Math-Net.Ru
Общероссийский математический портал

В. М. Левчук, Об одном свойстве групп Сузуки,
Алгебра и логика, 1972, том 11, номер 5, 551–557

https://www.mathnet.ru/al1350

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
https://www.mathnet.ru/rus/agreement

Параметры загрузки:
IP: 18.97.14.91
16 декабря 2025 г., 20:51:07

Алгебра и логика, 11, №5 (1972), 551-557.

УДК 519.45

ОБ ОДНОМ СВОЙСТВЕ ГРУПП СУЗУКИ

В.М.ЛЕВЧУК

В этой заметке частично решается вопрос Ю.М.Горчакова: аппроксимируется ли свободная группа ранга два любым бесконечным множеством конечных простых неабелевых групп? Доказана

ТЕОРЕМА 1. *Свободная группа ранга два аппроксимируется любым бесконечным множеством групп Сузуки* $Sz(q)$.

Ранее было известно, что свободная группа ранга два аппроксимируется бесконечными множествами знакопеременных групп подстановок нечётной степени [1], групп $PSL(2,q)$ [2], $PSL(3,q)$ [3,4]. Хейнекен и Нейман [5] доказали, что любое бесконечное множество групп $PSL(2,q)$ и $Sz(q)$ порождает многообразие всех групп. Результат Хейнекена и Неймана просто следует из теоремы 1 настоящей заметки и из [2].

§ 1.

Пусть x, y – коммутативные переменные и K – ассоциативное кольцо. Ниже будут рассматриваться рациональные функции над K от x, y, которые хотя бы одним способом можно представить в виде $x^k y^\ell f(x,y)$, где k, ℓ – целые числа, а $f(x,y)$ – многочлен над K. Совокупность всех таких рациональных функций над K образует кольцо, которое обозначим через $\Lambda_2[x,y]$, когда $K = GF(2)$.

ЛЕММА 1. *Группа, порожденная матрицами:*

$$\delta = \begin{pmatrix} xy & 0 & 0 & 0 \\ 0 & x & 0 & 0 \\ 0 & 0 & x^{-1} & 0 \\ 0 & 0 & 0 & x^{-1}y^{-1} \end{pmatrix} \quad \text{и} \quad \beta = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

над кольцом $\Lambda_2[x,y]$, распадается в свободное произведение подгруппы второго порядка и бесконечной циклической подгруппы.

ДОКАЗАТЕЛЬСТВО. Достаточно показать, что произвольное произведение

$$\delta^{\ell_1}\beta\delta^{\ell_2}\beta \ldots \delta^{\ell_\tau}\beta,$$

где $\tau \geqslant 1$, а $\ell_1, \ell_2, \ldots, \ell_\tau$ – ненулевые целые числа, не является диагональной матрицей. В свою очередь достаточно показать, что диагональной матрицей не является произведение $\alpha = \alpha_1\alpha_2 \ldots \alpha_\tau$,

$$\alpha_i \equiv (xy)^{|\ell_i|}\delta^{\ell_i}\beta, \qquad 1 \leqslant i \leqslant \tau.$$

Матрицы $\alpha_1, \alpha_2, \ldots, \alpha_\tau, \alpha$ можно рассматривать как многочлены от x, y над кольцом матриц степени 4, с элементами из поля $GF(2)$. Старший коэффициент многочлена α_i, $i = 1, 2, \ldots, \tau$, по совокупности переменных x, y определен однозначно и равен

$$\gamma_1 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{или} \quad \gamma_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

соответственно случаям $\ell_i > 0$ и $\ell_i < 0$. Полугруппа, порожденная матрицами γ_1 и γ_2 (по умножению), не содержит матриц, отличных от γ_1 и γ_2, в частности, нулевой матрицы. Поэтому старший коэффициент многочлена α по совокупности переменных x, y определен однозначно, равен произведению старших коэффициентов многочленов $\alpha_1, \alpha_2, \ldots, \alpha_\tau$ и, следовательно, равен γ_1 или γ_2. Отсюда следует, что матрица α имеет ненулевой элемент на месте (1,4) или (4, 1). Следовательно, α – недиагональная матрица. Лемма доказана.

Пусть h – собственный элемент поля $GF(q), q = 2^{2k-1}, k \geqslant 2$. Тогда существует и единствен гомоморфизм кольца $\Lambda_2[x,y]$ на поле

$GF(q)$, переводящий x в h, а y в h^{θ}, $\theta=2^{k}$. Обозначим его через φ_h. Если G – группа (кольцо) матриц над $\Lambda_2[x,y]$, то отображение

$$\|a_{ij}\| \longrightarrow \|\varphi_h(a_{ij})\|, \qquad \|a_{ij}\| \in G,$$

является гомоморфизмом группы (кольца) G, который далее будет обозначаться также символом φ_h.

§ 2.

ТЕОРЕМА 2. [6]. Группа $Sz(q)$, $q=2^{2k+1}$, $k\geq 1$, имеет следующие максимальные подгруппы:

1) группа диэдра порядка $2(q-1)$;

2) группа Фробениуса порядка $4(q+\tau+1)$, $\tau^2=2q$;

3) группа Фробениуса порядка $q^2(q-1)$: любые две её инволюции перестановочны;

4) $Sz(m)$, где $m^p=q$; p – простое число, делящее $2k+1$.

ЛЕММА 2. Пусть h – собственный элемент поля $GF(q)$, $q=2^{2k+1}$, $k\geq 1$, и β,δ – матрицы, определённые в лемме 1. Тогда

$$G=\varphi_h(\langle\beta,\delta\rangle)=Sz(q).$$

ДОКАЗАТЕЛЬСТВО. Очевидно, матрица $\varphi_h(\delta)$ содержится в группе $Sz(q)$. Матрица $\varphi_h(\beta)=\beta$ совпадает с матрицей $\gamma\tau\gamma$, где

$$\gamma=\begin{pmatrix}1&0&0&0\\0&1&0&0\\1&0&1&0\\1&1&0&1\end{pmatrix},\quad \tau=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix},$$

и поэтому также содержится в группе $Sz(q)$. Следовательно, G – подгруппа группы $Sz(q)$. Матрица $\varphi_h(\beta\delta\beta)$ не содержится в подгруппе $\varphi_h(\delta)$, и, следовательно, G – недиэдральная группа. Порядок

G не взаимно прост с числом $q-1$. Поэтому G есть группа Сузуки, либо подгруппа группы $Sz(q)$ типа (3) из теоремы 2. Допустим, что G - типа (3). Тогда $[\varphi_h(\delta^{-1}\beta\delta\beta)]^2$ - единичная матрица. С другой стороны, её элемент, стоящий на месте (1.3), равен

$$\varphi_h[x^{-4}y^{-4}(1+xy)^4(1+x^2y)] \neq 0.$$

Противоречие. Следовательно, $G=Sz(m)$, где в силу выбора h имеем $m=q$. Лемма доказана.

§ 3.

Пусть $f(x,y)$ и $g(x,y)$ - ненулевые многочлены над полем K. Результант многочленов $f(x,y)$ и $g(x,y)$, рассматриваемых как многочлены от y, будем обозначать символом $R_y(f,g)$. Напомним некоторые свойства результантов (см. [7], § 54).

(A) $R_y(f,g)$ есть многочлен от переменной x над K, степень которого не превосходит произведения степеней многочленов $f(x,y)$ и $g(x,y)$ по совокупности переменных x, y (если, конечно, он $\not\equiv 0$).

(B) Многочлен $R_y(f,g)$ обращается в нуль при $x=x_0$ в том и только в том случае, когда обращаются в нуль старшие коэффициенты многочленов $f(x,y)$ и $g(x,y)$ относительно y, либо существует такое $y=y_0$, что $f(x_0,y_0)=g(x_0,y_0)=0$.

ЛЕММА 3. Пусть $f(x,y)$ и $g(x,y)$ - многочлены над полем K, степени по y которых не равны нулю. Допустим, что результант $R_y(f,g)\equiv 0$. Тогда степень по y наибольшего общего делителя многочленов $f(x,y)$ и $g(x,y)$ не равна нулю. Верно и обратное.

ДОКАЗАТЕЛЬСТВО. Рассмотрим $f(x,y)$ и $g(x,y)$ как многочлены от y над трансцендентным расширением $K(x)$ поля K. Так как $R_y(f,g)\equiv 0$, то по свойству (B) в каком-либо расширении поля $K(x)$ найдется $y=y_0$, при котором $f(x,y_0)=g(x,y_0)=0$. Поэтому существует многочлен ненулевой степени по y, делящий $f(x,y)$ и $g(x,y)$. Обратное очевидно.

СЛЕДСТВИЕ 1. Пусть $f(x,y)$ и $g(x,y)$ - многочлены над полем K, причём $f(x,y)$ - не-

приводимый в поле K многочлен. Тогда $R_y(f,g)=0$ только в том случае, когда степень по y хотя бы одного из многочленов $f(x,y)$, $g(x,y)$ равна нулю, либо $f(x,y)$ делит $g(x,y)$.

Пусть $f(x,y)$ – многочлен над полем $GF(2)$, и допустим, что собственный элемент h поля $GF(2^{2k+1})$ такой, что $\varphi_h[f(x,y)] = f(h,h^\theta)=0$, $\theta=2^{k+1}$ (см. § 1). Тогда $[f(h,h^\theta)]^\theta = f(h^\theta,h^{\theta^2}) = f(h^\theta,h^2)=0$. Поэтому отображение φ_h переводит в нуль также и многочлен $f(y,x^2)=\bar{f}(x,y)$. Нетрудно убедиться, что отображение $f(x,y)\to\bar{f}(x,y)=f(y,x^p)$ является гомоморфизмом кольца всех многочленов над полем $GF(p)$, p – простое число, в себя. Кроме того, $\bar{\bar{f}}(x,y)=[f(x,y)]^p$.

ЛЕММА 4. Пусть $f(x,y)$ – ненулевой многочлен над полем $GF(2)$, неприводимый в этом поле и имеющий ненулевые степени по x и по y. Тогда $R_y(f,\bar{f})\neq 0$.

ДОКАЗАТЕЛЬСТВО. Допустим противное. Тогда по следствию 1 многочлен $f(x,y)$ делит $\bar{f}(x,y)$, то есть $\bar{f}(x,y)=f(x,y)g(x,y)$, где степень многочлена $g(x,y)$ не равна нулю по условию. Отсюда находим

$$[f(x,y)]^2=\bar{\bar{f}}(x,y)=\overline{f(x,y)g(x,y)}=\bar{f}(x,y)\bar{g}(x,y)=f(x,y)g(x,y)\bar{g}(x,y),$$

откуда $f(x,y)=g(x,y)g(y,x^2)$. Но это противоречит неприводимости многочлена $f(x,y)$ над полем $GF(2)$. Лемма доказана.

ЛЕММА 5. Свободное произведение бесконечной циклической группы и группы порядка два аппроксимируется группами Сузуки $Sz(m)$.

ДОКАЗАТЕЛЬСТВО. Лемма будет доказана, если для произвольного элемента $\alpha\neq\varepsilon$ группы $G=\langle\beta,\delta\rangle$, где β, δ определены в лемме 1, а ε – единичная матрица, найдется гомоморфизм группы G на группу $Sz(q)$ для некоторого $q=2^{2k+1}$, при котором α имеет неединичный образ. Матрица $\alpha-\varepsilon$ имеет ненулевые элементы. Пусть $g(x,y)\in\Lambda_2[x,y]$ – один из них. Тогда $g(x,y)=x^m y^n f(x,y)$, где m, n – целые числа, а $f(x,y)$ – многочлен над полем $GF(2)$.

Рассмотрим его разложение

$$f(x,y)=f_1(x)f_2(y)q_1(x,y)q_2(x,y)\dots q_r(x,y),\quad r\geq 0,$$

где $q_1(x,y),\dots,q_r(x,y)$ – неприводимые многочлены над полем $GF(2)$, степени по x и по y которых не равны нулю. Пусть t_1 и t_2 – степени многочленов f_1 и f_2 соответственно, а s_1, $s_2,\dots,s_r$ – степени по совокупности переменных x, y соответственно многочленов $q_1,q_2,\dots,q_r$. Выберем натуральное число k так, что

$$2k>\max\{t_1,t_2,2s_1^2,2s_2^2,\dots,2s_r^2\}.$$

и пусть h – примитивный элемент поля $GF(2^{2k+1})$. Наименьшая степень ненулевого многочлена над полем $GF(2)$, корнем которого является элемент h или сопряженный с ним, равна $2k+1$. В частности, $f_1(h)f_2(h^\theta)\neq 0$, $\theta=2^{k+1}$ Допустим, что $r>0$, и пусть $1\leq i\leq r$. Старший коэффициент многочлена $q_i(x,y)$, рассматриваемого как многочлен от y, не равен нулю при $x=h$, так как его степень $\leq s_i$. Степень многочлена $q_i(y,x^2)$ по совокупности переменных x, y не превосходит числа $2s_i$. Поэтому многочлен $R_y(q_i,\bar{q}_i)$ является ненулевым по лемме 4, и степень его не превосходит $2s_i^2$, по свойству (А). Поэтому h не является его корнем. Допустим, что $q_i(h,h^\theta)=0, \theta=2^{k+1}$. Но тогда $\bar{q}_i(h,h^\theta)=0$, и, следовательно, по свойству (В) результанта, h – корень многочлена $R_y(q_i,\bar{q}_i)$. Противоречие. Следовательно, $q_i(h,h^\theta)\neq 0$, $i=1,2,\dots,r$. Отсюда следует, что $\varphi_h[g(x,y)]=g(h,h^\theta)\neq 0$, $\theta=2^{k+1}$ и $\varphi_h(\alpha)\neq\varepsilon$. По лемме 2, гомоморфизм φ_h отображает группу G на группу $Sz(2^{2k+1})$. Лемма доказана.

Отметим, что если группа F аппроксимируется классом групп Ω_1, а каждая группа из класса Ω_1 аппроксимируется классом групп Ω_2, то и F аппроксимируется классом групп Ω_2. Поэтому теорема 1 вытекает из леммы 5 и следующей леммы.

ЛЕММА 6 (см., например, [1]). Свободная группа ранга два аппроксимируется свободным произведением бесконечной циклической группы и группы порядка два.

Автор благодарит Ю.М.Горчакова за постановку задачи и руководство в работе.

Литература

1. R.KATZ, W.MAGNUS, A residual properties of free groups, Comm.Pure Appl.Math.,22(1969),1-13.

2. Ю.М.ГОРЧАКОВ, В.М.ЛЕВЧУК, Об аппроксимации свободных групп, Алгебра и логика, 9, № 4 (1970). 415-421.

3. В.М.ЛЕВЧУК, Об аппроксимируемости свободных групп группами $PSL(3,q)$ при нечётном q, в сб. "Алгебра. Вложение групп. Алгоритмические вопросы", Красноярск, Ин-т физики СО АН СССР (1970), 71-93.

4. В.М.ЛЕВЧУК, О некоторых аппроксимациях свободных групп 11-й Всесоюзн. алгебр. колл., Рез. сообщ. и докл., Кишинев, 1971, 55.

5. H.HEINEKEN.,P.M.NEUMANN, Identical relations and decision procedures for groups,J.Austral.Math.Soc.,7, № 1 (1967),39-47.

6. M.SUZUKI, On a class of doubly transitive groups I,Ann. Math.,75(1962),105-145.

7. А.Г.КУРОШ, Курс высшей алгебры, изд. 9, Наука, М., 1968.

Поступило 18 апреля 1972 г.