Известия вузов. Математика
2008, № 12, с. 17–27

http://www.ksu.ru/journals/izv_vuz/
e-mail: izvuz.matem@ksu.ru

А.И. ДОЛГАРЕВ

ОПИСАНИЕ КОНЕЧНЫХ НИЛЬПОТЕНТНЫХ ГРУПП СТУПЕНИ 2 ПРОСТОГО НЕЧЕТНОГО ПЕРИОДА

Аннотация. Получено описание названных групп в результате задания значений коммутаторов порождающих элементов и при задании групповой операции на кортежах элементов поля Галуа простой нечетной характеристики. На указанных группах определены одули над полем Галуа и дано описание этих одулей. Доказано, что рассмотренные группы относятся к группам с однозначным извлечением корня.

Ключевые слова: конечные нильпотентные группы ступени 2, поле Галуа, одуль.

УДК: 512.544

Abstract. We describe the mentioned groups, assigning values to commutators of the generating elements and defining a group operation on corteges of elements of the Galois field with a prime odd characteristic. On the indicated groups we define odules over the Galois field and describe these odules. We prove that the considered groups are those with unique extraction of root.

Keywords: finite nilpotent groups of the 2nd degree, Galois field, odule.

Конечные p-группы являются нильпотентными. Ниже рассматриваются только группы простого нечетного периода p, ступень нильпотентности которых равна 2. Группы с 2-порожденным коммутантом описаны в [1], [2]. Ниже дан алгоритм описания названных групп с произвольным коммутантом посредством перечисления значений коммутаторов порождающих элементов групп. Кроме того, эти группы заданы операциями на кортежах скаляров из поля Галуа простой нечетной характеристики. Рассмотрены одули над полем Галуа на изучаемых группах, таким образом, имеется описание и этих одулей. Такие одули используются для построения конечных плоскостей [3]. Установлено с использованием одулей, что конечные нильпотентные группы ступени 2 с m порождающими элементами есть группы с однозначным извлечением корня.

Групповая операция записывается аддитивно. Обозначаем группу символом G, ее коммутант — G', центр — $Z(G)$, элементы группы — строчными греческими буквами, нулевой элемент группы — ϑ. Коммутант группы содержится в ее подгруппе Фраттини, поэтому элементы коммутанта являются непорождающими элементами группы. Через $\langle \alpha, \beta, \dots, \eta \rangle$ обозначается подгруппа, порожденная элементами $\alpha, \beta, \dots, \eta$; $\langle \gamma \rangle$ — циклическая подгруппа.

Циклические подгруппы обладают следующими тривиальными свойствами: если $\upsilon \in \langle \omega \rangle$ и $\upsilon \neq \omega, \upsilon \neq \vartheta$, то $\langle \upsilon \rangle = \langle \omega \rangle$; если $\upsilon \notin \langle \omega \rangle$, то $\langle \upsilon \rangle \cap \langle \omega \rangle = \langle \vartheta \rangle$.

Пользуемся тем, что нильпотентная группа имеет нетривиальный центр; в группе ступени 2 коммутант группы лежит в ее центре.

Поступила 19.03.2006

Приведем свойства коммутаторов элементов 2-ступенно нильпотентных групп: $[\sigma+\tau,\rho] = [\sigma,\rho]+[\tau,\rho]$; $[t\sigma, s\rho] = ts[\sigma,\rho]$, t, s — целые числа.

1. Группы с циклическим коммутантом

Группу, порожденную m элементами, обозначаем $\mathbf{G}^m$, а ее коммутант — $\mathbf{G}'^m$. Если $\mathbf{G}^2 = \langle\alpha,\beta\rangle$, то $[\beta,\alpha] \neq \vartheta$. Пусть $[\beta,\alpha] = \tau$, элемент τ является непорождающим для $\mathbf{G}^2$. Всякий элемент ρ группы $\mathbf{G}^2$ записывается в виде $\rho = \alpha^x\beta^y\tau^z$, где числа x, y, z принимают значения от 0 до $p-1$. Порядок группы $\mathbf{G}^2$ равен p^3, $\mathbf{G}'^2 = Z(\mathbf{G}^2) = \langle\tau\rangle$. Группа $\mathbf{G}^2$ единственная 2-порожденная.

Лемма 1. *В группе $\mathbf{G}^3$ существует такое множество порождающих элементов $\{\alpha,\beta,\gamma\}$, что $[\alpha,\beta]\neq\vartheta$, $[\gamma,\alpha] = [\gamma,\beta] = \vartheta$.*

Доказательство. Пусть $\alpha,\beta\in\mathbf{G}^3$, $[\beta,\alpha] = \tau$, $\mathbf{G}'^3 = \langle\tau\rangle$. В $\mathbf{G}^3$ имеем подгруппу $\mathbf{G}^2 = \langle\alpha,\beta\rangle$. Пусть далее $\delta\in\mathbf{G}^3$ и $\delta\notin\mathbf{G}^2$. Обозначим $[\alpha,\delta] = t\tau$, $[\beta,\delta] = s\tau$. Для элемента $\gamma = \delta - s\alpha - t\beta$ имеем $[\alpha,\gamma] = [\beta,\gamma] = \vartheta$. Таким образом, группа $\mathbf{G}^3$ есть прямая сумма своих подгрупп: $\mathbf{G}^3 = \mathbf{G}^2\oplus\langle\gamma\rangle$. Множество порождающих элементов $\{\alpha,\beta,\gamma\}$ группы $\mathbf{G}^3$ обладает указанными свойствами. □

Теперь легко устанавливается

Теорема 1 ([1])**.** *Группа $\mathbf{G}$ с циклическим коммутантом разлагается в прямую сумму*

$$\mathbf{G} = \mathbf{G}_r \oplus \mathbf{L}^n,$$

где $\mathbf{L}^n$ — элементарная абелева группа с n порождающими, подгруппа $\mathbf{G}_r$ является прямой суммой объединенной подгруппы r слагаемых и групп с двумя порождающими элементами, объединенная подгруппа которых есть коммутант группы $\mathbf{G}$.

Число порождающих элементов группы $\mathbf{G}$ равно $2r+n$, порядок группы $\mathbf{G}$ равен p^{2r+1+n}.
На основании леммы 1 справедлива

Лемма 2 ([1])**.** *Группа $\mathbf{G}$, порожденная не менее чем четырьмя элементами, обладает множеством таких порождающих $\{\alpha_1,\alpha_2,\ldots,\alpha_m\}$, что*

$$[\alpha_2,\alpha_1] = [\alpha_4,\alpha_3] = \cdots = [\alpha_k,\alpha_{k-1}] \neq \vartheta, \quad k\leq m,$$

остальные $[\alpha_i,\alpha_j]$ равны ϑ.

На этих известных утверждениях основаны дальнейшие исследования.

2. Группы с нециклическим коммутантом

2.1.*Связи элементов.* Коммутант всякой из рассматриваемых в данном разделе групп является элементарной абелевой группой. Считаем, что группа порождается m элементами $\alpha_1,\alpha_2,\ldots,\alpha_m$, $m\geq 3$; множество порождающих элементов группы обозначаем $\mathbf{A}$; коммутант группы порождается r элементами $\tau_1,\tau_2,\ldots,\tau_r$ и $\mathbf{T}$ есть множество порождающих элементов коммутанта. Выполняется условие $2\leq r\leq\frac{m(m-1)}{2}$. Порядок группы равен p^{m+r}.

Два элемента α,β группы называются *связанными*, если $[\alpha,\beta]\neq\vartheta$. Элементы $\alpha,\beta,\ldots,\sigma$ называются 1-*связанными,* если они связаны (среди их коммутаторов есть ненулевые) и коммутант группы $\langle\alpha,\beta,\ldots,\sigma\rangle$ циклический. Указанные элементы называются k-*связанными*, если коммутант группы $\langle\alpha,\beta,\ldots,\sigma\rangle$ имеет порядок p^k. Для определенности считаем, что элементы множества $\mathbf{A}$ занумерованы так, что сначала выписаны элементы, имеющие наибольшее количество связей. Согласно лемме 2 порождающие элементы группы с циклическим коммутантом 1-связаны.

2.2. *Выделение порождающего в коммутанте.* Сначала выявим ограничение на значения коммутаторов $[\alpha_k, \alpha_i]$, если индекс k фиксирован.

Лемма 3. *В группе* $\mathbf{G}$ *существует такое множество* $\mathbf{A}$ *порождающих элементов, что если* $[\alpha_k, \alpha_l] = \tau_1 \neq \vartheta$, k, l — *фиксированные индексы, то все остальные коммутаторы* $[\alpha_k, \alpha_i], i \neq k, i \neq l$, *лежат в подгруппе* $\langle \tau_2, \ldots, \tau_r \rangle$.

Доказательство. Пусть $[\alpha_1, \alpha_2] = \tau_1$, $[\alpha_1, \alpha_3] = t\tau_1 + \sigma_{13}$, $\sigma_{13} \in \langle \tau_2, \ldots, \tau_r \rangle$. Для элемента $\alpha_3' = \alpha_3 - t\alpha_2$ имеем $[\alpha_1, \alpha_3 - t\alpha_2] = [\alpha_1, \alpha_3] - t[\alpha_1, \alpha_2] = \sigma_{13}$. Порождающий α_3 группы $\mathbf{G}$ можно заменить порождающим α_3', $\mathbf{G} = \langle \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m \rangle = \langle \alpha_1, \alpha_2, \alpha_3', \ldots, \alpha_m \rangle$. Если для каких-то $i > 1$ $[\alpha_1, \alpha_i] = t_i\tau_1 + \sigma_{1i}$, то, заменив α_i на $\alpha_i' = \alpha_i - t\alpha_2$, имеем $[\alpha_1, \alpha_i] = \sigma_{1i} \in \langle \tau_2, \ldots, \tau_r \rangle$; при этом порождающий α_i заменяется на порождающий α_i'. Приведенные рассуждения повторяются, если вместо α_1 рассматривается α_k. ☐

Подгруппу коммутанта, порожденную всеми τ_i, кроме τ_1, обозначаем $\mathbf{G}_1'$. Такой же смысл имеют обозначения $\mathbf{G}_2'$, $\mathbf{G}_{12}'$ и т. д.

Коммутант фактор-группы $\mathbf{G}/\mathbf{G}_1'$ является циклическим. Пусть $\alpha_i + \mathbf{G}_1'$ и $\alpha_j + \mathbf{G}_1'$ — два смежных класса $\mathbf{G}$ по $\mathbf{G}_1'$. Выполняется равенство $[\alpha_i + \mathbf{G}_1', \alpha_j + \mathbf{G}_1'] = [\alpha_i, \alpha_j] + \mathbf{G}_1'$.

Лемма 4. *В группе* $\mathbf{G}$ *существует множество таких порождающих* $\mathbf{A}$, *что для них имеется* 1*-связь, состоящая из коммутаторов вида* $(\tau_1 + \mathbf{G}_1')$: $[\alpha_2, \alpha_1] = \tau_1$, *коммутаторы* $[\alpha_2, \alpha_1] + \mathbf{G}_1' = [\alpha_4, \alpha_3] + \mathbf{G}_1' = \cdots = [\alpha_k, \alpha_{k-1}] + \mathbf{G}_1'$ *принадлежат смежному классу* $\tau_1 + \mathbf{G}_1'$, $k \leq m$; *остальные* $[\alpha_i, \alpha_j] + \mathbf{G}_1'$ *принадлежат* $\mathbf{G}_1'$.

Утверждение выполняется на основе лемм 3 и 2.

По лемме 4 возможно $[\alpha_4, \alpha_3] + \mathbf{G}_1' = t\tau_1 + \mathbf{G}_1'$, $t \not\equiv 1 \pmod p$. Лемма 2 выделяет один порождающий элемент коммутанта группы; если выделен, например, α_1 и $[\alpha_2, \alpha_1] = \tau_1$, то при $r > 1$ выделяется порождающий элемент коммутанта группы τ_1, для которого выполняется лемма 2, для всех остальных порождающих элементов коммутанта выполняется лемма 4. Добиваясь равенства коммутаторов из $\langle \tau_2 \rangle$, теряем равенство коммутаторов из $\langle \tau_1 \rangle$ в 2-связи, состоящей из коммутаторов из $\langle \tau_1, \tau_2 \rangle$.

2.3. *Свойства коммутаторов.* Пусть $m > 4$ и $r \geq 2$. Упорядочиваем элементы α_i и последовательно выделяем порождающие элементы коммутанта группы. Пусть α_1, α_2, α_3 таковы, что $[\alpha_2, \alpha_1] \neq \vartheta$ и $[\alpha_2, \alpha_3] \neq \vartheta$. Обозначим $[\alpha_2, \alpha_1] = \tau_1$. Согласно лемме 3 элемент α_3 можно выбрать так, что $[\alpha_2, \alpha_3] \notin \langle \tau_1 \rangle$. Обозначим $[\alpha_2, \alpha_3] = \tau_2$. Рассматриваем фактор-группу $\mathbf{G}/\mathbf{G}_1'$; для нее выполняется лемма 2. Сначала выбираем порождающие $\alpha_4, \alpha_5, \ldots$, чтобы согласно лемме 2 порождающие $\alpha_1 + \mathbf{G}', \alpha_2 + \mathbf{G}', \ldots$ фактор-группы удовлетворяли соотношениям

$$[\alpha_2, \alpha_1] + \mathbf{G}_1' = [\alpha_4, \alpha_3] + \mathbf{G}_1' = \cdots = [\alpha_k, \alpha_{k-1}] + \mathbf{G}_1' = \tau_1 + \mathbf{G}_1', \quad k \leq m;$$

остальные коммутаторы $[\alpha_i, \alpha_j] + \mathbf{G}_1'$ лежат в $\mathbf{G}_1'$. Потом выбираем порождающие группы $\mathbf{G}$, чтобы в фактор-группе $\mathbf{G}/\mathbf{G}_1'$ соответствующие коммутаторы $[\alpha_i, \alpha_j] + \mathbf{G}_1'$ были отличны от нулевого, так как множество порождающих $\alpha_1 + \mathbf{G}'$ фактор-группы $\mathbf{G}/\mathbf{G}_1'$ 1-связано. Для порождающих элементов группы $\mathbf{G}$ выполняются соотношения

$$[\alpha_2, \alpha_1] = [\alpha_4, \alpha_3] = \cdots = [\alpha_k, \alpha_{k-1}] = \tau_1,$$

остальные коммутаторы $[\alpha_i, \alpha_j]$ лежат в подгруппе $\mathbf{G}_1'$.

Лемма 5. *Группа* $\mathbf{G}$, *в коммутанте которой имеется* $r \geq 2$ *порождающих, обладает множеством порождающих* $\mathbf{A}$, *для которых в фактор-группе* $\mathbf{G}/\mathbf{G}_{12}'$ *осуществляется* 2*-связь*

$$[\alpha_2, \alpha_1] + \mathbf{G}_{12}' = [\alpha_4, \alpha_3] + \mathbf{G}_{12}' = \cdots = \tau_1 + \mathbf{G}_{12}',$$

$$[\alpha_3,\alpha_2]+\mathbf{G}'_{12}=\tau_2+\mathbf{G}'_{12},\quad [\alpha_5,\alpha_4]+\mathbf{G}'_{12}=a_{44}\tau_2+\mathbf{G}'_{12},\ldots,$$

остальные коммутаторы $[\alpha_i,\alpha_j]+\mathbf{G}'_{12}$ *равны* $\mathbf{G}'_{12}$.

Доказательство. Если $[\alpha_3,\alpha_2]+\mathbf{G}'_1=\mathbf{G}'$, то $[\alpha_3,\alpha_2]+\mathbf{G}'_{12}=\sigma+\mathbf{G}'_{12}$. Ясно, что $\langle\tau_1\rangle\cap\langle\sigma\rangle=\langle\vartheta\rangle$ и $\langle\tau_1,\sigma\rangle$ имеет порядок p^2, $\langle\tau_1,\sigma\rangle+\mathbf{G}'_{12}$ есть коммутант $\mathbf{G}/\mathbf{G}'_{12}$. Пусть $\sigma=\tau_2$ — второй порождающий коммутанта группы. Если $[\alpha_5,\alpha_4]+\mathbf{G}'_{12}=\rho+\mathbf{G}'_{12}$, то возможно $\rho=s\tau_1+a^2_{45}\tau_2+\mathbf{G}'_{12}$. Но $[\alpha_5,\alpha_4]+\mathbf{G}'_1=\mathbf{G}'_1$, поэтому $s=0$. Значит, $[\alpha_5,\alpha_4]+\mathbf{G}'_{12}=a^2_{45}\tau_2+\mathbf{G}'_{12}$ и т. д. В фактор-группе $\mathbf{G}/\mathbf{G}'_{12}$ существует указанная 2-связь. □

При $r=2$ выполняется

Теорема 2. *Если порядок коммутанта группы* $\mathbf{G}^m$ *равен* p^2, *то в группе* $\mathbf{G}^m$ *имеется множество* $\mathbf{A}$ *порождающих элементов, находящихся в* 2*-связи*

$$[\alpha_2,\alpha_1]=[\alpha_4,\alpha_3]=\ldots=[\alpha_k,\alpha_{k-1}]=\tau_1,$$
$$[\alpha_3,\alpha_2]=\tau_2,\quad [\alpha_5,\alpha_4]=a^2_{45}\tau_2,\ldots,[\alpha_{k+1},\alpha_k]=a^2_{k,k+1}\tau_2,$$

где k *четное,* $k+1<m$; *остальные коммутаторы* $[\alpha_i,\alpha_j]$ *равны нулевому элементу группы.*

Далее, пусть $r>2$ и $[\alpha_3,\alpha_1]\neq\vartheta$. Обозначим $[\alpha_3,\alpha_1]=\tau_3$ и строим 3-связь в фактор-группе $\mathbf{G}^m/\mathbf{G}'_{123}$, используя теорему 2, лемму 3 и 2-связь в группе $\mathbf{G}^m$, коммутант которой 2-порожден.

Теорема 3. *Для группы* $\mathbf{G}^m$ *с* r*-порожденным коммутантом существует множество порождающих* $\mathbf{A}$ *и множество* $\mathbf{T}$ *порождающих коммутанта, причем в группе* $\mathbf{G}^m$ *имеется* r*-связь, удовлетворяющая лемме* 3, *и во всякой фактор-группе группы* $\mathbf{G}^m$ *по* $(r-2)$*-порожденной подгруппе коммутанта имеется* 2*-связь, описанная с точностью до нумерации порождающих элементов в теореме* 2.

Доказательство. Рассматриваем группу $\mathbf{G}^m$ с r-порожденным коммутатором. Считаем, что в группах $\mathbf{G}^m$ с $(r-1)$-порожденными коммутантами $(r-1)$-связь уже построена, в качестве значений коммутаторов порождающих элементов группы использованы порождающие коммутанта $\tau_1,\tau_2,\ldots,\tau_{r-1}$. Фактор-группа $\mathbf{G}^m/\langle\tau_r\rangle$ порождается m элементами $\alpha_i+\langle\tau_r\rangle$, $i=\overline{1,m}$, ее коммутант порождается $r-1$ элементами. По предположению $(r-1)$-связь в фактор-группе $\mathbf{G}^m/\langle\tau_r\rangle$ построена. На основании леммы 3 и рассуждений, аналогичных доказательству леммы 5, получаем r-связь в группе $\mathbf{G}^m$ с r-порожденным коммутантом. □

2.4. *Описание групп посредством задания значений коммутаторов порождающих элементов.* Установленные свойства коммутаторов порождающих элементов группы сформулируем в виде следующих принципов, которые положим в основу описания рассматриваемых групп.

Принцип 1. Для всякого фиксированного α_i и всех α_j, $i\neq j$, из множества $\mathbf{A}$ порождающих элементов группы все ненулевые коммутаторы $[\alpha_i,\alpha_j]$ лежат в разных циклических подгруппах $\langle\tau_l\rangle$ коммутанта, порожденных элементами из $\mathbf{T}$.

Принцип 2. На множестве $\mathbf{A}\times\mathbf{A}$ пар порождающих элементов группы определено отношение эквивалентности: пары (α_i,α_j), (α_k,α_l) эквивалентны, если и только если коммутаторы $[\alpha_i,\alpha_j],[\alpha_k,\alpha_l]$ лежат в одной циклической подгруппе $\langle\tau_s\rangle$ коммутанта; для любых двух пар одного класса все четыре порождающих различны. Пары порождающих (α_i,α_j), (α_k,α_l), для которых $[\alpha_i,\alpha_j]=\tau_g,[\alpha_k,\alpha_l]=\tau_s$ и $\tau_s\notin\langle\tau_g\rangle$, лежат в разных классах. Считаем, что пары (α_i,α_i) и (α_i,α_j), для которых $[\alpha_i,\alpha_j]=\vartheta$, принадлежат одному классу.

Множество пар $\mathbf{A} \times \mathbf{A} = \mathbf{A}^2$ распадается на не менее чем два класса эквивалентности. Такое разбиение происходит в группах с циклическим коммутантом. В них имеется 1-связь порождающих элементов группы. Один класс эквивалентности состоит из пар связанных элементов, другой — из всех остальных пар. Если $m \geq 3$, то для всех r, $1 \leq r \leq \frac{(m-1)m}{2}$, имеется $r+1$ классов эквивалентности.

Описываем группы с m порождающими элементами и имеющими r порождающих в коммутанте в следующем порядке. Сначала рассматривается случай $r = 1$. Перебираются все возможные разбиения пар из $\mathbf{A}^2$ на два класса эквивалентности. Затем при $r = 2$ производятся все разбиения пар из $\mathbf{A}^2$ на три класса. И так далее, вплоть до $r = \frac{(m-1)m}{2}$. При разбиении пар из $\mathbf{A}^2$ руководствуемся принципами 1 и 2. По каждому разбиению пар порождающих элементов выписываем значения коммутаторов порождающих. Тем самым получаем генетический код группы, содержащий перечисление порождающих элементов и значения их коммутаторов.

2.5. *Пример описания групп.* Пусть $m = 4$. Возможны значения r: $1, 2, \ldots, 6$. Имеем $\mathbf{A} = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$. Множества порождающих коммутанта таковы: $\mathbf{T} = \{\tau_1\}$, $\mathbf{T} = \{\tau_1, \tau_2\}, \ldots$, $\mathbf{T} = \{\tau_1, \tau_2, \ldots, \tau_6\}$. Наряду с множеством $\mathbf{A}$ рассматриваем множество $\mathbf{I} = \{1, 2, 3, 4\}$ индексов его элементов. Достаточно рассмотреть множество пар индексов с точностью до порядка

$$\mathbf{I} \cdot \mathbf{I} = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}.$$

Пары совпадающих индексов исключаем.

Разбиваем множество пар $\mathbf{I} \cdot \mathbf{I}$ на классы в соответствии с принципами 1 и 2 при каждом значении r. Класс k_0 состоит из пар индексов несвязанных элементов. Приведем всевозможные разбиения множества $\mathbf{I} \cdot \mathbf{I}$ на классы, перебирая значения r от 1 до 6. Классы эквивалентности обозначаем $k_1, k_2, \ldots, k_6$; каждому такому классу разбиения соответствует порождающий коммутанта группы.

$r = 1$

1) k_1 $(1,2)$;
k_0 $(1,3), (1,4), (2,3), (2,4), (3,4)$.

2) k_1 $(1,2), (3,4)$;
k_0 $(1,3), (1,4), (2,3), (2,4)$.

$r = 2$

3) k_1 $(1,2)$;
k_2 $(3,4)$;
k_0 $(1,3), (1,4), (2,3), (2,4)$.

4) k_1 $(1,2)$;
k_2 $(2,3)$;
k_0 $(1,3), (1,4), (2,4), (3,4)$.

5) k_1 $(1,2), (3,4)$;
k_2 $(2,3)$;
k_0 $(1,3), (1,4), (2,4)$.

6) k_1 $(1,2), (3,4)$;
k_2 $(2,3), (1,4)$;
k_0 $(1,3), (2,4)$.

$r = 3$

7) k_1 $(1,2)$;
k_2 $(1,4)$;
k_3 $(1,3)$;
k_0 $(2,3), (2,4), (3,4)$.

8) k_1 $(1,2), (3,4)$;
k_2 $(1,4)$;
k_3 $(1,3)$;
k_0 $(2,3), (2,4)$.

9) k_1 $(1,2),(3,4)$;
k_2 $(1,4),(2,3)$;
k_3 $(1,3)$;
k_0 $(2,4)$.

10) k_1 $(1,2),(3,4)$;
k_2 $(1,4),(2,3)$;
k_3 $(1,3),(2,4)$;
k_0 $\emptyset$.

$r=4$

11) k_1 $(1,2)$;
k_2 $(1,4)$;
k_3 $(1,3)$;
k_4 $(3,4)$;
k_0 $(2,3),(2,4)$.

12) k_1 $(1,2)$;
k_2 $(1,4),(2,3)$;
k_3 $(1,3)$;
k_4 $(3,4)$;
k_0 $(2,4)$.

13) k_1 $(1,2)$;
k_3 $(1,3),(2,4)$;
k_0 $(2,4)$.
k_2 $(1,4),(2,3)$;
k_3 $(3,4)$;

$r=5$

14) k_1 $(1,2)$;
k_2 $(1,4)$;
k_3 $(1,3)$;
k_4 $(3,4)$;
k_5 $(2,3)$;
k_0 $(2,4)$.

15) k_1 $(1,2)$;
k_2 $(1,4)$;
k_3 $(1,3),(2,4)$;
k_4 $(3,4)$;
k_5 $(2,3)$;
k_0 $\emptyset$.

$r=6$

16) k_1 $(1,2)$;
k_3 $(1,3)$;
k_5 $(2,3)$;
k_0 $\emptyset$.
k_2 $(1,4)$;
k_4 $(3,4)$;
k_6 $(2,4)$.

По классам пар индексов записываем значения коммутаторов порождающих элементов группы. Пару индексов (i,j) из класса k_s, $s\neq 0$, заменяем коммутатором $[\alpha_j,\alpha_i]=\tau_s$; пару индексов (i,j) из класса k_0 заменяем коммутатором $[\alpha_j,\alpha_i]=\vartheta$. Каждому случаю разбиения соответствует группа рассматриваемого вида, возможно не одна, разным разбиениям соответствуют неизоморфные группы.

$r=1$, $|\mathbf{G}|=p^5$, $\mathbf{G}'=\langle\tau_1\rangle$. Через $|\mathbf{G}|$ обозначен порядок группы $\mathbf{G}$.

1. Класс k_1 содержит одну пару $(1,2)$, значит, только один коммутатор порождающих элементов группы $[\alpha_2,\alpha_1]$ отличен от нулевого. Генетический код группы $\mathbf{G}=\{\alpha_i\mid[\alpha_2,\alpha_1]\neq\vartheta,\ i=\overline{1,4}\}$; выписан только ненулевой коммутатор порождающих;

$$\mathbf{G}=\langle\alpha_1,\alpha_2\rangle\oplus\langle\alpha_3,\alpha_4\rangle,\quad Z(\mathbf{G})=\langle\alpha_3,\alpha_4,\tau_1\rangle,\tau_1=[\alpha_2,\alpha_1].$$

2. Согласно классу k_1 : $[\alpha_2,\alpha_1]=[\alpha_4,\alpha_3]\neq\vartheta$. Остальные коммутаторы порождающих нулевые, $\mathbf{G}=\{\alpha_i\mid[\alpha_2,\alpha_1]=[\alpha_4,\alpha_3]\neq\vartheta\}$. Имеем прямую сумму подгрупп с объединенным

коммутантом, $\tau_1 = [\alpha_2, \alpha_1]$;

$$\mathbf{G} = \langle \alpha_1, \alpha_2 \rangle \cup \langle \alpha_3, \alpha_4 \rangle, \quad |\mathbf{G}| = p^5, \quad Z(\mathbf{G}) = \langle \tau_1 \rangle.$$

$r = 2$, $|\mathbf{G}| = p^6$, $\mathbf{G}' = \langle \tau_1, \tau_2 \rangle$.

3. По классу $k_1 : [\alpha_2, \alpha_1] = \tau_1$, по классу $k_2 : [\alpha_4, \alpha_3] = \tau_2$. Остальные коммутаторы порождающих элементов равны нулю;

$$\mathbf{G} = \langle \alpha_1, \alpha_2 \rangle \oplus \langle \alpha_3, \alpha_4 \rangle, \quad Z(\mathbf{G}) = \langle \tau_1, \tau_2 \rangle, \quad Z(\mathbf{G}) = \mathbf{G}'.$$

4. $[\alpha_2, \alpha_1] = \tau_1, [\alpha_3, \alpha_2] = \tau_2$;

$$\mathbf{G} = \langle \alpha_1, \alpha_2, \alpha_3 \rangle \oplus \langle \alpha_4 \rangle, \quad Z(\mathbf{G}) = \langle \alpha_4, \tau_1, \tau_2 \rangle.$$

5. $[\alpha_2, \alpha_1] = [\alpha_4, \alpha_3] = \tau_1$, $[\alpha_3, \alpha_2] = \tau_2$; $Z(\mathbf{G}) = \mathbf{G}'$.

6. Разбиению пар индексов соответствует два вида групп. Вопрос об изоморфизме групп рассмотрен ниже в п. 3.2. Имеем

$\mathbf{G_1}$. $[\alpha_2, \alpha_1] = [\alpha_4, \alpha_3] = \tau_1$, $[\alpha_3, \alpha_2] = [\alpha_4, \alpha_1] = \tau_2$.

$\mathbf{G_2}$. $[\alpha_2, \alpha_1] = [\alpha_4, \alpha_3] = \tau_1$, $[\alpha_3, \alpha_2] = \tau_2, [\alpha_4, \alpha_1] = a_{14}^2 \tau_2$, $a_{14}^2 \in GF(p) = \mathbf{P}$, $a_{14}^2 \not\equiv 0$ и $a_{14}^2 \not\equiv 1$.

$r = 3$, $|\mathbf{G}| = p^7$, $|\mathbf{G}'| = p^3$, $Z(\mathbf{G}) = \mathbf{G}'$.

7, 8. Значения коммутаторов порождающих записываются однозначно.

9. Имеется два вида групп по аналогии с разбиением 6.

10. $[\alpha_2, \alpha_1] = [\alpha_4, \alpha_3] = \tau_1$; $[\alpha_4, \alpha_1] = \tau_2$, $[\alpha_3, \alpha_2] = a\tau_2$, $[\alpha_3, \alpha_1] = \tau_3$, $[\alpha_4, \alpha_2] = b\tau_3$; $a, b \in \mathbf{P}$, $a \not\equiv 0$ и $b \not\equiv 0$. Имеются неизоморфные группы в случаях

(i) $a = b \equiv 1$; (ii) $a \equiv 1$, $b \not\equiv 1$; (iii) $a \not\equiv 1$, $b \not\equiv 1$.

$r = 4$, $|\mathbf{G}| = p^8$, $|\mathbf{G}'| = p^4$, $Z(\mathbf{G}) = \mathbf{G}'$.

11, 12. Определяется по одной группе.

13. Определяются два вида групп по аналогии с разбиением 6.

$r = 5, 6$, $|\mathbf{G}| = p^9$, $|\mathbf{G}'| = p^5$ или $|\mathbf{G}| = p^{10}$, $|\mathbf{G}'| = p^6$; $Z(\mathbf{G}) = \mathbf{G}'$.

14–16. Определяется по одной группе.

Аналогично перебираются группы с другим числом порождающих элементов.

3. Группы на множестве кортежей скаляров

Как и выше, рассматриваются конечные нильпотентные ступени 2 группы простого нечетного периода.

3.1. *Задание группы на множестве кортежей.* Рассматриваем множество кортежей $\mathbf{P}^n$ скаляров из поля Галуа $GF(p) = \mathbf{P}$. Длина кортежей равна $n = m + r$. Группе $\mathbf{G}^m$ с коммутантом порядка p^r сопоставим множество $\mathbf{P}^{m+r}$. Элементу $\gamma = \alpha_1^{x^1} \alpha_2^{x^2} \ldots \alpha_m^{x^m} \tau_1^{u^1} \ldots \tau_r^{u^r}$; $x^i, u^l \in \mathbf{P}$, $i = \overline{1, m}$, $l = \overline{1, r}$, группы $\mathbf{G}^m$ поставим в соответствие кортеж из $\mathbf{P}^{m+r}$ $\sigma = (x^1, x^2, \ldots, x^m, u^1, \ldots, u^r) = (x^i, u^l)$. Кортежи (x^i, u^l) и (y^i, v^l) равны, если $x^i \equiv y^i \pmod m$ и $u^l \equiv v^l \pmod m$. Далее все сравнения рассматриваются по $(\operatorname{mod} m)$. Соответствие между элементами группы $\mathbf{G}^m$ и кортежами из $\mathbf{P}^{m+r}$ взаимно однозначное.

Для примера возьмем $m = 4$, $r = 3$ и группы, определяемые разбиением 10 из п. 2.5. Пусть $\rho = (y^i, v^l)$ — еще один кортеж из $\mathbf{P}^7$. На множестве кортежей зададим операцию сложения

$$\sigma + \rho = (x^i, u^l) + (y^i, v^l) = (x^i + y^i, u^1 + v^1 + x^2 y^1 + x^4 y^3,$$
$$u^2 + v^2 + x^3 y^2 + a x^4 y^1, u^3 + v^3 + x^3 y^1 + b x^4 y^2). \quad (1)$$

Операция определена в соответствии с разбиением 10. Для группы $\mathbf{P}_1^7$: $a = b \equiv 1$, для группы $\mathbf{P}_2^7$: $a = a_{23}^2$, $b = a_{24}^3$ — элементы из $\mathbf{P}$, не сравнимые с 0 и 1. Суммирование в компонентах кортежей производится по $\bmod p$. Нулевой кортеж обозначим $(0, 0, \dots, 0) = \vartheta$. Проверка по равенству (1) дает $\sigma + \vartheta = \sigma$. Противоположным для σ является

$$-\sigma = (-x^i, -u^1 + x^2x^1 + x^4x^2, -u^2 + x^2x^3 + ax^1x^3, -u^3 + x^3x^1 + bx^4x^2). \qquad (2)$$

Каждый элемент x из поля $\mathbf{P}$ имеет в поле $\mathbf{P}$ противоположный, обозначаемый $-x$. Вычисляем по (1) $\sigma + (-\sigma) = \vartheta$. Кроме того, операция (1) удовлетворяет условию $(\sigma + \rho) + \eta = \sigma + (\rho + \eta)$. Таким образом, $(\mathbf{P}^7, +)$ есть группа.

Обозначим через $\overline{\alpha_i}$ кортеж, все компоненты которого из первых m, кроме i-й, равны нулю, а i-я равна единице; последние r компонент равны нулю. Через $\overline{\tau}_l$ обозначим кортеж, все компоненты которого, кроме $(m+l)$-й, равны нулю, а $(m+l)$-я компонента равна единице. Вычисления на основе (1) и (2) дают

$$[\overline{\alpha_2}, \overline{\alpha_1}] = [\overline{\alpha_4}, \overline{\alpha_3}] = \overline{\tau_1}, \quad [\overline{\alpha_3}, \overline{\alpha_2}] = \overline{\tau_2}, \quad [\overline{\alpha_4}, \overline{\alpha_1}] = a\overline{\tau_2}, \quad [\overline{\alpha_3}, \overline{\alpha_1}] = \overline{\tau_3}, \quad [\overline{\alpha_4}, \overline{\alpha_2}] = b\overline{\tau_3}.$$

Следовательно, группы $\mathbf{G}^4$, соответствующие разбиению 10 из п. 2.5, изоморфны группам $(\mathbf{P}^7, +)$ при соответствующих значениях параметров a, b в операции сложения (1).

Аналогично на кортежах из $\mathbf{P}^{m+r}$ при заданных m и r определяется операция сложения по разбиению пар индексов порождающих элементов множества $\mathbf{A}$ группы $\mathbf{G}^m$, составленному по принципам 1 и 2 из п. 2.4.

3.2. *Об изоморфных и неизоморфных группах.* Сначала зададим две группы на множестве кортежей $\mathbf{P}^3$. Операция сложения на группе $\mathbf{G}_1$:

$$(x^1, x^2, u) + (y^1, y^2, v) = (x^1 + y^1, x^2 + y^2, u + v + x^2y^1); \qquad (3)$$

операция сложения на группе $\mathbf{G}_2$:

$$(x^1, x^2, u) + (y^1, y^2, v) = (x^1 + y^1, x^2 + y^2, u + v + ax^2y^1); \quad a \not\equiv 0, \quad a \not\equiv 1. \qquad (4)$$

Определим соответствие $\varphi : \mathbf{G}_1 \leftrightarrow \mathbf{G}_2$. Элементу $\sigma_1 \in \mathbf{G}_1$ поставим в соответствие элемент $\sigma_2 \in \mathbf{G}_2$, где $\sigma_1 = (x^1, x^2, u)$, $\sigma_2 = (\overline{a}x^1, x^2, u)$, $a\overline{a} \equiv 1$. Соответствие φ взаимно однозначно. Если $x^1 \neq 0$, то и $\overline{a}x^1 \neq 0$. Для $\rho_1 = (y^1, y^2, v)$ и $\rho_2 = (\overline{a}y^1, y^2, v)$ в отображении φ имеем $\sigma_1 + \rho_1 \leftrightarrow \sigma_2 + \rho_2$. Действительно, по (4) $\sigma_2 + \rho_2 = (\overline{a}(x^1 + y^1), x^2 + y^2, u + v + ax^2y^1)$ и в отображении φ элементу $\sigma_1 + \rho_1$ из $\mathbf{G}_1$ с первой компонентой $x^1 + y^1$ соответствует элемент $\sigma_2 + \rho_2$ из $\mathbf{G}_2$ с первой компонентой $\overline{a}(x^1 + y^1)$; вторые и третьи компоненты у $\sigma_1 + \rho_1$ и $\sigma_2 + \rho_2$ одинаковы. Соответствие φ является изоморфизмом.

Полученный результат означает следующее. Если группа $\mathbf{G}^m$, $m \geq 4$, $|\mathbf{G}'^m| = p$, имеет подгруппы $\mathbf{G}_1 = \langle \alpha_1, \alpha_2 \rangle$ и $\mathbf{G}_2 = \langle \alpha_3, \alpha_4 \rangle, [\alpha_2, \alpha_1] \neq \vartheta$, $[\alpha_2, \alpha_1] \neq \vartheta$, то $\mathbf{G}^m$ обладает множеством порождающих элементов $\alpha_1, \alpha_2, \dots, \alpha_m$ со свойствами $[\alpha_2, \alpha_1] = [\alpha_2, \alpha_1] \neq \vartheta$ и остальные коммутаторы элементов α_1, α_2, α_3, α_4 равны нулю. Это часть 1-связи в $\mathbf{G}^m$ (см. лемму 2). Опираясь на лемму 1, можно построить в $\mathbf{G}^m$ 1-связь со всеми связанными элементами.

Теперь на множестве $\mathbf{P}^7$ зададим две группы, $m = 5, r = 2$. Операция сложения на группе $\mathbf{G}_3$:

$$(x^i, u^l) + (y^i, v^l) = (x^i + y^i, u^l + v^l + x^2y^1 + x^4y^3, u^2 + v^2 + x^3y^2 + x^5y^4); \qquad (5)$$

операция сложения на группе $\mathbf{G}_4$:

$$(x^i, u^l) + (y^i, v^l) = (x^i + y^i, u^l + v^l + x^2y^1 + x^4y^3, u^2 + v^2 + x^3y^2 + ax^5y^4); \qquad (6)$$

$i = \overline{1, 5}$, $l = 1, 2$; $a \not\equiv 1$, $a \not\equiv 0$. По аналогии с рассмотренным выше соответствием φ установим соответствие $\psi : \mathbf{G}_3 \leftrightarrow \mathbf{G}_4$; элементу $\sigma_1 \in \mathbf{G}_3$ соответствует элемент $\sigma_2 \in \mathbf{G}_4$, где $\sigma_1 = (x^i, u^l)$, $\sigma_2 = (x^1, x^2, x^3, \overline{a}x^4, x^5, u^1, u^2)$, $a\overline{a} \equiv 1$. Соответствие ψ взаимно однозначно. Возьмем еще по элементу в каждой группе: $\rho_1 = (y^i, v^l)$, $\rho_2 = (y^1, y^2, y^3, \overline{a}y^4, y^5, v^1, v^2)$. По (6) находим

$$\sigma_2 + \rho_2 = (x^1 + y^1, x^2 + y^2, x^3 + y^3, \overline{a}(x^4 + y^4), x^5 + y^5, \\ u^1 + v^1 + x^2y^1 + \overline{a}x^4y^3, u^2 + v^2 + x^3y^2 + a\overline{a}x^5y^4),$$

сумма $\sigma_1 + \rho_1$ задана равенством (5). Если $x^3 = y^3 = 0$, то суммы $\sigma_1 + \rho_1$ и $\sigma_2 + \rho_2$ соответственны в ψ. Если компоненты x^3 и y^3 ненулевые, то суммы $\sigma_1 + \rho_1$ и $\sigma_2 + \rho_2$ не соответственны в ψ. Поэтому ψ не является изоморфизмом групп $\mathbf{G}_3$ и $\mathbf{G}_4$, и группы $\mathbf{G}_3, \mathbf{G}_4$ не изоморфны.

Если $m > 5$, $r \geq 2$, то в группах $\mathbf{G}^m$ с разными значениями a^l_{ij} для коммутаторов $[\alpha_i, \alpha_j] = a^l_{ij}\tau_l$ можно выделить подгруппы с нециклическими коммутантами, в число порождающих которых входят α_i и α_j. Между подгруппами не существует изоморфного соответствия, а значит, и между группами, содержащими указанные подгруппы, нет изоморфизма.

Неизоморфизм групп с разными значениями a^l_{ij} заложен в свойствах 2-связи (см. лемму 5). По лемме 2 в группе существует такое множество порождающих $\mathbf{A}$, что ненулевые коммутаторы порождающих элементов группы из 1-связи равны между собой. Таким же свойством обладает 2-связь: ненулевые коммутаторы из подгруппы $\langle\tau_1\rangle$ равны между собой (см. лемму 5). Если $[\alpha_5, \alpha_4] + \mathbf{G}'_{12} = a^2_{45}\tau_2 + \mathbf{G}'_{12}$, $a^2_{45} \not\equiv 1$, $a^2_{45} \not\equiv 0$, то, заменив порождающий α_4 на порождающий $\alpha'_4 = \overline{a^2_{45}}\alpha$, получаем $[\alpha_5, \alpha'_4] + \mathbf{G}'_{12} = \tau_2 + \mathbf{G}'_{12}$, но тогда $[\alpha'_4, \alpha_3] + \mathbf{G}'_{12} = \overline{a^2_{45}}\tau_2 + \mathbf{G}'_{12}$; нарушается равенство коммутаторов порождающих элементов группы из $\langle\tau_1\rangle + \mathbf{G}'_{12}$.

3.3. *Алгоритм описания рассматриваемых групп.* Согласно вышеизложенному перебрать все нильпотентные группы ступени 2 простого нечетного периода p с $m \geq 2$ порождающими элементами можно следующим образом.

1) Задать m — число порождающих названных групп. Число r порождающих элементов коммутаторов групп с m порождающими изменяется от 1 до $\frac{(m-1)m}{2}$.

2) Выписать множество $\mathbf{I} \cdot \mathbf{I}$ пар индексов с точностью до порядка индексов, пары совпадающих индексов не рассматриваются.

3) Произвести разбиения множества $\mathbf{I} \cdot \mathbf{I}$ на $r + 1$ классов эквивалентности на основе принципов 1 и 2 из п. 2.4. Если в r классах несовпадающих пар из $\mathbf{I} \cdot \mathbf{I}$ использованы не все пары, то оставшиеся пары составляют класс k_0. Этот класс может оказаться и пустым.

4) Для пар (i, j) из классов, начиная со второго, в случае, если класс содержит более одной пары, указать наборы скаляров a^l_{ij} из поля $\mathbf{P}$, $a^l_{ij} \not\equiv 0$, $a^l_{ij} \not\equiv 1$.

5) По каждому из классов эквивалентности пар индексов выписать значения соответствующих коммутаторов порождающих элементов групп, как указано в п. 2.5. Одному классу эквивалентных пар соответствует столько неизоморфных между собой групп, сколько существует наборов скаляров a^l_{ij} (см. п. 4) алгоритма).

Тем самым получаем все возможные из рассматриваемых групп, заданные перечислением значений коммутаторов порождающих элементов групп.

3.4. *Одули над полем Галуа.* Алгебраическая структура одуля над кольцом $\mathbf{K}$, введенная Л.В. Сабининым в 1977 г. [4], обобщает структуру $\mathbf{K}$-модуля и линейного пространства над полем $\mathbf{F}$. Приведем определение $\mathbf{K}$-одуля согласно [4].

Пусть $\Omega = (\Omega, +)$ — структура с внутренней бинарной операцией, ее коммутативности не требуется, операцию называем сложением. На структуре Ω задана внешняя операция $\omega_K(+)$ умножения элементов из Ω на скаляры из ассоциативного кольца $\mathbf{K}$

$$\omega_K(+) : \mathbf{K} \times \Omega \ni (t, v) \to tv \in \Omega.$$

Структура $\Omega = (\Omega, +, \omega_K(+))$ называется **K**-одулем или одулем над кольцом **K**, если для всех $s, t \in \mathbf{K}$, $\upsilon \in \Omega$ выполняются аксиомы

$$s(t\upsilon) = (st)\upsilon, \quad (t+s)\upsilon = t\upsilon + s\upsilon.$$

Частным случаем **K**-одуля является группа Ω^K над кольцом **K** с единицей 1 ([5], с. 104–105), это одуль на группе. Дополнительно к двум приведенным аксиомам одуля выполняются также

$$1\upsilon = \upsilon, (-1)\upsilon = -\upsilon, t(-\eta + \upsilon + \eta) = -\eta + t\upsilon + \eta.$$

Выше в п. 3.1 рассматриваемые группы заданы операциями на множествах кортежей скаляров из поля Галуа $\mathbf{P} = GF(p)$. Для каждой группы $(\mathbf{P}^n, +)$ зададим внешнюю операцию элементов группы на скаляры из $\mathbf{P}$. Пусть, например, операция на $\mathbf{P}^7$ задана равенством (6). Тогда внешняя операция такова:

$$t(x^i, u^l) = \left(x^i t, u^1 t + \frac{(t-1)t}{2}(x^1x^2 + x^3x^4), u^2 t + \frac{(t-1)t}{2}(x^2x^3 + ax^4x^5)\right)$$

для всех $t \in \mathbf{P}$. Вообще, если в $(m+l)$-й компоненте суммы $(x^i, u^l) + (y^i, v^l)$ имеем $u^l + v^l + x^iy^j + a^l_{gh}x^gy^h + \dots + a^l_{nq}x^ny^q$, то в $(m+l)$-й компоненте произведения $t(x^i, u^l)$ пишем

$$u^l t + \frac{(t-1)t}{2}(x^ix^j + a^l_{gh}x^gx^h + \dots + a^l_{nq}x^nx^q).$$

В i-й компоненте произведения пишем $x^i t$. Аксиомы одуля на группе выполняются. Тем самым получены одули $\mathbf{P}^n = (\mathbf{P}^n, +, \omega_P(+))$ над полем Галуа $\mathbf{P}$. Одули на нильпотентных группах называются нильпотентными. Перебирая все группы с m порождающими согласно алгоритму из п. 3.3, получаем и все нильпотентные ступени 2 одули над полем Галуа $\mathbf{P}$, имеющие m порождающих. Имеем описание названных одулей. По этим одулям строятся конечные плоскости [3].

3.5. *Делимость (полнота) групп.* Группа $\mathbf{G}$ называется делимой (полной), если для любого $\eta \in \mathbf{G}$ и любого натурального n существует такое $\sigma \in \mathbf{G}$, что $n\sigma = \eta$ (в мультипликативной записи операции: $\sigma^n = \eta$; тогда σ есть корень n-й степени из η). В ([4], с. 104; [6], с. 165–168) в качестве делимых рассматриваются группы без кручения. Ниже рассматривается делимость конечных групп.

Теорема 4. *Конечные нильпотентные ступени* 2 *группы простого нечетного периода являются делимыми, точнее: в каждой такой группе для всякого* η *и всякого натурального* n *существует единственный элемент* σ, *для которого* $n\sigma = \eta$.

Доказательство. Всякое натуральное число n сравнимо с некоторым q из $\mathbf{P}$ по модулю p. Далее в качестве n рассматриваются скаляры из $\mathbf{P}$ и одуль $\mathbf{P}^n = (\mathbf{P}^n, +, \omega_P(+))$. Пусть $\sigma = (x^i, u^l), \eta = (b^i, c^l)$; задана внутренняя (групповая) операция

$$(x^i, u^l) + (y^i, v^l) = (x^i + y^i, u^l + v^l + x^iy^j + a^l_{gh}x^gy^h + \dots + a^l_{nq}x^ny^q).$$

Сумма $w^l(x, y) = x^iy^j + a^l_{gh}x^gy^h + \dots + a^l_{nq}x^ny^q$ соответствует l-му классу эквивалентности k_l в разбиении множества $\mathbf{I} \cdot \mathbf{I}$ пар индексов порождающих элементов группы. Это разбиение определяет группу согласно алгоритму из п. 3.3. С использованием обозначения $w^l(x, y)$ групповая операция имеет вид $(x^i, u^l) + (y^i, v^l) = (x^i + y^i, u^l + v^l + w^l(x, y))$. Согласно групповой операции записываем внешнюю операцию одуля $\mathbf{P}^n$

$$q(x^i, u^l) = \left(x^i q, u^l q + \frac{(q-1)q}{2} w^l(x, x)\right), \quad q \in \mathbf{P},$$

функция $w^l(x,x)$ получается из $w^l(x,y)$ заменой y на x. Уравнению $q\sigma = \eta$ соответствуют покомпонентные сравнения

$$x^i q \equiv b^i, \quad u^l q + \frac{(q-1)q}{2} w^l(x,x) \equiv c^l.$$

Существует единственный скаляр $\overline{q} \in \mathbf{P}$, для которого $q\overline{q} \equiv 1$, поэтому $x^i \equiv \overline{q} b^i$. Из сравнений второго вида получаем

$$u^l q \equiv c^l - \frac{(q-1)q}{2} w^l(x,x),$$

откуда

$$u^l \equiv \overline{q}\left(c^l - \frac{(q-1)q}{2} w^l(x,x)\right).$$

Скаляры x^i, u^l найдены, их значения единственны, следовательно, найден и единственный кортеж σ, удовлетворяющий уравнению $q\sigma = \eta$. Каждому кортежу (x^i, u^l) из группы $\mathbf{P}^n$ соответствует единственный элемент $\alpha_i^{x^i} \tau_l^{u^l}$ из группы $\mathbf{G}^m$, значит, утверждение доказано для группы $\mathbf{G}^m$. $\square$

В случае мультипликативной записи групповой операции доказанная теорема означает, что $\mathbf{G}^m$ является конечной группой с однозначным извлечением корня.

Литература

[1] Долгарев А.И. *К вопросу об описании конечных метабелевых групп степени p* // IX Всесоюзный алгебраический коллоквиум, резюме научн. сообщ. – Гомель, 1968. – С. 69.

[2] Мазурок О.О. *Групи з елементарним абелевим комутантом порядку не більше ніж p^2* // Укр. матем. журн. – 1998. – Т. 50. – № 4. – С. 534–539.

[3] Долгарев А.И. *Конечные одулярные плоскости и модулярные решетки* // Междунар. конф. по алгебре памяти А.И. Ширшова, тез. докл. по логике и универс. алгебрам, прикл. алгебре. – Новосибирск, 1991. – С. 38.

[4] Сабинин Л.В. *Одули как новый подход к геометрии со связностью* // ДАН СССР. – 1977. – № 5. – С. 800–803.

[5] *Общая алгебра.* Т. 1. / Под ред. Л.А. Скорнякова. – М.: Наука, 1990. – 592 с.

[6] Каргаполов М.И., Мерзляков Ю.И. *Основы теории групп.* – М.: Наука, 1982 – 288 с.

А.И. Долгарев

доцент, кафедра математики и математического моделирования,
Пензенский государственный университет,
440026, г. Пенза, ул. Красная, д. 40,

e-mail: delivar@yandex.ru

A.I. Dolgarev

Associate Professor, Chair of Mathematics and Mathematical Modeling,
Penza State University,
40 Krasnaya str., Penza, 440026 Russia,

e-mail: delivar@yandex.ru