Доклады Академии наук СССР
1974. Том 216, № 5

УДК 513.6

МАТЕМАТИКА

Академик АН БССР В. П. ПЛАТОНОВ

ГИПОТЕЗА ДЬЕДОННЕ И НЕСЮРЪЕКТИВНОСТЬ НАКРЫТИЙ АЛГЕБРАИЧЕСКИХ ГРУПП НА k-ТОЧКАХ

Пусть D/k — некоммутативное тело конечной размерности m^2 над центром k ($\mathrm{char}\, k\neq 2$) с нетривиальной инволюцией τ. S_τ — подпространство элементов D, симметричных относительно τ. Σ — подгруппа мультипликативной группы D^*, порожденная ненулевыми симметричными элементами. Легко видеть, что Σ — нормальный делитель D^* и изучение строения фактор-группы D^*/Σ представляет интерес с разных точек зрения (см. ([1-4])).

Предположим, что $k\subseteq S_\tau$, т. е. инволюция первого рода. Тогда $\dim S_\tau = m(m+1)/2 \vee m(m-1)/2$. Это соответствует случаю симплектических или ортогональных «форм». Если $\dim S_\tau = m(m+1)/2$, то $D^*=\Sigma$, ибо если $x\in D^*$, то из размерностных соображений $xS_\tau \cap S_\tau \neq (0)$ ([1]).

В связи с этим Дьедонне в 1952 г. в ([1]) высказал гипотезу, что и для более существенного случая — $\dim S_\tau = m(m-1)/2$ — группа $D^*=\Sigma$, если только $m>2$ (для $m=2$ очевидно, что $\Sigma=k^*$ и $D^*\neq\Sigma$). При этом Дьедонне отмечает (([1]), стр. 379), что считает эту гипотезу весьма вероятной. Ниже будет показано, что эта гипотеза имеет почти абсолютное опровержение. А именно, по крайней мере для любого конечно-порожденного поля k $D^*\neq\Sigma$ (очевидно, что D всегда определено над конечно-порожденным полем). Метод доказательства, на наш взгляд, довольно неожиданный, имеет существенно более общую природу. Сначала обнаруживается, что гипотеза Дьедонне является очень частным случаем общей задачи о сюръективности изогений k-определенных алгебраических групп на подгруппах k-точек, а затем применяется, по-видимому, впервые, техника локально-компактных локализаций для произвольных конечно-порожденных полей.

Прежде всего заметим, что если Φ — n-мерная ($n>2$) невырожденная эрмитова форма над D положительного индекса, $U(\Phi)$ — унитарная группа, соответствующая Φ, и $TU(\Phi)$ — подгруппа, порожденная трансвекциями, то по теореме Уолла ([3]) $U(\Phi)/TU(\Phi)\cong D^*/\Sigma D'$, где D' — коммутант D^*. Следовательно, гипотеза $D^*=\Sigma \Leftrightarrow U(\Phi)=TU(\Phi)$, т. е. эквивалентна тривиальности спинорной нормы ([2, 3]) для унитарной группы $U(\Phi)$. Хорошо известно, что группа $U(\Phi)$ является группой k-рациональных точек G_k некоторой k-формы G обычно ортогональной группы над универсальным полем ([5]). Пусть $\tilde{G}$ — односвязная накрывающая группы G, определенная над k, т. е. $\tilde{G}$ — спинорная k-группа; $\varphi:\tilde{G}\to G$ — соответствующая k-изогения.

Предложение 1. *Если* $\varphi(\tilde{G}_k)\neq G_k$, *то* $D^*\neq\Sigma$.

Таким образом, гипотеза Дьедонне входит весьма частным случаем в следующую общую задачу: пусть f: $G\to G'$ — k-изогения связных k-определенных алгебраических групп; когда $f(G_k)\neq G_k'$? Для некоторых специальных полей эта задача исследовалась в ряде работ (например, для конечного поля Ленгом ([6]), для поля вещественных чисел Борелем и Титсом ([7])).

В дальнейшем поле k предполагается бесконечным. Что касается конечного поля k, то в этом случае решение сформулированной задачи непосредственно вытекает из ([6]) в виде следующего утверждения.

П р е д л о ж е н и е 2. *Если k — конечное поле и $f\colon G\to G'$ — k-изогения, то $f(G_k)\neq G_k' \Leftrightarrow (\mathrm{Ker}\, f)_k\neq(1)$.*

Дадим теперь когомологическую интерпретацию. Точной последовательности $0\to\mathrm{Ker}\, f\to G\to G'\to 0$ обычным образом соответствует точная последовательность когомологий Галуа

$$0\to(\mathrm{Ker}\, f)_k\to G_k\xrightarrow{f} G_k'\to H^1(k,\ \mathrm{Ker}\, f)\xrightarrow{\psi} H^1(k,\ G)\to H^1(k,\ G').$$

Тогда $f(G_k)=G_k'\Leftrightarrow\psi$ инъективно; в частности, если $H^1(k,\ \mathrm{Ker}\, f)=0$, то $f(G_k)=G_k'$.

Будем предполагать, что изогения f мультипликативного типа, т. е. $\mathrm{Ker}\, f$ не содержит неединичных унипотентных элементов. Это условие всегда выполнено, если $\mathrm{char}\, k=0$ или G — редуктивная группа.

О с н о в н а я т е о р е м а. *Пусть k — конечно-порожденное поле, $f\colon G\to G'$ — нетривиальная k-изогения. Тогда $f(G_k)\neq G_k'$.*

З а м е ч а н и е. В общем случае условие конечно-порожденности k существенно, например, даже для вещественных или $\mathfrak{p}$-адических полей основная теорема не верна.

Пусть k_0 — простое подполе в k. Тогда k есть конечное расширение подполя рациональных функций $k_0(x_1,\ x_2,\dots,x_r)$. Следующее утверждение играет важную роль при доказательстве основной теоремы.

П р е д л о ж е н и е 3. *Пусть Δ — конечное сепарабельное расширение поля k. Тогда существует такое неархимедово локально-компактное нормирование v поля k, что пополнение $k_v\supset\Delta$.*

Д о к а з а т е л ь с т в о. Ограничимся основным случаем, когда $k=k_0(x_1,\ x_2,\dots,x_r)$. Для $\mathrm{char}\, k=0$ это равносильно рассмотрению общей ситуации, а при $\mathrm{char}\, k\neq 0$ нужно еще дополнительно рассмотреть случай, когда k есть чисто несепарабельное расширение поля $k_0(x_1,\ x_2,\dots,x_r)$.

Ввиду сепарабельности Δ/k существует примитивный элемент $a\in\Delta$, $k[a]=\Delta$. Если $[\Delta:k]=n$, то a является корнем неприводимого многочлена $f(y)=a_ny^n+a_{n-1}y^{n-1}+\dots+a_0\in k[y]$. При этом можно считать, что $a_n=1$, а все $a_i\in k_0[x_1,\ x_2,\dots,\ x_r]$.

Локально-компактные неархимедовы нормирования на $k_0(x_1,\dots,x_r)$, т. е. плотные вложения в локально-компактное поле, определяются следующим образом. Если $k_0=Q$, то Q вкладывается в поле $\mathfrak{p}$-адических чисел $Q_\mathfrak{p}$ обычным образом, а $x_i\to x_i^0$, где $x_1^0,\ x_2^0,\dots,x_r^0$ — произвольные Q-алгебраически независимые элементы $Q_\mathfrak{p}$ (степень трансцендентности $Q_\mathfrak{p}$ над Q бесконечна). Полученные нормирования далее продолжаются на любое конечное расширение поля $k_0(x_1,\ x_2,\dots,x_r)$. Если k — конечное поле, то построения аналогичны, только в качестве базисного рассматривается стандартное вложение $k_0(x_1)$ в поле формальных степенных рядов.

Так как дальнейшие рассуждения для $\mathrm{char}\, k=0$ и $\mathrm{char}\, k\neq 0$ совершенно аналогичны, то в целях большей выпуклости изложения ограничимся случаем $\mathrm{char}\, k=0$, т. е. $k_0=Q$.

Обозначим через $R(f,\ f')$ результант f и производной f'. Из сепарабельности f следует, что $R(f,\ f')\neq 0$, $R(f,\ f')\in k_0[x_1,\ x_2,\dots,\ x_r]$. Если заранее выбрать $f\in Z[x_1,\ x_2,\dots,\ x_r]$, то $R(f,\ f')\in Z[x_1,\ x_2,\dots,\ x_r]$. Существуют такие целые числа $z_1,\ z_2,\dots,\ z_r$, что $R(f,\ f')(z_1,\ z_2,\dots,\ z_r)\neq 0$. Тогда многочлен $f(y)_{(z_1,\ z_2,\dots,\ z_r)}=y^n+a_{n-1}(z_1,\dots,z_r)y^{n-1}+\dots+a_0$ будет сепарабельным многочленом с целыми коэффициентами. По теореме плотности Артина — Чеботарева существует такая бесконечная совокупность $\mathfrak{p}_i$-адических полей $Q_{\mathfrak{p}_i}$, $i=1,2,\dots,$ что $f(y)_{(z_1,\dots,z_r)}$ разлагается над кольцами целых $Z_{\mathfrak{p}_i}$ на линейные множители. Пусть $\bar f_i(y)_{(z_1,\dots,z_r)}$ — многочлен, полученный из $f(y)_{(z_1,\dots,z_r)}$ редуцированием его коэффициентов по модулю $\mathfrak{p}_i$. Тогда $\bar f_i(y)_{(z_1,\dots,z_r)}$ разлагается на линейные множители над конечным полем $Z/(p_i)$. Можно считать, что для всех $\mathfrak{p}_i$ результант $R(f,f')(z_1,\dots$ $\dots,z_r)$ является единицей кольца $Z_{\mathfrak{p}_i}$. Специализируем для каждого $\mathfrak{p}_i$ построенное ранее вложение $\tau_i\colon Q(x_1,\ x_2,\dots,x_r)\to Q_{\mathfrak{p}_i}$ следующим образом:

$\tau_i(x_j)\in Z_{\mathfrak{p}_i}$, где $\tau_i(x_j)\,(\mathrm{mod}\,(\mathfrak{p}_i))=z_j(\mathrm{mod}\,(\mathfrak{p}_i))$. Тогда многочлен $\tau_i(f)\,(y)=$ $=y^n+\tau_i(a_{n-1})\,y^{n-1}+\ldots+\tau_i(a_0)$ по модулю $(\mathfrak{p}_i)$ совпадает с $\bar{f}_i(y)_{(z_1,\ldots,z_r)}$. По одному из вариантов теоремы Хензеля (см. ([8]), стр. 312) $\tau_i(f)\,(y)$ разлагается на линейные множители над полем $Q_{\mathfrak{p}_i}$. Следовательно, $\Delta\to k_{v_i}=Q_{\mathfrak{p}_i}$ для всех $\mathfrak{p}_i$.

Предложение 3 доказано.

З а м е ч а н и е. Условие сепарабельности в предложении 3 существенно и не может быть опущено, как показывает пример уже простейшего чисто несепарабельного расширения.

Напомним, что алгебраическая k-группа G обладает свойством слабой аппроксимации относительно некоторого нормирования v поля k, если $\bar{G}_k=G_{kv}$, где $\bar{G}_k$ означает замыкание G_k в v-адической топологии. Следующее утверждение, в существенном принадлежащее Серру, впервые отмечено Хардером ([9]).

П р е д л о ж е н и е 4. *Пусть T — k-определенный алгебраический тор, разложимый над локально-компактным пополнением k_v. Тогда T обладает свойством слабой аппроксимации относительно v.*

Д о к а з а т е л ь с т в о о с н о в н о й т е о р е м ы. Пусть T' — k-определенный максимальный тор группы G'. Тогда $f^{-1}(T')=T$ — k-определенный максимальный тор в G, разложимый над конечным сепарабельным расширением Δ/k (см. ([10]), гл. 3). Достаточно доказать, что изогения f_T: $T\to T'$ несюръективна на k-точках. Согласно предложению 3 существует такое локально-компактное неархимедово нормирование v поля k, что $\Delta\subset k_v$, следовательно, торы T и T' разложимы над k_v. Из предложения 4 тогда вытекает, что $\bar{T}_k=T_{k_v}$, $\bar{T}_k'=T_{k_v}'$. Так как $f_T(k_v):T_{k_v}\to T_{k_v}'$ — открытое отображение, то $f_T(T_k)\neq T_k'\Leftarrow f_T(T_{k_v})\neq T_{k_v}'$.

Для доказательства последнего неравенства воспользуемся точной последовательностью

$$0\to(\mathrm{Ker}\,f)_{k_v}\to T_{k_v}\xrightarrow{f_T}T_{k_v}'\to H^1(k_v,\ \mathrm{Ker}\,f)\to H^1(k_v,\ T).$$

По теореме Гильберта 90 $H^1(k_v,\ T)=0$; значит, достаточно доказать, что $H^1(k_v,\ \mathrm{Ker}\,f)\neq0$. А это следует из рассмотрения той же последовательности, только f_T необходимо заменить на отображение φ_m: $x\to x^m$, где m — экспонента $\mathrm{Ker}\,f$; тогда card $(H^1(k_v,\mathrm{Ker}\,f))\geqslant[k_v^*:k_v^{*m}]$ (см. ([11])). Остается заметить, что для локально-компактного неархимедова поля k_v при $m>1$ всегда $[k_v^*:k_v^{*m}]>1$.

Основная теорема доказана.

Как уже отмечалось ранее, в качестве частного случая основная теорема содержит следующую теорему, опровергающую гипотезу Дьедонне для произвольных конечно-порожденных полей.

Т е о р е м а. *Если k — конечно-порожденное поле, то $D^*\neq\Sigma$.*

В действительности, следуя общему плану, развитому выше, можно дать непосредственное доказательство этой теоремы, не переходя к унитарным группам. Ниже приводится это доказательство, представляющее самостоятельный интерес и позволяющее получить о Σ новую информацию.

Пусть Δ — сепарабельное максимальное подполе в D. Тогда существует такое неархимедово локально-компактное нормирование v поля k, что $\Delta\subset k_v$ и $D\otimes_k k_v\cong L(m,\ k_v)$. Инволюция τ продолжается на $D\otimes_k k_v$ и из общих свойств инволюций (см. ([12]), гл. 10) следует, что $S_\tau\otimes_k k_v=S_\tau(k_v)=aS^-$, где $a\in S^-$, S^- обозначает подпространство в $L(m,\ k_v)$, состоящее из обычных кососимметрических матриц. Если $x\in S_\tau(k_v)$, то $x=as^-$, $\det x=\det a\det s^-=$ $=(Pf(a)Pf(s^{-1}))^2$, где Pf обозначает пфаффиан (см. ([13]), гл. 9). Тогда подгруппа $\Sigma(k_v)=\{S_\tau(k_v)^*\}$ обладает свойством: если $y\in\Sigma(k_v)$, то $\det y\in k_v^2$. Так как $k_v\neq k_v^2$, то $\Sigma(k_v)\neq GL(m,\ k_v)$. Используя свойства v-адической топологии можно показать, что $\Sigma(k_v)$ — замкнутая подгруппа в $GL(m,\ k_v)$. Здесь существенно, что $\Sigma(k_v)$ — нормальный делитель в $GL(m,\ k_v)$; значит, $SL(m,\ k_v)\subset\Sigma(k_v)$, и для всякого $\alpha\in k_v^2$ найдется $y_\alpha\in\Sigma(k_v)$ с $\det y_\alpha=\alpha$.

Если теперь $D^*=\Sigma$, то замыкание в v-адической топологии $\overline{D}^*=\overline{\Sigma}$. Тогда $\overline{D}^*=GL(m, k_v)=\Sigma(k_v)$, что невозможно. Противоречие. Следовательно, $D^*\neq\Sigma$. Теорема доказана.

Предыдущие рассуждения почти доказывают следующее утверждение.

Предложение 5. *Если $x\in S_\tau$, то $k(x)$ — немаксимальное подполе в D; в частности, если $\sigma\in\Sigma$, то редуцированная норма $N_{\mathrm{red}}(\sigma)=k^{*2}$.*

Замечание. Для поля $Q(x)$ рациональных функций одной переменной В. И. Янчевский явно построил (не опубликовано) тело D индекса четыре над $Q(x)$ с инволюцией первого рода, в котором $N_{\mathrm{red}}(D)\not\subset(Q(x))^2$. Это, по-видимому, было первым контрпримером к гипотезе Дьедонне.

Институт математики
Академии наук БССР
Минск

Поступило
4 XII 1973

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] *J. Dieudonne*, Trans. Am. Matt, Soc., v. 72, 367 (1952). [2] *J. Dieudonne*, La Geometrie des Groupes Classiques, 1971. [3] *G. Wall*, Publ. Math. I.H.E.S., № 1, 5 (1959). [4] *В. П. Платонов, В. И. Янчевский*, ДАН, т. 208, № 3, 541 (1973). [5] *А. Вейль*, Основы теории чисел, М., 1972. [6] *S. Lang*, Am. J. Math., v. 78, 555 (1956). [7] *A. Borel, J. Tits*, Publ. Math. I.H.E.S., № 41, 253 (1972). [8] *З. И. Боревич, И. Р. Шафаревич*, Теория чисел, М., 1972. [9] *G. Harder*, Arch. Math., v. 19, № 5, 465 (1968). [10] *А. Борель*, Линейные алгебраические группы, М., 1972. [11] *Ж.-П. Серр*, Когомологии Галуа, М., 1968. [12] *A. Albert*, Structure of Algebras, N. Y., 1939. [13] *Н. Бурбаки*, Алгебра: модули, кольца, формы, М., 1966.