Chapter 5
On Norm Maps and "Universal Norms" of Formal Groups Over Integer Rings of Local Fields

Nikolaj M. Glazunov

To the memory of Oleg Nikolaevich Vvedenskii (1937–1981)

Abstract We review and investigate norm maps and "universal norms" of formal groups over integer ring of local and quasi-local fields. Theorem on triviality of universal norm group of one dimensional fornal groups of reduction height 3 over integer ring of local and quasi-local fields is presented. The theorem on triviality of universal norm group is based on the lemma about function that gives the minimal degree of elements of the subgroup F_K^t of the group F_K that contains the norm group $N_{L/K}(F_L^n)$. In the case of formal groups of elliptic curves the function has used by O. N. Vvedenskii and is denoted as $\mu(n)$. The proof of the lemma is also presented.

5.1 Introduction

Under the construction by Shafarevich [1], Tate [2], Ogg [3], Vvedenskii [4, 5] the analog of local and quasi-local class field theory for elliptic curves and abelian varieties the authors use arithmetic properties of formal groups that corresponds to elliptic curves. Foundations of local and quasi-local class field theories of elliptic curves in the framework were constructed by Vvedenskii [4, 5] in contexts of elliptic curves over local and quasi-local fields. Important statements of these theories were introduced as statements about norm maps of commutative formal groups of elliptic curves.

It is well known that formal groups of elliptic curves over finite fields have height (reduction height) one or two [6–11].

N. M. Glazunov (✉)
National Aviation University, Kiev, Ukraine
e-mail: glanm@yahoo.com

M. Z. Zgurovsky and V. A. Sadovnichiy (eds.), *Continuous and Distributed Systems*, Solid Mechanics and Its Applications 211, DOI: 10.1007/978-3-319-03146-0_5,

Let A be an elliptic curves over quasi-local fields K, $F(x, y)$ its formal group over the ring of integers O_K of K, $\mathscr{D}_K^*$ it's group of universal norms [4, 5]. In the case O.N. Vvedenskii have proved.

Theorem 5.1 [4, 5] $\mathscr{D}_K^* = 0$.

Author extends, following to the advice of O. N. Vvedenskii, Theorem 5.1 and some another results of O. N. Vvedenskii to more general formal groups and present their in papers [8, 10]. Complete proves of the results are contained in author's candidate dissertation that is not published.

Here we present theorem on triviality of universal norm group of one dimensional formal groups of height 3 over integer ring of local and quasi-local fields and present the lemma about function $\mu(n)$ that gives the minimal degree of elements of the subgroup F_K^t of the group F_K that contains the norm group $N_{L/K}(F_L^n)$.

Let K be a complete discrete variation field with the ring of integers O_K and the maximal ideal M_K.

A complete discrete variation field with finite residue field is called a *local* field [12].

A complete discrete variation field K with algebraically closed residue field k is called a *quasi-local* field [5]. Below we will suppose that in the case the characteristic of k satisfies $p > 0$.

Let K be a local or quasi-local field. If K is a local field [12] and has the characteristic 0 then it is a finite extension of the field of p-adic numbers $\mathbf{Q}_p$. Let ν_K be the normalized exponential valuation of K. If $[K : \mathbf{Q}_p] = n$ then $n = e \cdot f$, where $e = \nu_K(p)$ and $f = [k : \mathbf{F}_p]$, where k is the residue field of K (always assumed perfect).

If K has the characteristic $p > 0$ then it isomorphic to the field $k((T))$ of formal power series, where T is uniformizing parameter.

Let L be a finite extension of a local field K, k, l their residue fields, $p = char\ k$ and $e_{L/K}$ ramification index of L over K.

An extension L/K is said to be *unramified* if $e_{L/K} = 1$ and extension l/k is separable.

An extension L/K is said to be *tamely ramified* if p not devides $e_{L/K}$ and the residue extension l/k is separable.

An extension L/K is said to be *totally ramified* if $e_{L/K} = [L : K] = (char\ k)^s, s \geq 1$.

Let L/K be the finite Galois extension of quasi-local field K with Galois group G, $F(x, y)$ one dimensional formal group low over the ring of integers O_K of the field K, $F(M_K)$ be the G-module, that is defined by the group low $F(x, y)$ on the maxilal ideal M_K of the ring O_K, $M_K^t (t \in \mathbf{Z}, t \geq 1)$ be the subgroup of t-th degrees of elements from M_K, $F_K^t := F(M_K^t)$.

Definition 5.1 For $n \in \mathbf{Z}$ the function $\mu(n)$, $N_{L/K}(F_L^n) \subset F_K^{\mu(n)}$ is defined by the condition: $F_K^{\mu(n)}$ is the least of subgroups F_K^t $(t = 1, 2, \ldots)$ containes $N_{L/K}(F_L^n)$.

Below we will suppose that $char\ k > 3$.

5.2 Norm Maps

Here we use results on formal groups from [9–11, 13]. Let $F_L = F(M_L)$ be the G-module that is defined by the n-dimentional group low $F(x, y)$ on the product $(M_L)^n := M_L \times \cdots \times M_L$, ($n$ times) of maximal ideals of the ring O_L of any finite Galois extension L of the field K.

Definition 5.2 The norm map $N : F_L \to F_K$ of the module F_L to F_K is defined by the formula $N(a) = (((a +_F \sigma a) +_F \cdots) +_F \sigma_s a)$, where $a +_F b$ denotes the addition of points in the sense of group structure of the module F_L, $a, b \in M_L$, $G = Gal(L/K)$, $\sigma_s \in G$, $[G : 1] = s$.

Let $p := char\ k$, $e := \nu_K(p)$, ($e = +\infty$, if characteristic of the field K is equal p and e is positive integer in the opposide case), L/K be the Galois extension of the prime degree q, $F(x, y)$ be the one dimensional group low over O_K. Let $p := char\ k > 0$.

Lemma 5.1 *If $\Pi_s \in \pi_L^s \cdot O_L$, $s \geq 1$ then*
$N(\Pi_s) \equiv Tr(\Pi_s) + \sum_{n=1}^{\infty} c_n [Norm\ \Pi_s]^n (mod\ Tr(\pi_L^{2s} \cdot O_L))$
where $c_n \in O_K$ are coefficients of the p-iteration of the group low. The iteration is defined below.

(In paper [6] the lemma has proved for one dimensional group lows that correspond to elliptic curves)

Proof At first make two remarks:

1. If $F(x, y)$—one dimensional group low over the ring O_K, then p-iteration $[p]_F(T)$ of the group low F has the form [9]
   $[p]_F(T) = p(T + \cdots) + \sum_{i=1}^{\infty} c_i T^{pi}$,
   where dots denote intermediates of the degree greater than one.
2. If the series expansion of the expression $(((t_1 +_F t_2) +_F \cdots) +_F t_n)$ includes monomial ${t_1}^{\alpha_1} \cdots {t_q}^{\alpha_q}$, then it also includes a monomial that is the result of acting of arbitrary permutation of digits $1, 2, \ldots, q$ on it.

Let us go to the proof of the lemma. Let $G = Gal(L/K)$. If $\omega = r_1 + r_2\sigma + \cdots + r_q\sigma^{q-1}$ is an element of the group algebra $\mathbf{Z}[G]$ (where $\mathbf{Z}$ is the ring of integers). Let
$\Pi_s^{\omega} := \Pi_s^{r_1}(\sigma \Pi_s^{r_2}) \cdots (\sigma^{q-1} \Pi_s^{r_q})$.
We have $N(\Pi_s) = (((\Pi_s +_F \sigma \Pi_s) +_F \cdots) +_F \sigma^{q-1} \Pi_s) = \sum_{(r_1,\ldots,r_q)} d_{r_1,\ldots,r_q} \Pi_s^{\omega}$ where $d_{r_1,\ldots,r_q} \in O_K$, and sum by corresponding ω. By symmetry (see remark 2) in the expansion of $N(\Pi_s)$ with $d_{r_1,\ldots,r_q} \Pi_s^{\omega}$ comes also $d_{r_1,\ldots,r_q} \Pi_s^{\sigma^i \omega}$ ($i = 1, 2, \ldots, q-1$). Since
$\sigma^i \omega = \omega$
(i is one of numbers $i = 1, 2, \ldots, q-1$), so $\omega = n(1 + \sigma + \cdots + \sigma^{q-1})$. Hence

$$N(\Pi_s) = \sum_{n=1}^{\infty} d_n [Norm(\Pi_s)]^n + \sum_{\omega} d_{r_1,\ldots,r_q} Tr(\Pi_s^{\omega}), \tag{5.1}$$

where sum by ω such that do not satisfy the condition $\sigma^i \omega = \omega$.
If $r_1 + \cdots + r_q > 1$ then by ([14], lemma 2)
$Tr(\Pi_s^{\omega}) \subset Tr(\pi_L^{2s} \cdot O_L)$, hence

$$N(\Pi_s) \equiv Tr(\Pi_s) + \sum_{n=1}^{\infty} d_n [Norm\ \Pi_s]^n (mod\ Tr(\pi_L^{2s} \cdot O_L)). \tag{5.2}$$

Demonstrate that as a d_n we may take c_n from the expansion of $[p]_F(T)$. This follow from the fact that as d_n so c_n define to $mod\ p$.

Let $r := \nu_K(c_1), r_j := \nu_K(c_j),\ j > 1$ and let the height of F is $\infty > h \geq 1$; recall that $\nu_K(c_{p^{h-1}}) = 0$.

By ([14], lemma 2) $Tr(\pi_L^n \cdot O_L) = \pi_K^{y_0(n)}$ where $y_0(n) = \lfloor \frac{(m+1)(p-1)+n}{p} \rfloor$.

Put $y_1(n) = r + n,\ y_2(n) = r_2 + 2n, \ldots, y_{p-1}(n) = r_{p-1} + (p-1)n,\ y_p(n) = r_n + pn, \ldots, y_{p^{h-1}}(n) = r_n + pn.$

Lemma 5.2

$$\mu(n) = \min\{y_0(n), y_1(n), y_p(n), y_{p^2}(n), \ldots, y_{p^{h-1}}(n)\}. \tag{5.3}$$

Proof (we follow to [7]).

Define $\mu_1(n) = \min\{y_0(n), y_1(n), y_2(n), \ldots, y_p(n), y_{p^2}(n), \ldots, y_{p^{h-1}}(n)\}$.

It is clear since the estimation (5.2) that $\mu(n) \geq \mu_1(n)$ ($\mu(n)$ is understood in the sense of the definition 5.1). Choose Π_n such that $\nu_L(\Pi_n) = n$, $\nu_K(Tr(\Pi_n)) = y_0$.

Let $d \in O_K$. Consider expression $N(d\Pi_n)$. By (5.1) in the case $d \in O_K$ the terms from $N(d\Pi_n)$ that are included in the ideal $Tr(\pi_L^{2n})$ and have the form

$$Tr(\sigma^{i_1}(d\Pi_n)^{k_1} \cdots \sigma^{i_s}(d\Pi_n)^{k_s}) \tag{5.4}$$

under $k_1 + \cdots + k_s \geq p + 1$ will have the norm in K greater then $y_0(n)$. This follow from the computation by the formula for $y_0(n)$. Hence

$N(d\Pi_n) = \pi_K^{\mu_1(n)}[(\pi_K^{-\mu_1(n)} Tr(\Pi_n))d +$ (summands contain d from 2 to p-s degree, that obtained from terms of N(dΠ_n), that include in

$$Tr(\pi_L^{2n})) + \sum_{i=1}^{ph} \pi_K^{-\mu_1(n)} \times c_i [Norm(\Pi_n)]^i d^{pi} + \cdots] \tag{5.5}$$

where dots denote terms of higher orders.

Term $\pi_K^{\mu_1(n)}$ in (5.5) helds coefficient that is polynomial from d of degree not greater than p^h; if $\mu_1(n) = y_j(n)(j = 0, 2, 3, \dots, p^{h-1}$; j is different from 1) then the coefficient under d^{pj} is not equal zero $mod\ \pi_K$, hence $\mu(n) = \mu_1(n)$; if

$$\mu_1(n) = y_1(n) < y_0(n), y_2(n), \dots, y_p(n), y_{p^2}(n), \dots, y_{p^{h-1}}(n).$$

then terms from $N(d\Pi_n)$ that are included in $Tr(\pi_L^{2n})$, will have in K a norm that is not less then $y_0(n)$, hence only coefficient under d^p will differ from zero under $mod\ \pi_K$, hence again $\mu(n) = \mu_1(n)$. Hence always

$$\mu(n) = \mu_1(n).$$

Demonstrate now that actually

$$\mu_1(n) = \min\{y_0(n), y_1(n), y_p(n), y_{p^2}(n), \dots, y_{p^{h-1}}(n)\}.$$

We prove this by induction on n. If $n = 1$ and $\mu_1(1) = y_0(1)$ then the lemma is proved, and then

$y_0(1) \le y_i(1)$ $(i = 1, 2, 3, ..., p^{h-1})$ and all $y_i(n)$, $i \neq 0$ grow faster then $y_0(n)$.

If $\mu_1(1) = y_i(1) < y_0(1)$, $1 \le i \le p^{h-1}$ (specifically: $i = r_0$), then demonstrate at first that $\mu_1(n)$ is strictly increasing function

$$\mu_1(1) < \mu_1(2).$$

If $\mu_1(2) = y_{r_0}(2)$ $(r_0 \neq 0)$ then we have

$y_2(1) \le y_{r_0}(2)$, that is $\mu_1(1) < \mu_1(2)$.

But if $\mu_1(2) = y_0(2)$ then $\mu_1(1) = y_r(1) < y_0(1)$, hence $y_2(1) < y_0(1) \le y_0(2)$, and again $\mu_1(1) < \mu_1(2)$.

Thereby the homomorphism

$$F_L^1/F_L^2 \xrightarrow{N_1^*} F_K^{\mu_1(1)}/F_K^{\mu_1(1)+1} \tag{5.6}$$

that is induced by N is defined. Under $\pi_L - \pi_K$ isomorphisms [7] it passes to homomorphism $\overline{N}_1{}^* : G_a(l) \to G_a(k)$ where $G_a(k)$ is the additive group of the field $l = O_L/M_L$ that is defined by polynomial from (5.5) under reduction by $mod\ \pi_K$. But any homomorphism of additive groups of the field of characteristic $p > 0$ is given by the polynomial from $T, T^p, T^{p^2}, \dots$ (sums of degrees of Frobenius automorphism), hence in the case $n = 1$ the lemma is proved.

Let lemma is true for $n = n_0$. Prove it for $n = n_0 + 1$. If $\mu_1(n_0) = y_{n_0}(n)$ then the lemma is proved. If $\mu_1(n_0) = y_j(n_0)$ $(1 \le j \le p^{h-1}, j \neq 0)$ then we have

$$\mu_1(n_0) < \mu_1(n_0 + 1)$$

Ipso facto the homomorphism

$$F_L^{n_0}/F_L^{n_0+1} \xrightarrow{N_{n_0}^*} F_K^{\mu_1(n_0)}/F_K^{\mu_1(n_0)+1} \tag{5.7}$$

that is induced by N is defined. And again the passage to the homomorphism $\overline{N}_{n_0}{}^*$: $G_a(l) \to G_a(k)$ demonstrates that (5.3) takes place.

5.3 Results

Let $F(x, y)$ be the one dimensional formal groups of height 3 over integer ring of local and quasi-local fields K.

Consider the tower of fields

$$K = L_0 - L_1 - L_2 - \cdots - L_{s-1} - L_s \tag{5.8}$$

where L_i/L_{i-1}, $(i = 1, 2, \ldots, s)$ are Galois extensions with Galois groups $\mathbf{Z}/p\mathbf{Z}$.

Let $\mu_i(n)$ be the function of the definition 5.1 that is computed on the i-s floor of the tower (5.8) and let m_i be the number of the last nontrivial ramification group of the extension L_i/L_{i-1}.

Put $r_1 := \nu_K(c_p)$, $r_2 := \nu_K(c_{p^2})$, $e := \nu_K(p)$.

Lemma 5.3 *Depend on numbers r_1, r_2, e the function $\mu_i(n)$ is computed by the next four formulas:*

(i) *If $r_1, r_2 \geq e$ then the computation of the $\mu_i(n)$ makes by the formula*

$$\mu_i(n) = \begin{cases} p^2 n, n \leq \frac{m_i+1}{p^2+p+1} \\ \lfloor \frac{(m_1+1)(p-1)+n}{p} \rfloor, n > \frac{m_i+1}{p^2+p+1} \end{cases} \tag{A}$$

(ii) *If $\frac{r_2}{p^2} \leq \frac{e}{p^2+p+1} \leq \frac{r_1}{p^2+p}$ then the computation of the $\mu_i(n)$ makes by the formula*

$$\mu_i(n) = \begin{cases} p^2 n, n \leq \frac{r_2 p^{i-1}}{p(p-1)} \\ r_2 p^{i-1} + pn, \frac{r_2 p^{i-1}}{p(p-1)} < n < \left[\frac{(m_i+1)(p-1)+p^i r_2}{p^2-1}\right] \\ \lfloor \frac{(m_1+1)(p-1)+n}{p} \rfloor, n > \left[\frac{(m_i+1)(p-1)+p^i r_2}{p^2-1}\right] \end{cases} \tag{B}$$

(iii) *If $\frac{r_1}{p^2+p} \leq \frac{r_2}{p^2} \leq \frac{e}{p^2+p+1}$ then the computation of the $\mu_i(n)$ makes by the formula*

$$\mu_i(n) = \begin{cases} p^2 n, n \leq \frac{r_2 p^{i-1}}{(p^2-1)} \\ r_1 p^{i-1} + n, \frac{r_1 p^{i-1}}{(p^2-1)} < n < \left[\frac{(m_i+1)(p-1)+p^i r_1}{p-1}\right] \\ \lfloor \frac{(m_1+1)(p-1)+n}{p} \rfloor, n > \left[\frac{(m_i+1)(p-1)+p^i r_1}{p-1}\right] \end{cases} \tag{C}$$

(iv) *If $\frac{r_2}{p^2} \leq \frac{r_1}{p^2+p} \leq \frac{e}{p^2+p+1}$ then the computation of the $\mu_i(n)$ makes by the formula*

$$\mu_i(n) = \begin{cases} p^2 n, n \leq \frac{r_2 p^{i-1}}{p(p-1)} \\ r_2 p^{i-1} + pn, \frac{r_2 p^{i-1}}{p(p-1)} < n \leq \frac{(r_1 - r_2) p^{i-1}}{p-1} \\ r_1 p^{i-1} + n, \frac{(r_1 - r_2) p^{i-1}}{p-1} < n \leq \left\lceil \frac{(m_i+1)(p-1)+p^i r_1}{p-1} \right\rceil \\ \lfloor \frac{(m_1+1)(p-1)+n}{p} \rfloor, n > \left\lceil \frac{(m_i+1)(p-1)+p^i r_1}{p-1} \right\rceil \end{cases} \tag{D}$$

The lemma is proved by direct computation.

Let K be a local or quasi-local field and $F(x, y)$ be the one dimensional formal group over integer ring of K. Let $F_L = F(M_L)$ be the G-module that is defined by the group low $F(x, y)$ on the maximal ideal M_L of the ring O_L of any finite Galois extension L of the field K.

In the case when K is the quasi-local field it is possible, follow to Serre [15], induced on F_L the structure of the proalgebraic group. Denote the group as $\overline{F}_L$. Let $\pi_1(\overline{F}_L)$ be its fundamental group.

Definition 5.3 Let K be a local field, $N_{L/K} : F_L \to F_K$ the norm homomorphism. The subgroup

$$\mathcal{V}_K = \bigcap_K N_{L/K}(F_L)$$

(intersection on all finite Galois extensions L/K) of the group F_K is called the universal norm group of the group F defined over ring O_K.

If K is a quasi-local field, then the subgroup

$$\mathcal{V}_K^* = \bigcap_K N_{L/K}(\pi_1(\overline{F}_L))$$

(intersection on all finite Galois extensions L/K) of the group $\pi_1(\overline{F}_L)$ is called the universal norm group of the group F defined over ring O_K.

Theorem 5.2

$$\mathcal{V}_K \,(\text{respectively } \mathcal{V}_K^*) = 0.$$

Sketch of the proof We use an extension of the method of Vvedenskii [4] by which he prove the result for one dimensional fornal groups of reduction height 1 and 2 over integer ring of local and quasi-local fields.

If K is a local field, then the prove of the theorem reduced to the prove of the next lemma 5.4. If K is a quasi-local field, then we follow the method that has proposed in the paper [13]. In the case it is sufficient to prove that for any finite Galois extensions L/K the next equality and inclusion take place

$$N_{L/K}(\mathcal{V}_L^*) = \mathcal{V}_K^*$$

$$\mathcal{V}_L^* \subset p\pi_1(\overline{F}_L)$$

Lemma 5.4 *For any integer* n, $n \geq 1$ *there is such finite Galois extension* L/K, *that the image* $N_{L/K}(F_L)$ *(respectively* $N_{L/K}(\pi_1(\overline{F}_L))$*) of the norm homomorphism*

$$N_{L/K} : F_L \to F_K$$

(respectively $N_{L/K} : \pi_1(\overline{F}_L) \to \pi_1(\overline{F}_K)$*) is contained in* F_K^n *(respectively in* $\pi_1(\overline{F}_K)$*).*

References

1. Shafarevich, I.R.: Principal homogenious spaces over function fields (in Russian). Tr. Math. Steklov Inst. **64**, 316–346 (1961)
2. Tate, J.: Principal homogenious spaces for abelian varieties. J. Reine Angew. Math. **209**, 98–99 (1962)
3. Ogg, A.: Cohomology of abelian varieties over function fields. Ann. Math. **76**, 185–220 (1962)
4. Vvedenskii, O.N.: On local "class fields" of elliptic curves (in Russian). Izv. Akad. Nauk SSSR Math. USSR Izvestija Ser Mat. **37**(1), 20–88 (1973)
5. Vvedenskii, O.N.: On quasi-local "class fields" of elliptic curves I (in Russian). Izv. Akad. Nauk SSSR Math. USSR Izvestija Ser Mat. **40**(5), 969–992 (1976)
6. Vvedenskii, O.N.: Duality in elliptic curves over local fields I (in Russian). Izv. Akad. Nauk SSSR Math. USSR Izvestija Ser Mat. Tom **28**(4), 1091–1112 (1964)
7. Vvedenskii, O.N.: Duality in elliptic curves over local fields II (in Russian). Izv. Akad. Nauk SSSR Math. USSR Izvestija Ser Mat. Tom **30**(4), 891–922 (1966)
8. Glazunov, N.M.: On the "norm subgroups" of one-parameter formal groups over integer ring of local field (in Russian). Dokl. Akad. Nauk Ukr. SSR, Ser. A **11**, 965–968 (1973)
9. Lubin, J.: One parameter formal Lie groups over ρ-adic integer rings. Ann. Math. **80**(3), 464–484 (1964)
10. Glazunov, N.M.: Remarks on n-dimensional commutative formal groups over integer ring of ρ-adic field (in Russian). Ukr. Math. J. **25**(3), 352–355 (1973)
11. Hazewinkel, M.: Formal Groups. Academic Press, New York (1977)
12. Cassels, J., Fröhlich, A. (eds.): Algebraic Number Theory. Academic Press, London (2003)
13. Vvedenskii, O.N.: On "universal norms" of formal groups over integer ring of local fields (In Russian). Izv. Akad. Nauk SSSR Math. USSR Izvestija Ser Mat. Tom **37**, 737–751 (1973)
14. Glazunov, N.M.: Quasi-local class fields of elliptic curves and formal groups I. Proc. IAMM NANU **24**, 87–98 (2012)
15. Serre, J.-P. Géométrie algébrique. In: Proceedings of the International Congress of Mathematicians, pp.190–196. Institut Mittag-Leffler, Djursholm (1963)