Доклады Академии наук СССР
1970. Том 193, № 5

УДК 519.44 *МАТЕМАТИКА*

С. А. РУСАКОВ

ОБОБЩЕНИЕ ТЕОРЕМЫ ПОСТА

(Представлено академиком В. М. Глушковым 29 I 1970)

§ 1. Как известно, теорема Лагранжа для конечных n-групп в общем случае необратима уже при $n=2$. Поэтому весьма существенным является отыскание тех классов конечных n-групп, для которых имеет место обратимость теоремы Лагранжа хотя бы для определенного вида делителей порядка n-группы.

В настоящей статье исследуется «насыщенность» абелевых n-групп (см. определение 3) подгруппами, причем полученные нами результаты обобщают известный результат Е. Поста ([2], стр. 284) о существовании подгрупп у циклических n-групп, выраженный следующей теоремой:

Пусть $\mathfrak{G}$ — циклическая n-группа порядка $g = rs$, где r — наибольший делитель g, взаимно простой с $n-1$. Тогда $\mathfrak{G}$ имеет по крайней мере один элемент и точно одну подгруппу тех и только тех порядков γ, для которых $\gamma = \delta s$, где δ — произвольный делитель r.

§ 2. Приведем используемые в работе определения и обозначения.

Пусть $\mathfrak{G}$ — множество, на котором определена n-арная операция σ_n ([1], стр. 5), где $n \geqslant 2$ — арность операции, и пусть $\sigma_n(x_1x_2\ldots x_n)$ — значение n-арной операции σ_n, примененной к элементам $x_1, x_2, \ldots, x_n$ из $\mathfrak{G}$. Тогда имеет место

Определение 1 (ср. с ([3]), стр. 158; ([2]), стр. 213). Множество $\mathfrak{G}$ называется n-группой, если выполняются следующие постулаты:

1. Операция σ_n ассоциативна, т. е. для любых элементов $x_1, x_2, \ldots, x_n, x_{n+1}, \ldots, x_{2n-1}$ из $\mathfrak{G}$ имеет место равенство $\sigma_n(\sigma_n(x_1x_2\ldots x_n)x_{n+1}\ldots x_{2n-1}) = \sigma_n(x_1x_2\ldots x_j\sigma_n(x_{j+1}\ldots x_{j+n})\ldots x_{2n-1})$, где $j = 1, 2, \ldots, n-1$.

2. Верен закон однозначной и неограниченной обратимости, т. е. для любых элементов $a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n, a$, принадлежащих $\mathfrak{G}$, каждое из уравнений $\sigma_n(a_1a_2\ldots a_{i-1}x_ia_{i+1}\ldots a_n) = a$ $(i = 1, 2, \ldots, n)$ в $\mathfrak{G}$ всегда разрешимо относительно x_i, причем однозначно.

Понятие подгруппы для n-групп при $n > 2$ вводится тем же путем, что и при $n = 2$.

Мощность любого множества $\mathfrak{S}$ (в частности, n-группы $\mathfrak{G}$) обозначим через $|\mathfrak{S}|$. Если $\mathfrak{S} = \mathfrak{G}$, то $|\mathfrak{G}|$ назовем порядком n-группы $\mathfrak{G}$. При $|\mathfrak{G}|$ конечном n-группа $\mathfrak{G}$ тоже называется конечной.

Пусть Γ — множество всех непустых подмножеств, составленных из элементов n-группы $\mathfrak{G}$. На этом множестве определим n-арную операцию ω_n следующим образом. Пусть $\mathfrak{M}_i \in \Gamma$ $(i = 1, 2, \ldots, n)$. Тогда под $\omega_n(\mathfrak{M}_1\mathfrak{M}_2\ldots\mathfrak{M}_n)$ будем понимать множество всех элементов из $\mathfrak{G}$, каждый из которых равен $\sigma_n(m_1m_2\ldots m_n)$, где $m_i \in \mathfrak{M}_i$ и m_i принимает любое значение из $\mathfrak{M}_i$. Ясно, что некоторые из $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_n$, а может быть и все, могут состоять из одного элемента. Если $\mathfrak{M}_i = \{m_i\}$ $(i = 1, 2, \ldots, n)$, то очевидно, что $\omega_n(m_1m_2\ldots m_n) = \sigma_n(m_1m_2\ldots m_n)$.

Определение 2 (([3]), стр. 165). Подгруппа $\mathfrak{H}$ n-группы $\mathfrak{G}$ называется инвариантной в $\mathfrak{G}$, если для любого элемента $x \in \mathfrak{G}$ имеет место равенство $\omega_n(x\mathfrak{H}\ldots\mathfrak{H}) = \omega_n(\underbrace{\mathfrak{H}\ldots\mathfrak{H}}_{i-1}x\underbrace{\mathfrak{H}\ldots\mathfrak{H}}_{n-i})$ $(i = 2, \ldots, n)$. Если же $\omega_n(x\mathfrak{H}\ldots\mathfrak{H}) = \omega_n(\mathfrak{H}\ldots\mathfrak{H}x)$, то $\mathfrak{H}$ называется полуинвариантной подгруппой n-группы $\mathfrak{G}$.

Определение 3 (ср. с ([2]), стр. 217). n-Группу $\mathfrak{G}$ назовем абелевой, если для всяких элементов $x_1, x_2, \ldots, x_n$ из $\mathfrak{G}$ значение $\sigma_n(x_1x_2\ldots x_n)$ не изменяется при любой перестановке этих элементов.

§ 3. Нам потребуются еще следующие теоремы.

Теорема 1 (ср. с ([3]), стр. 163). *Пусть $\mathfrak{H}$ — некоторая подгруппа произвольной n-группы $\mathfrak{G}$ и пусть $a_1, a_2, \ldots, a_{k-1}, a_{k+l}, \ldots, a_n$ — фиксированные элементы n-группы $\mathfrak{G}$, где $k \geqslant 1$, $l \geqslant 1$. Если в*

$$\omega_n(a_1a_2\ldots a_{k-1}\underbrace{\mathfrak{H}\ldots\mathfrak{H}}_{l}a_{k+l}\ldots a_n)$$

один из элементов a_i $(i = 1, 2, \ldots, k-1, k+l, \ldots, n)$ заменить переменным элементом x, то для различных x два таких полученных подмножества n-группы $\mathfrak{G}$ или совпадают, или не имеют ни одного общего элемента; такие подмножества одной и той же мощности и в своей совокупности исчерпывают всю n-группу $\mathfrak{G}$. Если же $\mathfrak{G}$ конечна, то мощность каждого такого подмножества равна $|\mathfrak{H}|$.

Теорема 2 (([3]), стр. 165). *Если $\mathfrak{H}$ — полуинвариантная подгруппа для n-группы $\mathfrak{G}$, то все подмножества n-группы $\mathfrak{G}$ вида $\omega_n(x\mathfrak{H}\ldots\mathfrak{H})$ образуют n-группу относительно операции ω_n.*

Такую n-группу назовем фактор-группой для $\mathfrak{G}$ относительно $\mathfrak{H}$ и ее обозначим через $\mathfrak{G}/\mathfrak{H}$. В дальнейшем будем рассматривать только конечные n-группы.

§ 4. Изложим теперь полученные нами результаты.

Теорема 3. *Непустое подмножество $\mathfrak{H}$ конечной n-группы $\mathfrak{G}$ тогда и только тогда является n-подгруппой, когда $\mathfrak{H}$ — подмножество, на котором определена n-арная операция σ_n.*

Доказательство проводится тем же методом, что и при $n = 2$.

Теорема 4. *Пусть фактор-группа $\mathfrak{G}/\mathfrak{N}$ для конечной n-группы $\mathfrak{G}$ относительно $\mathfrak{N}$ обладает некоторой подгруппой $\overline{\mathfrak{B}}$. Тогда $\mathfrak{G}$ содержит такую подгруппу $\mathfrak{B}$, что $|\mathfrak{B}| = |\mathfrak{N}|\ |\overline{\mathfrak{B}}|$.*

Доказательство. На основании теоремы 1 n-группу $\mathfrak{G}$ можем представить так:

$$\mathfrak{G} = \omega_n(x_1\mathfrak{N}\ldots\mathfrak{N}) + \omega_n(x_2\mathfrak{N}\ldots\mathfrak{N}) + \ldots + \omega_n(x_\rho\mathfrak{N}\ldots\mathfrak{N}), \tag{1}$$

причем $|\omega_n(x_i\mathfrak{N}\ldots\mathfrak{N})| = |\mathfrak{N}|$, где $i = 1, 2, \ldots, \rho$. Считая теперь в (1) каждое слагаемое как отдельный элемент, получим, согласно теореме 2, фактор-группу $\mathfrak{G}/\mathfrak{N}$. Так как $\overline{\mathfrak{B}} \subseteq \mathfrak{G}/\mathfrak{N}$, то

$$\overline{\mathfrak{B}} = \omega_n(y_1\mathfrak{N}\ldots\mathfrak{N}) + \omega_n(y_2\mathfrak{N}\ldots\mathfrak{N}) + \ldots + \omega_n(y_\tau\mathfrak{N}\ldots\mathfrak{N}), \tag{2}$$

где $y_1, y_2, \ldots, y_\tau$ находятся среди $x_1, x_2, \ldots, x_\rho$ и $\tau = |\overline{\mathfrak{B}}|$.

Пусть теперь $\mathfrak{B}$ — совокупность всех элементов n-группы $\mathfrak{G}$ вида $\sigma_n(y_jv_1\ldots v_{n-1})$, где $j = 1, 2, \ldots, \tau$ и $v_1, \ldots, v_{n-1}$ — произвольные элементы из $\mathfrak{N}$. Тогда очевидно, что

$$\sigma_n(y_jv_1\ldots v_{n-1}) \in \omega_n(y_j\mathfrak{N}\ldots\mathfrak{N}). \tag{3}$$

Покажем, что $\overline{\mathfrak{B}}$ является подгруппой n-группы $\mathfrak{G}$. Действительно, пусть $\sigma_n(z_1v_1'\ldots v_{n-1}')$, $\sigma_n(z_2v_1''\ldots v_{n-1}'')$, $\ldots$, $\sigma_n(z_nv_1^{(n)}\ldots v_{n-1}^{(n)})$ — любые элементы из $\mathfrak{B}$, где $z_1, z_2, \ldots, z_n$ находятся среди элементов $y_1, y_2, \ldots, y_\tau$. Тогда, учитывая равенство (3), получим

$$\sigma_n(\sigma_n(z_1v_1'\ldots v_{n-1}')\sigma_n(z_2v_1''\ldots v_{n-1}'')\ldots\sigma_n(z_nv_1^{(n)}\ldots v_{n-1}^{(n)})) = z \in \mathfrak{R} =$$
$$= \omega_n(\omega_n(z_1\mathfrak{N}\ldots\mathfrak{N})\omega_n(z_2\mathfrak{N}\ldots\mathfrak{N})\ldots\omega_n(z_n\mathfrak{N}\ldots\mathfrak{N})).$$

Так как $\overline{\mathfrak{B}}$ является подгруппой фактор-группы $\mathfrak{G}/\mathfrak{N}$, то $\mathfrak{R} \in \overline{\mathfrak{B}}$ и, следовательно, $\mathfrak{R} = \omega_n(y_\lambda\mathfrak{N}\ldots\mathfrak{N})$ $(1 \leqslant \lambda \leqslant \tau)$. Отсюда $z \in \mathfrak{B}$ и по теореме 3, $\mathfrak{B}$ будет подгруппой n-группы $\mathfrak{G}$. Далее, так как каждое слагаемое из (2) имеет $|\mathfrak{N}|$ элементов из $\mathfrak{G}$ и эти слагаемые не имеют общих элементов, то $|\mathfrak{B}| = |\mathfrak{N}|\tau = |\mathfrak{N}|\ |\overline{\mathfrak{B}}|$. Теорема доказана.

Используемые нами определения и обозначения, относящиеся к степени и порядку элемента n-группы, можно найти в ([2]), стр. 282.

Теорема 5. *Абелева n-группа $\mathfrak{G}$ порядка $g = rs$, где $(r, s) = 1$ и $(r, n-1) = 1$, обладает подгруппой порядка δs, где δ — произвольный делитель r.*

Доказательство. Допустим, что теорема неверна. Тогда из всех абелевых n-групп, удовлетворяющих условию теоремы, выберем n-группу $\mathfrak{G}$ наименьшего порядка g, для которой теорема не выполняется. Так как для $g = 1$ теорема выполняется, то $g > 1$.

В дальнейшем рассмотрим следующие возможности:

1. В $\mathfrak{G}$ имеется хотя бы один элемент первого порядка. Пусть a — элемент первого порядка n-группы $\mathfrak{G}$, т. е. $\sigma_n(aa\ldots a) = a$. Тогда $(n-1)$-членная последовательность $\{a, a, \ldots, a\}$ является единицей n-группы $\mathfrak{G}$ (см. ([2]), стр. 214). На множестве $\mathfrak{G}$ определим бинарную операцию σ_2 следующим образом:

$$\sigma_2(x_1x_2) = x_1x_2 = \sigma_n(x_1x_2a\ldots a), \tag{4}$$

где x_1 и x_2 — произвольные элементы из $\mathfrak{G}$.

Покажем, что относительно этой операции $\mathfrak{G}$ является 2-группой. Действительно, учитывая (4), имеем $(x_1x_2)x_3 = \sigma_n(\sigma_n(x_1x_2a\ldots a)x_3a\ldots a)$ и $x_1(x_2x_3) = \sigma_n(x_1\sigma_n(x_2x_3a\ldots a)a\ldots a)$, где x_1, x_2 и x_3 — произвольные элементы из $\mathfrak{G}$.

Согласно постулату 1 определения 1 и с учетом того, что $\mathfrak{G}$ — абелева n-группа, получаем, что $\sigma_n(\sigma_n(x_1x_2a\ldots a)x_3a\ldots a) = \sigma_n(x_1\sigma_n(x_2x_3a\ldots a)a\ldots a)$. Поэтому $(x_1x_2)x_3 = x_1(x_2x_3)$, т. е. ассоциативность для бинарной операции выполняется.

Так как уравнение $\sigma_n(xb_1a\ldots a) = b$ (b_1 и b — любые элементы n-группы $\mathfrak{G}$) всегда в $\mathfrak{G}$ однозначно разрешимо относительно x, то и уравнение $xb_1 = b$ также однозначно разрешимо в $\mathfrak{G}$ относительно x. Это же утверждение справедливо и для уравнения $b_1y = b$. Следовательно, $\mathfrak{G}$ является 2-группой.

Покажем теперь, что для любых элементов $x_1, x_2, \ldots, x_n$ из $\mathfrak{G}$ имеет место равенство

$$x_1x_2\ldots x_n = \sigma_n(x_1x_2\ldots x_n). \tag{5}$$

В самом деле, из равенства (4) вытекает, что

$$\begin{aligned} x_1x_2x_3\ldots x_n &= (\ldots((x_1x_2)x_3)\ldots)x_{n-1})x_n = \\ &= \sigma_n(\sigma_n(\ldots(\sigma_n(\sigma_n(x_1x_2a\ldots a)x_3a\ldots a)\ldots)x_{n-1}a\ldots a)x_na\ldots a) = \\ &= \sigma_n(x_1x_2\underbrace{a\ldots a}_{n-2}x_3\underbrace{a\ldots a}_{n-2}\ldots x_{n-1}\underbrace{a\ldots a}_{n-2}x_n\underbrace{a\ldots a}_{n-2}), \end{aligned}$$

причем, как легко показать, число всех a, входящих под знак σ_n, равно $(n-1)(n-2)$. Так как $\mathfrak{G}$ — абелева n-группа, то

$$x_1x_2\ldots x_n = \sigma_n(x_1x_2\ldots x_n\underbrace{a\ldots a}_{(n-1)(n-2)}) = \sigma_n(x_1x_2\ldots x_n\underbrace{a\ldots a}_{n-1}\ldots\underbrace{a\ldots a}_{n-1}).$$

Поскольку $(n-1)$-членная последовательность $\{a, a, \ldots, a\}$ является единицей n-группы $\mathfrak{G}$, то $x_1x_2\ldots x_n = \sigma_n(x_1x_2\ldots x_n)$.

Нетрудно показать, что 2-группа $\mathfrak{G}$ является также абелевой. Поэтому $\mathfrak{G}$ как абелева 2-группа порядка $g = rs$ обладает подгруппой $\mathfrak{H}$ порядка δs, где δ — произвольный делитель r. Покажем, что $\mathfrak{H}$ — подгруппа n-группы $\mathfrak{G}$. Действительно, пусть $h_1, h_2, \ldots, h_n$ — произвольные элементы из $\mathfrak{H}$. Тогда $h_1h_2\ldots h_n \in \mathfrak{H}$. Отсюда и из равенства (5) заключаем, что $\sigma_n(h_1h_2\ldots h_n) \in \mathfrak{H}$, т. е. $\mathfrak{H}$ по теореме 3 является подгруппой n-группы $\mathfrak{G}$. Имеем противоречие.

2. Порядок любого элемента n-группы $\mathfrak{G}$ отличен от 1.

Пусть b — произвольный элемент n-группы $\mathfrak{G}$ и $\mathfrak{B}$ — циклическая подгруппа, порожденная этим элементом. На основании теоремы Лагранжа для n-групп ([2], стр. 222) $g_1 = |\mathfrak{B}|$ является делителем g. Так как $(r, s) = 1$, то g_1 можем представить так: $g_1 = r_1 s_1$, где r_1 и s_1 делят соответственно r и s. Тогда $(r_1, s_1) = 1$. Поэтому в $\mathfrak{B}$ имеется элемент, а следовательно, и подгруппа, порядка s. В самом деле, потребуем, чтобы $(b^{[\theta]})^{[s_1]} = b^{[\theta]}$, где θ — пока неизвестное число. На основании соотношения 2 (см. [2], стр. 282) имеем, что $b^{[(n-1)\theta s_1 + \theta + s_1]} = b^{[\theta]}$. Поскольку элемент b имеет своим порядком число g_1, то, согласно утверждению Е. Поста ([2], стр. 283), имеет место сравнение: $(n-1)\theta s_1 + \theta + s_1 - \theta \equiv 0 \pmod{g_1}$. Отсюда следует

$$s_1(n-1)\theta \equiv -s_1 \pmod{g_1}. \tag{6}$$

Согласно условию теоремы $(r, n-1) = 1$. Поэтому $(s_1(n-1), g_1) = s_1$ и, следовательно, сравнение (6) имеет всего s_1 различных решений $t, t + r_1, \ldots, t + (s_1 - 1) r_1$, где t — решение сравнения $(n-1)\theta \equiv -1 \pmod{r_1}$.

Рассмотрим теперь класс чисел, сравнимых с t по модулю r_1. Пусть c — произвольное положительное число, принадлежащие этому классу. Тогда $c = g_1 q + g_2$, где $0 \geqslant g_2 < g_1$, и поэтому $(b^{[g_1 q + g_2]})^{[s_1]} = b^{[g_1 q + g_2]}$. Отсюда и из того, что g_1 — порядок элемента b, вытекает равенство $(b^{[g_2]})^{[s_1]} = b^{[g_2]}$, т. е. в $\mathfrak{B}$ существует элемент $b_1 = b^{[g_2]}$, а следовательно, и подгруппа $\mathfrak{S}$ порядка s_1. Если бы $s_1 = 1$, то в $\mathfrak{G}$ существовал бы элемент b_1 первого порядка, что противоречит рассматриваемому случаю. Поэтому будем считать $s_1 > 1$, т. е. $|\mathfrak{S}| > 1$. Ввиду абелевости n-группы $\mathfrak{G}$, заключаем, что $\mathfrak{S}$ — инвариантная подгруппа.

Рассмотрим фактор-группу $\mathfrak{G}/\mathfrak{S}$. Легко показать, что $\mathfrak{G}/\mathfrak{S}$ является абелевой n-группой. Так как $|\mathfrak{G}/\mathfrak{S}| = r\frac{s}{s_1} < g$ и $\left(r, \frac{s}{s_1}\right) = 1$, то для $\mathfrak{G}/\mathfrak{S}$ теорема верна, т. е. $\mathfrak{G}/\mathfrak{S}$ содержит подгруппу $\overline{\mathfrak{H}}$ порядка $\delta\frac{s}{s_1}$, где δ — произвольный делитель r. Тогда на основании теоремы 4 заключаем, что $\mathfrak{G}$ содержит подгруппу $\mathfrak{H}$ порядка δs. Снова получили противоречие. Тем самым теорема полностью доказана.

Из теоремы 5 вытекает следующее

С л е д с т в и е 1. *Абелева n-группа $\mathfrak{G}$ порядка $g = rs$, где r — наибольший делитель g, взаимно простой с $n-1$, обладает подгруппой порядка δs, где δ — произвольный делитель r.*

Д о к а з а т е л ь с т в о. Поскольку r — наибольший делитель g, взаимно простой с $(n-1)$, то $(r, s) = 1$, и на основании теоремы 5 заключаем, что $\mathfrak{G}$ обладает подгруппой порядка δs, где δ — произвольный делитель r.

Следствие 1 обобщает теорему Е. Поста ([2], стр. 284) о существовании подгрупп у циклических n-групп.

Гомельская лаборатория
Института математики
Академии наук БССР

Поступило
12 XII 1969

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] В. Д. Б е л о у с о в, Основы теории квазигрупп и луп, М., 1967. [2] E. L. P o s t, Trans. Am. Math. Soc., 48, № 2, 208 (1940). [3] А. К. С у ш к е в и ч, Теория обобщенных групп, Харьков — Киев, 1937.