К. Н. Пономарев, Алгебраические группы и экспоненциальное действие,
Изв. вузов. Матем., 1991, номер 7, 58–61

https://www.mathnet.ru/ivm5117

К. Н. Пономарев УДК 512.623.27, 512.743

АЛГЕБРАИЧЕСКИЕ ГРУППЫ И ЭКСПОНЕНЦИАЛЬНОЕ ДЕЙСТВИЕ

Пусть F — поле, G — группа автоморфизмов поля F. Естественное действие на мультипликативной группе поля F^* кольца целых чисел $\mathbf{Z}$ и группы G определяет на F^* действие группового кольца $\mathbf{Z}G$. Это действие будем называть экспоненциальным.

Цель данной статьи — исследование свойств экспоненциального действия в случае бесконечного поля F и конечной группы автоморфизмов G. В первой части работы установлена точность этого действия. Показана связь экспоненциального действия с алгебраическими группами, на которую было указано еще К. Шевалле [1]. Во второй части работы установлено частичное обобщение на случай экспоненциального действия одной леммы И. Капланского.

Во всей работе придерживаемся следующих соглашений: F — бесконечное поле, а G — конечная группа автоморфизмов. Как обычно, через F^G обозначается поле инвариантов группы G. Для экспоненциального действия выбрана экспоненциальная запись. Поле инвариантов группы G в поле F обозначается через K.

§ 1. Экспоненциальное действие

Если $f\in\mathbf{Z}G$ и $f=\sum\limits_{\sigma\in G}n_\sigma\sigma$, а $x\in F^*$, то экспоненциальное действие f на x определяется как

$$x^f=\prod_{\sigma\in G}(x^\sigma)^{n_\sigma}.$$

Экспоненциальное действие $\mathbf{Z}G$ на F определяет гомоморфизм кольца $\mathbf{Z}G$ в кольцо эндоморфизмов, который является в указанных выше предположениях на F и G вложением.

Лемма 1. *Действие $\mathbf{Z}G$ на F^* точно. Иными словами, если $f\in\mathbf{Z}G$ и $x^f=1$ для любого $x\in F^*$, то $f=0$.*

Доказательство. Пусть $G=\{g_1,\dots,g_n\}$, а $\nu:G\to[1,n]$ — соответствующая нумерация элементов G, т.е. $\nu(g_i)=i$, $i=1,2,\dots,n$, и $g_{\nu(\sigma)}=\sigma$, $\sigma\in G$.

Напомним лемму Дедекинда о независимости автоморфизмов (см. [2]): если h — такой многочлен кольца $F[x_1,\dots,x_n]$, что для любого $x\in F$ $h(x^{g_1},\dots,x^{g_n})=0$, то $h=0$.

Приступим к доказательству леммы. Пусть выполнены все условия леммы, а N и M — такие непересекающиеся подмножества в G, что $f=\sum\limits_{\sigma\in N}n_\sigma\sigma-\sum\limits_{\sigma\in M}n_\sigma\sigma$ и $n_\sigma>0$, $\sigma\in M\cup N$. Если $x\in F^*$, то по условию

$$0=x^f-1=\prod_{\sigma\in N}(x^\sigma)^{n_\sigma}/\prod_{\sigma\in M}(x^\sigma)^{n_\sigma}-1,$$

т.е. $\prod\limits_N x^{\sigma n_\sigma}-\prod\limits_M x^{\sigma n_\sigma}=0$. Рассмотрим многочлен $h(X_1,\dots,X_n)=\prod\limits_N X^{n_\sigma}_{\nu(\sigma)}-\prod\limits_M X^{n_\sigma}_{\nu(\sigma)}$. Как указано выше, для любого $x\in F^*$ $h(x^{g_1},\dots,x^{g_n})=0$, а поскольку многочлен h не имеет свободных членов, то $h(0,\dots,0)=0$. По лемме Дедекинда $h=0$ и, значит, $f=0$. Лемма доказана.

По поводу всех определений и фактов по алгебраическим группам отсылаем читателя к книге [3].

Пусть C — категория k-групп конечного мультипликативного типа, расщепимых над полем F. Взятие характеров определяет двойственность этой категории G-модулей конечного типа.

Как обычно, через $R_{F/K}$ обозначаем функтор ограничения поля, пусть $R=R_{F/K}\boldsymbol{G}_{m,F}$ Из свойств функтора $R_{F/K}$ (см. [3]) следует, что имеется такой F-морфизм $\varphi:R\to\boldsymbol{G}_{m,F}$ (который мы зафиксируем), что для любого F-морфизма $\psi:R\to\boldsymbol{G}_{m,F}$ существует K-морфизм $\alpha:R\to R$ такой, что $\psi=\alpha\varphi$. Рассмотрим множество $H=\mathrm{Hom}_{K-gr}(R,R)$. Указанное свойство отождествляет H с G-модулем характеров $\hat{R}=\boldsymbol{Z}G$. Любой элемент из H определяется его действием на K-точках $R(K)$, а группа K-точек $R(K)$ естественно отождествляется с $F^*=R(K)$. Действие H на K-точках совпадает с экспоненциальным действием $\boldsymbol{Z}G$ на F^* при указанных отождествлениях. Все это позволяет отождествить действие группы характеров $\hat{R}$ на K-точках с экспоненциальным действием $\boldsymbol{Z}G$ на F^*.

Пусть теперь D есть K-подгруппа в R, а $i:D\to R$ — соответствующее K-вложение. Тогда D — тоже группа категории C. Пусть $\hat{i}:\boldsymbol{Z}G\to\hat{D}$ — двойственный эпиморфизм и $I=\ker\hat{i}$ — правый идеал в кольце $\boldsymbol{Z}G$, $I\triangleleft_r\boldsymbol{Z}G$. Из указанного выше отождествления следует, что на K-точках

$$D(K)=\{a\in F^*\mid \text{для любого } i\in I\ a^i=1\}.$$

Если I — правый идеал $\boldsymbol{Z}G$, то обозначим $M(I)=\{a\in F^*\mid$ для любого $i\in I\ a^i=1\}$, и это множество назовем множеством единиц идеала I (в поле F для группы автоморфизмов G). Выше установлено следующее утверждение.

Лемма 2. *Множества единиц правых идеалов $\boldsymbol{Z}G$ есть K-точки алгебраических подгрупп $R_{F/K}\boldsymbol{G}_{m,F}$, и наоборот.*

Алгебраическую K-определенную группу называем вложимой (в $R_{F/K}\boldsymbol{G}_{m,F}$), если она вкладывается в R.

Если S — кольцо, то образы гомоморфизмов будем называть проекциями S.

Из двойственности следует, что группа является вложимой тогда и только тогда, когда ее группа характеров есть проекция $\boldsymbol{Z}G$.

Лемма 3. *Любая группа категории C изогенна прямому произведению вложимых групп.*

Доказательство. Любая группа в категории C есть произведение тора на конечную группу. В силу этого достаточно доказать лемму в случае торов. Известно, что торы T_1 и T_2 изогенны, если и только если $\hat{T}_1\otimes\boldsymbol{Q}\simeq\hat{T}_2\otimes\boldsymbol{Q}$. Кольцо $\boldsymbol{Q}G$ полупросто, значит, любой $\boldsymbol{Q}G$-модуль есть прямое произведение простых, т.е. проекций $\boldsymbol{Q}G$. Этим доказательство завершается.

Правый идеал $I\triangleleft_r\boldsymbol{Z}G$ назовем идеалом конечного индекса, если $I\cap\boldsymbol{Z}\neq 0$. Это равносильно тому, что в тензорном пополнении $I\otimes\boldsymbol{Q}=\boldsymbol{Q}G$.

Лемма 4. *Идеал $I\triangleleft_r\boldsymbol{Z}G$ является идеалом конечного индекса тогда и только тогда, когда $M(I)$ конечно.*

Доказательство. Пусть I — идеал конечного индекса в $\boldsymbol{Z}G$, $I\cap\boldsymbol{Z}\ni n\neq 0$. Тогда по определению $M(I)$ имеем $M(I)^n=1$, но $M(I)$ есть подгруппа F^* и, значит, $M(I)$ конечно.

Обратно, пусть $M(I)$ конечно, тогда для некоторого $m\in\boldsymbol{Z}$ $M(I)^m=1$. Предположим, что I не является идеалом конечного индекса в $\boldsymbol{Z}G$, $\overline{I}=I\otimes\boldsymbol{Q}\neq\boldsymbol{Q}G$. Кольцо $\boldsymbol{Q}G$ полупросто, и любой идеал порождается идемпотентом. Значит, для левого аннулятора A имеет место $A=\mathrm{Ann}_l\overline{I}=(\mathrm{Ann}_l I)\otimes\boldsymbol{Q}\neq 0$. Пусть $e\in A$, $e\neq 0$. Тогда $(F^*)^{eI}=(F^*)^0=1$, т.е. $(F^*)^e\subset M(I)$, и $(F^*)^{me}\subset M(I)^m=1$. Из леммы 1 следует, что $me=0$ и $e=0$ — противоречие, полученное из предположения $\overline{I}\neq\boldsymbol{Q}G$. Значит, $\overline{I}=\boldsymbol{Q}G$, и I — идеал конечного индекса. Этим доказательство леммы завершено.

В качестве немедленного следствия укажем, что если T есть K-определенный F-расщепимый тор, который является вложимым, то, поскольку поле F бесконечно, группа K-точек $T(K)$ бесконечна, и, значит, идеал, определяющий вложение T в $R_{F/K}\,\boldsymbol{G}_{m,F}$, не является идеалом конечного индекса.

§ 2. Определимость поля инвариантов при экспоненциальном действии

Известна следующая лемма И. Капланского (см. [4]).

Лемма 1. *Пусть $L \diagdown K$ — расширение полей и пусть для любого $x \in L$ существует такое натуральное n, что $x^n \in K$. Тогда либо $L = K$, либо поле L имеет простую характеристику, и расширение L/K чисто несепарабельно, или же L — алгебраическое расширение простого конечного поля.*

Для изучения абстрактных изоморфизмов алгебраических групп необходимо следующее утверждение, выводимое из леммы 1.

Лемма 2. *Пусть $L \diagdown K$ — расширение полей, а $p = \operatorname{ch} L$ — характеристика поля L. Пусть $f \in \mathbf{Z}/p\mathbf{Z}$ и для любого $x \in L$ $x^f \in K$, тогда $L = K$.*

Докажем следующую теорему.

Теорема. *Пусть F — бесконечное поле, G — конечная группа автоморфизмов F, $K = F^G$. Пусть S — такое подполе в F, что $S \cap K$ бесконечно, а $f \in \mathbf{Z}G \diagdown p\mathbf{Z}G$. Если для любого $x \in F^*$ $x^f \in S$, то $S \supseteq K$.*

Доказательству предпошлем лемму.

Лемма 3. *Пусть F — поле, S — подполе F, а X — переменная. Пусть f_1, f_2 — унитарные (т.е. со старшим коэффициентом единица) взаимно-простые многочлены из кольца $F[X]$. Пусть для бесконечного числа значений $x \in S$ $f_1(x)/f_2(x) \in S$, тогда коэффициенты многочленов принадлежат полю S.*

Доказательство леммы. Пусть W — векторное пространство над полем S, образованное в F коэффициентами многочленов f_1 и f_2, а $v_1, \ldots, v_n$ — его базис. Пусть $f_{11}, \ldots, f_{1n}, f_{21}, \ldots, f_{2n}$ — такие многочлены из кольца $S[X]$, что $f_1 = \sum_1^n v_i f_{1i}$, $f_2 = \sum_1^n v_i f_{2i}$, тогда $f_1(X)/f_2(X) = \sum v_i f_{1i}(X)/\sum v_i f_{2i}(X)$. По условию леммы для бесконечного числа значений $x \in S$ $f_1(x)/f_2(x) \in S$, т.е. для бесконечного числа значений $x \in S$ $f_{11}(x)/f_{21}(x) = \ldots = f_{1n}(x)/f_{2n}(x)$.

Таким образом, $f_{11}(X)/f_{21}(X) = \ldots = f_{1n}(X)/f_{2n}(X) = f_1(X)/f_2(X)$. В силу того, что $F[X]$ — область с однозначным разложением на множители, f_1, $f_2 \in S[X]$. Доказательство леммы окончено.

Прежде чем приступить к доказательству теоремы, сделаем несколько замечаний. Напомним (см. [2]), что если F — поле, G — конечная группа его автоморфизмов, а $K = F^G$ — поле инвариантов G, то нормальным базисом поля F над K называют такой базис F над K, действие группы G на элементах которого переставляет его элементы. Элемент $a \in F$ называем базисным (для группы автоморфизмов G поля F), если множество $\{a^g \mid g \in G\}$ есть нормальный базис F над K. Заметим, что если a — базисный элемент, а $b \in K$, то ab — тоже базисный элемент.

Приступим к доказательству теоремы. Пусть выполнены все условия теоремы. Пусть M и N — такие непересекающиеся подмножества в G, что $f = g_1 - g_2$, причем $g_1 = \sum_{\sigma \in M} n_\sigma \sigma$, $g_2 = \sum_{\sigma \in N} n_\sigma \sigma$, $n_\sigma > 0$. По условию $f \notin p\mathbf{Z}G$, заменяя, если необходимо, f на $-f$, можно считать, что $g_1 \notin p\mathbf{Z}G$. Для любого $x \in F^*$

$$x^f = x^{g_1}/x^{g_2} = \prod_{\sigma \in M} x^{\sigma n_\sigma} / \prod_{\sigma \in N} x^{\sigma n_\sigma}.$$

Если a — базисный элемент для группы автоморфизмов G поля F, то рассмотрим унитарные взаимно-простые многочлены

$$f_{1,a}(X) = \prod_{\sigma \in M} (X + a^\sigma)^{n_\sigma}, \quad f_{2,a}(X) = \prod_{\sigma \in N} (X + a^\sigma)^{n_\sigma}.$$

Обратим внимание, что т. к. $g_1 \notin pZG$, то

$$f_{1,a}(X) = a^{g_1} + \ldots + (\sum_{\substack{\sigma \in M \\ p \nmid n_\sigma}} n_\sigma a^\sigma) X^{l-1} + X^l, \quad l = \sum_{\sigma \in M} n_\sigma .$$

Если $x \in K$, то по условию

$$(a+x)^f = \frac{(a+x)^{g_1}}{(a+x)^{g_2}} = \frac{f_{1,a}(x)}{f_{2,a}(x)} \in S.$$

В частности, для бесконечного числа элементов из $S \cap K$

$$x \in S \cap K, \quad (a+x)^f = f_{1,a}(x)/f_{2,a}(x) \in S.$$

Отсюда по лемме 3 $f_{1,a} \in S[X]$. Значит, если a — базисный элемент, то $\sum_{p \nmid n_\sigma} n_\sigma a^\sigma \in S$. А если x — произвольный элемент из K, то и ax — базисный элемент, и $\sum_{p \nmid n_\sigma} n_\sigma (ax)^\sigma = x \sum_{p \nmid n_\sigma} n_\sigma a^\sigma \in S$. Отсюда следует, что $x \in S$, поскольку из базисности a вытекает $\sum_{p \nmid n_\sigma} n_\sigma a^\sigma \neq 0$. Доказательство теоремы окончено.

Автор благодарен В. Е. Воскресенскому за полезные указания, а А. И. Валицкасу — за помощь в выполнении работы.

ЛИТЕРАТУРА

1. Шевалле К. Теория групп Ли. Т. 2. Алгебраические группы: Пер. с франц.— М.: Ин. лит., 1958.— 375 с.
2. Ленг С. Алгебра: Пер. с англ.— М.: Мир, 1968.— 564 с.
3. Воскресенский В. Е. Алгебраические торы.— М.: Наука, 1977.— 224 с.
4. Kaplansky I. A theorem on division rings // Canad. J. Math.— 1951.— V. 3.— № 3.— P. 290—292.

г. Новосибирск

Поступила
06.06.1990

Г. О. Эльстинг

УДК 512.554.31

ОБ АНАЛОГАХ КЛАССИЧЕСКИХ АЛГЕБР ЛИ НАД ПОЛЕМ ХАРАКТЕРИСТИКИ 3

Основное поле k предполагается алгебраически замкнутым полем характеристики p. Непосредственно проверяется, что при $p > 3$ простые классические k-алгебры Ли, отличные от A, обладают неприводимой транзитивной градуировкой вида

$$L = L_{-2} + L_{-1} + L_0 + L_1 + L_2, \qquad (1)$$

в которой: а) $\dim L_{-2} = \dim L_2 = 1$; б) L_0 — прямая сумма одномерного центра $z(L_0)$ и подалгебры L_0'; в) $[L_{\pm 2}, L_0'] = \langle 0 \rangle$. Более того, исходя из результатов [1] и [2], нетрудно показать, что при $p > 3$ любая простая алгебра Ли с градуировкой вида (1) является классической. В противоположность этому для $p = 3$, $\dim L_{-1} = 2$ в работе [3] построено бесконечное семейство простых неклассических алгебр Ли $L(\varepsilon)$, обладающих градуировкой вида (1). Предположим, что $p = 3$ (как и всегда в дальнейшем) и введем следующие обозначения: $K_{2n+1}(E) = L_{-2} + L_{-1} + \ldots$ — контактная алгебра Ли, наделенная стандартной градуировкой (см. [4]), V — подгруппа в $\mathrm{Aut}_k(K_{2n+1}(E))$, индуцированная k-линейными преобразованиями подпространства $E' = kx_1 + \ldots + kx_{2n}$ пространства E; $(O_{2n}(E'))_i$ — пространство однородных многочленов степени i в алгебре разделенных степеней $O_{2n}(E')$; $\pi i = i \pm n$, $i = 1, \ldots, 2n$; $\varepsilon_1 = \ldots = \varepsilon_n = 1 = -\varepsilon_{n+1} = \ldots = -\varepsilon_{2n}$; $\{u, w\} = \varepsilon_1 (\partial_1 u)(\partial_{\pi 1} w) + \ldots + \varepsilon_{2n} (\partial_{2n} u)(\partial_{\pi(2n)} w)$;