К вопросу построения примитивных разрешимых групп

С. Барская

Введение

Проблема построения примитивных разрешимых групп подстановок была поставлена еще Галуа [1] в связи с проблемой разрешимости алгебраических уравнений в радикалах. Галуа установил теорему: для того чтобы уравнение было разрешимо в радикалах, необходимо и достаточно, чтобы его группа была разрешимой. Решение любого уравнения сводится к решению уравнения примитивного, а примитивному уравнению соответствует примитивная группа. Таким образом, задача сводится к построению примитивных разрешимых групп подстановок. Степень таких групп есть p^n, где p — простое, n — любое число.

Галуа решил вопрос для $n=1$. Камилл Жордан решил его для $n=2$, указав общий способ нахождения примитивных разрешимых групп [2].

Дальнейший шаг в решении проблемы принадлежит О. Ю. Шмидту [3], который нашел общий вид функций, определяющих подстановки линейной группы степени p^n и установил ряд важных свойств этих функций. Построение примитивных разрешимых групп О. Ю. Шмидт свел к решению некоторых систем уравнений в конечном поле. Свой метод он прилагает к группам степени p^2.

Для случая любого простого числа n все типы примитивных разрешимых групп степени p^n построены Д. А. Супруненко в работе „Примитивные разрешимые группы подстановок“ [1] [4].

В настоящей статье проводится построение одного из типов примитивных разрешимых групп степени $p^q t$, где q, t — простые числа и $q \neq t$.

Построение примитивных разрешимых групп подстановок сводится к построению примарных разрешимых групп подстановок. Все типы примарных разрешимых групп данной степени классифицируются по строению их максимальных абелевых нормальных делителей. Классификация их основана на следующей теореме Д. А. Супруненко:

---

[1] В дальнейшем будут использованы терминология и обозначения этой статьи.

Пусть $\mathfrak{Z}$ *— общая примарная разрешимая группа степени* p^n; $\mathfrak{H}$ *— ее максимальный абелев нормальный делитель;* $GF[p^n]$ *— конечное поле с характеристикой* p, *над элементами которого группа* $\mathfrak{Z}$ *осуществляет подстановки. Тогда подстановки* H *группы* $\mathfrak{H}$ *задаются равенствами:*

$$H(\mu\eta_k^{(i)}) = \lambda_i \mu \eta_k^{(i)} \qquad (i=1, 2, \ldots, s;\ k=1, 2, \ldots r),$$

где

$$\lambda_1,\ \lambda_2, \ldots \lambda_s$$

s *произвольных, отличных от нуля элементов подполя* $GF[p^m]$ *поля* $GF[p^n]$, μ *— произвольный элемент* $GF[p^m]$;

$$\eta_1^{(1)}, \ldots, \eta_r^{(1)},\quad \eta_1^{(2)}, \ldots, \eta_r^{(2)}, \ldots, \eta_1^{(s)}, \ldots, \eta_r^{(s)}$$

базис поля $GF[p^n]$ *относительно подполя* $GF[p^m]$.

Порядок группы $\mathfrak{H}$ *равен* $(p^m-1)^s$. *Числа* m, r, s *связаны соотношением*

$$mrs=n. \tag{1}$$

Из этой теоремы и, в частности, соотношения (1) следует, что при $n=qt$ возможно существование шести типов максимальных абелевых нормальных делителей $\mathfrak{H}$ общей примарной разрешимой группы $\mathfrak{Z}$, соответствующих различным значениям чисел m, r, s, а именно:

1) $m=qt$; $s=r=1$;
2) $m=q$; $s=t$; $r=1$;
3) $m=1$; $s=qt$; $r=1$;
4) $m=1$; $s=q$; $r=t$;
5) $m=q$; $s=1$; $r=t$;
6) $m=s=1$; $r=qt$.

Построение примарных разрешимых групп, соответствующих нормальным делителям типов 1, 2, 3, 4, не трудно свести к построению примарных разрешимых групп степеней p^q (p^t), то есть к построению, разработанному Д. А. Супруненко. Специфические особенности случая p^{qt} сказываются при построении групп, соответствующих нормальным делителям типов 5 и 6.

В настоящей статье проводится построение групп, соответствующих нормальному делителю типа 6 [1], то есть рассматривается случай, когда максимальный абелев нормальный делитель $\mathfrak{H}$ искомой группы состоит из $p-1$ подстановок, осуществляющих умножение элементов поля $GF[p^n]$ на отличные от нуля вычеты по модулю p.

§ 1

Предположим, что существует общая примарная разрешимая группа $\mathfrak{Z}$ степени p^{qt} (p, q, t — простые числа, $q \neq t$), содержащая в качестве максимального абелевого нормального делителя группу $\mathfrak{H}$ подстановок, осуществляющих умножение на отличные от нуля вычеты

[1] Построение групп, соответствующих нормальному делителю типа 5, составляет содержание отдельной статьи.

по модулю p. Задача заключается в том, чтобы установить, каким условиям должны при этом удовлетворять числа p, q, t и изучить строение группы $\mathfrak{Z}$.

Рассмотрим фактор-группу $\mathfrak{Z}/\mathfrak{H}$ и в ней выделим максимальный абелев нормальный делитель $\mathfrak{N}/\mathfrak{H}$. Выясним прежде всего строение группы $\mathfrak{N}$. Так как группа $\mathfrak{N}/\mathfrak{H}$ абелева, то для любых двух подстановок N_1, N_2 из $\mathfrak{N}$ справедливо соотношение

$$N_2N_1=\varrho N_1N_2, \tag{2}$$

где

$$\varrho\in GF[p]; \quad \varrho\neq 0.$$

По условию максимальности группы $\mathfrak{H}$ группа $\mathfrak{N}$ не абелева, то есть среди соотношений (2) найдется такое, в котором

$$\varrho\neq 1,$$

откуда следует, что ϱ принадлежит некоторому отличному от единицы показателю по модулю p. Пусть d — наибольший показатель, которому принадлежат числа ϱ в соотношениях вида (2). Очевидно, что d есть делитель чисел $p-1$ и n, то есть рассматриваемые группы могут существовать лишь при условии, что общий наибольший делитель чисел $p-1$ и n больше единицы. При выполнении этого условия могут быть две возможности: либо $d=n$, либо $d<n$, то есть $d=q$ (либо $d=t$).

Теорема 1. *В группе $\mathfrak{N}$ существуют подстановки N_1, N_2 такие, что*

1) $$N_2N_1=\varrho N_1N_2,$$

где

$$\varrho^d=1; \quad \varrho^k\neq 1 \qquad (0<k<d);$$

2) *N_1, N_2 удовлетворяют уравнению*

$$x^d+(-1)^d=0.$$

Доказательство. а) Докажем, что в любом соотношении (2) числу ϱ принадлежит показателю, являющемуся делителем числа d. Для $d=n$ это очевидно. Пусть $d<n$, для определенности $d=q$. Допустим, что для некоторых M_1, M_2 из $\mathfrak{N}$

$$M_2M_1=\varrho_1M_1M_2,$$

где ϱ_1 принадлежит показателю t.

Тогда легко видеть, что

$$(M_2N_2)\,(M_1N_1)=\varrho\varrho_1\,(M_1N_1)\,(M_2N_2),$$

но $\varrho\varrho_1$ принадлежит показателю qt, что противоречит предположению о максимальности d.

б) Докажем далее, что для каждой подстановки $N\in\mathfrak{N}$

$$N^d\in\mathfrak{H}.$$

В самом деле, на основании доказанного в п. а) подстановка N^d перестановочна с каждой подстановкой группы $\mathfrak{N}$. Группа $\mathfrak{M}$, образованная

подстановками N^d, где N пробегает всю группу $\mathfrak{N}$, является абелевым нормальным делителем группы $\mathfrak{I}$ и, следовательно, группа $\mathfrak{M}$ входит в $\mathfrak{H}$.

в) Рассмотрим то из соотношений (2), в котором ϱ принадлежит показателю d. Докажем, что при этом подстановки N_1, N_2 всегда можно выбрать так, чтобы определители соответствующих им матриц были равны единице. В самом деле, для группы $\mathfrak{N}$ можно записать разложение

$$\mathfrak{N}=\mathfrak{N}_0+M\mathfrak{N}_0+\ldots+M^{k-1}\mathfrak{N}_0,$$

где $\mathfrak{N}_0$ — подгруппа группы $\mathfrak{N}$, состоящая из подстановок с единичными определителями; M — подстановка группы $\mathfrak{N}$, определитель которой принадлежит максимальному показателю по модулю p. Из этого разложения следует, что среди подстановок группы $\mathfrak{N}_0$ найдутся такие, для которых ϱ в соотношении (2) принадлежит показателю d.

г) На основании доказанного в п. б) подстановки N_1, N_2 удовлетворяют соответственно уравнениям

$$x^d-\varrho_1=0;\quad x^d-\varrho_2=0;\quad \varrho_1,\ \varrho_2\in GF[p]. \tag{3}$$

Покажем, что подстановки N_1, N_2 можно подобрать так, чтобы они обладали указанными выше свойствами и, кроме того,

$$-\varrho_1=-\varrho_2=(-1)^d.$$

Заметим, что характеристический полином подстановки N_1 содержит только члены со степенями, кратными числу d, — это вытекает из сравнения характеристических полиномов матриц N_1 и $\varrho N_1=N_2N_1N_2^{-1}$. Но тогда $x^d-\varrho_1$ — минимальный полином N_1, а $(x^d-\varrho_1)^{\frac{n}{d}}$ — характеристический полином матрицы N_1. Аналогичны рассуждения для подстановки N_2. Учитывая, что определители матриц N_1 и N_2 равны единице, получаем для свободных членов характеристических полиномов равенства

$$(-1)^n(-\varrho_1)^{\frac{n}{d}}=1;\quad (-1)^n(-\varrho_2)^{\frac{n}{d}}=1. \tag{4}$$

При $d=n$ отсюда сразу следует

$$-\varrho_1=-\varrho_2=(-1)^n,$$

то есть для этого случая теорема доказана.

Пусть теперь $d=q$. Из соотношения (4) следует

$$\varrho_1^t=\varrho_2^t=(-1)^{(q+1)t}.$$

Рассмотрим новые подстановки

$$N_1'=N_1^t;\quad N_2'=N_2^t.$$

$$(N_i')^q=N_i^{qt}=(N_i^q)^t=\varrho_i^t=(-1)^{(q+1)t}=\begin{cases}(-1)^{q+1} & \text{при } t\neq 2,\\ 1 & \text{при } t=2.\end{cases}$$

$(i=1,\ 2)$

В обоих случаях подстановки N_i' удовлетворяют уравнению

$$x^q+(-1)^q=0$$

(при $t=2$ число $q\neq 2$, так как $q\neq t$).

Для подстановок N_2', N_1' имеем

$$N_2'N_1' = N_2^tN_1^t = \varrho^{t^2}N_1^tN_2^t = \varrho^{t^2}N_1'N_2',$$

причем ϱ^{t^2} также принадлежит показателю q, ибо q, t — взаимно простые числа. Итак, теорема доказана и для случая $d=q$.

Приведем теперь матрицы подстановок N_1, N_2, существование которых доказано в теореме 1, к простейшему виду.

Пусть μ — корень минимального полинома подстановки N_1.

Тогда

$$\varrho\mu,\ \varrho^2\mu,\ \ldots,\varrho^{d-1}\mu,\ \varrho^d\mu=\mu$$

суть d его корней. Каждый из них является корнем характеристического полинома кратности $k=\dfrac{n}{d}$. Следовательно, матрица подстановки N_1 с помощью некоторого преобразования может быть приведена к виду

$$N_1=\begin{Vmatrix} \varrho\mu I_k & 0 & \ldots & 0 \\ 0 & \varrho^2\mu I_k & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \varrho^d\mu I_k \end{Vmatrix} \tag{5}$$

(I_k — единичная матрица порядка k).

В силу соотношения

$$N_2N_1=\varrho N_1N_2$$

матрица N_2 после того же преобразования приводится к виду

$$N_2=\begin{Vmatrix} 0 & A_1 & 0 & \ldots & 0 \\ 0 & 0 & A_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & A_{d-1} \\ A_d & 0 & 0 & \ldots & 0 \end{Vmatrix},$$

где A_i $(i=1, 2, \ldots, d)$ — матрицы порядка k, связанные соотношением

$$A_1A_2\ldots A_{d-1}A_d=(-1)^{d-1}I_k,$$

являющимся следствием того, что

$$x^d+(-1)^d$$

минимальный полином матрицы N_2.

Элементы матриц N_1, N_2 при этом принадлежат полю $GF[p]$, если $\mu \in GF[p]$. В противном случае элементы матриц N_1, N_2 суть элементы того подполя поля $GF[p^n]$, которому принадлежит μ. Применим, далее, к матрицам N_1, N_2 преобразование T, перестановочное с N_1

$$T=\begin{Vmatrix} T_1 & 0 & \dots & 0 \\ 0 & T_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & T_d \end{Vmatrix},$$

где T_i $(i=1, 2, \dots, d)$ — некоторые матрицы порядка k. Матрица N_1 после такого преобразования не изменится, а матрица N_2 примет вид

$$\begin{Vmatrix} 0 & T_1A_1T_2^{-1} & 0 & \dots & 0 \\ 0 & 0 & T_2A_2T_3^{-1} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & T_{d-1}A_{d-1}T_d^{-1} \\ T_dA_dT_1^{-1} & 0 & 0 & \dots & 0 \end{Vmatrix}.$$

Положим

$$T_1=I_k,$$

$$T_2=\frac{1}{\mu}A_1,$$

$$T_3=\frac{1}{\mu^2}A_1A_2,$$

$$\dots\dots\dots$$

$$T_{d-1}=\frac{1}{\mu^{d-2}}A_1A_2\dots A_{d-2},$$

$$T_d=\frac{1}{\mu^{d-1}}A_1A_2\dots A_{d-1}.$$

Тогда получим

$$T_1A_1T_2^{-1}=T_2A_2T_3^{-1}=\dots=T_{d-1}A_{d-1}T_d^{-1}=\mu I_k,$$

$$T_dA_dT_1^{-1}=\frac{1}{\mu^{d-1}}A_1A_2\dots A_{d-1}A_d=\frac{1}{\mu^{d-1}}(-1)^{d-1}I_k=\mu I_k.$$

$$(\mu^d=(-1)^{d-1}).$$

Итак, матрица подстановки N_2 после преобразования приводится к виду

$$N_2=\left.\begin{Vmatrix} 0 & \mu I_k & 0 & \dots & 0 \\ 0 & 0 & \mu I_k & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \mu I_k \\ \mu I_k & 0 & 0 & \dots & 0 \end{Vmatrix}\right\} d, \tag{6}$$

при этом N_1 имеет вид (5).

Пользуясь полученным представлением матриц N_1 и N_2, можно доказать теорему, дающую представление для любой подстановки N из группы $\mathfrak{N}$.

Теорема 2. *Для любой подстановки N группы $\mathfrak{N}$ имеет место однозначное представление*

$$N=\lambda N_1^a N_2^b,$$

где

$$\lambda \in GF[p];\quad \lambda \neq 0;\quad 0 \leqslant a < d;\quad 0 \leqslant b < d.$$

Доказательство. Пусть $N \in \mathfrak{N}$. Тогда

$$NN_1=\varrho_1 N_1 N,$$
$$NN_2=\varrho_2 N_2 N,$$

где

$$\varrho_1,\ \varrho_2 \in GF[p];\quad \varrho_1^d=\varrho_2^d=1.$$

Так как число ϱ принадлежит показателю d по модулю p, то

$$\varrho_1=\varrho^\alpha;\quad \varrho_2=\varrho^\beta,$$
$$0 \leqslant \alpha < d,$$
$$0 \leqslant \beta < d.$$

Рассмотрим подстановку $U \in \mathfrak{N}$

$$U=NN_2^{-\alpha}N_1^{\beta}.$$

Легко видеть, что подстановка U перестановочна с N_1 и с N_2, а для подстановки N имеем представление

$$N=UN_1^a N_2^b,$$

где

$$a=-\beta;\quad b=\alpha.$$

Докажем, что подстановка U принадлежит группе $\mathfrak{H}$. Допустим противное. Тогда U не может быть перестановочна со всеми подстановками группы $\mathfrak{N}$: если бы U была перестановочна с каждой подстановкой $N \in \mathfrak{N}$, то совокупность всех таких подстановок $U \in \mathfrak{N}$ образовала бы

абелев нормальный делитель группы $\mathfrak{J}$, содержащий $\mathfrak{H}$ в качестве подгруппы. Итак, в группе $\mathfrak{N}$ найдется подстановка M такая, что

$$UM=\varrho' MU,$$

$$\varrho' \in GF[p],$$
$$\varrho' \neq 1, \quad \varrho'^{d}=1.$$

Учитывая, что и для M имеет место представление

$$M=VN_1^a N_2^b,$$

где V — подстановка группы $\mathfrak{N}$, перестановочная с N_1 и с N_2, получаем соотношение

$$UV=\varrho' VU. \tag{7}$$

Из представления (5) матрицы подстановки N_1 следует, что матрицы подстановок U и V, перестановочных с N_1, имеют вид

$$U=\begin{Vmatrix} U_1 & 0 & \dots & 0 \\ 0 & U_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & U_d \end{Vmatrix}; \quad V=\begin{Vmatrix} V_1 & 0 & \dots & 0 \\ 0 & V_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & V_d \end{Vmatrix},$$

где U_i, V_i $(i=1, 2, \dots d)$ — неособенные матрицы порядка $k=\frac{n}{d}$.

Из соотношения (7) следует

$$U_i V_i=\varrho' V_i U_i,$$

откуда, сравнивая определители матриц с левой и правой сторон, получаем

$$\varrho'^{k}=1.$$

Однако

$$\varrho'^{d}=1,$$

следовательно простое число k является делителем числа

$$d=\frac{n}{k}.$$

Но тогда число n делится на k^2, что невозможно, так как

$$n=qt, \quad q \neq t.$$

Полученное противоречие приводит к выводу

$$U \in \mathfrak{H},$$

и для подстановки $N \in \mathfrak{N}$ имеем представление

$$N=\lambda N_1^{\alpha} N_2^{\beta};$$

$$\lambda \in GF[p]; \quad \lambda \neq 0; \quad 0 \leqslant a < d; \quad 0 \leqslant b < d.$$

Однозначность этого представления вытекает из того, что числа α, β, а значит, и числа a, b определяются однозначно, а при заданных a и b число λ также определяется однозначно. Теорема доказана.

Итак, строение группы $\mathfrak{N}$ полностью выяснено. Ее порядок равен

$$(p-1)d^2.$$

§ 2

Перейдем к изучению фактор-группы

$$\mathfrak{I}/\mathfrak{R}.$$

Для любой подстановки G группы $\mathfrak{I}$ имеют место соотношения

$$GN_1G^{-1}=\lambda_1 N_1^{\alpha}N_2^{\beta},$$

$$GN_2G^{-1}=\lambda_2 N_1^{\gamma}N_2^{\delta},$$

$$\lambda_1,\ \lambda_2 \in GF[p];\quad 0\leqslant \alpha<d;\quad 0\leqslant\beta<d;\quad 0\leqslant\gamma<d;\quad 0\leqslant\delta<d.$$

Из соотношения

$$N_2N_1=\varrho N_1N_2,$$

сохраняющегося для преобразованных подстановок GN_1G^{-1}, GN_2G^{-1}, следует, что определитель матрицы A

$$A=\begin{Vmatrix}\alpha & \beta\\ \gamma & \delta\end{Vmatrix}$$

равен единице.

Легко видеть, что если подстановке G_1 соответствует матрица A_1, а подстановке G_2 — матрица A_2, то произведению подстановок G_1G_2 соответствует матрица A_1A_2, то есть группа $\mathfrak{I}$ гомоморфно отображается на некоторую подгруппу $\mathfrak{A}'$ группы $\mathfrak{A}$ матриц второго порядка с элементами — вычетами по модулю d и определителями, равными единице. Покажем, что фактор-группа $\mathfrak{I}/\mathfrak{R}$ отображается изоморфно на группу $\mathfrak{A}'$. Для этого достаточно доказать, что если подстановке $G\in\mathfrak{I}$ соответствует единичная матрица группы $\mathfrak{A}'$, то подстановка G входит в $\mathfrak{R}$.

Пусть

$$GN_1=\mu_1N_1G,$$

$$GN_2=\mu_2N_2G \qquad (\mu_1,\ \mu_2\in GF[p]).$$

Так как N_1^d и N_2^d суть подстановки группы $\mathfrak{H}$, то есть перестановочны с подстановкой G, то

$$\mu_1^d=\mu_2^d=1.$$

Отсюда, как в § 1 для подстановки $N\in\mathfrak{R}$, получаем для G представление

$$G=UN_1^aN_2^b,$$

где U — подстановка группы $\mathfrak{I}$, перестановочная с N_1 и с N_2.

Теорема 3. *Всякая подстановка группы* $\mathfrak{I}$, *перестановочная с* N_1 *и с* N_2, *принадлежит группе* $\mathfrak{H}$.

Доказательство. Обозначим через $\mathfrak{U}$ группу всех подстановок $U\in\mathfrak{I}$, перестановочных с N_1 и с N_2 (то есть и с каждой подста-

новкой $N \in \mathfrak{N}$). $\mathfrak{U}$, очевидно, образует нормальный делитель группы $\mathfrak{J}$. $\mathfrak{U}$, как подгруппа разрешимой группы $\mathfrak{J}$, разрешима. Составим ряд коммутантов для группы $\mathfrak{U}$

$$R_0 = \mathfrak{U} \supset R_1 \supset R_2 \supset \ldots \supset R_{m-2} \supset R_{m-1} \supset J = R_m.$$

В силу разрешимости группы $\mathfrak{U}$ этот ряд заканчивается единичной группой J. Рассмотрим группу R_{m-1}.

Эта группа абелева, так как ее коммутант — единичная группа. Группа R_{m-1} является нормальным делителем групп R_{m-2}, $R_{m-3} \ldots \mathfrak{U}$, а значит, и группы $\mathfrak{J}$, так как коммутант является характеристической подгруппой. Значит

$$R_{m-1} \subset \mathfrak{H},$$

ибо в противном случае группа $R_{m-1}\mathfrak{H}$ давала бы абелев нормальный делитель группы $\mathfrak{J}$, содержащий $\mathfrak{H}$ в качестве подгруппы.

Рассмотрим группу R_{m-2} и докажем, что и

$$R_{m-2} \subset \mathfrak{H}.$$

Допустим противное, то есть что группа R_{m-2} содержит подстановки, отличные от подстановок $\mathfrak{H}$. Эти подстановки не принадлежат к группе $\mathfrak{N}$, так как они перестановочны с каждой подстановкой группы $\mathfrak{N}$. Рассмотрим группу

$$\mathfrak{N}_1 = R_{m-2}\mathfrak{N}.$$

Легко видеть, что

а) группа $\mathfrak{N}_1/\mathfrak{H}$ абелева,

б) $\mathfrak{N}_1/\mathfrak{H}$ нормальный делитель $\mathfrak{J}/\mathfrak{H}$,

в) $\mathfrak{N}_1/\mathfrak{H}$ содержит $\mathfrak{N}/\mathfrak{H}$ в качестве подгруппы, причем $\mathfrak{N}/\mathfrak{H}$ не совпадает с $\mathfrak{N}_1/\mathfrak{H}$.

Однако полученный результат противоречит тому, что $\mathfrak{N}/\mathfrak{H}$ максимальный абелев нормальный делитель группы $\mathfrak{J}/\mathfrak{H}$. Итак,

$$R_{m-2} \subset \mathfrak{H}.$$

Продолжая те же рассуждения, приходим к выводу, что и $R_{m-3}, \ldots, R_1$, $R_0 = \mathfrak{U}$ входят в $\mathfrak{H}$, то есть

$$\mathfrak{U} = \mathfrak{H}.$$

Теорема доказана.

Из доказанной теоремы следует изоморфизм фактор-группы $\mathfrak{J}/\mathfrak{N}$ группе $\mathfrak{A}'$.

Дальнейшая задача заключается в том, чтобы показать, что для каждой матрицы A

$$A = \begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix}$$

с элементами-вычетами по модулю d и определителем, равным единице, существует неособенная матрица G порядка n с элементами из $GF[p]$, соответствующая матрице A в установленном ранее гомоморфном соотношении. Предварительно произведем еще некоторые преобразования матриц N_1 и N_2.

При этом рассмотрим отдельно два случая: 1) $d=n$ и 2) $d<n$ — для определенности будем считать при этом $d=q$.

1. Если $d=n$, то $k=\frac{n}{d}=1$ и полученные ранее представления (5) и (6) (стр. 65—67) матриц подстановок N_1 и N_2 дают

$$N_1=\begin{Vmatrix} \varrho\mu & 0 & \dots & 0 \\ 0 & \varrho^2\mu & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \varrho^n\mu \end{Vmatrix}; \quad N_2=\left.\begin{Vmatrix} 0 & \mu & 0 \dots & 0 \\ 0 & 0 & \mu \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 \dots & \mu \\ \mu & 0 & 0 \dots & 0 \end{Vmatrix}\right\} n. \tag{8}$$

Так как ϱ принадлежит показателю $n=qt$, то ϱ можно записать в виде

$$\varrho=\sigma\tau,$$

где σ принадлежит показателю q, τ — показателю t, причем если u пробегает значения $1, 2, \dots, q$, а v — значения $1, 2, \dots, t$, то

$$\sigma^u\tau^v$$

пробегает все степени ϱ от 1 до n. Произведем теперь в матрицах N_1 и N_2 перестановку строк и соответствующих колонок так, чтобы матрица подстановки N_1 приняла вид

$$N_1=\begin{Vmatrix} \tau U_1 & 0 & \dots & 0 \\ 0 & \tau^2 U_1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \tau^t U_1 \end{Vmatrix}, \tag{9}$$

где

$$U_1=\begin{Vmatrix} \sigma\mu & 0 & \dots & 0 \\ 0 & \sigma^2\mu & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sigma^q\mu \end{Vmatrix}. \tag{9'}$$

Матрица подстановки N_2 при этом приводится к виду

$$N_2=\left.\begin{Vmatrix} 0 & U_2 & 0 \dots & 0 \\ 0 & 0 & U_2 \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 \dots & U_2 \\ U_2 & 0 & 0 \dots & 0 \end{Vmatrix}\right\} t, \tag{10}$$

где

$$U_2=\left.\begin{Vmatrix} 0 & \mu & 0 & \dots & 0 \\ 0 & 0 & \mu & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \mu \\ \mu & 0 & 0 & \dots & 0 \end{Vmatrix}\right\} q. \tag{10'}$$

Если $\mu \in GF[p]$, то полученное представление матриц N_1, N_2 является окончательным. Пусть $\mu \overline{\in} GF[p]$. Это имеет место при четном n ($n=2t$) и $p \equiv n+1 \pmod{2n}$.

В этом случае характеристический полином матриц N_1 и N_2

$$x^{2t}+1$$

разлагается в поле $GF[p]$ на неприводимые множители второй степени и имеет корень μ, удовлетворяющий уравнению

$$x^2+1=0.$$

Для того чтобы привести N_1, N_2 к рациональному виду, применим к N_1, N_2 преобразование $\tilde{T}$

$$\tilde{T}=\left\|\begin{matrix} T & 0 & \dots & 0 \\ 0 & T & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & T \end{matrix}\right\} t,$$

где

$$T=\left\|\begin{matrix} 1 & b+a\mu \\ \mu & -b\mu+a \end{matrix}\right\};$$

$$a,\ b \in GF[p];$$

$$a^2+b^2 \equiv -1 \pmod{p};$$

$$T^{-1}=\frac{1}{2}\left\|\begin{matrix} 1 & -\mu \\ -b+a\mu & -a-b\mu \end{matrix}\right\|.$$

В результате этого преобразования для матриц N_1 и N_2 сохраняются соответственно представления (9) и (10), но матрицы U_1 и U_2 при этом приводятся к виду

$$U_1=\left\|\begin{matrix} 0 & -1 \\ 1 & 0 \end{matrix}\right\|, \tag{9''}$$

$$U_2=\left\|\begin{matrix} -a & b \\ b & a \end{matrix}\right\|. \tag{10''}$$

2. Если $d=q$, то $k=\frac{n}{d}=t$. Переставляя строки и соответствующие колонки матриц N_1 и N_2 [см. представления (5) и (6)], приводим их к виду

$$N_1=\left\|\begin{matrix} U_1 & 0 & \dots & 0 \\ 0 & U_1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & U_1 \end{matrix}\right\} t, \tag{11}$$

где

$$U_1=\begin{Vmatrix} \varrho\mu & 0 & \dots & 0 \\ 0 & \varrho^2\mu & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \varrho^q\mu \end{Vmatrix}, \tag{11'}$$

$$N_2=\left.\begin{Vmatrix} U_2 & 0 & \dots & 0 \\ 0 & U_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & U_2 \end{Vmatrix}\right\} t, \tag{12}$$

где

$$U_2=\left.\begin{Vmatrix} 0 & \mu & 0 & \dots & 0 \\ 0 & 0 & \mu & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \mu \\ \mu & 0 & 0 & \dots & 0 \end{Vmatrix}\right\} q. \tag{12'}$$

Как и прежде, если $\mu \in GF[p]$, то полученное представление матриц N_1 и N_2 является окончательным.

Пусть $\mu \bar{\in} GF[p]$. Это имеет место при $q=2$ и $p\equiv 3 \pmod 4$; при этом $\varrho=-1$ и матрицы U_1 и U_2 в (11′) и (12′) имеют вид

$$U_1=\begin{Vmatrix} -\mu & 0 \\ 0 & \mu \end{Vmatrix}; \qquad U_2=\begin{Vmatrix} 0 & \mu \\ \mu & 0 \end{Vmatrix}.$$

Применяя снова к N_1, N_2 преобразование $\tilde{T}$ (стр. 72), приводим U_1 и U_2 к виду

$$U_1=\begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}, \tag{11''}$$

$$U_2=\begin{Vmatrix} -a & b \\ b & a \end{Vmatrix}. \tag{12''}$$

Представления (11) и (12) при этом сохраняются.

Перейдем к решению задачи, сформулированной на стр. 70, а именно докажем следующее предложение:

Теорема 4. *Для каждой матрицы второго порядка* A

$$A=\begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix}$$

с элементами-вычетами по модулю d *и определителем, равным единице, существует неособенная матрица* G *порядка* n *с элементами из* $GF[p]$, *удовлетворяющая системе уравнений*

$$\begin{aligned} GN_1 &= N_1^{\alpha} N_2^{\beta} G, \\ GN_2 &= N_1^{\gamma} N_2^{\delta} G. \end{aligned} \tag{13}$$

Доказательство. Доказывать теорему будем отдельно для двух случаев:

1) $d=q$; 2) $d=n$.

1) Пользуясь представлениями (11) и (12) матриц N_1 и N_2, будем искать решение G системы (13) в виде

$$G=\|\mathfrak{G}_{ik}\|_1^t,$$

где $\mathfrak{G}_{ik}$ — матрицы порядка q, удовлетворяющие при всех i, k одной и той же системе уравнений

$$\begin{aligned}\mathfrak{G}U_1&=U_1^{\alpha}U_2^{\beta}\mathfrak{G},\\ \mathfrak{G}U_2&=U_1^{\gamma}U_2^{\delta}\mathfrak{G}.\end{aligned}\tag{14}$$

Найдем решение системы (14)

$$\mathfrak{G}=\|g_{ik}\|_1^q$$

сначала для случая, когда $\mu\in GF[p]$, то есть исходя из представлений (11′) и (12′) матриц U_1 и U_2.

Перепишем систему (14) подробнее

$$\begin{Vmatrix} g_{11}\varrho & g_{12}\varrho^2 & \cdots & g_{1q}\varrho^q\\ g_{21}\varrho & g_{22}\varrho^2 & \cdots & g_{2q}\varrho^q\\ \cdot & \cdot & \cdots & \cdot\\ g_{q1}\varrho & g_{q2}\varrho^2 & \cdots & g_{qq}\varrho^q \end{Vmatrix} = \begin{Vmatrix} \varrho^{\alpha}g_{\beta+1,1} & \varrho^{\alpha}g_{\beta+1,2} & \cdots & \varrho^{\alpha}g_{\beta+1,q}\\ \varrho^{2\alpha}g_{\beta+2,1} & \varrho^{2\alpha}g_{\beta+2,2} & \cdots & \varrho^{2\alpha}g_{\beta+2,q}\\ \cdot & \cdot & \cdots & \cdot\\ \varrho^{q\alpha}g_{\beta 1} & \varrho^{q\alpha}g_{\beta 2} & \cdots & \varrho^{q\alpha}g_{\beta q} \end{Vmatrix};\tag{14_1}$$

$$\begin{Vmatrix} g_{1q} & g_{11} & g_{12} & \cdots & g_{1q-1}\\ g_{2q} & g_{21} & g_{22} & \cdots & g_{2q-1}\\ \cdot & \cdot & \cdot & \cdots & \cdot\\ g_{qq} & g_{q1} & g_{q2} & \cdots & g_{qq-1} \end{Vmatrix} = \begin{Vmatrix} \varrho^{\gamma}g_{\delta+1,1} & \varrho^{\gamma}g_{\delta+1,2} & \cdots & \varrho^{\gamma}g_{\delta+1,q}\\ \varrho^{2\gamma}g_{\delta+2,1} & \varrho^{2\gamma}g_{\delta+2,2} & \cdots & \varrho^{2\gamma}g_{\delta+2,q}\\ \cdot & \cdot & \cdots & \cdot\\ \varrho^{q\gamma}g_{\delta 1} & \varrho^{q\gamma}g_{\delta 2} & \cdots & \varrho^{q\gamma}g_{\delta q} \end{Vmatrix}.\tag{14_2}$$

Из (14_1) получаем

$$\varrho^k g_{ik}=\varrho^{i\alpha}g_{\beta+1,\,k},$$

откуда при $\beta\neq 0$ следует

$$g_{ik}=\varrho^{\frac{1-i}{\beta}(i\alpha-k)+\frac{(1-i)(1-i-\beta)\alpha}{2\beta}}g_{1k},\tag{15}$$

а при $\beta=0$

$$g_{ik}=0,\quad \text{если } i\alpha\not\equiv k \pmod q.$$

Из (14_2) получаем

$$g_{ik}=\varrho^{i\gamma}g_{\delta+i,\,k+1},\tag{16}$$

откуда при $\beta\neq 0$, учитывая (15), имеем

$$g_{1k}=\varrho^{k(k-1)\delta+(k-1)(2\beta\gamma-\alpha\delta-\beta\gamma+2)}g_{11},$$

При $\beta=0$ из (16) следует

$$g_{i,\ i\alpha}=\varrho^{\frac{1-i}{\delta}\gamma+\frac{(1-i)(1-i-\delta)}{2\delta}\gamma}g_{1\alpha}$$

(δ при этом отлично от нуля).

Итак, выбрав один элемент матрицы $\mathfrak{G}$ (g_{11} при $\beta\neq0$ и $g_{1\alpha}$ при $\beta=0$) произвольно, мы по этому элементу определяем все остальные элементы матрицы $\mathfrak{G}$. Следовательно, решение системы (14) определяется однозначно с точностью до множителя, в качестве которого можно взять произвольный элемент из $GF[p]$.

Покажем, что если этот множитель отличен от нуля, то и определитель $\Delta\mathfrak{G}$ матрицы $\mathfrak{G}$ отличен от нуля. Вычислим $\Delta\mathfrak{G}$ для случая $\beta\neq0$. Вынося за знак определителя общие, отличные от нуля множители из каждой строки и каждого столбца, получаем

$$\Delta\mathfrak{G}=C\begin{vmatrix} 1 & 1 & \dots & 1 \\ \varrho^{\frac{1}{\beta}} & \varrho^{\frac{2}{\beta}} & \dots & \varrho^{\frac{q}{\beta}} \\ \varrho^{\frac{2}{\beta}} & \varrho^{\frac{4}{\beta}} & \dots & \varrho^{\frac{2q}{\beta}} \\ \dots & \dots & \dots & \dots \\ \varrho^{\frac{q-1}{\beta}} & \varrho^{\frac{(q-1)2}{\beta}} & \dots & \varrho^{\frac{(q-1)q}{\beta}} \end{vmatrix}\neq0.$$

При $\beta=0$

$$\Delta\mathfrak{G}=\pm\prod_{i=1}^{q}g_{i,\ i\alpha}$$

и, следовательно,

$$\Delta\mathfrak{G}\neq0\ \text{ при }\ g_{1\alpha}\neq0.$$

Итак, для случая $\mu\in GF[p]$ существование решения системы (14) доказано.

Пусть $\mu\bar{\in}GF[p]$, при этом $q=2$ и группа $\mathfrak{A}$ матриц A

$$A=\begin{Vmatrix}\alpha & \beta\\ \gamma & \delta\end{Vmatrix}$$

есть группа шестого порядка.

Она имеет нормальный делитель третьего порядка — циклическую группу, образующая которой может быть определена матрицей

$$\begin{Vmatrix}1 & 1\\ 1 & 0\end{Vmatrix};$$

класс смежности по этому нормальному делителю можно определить матрицей

$$\begin{Vmatrix}0 & 1\\ 1 & 0\end{Vmatrix}.$$

Таким образом, для решения системы (14) достаточно найти две матрицы $\mathfrak{G}_1$ и $\mathfrak{G}_2$, удовлетворяющие соответственно системам уравнений

$$\mathfrak{G}_1 U_1 = U_1 U_2 \mathfrak{G}_1;$$
$$\mathfrak{G}_1 U_2 = U_1 \mathfrak{G}_1;$$
$$\mathfrak{G}_2 U_1 = U_2 \mathfrak{G}_2;$$
$$\mathfrak{G}_2 U_2 = U_1 \mathfrak{G}_2.$$

Зададим матрицы $\mathfrak{G}_1$ и $\mathfrak{G}_2$ равенствами

$$\mathfrak{G}_1 = (I_2 + U_1)(U_1 + U_2),$$
$$\mathfrak{G}_2 = U_1 + U_2.$$

Учитывая соотношения

$$U_1^2 = U_2^2 = -I_2; \quad U_2 U_1 = -U_1 U_2,$$

непосредственно проверяем, что $\mathfrak{G}_1$ и $\mathfrak{G}_2$ действительно являются решениями указанных систем.

Далее, из соотношений

$$(I_2 + U_1)^2 = 2U_1$$

и

$$(U_1 + U_2)^2 = U_1^2 + U_2^2 = -2I_2$$

следует, что определители матриц $\mathfrak{G}_1$ и $\mathfrak{G}_2$ отличны от нуля.

Итак, доказано существование неособенной матрицы порядка q, удовлетворяющей системе (14), для любого числа q.

Вернемся к решению системы (13). Искомая матрица G, удовлетворяющая системе (13), на основании доказанного может быть представлена в виде

$$G = \| C_{ik} \mathfrak{G}_0 \|_1^t,$$

где $\mathfrak{G}_0$ — одно из решений системы (14), C_{ik} — произвольные элементы $GF[p]$. При этом матрица G является неособенной, то есть определяет подстановку, тогда и только тогда, когда определитель Δ_C матрицы $\| C_{ik} \|_1^t$ отличен от нуля. Это утверждение вытекает из того, что для определителя Δ_G матрицы G имеет место соотношение

$$\Delta_G = \Delta \left\| \begin{matrix} \mathfrak{G}_0 & 0 & \dots & 0 \\ 0 & \mathfrak{G}_0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & \mathfrak{G}_0 \end{matrix} \right\| \cdot \Delta \left\| \begin{matrix} C_{11} I_q & C_{12} I_q & \dots & C_{1t} I_q \\ C_{21} I_q & C_{22} I_q & \dots & C_{2t} I_q \\ \cdot & \cdot & \cdot & \cdot \\ C_{t1} I_q & C_{t2} I_q & \dots & C_{tt} I_q \end{matrix} \right\| = (\Delta \mathfrak{G}_0)^t (\Delta_C)^q.$$

Для случая 1) $(d = q)$ теорема доказана.

2) Будем снова решение G системы (13) искать в виде

$$G = \| \mathfrak{G}_{ik} \|_1^t,$$

где $\mathfrak{G}_{ik}$ — некоторые матрицы порядка q, для определения которых возведем каждое из уравнений системы (13) в степень ts (s определяется из уравнения $ts-qr=1$). Получим

$$GN_1^{ts}=\varrho^{\frac{ts(ts-1)}{2}\alpha\beta}N_1^{ts\alpha}N_2^{ts\beta}G,$$

$$GN_2^{ts}=\varrho^{\frac{ts(ts-1)}{2}\gamma\delta}N_1^{ts\gamma}N_2^{ts\delta}G.$$

Однако, учитывая представления (9) и (10) матриц N_1 и N_2, имеем

$$N_1^{ts}=(-1)^{(q-1)r}\begin{Vmatrix} U_1 & 0 & \dots & 0 \\ 0 & U_1 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & U_1 \end{Vmatrix},$$

$$N_2^{ts}=(-1)^{(q-1)r}\begin{Vmatrix} U_2 & 0 & \dots & 0 \\ 0 & U_2 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & U_2 \end{Vmatrix}.$$

Отсюда следует, как и ранее, что каждая матрица $\mathfrak{G}_{ik}$ удовлетворяет одной и той же системе уравнений

$$\begin{aligned}\mathfrak{G}U_1&=U_1^{\alpha}U_2^{\beta}\mathfrak{G},\\ \mathfrak{G}U_2&=U_1^{\gamma}U_2^{\delta}\mathfrak{G},\end{aligned}\qquad(17)$$

так как

$$\varrho^{\frac{tsqr}{2}\alpha\beta}(-1)^{(q-1)r(\alpha+\beta-1)}=\varrho^{\frac{tsqr}{2}\gamma\delta}(-1)^{(q-1)r(\gamma+\delta-1)}=1$$

(для $q\neq 2$ это вытекает из того, что rs — четное число; для $q=2$ — из того, что хотя бы одно из чисел α, β и соответственно γ, δ — отлично от нуля).

Как и в случае 1, получаем

$$\mathfrak{G}_{ik}=C_{ik}\mathfrak{G}_0,$$

где C_{ik} — элементы из $GF[p]$; $\mathfrak{G}_0$ — одно из решений системы (17). При этом C_{ik} не произвольны, а связаны зависимостями, вытекающими из уравнений системы (13)

$$\varepsilon^k C_{ik}\mathfrak{G}_0U_1=\varepsilon^{i\alpha}U_1^{\alpha}U_2^{\beta}C_{\beta+i,\,k}\mathfrak{G}_0,$$

$$C_{ik}\mathfrak{G}_0U_2=\varepsilon^{i\gamma}U_1^{\gamma}U_2^{\delta}C_{\delta+i,\,k+i}\mathfrak{G}_0,$$

откуда получаем

$$C_{ik}=\varepsilon^{i\alpha-k}C_{\beta+i,\,k},$$

$$C_{ik}=\varepsilon^{i\gamma}C_{\delta+i,\,k+1}.$$

Эти рекуррентные формулы, как и в предыдущем случае, определяют неособенную матрицу $\|C_{ik}\|_1^t$ с точностью до множителя из $GF[p]$. Следовательно, и в этом случае решение системы (13) имеет вид

$$\mathfrak{G} = \|C_{ik}\,\mathfrak{G}_0\|_1^t,$$

представляет неособенную матрицу, так как $\|C_{ik}\|_1^t$ и $\mathfrak{G}_0$ — неособенные матрицы, и определяется однозначно с точностью до множителя из $GF[p]$.

Теорема доказана полностью.

Из доказанной теоремы и изоморфизма фактор-группы $\mathfrak{J}/\mathfrak{N}$ с подгруппой группы $\mathfrak{A}$ матриц второго порядка с элементами-вычетами по модулю d и определителями, равными единице, вытекает, что для построения группы $\mathfrak{J}$ следует рассмотреть все разрешимые подгруппы группы $\mathfrak{A}$ и из них выделить те, при которых группа $\mathfrak{J}$ окажется примарной.

§ 3

Перейдем к отысканию разрешимых подгрупп группы $\mathfrak{A}$.

Рассмотрим снова два случая:

1) $d=q$. В этом случае группа $\mathfrak{A}$ является подгруппой однородной линейной группы степени q^2, состоящей из подстановок с единичными определителями, и имеет, как известно, четыре типа разрешимых подгрупп.

2) $d=n$. В этом случае элементы матриц группы $\mathfrak{A}$ суть вычеты по модулю $n=qt$. Сведем вопрос о строении разрешимых групп таких матриц к вопросу о строении разрешимых групп матриц с элементами-вычетами по простому модулю, то есть к уже решенной задаче о строении разрешимых групп степени k^2, где k — простое число.

Для этого поставим в соответствие каждой матрице A

$$A=\left\|\begin{matrix}\alpha & \beta\\ \gamma & \delta\end{matrix}\right\|$$

с элементами-выч тами по модулю n пару матриц (A_1, A_2)

$$A_1=\left\|\begin{matrix}r_\alpha & r_\beta\\ r_\gamma & r_\delta\end{matrix}\right\|; \qquad A_2=\left\|\begin{matrix}s_\alpha & s_\beta\\ s_\gamma & s_\delta\end{matrix}\right\|,$$

где r_x — вычет числа x по модулю q, s_x — вычет числа x по модулю t.

Ввиду того, что числа r_x и s_x определяются числом x однозначно, то и пара матриц (A_1, A_2) матрицей A определяется однозначно.

Рассмотрим свойства установленного соответствия:

а) если

$$\left|\begin{matrix}\alpha & \beta\\ \gamma & \delta\end{matrix}\right| \equiv 1 \pmod{n},$$

то

$$\begin{vmatrix} r_\alpha & r_\beta \\ r_\gamma & r_\delta \end{vmatrix} \equiv 1 \pmod{q}; \qquad \begin{vmatrix} s_\alpha & s_\beta \\ s_\gamma & s_\delta \end{vmatrix} \equiv 1 \pmod{t}$$

(проверяется непосредственно);

б) если для матриц A_1, A_2

$$\begin{vmatrix} r_\alpha & r_\beta \\ r_\gamma & r_\delta \end{vmatrix} \equiv 1 \pmod{q}; \qquad \begin{vmatrix} s_\alpha & s_\beta \\ s_\gamma & s_\delta \end{vmatrix} \equiv 1 \pmod{t},$$

то существует одна и только одна матрица A

$$A = \left\| \begin{matrix} \alpha & \beta \\ \gamma & \delta \end{matrix} \right\|$$

с элементами-вычетами по модулю $n = qt$ и определителем, равным единице, которой соответствует пара матриц (A_1, A_2). В самом деле, для отыскания этой матрицы достаточно решить четыре системы сравнений:

$$\begin{cases} x \equiv r_\alpha \pmod{q} \\ x \equiv s_\alpha \pmod{t} \end{cases} \quad \dots \quad \begin{cases} x \equiv r_\delta \pmod{q}, \\ x \equiv s_\delta \pmod{t}, \end{cases}$$

каждая из которых имеет единственное по модулю qt решение, так как q, t — взаимно простые числа. Легко проверить, что при этом

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \equiv 1 \pmod{qt};$$

в) если матрице A соответствует пара матриц (A_1, A_2), а матрице B пара матриц (B_1, B_2), то матрице AB соответствует пара (A_1B_1, A_2B_2) (проверяется непосредственно).

Из указанных свойств вытекает изоморфизм группы $\mathfrak{A}$ прямому произведению групп $\mathfrak{A}_q$ и $\mathfrak{A}_t$ степеней q^2 и t^2 соответственно. Подгруппа группы $\mathfrak{A}$ тогда и только тогда разрешима, когда каждая из соответствующих подгрупп групп $\mathfrak{A}_q$ и $\mathfrak{A}_t$ будет разрешимой. Но для каждой из групп $\mathfrak{A}_q$ и $\mathfrak{A}_t$ существует по четыре типа разрешимых подгрупп, следовательно, для группы $\mathfrak{A}$ получаем всего 16 типов разрешимых подгрупп, строение которых известно.

§ 4

Остается решить вопрос о примарности построенных групп. При этом снова рассмотрим отдельно два случая.

1) $d = q$. Для группы $\mathfrak{I}$ в этом случае можно записать разложение

$$\mathfrak{I} = \mathfrak{N} + G_1\mathfrak{N} + \dots + G_h\mathfrak{N}, \tag{18}$$

где подстановки $I_n, G_1, \dots, G_h$ образуют группу, изоморфную одной из разрешимых подгрупп группы $\mathfrak{A}$.

При этом матрицы G_l $(l = 1, 2, \dots, h)$ представляют решение системы

$$GN_1 = N_1^{\alpha_l} N_2^{\beta_l} G,$$
$$GN_2 = N_1^{\gamma_l} N_2^{\delta_l} G$$

и представимы в виде

$$G_l = \| C_{ik}^{(l)} \mathfrak{G}_0^{(l)} \|_1^t.$$

В качестве матриц $C^{(l)} = \| C_{ik}^{(l)} \|_1^t$ при решении соответствующих систем можно было взять произвольные неособенные матрицы порядка t, но в силу разложения (18) эти матрицы между собой должны быть связаны некоторыми соотношениями, так как не трудно видеть, что их совокупность $\{I_p C^{(1)} \dots C^{(h)}\}$ образует группу $\mathfrak{B}$, гомоморфную фактор-группе $\mathfrak{Z}/\mathfrak{N}$. Группа $\mathfrak{B}$, следовательно, должна быть разрешимой. Покажем, что группа $\mathfrak{B}$ должна быть и примарной.

Теорема 5. *Группа* $\mathfrak{Z}$ *тогда и только тогда примарна, когда* $\mathfrak{B}$ *примарна.*

Доказательство. Если группа $\mathfrak{B}$ не примарна, то почти очевидно, что и группа $\mathfrak{Z}$ не примарна, так как группа $\mathfrak{N}$ не примарна.

Пусть теперь группа $\mathfrak{B}$ примарна. Докажем, что и группа $\mathfrak{Z}$ примарна.

Заметим прежде всего, что любая линейная комбинация матриц $N \in \mathfrak{N}$ может быть записана в виде полинома

$$\sum_{i,\,k=0}^{q-1} a_{ik} N_1^i N_2^k \qquad (a_{ik} \in GF[p])$$

и покажем, что за счет выбора коэфициентов a_{ik} матрица

$$\sum_{i,\,k=0}^{q-1} a_{ik} U_1^i U_2^k$$

может стать равной любой матрице B порядка q с элементами из $GF[p]$

$$B = \| b_{ik} \|_0^{q-1}.$$

Действительно, если U_1, U_2 имеют вид (11′) и (12′) (стр. 73), то

$$\sum_{i,\,k=0}^{q-1} a_{ik} U_1^i U_2^k = \sum_{i,\,k=0}^{q-1} \mu^{i+k} a_{ik} \begin{vmatrix} \overbrace{0 \quad \dots \quad 0}^{k} & \varrho^i & 0 \dots & 0 \\ 0 \quad \dots \quad 0 & 0 & \varrho^{2i} \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 \quad \dots \quad 0 & 0 & 0 \dots & \varrho^{(q-k)i} \\ \varrho^{(q-k+1)i} \dots & 0 & 0 \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 \quad \dots \quad \varrho^{qi} & 0 & 0 \dots & 0 \end{vmatrix} =$$

$$= \sum_{k=0}^{q-1} \mu^k \begin{Vmatrix} 0 & 0 & \dots & 0 & \sum_{i=0}^{q-1} \mu^i a_{ik} \varrho^i & 0 & \dots 0 \\ 0 & 0 & \dots & 0 & 0 & \sum_{i=0}^{q-1} \mu^i a_{ik} \varrho^{2i} & \dots 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sum_{i=0}^{q-1} \mu^i a_{ik} \varrho^{qi} & 0 & 0 & \dots 0 \end{Vmatrix}$$

и для определения a_{ik} при фиксированном k и $i=1, 2, \ldots q$ получаем систему уравнений

$$\mu^k \sum_{i=0}^{q-1} \mu^i a_{ik} \varrho^i = b_{0k},$$

$$\mu^k \sum_{i=0}^{q-1} \mu^i a_{ik} \varrho^{2i} = b_{1\,k+1},$$

$$\ldots\ldots\ldots\ldots,$$

$$\mu^k \sum_{i=0}^{q-1} \mu^i a_{ik} \varrho^{qi} = b_{q-1,\,k-1},$$

определитель которой, как легко видеть, отличен от нуля. Если же U_1 и U_2 имеют вид (11″) и (12″), то есть $q=2$ (стр. 73), то

$$\sum_{i,\,k=0}^{q-2} a_{ik} U_1^i U_2^k = a_{00} \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} + a_{10} \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix} + a_{01} \begin{Vmatrix} -a & b \\ b & a \end{Vmatrix} + a_{11} \begin{Vmatrix} -b & -a \\ -a & b \end{Vmatrix},$$

и для определения a_{ik} получаем систему

$$\begin{aligned} a_{00} - a a_{01} - b a_{11} &= b_{00} \\ -a_{10} + b a_{01} - a a_{11} &= b_{01} \\ a_{10} + b a_{01} - a a_{11} &= b_{10} \\ a_{00} + a a_{01} + b a_{11} &= b_{11}, \end{aligned}$$

определитель которой (в силу $a^2+b^2 \equiv -1 \pmod p$) равен 4, то есть отличен от нуля ($p \neq 2$).

Предположим теперь, что D — аддитивная подгруппа поля $GF[p^n]$, инвариантная по отношению к подстановкам из $\mathfrak{Z}$, а элемент $\xi \in D$

$$\xi = \lambda_1 \eta_{i_1} + \ldots + \lambda_q \eta_{i_q} + \lambda_{q+1} \eta_{i_{q+1}} + \ldots + \lambda_{2q} \eta_{i_{2q}} + \ldots +$$

$$+ \lambda_{(t-1)q+1} \eta_{i_{(t-1)q+1}} + \ldots + \lambda_{tq} \eta_{i_{tq}},$$

$\eta_{i_1}, \eta_{i_2}, \ldots, \eta_{i_n}$ — базис $GF[p^n]$;

$\lambda_i \in GF[p] \qquad (i=1, 2, \ldots, n)$.

Обозначим через D_i группу, построенную на базисных элементах $\eta_{qi+1}, \eta_{qi+2}, \ldots, \eta_{qi+q}$. Действие матрицы $N \in \mathfrak{N}$ одно и то же на всех аддитивных группах D_i и, вследствие доказанного выше свойства, найдется полином $P(U_1, U_2)$, преобразующий элементы

$$d_1 = \lambda_1 \eta_{i_1} + \ldots + \lambda_q \eta_{i_q}; \quad d_2 = \lambda_{q+1} \eta_{i_{q+1}} + \ldots + \lambda_{2q} \eta_{i_{2q}}; \ldots d_t =$$

$$= \lambda_{(t-1)q+1} \eta_{i_{(t-1)q+1}} + \ldots + \lambda_{tq} \eta_{i_{tq}}$$

соответственно в элементы

$$d_1' = \lambda_1 \eta_{i_1}; \quad d_2' = \lambda_{q+1} \eta_{i_{q+1}}; \ldots \quad d_t' = \lambda_{(t-1)q+1} \eta_{i_{(t-1)q+1}}.$$

Таким образом, найдется линейная комбинация подстановок $N \in \mathfrak{N}$, преобразующая элемент ξ в элемент $\xi_0 \in D$

$$\xi_0 = \lambda_1 \eta_1 + \lambda_{q+1} \eta_{q+1} + \ldots + \lambda_{(t-1)q+1} \eta_{(t-1)q+1}.$$

Далее, в силу примарности группы $\mathfrak{B}$ найдется комбинация матриц

$$a_1 C_1 + a_2 C_2 + \ldots,$$

преобразующая ξ_0 в η_1. Рассмотрим соответствующую комбинацию матриц из группы $\mathfrak{Z}$

$$a_1 C_1 \mathfrak{G}_{01} + a_2 C_2 \mathfrak{G}_{02} + \ldots$$

и для каждой матрицы $\mathfrak{G}_{0i}$ подберем линейную комбинацию $L_i(N)$ так, чтобы

$$L_i(N) = g_{0i}^{-1}.$$

Тогда, очевидно, линейная комбинация матриц $C \mathfrak{G}_0 N$ из $\mathfrak{Z}$

$$a_1 C_1 \mathfrak{G}_{01} L_1(N) + a_2 C_2 \mathfrak{G}_{02} L_2(N) + \ldots,$$

совпадая с

$$a_1 C_1 + a_2 C_2 + \ldots,$$

переводит ξ_0 в η_1. Таким образом, группа D содержит элемент η_1 и это же справедливо для любого базисного элемента. То есть

$$D = GF[p^n].$$

Теорема доказана.

Итак, для построения группы $\mathfrak{Z}$ остается для каждой примарной разрешимой группы степени p^t отыскать ее подгруппы, гомоморфные одной из разрешимых групп степени q^2, определители подстановок которых равны единице. Эта задача решается без труда, так как строение всех типов примарных разрешимых групп степени p^t (t — простое), как и строение разрешимых групп степени q^2, известно.

2) $d = n$. В этом случае всякая группа $\mathfrak{Z}$, содержащая в качестве нормального делителя группу $\mathfrak{N}$, причем фактор-группа $\mathfrak{Z}/\mathfrak{N}$ изоморфна одной из 16 разрешимых групп, построенных в § 3, примарна. Этот факт вытекает из того, что имеет место

Теорема 6. *При $d = n$ группа $\mathfrak{N}$ примарна.*

Доказательство. Рассмотрим два подслучая:

а) корень μ минимального полинома N_1 принадлежит полю $GF[p]$. В этом случае будем исходить из представления (8) (стр. 71) матриц N_1 и N_2. Пусть D — аддитивная подгруппа поля $GF[p^n]$, инвариантная по отношению к подстановкам группы $\mathfrak{N}$. Докажем, что $D = GF[p^n]$.

Пусть $\xi \in D$

$$\xi = \varrho_1 \eta_1 + \varrho_2 \eta_2 + \ldots + \varrho_n \eta_n,$$

$\eta_1, \eta_2, \ldots, \eta_n$ базис $GF[p^n]$;

$$\varrho_k \in GF[p] \qquad (k = 1, 2, \ldots, n)$$

и для определенности $\varrho_i \neq 0$.

Группа D содержит также элемент $P(N_1)\xi$, где

$$P(N_1)=a_1N_1^n+a_2N_1^{n-1}+\ldots+a_nN_1;\quad a_i\in GF[p]\quad (i=1, 2, \ldots, n).$$

Легко видеть, что коэфициенты $a_1, a_2, \ldots, a_n$ можно подобрать так, чтобы

$$P(N_1)\,\xi=\eta_i.$$

Однако тогда группа D содержит элемент η_i, а значит, и любой элемент базиса, так как подстановка N_2 перемещает элементы базиса транзитивно.

Итак,

$$D=GF[p^n]$$

и теорема для этого случая доказана;

б) корень μ минимального полинома не принадлежит полю $GF[p]$. В этом случае будем исходить из представлений (9) и (10) матриц N_1 и N_2, причем U_1, U_2 задаются соответственно формулами (9′) и (10′). Пусть $\eta_1,\ldots,\eta_n$ — базис поля $GF[p^n]$. Аддитивные группы D_i, построенные на базисных элементах η_{2i-1}, η_{2i}, являются инвариантными подгруппами для подстановки N_1, а подстановка N_2 транзитивно перемещает эти группы между собой.

Пусть снова D — аддитивная подгруппа поля $GF[p^n]$, инвариантная по отношению к подстановкам группы $\mathfrak{N}$. Пусть $\xi\in D$

$$\xi=\sum_{i=1}^{k}d_i;\quad d_i\in D_i;\quad d_k\neq 0;\qquad (k\leqslant l).$$

Построим снова полином $P(N_1)$ так, чтобы

$$P(N_1)\,\xi=d_k.$$

Тогда

$$d_k=\alpha\eta_{2k-1}+\beta\eta_{2k}\in D,$$

$$\alpha,\ \beta\in GF[p];\quad \alpha^2+\beta^2\not\equiv 0\pmod p.$$

Но отсюда следует, что и элементы базиса

$$\eta_{2k}=\frac{\tau^{-k}}{\alpha^2+\beta^2}[\tau^k\beta d_k-\alpha N_1(d_k)],$$

$$\eta_{2k-1}=\frac{\tau^{-k}}{\alpha^2+\beta^2}[\tau^k\alpha d_k+\beta N_1(d_k)]$$

входят в D. Применяя к η_{2k-1}, η_{2k} степени подстановки N_2, получим, что каждый элемент базиса входит в D, то есть $D=GF[p^n]$; теорема доказана и для этого случая.

Таким образом, построены примарные разрешимые группы степени $p^{\eta l}$, содержащие в качестве максимального абелевого нормального делителя группу подстановок, осуществляющих умножение на отличные от нуля вычеты по модулю p.

Для построения соответствующих примитивных разрешимых групп достаточно, как обычно, каждую из общих примарных разрешимых групп умножить на группу $\mathfrak{F}$ порядка p^{qt}, состоящую из подстановок F

$$F(\xi) = \xi + a,$$

$$(\xi,\ a \in GF[p^{qt}]).$$

ЛИТЕРАТУРА

1. Эварист Галуа, Сочинения, ОНТИ, 1938.

2. **C. Jordan, Traité des substitutions, Paris, 1870.**

3. О. Ю. Шмидт, Об уравнениях, решаемых в радикалах, степень которых есть степень простого числа p^m, Киев, 1913.

4. Д. А. Супруненко, Примитивные разрешимые группы подстановок, Матем. сб., 20(62) : 2, 1947.

5. Н. Г. Чеботарев, Теория Галуа (Монография), ОНТИ, 1936.

6. **I. Bucht, Die umfassendsten primitiven metazyklischen Kongruenzgruppen mit drei oder vier Variablen. Ark. f. Mat., 11 (1916).**

Поступила 14.X 1950 г.