Записки научных
семинаров ПОМИ
Том 321, 2005 г.

Н. Н. Кушпель

О КОНЕЧНЫХ ОДНОИНВАРИАНТНЫХ ЛИНЕЙНЫХ ГРУППАХ

1. Введение

Пусть V – конечномерное пространство над полем K и пусть $G \leq \mathrm{GL}(V)$ – линейная группа. Обозначим $V^g = \{v \in V \mid g(v) = v\}$ и, соответственно, $V^G = \{v \in V \mid g(v) = v \text{ для всех } g \in G\}$. Будем говорить, что G *одноинвариантная*, если

$$V^g = V^G,$$

для любых $g \in G$, $g \neq 1$.

Если G – конечная группа и $V^G = 0$, имеем случай действия группы без неподвижных точек на $V \setminus 0$. Такие группы классифицированы для $K = \mathbb{C}, \mathbb{R}$ (см., например, [6]). Заметим, что если поле K имеет конечную характеристику и при этом G действует без неподвижных точек на $V \setminus 0$, то характеристика поля K не делит порядок группы G. Одноинвариантные линейные группы являются естественным обобщением линейных групп, действующих без неподвижных точек (другое обобщение линейных групп, действующих без неподвижных точек, рассматривалось в работах [2–4]).

В работе [7] рассмотрены общие свойства одноинвариантных групп. В частности, доказано, что конечная одноинвариантная группа G, порядок которой кратен $p = \operatorname{char} K$, является полупрямым произведением $U \cdot D$, где U – нормальная силовская p-подгруппа G, U – абелева, а D действует на $U \setminus \{1\}$ (сопряжением) без неподвижных точек.

В этой статье будет дана классификация конечных одноинвариантных линейных групп над алгебраически замкнутым полем характеристики p в следующих двух случаях. В первом случае мы предполагаем, что порядок группы G равен pq, $(p, q) = 1$

Работа финансировалась грантом E02-1.0-15 Министерства Образования Российской Федерации.

(результат для этого случая без доказательства сформулирован в [7]). Второй случай, когда порядок группы G равен p^2, то есть G – абелева унипотентная группа. При этом будет дана классификация таких групп, удовлетворяющих определенному условию. А именно, пусть V – G-модуль. Предположим, что $V_0 \leq V_1 \leq \cdots \leq V_m = V$, где

$$V_0 = V^G, V_1 = \{v \in V \mid g(v) \equiv v (\operatorname{mod} V_0) \quad \text{для любого} \quad g \in G\}, \dots,$$

$$\dots V_{i+1} = \{v \in V \mid g(v) \equiv v (\operatorname{mod} V_i) \quad \text{для любого} \quad g \in G\}, \dots.$$

Далее обозначим $m = \mathfrak{l}_{I_G}(V)$ и назовем число m I_G-длиной группы G. В работе классифицированы группы I_G-длины 1. Однако, уже в этом случае неизоморфных неразложимых одноинвариантных групп, при некоторых условиях, бесконечно много.

2. Случай I

Пусть размерность пространства V равна n, характеристика поля K равна p и K алгебраически замкнуто.

Пусть $G \leq \mathrm{GL}(V)$ – конечная одноинвариантная группа, порядок которой кратен p. Тогда $G = U \cdot D$, где U – нормальная силовская p-подгруппа группы G, а D – циклическая подгруппа порядка q ([7]). При этом, действие группы D на U сопряжением не имеет неподвижных точек. Пусть теперь $G = U \cdot D$ – абстрактная конечная группа, являющаяся полупрямым произведением своей нормальной силовской p-подгруппы $U = \langle u \rangle$ и циклической подгруппы $D = \langle \delta \rangle$ порядка q. Предположим, также, что порядок группы U равен p (отсюда следует $q \mid p-1$). Тогда $\delta u \delta^{-1} = u^k$ для некоторого $k \in \mathbb{N}$. Мы будем также отождествлять k с элементом простого поля $\mathbb{F}_p \subset K$. Заметим, что $k \in \mathbb{F}_p^*$ – это первообразный корень степени q из единицы.

Нас будет интересовать вопрос: когда существует точное неразложимое представление $\rho : G \longrightarrow \mathrm{GL}(V)$, такое, что $\rho(G)$ – одноинвариантная группа.

Обозначим q' наименьший простой делитель q.

Теорема 1. *Если $n \leqslant q'$, то существует неразложимое представление ρ группы G в $\mathrm{GL}(V)$ такое, что $\rho(G)$ одноинвариантна. При этом для любого такого представления ρ в некотором базисе про-*

странства V

$$\rho(u) = \exp\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & & & & \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

$$(*)$$

$$\rho(\delta) = \begin{pmatrix} k^{n-1} & 0 & \dots & 0 & 0 \\ 0 & k^{n-2} & 0\dots & 0 & 0 \\ \dots & & & & \\ 0 & 0 & \dots & k & 0 \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Если $n > q'$, то представления группы G в $\mathrm{GL}(V)$, такого, что $\rho(G)$ одноинвариантна, не существует.

Доказательство. Пусть $\rho : G \longrightarrow \mathrm{GL}(V)$ – некоторое неразложимое представление группы G, при этом $\rho(G)$ одноинвариантна.

Пусть $v \in V$, V/Y – некоторое факторпространство. Будем обозначать символом $\overline{v}$ класс элемента v в V/Y.

Лемма 1. *Пусть $W = V/Y$, где $V^G \leq Y$ – некоторое инвариантное относительно $\rho(G)$ подпространство. Пусть также ρ' соответствующее представление группы G в W, т.е. $\rho'(g)(\overline{v}) = \overline{\rho(g)(v)}$ для любого $g \in G$. Тогда собственные значения $\rho'(\delta)$ отличны от 1.*

Доказательство. Множество собственных значений оператора $\rho(\delta)$ есть объединение множества его собственных значений его ограничения на Y и множества собственнных значений $\rho'(\delta)$ на W (см., например, [8]). $\square$

Лемма 2. *Элемент $\rho(u)$ имеет один жорданов блок.*

Доказательство. Предположим, что у оператора $\rho(u)$ несколько блоков. Покажем тогда, что представление ρ – разложимо. Рассмотрим базис $e_1, \dots, e_n$, в котором элемент $\rho(u)$ имеет жорданову форму:

$$\rho(u) = \begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ . & . & . & . \\ 0 & 0 & \dots & J_l \end{pmatrix},$$

где J_i – жордановы блоки.

Пусть $V_i = \langle e_{i_1}, e_{i_1+1}, \dots, e_{i_m} \rangle$ – подпространство, соответствующее i-му блоку, и пусть $V_1 = \langle e_1, \dots, e_k \rangle$, (где $\rho(u)(e_k) = e_k$, $\rho(u)(e_j) = e_j + e_{j+1}$ при $j < k$.)

Так как группа G одноинвариантна, то $\rho(\delta)(e_k) = e_k$. Рассмотрим пространство $W_k = V/\langle e_k \rangle$ и представление $\rho_k : G \longrightarrow \mathrm{GL}(W_k)$, являющееся фактор-представлением ρ.

Очевидно,

$$W_k^{\rho_k(U)} = \langle \overline{V^G}, \overline{e_{k-1}} \rangle.$$

Так как $\overline{e_{k-1}}$ – инвариант $\rho_k(u)$ и δ нормализует U, то $\rho_k(\delta)\overline{(e_{k-1})} \in W_k^{\rho_k(U)}$. Значит, $\rho(\delta)(e_{k-1}) = a_{k-1}e_{k-1} + w$, где $w \in V^G$, $a_{k-1} \in K$. При этом $a_{k-1} \neq 1$, так как a_{k-1} собственное значение оператора в V/V^G, соответствующего оператору $\rho(\delta)$ в V (лемма 1). Положим

$$e'_k = e_k, \quad e'_{k-1} = e_{k-1} + \frac{1}{(a_{k-1} - 1)}\, w.$$

Тогда

$$\rho(\delta)(e'_{k-1}) = a_{k-1}e_{k-1}, \qquad \rho(u)(e'_{k-1}) = e'_{k-1} + e'_k.$$

Пусть $\{e'_k, e'_{k-1}, \dots, e'_{m+1}\}$ – последовательность векторов пространства $\langle e_k, e_{k-1}, \dots, e_{m+1}, V^G \rangle$, таких, что при всех $m < i < k$

$$\rho(\delta)(e'_i) = a_i e'_i + z_i, \quad z_i \in \langle e'_{i+1}, \dots, e'_k \rangle, \quad \rho(u)(e'_i) = e'_i + e'_{i+1}.$$

Построим вектор e'_m.

Рассмотрим $W_{m+1} = V/\langle e'_{m+1}, \dots, e'_k \rangle$. Так как пространство $\langle e'_{m+1}, \dots, e'_k \rangle$ инвариантно относительно $\rho(G)$ (по построению), то определено фактор-представление $\rho_{m+1} : G \longrightarrow W_{m+1}$. При этом

$$W_{m+1}^{\rho_{m+1}(U)} = \langle \overline{V^G}, \overline{e_m} \rangle.$$

Так как $\overline{e_m}$ – ивариант $\rho_{m+1}(u)$ и δ нормализует U, то $\rho_{m+1}(\delta)\overline{(e_m)} \in W_{m+1}^{\rho_{m+1}(U)}$. Следовательно, $\rho(\delta)(e_m) = a_m e_m + z_m + w_m$, где $z_m \in \langle e'_{m+1}, \dots, e'_k \rangle$, $w_m \in V^G$, $a_i \in K$. При этом, $a_m \neq 1$, так как a_m – собственное значение, соответствующее вектору $\overline{e_m} \in V/\langle V^G, e'_{m+1}, \dots, e'_k \rangle$ (лемма 1). Положим:

$$e'_m = e_m + \frac{1}{a_m - 1} w_m.$$

Получаем $\rho(\delta)(e'_m) = a_m e'_m + z_m$ и $\rho(u)(e'_m) = e'_m + e'_{m+1}$.

Таким образом, мы можем построить последовательность векторов

$$e'_1 = e_1 + v_1, e'_2 = e_2 + v_2, \dots, e'_{k-1} = e_{k-1} + v_{k-1}, e'_k = e_k, \quad v_i \in V^G,$$

таких, что $V'_1 = \langle e'_1, \dots, e'_k \rangle$ – $\rho(G)$-инвариантное подпространство V. Такую же процедуру мы можем проделать и с векторами базисов других компонент $V_i = \langle e_{i_1}, e_{i_1+1}, \dots, e_{i_m} \rangle$. Получаем последовательность из n векторов $e'_1, \dots, e'_n$. Проверим теперь, что построенная последовательность – базис V.

Предположим, что существуют $\alpha_1, \dots, \alpha_n$ (не все нули) такие, что:

$$\alpha_1 e'_1 + \ldots + \alpha_n e'_n = 0.$$

Выберем такое минимальное m, что $\alpha_m \neq 0$ и при этом $e'_m \notin V^G$. Заменим каждый вектор в этой сумме на его разложение по старому базису. Получим новую сумму:

$$\alpha_1(e_1 + \ldots) + \alpha_2(e_2 + \ldots) + \ldots + \alpha_n e_n = 0.$$

Заметим, что $e'_m = e_m + \ldots$, при этом в данной сумме слагаемое вида αe_m, $\alpha \in K$, больше не встречается, и e_m не может быть выражен через остальные векторы $(e_1, \dots, e_{m-1},\ e_{m+1}, \dots, e_n)$, так как $(e_1, \dots, e_n)$ – базис. Поэтому коэффициент при e_m будет $\alpha_m \neq 0$, а значит вся сумма не ноль. Следовательно, ненулевыми могут быть только коэффициенты при $\rho(G)$-инвариантных элементах этой последовательности: $e'_k, \dots, e'_{i_m}, \dots, e'_n$. Но эти элементы образуют подмножество базиса $e_1, \dots, e_n$, значит, линейно независимы. Противоречие.

Итак, получаем, что в V раскладывается в прямую сумму инвариантных относительно $\rho(G)$ подпространств, а именно:

$$V = V'_1 \oplus V'_2 \oplus \ldots \oplus V'_l,$$

где $V'_i = \langle e'_{i_1}, \dots, e'_{i_m} \rangle$. Следовательно, ρ – разложимо. □

По лемме 2 $\rho(u)$ имеет один блок. Так как порядок элемента u равен p, то размер данного блока не превосходит p, а значит в некотором базисе пространства V имеем

$$\rho(u) = \exp \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Положим

$$\delta_0 = \begin{pmatrix} k^{n-1} & 0 & \dots & 0 & 0 \\ 0 & k^{n-2} & 0 & 0 & 0 \\ \dots & & \dots & & \\ 0 & 0 & \dots & k & 0 \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Имеет место:

(I) $\delta_0\rho(u)\delta_0^{-1} = \rho(u)^k$.

(II) оператор δ_0 имеет тот же инвариантный вектор e_n, что и $\rho(u)$, а значит и $\rho(\delta)$.

(III) элемент $q = \delta_0^{-1}\rho(\delta)$ коммутирует с элементом $\rho(u)$, то есть $q \in C_u$ (C_u – централизатор элемента $\rho(u)$ в группе $\mathrm{GL}(V)$).

(I) и (II) очевидны по построению δ_0, а (III) следует из (I) и аналогичного соотношения для $\rho(\delta)$.

Лемма 3. *Пусть $n \leq q$. Тогда $q = [\delta_0^{-1}, c]$ для некоторого $c \in C_u$.*

Доказательство. Пусть $\mathfrak{U} \leq \mathrm{GL}(V)$ – подгруппа верхних треугольных унипотентых матриц. Тогда $C_u \leq Z(\mathrm{GL}(V))\mathfrak{U}$ (см., например, [8, с. 199–201]). Следовательно, $q = z\mathfrak{u}$, где $z \in Z(\mathrm{GL}(V))$, $\mathfrak{u} \in \mathfrak{U}$. Из условия (II) получаем $z = 1$, а значит $q \in \mathfrak{U}$. Далее, пусть $Q = C_u \cap \mathfrak{U}$, $Q_i = Q \cap \mathfrak{U}_i$, где $\mathfrak{U}_i$ – это i-тый член убывающего центрального ряда группы $\mathfrak{U}$. Так как $\delta_0^{-1}\mathfrak{U}_i\delta_0 = \mathfrak{U}_i$, $\delta_0^{-1}Q\delta_0 = Q$ (δ_0 нормализует $\langle\rho(u)\rangle$, а следовательно, и Q), то $\delta_0^{-1}Q_i\delta_0 = Q_i$. Далее, для любого i определено отображение

$$\phi_i : \mathfrak{U}_i/\mathfrak{U}_{i+1} \longrightarrow \mathfrak{U}_i/\mathfrak{U}_{i+1},$$

индуцированное отображением $x \longrightarrow [\delta_0^{-1}, x]$ на $\mathfrak{U}_i$. При этом ϕ_i – обратимый линейный оператор на линейном пространстве $\mathfrak{U}_i/\mathfrak{U}_{i+1}$ (действительно, из условия $n \leq q$ следует, что δ_0 – регулярный полупростой элемент), а значит, $\phi_i(Q_i/Q_{i+1}) = \phi(Q_i/Q_{i+1})$. Отсюда получаем $[\delta_0^{-1}, Q] = Q$. □

Теперь пусть $n \leq q' \leq q$. Ввиду леммы 3,

$$\rho(\delta) = \delta_0 q = c\delta_0 c^{-1}$$

для некоторого $c \in C_u$. Следовательно, в некотором базисе операторы $\rho(u)$, $\rho(\delta)$ имеют форму $(*)$. При этом условие $n \leq q'$ обеспечивает одноинвариантность группы $\rho(G)$.

Докажем теперь, что при $n > q'$ неразложимого одноивариантного представления не существует. Предположим, что такое представление существует. Из доказательства леммы 2 (построение базиса $e'_1, \ldots, e'_n$) следует, что в некотором базисе $\rho(u)$ – это жорданов блок, а $\rho(\delta)$ – верхняя треугольная матрица. Из соотношения $\rho(\delta)\rho(u)\rho(\delta^{-1}) = \rho(u^k)$ следует, что диагональные элементы матрицы $\rho(\delta)$, выписанные снизу вверх, – это $1, k, k^2, \ldots, k^{n-1}$. Но при $n > q'$ среди этих собственных значений не все будут первообразными корнями степени q из единицы, а значит, для некоторого $d < q$ оператор $\rho(\delta^d)$ будет иметь более одного единичного собственного значения, что противоречит одноинвариантности группы $\rho(G)$. $\square$

Случай II

Пусть K – поле, V – конечномерное линейное пространство над полем K и пусть $G \leq \mathrm{GL}(V)$.

Пусть далее I_G – идеал группового кольца $\mathbb{Z}[G]$, порождённый элементами $g-1$, где $g \in G$. Положим

$$V_0 = \{v \in V \mid I_G\, v = 0\},$$
$$V_1 = \{v \in V \mid I_G\, v \subset V_0\}, \ldots, V_{i+1} = \{v \in V \mid I_G\, v \subset V_i\}, \ldots .$$

Далее обозначим $\mathfrak{l}_{I_G}(V) = \min\{n \in \mathbb{N} \mid V_n = V\}$ и назовём это число I_G-длиной G-модуля V.

Теорема 2. *Пусть K – поле характеристики p; $G = \langle \sigma, \tau \rangle$, где $\sigma^p = \tau^p = 1$, $\sigma\tau = \tau\sigma$; V – неразложимый одноинвариантный G-модуль I_G-длины 1. Пусть коразмерность V^G в V равна k. Тогда размерность V равна либо $2k+1$, либо $2k$. Более того, для любого $m = 2k+1$ существует единственный такой $K[G]$-модуль. Для любого $m = 2k$ существует такой $K[G]$-модуль, при этом, если K – бесконечное поле, то число неизоморфных неразложимых $K[G]$-модулей бесконечно.*

Доказательство. Пусть $\Gamma \leq \mathrm{GL}(W)$ – линейная группа, где W – одноинвариантный Γ-модуль I_G-длины 1 над полем K. Тогда в пространстве W существует базис такой, что все элементы группы Γ представлены матрицами вида

$$\gamma = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & a_{1\,k+1} & \cdots & a_{1\,m} \\ 0 & 1 & 0 & \cdots & 0 & a_{2\,k+1} & \cdots & a_{2\,m} \\ \cdots \\ 0 & 0 & 0 & \cdots & 1 & a_{k\,k+1} & \cdots & a_{k\,m} \\ 0 & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 \\ \cdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 1 \end{pmatrix}, \qquad (1)$$

где $m = \dim W$, $m - k = \dim W^{\Gamma}$. Более того, если обозначить $A(\gamma) \in M_{k\times(m-k)}(K)$ матрицу в верхнем правом углу (1), то

$$\operatorname{rank} A(\gamma) = k \qquad (2)$$

для всех $\gamma \in \Gamma$, $\gamma \neq 1$ и

$$A(\gamma_1\gamma_2) = A(\gamma_1) + A(\gamma_2)$$

для любых $\gamma_1, \gamma_2 \in \Gamma$. $\square$

Лемма 4. *Пусть*

$$S = \begin{pmatrix} B & | & X \\ --- & | & --- \\ 0 & | & C \end{pmatrix} \in \mathrm{GL}_m(K),$$

где $B \in \mathrm{GL}_k(K)$, $C \in \mathrm{GL}_{(m-k)\times(m-k)}(K)$, $X \in M_{k\times(m-k)}(K)$. *Тогда*

$$A(S\gamma S^{-1}) = BA(\gamma)C^{-1}.$$

Доказательство. Очевидно имеем

$$S\gamma S^{-1} =$$

$$\begin{pmatrix} B & | & X \\ --- & | & --- \\ 0 & | & C \end{pmatrix} \begin{pmatrix} E & | & A \\ --- & | & --- \\ 0 & | & E \end{pmatrix} \begin{pmatrix} B^{-1} & | & -B^{-1}XC^{-1} \\ --- & | & --- \\ 0 & | & C^{-1} \end{pmatrix} =$$

$$\begin{pmatrix} B & | & X+BA \\ --- & | & --- \\ 0 & | & C \end{pmatrix} \begin{pmatrix} B^{-1} & | & -B^{-1}XC^{-1} \\ --- & | & --- \\ 0 & | & C^{-1} \end{pmatrix} = \begin{pmatrix} E & | & BAC^{-1} \\ --- & | & --- \\ 0 & | & E \end{pmatrix}.$$

$\square$

Пусть группа $\Delta = \mathrm{GL}_n(K) \times \mathrm{GL}_{n+s}(K)$ действует на $M_{n\times(n+s)}(K)$ следующим образом:

$$(B, C)M \stackrel{\text{def}}{=} BMC^{-1},$$

где $B \in \mathrm{GL}_n(K)$, $C \in \mathrm{GL}_{n+s}(K)$, $M \in M_{n\times(n+s)}(K)$. Пусть E_n – единичная матрица в $\mathrm{GL}_n(K)$ и $0_{n\times s} \in M_{n\times s}(K)$ – нулевая матрица. Положим

$$M_1 = \bigl(E_n \mid 0_{n\times s}\bigr).$$

Пусть $G_1 \leq \Delta$ – стабилизатор M_1.

Лемма 5. *G_1 – множество пар (A, B), где $A \in \mathrm{GL}_n(K)$, при этом*

$$B = \begin{pmatrix} A & | & 0_{n\times s} \\ --- & | & --- \\ Y & | & D \end{pmatrix} \in \mathrm{GL}_{n+s}(K), \tag{3}$$

где $Y \in M_{s\times n}(K)$, $D \in \mathrm{GL}_s(K)$.

Доказательство. Действительно, пусть $(A, B) \in \Delta$, $A \in \mathrm{GL}_n(K)$, $B \in \mathrm{GL}_{n+s}(K)$. Значит, $(A, B) \in G_1$ тогда и только тогда, когда $AM_1B^{-1} = M_1$. Получаем

$$AM_1B^{-1} = \bigl(A \mid 0_{n\times s}\bigr)B^{-1} = \bigl(E_n \mid 0_{n\times s}\bigr).$$

Следовательно, матрица B должна иметь вид (3). □

Далее, пусть $L_1, L_2 \in M_{n\times(n+s)}(K)$ – матрицы такие, что

$$\operatorname{rank} L_1 = \operatorname{rank} L_2 = n. \tag{4}$$

Лемма 6. *Предположим $s \leq n$. Тогда существуют $A \in \mathrm{GL}_n(K)$, $B \in \mathrm{GL}_{n+s}(K)$ такие, что $AL_1B^{-1} = M_1$ и выполнено одно из двух*

$$AL_2B^{-1} = \bigl(T \mid 0_{n\times 1}\bigr), \quad T \in M_{n\times(n+s-1)}(K), \tag{5}$$

или

$$AL_2B^{-1} = \begin{pmatrix} T & | & 0_{(n-s)\times s} \\ -- & & -- \\ 0_{s\times n} & | & E_s \end{pmatrix}, \quad T \in M_{(n-s)\times n}(K),\ \operatorname{rank} T = n - s. \tag{6}$$

Доказательство. Можно считать, что $L_1 = M_1$, а B имеет вид (3) по лемме 5. Предположим, что последние s столбцов L_2 линейно зависимы, тогда с помощью преобразования $L_2 \to AL_2B^{-1}$ можно получить вид (5). Значит, можно считать, что последние s столбцов L_2 линейно независимы. Представим

$$L_2 = \bigl(\widetilde{L} \mid L'\bigr), \quad \widetilde{L} \in M_n(K), \quad L' \in M_{n\times s}(K).$$

Положим в форме (3) $Y = 0_{s\times n}$, $D = E_s$, тогда

$$AL_2B^{-1} = \big(A\widetilde{L}A^{-1} \mid AL'\big).$$

Поскольку rank $L' = s$, найдётся матрица A такая, что

$$AL' = \begin{pmatrix} 0_{(n-s)\times s} \\ E_s \end{pmatrix}.$$

При таком преобразовании мы получаем $L_1 = M_1$,

$$AL_2B^{-1} = \begin{pmatrix} T & | & 0_{(n-s)\times s} \\ -- & & -- \\ Z & | & E_s \end{pmatrix}.$$

Далее, прибавляя к первым n столбцам L_2 подходящие кратные последних s столбцов, мы приведем L_2 к виду

$$\begin{pmatrix} T & | & 0_{(n-s)\times s} \\ -- & & -- \\ 0_{s\times n} & | & E_s \end{pmatrix},\ T \in M_{(n-s)\times n}(K),\ \ \operatorname{rank} T = n - s.$$

Заметим, что $L_1 = M_1$ при этом не изменится. □

Лемма 7. *Пусть $s \le n$, $L_1 = M_1$ и*

$$L_2 = \begin{pmatrix} T & | & 0_{(n-s)\times s} \\ -- & & -- \\ 0_{s\times n} & | & E_s \end{pmatrix}, \quad T \in M_{(n-s)\times n}(K), \quad \operatorname{rank} T = n - s.$$

Далее, пусть

$$A = \begin{pmatrix} A_1 & | & 0_{(n-s)\times s} \\ -- & & -- \\ C & | & D \end{pmatrix},$$

где $A_1 \in \mathrm{GL}_{n-s}(K)$, $C \in M_{s\times(n-s)}(K)$, $D \in \mathrm{GL}_s(K)$, а

$$B = \begin{pmatrix} A & | & 0_{n\times s} \\ --- & | & --- \\ CT & | & D \end{pmatrix}.$$

Тогда $AL_1B^{-1} = L_1$ и

$$AL_2B^{-1} = \begin{pmatrix} A_1TA^{-1} & | & 0_{(n-s)\times s} \\ -- & & -- \\ 0_{s\times n} & | & E_s \end{pmatrix}.$$

Доказательство. Равенство $AL_1B^{-1} = L_1$ следует из леммы 5, так как матрица B имеет вид (3). При этом,

$$AL_2B^{-1} = \begin{pmatrix} A_1T & \mid & 0_{(n-s)\times s} \\ -- & & -- \\ CT & \mid & D \end{pmatrix} \begin{pmatrix} A^{-1} & \mid & 0_{n\times s} \\ --- & \mid & --- \\ -D^{-1}CTA^{-1} & \mid & D^{-1} \end{pmatrix} =$$
$$= \begin{pmatrix} A_1TA^{-1} & \mid & 0_{(n-s)\times s} \\ -- & & -- \\ 0_{s\times n} & \mid & E_s \end{pmatrix}.$$

□

Лемма 8. *Пусть $n - s \le s < n$. Тогда найдутся $A \in \mathrm{GL}_n(K)$, $B \in \mathrm{GL}_{n+s}(K)$ такие, что $AL_1B = M_1$ и AL_2B^{-1} имеет вид* (5), *либо*

$$AL_2B^{-1} = \begin{pmatrix} T' & \mid & 0_{(n-s)\times 1} & \mid & 0_{(n-s)\times s} \\ -- & & -- & & -- \\ 0_{s\times(n-1)} & \mid & 0_{s\times 1} & \mid & E_s \end{pmatrix}, \qquad (7)$$

где $T' \in M_{(n-s)\times(n-1)}(K)$,

или $n = 2s$ *и*

$$AL_2B^{-1} = \begin{pmatrix} 0_{s\times s} & \mid & E_s & \mid & 0_{s\times s} \\ -- & & -- & & -- \\ 0_{s\times s} & \mid & 0_{s\times s} & \mid & E_s \end{pmatrix}. \qquad (8)$$

Доказательство. Можно считать по лемме 6, что $L_1 = M_1$ и L_2 имеет вид (6). По лемме 7 можно вместо T рассматривать A_1TA^{-1}. Заметим, что при $n - s < s$ последние s столбцов матрицы T линейно зависимы. Рассмотрим этот случай. Положим $A_1 = E_{n-s}$, $C = 0$. Тогда, если

$$T = \big(T_1 \mid T_2\big), \quad T_1 \in M_{n-s}(K), \quad T_2 \in M_{(n-s)\times s}(K),$$

то мы получаем

$$A_1TA^{-1} = \big(T_1 \mid T_2D^{-1}\big). \qquad (9)$$

С помощью матрицы D^{-1} можно получить, что последний столбец матрицы T_2 (а значит и T) будет нулевым, таким образом получили вид (7) для L_2.

Рассмотрим случай $n-s=s$ и последние s столбцов линейно независимы. Тогда $T_2 \in \mathrm{GL}_s(K)$ и, следовательно существует D^{-1} такая, что $T_2 D^{-1} = E_s$. То есть можно считать, что

$$T = \left(T_1 \mid E_s\right), \quad T_1 \in M_s(K).$$

Далее, положим $A_1 = E_s$, $D = E_s$, $C = T_1$ (где A_1, D, C из леммы 7). Теперь

$$A_1 T A^{-1} = \left(T_1 \mid E_s\right) \begin{pmatrix} E_s & \mid & 0_{s\times s} \\ -- & & -- \\ -T_1 & \mid & E_s \end{pmatrix} = \left(0_{s\times s} \mid E_s\right)$$

и, таким образом, получаем вид (8). □

Лемма 9. *Пусть $s \geq n$. Тогда существуют $A \in \mathrm{GL}_n(K)$, $B \in \mathrm{GL}_{n+s}(K)$ такие, что $AL_1B = M_1$ а также AL_2B^{-1} имеет вид (5) или*

$$AL_2B^{-1} = \left(0_{n\times s} \mid E_n\right).$$

Доказательство. Можно считать, что $L_1 = M_1$, $A = E_n$, а блок Y матрицы B в форме (3) – нулевой. Тогда, если L_2' – матрица, состоящая из s последних столбцов матрицы L_2, то матрица из s последних столбцов матрицы AL_2B^{-1} равна $L_2'D^{-1}$. Если столбцы L_2' линейно зависимы, то, очевидно, можно получить последний нулевой столбец у $L_2'D^{-1}$, а если линейно независимы (это возможно только при $n=s$), то при подходящем D матрица $L_2'D^{-1}$ – единичная. Теперь соответствующие преобразования со столбцами дадут требуемый результат. □

Лемма 10. *Пусть $1 \leq s < n$. Тогда найдутся $A \in \mathrm{GL}_n(K)$, $B \in \mathrm{GL}_{n+s}(K)$ такие, что $AL_1B = M_1$ и*

$$AL_2B^{-1} = \begin{pmatrix} T & \mid & 0_{r\times 1} & \mid & 0_{r\times(n-r)} \\ -- & & -- & & -- \\ 0_{(n-r)\times(r+s-1)} & \mid & 0_{(n-r)\times 1} & \mid & E_{n-r} \end{pmatrix}, \qquad (10)$$

где $T \in M_{r\times(r+s-1)}(K)$, $n = qs + r$ для некоторого $q \in \mathbb{N}\cup\{0\}$, $0 \leq r \leq n$.

Доказательство. Если в лемме 8 мы имели (5), то лемма 10 выполенена при $r=n$. Пусть мы имели (6).

Если $n-s \leqslant s$, то наше утверждение следует из леммы 8. Предположим $n-s \geq s$. Докажем наше утверждение индукцией по $l = n - s - s$ начиная с $l = 0$. При $l = 0$ утверждение следует из леммы 8. Теперь пусть наше утверждение выполнено для всех пар (n, s), таких, что $0 \leq n - 2s < l$ и рассмотрим пару (n, s), где $n - 2s = l$. Можно предположить, что $L_1 = M_1$ и L_2 имеет вид (6), где $T \in M_{(n-s)\times n}(K)$. Теперь положим $n_1 = n - s$, $s_1 = s$. Если $s_1 \geq n_1$ то мы можем получить наше утверждение из лемм 9 и 7. Если $s_1 \leq n_1$, тогда мы имеем $n_1 - 2s_1 < l$, применим предположение индукции и лемму 7, если $n_1 - 2s_1 \geq 0$, или леммы 7, 8, если $n_1 - s_1 < s_1$. $\square$

Переходим к доказательству теоремы. Пусть V – неразложимый $K[G]$-модуль, $\dim V = m$, положим $\dim V^G = m - k$.

Покажем, что $m \leq 2k + 1$. Пусть $m > 2k + 1$. Положим $n := k$, $s := m - 2k$. Тогда по (1) и леммам 4, 9, 10 имеем

$$\sigma = \begin{pmatrix} E_n & | & L_\sigma \\ -- & & -- \\ 0_{(m-n)\times n} & | & E_{m-n} \end{pmatrix}, \quad \tau = \begin{pmatrix} E_n & | & L_\tau \\ -- & & -- \\ 0_{(m-n)\times n} & | & E_{m-n} \end{pmatrix}, \quad (11)$$

где

$$\begin{aligned} L_\sigma &= \big(E_n \mid 0_{n\times s}\big), \\ L_\tau &= \begin{pmatrix} T & | & 0_{r\times 1} & | & 0_{r\times(n-r)} \\ -- & & -- & & -- \\ 0_{(n-r)\times(r+s-1)} & | & 0_{(n-r)\times 1} & | & E_{n-r} \end{pmatrix}, \end{aligned} \quad (12)$$

где $T \in M_{r\times(r+s-1)}(K)$.

Пусть теперь $e_1, \dots, e_n, f_1, \dots f_{m-n}$ — базис пространства V, в котором σ, τ имеют вид (11). Положим

$$\mathfrak{B}_1 = \{e_{r+is}, f_{r+js} \mid i, j \in \mathbb{N}\}, \qquad \mathfrak{B}_2 = \{e_a, f_b \mid e_a, f_b \notin \mathfrak{B}_1\}.$$

Заметим, что $r < n$. Действительно, если $n = r$, то $V = \langle e_1, \dots, e_n, f_1, \dots, f_{m-n-1}\rangle \oplus \langle f_{m-n}\rangle$ – разложение $K[G]$-модуля V.

Таким образом, $\mathfrak{B}_1 \neq \emptyset$.

Пусть $e_a \in \mathfrak{B}_1$. Тогда $a = r + is$, $i \in \mathbb{N}$ и

$$\begin{aligned} \sigma(e_{r+is}) &= e_{r+is} + f_{r+is} \in \langle \mathfrak{B}_1 \rangle, \\ \tau(e_{r+is}) &= e_{r+is} + f_{r+(i+1)s} \in \langle \mathfrak{B}_1 \rangle. \end{aligned} \quad (13)$$

(следует из (11) и (12)).

Пусть теперь $e_a \notin \mathfrak{B}_1$ и $a \le r$. Тогда

$$\begin{aligned} \sigma(e_a) &= e_a + f_a \in \langle \mathfrak{B}_2 \rangle, \\ \tau(e_a) &= e_a + \sum_{l<r+s} k_l f_l \in \langle \mathfrak{B}_2 \rangle, \text{ где } \ k_l \in K. \end{aligned} \tag{14}$$

Пусть $a > r$. Так как $a \ne r + is$ ни для какого $i \in \mathbb{N}$, получаем $a + s \ne r + js$ при всех $j \in \mathbb{N}$. Таким образом,

$$\sigma(e_a) = e_a + f_a \in \langle \mathfrak{B}_2 \rangle, \qquad \tau(e_a) = e_a + f_{a+s} \in \langle \mathfrak{B}_2 \rangle. \tag{15}$$

Заметим, что $s > 1$, так как $m > 2k+1$ по предположению. Получаем $\mathfrak{B}_2 \ne \emptyset$. Положим $V_1 = \langle \mathfrak{B}_1 \rangle$, $V_2 = \langle \mathfrak{B}_2 \rangle$. Тогда из (13)–(15) получаем разложение $V = V_1 \oplus V_2$ для $K[G]$-модуля V, которое противоречит предположению о неразложимости V.

Пусть теперь $m = 2k + 1$ и мы рассмариваем вид (11) и (12). Если $r > 0$, тогда $\mathfrak{B}_1 = \{e_a, f_b \mid a, b \le r\}, \mathfrak{B}_2 = \{e_a, f_b \mid a, b > r\} \ne \emptyset$ и имеем разложение $K[G]$-модуля V аналогичное привёденному выше. Следовательно, $r = 0$ и в соответствующем базисе σ, τ имеют вид (11), где

$$L_\sigma = \big(E_n \mid 0_{n\times 1}\big), \quad L_\tau = \big(0_{n\times 1} \mid E_n\big).$$

Это в точности пример неразложимого $p{\times}p$-модуля, приведенный в [1, стр. 397–398].

Пусть теперь $m = 2k$.

Предположим, что $K[G]$-модуль V разложим. Тогда в соответствующем базисе получаем вид (11), при этом

$$\begin{aligned} L_\sigma &= \begin{pmatrix} L_{1\sigma} & \mid & 0_{r\times(k-r)} \\ -- & & -- \\ 0_{(k-r)\times r} & \mid & L_{2\sigma} \end{pmatrix}, \\ L_\tau &= \begin{pmatrix} L_{1\tau} & \mid & 0_{r\times(k-r)} \\ -- & & -- \\ 0_{(k-r)\times r} & \mid & L_{2\tau} \end{pmatrix}, \end{aligned} \tag{16}$$

где $L_{1\sigma}$, $L_{1\tau} \in \mathrm{GL}_r(K)$, а $L_{2\sigma}$, $L_{2\tau} \in \mathrm{GL}_{k-r}(K)$ для некоторого $0 < r < k$. Заметим также, что в соответствующем базисе можно получить $L_{1\sigma} = E_r$, $L_{2\sigma} = E_{k-r}$. Таким образом, если V – разложим, то в некотором базисе $L_\sigma = E_k$ и L_τ имеет вид (16).

Пусть теперь σ, τ имеют вид (11) и при этом $L_\sigma = E_k$. Тогда, для того чтобы при некоторой смене базиса L_σ не изменилась, а

L_τ имела вид (16) необходимо и достаточно, чтобы существовала такая матрица $A \in \mathrm{GL}_k(K)$, что $AL_\tau A^{-1}$ имеет вид (16). Это следует из лемм 4 и 5. Поэтому, если

$$\sigma = \begin{pmatrix} E_k & | & E_k \\ -- & & -- \\ 0_{k\times k} & | & E_k \end{pmatrix}, \quad \tau = \begin{pmatrix} E_k & | & L_\tau \\ -- & & -- \\ 0_{k\times k} & | & E_k \end{pmatrix} \tag{17}$$

тогда

$$V \ \text{ – разложимый } \ K[G]\text{-модуль} \Leftrightarrow AL_\tau A^{-1} = \\ = \begin{pmatrix} L_{1\tau} & | & 0_{r\times(k-r)} \\ -- & & -- \\ 0_{(k-r)\times r} & | & L_{2\tau} \end{pmatrix} \tag{18}$$

для некоторой $A \in \mathrm{GL}_k(K)$, $L_{1\tau} \in \mathrm{GL}_r(K)$, $L_{2\tau} \in \mathrm{GL}_{k-r}(K)$, $0 < r < k$.

Пусть теперь $K \neq \mathbb{F}_p$, а $\alpha \in K \setminus \mathbb{F}_p$. В случае, если в форме (17) $L_\tau = \alpha J_k$, где J_k – жорданов блок, нам не получить вид (18), и поэтому V – неразложимый $K[G]$-модуль. При этом он одноинвариантный, так как $\mathrm{rank}(s\alpha J_k + tE_k) = k$ при всех $s, t \in \mathbb{F}_p$ таких, что $s \neq 0$ или $t \neq 0$. В частности, таким способом можно получить бесконечное число неизоморфных модулей, если K является бесконечным полем.

Пусть теперь $K = \mathbb{F}_p$ и пусть $L/\mathbb{F}_p$ – расширение степени k. Тогда существует элемент $\epsilon \in L$, такой, что минимальный многочлен ϵ над полем $\mathbb{F}_p$ неприводим и имеет степень n. Пусть $Y_\epsilon \in \mathrm{GL}_n(K)$ – матрица, которая соответствует умножению в L на ϵ (в каком-нибудь базисе). Тогда для всех $S \in \mathrm{GL}_n(\mathbb{F}_p)$ матрица $SY_\epsilon S^{-1}$ не может иметь вид (16) (так как характеристический многочлен Y_ϵ, который равен минимальному многочлену ϵ, был бы приводим). Мы положим $L_\tau = Y_\epsilon$. Очевидно, $\mathrm{rank}(sL_\tau + tE_k) = k$ при всех $s, t \in \mathbb{F}_p$ таких, что $s \neq 0$ или $t \neq 0$, а следовательно, $G = \langle \sigma, \tau \rangle$ – одноинвариантная неразложимая группа. $\square$

Литература

1. Ч. Кэртис, И. Райнер, *Теория представлений конечных групп и ассоциативных алгебр.* М. (1969).
2. R. Guralnick, R. Wiegand, *Galois groups and the multiplicative structure of field extensions.* — Trans. Amer. Math. Soc. **331** (1992), No. 2, 563–584.

3. P. Fleischmann, W. Lempken, P. H. Tiep, *The p-intersection subgroups in quasi-simple and almost simple finite groups.* — J. Algebra **207** (1998), No. 1, 1–42.
4. P. Fleischmann, W. Lempken, P. H. Tiep, *The primitive p-Frobenius groups.* — Proc. Amer. Math. Soc. **126** (1998), No. 5, 1337–1343.
5. T. Springer, *Linear Algebraic Groups.* 2nd ed. Progress in Mathematics **9**, Boston (1998).
6. Дж. Вольф, *Пространство постоянной кривизны.* Наука, М. (1982).
7. N. Gordeev, N. Kushpel, *On same-invariant linear groups.* — Зап. научн. семин. ПОМИ **289** (2002), 134–148.
8. Ф. Гантмахер, *Теория матриц.* Наука, Москва (1967).

Kushpel N. N. On same-invariant linear groups.

A linear group $G \leq \mathrm{GL}(V)$ is called *same-invariant* if the subspaces of linear invariants V^g are the same for all $g \in G, g \neq 1$. In this paper, we consider finite same-invariant linear groups over a field of characteristic p which have order p^2 or pq, $(p,q)=1$.

Российский государственный
педагогический университет
им. А. И. Герцена

E-mail: kushpel@mail.ru

Поступило 25 декабря 2003 г.