline{n}}} - \theta_0 \Theta^{p^{\overline{n}-1}}, \quad \text{и} \quad \epsilon(\theta_0^\mu \Psi \pi^{\frac{pe}{p-1}+\mu e}).$$

б) $\overline{K}$ – несовершенное поле, $\operatorname{Ker}\psi \neq (0)$**.** *Пусть* $\overline{\alpha}_0 \in \overline{A}$ *порождает* $\operatorname{Ker}\psi$, *то есть* $\overline{\alpha}_0^{p^{\overline{n}}} - \theta_0\overline{\alpha}_0^{p^{\overline{n}-1}} = 0$.

Пусть $\psi(\overline{A}) = \overline{A}^{p^{\overline{n}}} - \overline{\theta}_0\overline{A}^{p^{\overline{n}-1}}$, при этом

$$\overline{A} = \sum_{i=0}^{\overline{n}-1} \overline{A}^{p^{\overline{n}-1}}[\overline{T}_i^{p^{\overline{n}-1-i}}], \quad p \nmid T_i$$

(см. 2).

Пусть $A_0 = A \setminus \{\alpha_0\}$. Учитывая равенство

$$A = A^{p^n-1} + \sum_{i=0}^{\overline{n}-1} A^{p^{\overline{n}-1}}[T_i^{p^{\overline{n}-1-i}}], \quad p \nmid T_i,$$

(см. 2) получаем

$$\psi(A) = (A_0^{p^{\overline{n}}} - \theta_0 A_0^{p^{\overline{n}-1}}) + \sum_{i=1}^{\overline{n}-1} \mathfrak{B}i, \quad \text{где} \tag{23}$$

$$\mathfrak{B}_i = A^{p^{\overline{n}}}[T_i^{p^{\overline{n}-i}}] - \theta_0 A^{p^{\overline{n}-1}}[T_i^{p^{\overline{n}-1-i}}], \quad p \nmid T_i.$$

Пусть, далее, $\Gamma = \{\gamma \in O_K : \overline{\gamma} \in \overline{K}/\operatorname{Im}\psi\}$.

Отсюда и из формул (3) получаем

Предложение 4. а) *Пусть* $s \in S_e$, μ *из* (4). *Тогда полной системой представителей ступени*

$$U_{p^\mu s} \setminus U_{p^\mu s+1}, \quad 0 \le \mu \le \mu_s,$$

является система (16) *предложения* 2.

б) *Полной системой представителей ступени*

$$U_{p^{\mu_s} s+\mu e} \setminus U_{p^{\mu_s} s+\mu e+1},\ 0 \le \mu \le \mu_s,\ s \in S_e,\ s \ne e_0,$$

является система (17) *предложения* 2.

в) *Полной системой представителей ступени*

$$U_{\frac{pe}{p-1}+\mu e} \setminus U_{\frac{pe}{p-1}+\mu e+1}, \quad \mu \ge 0,$$

будут единицы:

$$\epsilon(A\pi^{e_0})^{p^{\overline{n}+\mu}} = \epsilon(\theta_0^{mu}(A_0^{p^{\overline{n}}} - \theta_0 A_0^{p^{\overline{n}-1}})\pi^{\frac{pe}{p-1}+\mu e}),$$
$$\epsilon(\theta_0^\mu \mathfrak{B}_i \pi^{\frac{pe}{p-1}+\mu e}), \quad \epsilon(\theta_0^\mu \Gamma \pi^{\frac{pe}{p-1}+\mu e}). \tag{24}$$

§2. Теорема Гензеля

В этом параграфе мы докажем теорему о системе образующих группы главных единиц поля K. Сам Гензель доказал теорему в случае совершенного поля вычетов:

Теорема 1 (см. [4]). *Пусть поле вычетов $\overline{K}$ – совершенно и для каждого $s \in S_e$, а также для $s = \frac{pe}{p-1}$, и для каждого $\alpha \in \mathfrak{R}$ (мультипликативная система Тейхмюллера) выбрана единица $\epsilon_s(\alpha) \equiv 1 + \alpha\pi^s \mod (\pi^{s+1})$. Тогда всякая главная единица $\epsilon \in U_1$ может быть представлена в виде*

$$\epsilon = \prod_{s,r\geq 0} \epsilon_s(\alpha_{s,r})^{p^r}.$$

Доказательство основано на формулах возведения в степень p (см.(3)) и на следующем утверждении, верном для совершенных полей вычетов. Если α пробегает всю систему представителей поля вычетов $\overline{K}$ в кольце O_K, то α^p тоже пробегает всю систему представителей. Это дает нам возможность заменить ступени

$$U_{p^\mu s}, \quad p \nmid s, \quad p^\mu s < \frac{pe}{p-1},$$

на ступени U_s с помощью формул (3).

Когда мы переходим к несовершенному полю вычетов, то это свойство: $O_K^p \equiv O_K \mod \pi$ пропадает и теорема Гензеля формулируется в следующем виде.

Теорема 2. *Пусть поле вычетов $\overline{K}$ – несовершенно и для каждого s, $1 \leq s \leq \frac{pe}{p-1}$, и для каждого $\alpha \in A$ выбрана единица*

$$\epsilon_s(\alpha) \equiv 1 + \alpha\pi^s \mod (\pi^{s+1}).$$

Тогда всякая главная единица $\epsilon \in U_1$ может быть представлена в виде

$$\epsilon = \prod_{s,r\geq 0} \epsilon_s(\alpha_{s,r})^{p^r}.$$

Доказательство. Методом итерации любую единицу $\epsilon \in U_1$ можно записать в виде:

$$\epsilon = \prod_{s\geq 1}(1 + \alpha_s\pi^s), \quad \alpha_s \in A.$$

Если $s > \frac{pe}{p-1}$, то единицу $\epsilon_s(\alpha) \equiv 1 + \alpha\pi^s \mod (\pi^{s+1})$ можно заменить на $\epsilon_{s-e}(\alpha) \equiv 1 + \theta_0^{-1}\alpha\pi^{s-e} \mod (\pi^{s-e+1})$ согласно формулам

(3), где $-p \equiv \theta_0 \pi^e \mod (\pi^{e+1})$. Продолжая этот процесс, мы получим разложение ϵ по образующим, в условии теоремы. $\square$

§3. Базис группы главных единиц

A) K не имеет нетривиальных p-х корней из 1

a) $\overline{K}$ – совершенно

Теорема 3. *Пусть поле вычетов $\overline{K}$ – совершенно. Тогда система единиц*

$$\{\epsilon_{i,s} \mid i \in I, s \in S_e\},$$

где $\epsilon_{i,s} \equiv 1 + \theta\pi^s \mod (\pi^{s+1})$ является $\mathbb{Z}_p$-базисом группы главных единиц поля K, т.е. любая единица $\epsilon \in U_1$ однозначно представляется в виде

$$\epsilon = \prod_{i,s} \epsilon_{i,s}^{a_{i,s}}, \quad a_{i,s} \in \mathbb{Z}_p, \tag{25}$$

где множество индексов

$$I_{s,c} = \{i \in I \mid v_p(a_{i,s}) \leq c\} \tag{26}$$

конечно для любых $c \geq 0$ при фиксированном s.

Доказательство. Из теоремы Гензеля (см. теорему 1, §2) следует, что система (26) является системой образующих для U_1.

Единственность. Пусть

$$\prod_{i,s} \epsilon_{i,s}^{a_{i,s}} = 1.$$

Надо доказать, что $a_{i,s} = 0$ для всех пар (i, s).

Пусть для каждого $s \in S_e$ и каждого $c \geq 1$, $I_c \subset I$, обозначает множество индексов, для которых $v_p(a_{i,s}) = c$. По условию теоремы это множество конечно. Напишем

$$1 = \prod_{i,s} \epsilon_{i,s}^{a_{i,s}} = \prod_{s \in S_e} \prod_{c \geq 1} \epsilon_{s,c}, \tag{27}$$

$$\text{где} \quad \epsilon_{s,c} = \prod_{i \in I_c} \epsilon_{i,s}^{a_{i,s}}$$

Для каждой фиксированной пары (s, c) произведение $\prod\limits_{i \in I_c} \epsilon_{i,s}^{a_{i,s}}$ либо равно 1, когда все $a_{i,s} = 0$, $i \in I_c$, либо все единицы, отличные от 1, из этого произведения лежат в одной ступени. Причем для разных пар (s, c) и (s', c') ступени, в которых лежат $\epsilon_{s,c}$ и $\epsilon_{s',c'}$, не совпадают.

Если не все $a_{i,s}$ в (27) равны нулю, то найдется пара (s,c), для которой $\epsilon_{s,c}$ лежит в ступени $U_r \setminus U_{r+1}$ с наименьшим номером r. Тогда

$$1 = \prod_{i,s} \epsilon_{i,s}^{a_{i,s}} = \prod_{s \in S_e} \prod_{c \geq 1} \epsilon_{s,c} \in U_r \setminus U_{r+1}$$

– противоречие. □

б) $\overline{K}$ – несовершенное поле.

Пусть μ_s взято из (4).

Теорема 4. *Система единиц*

$$\{1 + \alpha^{p^\mu} t_{(r)}^{(k)} \pi^{p^\mu s} \mod (\pi^{p^\mu s+1})\}, \tag{28}$$

где $\alpha \in A$, $s \in S_e$, $0 \leq \mu \leq \mu_s$, $1 \leq (k) \leq p^\mu$, $p \nmid (k)$, $(r) \subset R$ является $\mathbb{Z}_p$-базисом группы главных единиц поля K, то есть любая единица $\epsilon \in U_1$ однозначно представляется в виде

$$\epsilon = \prod_{s,\mu,(k),(r)} (1 + \alpha^{p^\mu} t_{(r)}^{(k)} \pi^{p^\mu s})^{a_{\epsilon,\alpha}}, \quad a_{\epsilon,\alpha} \in \mathbb{Z}_p, \tag{29}$$

при этом (r) пробегает конечное число наборов индексов из R, а множество

$$I_{s,\mu} = \{\alpha \in A, (k), (r) \mid v_p(a_{\epsilon,\alpha}) \leq c\} \tag{30}$$

конечно для каждого $c \geq 0$ при фиксированных $s \in S_e$ и μ, $0 \leq \mu \leq \mu_s$.

Доказательство. Существование разложения (29) следует из теоремы Гензеля для несовершенного поля вычетов и предложения 2.

Докажем единственность. Пусть в представлении (29) единица $\epsilon = 1$. Для каждой пары (s,μ) и каждого $c \geq 1$, пусть I_c – множество всех наборов $(k),(r)$ и элементов $\alpha \in A$, для которых $v_p(a_{\epsilon,\alpha}) = c$. По условию (30) это множество должно быть конечным. Обозначим

$$\epsilon_{s,\mu,c} = \prod \left(1 + \alpha^{p^\mu} t_{(r)}^{(k)} \pi^{p^\mu s}\right)^{a_{\epsilon,\alpha}},$$

где s, μ – фиксированны, а (k), (r), α пробегают все наборы, для которых $v_p(a_{\epsilon,\alpha}) = c$. Тогда

$$\prod_{(s,\mu)} \left(\prod_{c \geq 1} \epsilon_{s,\mu,c} \right) = 1.$$

Для каждой фиксированной тройки (s,μ,c) произведение $\epsilon_{s,\mu,c}$ либо равно единице, когда $a_{\epsilon,\alpha} = 0$, либо все единицы этого произведения, отличные от 1, лежат в одной ступени. Причем для разных троек

(s,μ,c) и (s',μ',c') ступени, в которых находятся $\epsilon_{s,\mu,c}$ и $\epsilon_{s',\mu',c'}$, не совпадают. Поэтому, если не все $a_{\epsilon,\alpha}$ в (29) равны нулю, то найдется тройка (s,μ,c), для которой $\epsilon_{s,\mu,c}$ лежит в ступени $U_r \setminus U_{r+1}$ с наименьшим номером r. А тогда и

$$\prod_{s,\mu,c} \epsilon_{s,\mu,c} = 1 \in U_r \setminus U_{r+1}$$

– противоречие. □

Замечание. Так как поле K не содержит нетривиальных p-х корней из 1, то разложения теорем 3, 4 будут однозначными и по любому модулю $U_1^{p^n}$, $n \geq 1$.

B) K **содержит все** p**-е корни из 1**. Пусть ζ_n – максимальный корень степени p^n в K,

$$e_0 = \frac{e}{p^{\overline{n}-1}(p-1)} \not\equiv 0 \mod (p), \quad n \leq \overline{n}.$$

a) $\overline{K}$ – **совершенное поле**.

Теорема 5. *Система единиц*

$$\left\{\epsilon_{i,s} \equiv 1 + \theta_i \pi^s \mod (\pi^{s+1}), \quad i \in I, \quad s \in S_e, \quad s \neq e_0\right\}$$

вместе с единицами

$$\left\{\epsilon_{i,e_0} \equiv 1 + \eta_i \pi^{e_0} \mod (\pi^{e_0+1}), \quad i \in I \cup \{*\}\right\}, \qquad \text{см. (21)},$$

а также

$$\left\{\omega_j \equiv 1 + \xi_j \pi^{\frac{pe}{p-1}} \mod \left(\pi^{\frac{pe}{p-1}+1}\right), \quad j \in J\right\}, \qquad \text{см. (22)},$$

образуют $\mathbb{Z}_p$*-базис группы главных единиц поля* K*, т.е. любая единица* $\epsilon \in U_1$ *однозначно представляется в виде*

$$\epsilon = \epsilon_{*,e_0}^{a_{*,e_0}} \prod_{\substack{i \in I, s \in S_e, \\ (i,s) \neq (*,e_0)}} \prod_{j \in J} \omega_j^{b_j}, \tag{31}$$

где $a_{i,s}, b_j \in \mathbb{Z}_p$, $0 \leq a_{i_0,e_0} \leq p^{\overline{n}}$ *и* I_c *– конечное для любого* c.

Доказательство аналогично доказательству теоремы 2 с использованием предложения 1.

$\overline{K}$ – **несовершенное поле**.

Теорема 6. *Система единиц*

$$\left\{1+\alpha^{p^\mu}t_{(r)}^{(k)}\pi^{p^\mu s} \mod (\pi^{p^\mu s+1})\right\},$$

где $\alpha\in A$, $s\in S_e$, $0\le\mu\le\mu_s$, $1\le(k)\le p^\mu$, $p\nmid(k)$, $(r)\subset R$ (см. (28)) *вместе с единицами*

$$\left\{\omega_\gamma\equiv 1+\gamma\pi^{\frac{pe}{p-1}} \mod \left(\pi^{\frac{pe}{p-1}+1}\right),\quad \overline{\gamma}\in\overline{K}/\operatorname{Ker}\psi\right\},$$

(*см.* (24) *в предложении* 4) *образуют* $\mathbb{Z}_p$*-базис группы главных единиц поля* K, *т.е. каждая единица* $\epsilon\in U_1$ *однозначно представляется в виде*

$$\epsilon=(1+\alpha_0\pi^{e_0})^{b_{\alpha_0}}\prod\left(1+\alpha^{p^\mu}t_{(r)}^{(k)}\pi^{p^\mu s}\right)^{a_{\epsilon,\alpha}}\prod\omega(\gamma)^{b_\gamma}, \tag{32}$$

где $a_{\epsilon,\alpha}$, $b_\gamma\in\mathbb{Z}_p$, $0\le b_{\alpha_0}<p^{\overline{n}}$. *Во втором произведении исключается набор индексов* $\alpha=\alpha_0$, $s=e_0$, $\mu=0$ ($\overline{\alpha}_0$ *порождает* $\operatorname{Ker}\psi$).

Доказательство аналогично доказательству теоремы 3, с использованием предложения 4. □

§4. Единственность разложения по модулю p^n-х степеней в случае совершенного поля вычетов

A. Пусть K содержит первообразный корень ζ_n степени p^n из 1 и поле $\overline{K}$ – совершенно.

Теорема 7. *Единица* ϵ *тогда и только тогда принадлежит* $U_1^{p^n}$, *когда все показатели в разложении*

$$\epsilon=\epsilon_{*,e_0}^{a_{*,e_0}}\prod_{(i,s)\ne(*,e_0)}\epsilon_{i,s}^{a_{i,s}}\prod_j\omega_j^{b_j} \mod U_1^{p^n} \tag{32}$$

делятся на p^n (*см.* (31), *теорема* 5).

Замечание. При $n=\overline{n}$ показатель $a_{*,e_0}=0$.

Доказательство. 1. Пусть

$$a_{i,s}=p^{m_{i,s}}a'_{i,s},\ b_j=p^{m_j}b'_j,\qquad \text{где}\quad p\not|a'_{i,s},b'_j,$$

и пусть $m_*=\min(m_{i,s},m_j)$. Если $m_*\ge n$, то теорема доказана. Пусть поэтому $m_*<n$. Тогда

$$\sqrt[p^{m_*}]{\epsilon}=\zeta_n^{p^{n-m_*}}\epsilon_{*,e_0}^{p^{m_{*,e_0}-m_*}a'_{*,e_0}}\prod\epsilon_{i,s}^{p^{m_{i,s}-m_*}a'_{i,s}}\prod\omega_j^{p^{m_j-m_*}b'_j}\in K^*,$$

где $\zeta_{m_*}=\zeta_n^{p^{n-m_*}}$ – корень степени p^{m_*} из 1 и при этом $n-m_*\ge 1$.

2. Пусть все $m_{*,e_0}, m_{i,s} > m_*$, но среди показателей m_j найдется равный m_*, например $m_{j_1} = m_*$. Тогда

$$\sqrt[p^{m_*}]{\epsilon} \equiv \omega = \omega_{j_1}^{b'_{j_1}} \prod_{\beta=2}^{k} \omega_{j_\beta}^{b_{j_\beta}/p^{m_*}} \mod K^{*p}$$

Так как b'_{j_1} не делится на p, и система $\{\overline{\xi}_j,\ j \in J\}$ – базис $\overline{K}/\operatorname{Im}\psi$ (см. (22)), то из определения единиц ω_j видим, что

$$\omega \equiv 1 + \alpha\pi^{\frac{pe}{p-1}} \mod \left(\pi^{\frac{pe}{p-1}+1}\right),$$

где $\alpha = a'_{j_1}\xi_{j_1} + \sum\limits_{\beta=2}^{k} \frac{b_{j_\beta}}{p^m}\xi_{j_\beta} \not\equiv 0 \mod (\pi)$ и $\overline{\alpha} \in \operatorname{Im}\psi$. Значит, расширение $K(\sqrt[p^{m+1}]{\epsilon})/K = K(\sqrt[p]{\omega})/K$ будет нетривиальным, что противоречит условию $\epsilon \in K^{*p^n}$.

3. Пусть s_0 – наименьший возможный индекс, для которого найдется $m_{i,s_0} = m_*$.

a) $s_0 \neq e_0$ и, например, $m_{i_0,s_0} = m_*$, тогда

$$\sqrt[p^{m_*}]{\epsilon} \equiv \epsilon_{s_0} = \epsilon_{i_0,s_0}^{a'_{i_0,s_0}} \prod_{i \neq i_0} \epsilon_{i,s_0}^{a_{i,s_0}/p^{m_*}} \mod K^{*p}.$$

Так как a'_{i_0,s_0} не делится на p, и система $\{\overline{\theta}_i, i \in I\}$ – базис $\overline{K}$ (см. (22)), то

$$\epsilon_{s_0} \equiv 1 + \alpha\pi^{s_0} \mod \left(\pi^{\frac{pe}{p-1}+1}\right),$$

где $\alpha = a'_{i_0,s_0}\theta_{i_0} + \sum\limits_{i \neq i_0} \frac{a_{i,s_0}}{p^m}\theta_i \not\equiv 0 \mod (\pi)$.

b) $s_0 = e_0$. Рассуждаем точно так же с заменой базиса $\{\overline{\theta}_i, i \in I\}$ на базис $\{\overline{\eta}_i,\ i \in I_0 \cup \{*\}\}$ (см. (21)).

Из a) и b) следует, что расширение $K(\sqrt[p^{m_*+1}]{\epsilon})/K = K(\sqrt[p]{\epsilon_{s_0}})/K$ будет нетривиальным вполне разветвленным расширением, так как $p \not| s_0$, что противоречит условию $\epsilon \in K^{*p^n}$.

4. Утверждение теоремы в обратную сторону очевидно. Теорема доказана. □

B. В этом пункте мы из теоремы 7 выведем как частный случай теорему Шафаревича о каноническом базисе (см.[2, §4, п. 3]).

Пусть α – элемент из кольца $\widetilde{O}$ (кольцо целых пополнения максимального неразветвленного расширения поля $\mathbb{Q}_p$). Ясно, что $O_N \subset \widetilde{O}$.

Пусть ϕ – автоморфизм Фробениуса в $\widetilde{O}/\mathbb{Z}_p$. Тогда определим функцию

$$E(\alpha\pi^s) = \exp(\alpha\pi^s + \frac{\phi(\alpha)\pi^{ps}}{p} + \frac{\phi^2(\alpha)\pi^{p^2 s}}{p^2} + \cdots) \in 1 + \pi\widetilde{O} \qquad (33')$$

(см. [3]).

Пусть $a \in O_N$ и $\alpha \in \widetilde{O}$ – такой элемент, что $\alpha^\phi - \alpha = a$. Тогда расширение $N(\alpha)/N$ является пополнением Г-расширения и, если σ – образующий элемент группы Галуа $G(N(\alpha)/N) =< \sigma >$, то

$$\alpha^\sigma - \alpha = \kappa \in \mathbb{Z}_p.$$

Нормируем σ равенством $\alpha^\sigma = \alpha + 1$.

Замечание. Если $N/\mathbb{Q}_p$ – конечно, то $\sigma = \phi^f$, где $f = (N : \mathbb{Q}_p)$. Тогда $\alpha^\sigma - \alpha = 1$ с одной стороны, а с другой $\alpha^\sigma - \alpha = \alpha^{\phi^f} - \alpha = \mathrm{tr}\ a$, т.е. $\mathrm{tr}\, a = 1$.

Лемма 5. *Единица*

$$H(\alpha) = E(p^n\alpha\xi), \quad \text{где} \quad \zeta_n = E(\xi), \xi \in \pi O_K,$$

является p^n-примарной, т.е. расширение $K(\sqrt[p^n]{H(a)}) = K(E(\alpha\xi))/K$ неразветвленно и

$$\sqrt[p^n]{H(a)}^{\sigma-1} = \zeta_n. \qquad (33'')$$

Доказательство. 1) $H(a) \in K$, т.к.

$H(a)^\sigma = E(p^n\alpha^\sigma\xi) = E(p^n(\alpha+1)\xi) = H(a)$, $E(\xi)^{p^n} = H(a)\cdot\zeta_n^{p^n} = H(a)$.

Равенство $(33'')$ получается аналогично. □

Теорема о каноническом базисе. *Единицы*

$$\{E(a_s\pi^s), \quad H(a_s) \mid a \in O_N, \quad s \in S_s\}$$

образуют базис $U_1 \mod (U_1^{p^n})$, при этом

$$\epsilon = \prod_{s\in S_e} E(a_s\pi^s)H(a) \in U_1^{p^n} \Longleftrightarrow a_s \equiv 0 \mod (p^n), \quad a \in \mathfrak{p}(O_N), \quad (33)$$

где $\mathfrak{p}(a) = a^\sigma - a$, $a \in O_N$.

Замечание. Если поле вычетов $\overline{K}$ конечно, то последнее условие заменяется на

$$\mathrm{tr}\, a \equiv 0 \mod p^n.$$

Доказательство. В работах [3] и [2] показано, что

$$H(a) \equiv 1 + a'\pi^{\frac{pe}{p-1}} \mod \pi^{\frac{pe}{p-1}+1},$$

причем a, a' одновременно пробегают всё кольцо O_N. При этом

$$H(a) \in U_1^{p^n} \Longleftrightarrow \overline{a} \in \mathfrak{p}(\overline{K}) \Longleftrightarrow \overline{a'} \in \operatorname{Im}\psi \tag{34}$$

(относительно гомоморфизма ψ см. (12)). Поэтому в качестве базисных элементов ω_j из системы (32) теоремы 7 можно взять

$$\omega_j = H(\xi_j), \quad j \in J.$$

В качестве остальных базисных элементов теоремы 6 возьмем

$$\epsilon_{i,s} = E(\theta_i\pi^s), \quad s \in S_e, \quad i \in I, \quad s \neq e_0,$$
$$\epsilon_{i,s} = E(\eta_i\pi^{e_0}), \quad i \in I_0 \cup \{*\}.$$

Разложив каждый элемент a_s из (33) по базису $\{\theta_i, i \in I\}$ для $s \neq e_0$, и по базису $\{\theta_i,\ i \in I_0 \cup \{*\}\}$ для $s = e_0$, и используя теорему 7, получаем теорему Шафаревича. □

§5. Единственность разложения по модулю p^n-х степеней в случае несовершенного поля вычетов

A. Поле вычетов $\overline{K}$ – несовершенно.

Теорема 8. *Единица ϵ тогда и только тогда принадлежит $U_1^{p^n}$, когда все показатели в разложении* (32) *делятся на p^n.*

Доказательство проходит точно так же, как и доказательство теоремы 7. Единственное отличие в том, что в п. 3 доказательства теоремы 7 может встретиться ступень

$$U_{p^\mu s_0} \setminus U_{p^\mu s_0+1}, \quad 1 \leq \mu < \mu_{s_0},$$

для которой

$$\sqrt[p^\mu]{\epsilon} \equiv \epsilon_{p^\mu s_0} \in U_{p^\mu s_0} \setminus U_{p^\mu s_0+1} \mod K^{*p}.$$

Но единицы теоремы 7 из этой ступени входят в базис группы U_1, и значит, $K(\sqrt[p]{\epsilon})/K$ снова будет неразветвленным расширением.

B. В этом пункте мы выведем из теоремы 8 теорему о каноническом базисе группы главных единиц в полном дискретно нормированном поле K с несовершенным полем вычетов $\overline{K}$.

a) σ-поле. В работе [1] М. Бондарко доказал структурную теорему о полных дискретно нормированных полях. Для формулировки этой теоремы дадим основные понятия о σ-полях.

Определение 1. *$\mathbb{Z}_p$-алгебра $\mathfrak{A}$ без кручения называется σ-кольцом, если в $\mathfrak{A}$ определен оператор $\sigma : \sigma(x) - x^p \in p\mathfrak{A}$, для любого $x \in \mathfrak{A}$.*

Определение 2. *Пусть N – полное абсолютно неразветвленное дискретно нормированное поле. Пару (N, σ) назовем σ-полем, если определен эндоморфизм σ поля N, удовлетворяющий соотношению $\sigma(x) - x^p \in pO_N$, для любого x из кольца целых O_N поля N.*

Многие кольца допускают более одного эндоморфизма σ. Например, пусть $N = \mathbb{Q}_p\{\{x\}\}$ – двумерное локальное поле, $O_N = \mathbb{Z}_p\{\{x\}\}$. Тогда $\sigma : x \mapsto x^p + \alpha$, $\alpha \in \mathbb{Z}_p\{\{x\}\}$, является эндоморфизмом на N для любого α.

b) Структурная теорема ([1]). Каждое полное дискретно нормированное поле K является вполне разветвленным расширением некоторого абсолютно неразветвленного σ-поля N, поле вычетов $\overline{N}$ которого совпадает с полем вычетов $\overline{K}$ поля K.

Дадим набросок доказательства. Известно (см., например, [5], предложение 5.5, главы 2), что любое полное дискретно нормированное поле является вполне разветвленным расширением некоторого абсолютно неразветвленного поля N. Осталось задать на N структуру σ-поля. Для этого выберем p-базис в поле вычетов $\overline{K}(= \overline{N}) : \{\overline{t}_r, r \in R\}$ (см. §1, п. 1) и набор его представителей $\{t_r, r \in R\}$ в поле N.

Рассмотрим цепочку расширений $N_n = N_{n-1}$, $t_{r,n-1}$, $r \in R$, в которой $t_{r,0} = t_r$, $r \in R, N_0 = N$, $t_{r,n}^p = t_{r,n-1}$. Тогда пополнение N' поля $L = \cup_{n \geq 0} N_n$ будет абсолютно неразветвленным расширением с совершенным полем вычетов, которое является совершеннизацией поля $\overline{K} = \overline{N}$.

Так как $t_r \in \cap_{n \geq 0} N'^{p^n}$, то t_r является представителем Тейхмюллера для $\overline{t}_r$ в поле N' и $\sigma(t_r) = t_r^p$ – автоморфизм Фробениуса в N'. В работе [1] доказывается, что для автоморфизма Фробениуса σ поля N' выполнено:

$$\sigma(N) \subset N, \quad \sigma(O_N) \subset O_N, \tag{35}$$

и так как $\sigma(x) \equiv x^p \mod (pO_{N'})$, то $\sigma(x) \equiv x^p \mod (pO_N)$ для любого $x \in O_n$.

c) Экспонента Артина–Хассе в полном дискретно нормированном поле.

Обобщим классическую функцию Артина–Хассе (см. лемму 5) на полное дискретно нормированное поле K. Пусть N – его абсолютно неразветвленое σ-подполе. Для любого $\alpha \in O_N$ определим функцию Артина–Хассе

$$E(\alpha X) = \exp \sum_{m \geq 0} \frac{\sigma^m(\alpha)}{p^m} X^{p^m}. \tag{36}$$

Лемма 6. $E(\alpha X) \in 1 + O_N[[X]]X$, $E(\alpha X) \equiv 1 + \alpha X \mod (X^2)$.

Доказательство. σ-поле N содержится в абсолютно неразветвленном поле N' с совершенным полем вычетов (см. доказательство структурной теоремы). Поэтому для любого $\alpha' \in O_{N'}$ выполнено $E(\alpha' X) \in 1 + O_{N'}[[X]]X$ (см. (33')).

Второе утверждение следует из определения экспоненты. □

d) Теорема о каноническом базисе. Пусть $\{t_r, r \in R\}$ – представители p-базиса поля $\overline{K}$ в σ-кольце O_N, $A = \{\alpha\}$ – представители всех элементов поля $\overline{K}$ в O_N.

Пусть $\alpha_0 \in O_N$ – образующие ядра гомоморфизма ψ (см. (12)).

$\overline{k}$ – максимальное совершенное подполе в $\overline{K}$ и $T \subset N$ – поле частных кольца векторов Витта $W(\overline{k})$. Обозначим

$$C = \left\{ c \in O_N \,|\, \overline{c} \in \overline{K}/\operatorname{Im}\psi \right\},$$
$$\mathfrak{O} = \left\{ \delta \in O_T \,|\, \overline{\delta} \in \overline{K}/\operatorname{Im}\psi \right\},$$

и $\Gamma \subset O_N$ – дополнение $\mathfrak{O}$ до C, т.е. $C = \mathfrak{O} + \Gamma$.

Возьмем единицы

$$E(\alpha_0 \pi^{e_0}), \quad E(\alpha^{p^m} t_{(r)}^{(n)} \pi^{p^m s}), \quad H(\delta), \quad \omega(\gamma) = E(\gamma \pi^{\frac{pe}{p-1}}), \tag{37}$$

где $\delta \in \mathfrak{O}$, $\gamma \in \Gamma$, $H(\delta)$ взято из (33).

Теорема 9. *Единицы системы* (37) *образуют базис* $U_1 \mod (U_1)^{p^n}$. *При этом*

$$\epsilon = E(\alpha_0 \pi^{e_0})^a \prod E(\alpha^{p^m} t_{(r)}^{(n)} \pi^{p^m s})^{a_{\epsilon,s,m}} \prod H(\delta) \prod \omega(\gamma)^{b_j} \in U_1)^{p^n}$$
$$\Longleftrightarrow a, a_{\epsilon,s,m}, b_j \ \textit{все делятся на} \ p^n, \delta \in \mathfrak{p}(O_n), \ \textit{где} \ \mathfrak{p}(\delta) = \delta^{\phi} - \delta.$$

Замечание. При $n = \overline{n}$, $a = 0$.

Доказательство. Согласно леммам 5 и 6 единицы (37) удовлетворяют теореме 8, из которой следует наше утверждение. □

Литература

1. М. В. Бондарко, *Явная классификация формальных групп над полными дискретно нормированными полями с несовершенным полем вычетов.* — Труды С.-Петербургского мат. общества, **11** (2005), 1–36.
2. И. Р. Шафаревич, *Общий закон взаимности.* — Мат. сборник, **26(68)**: 1 (1950), 113–146.
3. H. Hasse, *Die Gruppe der p^n-primären Zahlen für einen Primteiler* $\mathfrak{p}$ von p. — J. reine angew. Math. **176** (1936), 174–183.
4. K. Hensel, *Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers.* — J. reine angew. Math. **136** (1916).
5. I. Fesenko, S. Vostokov, *Local Fields and Their Extensions.* AMS, Providence (1993).
6. И. Б. Жуков, *Коммутативная алгебра.* Изд. Санкт-Петербургского университета, 2009.

Vostokov S. V. Canonical basis of Hensel–Shafarevich in complete discrete valuation fields.

Starting with Hensel's generating set of principal units, we construct a base of the module of principal units, in the multiplicative group of a complete descrete valuation field with the residue field of prime characteristic we prove the uniqueness of the above base, and as a corollary, the uniqueness of the canonical Shafarevich base.

С.-Петербургский
государственный университет,
Университетский пр. 28, Петродворец,
198504 Санкт-Петербург, Россия

E-mail: sergei.vostokov@gmail.com

Поступило 27 сентября 2011 г.