ВІСНИК ЛЬВІВСЬКОГО ОРДЕНА ЛЕНІНА ДЕРЖАВНОГО УНІВЕРСИТЕТУ ім. Ів. ФРАНКА
1965 *Серія механіко-математична* *Випуск 2*

О. М. ВВЕДЕНСЬКИЙ

ПРОАЛГЕБРАЇЧНІ ГРУПИ З ВИСОТОЮ ДВА РЕДУКЦІЇ

0. Мета цієї замітки — викласти елементарні властивості підгрупи Лютц [1] Γ_L проалгебраїчної групи раціональних над конечним розширенням Галуа L повного дискретно нормованого поля K з алгебраїчно замкненим полем лишків k характеристики $p>3$ точок еліптичної кривої

$$y^2=x^3+ax+b \quad (a,\ b\in O_K;\ 4a^3+27b^2\not\equiv 0 \pmod t),$$

де O_K — кільце цілих в K, а t — його уніформізуюча, причому інваріант Хассе редукції A' кривої A рівний нулеві. Але всі результати залежать від того факту, що підгрупа Лютц як аналітична група Лі над O_K, що має проалгебраїчну структуру, сумісну з аналітичною, група, редукція якої (в розумінні зведення коефіцієнтів по mod t) є формальна група висоти 2 над O_K [2].

1. Для нашого випадку неважко довести, що точна послідовність редукції

$$0\to\Gamma_L\to A_L\to A'\to 0$$

розпадається. Підгрупа Лютц Γ_L є аналітичною групою Лі над O_K, груповий закон якої

$$z_1\circ z_2=(z_1+z_2)(1+\ldots)$$

задає формальна група, що відповідає A. Коли $z\in t^n\cdot O_K$, а $n=1, 2, \ldots$, ми одержуємо фільтрацію

$$\Gamma_L=\Gamma_L^1\supset\Gamma_L^2\supset\ldots,$$

причому $\Gamma_L^n/\Gamma_L^{n+1}\approx G_a$ (адитивній групі поля k).

Якщо

$$z\circ\cdots\circ z=p(z+\ldots)+\sum_{s=1}^{\infty}c_sz^{ps}\ (c_s\in O_K) \tag{1}$$

p-а ітерація формальної групи, що відповідає A, то c_p — одиниця в K, а $c_1, \ldots, c_{p-1}\in t\cdot O_K$. Нехай $r=\nu_K(c_1)$ — норма c_1 в K, $e=\nu_K(p)$ — норма p в K і

$$e_2=\frac{e}{p^2-1},\quad h_1=\frac{r}{p(p-1)},\quad h_2=\frac{e-r}{p-1}.$$

Пропозиція 1. Гомоморфізм u множення на p в Γ_K відображає Γ_K^n у $\Gamma_K^{\lambda(n)}$, де у випадку

1) характеристика K дорівнює p, інваріант Хассе у A рівний нулю — буде $\lambda(n)=p^2n$;

2) те ж, але інваріант Хассе у A, відмінний від нуля — буде

$$\lambda(n)=\begin{cases}p^2n, & n\leqslant h_1,\\ pn+r, & n\geqslant h_1;\end{cases}$$

3) характеристика K дорівнює 0, $h_1\geqslant e_2$ буде

$$\lambda(n)=\begin{cases}p^2n, & n\leqslant e_2\\ n+e, & n\geqslant e_2;\end{cases}$$

4) те ж, але $h_1<e_2$ буде

$$\lambda(n)=\begin{cases}p^2n, & n\leqslant h_1,\\ pn+r, & h_1\leqslant n\leqslant h_2,\\ n+e, & n\geqslant h_2\end{cases}$$

і визначає епіморфізми

$$\Gamma_K^n/\Gamma_K^{n+1}\xrightarrow{u_n}\Gamma_K^{\lambda(n)}/\Gamma_K^{\lambda(n)+1},$$

які при відповідних ізоморфізмах переходять у гомоморфізми

$$G_a\xrightarrow{u_n}G_a$$

вигляду (у всіх випадках $\bar\alpha,\bar\beta,\bar\gamma\in k$; $\bar\alpha,\bar\beta,\bar\gamma\neq 0$) у випадку

1) $\bar u_n(\bar z)=\bar\alpha\bar z^{p^n}$;

2) $$\bar u_n(\bar z)=\begin{cases}\bar\alpha\bar z^{p^n}, & n<h_1,\\ \bar\alpha\bar z^{p^n}+\bar\beta\bar z^{p}, & n=h_1,\\ \bar\beta\bar z^{p}, & n>h_1;\end{cases}$$

3) $$\bar u_n(\bar z)=\begin{cases}\bar\alpha\bar z^{p^n}, & n<e_2,\\ \bar\alpha\bar z^{p^n}+\bar\gamma\bar z, & n=e_2\ (h_1>e_2),\\ \bar\alpha\bar z^{p^n}+\bar\beta\bar z^{p}+\bar\gamma\bar z, & n=e_2\ (h_1=e_2),\\ \bar\gamma\bar z, & n>e_2;\end{cases}$$

4) $$\bar u_n(\bar z)=\begin{cases}\bar\alpha\bar z^{p^n}, & n<h_1,\\ \bar\alpha\bar z^{p^n}+\bar\beta\bar z^{p}, & n=h_1,\\ \bar\beta\bar z^{p}, & h_1<n<h_2,\\ \bar\beta\bar z^{p}+\bar\gamma\bar z, & n=h_2,\\ \bar\gamma\bar z, & n>h_2\end{cases}$$

і $\Gamma_K\approx W^e$ (добуток екземплярів адитивної групи W векторів Вітта над k), якщо має місце випадок

1), 2) (коли h_1 не ціле), 3) (коли e_2 не ціле), 4) (коли h_1 і h_2 не цілі),

має місце точна послідовність проалгебраїчних груп (Z_p — група цілих p-адичних чисел)

$$0 \to Z_p \to W^e \to \Gamma_L \to 0,$$

якщо має місце випадок 2) (коли h_1 ціле), 4) (коли або h_1 ціле, а h_2 — не ціле, або навпаки); має місце точна послідовність проалгебраїчних груп

$$0 \to Z_p^2 \to W^e \to \Gamma_L \to 0$$

у випадках 3) (коли e_2 — ціле) та 4) (коли h_1, h_2 — цілі).

Доведення. З (1) випливає, що $\lambda(n)$ строго зростаюча функція, яка визначає гомоморфізм

$$\Gamma_K^n / \Gamma_K^{n+1} \xrightarrow{u_n} \Gamma_K^{\lambda(n)} / \Gamma_K^{\lambda(n)+1}.$$

Але ендоморфізм G_a визначається поліномом, в розклад якого входять лише степені x, які є степенями p. Залишається зробити елементарні підрахунки.

Наслідок 1. p-компонента кручення групи A_K конечна. Доведення класичне.

Наслідок 2. p-компонента $\pi_1(A_K)$ ізоморфна $\pi_1(W)^e \times X$, де X — добуток не більш як двох множників Z_p.

Доведення — очевидне.

Відзначимо, що r може бути довільним — це випливає з властивостей полінома, який задає інваріант Хассе [3].

2. Нехай L/K — розширення Галуа з простою циклічною групою g. Обчислимо групи когомологій

$$H^n(g, \Gamma_L),$$

які дадуть нам деяку інформацію про групи когомологій і розширень з більшою групою Галуа. Тут обчислення проводиться за класичною схемою [4].

Якщо N-нормений гомоморфізм g-модуля Γ_L і $\Gamma_L^{\mu(n)}$ — найменша з підгруп Γ_K^s, $s=1, 2, \ldots$, яка містить $N(\Gamma_L^n)$, то детальне вивчення формули

$$N(z) \equiv Trz + \sum_{s=1}^{\infty} c_s [\mathrm{Norm}\, z]^s \pmod{TrP^{2n}}$$

($z \in P^n$, де P — максимальний ідеал кільця цілих поля K), приводить до висновку

Лема 1. $\mu(n) = \min\left\{\left[\frac{(m+1)(p-1)+n}{p}\right],\ r+n,\ pn\right\}$, де $[v]$ — ціла частина дійсного числа v, а m — номер останньої відмінної від одиниці групи вітвлення розширення L/K.

Доведення. Те, що

$$\mu(n) = \min\left\{\left[\frac{(m+1)(p-1)+n}{p}\right],\ r+n,\ v_K(c_2)+ \right.$$

$$\left. +2n, \ldots, v_K(c_{p-1})+(p-1)n,\ pn\right\},$$

майже тривіально. Але, коли $\mu(n) \neq \left[\frac{(m+1)(p-1)+n}{p}\right] \Rightarrow \mu(n+1) > \mu(n)$, тобто визначений гомоморфізм

$$\Gamma_L^n / \Gamma_L^{n+1} \xrightarrow{N_n^*} \Gamma_K^{\mu(n)} / \Gamma_K^{\mu(n)+1}, \tag{2}$$

який як ендоморфізм G_a повинен мати «добрий» вигляд. Звідси випливає результат.

Наслідок. Коли $\frac{r}{p-1} \geqslant \frac{m+1}{p+1}$,

$$\mu(n) = \begin{cases} pn \text{ при } n \leqslant \frac{m+1}{p+1}, \\ \left[\frac{(m+1)(p-1)+n}{p}\right] \text{ при } n \geqslant \frac{m+1}{p+1}; \end{cases}$$

коли $\frac{r}{p-1} < \frac{m+1}{p+1}$, то

$$\mu(n) = \begin{cases} pn, \ n \leqslant \frac{r}{p-1}, \\ n+r, \ \frac{r}{p-1} \leqslant n \leqslant m+1-\frac{pr}{p-1}, \\ \left[\frac{(m+1)(p-1)+n}{p}\right], \ n \geqslant m+1-\frac{pr}{p-1}. \end{cases}$$

Нехай J — доповнення $\mu(Z_+)$ у Z_+.

Лема 2. Якщо n таке, що $\mu(n+1) > \mu(n)$, то мають місце точні послідовності

$$0 \to (N(\Gamma_L))^{\mu(n)} / (N(\Gamma_L))^{\mu(n)+1} \to \Gamma_K^{\mu(n)} / \Gamma_K^{\mu(n)+1} \to 0;$$

для всіх $j \in J$

$$(N(\Gamma_L))^j / (N(\Gamma_L))^{j+1} = 0.$$

Доведення. Вивчаємо за допомогою леми 1 гомоморфізм (2). Перша частина леми тривіальна. Обчислюємо $J : J$ складається з усіх взаємно-простих з p чисел при $\frac{r}{p-1} \geqslant \frac{m+1}{p+1}$ у випадку

1*) $m \equiv p \pmod{(p+1)}$ не більших $p\frac{m+1}{p+1}$;

2*) $m \equiv 0 \pmod{(p+1)}$ не більших $p\frac{m}{p+1}$;

3*) $m \equiv l \pmod{(p+1)}$, $0 < l < p$ не більших $p\frac{m+1}{p+1} + \frac{l-2p-1}{p+1}$,

а при $\frac{r}{p-1} < \frac{m+1}{p+1}$ у випадку

4*) $r \equiv 0 \pmod{(p-1)}$ не більших $p\frac{r}{p-1}$;

5*) $\frac{m+1}{p+1} \geqslant \frac{r}{p-1} + \frac{p}{p^2-1}$, $\left(\frac{r}{p-1} + \alpha\right)$ — ціле, де $0 < \alpha < 1$, — не більших $p\frac{r}{p-1} + \alpha - 1$;

6*) $\frac{m+1}{p+1} < \frac{r}{p-1} + \frac{p}{p^2-1}$, $\left(\frac{r}{p-1} + \alpha\right)$ — ціле, $0<\alpha<1$, — не більших $p\frac{r}{p-1} + \alpha - 1$; $\frac{m+1}{p+1} - \frac{r}{p-1} - \frac{\alpha}{p+1} \geqslant 0$;

7*) $\frac{m+1}{p+1} < \frac{r}{p-1} + \frac{p}{p^2-1}$, $\left(\frac{r}{p-1} + \alpha\right)$ — ціле, $0<\alpha<1$, а $\frac{m+1}{p+1} - \frac{r}{p-1} - \frac{\alpha}{p+1} < 0$ — не менших $p\frac{r}{p-1} + \alpha - 2$.

З доведення леми 2 неважко знайти, що при значеннях n, які задовольняють нерівності у випадку

1*) $n < \frac{m+1}{p+1}$, 2*) $n < \frac{m}{p+1}$, 3*) $n \leqslant \frac{m+1}{p+1} - \frac{l+1}{p+1}$,

4*) $n < \frac{r}{p-1}$, 5*)–7*) $n \leqslant \frac{r}{p-1} + \alpha - 1$,

N_n^* у (2) ізоморфізми (квазіалгебраїчних груп). Звідси легко одержати другу частину леми 2.

Пропозиція 2. $H^0(g, \Gamma_L)$ зв'язна і ізоморфна зв'язній компоненті $H^1(g, \Gamma_L)$, яка у випадках, наведених раніше, є прямою сумою такого числа екземплярів G_a:

1*) $(p-1)\frac{m+1}{p+1}$, 2*) $(p-1)\frac{m}{p+1}$, 3*) $(p-1)\left(\frac{m+1}{p+1} - \frac{l+1}{p+1}\right) + (l-1)$, 4*) – 6*) r, 7*) $r-1$;

зв'язна компонента $H^1(g, \Gamma_L)$ є прямим додатком останньої, а нульвимірна компонента $\pi_0 H^1(g, \Gamma_L)$ є у випадках

2*) $(Z/pZ)^2$, 4*) $(Z/pZ)^2$,

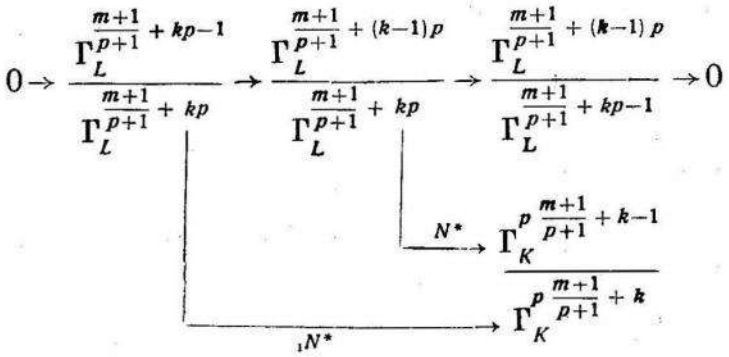
а в інших — тривіальна.

Доведення. Спуск по точних послідовностях вигляду

$$0 \to \Gamma_K^2 / N(\Gamma_L) \to \Gamma_K^1 / N(\Gamma_L) \to G_a \to 0$$

дозволяє визначити $H^0(g, \Gamma_L)$ як розширення деякого числа груп G_a. Залишається врахувати попередні обчислення і відомий результат Серра [5].

Для підрахунку $H^{-1}(g, \Gamma_L)$ треба використати $(I_g \cdot \Gamma_L) = (\mathrm{Ker}\, N)^{m+1}$ (у позначеннях роботи [6]), лему 1 і підрахунки такого типу: якщо в комутативній діаграмі (випадок 1)



${}_1N^*$ — ізоморфізм, то $\operatorname{Ker} N^* \approx G_a^{p-1}$, використовуючи той же результат Серра [5], що і треба було довести.

Зазначимо, що пропозиція 2 має місце для значно ширшого класу груп, але нам будуть потрібні конкретні обчислення для даного випадку; до інших ми повернемося іншим разом.

Наслідок. $H^{1-n}(g, \pi_1(\Gamma_L))^* \approx H^n(g, \Gamma_L)$.

Доведення. З точної послідовності накриття випливає точна послідовність

$$0 \to \pi_0(H^{-n}(g, \Gamma_L)) \to H^{1-n}(g, \pi_1(\Gamma_L)) \to \pi_1(H^{1-n}(g, \Gamma_L)) \to 0.$$

Залишається врахувати пропозицію 2 і дуальність Серра [7].

Відмітимо, що для абелевих g і для проалгебраїчних груп з висотою редукції 3 це вже не має місця. Викладки будуть наведені.

Примітка. З наведених результатів випливає дуальність $\pi_1(A_K)$ і групи головних однорідних просторів над полем нульової характеристики.

ЛІТЕРАТУРА

1. E. Lutz. Journ. für Math., **177**, 238—247 (1937).
2. J. Diendonné. Amer. J. Math., **77**, 218—244 (1955).
3. M. Deuring. Abh. Sem. Hamb., **14**, 197—272 (1941).
4. J.—P. Serre. Bull. Math. France, **89**, 105—154 (1961).
5. J.—P. Serre. Groupes algebriques.., Paris, 1959.
6. О. Введенский. Изв. АН СССР, **28**, 1091—1112 (1964).
7. J.—P. Serre. Groupes proalgebriques, I.H.E.S., Publ. Math., № 7 (1960).

О. Н. ВВЕДЕНСКИЙ

ПРОАЛГЕБРАИЧЕСКИЕ ГРУППЫ С ВЫСОТОЮ ДВА РЕДУКЦИИ

(резюме)

Исследуются элементарные свойства подгруппы Лютц эллиптической кривой.