Доклады Академии Наук СССР
1940. Том XXVI, № 4

МАТЕМАТИКА

А. П. ДИЦМАН

О СРАВНЕНИИ СИСТЕМ ЭЛЕМЕНТОВ ГРУППЫ ПО ДВОЙНОМУ МОДУЛЮ

(Представлено академиком О. Ю. Шмидтом 13 XII 1939)

В настоящей статье устанавливаются некоторые свойства сравнений систем элементов группы по двойному модулю и некоторые критерии непростоты групп. Отсюда, в частности, следуют некоторые результаты, ранее полученные А. А. Кулаковым [1] и автором [1,2] этой статьи, а также результаты П. К. Щипанова [3].

§ 1. Пусть $\mathfrak{H}$ и Q суть подгруппы $\mathfrak{G}$. Два подмножества M и M_1 элементов группы $\mathfrak{G}$ будем называть сравнимыми по двойному модулю $(\mathfrak{H}, Q)$:

$$M \equiv M_1 (\mathfrak{H}, Q),$$

если

$$\mathfrak{H}MQ = \mathfrak{H}M_1Q.$$

Очевидно, определенное таким образом отношение сравнимости подмножеств $\mathfrak{G}$ рефлективно, симметрично и транзитивно.

Непосредственно из определения легко получаются следующие свойства сравнений по двойному модулю.

1. Сравнения можно почленно складывать, т. е. если L, L_1, M, $M_1, \ldots, N$, N_1 суть подмножества группы $\mathfrak{G}$, то из

$$\begin{aligned} L &\equiv L_1 \ (\mathfrak{H}, Q), \\ M &\equiv M_1 (\mathfrak{H}, Q). \\ &\cdots\cdots\cdots \\ N &\equiv N_1 (\mathfrak{H}, Q) \end{aligned} \tag{1}$$

следует

$$L + M + \ldots + N \equiv L_1 + M_1 + \ldots + N_1 (\mathfrak{H}, Q).$$

Здесь $L + M + \ldots + N$ представляет теоретико-множественную сумму $L, M, \ldots, N$. Множество сравнений (1) может быть как конечным, так и бесконечным.

2. Если $\mathfrak{H}_1$—подгруппа $\mathfrak{H}$ и Q_1—подгруппа Q, то из $M \equiv M_1 (\mathfrak{H}_1, Q_1)$ следует $M \equiv M_1 (\mathfrak{H}, Q)$.

Следствие. Если $\mathfrak{H}$—общее наименьшее кратное подгрупп $\mathfrak{H}_1$, $\mathfrak{H}_2, \ldots, \mathfrak{H}_k$ и Q—общее наименьшее кратное подгрупп $Q_1, Q_2, \ldots, Q_k$ группы $\mathfrak{G}$, то из

$$M \equiv M_1 \ (\mathfrak{H}_i, Q_i) \quad (i = 1, 2, \ldots, k)$$

следует

$$M \equiv M_1 \ (\mathfrak{H}, Q).$$

3. Если $\mathfrak{K}$ — инвариантный комплекс элементов группы $\mathfrak{G}$ и

$$M \equiv M_1 \ (\mathfrak{H}, Q),$$

то

$$\mathfrak{K}M \equiv \mathfrak{K}M_1 \ (\mathfrak{H}, Q).$$

4. Если Q — нормальный делитель, $\mathfrak{H}$—подгруппа, а N—подмножество элементов группы $\mathfrak{G}$, то из

$$M \equiv M_1 (\mathfrak{H}, Q)$$

следует

$$M \equiv M_1 \ (\mathfrak{H}Q, 1) \text{ и } MN \equiv M_1 N \ (\mathfrak{H}, Q),$$

где MN понимается как произведение комплексов M и N.

5. Если $\mathfrak{H}$—нормальный делитель, Q—подгруппа, а N—подмножество элементов группы $\mathfrak{G}$, то из

$$M \equiv M_1 (\mathfrak{H}, Q)$$

следует

$$M \equiv M_1 (1, \mathfrak{H}Q) \text{ и } NM \equiv NM_1 (\mathfrak{H}, Q).$$

6. Если $\mathfrak{H}$ и Q суть нормальные делители, N и N_1—подмножества элементов группы $\mathfrak{G}$, то из

$$M \equiv M_1 (\mathfrak{H}, Q),$$
$$N \equiv N_1 (\mathfrak{H}, Q)$$

следует

$$MN \equiv M_1 N_1 (\mathfrak{H}, Q).$$

Обозначим через M^{-1} подмножество, состоящее из всех элементов, обратных элементам подмножества M группы $\mathfrak{G}$.

7. Если $\mathfrak{H}$ и Q суть подгруппы $\mathfrak{G}$ и

$$M \equiv M_1 (\mathfrak{H}, Q),$$

то

$$M^{-1} \equiv M_1^{-1} (Q, \mathfrak{H}).$$

Следствие. Если

$$M \equiv M_1 (\mathfrak{H}, \mathfrak{H}),$$

тогда

$$M^{-1} \equiv M_1^{-1} (\mathfrak{H}, \mathfrak{H}).$$

§ 2. Теорема 1. *Пусть $\mathfrak{H}$—подгруппа, Q—нормальный делитель и M — подмножество элементов группы $\mathfrak{G}$. Совокупность $\mathfrak{V}$ элементов x группы $\mathfrak{G}$, удовлетворяющих условию*

$$Mx \equiv M (\mathfrak{H}, Q),$$

есть подгруппа $\mathfrak{G}$.

Если $\mathfrak{H}MQ \neq \mathfrak{G}$, то $\mathfrak{V} \neq \mathfrak{G}$.

Доказательство. Пусть x_1 и x_2—элементы, принадлежащие $\mathfrak{V}$. Так как Q—нормальный делитель группы $\mathfrak{G}$, то из условия

$$Mx_2 \equiv M (\mathfrak{H}, Q),$$

как легко видеть, следует

$$Mx_2^{-1} \equiv M(\mathfrak{H}, Q), \tag{2}$$

т. е. x_2^{-1} также принадлежит $\mathfrak{V}$.

Из условия

$$Mx_1 \equiv M(\mathfrak{H}, Q),$$

пользуясь свойством 4, получаем

$$Mx_1x_2^{-1} \equiv Mx_2^{-1}(\mathfrak{H}, Q). \tag{3}$$

Из (2) и (3) имеем

$$Mx_1x_2^{-1} \equiv M(\mathfrak{H}, Q),$$

т. е. $\mathfrak{V}$ вместе с элементами x_1 и x_2 содержит и элемент $x_1x_2^{-1}$, следовательно, $\mathfrak{V}$ есть подгруппа группы $\mathfrak{G}$. Согласно условиям теоремы и свойству 1 имеем

$$M\mathfrak{V} \equiv M(\mathfrak{H}, Q),$$

т. е.

$$\mathfrak{H}M\mathfrak{V}Q = \mathfrak{H}MQ.$$

Если $\mathfrak{H}MQ \neq \mathfrak{G}$, то, очевидно, и $\mathfrak{V} \neq \mathfrak{G}$.

Пусть $\mathfrak{K}$—подмножество элементов группы $\mathfrak{G}$ и n—натуральное число; обозначим через $\mathfrak{K}^n$ произведение n комплексов, равных $\mathfrak{K}$. Отметим два вспомогательных предложения, необходимых для дальнейшего.

Лемма 1. Пусть $\mathfrak{K}$ есть подмножество элементов группы $\mathfrak{G}$ и $\mathfrak{F}$—подгруппа, порождаемая всеми элементами $\mathfrak{K}$. Если $\mathfrak{K} = \mathfrak{K}^{-1}$, тогда

$$\mathfrak{F} = \sum_n \mathfrak{K}^n,$$

где $\sum_n \mathfrak{K}^n$—теоретико-множественная сумма подмножеств $\mathfrak{K}^n$, причем n пробегает все натуральные числа.

Действительно, всякий элемент F подгруппы $\mathfrak{F}$ можно представить в виде произведения конечного числа степеней некоторых элементов K_i подмножества $\mathfrak{K}$:

$$F = K_1^{\alpha_1} K_2^{\alpha_2}, \ldots, K_e^{\alpha_e}. \tag{4}$$

Обозначим через m сумму абсолютных величин показателей в (4), т. е.

$$m = |\alpha_1| + |\alpha_2| + \ldots + |\alpha_e|.$$

Очевидно, F принадлежит подмножеству $\mathfrak{K}^m$ и, следовательно, F входит в $\sum_n \mathfrak{K}^n$, т. е.

$$\mathfrak{F} \subseteq \sum_n \mathfrak{K}^n; \tag{5}$$

но для любого натурального числа n, очевидно, имеем

$$\mathfrak{K}^n \subseteq \mathfrak{F},$$

т. е.

$$\sum_n \mathfrak{K}^n \subseteq \mathfrak{F}. \tag{6}$$

Сопоставляя (5) и (6), получаем

$$\mathfrak{F} = \sum_n \mathfrak{K}^n.$$

Лемма 2. Если $\mathfrak{K}$—подмножество элементов группы $\mathfrak{G}$, содержащее лишь элементы конечного порядка, и $\mathfrak{F}$—подгруппа $\mathfrak{G}$, порождаемая всеми элементами $\mathfrak{K}$, то

$$\mathfrak{F} = \sum_n \mathfrak{K}^n,$$

где n пробегает все натуральные числа.

Для доказательства достаточно заметить, что всякий элемент F подгруппы $\mathfrak{F}$ может быть представлен в виде произведения конечного числа степеней некоторых элементов K_i подмножества $\mathfrak{K}$:

$$F = K_1^{\alpha_1} K_2^{\alpha_2}, \ldots, K_e^{\alpha_e}. \tag{7}$$

Но так как $\mathfrak{K}$ содержит лишь элементы конечного порядка, то в качестве показателей $\alpha_1, \alpha_2, \ldots, \alpha_e$ в (7) могут быть взяты натуральные числа. Дальнейшие рассуждения аналогичны доказательству леммы 1.

Теорема 2. *Пусть $\mathfrak{H}$ и Q суть подгруппы, $\mathfrak{K}$—инвариантный комплекс и M—подмножество элементов группы $\mathfrak{G}$. Если*

$$\mathfrak{K} = \mathfrak{K}^{-1},$$
$$M\mathfrak{K} \equiv M(\mathfrak{H}, Q) \tag{8}$$

и

$$\mathfrak{H}MQ \neq \mathfrak{G},$$

то все элементы $\mathfrak{K}$ порождают нормальный делитель $\mathfrak{F}$ группы $\mathfrak{G}$, не совпадающий с $\mathfrak{G}$.

Доказательство. Пользуясь свойством 3 и свойством транзитивности, из (8) для любого натурального числа n получаем

$$M\mathfrak{K}^n \equiv M(\mathfrak{H}, Q). \tag{9}$$

Обозначим через $\mathfrak{F}$ инвариантную подгруппу, порождаемую всеми элементами $\mathfrak{K}$; тогда по лемме 1

$$\mathfrak{F} = \sum_n \mathfrak{K}^n, \tag{10}$$

где n пробегает все натуральные числа.

Из (9) и (10) по свойству 1 имеем

$$M\mathfrak{F} \equiv M(\mathfrak{H}, Q),$$

т. е.

$$\mathfrak{H}M\mathfrak{F}Q = \mathfrak{H}MQ \neq \mathfrak{G},$$

следовательно, $\mathfrak{F} \neq \mathfrak{G}$. Доказательство теоремы 2 завершено.

Теорема 3. *Пусть $\mathfrak{K}$—отличный от единицы, инвариантный комплекс элементов группы $\mathfrak{G}$, содержащий лишь элементы конечного порядка; $\mathfrak{H}$ и Q—подгруппы и M—подмножество элементов $\mathfrak{G}$. Если*

$$M\mathfrak{K} \equiv M(\mathfrak{H}, Q)$$

и

$$\mathfrak{H}MQ \neq \mathfrak{G},$$

то $\mathfrak{G}$—непростая группа.

Для доказательства теоремы 3 достаточно повторить доказательство теоремы 2, заменяя в этом доказательстве лемму 1 леммой 2.

Теорема 4. *Пусть* $\mathfrak{H}$ *и* Q*—подгруппы,* $\mathfrak{K}$*—инвариантный комплекс, при этом* $\mathfrak{K} \neq 1$, M *и* M_1*—подмножества элементов группы* $\mathfrak{G}$. *Если для любого элемента* K *из* $\mathfrak{K}$

$$MK \equiv M_1 (\mathfrak{H}, Q), \quad M \equiv M_1 K^{-1} (\mathfrak{H}, Q)$$

и

$$\mathfrak{H} M Q \neq \mathfrak{G}, \tag{11}$$

то $\mathfrak{G}$*—непростая группа.*

Доказательство. Из условий теоремы по свойству 1 имеем

$$M\mathfrak{K} \equiv M_1 \ (\mathfrak{H}, Q) \ \text{ и } \ M \equiv M_1 \mathfrak{K}^{-1} (\mathfrak{H}, Q). \tag{12}$$

Умножая обе части первого из сравнений (12) на $\mathfrak{K}^{-1}$ и принимая во внимание второе, вследствие свойств симметрии и транзитивности получаем

$$M\mathfrak{K}\mathfrak{K}^{-1} \equiv M (\mathfrak{H}, Q). \tag{13}$$

Так как $\mathfrak{K}\mathfrak{K}^{-1} = (\mathfrak{K}\mathfrak{K}^{-1})^{-1}$, то из (11) и (13), пользуясь теоремой 2, заключаем, что $\mathfrak{G}$—непростая группа.

Теорема 5. *Пусть* $\mathfrak{H}$ *и* Q*—подгруппы,* $\mathfrak{K}$*—инвариантный комплекс, отличный от единицы,* M*—подмножество элементов группы* $\mathfrak{G}$. *Если*

$$M = M^{-1}; \quad M\mathfrak{K} \equiv M (\mathfrak{H}, \mathfrak{H}) \tag{14}$$

и

$$\mathfrak{H} M \mathfrak{H} \neq \mathfrak{G}, \tag{15}$$

то $\mathfrak{G}$*—непростая группа.*

Доказательство. Из условий теоремы, пользуясь следствием свойства 7, получаем

$$M\mathfrak{K}^{-1} \equiv M (\mathfrak{H}, \mathfrak{H}). \tag{16}$$

Пусть $\mathfrak{K}_1 = \mathfrak{K} + \mathfrak{K}^{-1}$. Из (14) и (16) по свойству 1 имеем

$$M\mathfrak{K}_1 \equiv M (\mathfrak{H}, \mathfrak{H}). \tag{17}$$

Очевидно, $\mathfrak{K}_1 = \mathfrak{K}_1^{-1}$; принимая во внимание (15) и (17) и пользуясь теоремой 2, заключаем, что группа $\mathfrak{G}$—непростая.

§ 3. Полагая $Q = 1$, получаем, в частности, результаты, ранее полученные А. А. Кулаковым [1] и автором [1,2] этой статьи, а также результаты П. К. Щипанова [3], так как сравнение

$$M \equiv M_1 (\mathfrak{H}, 1) \tag{18}$$

равносильно равенству $\mathfrak{H}M = \mathfrak{H}M_1$ и сравнение (18) можно записать как сравнение по модулю $\mathfrak{H}$:

$$M \equiv M_1 (\mathrm{mod}\ \mathfrak{H}).$$

Поступило
12 XII 1939

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] А. П. Дицман и А. А. Кулаков, ДАН, III, № 1 (1935). [2] А. П. Дицман, Тр. семинара по теории групп, стр. 27—29 (1938). [3] П. К. Щипанов, ДАН, XXV, № 2 (1939).