УДК 513.015.7

Замечания об n-мерных коммутативных формальных группах над кольцом целых поля $\mathfrak{p}$-адических чисел

Н. М. Глазунов

В заметке изучаются гомоморфизмы и изогении n-мерных коммутативных формальных групповых законов [1, стр. 193] над кольцом целых поля $\mathfrak{p}$-адических чисел — конечным расширением поля p-адических чисел Q_p.

Пусть F и G — соответственно n- и m- мерные коммутативные групповые законы над коммутативным кольцом R, f — гомоморфизм из F в G.

Определим гомоморфизм Любина c: $f \to M_{nm}(R)$. Он сопоставляет набору степенных рядов, задающих f, элемент $c(f)$ алгебры $M_{nm}(R)$ матриц размера $n \times m$ над кольцом R, образованный коэффициентами в линейной части гомоморфизма f. Если $n = m$ и f — изоморфизм, то ясно, что $\det(c(f))$ — единица кольца R. Изоморфизм f называется сильным (см. Хонда [2], где рассмотрен одномерный случай), если $c(f) = E$, E — единичная матрица.

Предложение 1. *Если кольцо R есть Q-алгебра, то n-мерный коммутативный групповой закон сильно изоморфен аддитивному.*

(Это предложение доказано в работе [3, гл. II] с применением теории Ли, а также может быть получено использованием методов Лазара [4] и Хонды [2].)

П р е д л о ж е н и е 2. *Если R — кольцо целых поля $\mathfrak{p}$-адических чисел, то отображение c: $\operatorname{Hom}_R(F, G) \to M_{nm}(R)$ есть инъективный гомоморфизм групп.*

(Для одномерных групповых законов это доказал Любин [5, лемма 2.1.1].)

Доказательство. Ввиду предложения 1 $F(X, Y) = \varphi^{-1}\circ(\varphi(X) + \varphi(Y))$, $G(X,Y) = \psi^{-1}\circ(\psi(X)+\psi(Y))$, $f(T) \in \operatorname{Hom}_R(F,G)$. Тогда $\psi\circ f\circ\varphi^{-1}\circ(\varphi(X) + \varphi(Y)) = \psi\circ f(X) + \psi\circ f(Y)$. Введя замену переменных $X \to \varphi^{-1}(X)$, получим

$$\psi\circ f\circ\varphi^{-1}(X+Y) = \psi\circ f\circ\varphi^{-1}(X) + \psi\circ f\circ\varphi^{-1}(Y).$$

Теперь нетрудно проверить, что в наборе степенных рядов $g(T) = \psi\circ f\circ\varphi^{-1}(T)$ все коэффициенты при степенях, больших или равных 2, нулевые, и, значит, $g(T) = (a_{ij})T$, где $(a_{ij}) \in M_{nm}(R)$. Покажем инъективность. Допустим $c(f) = 0$. Тогда $\psi\circ f\circ\varphi^{-1}(T) = 0$, и умножая слева и справа на ψ и φ^{-1}, получим $f = 0$, что и требовалось.

Далее через $\mathfrak{o}$ обозначаем кольцо целых поля $\mathfrak{p}$-адических чисел, через $\mathfrak{p} = \pi\mathfrak{o}$ — максимальный идеал кольца $\mathfrak{o}$, через $k = \mathfrak{o}/\mathfrak{p}$ — поля вычетов кольца $\mathfrak{o}$. Через $f^*(T)$ будем обозначать набор рядов, коэффициенты которого локализованы по $\operatorname{mod}\mathfrak{p}$.

Для всякого целого рационального m известный гомоморфизм умножения на m определяется формулами: $[0]_F(T) = 0$, $[m]_F(T), = F([m-1]_F(T), T)$, $[-1]_F(T)$— набор рядов, для которого $F([-1]_F(T), T) = 0$.

Пусть $f \in \operatorname{Hom}_k(F, G)$ и p — характеристика поля k. Напомним, что ввиду [3, гл. I, § 3, теорема 2] имеет место разложение $f(T) = g(T^{p^h})$, которое будем обозначать через $g(T)\circ\pi^h$, где $c(g) \neq 0$ в k и число $\operatorname{ht}(f) = h$ является наибольшим целым таким, что g есть набор степенных рядов от T^{p^h}. Это число $\operatorname{ht}(f)$ называется высотой f. Если $f = 0$, то положим $\operatorname{ht}(f) = \infty$. Число $\operatorname{ht}([p]^*_F(T))$ называется высотой группового закона F. В отличие от одномерного случая для $n(n \geqslant 2)$-мерных групповых законов уже не верно утверждение о том, что $\operatorname{Hom}_k(F, G) = 0$, если высоты F и G разные. Например, если $F(X, Y) = \begin{cases} X_1 + Y_1, \\ X_2 + Y_2 + X_2Y_2 \end{cases}$ и $G(X, Y) = X_1 + Y_1$, то $\operatorname{ht}(F) = 1$, $\operatorname{ht}(G) = \infty$, но $f(T) = (T_1, 0)$ — гомоморфизм из F в G.

Изогении. Однако такое утверждение будет верно для изогений, т. е. для таких гомоморфизмов f групповых законов F и G с одним и тем же кольцом функций $A = R[[T_1, \ldots, T_n]]$, для которых определяемый по f гомоморфизм колец $\vartheta_f : A \to A$, $T_i\vartheta_f = f_i(T_1, \ldots, T_n)$ превращает A в свободный модуль конечного ранга над $\operatorname{Im}\vartheta_f$.

Далее через $\operatorname{Iso}_R(F, G)$ обозначаем множество изогений группового закона F в G.

Лема 1.1. *Пусть R—кольцо, поле отношений которого имеет характеристику 0, F, G — групповые законы над R, f — гомоморфизм из F в G над R. Гомоморфизм f будет изогенией тогда и только тогда, когда $\det\left(\frac{\partial f_i(0)}{\partial T_j}\right) \neq 0$. И в этом случае f будет сепарабельной изогенией.*

2. *Если $k = \mathfrak{o}/\mathfrak{p}$ и $f(T) = g(T)\circ\pi^h$, то гомоморфизм f будет изогенией тогда и только тогда, когда $\det(c(g)) \neq 0$ в k.*

Доказательство. Утверждения леммы являются простым следствием фактов об алгебраической независимости элементов над полями (см. [6, гл. X, § 7]).

П р е д л о ж е н и е 3. 1. *Если групповые законы над кольцом $\mathfrak{o}$ изоморфны, то их высоты совпадают.*

2. *Если же высоты групповых законов F и G над k разные, то множество* $\mathrm{Iso}_k(F, G)$ *пусто.*

Доказательство. 1. Пусть F и G — изоморфные групповые законы и f — изоморфизм. Тогда, применяя к левой и правой частям тождества

$$f(F(X, Y)) = G(f(X), f(Y))$$

эндоморфизм умножения на p и локализуя затем по $\mathrm{mod}\, \mathfrak{p}$, получаем

$$f^* \circ [p]_F^*(T) = [p]_G^* \circ f^*(T). \tag{1}$$

Если F и G — оба бесконечной высоты, то первое утверждение доказано. Так как $c(f)$ — невырожденная матрица, то случай, когда высота одного группового закона конечна, а другого бесконечна, невозможен. Пусть теперь $\mathrm{ht}(F) = h_1 < \infty$, $\mathrm{ht}(G) = h_2 < \infty$. Введем в рассмотрение матрицы $A = c([p]_F^*)$, $B = c([p]_G^*)$, $C = c(f^*)$. Они все квадратные и ненулевые, так как f — изоморфизм, а C — невырожденная. Тогда

$$[p]_F^*(T) \equiv AT^{p^{h_1}} [\mathrm{mod}\deg p^{h_1} + 1], \tag{2}$$

$$[p]_G^*(T) \equiv BT^{p^{h_2}} [\mathrm{mod}\deg p^{h_2} + 1], \tag{3}$$

$$f^* \equiv CT\, [\mathrm{mod}\deg 2], \tag{4}$$

где $T^h = \begin{pmatrix} T_1^h \\ \vdots \\ T_n^h \end{pmatrix}$, $C^{p^h} = (c_{ij}^{p^h})$. Подставляя (2) — (4) в тождество (1) и рассматривая его по $\mathrm{mod}\deg q$, где $q = p^{\min(h_1, h_2)} + 1$, видим, что тождества

$$CAT^{p^{h_1}} \equiv 0\, [\mathrm{mod}\deg q] \quad \text{и} \quad BC^{p^{h_2}}T^{p^{h_2}} [\mathrm{mod}\deg q]$$

невозможны. Следовательно, остается только возможность

$$CAT^{p^{h_1}} \equiv BC^{p^{h_2}}T^{p^{h_2}} [\mathrm{mod}\deg q],$$

а это и показывает, что $h_1 = h_2$.

2. Предположим теперь, что существует изогения $f(T) = g(T) \circ \pi^h$ из F в G над $k = \mathfrak{o}/\mathfrak{p}$ и $h_2 < h_1$. Тогда после применения к (1), рассматриваемому над полем k, эндоморфизма умножения на p, будем иметь

$$g(T) \circ \pi^h \circ [p]_F(T) = [p]_G \circ g(T) \circ \pi^h. \tag{5}$$

Пусть $c(g) = A$, $[p]_F(T) \equiv BT^{h_1} [\mathrm{mod}\deg h_1 + 1]$, $[p]_G(T) \equiv CT^{h_2} [\mathrm{mod}\deg h_2 + 1]$. Рассматривая тождество (5) по $\mathrm{mod}\deg [\min(h + h_1, h + h_2) + 1]$, при $h_2 < h_1$ получим

$$ACT^{h_2 + h} \equiv 0\, [\mathrm{mod}\deg (h + h_2 + 1)],$$

и так как $\det(A) \neq 0$ по лемме 1, то $C = 0$. Но $h_2 < h_1 \leqslant \infty$ и $h_1 \neq h_2$. Тем самым невозможно, чтобы f было изогенией.

Предложение 4. *Отображение*:* $\mathrm{Iso}_0(F, G) \to \mathrm{Iso}_k(F^*, G^*)$ *есть инъекция, если* $[p]_F^*(T)$ — *изогения.*

Доказательство (Любин [5, лемма 2.3.1] разобрал одномерный случай). Допустим $f \in \mathrm{Iso}_0(F, G)$. Если хотя бы один коэффициент в наборе рядов f есть единица кольца $\mathfrak{o}$, то $f^* \neq 0$. Предположим, что ни один коэффициент набора f не является единицей. Тогда $f(T) = \pi^r g(T)$, $r > 0$, и $g^*(T) \neq 0$. Так как f — изогения, то

$$\pi^r g(F(X, Y)) = G(\pi^r g(X), \pi^r g(Y)) = \pi^r g(X) + \pi^r g(Y) + \pi^{2r}$$

— набор степенных рядов от X и Y. Деля на π' и редуцируя по $\mathrm{mod}\,\mathfrak{p}$, получаем, что $g^*(F^*(X, Y)) = g^*(X) + g^*(Y)$. Но высота F — конечная, а мы получили, что F изогенен аддитивной группе, высота которой бесконечна. Это невозможно по предложению 3, п. 2, следовательно, $f^* \neq 0$.

Автор благодарит О. М. Введенского за внимание и советы.

ЛИТЕРАТУРА

1. Ж. П. Серр, Алгебры Ли и группы Ли, «Мир», М., 1969.
2. Т. Хонда, Формальные группы и дзета-функции, Математика (сб. переводов,) т. 13, № 6, 1969.
3. A. Fröchlich, Formal Groups, Lecture notes in Mathematics, **74**, Springer verlag, 1968.
4. M. Lazard, Sur les groupes de Lie formels á un paramétre, Bull. Soc. Math. France, **83**, 1955, 251—274.
5. J. Lubin, One-parameter formal Lie groups over $\mathfrak{p}$-adic integer rings, Ann. of Math., **vol**. 80, 1964, 464—484.
6. С. Ленг, Алгебра, «Мир», М., 1968.

Поступила 11.VIII 1972 г.
Институт кибернетики АН УССР