О. М. ВВЕДЕНСЬКИЙ

КОГОМОЛОГІЇ ПІДГРУПИ ЛЮТЦ ЕЛІПТИЧНОЇ КРИВОЇ*

Нехай K — локальне поле (тобто дискретно нормоване поле, повне відносно топології, яка визначена цією нормою) з алгебраїчно замкненим полем лишків k характеристики $p > 3$. L — конечне нормальне розширення K з групою Галуа g, Q_K і ν_K (відповідно Q_L і ν_L) — кільце цілих і норма в K (відповідно в L). T — уніформізуюча L, а P (відповідно p_1) — максимальний ідеал Q_L (відповідно Q_K).

Розглядаємо над K еліптичну криву A:

$$y^2 = x^3 + ax + b \quad (a, b \in Q_K;\ 4a^3 + 27b^2 \not\equiv 0 \pmod{p_1}). \tag{1}$$

Має місце точна послідовність

$$0 \to S_K \to A_K \xrightarrow{j} A' \to 0, \tag{2}$$

де A_K — група раціональних над K точок A, A' — редукція (1) кривої A, j — епіморфізм редукції, S_K — ядро редукції. Ми допустимо, що інваріант Хассе (2) у A' відмінний від нуля.

Мета цієї роботи — визначити $H^q(g, S_L)$ (Тейтовські когомології (3)) за допомогою локальної теорії полів класів (4).

Припустимо спочатку, що $[g:1] = p$.

Лема 1. (Серр (4)). Диферента D розширення L/K дорівнює P^m, де $m = (l+1)(p-1)$, а l — номер останньої, відмінної від одиниці, групи вітвлення (5):

$$g = g_0 = g_1 = \ldots = g_l;\ g_{l+1} = \ldots = \{1\}.$$

Лема 2. (Серр (4)). Нехай $Tr: L \to K$ слід розширення L/K. Покладемо $m = (l+1)(p-1)$. Для всіх цілих $s \geqslant 1$ буде

$$Tr(P^s) = p_1^r,$$

де $r = \left[\frac{m+s}{p}\right]$,

$[x]$ — ціла частина дійсного числа x.

Підгрупу S_L можна параметризувати (6) так, що додаванню елементів, які відповідають значенням t_1 і t_2 параметра t, відповідає композиція значень параметрів $t_1 \circ t_2 = (t_1 + t_2) \cdot (1 + t_1 t_2 g_1(t_1, t_2))$, $g_1(t_1, t_2)$ — ряд від t_1, t_2 з коефіцієнтами з Q_K.

Через $N: S_L \to S_K$ будемо позначати нормений гомоморфізм з S_L в S_K, а коли T_s значення параметра t, відповідаюче початковій точці

*Науковий керівник — член-кореспондент АН СРСР І. Р. Шафаревич.

з S_L, то $N(T_s)$ значення параметра t, відповідаюче образу цієї точки при гомоморфізмі N. $N\text{orm}: L \to K$ — норма розширення L/K.

Лема 3. Нехай T_s — елемент Q_L, норма якого $\geqslant s$; тоді

$$N(T_s) \equiv Tr(T_s) + \varepsilon N\text{orm}\,(T_s) + \\ + \sum_{m=2}^{\infty} \alpha_m [N\text{orm}\,(T_s)]^m \,(\text{mod}\, Tr(P^{2s})). \tag{3}$$

Тут ε — одиниця в K, α_m — елементи з Q_K.

Доведення. Нехай σ — твірна g (ми допустили, що $[g:1]=p$). Коли $\lambda = n_0 + n_1\sigma + \ldots + n_{p-1}\sigma^{p-1}$ елемент групової алгебри $Z[g]$, то $T_s^{\lambda} = T_s^{n_0} \cdot (\sigma T_s)^{n_1} \ldots (\sigma^{p-1} T_s)^{n_{p-1}}$.

$Z_+[g]$ — частина $Z[g]$, яка складається з тих λ, що всі n_l невід'ємні, але хоч одне з них додатне. Тоді, позначаючи $t_1 \circ t_2 = S(t_1, t_2)$, одержуємо

$$N(T_s) = S(T_s, \sigma(T_s), \ldots, \sigma^{p-1}(T_s)) = \sum_{\lambda \in Z_+[g]} r_\lambda T_s^{\lambda},$$

$r_\lambda \in Q_K$, r_λ підлягають деяким умовам симетричності. Коли $\sigma^i \lambda = \lambda$, то $\lambda = n(1 + \sigma + \ldots + \sigma^{p-1})$ (i = одному з чисел $0,1,\ldots,p-1$). Коли λ не має такого вигляду, то по симетричності S, в $N(T_s)$ входить разом з $r_\lambda T_s^{\lambda}$ також і $r_\lambda Tr(T_s^{\lambda})$; залишається врахувати формулу множення на p в A, і лема доведена.

Нехай

$$\psi(x) = \begin{cases} x, & \text{коли } x \leqslant l \\ l + p(x-l), & \text{коли } x \geqslant l. \end{cases}$$

В S_L виникає фільтрація: S_L^n — підгрупа тих точок S_L, значення параметра t в яких належить до P^n.

Лема 4. Для всіх цілих $n \geqslant 1$ має місце

(а) $N(S_L^{\psi(n)}) = S_K^n$, $N(S_L^{\psi(n)+1}) = S_K^{n+1}$,

(в) коли $N_n: \dfrac{S_L^{\psi(n)}}{S_L^{\psi(n)+1}} \to \dfrac{S_K^n}{S_K^{n+1}}$

гомоморфізм, одержаний з N факторизацією, то при всіх $n \neq l$, N_n ізоморфізми. При $n = l$ має місце точна послідовність

$$0 \to g \to \frac{S_L^l}{S_L^{l+1}} \xrightarrow{N_l} \frac{S_K^l}{S_K^{l+1}} \to 0.$$

Доведення. Досить довести (в) і

(а^1) $N(S_L^{\psi(n)}) \subset S_K^n$; $N(S_L^{\psi(n)+1}) \subset S_K^{n+1}$;

з них (а) випливає по властивостях груп з фільтрацією (6).

Метод доведення далі класичний.

Наслідок 1. $H^0(g, S_L) = 0$, $H^{-1}(g, S_L) = \dfrac{Z}{pZ}$.

Доведення. Слід врахувати формулу

$$\sigma(aT^r) \circ (-aT^r) = a[\sigma(T) - T][rT^{r-1} + T^r(\ldots)][1 + T(\ldots)].$$

Лема 5. Для всіх цілих $n \geqslant 1$ і довільної p — групи g

(а) $N(S_L^{\psi(n)}) = S_K^n$, $N(S_L^{\psi(n)+1}) = S_K^{n+1}$.

(в) Нехай $N_n: \frac{S_L^{\psi(n)}}{S_L^{\psi(n)+1}} \to \frac{S_K^n}{S_K^{n+1}}$

гомоморфізм, одержаний з N факторизацією. Тоді має місце точна послідовність

$$0 \to \frac{g_{\psi(n)}}{g_{\psi(n)+1}} \to \frac{S_L^{\psi(n)}}{S_L^{\psi(n)+1}} \xrightarrow{N_n} \frac{S_K^n}{S_K^{n+1}} \to 0$$

(ψ — відповідаюча розширенню $\frac{L}{K}$ функція (4)). Доведення класичне.

Лема 6. Коли g — абелева група, то ($[g:1] = p^n$)

$$H^1(g, S_L) = \frac{Z}{p^n Z}.$$

Доведення — по аналогії з відомою $H^1(g, U_L) = \frac{Z}{p^n Z}$, ($U_L$ — група одиниць L).

Нехай $K(p)$ — максимальне сепарабельне p-розширення K з групою Галуа $GK(p)$. $S_K(p)$ — індуктивна границя груп S_L, де L — конечне p-розширення Галуа поля K. Позначимо $H^1(GK(p), S_K(p))$ через $H^1(*, S_K(p))$ (коцепи неперервні). Нехай $Z_{p^\infty} = \varinjlim \frac{Z}{p^n Z}$.

Лема 7. (Артін (7)). Коли для кожного конечного p-розширення Галуа F поля K існує підгрупа $\overline{H}^1(*, S_F(p))$ групи $H^1(*, S_F(p))$, ізоморфна Z_{p^∞} (ізоморфізм позначається через $\overline{\text{inv}_F}$) така, що

а) для кожного конечного нормального сепарабельного p-розширення $\frac{F}{K}$ буде

$$\text{res}_{\frac{F}{K}} \overline{H}^1(*, S_K(p)) \subset \overline{H}^1(*, S_F(p))$$

і

$$\overline{\text{inv}_F} \text{res}_{F,K} \alpha = [F:K] \overline{\text{inv}_K} \alpha$$

для всіх $\alpha \in \overline{H}^1(*, S_K(p))$.

Тоді

$$H^1\left(g_{\frac{F}{K}}, S_F\right) = \frac{Z}{p^n Z}, \quad H^1(*, S_K(p)) = Z_{p^\infty}.$$

Щоб застосувати цю лему в нашому випадку, треба взяти M — максимальне абелеве p-розширення K: нехай його група Галуа буде $AB_K(p)$. Тоді $H^1(AB_K(p), S_M) = Z_{p^\infty}$ і по спектральній послідовності Серра—Хохшільда є підгрупою $H^1(*, S_K(p))$.

Лема 8. (Тейт (7)). Нехай $f: A \times B \to C$ гомоморфізм g-модулів, а $\alpha \in H^p(g, B)$ такий, що для деякого q буде

$H^{q-1}(g, A) \times \alpha \to H^{p+q-1}(g, C)$ епіморфізм

$H^q(g, A) \times \alpha \to H^{p+q}(g, C)$ ізоморфізм

$H^{q+1}(g, A) \times \alpha \to H^{p+q+1}(g, C)$ мономорфізм.

Тоді

$$H^r(g, A) = H^{p+r}(g, C) \quad (r \in Z).$$

Щоб застосувати цю лему в нашому випадку, візьмемо $A = Z$, $B = S_L$, $C = S_L$, $p = 1$, $q = 1$. Тоді з існування фундаментального класу в $H^1(g, S_L)$ випливає

Теорема. Коли g — p-група, то

$$H^q(g, S_L) = H^{q-1}(g, Z) \text{ (для всіх } q \in Z).$$

За допомогою цієї теореми легко обчислити $H^1(G, A)$, і довести, що $H^1(G, A) = \pi_1(A_K)^*$ в нашому випадку (G — група Галуа максимального розширення Галуа поля K).

ЛІТЕРАТУРА

1. G. Shimura. Reduction of algebraic varieties with respect to a discrete valuation of the basic field. Amer. J. of Math. 77, № 1, 1955.
2. H. Hasse. Existenz separabeler zyklischer unverzweigter Erweilerungskörper vom Primzahlgrade p.., J. Reine angew. Math. 172, 1934.
3. А. Картан, С. Эйленберг. Гомологическая алгебра. М., 1960.
4. J. P. Serre. Sur les corps locaux... Bull Soc. Math. France, 1961.
5. P. Samuel and O. Zarisky. Commutative algebra, vol. I. New Jork, 1959.
6. N. Bourbani. Algébre, Paris, 1949.
7. E. Artin, J. Tate. Class field theory. Princeton, 1959.

О. Н. ВВЕДЕНСКИЙ

КОГОМОЛОГИИ ПОДГРУППЫ ЛЮТЦ ЭЛЛИПТИЧЕСКОЙ КРИВОЙ

Резюме

Вычисляются когомологии подгруппы Лютц и на основе этого доказывается двойственность в одномерном случае — гипотеза Шафаревича.