УДК 513.6

Г. Т. Коновалов

Про нормові підгрупи формальних груп над локальним полем

У класичній локальній теорії полів класів і при побудові аналога цієї теорії для абелевих многовидів виникає питання про співвідношення між замкненими підгрупами скінченного індексу у відповідних групах і підгру-

пами норм (див., наприклад, [1—3]). У роботі О. М. Введенського [4] звертається увага на можливість постановки цього питання в більш загальній ситуації при вивченні арифметичних властивостей формальних груп. У цій замітці проводиться таке узагальнення для випадку довільних комутативних багатопараметричних формальних груп, визначених над кільцем цілих p-адичних чисел, $p > 2$.

Нехай k — повне дискретне нормоване поле з скінченним полем лишків $\varkappa$, $p = \operatorname{char} \varkappa$, l/k — скінченне сепарабельне розширення, $\mathfrak{o}_l$ — його кільце цілих, U_l, $\mathfrak{m}_l$ і π_l — відповідно група одиниць, максимальний ідеал і простий елемент кільця $\mathfrak{o}_l$, $F(X, Y)$ — визначена над $\mathfrak{o}_k$ комутативна n-параметрична формальна група, F_l — група, що одержується на добутку $\mathfrak{m}_l \times \ldots \times \mathfrak{m}_l$ (n разів) за допомогою $F(X, Y)$, $\oplus$ — закон композиції в F_l, F_l^{λ} для натурального λ — підгрупа в F_l, елементи якої належать $\mathfrak{m}_l^{\lambda} \times \ldots \times \mathfrak{m}_l^{\lambda}$ (n разів), $p^u F_l$ для цілого $u \geqslant 0$ — образ F_l при u-й ітерації гомоморфізму множення на p в F_l. Очевидно визначається нормовий гомоморфізм $N_{l/k} : F_l \to F_k$, образ якого називається нормовою підгрупою в F_k. Фільтрація F_l^{λ} задає на F_l топологію, в якій множення на p і нормовий гомоморфізм неперервні.

Теорема. *Нехай k — поле p-адичних чисел для $p > 2$ і $F(X, Y)$ — визначена над $\mathfrak{o}_k$ комутативна n-параметрична формальна група. Тоді для довільної замкненої підгрупи $\mathfrak{A}$ індексу $I < \infty$ в F_k існує сепарабельне розширення l/k таке, що $[l : k]$ ділить I^n і $N_{l/k}(F_l) \subset \mathfrak{A}$.*

Доведення. Тому що $I = p^r$ для деякого натурального r, то доведення можна проводити індукцією по r.

Нехай $r = 1$. Використаємо для цього випадку підхід П. А. Медведєва [3].

Якщо k — поле p-адичних чисел для $p > 2$, то $pF_k = F_k^2$ [5, с. 204]. Тому що $\mathfrak{A} \supset pF_k$, то $\mathfrak{A}/pF_k$ можна ототожнити з підпростором корозмірності 1 лінійного простору $F_k/pF_k \cong (Z/pZ)^n$. Тоді $\mathfrak{A}/pF_k$ задається як підпростір, ортогональний до деякого елемента з F_k/pF_k. Таким чином, існують такі $b_i \in \mathfrak{o}_k$, $i = 1, 2, \ldots, n$, хоч один з яких належить U_k, що підгрупа $\mathfrak{A}$ задається як множина таких елементів $\begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix} \in F_k$, що

$$b_1 X_1 + b_2 X_2 + \ldots + b_n X_n \equiv 0 \pmod{p^2}.$$

Потрібне l/k будемо шукати серед дико розгалужених розширень степеня p^v над k, де v — деяке натуральне число.

Нехай $(x)_j$ для $j = 1, 2, \ldots, n$ — стовпчик розмірності n з j-ю координатою x і нульовими іншими координатами. Досить показати, що для деякого дико розгалуженого l/k, $[l : k] \leqq p^n$, елементи

$$N_{l/k}((\pi_l^{\gamma})_j), \quad j = 1, 2, \ldots, n; \ \gamma = 1, 2, \ldots, \tag{1}$$

містяться в $\mathfrak{A}$, тому що будь-який елемент з $N_{l/k}(F_l)$ для дико розгалужених l/k зображується сумою (у сенсі $F(X, Y)$) таких елементів. Крім того, досить обмежитись розглядом елементів (1) з $\gamma \not\equiv 0 \pmod{p}$, бо якщо γ ділиться на p, то π_l^{γ} у цих елементах можна поміняти на $\pi_m^{\gamma/p}$, де m — підрозширення l/k таке, що $[l : m] = p$, і тоді

$$N_{l/k}((\pi_m^{\gamma/p})_j) = pN_{m/k}((\pi_m^{\gamma/p})_j) \in \mathfrak{A}.$$

Нехай $s_t(x)$ для $t = 1, 2, \ldots, p^v$ — елементарна симетрична функція степеня t від $x_1, x_2, \ldots, x_{p^v}$. Запишемо вираз $N_v((x)_j) = (x_1)_j \oplus (x_2)_j \oplus \ldots \ldots \oplus (x_{p^v})_j$ у вигляді

$$N_v((x)_j) = A_v^j \begin{pmatrix} s_1(x) \\ s_p(x) \\ s_{p^2}(x) \\ \vdots \\ s_{p^v}(x) \end{pmatrix} + \ldots, \tag{2}$$

де через A_v^j позначена матриця з n рядків і $v+1$ стовпчика, що складена з коефіцієнтів при $s_p i(x)$, $i = 0, 1, \ldots, v$, у зображенні виразу $N_v((x)_j)$ у вигляді сукупності n рядів над $\mathfrak{o}_k$ від $s_1(x)$, $s_2(x)$, $\ldots$, $s_p^v(x)$, а крапками позначена решта членів цього зображення.

Тому що матриця A_v^j одержується з матриці A_{v-1}^j додаванням нового $(v+1)$-го стовпчика (для перевірки цієї властивості досить в (2) покласти $x_{p^{v-1}+1} = x_{p^{v-1}+2} = \ldots = x_{p^v} = 0$), то для деякого натурального $v \leqq n$ існують такі $c_i \in \mathfrak{o}_k$, $i = 0, 1, \ldots, v-1$, що

$$(b_1, b_2, \ldots, b_n) A_v^j \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{v-1} \\ 1 \end{pmatrix} \equiv 0 \pmod{p}$$

для всіх $j = 1, 2, \ldots, n$.

Зафіксуємо вказані v і $c_0, c_1, \ldots, c_{v-1}$, і покажемо, що розширення l/k, породжене над k коренем π_l рівняння Ейзенштейна

$$x^{p^v} - \sum_{i=0}^{v-1} c_i p x^{p^v - p^i} - p = 0, \tag{3}$$

є шукане.

Покладаючи в (2) $x_i = \sigma_i(\pi_l^\gamma)$, де σ_i для $i = 1, 2, \ldots, p^v$ — всі ізоморфні вкладення l над k у сепарабельне замкнення поля k, зобразимо елементи (1) у вигляді сукупності n рядів над $\mathfrak{o}_k$ від $s_t(\pi_l^\gamma)$, $t = 1, 2, \ldots, p^v$. Вирази $s_t(\pi_l^\gamma)$ можна зобразити у вигляді многочленів від $s_{p^i}(\pi_l)$, $i = 0, 1, \ldots \ldots, v$. Якщо $\gamma > 1$, то в такий многочлен не може входити одночлен $s_{p^i}(\pi_l)$, $i = 0, 1, \ldots, v$, бо розглядаються лише ті елементи (1), у яких $\gamma \not\equiv 0 \pmod{p}$. Таким чином, $s_t(\pi_l^\gamma)$ для $\gamma > 1$, $\gamma \not\equiv 0 \pmod{p}$, діляться на p^2, бо всі $s_{p^i}(\pi_l)$ діляться на p за вибором рівняння (3). Нарешті

$$N_{l/k}((\pi_l)_j) \equiv A_v^j \begin{pmatrix} c_0 p \\ c_1 p \\ \vdots \\ c_{v-1} p \\ p \end{pmatrix} \pmod{p^2},$$

і для завершення доведення основи індукції лишається врахувати вибір $c_0, c_1, \ldots, c_{v-1}$.

Проведемо тепер індукційний перехід. Відзначимо, що він вірний для довільного повного дискретного нормованого поля k з скінченним полем лишків.

Нехай для $r \leqq w-1$ теорему доведено. Розглянемо в F_k підгрупу $\mathfrak{A}$ індексу p^w і покажемо, що існує сепарабельне розширення l/k таке, що $[l:k]$ ділить p^{wn} і $N_{l/k}(F_l) \subset \mathfrak{A}$.

Розглянемо спочатку випадок, коли $\mathfrak{A} \supset pF_k$. У цьому випадку підгрупа $\mathfrak{A}$ задається як перетин w підгруп індексу p в F_k. Позначимо ці підгрупи через $\mathfrak{A}_i$, $i = 1, 2, \ldots, w$. Тоді за доведеною основою індукції, існують сепарабельні розширення l_i/k, $i = 1, 2, \ldots, w$, такі, що $[l_i : k]$ ділять p^n і $N_{l_i/k}(F_{l_i}) \subset \mathfrak{A}_i$, і композит $l = l_1 \cdot l_2 \ldots l_w$ дає шукане розширення для підгрупи $\mathfrak{A}$.

Перейдемо тепер до випадку, коли $\mathfrak{A} \not\supset pF_k$. У цьому випадку шукане l/k будемо будувати таким способом.

Розглянемо в F_k підгрупу $\mathfrak{A}_1 = p^{-1}(\mathfrak{A} \cap pF_k)$ (за неперервністю гомоморфізму множення на p ця підгрупа замкнена), і розглянемо такі комутативні діаграми з точними рядками і стовпчиками:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathfrak{A} \cap pF_k & \to & \mathfrak{A} & \to & \mathfrak{A} \oplus pF_k/pF_k & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & pF_k & \to & F_k & \to & F_k/pF_k & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & A & \to & B & \to & C & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{4}$$

$$\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow 1 & & \downarrow & & \\
0 & \to & \operatorname{Ker} p & \to & \operatorname{Ker} p & \to & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathfrak{A}_1 & \to & F_k & \to & A_1 & \to & 0 \\
 & & \downarrow p & & \downarrow p & & \downarrow & & \\
0 & \to & \mathfrak{A} \cap pF_k & \to & pF_k & \to & A & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{5}$$

У діаграмі (4) $C \neq 0$. Дійсно, нехай u — таке натуральне число, що $\mathfrak{A} \supset p^u F_k$ і $\mathfrak{A} \not\supset p^{u-1} F_k$. Якщо $C = 0$, то $\mathfrak{A} \oplus pF_k = pF_k$, звідки $p^{u-1}\mathfrak{A} \oplus \oplus p^u F_k = p^{u-1} F_k$, тобто $\mathfrak{A} \supset p^{u-1} F_k$, що суперечить вибору u.

Таким чином, як бачимо з діаграм (4) і (5) з врахуванням останнього зауваження, $[F_k : \mathfrak{A}_1] = [A : 1] < p^\omega$, і за припущенням індукції існує таке сепарабельне розширення m/k, що $[m : k]$ ділить $[A : 1]^n$ і $N_{m/k}(F_m) \subset \mathfrak{A}_1$.

Розглянемо тепер в F_m підгрупу $\mathfrak{A}_2 = N_{m/k}^{-1}(\mathfrak{A} \cap N_{m/k}(F_m))$ (за неперервністю нормового гомоморфізму ця підгрупа замкнена). Для доведення індукційного переходу досить показати, що $[F_m : \mathfrak{A}_2] \leqq [C : 1] < p^\omega$. Дійсно, тоді за припущенням індукції існує сепарабельне розширення l/m таке, що $[l : m]$ ділить $[C : 1]^n$ і $N_{l/m}(F_l) \subset \mathfrak{A}_2$, і розширення l/k є шукане для підгрупи $\mathfrak{A}$.

Покажемо спочатку, що $[C : 1] < p^\omega$. Інакше в діаграмі (4) $A = 0$, тобто $\mathfrak{A} \supset pF_k$, що не відповідає розглядуваному випадку.

Нарешті, покажемо, що $[F_m : \mathfrak{A}_2] \leqq [C : 1]$. Розглянемо такі дві комутативні діаграми з точними рядками і стовпчиками:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \to & \operatorname{Ker} N_{m/k} & \to & \operatorname{Ker} N_{m/k} & \to & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \mathfrak{A}_2 & \to & F_m & \to & F_m/\mathfrak{A}_2 & \to & 0 \\
 & & \downarrow N_{m/k} & & \downarrow N_{m/k} & & \downarrow & & \\
0 & \to & \mathfrak{A} \cap N_{m/k}(F_m) & \to & N_{m/k}(F_m) & \to & C_1 & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \tag{6}$$

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathfrak{A} \cap N_{m/k}(F_m) & \to & N_{m/k}(F_m) & \to & C_1 \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathfrak{A} & \to & F_k & \to & B \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathfrak{A} \oplus N_{m/k}(F_m)/N_{m/k}(F_m) & \to & F_k/N_{m/k}(F_m) & \to & A_2 \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
\end{array} \qquad (7)$$

Як бачимо з діаграм (4), (6), (7), досить довести, що $[A_2 : 1] \geqslant [A : 1]$. Потрібна нерівність одержується з такої комутативної діаграми з точними рядками і стовпчиками:

$$\begin{array}{ccccccc}
0 & \to & \mathfrak{A} \oplus N_{m/k}(F_m) & \to & F_k & \to & A_2 \to 0 \\
 & & \downarrow p & & \downarrow p & & \downarrow \\
0 & \to & \mathfrak{A} \cap pF_k & \to & pF_k & \to & A \to 0 \\
 & & & & \downarrow & & \downarrow \\
 & & & & 0 & & 0
\end{array}$$

(нагадаємо, що $N_{m/k}(F_m) \subset \mathfrak{A}_1 = p^{-1}(\mathfrak{A} \cap pF_k)$).

Теорему доведено.

На закінчення висловлюю щиру подяку О. М. Введенському, під керівництвом якого виконана ця работа.

ЛІТЕРАТУРА

1. Алгебраическая теория чисел. М., «Мир», 1969.
2. Введенский О. Н. Подгруппы норм в эллиптических кривых, определенных над локальным полем.— УМЖ, 1970, **22**, № 4, с. 531—533.
3. Медведев П. А. Порядок и показатель эллиптической кривой.— Изв. АН СССР. Сер. мат., 1966, **30**, № 5, с. 1179—1192.
4. Введенский О. Н. О локальных «полях классов» эллиптических кривых.— Изв. АН СССР. Сер. мат., 1973, **37**, № 1, с. 20—88.
5. Серр Ж.-П. Алгебры Ли и группы Ли, М., «Мир», 1969.

ОЦ при Львівському відділенні
Інституту економіки АН УРСР

Надійшла до редакції
30.I 1975 р.