Доклады Академии Наук СССР
1939. Том XXV, № 2

МАТЕМАТИКА

П. К. ЩИПАНОВ

О СРАВНЕНИИ СИСТЕМ ЭЛЕМЕНТОВ ГРУППЫ

(Представлено академиком О. Ю. Шмидтом 10 VIII 1939)

В настоящей работе вводится понятие о сравнении систем элементов $\mathfrak{S}$ и $\mathfrak{S}'$, принадлежащих некоторой группе $\mathfrak{G}$.

В п. 1 дается основное определение и устанавливается ряд свойств сравнений систем по модулю $\mathfrak{H}$.

Полученные результаты позволяют далее (п. 2) просто формулировать и обосновать некоторые теоремы о существовании инвариантных подгрупп в конечных и бесконечных группах.

Теоремы эти заключают в себе, как частный случай, предложения, выведенные ранее А. А. Кулаковым и А. П. Дицманом ([1].

§ 1. Пусть $\mathfrak{G}$ — некоторая группа, $\mathfrak{H}$ — ее подгруппа и $\mathfrak{S}$ и $\mathfrak{S}'$ — системы элементов, принадлежащие группе $\mathfrak{G}$. Системы $\mathfrak{S}$ и $\mathfrak{S}'$ мы будем называть сравнимыми по модулю $\mathfrak{H}$ при соблюдении следующих условий: 1) если каждый элемент S системы $\mathfrak{S}$ может быть представлен в виде HS', где H — некоторый элемент группы $\mathfrak{H}$ и S' — некоторый элемент системы $\mathfrak{S}'$ и 2) если каждый элемент S_1' системы $\mathfrak{S}'$ может быть представлен в виде H_1S_1, где H_1 — некоторый элемент группы $\mathfrak{H}$ и S_1 — некоторый элемент системы $\mathfrak{S}$.

Сравнимость систем $\mathfrak{S}$ и $\mathfrak{S}'$ по модулю $\mathfrak{H}$ мы будем символически обозначать так:

$$\mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}}.$$

Из данного нами определения вытекают непосредственно следующие свойства сравнений:

I. При любом модуле сравнения $\mathfrak{H}$

$$\mathfrak{S} \equiv \mathfrak{S} \pmod{\mathfrak{H}}.$$

II. Из

$$\mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}}$$

следует

$$\mathfrak{S}' \equiv \mathfrak{S} \pmod{\mathfrak{H}}.$$

III. Из

$$\mathfrak{S} \equiv \mathfrak{S}_1 \pmod{\mathfrak{H}},$$
$$\mathfrak{S}_1 \equiv \mathfrak{S}_2 \pmod{\mathfrak{H}}$$

следует

$$\mathfrak{S} \equiv \mathfrak{S}_2 \pmod{\mathfrak{H}}.$$

([1] ДАН, III, № 1 (1935).

В самом деле любой элемент S системы $\mathfrak{S}$ может быть представлен в виде $S = HS_1$, где H — некоторый элемент группы $\mathfrak{H}$ и S_1 — некоторый элемент системы $\mathfrak{S}_1$. С другой стороны $S_1 = H_1 S_2$, где H_1 — некоторый элемент группы $\mathfrak{H}$ и S_2 — некоторый элемент $\mathfrak{S}_2$. Имеем таким образом, что $S = HH_1S_2 = H'S_2$, где $H' = HH_1$. Переписав сравнения (1) и (2) по свойству II в виде

$$\mathfrak{S}_2 \equiv \mathfrak{S}_1 \pmod{\mathfrak{H}}$$

и

$$\mathfrak{S}_1 \equiv \mathfrak{S} \pmod{\mathfrak{H}},$$

аналогичным образом приходим к выводу, что каждый элемент S_2' системы $\mathfrak{S}_2$ может быть представлен в виде $H''S'$, где H''—элемент группы $\mathfrak{H}$.

Таким образом $\mathfrak{S} \equiv \mathfrak{S}_2 \pmod{\mathfrak{H}}$.

IV. Если $\mathfrak{H}_1$ и $\mathfrak{H}_2$—подгруппы группы $\mathfrak{G}$, причем $\mathfrak{H}_2 \supseteq \mathfrak{H}_1$, то из

$$\mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}_1}$$

следует

$$\mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}_2}.$$

В частности, если

$$\begin{gathered} \mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}_1} \\ \mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}_2} \\ \cdots\cdots\cdots \\ \mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}_n}, \end{gathered}$$

где $\mathfrak{H}_1, \mathfrak{H}_2, \ldots \mathfrak{H}_n$ — подгруппы группы $\mathfrak{G}$, то

$$\mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}},$$

где $\mathfrak{H}$ — наименьшее кратное групп $\mathfrak{H}_1, \mathfrak{H}_2, \ldots \mathfrak{H}_n$.

V. Условимся совокупность элементов, принадлежащих по крайней мере одной из систем $\mathfrak{A}, \mathfrak{B}, \ldots \mathfrak{F}$, обозначать через $\mathfrak{A} + \mathfrak{B} + \ldots + \mathfrak{F}$.

Тогда из

$$\begin{gathered} \mathfrak{S}_1 \equiv \mathfrak{T}_1 \pmod{\mathfrak{H}}, \\ \mathfrak{S}_2 \equiv \mathfrak{T}_2 \pmod{\mathfrak{H}} \\ \cdots\cdots\cdots \\ \cdots\cdots\cdots \\ \mathfrak{S}_n \equiv \mathfrak{T}_n \pmod{\mathfrak{H}} \end{gathered} \tag{1}$$

следует:

$$\mathfrak{S}_1 + \mathfrak{S}_2 + \ldots + \mathfrak{S}_n \equiv \mathfrak{T}_1 + \mathfrak{T}_2 + \ldots + \mathfrak{T}_n \pmod{\mathfrak{H}}.$$

Заметим, что свойство V сохраняет свою силу и в том случае, если число сравнений (I) бесконечно.

VI. Пусть $\mathfrak{A}$ — произвольная система, принадлежащая (как и системы $\mathfrak{S}$ и $\mathfrak{S}'$) группе $\mathfrak{G}$. Тогда из

$$\mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}}$$

следует:

$$\mathfrak{S}\mathfrak{A} \equiv \mathfrak{S}'\mathfrak{A} \pmod{\mathfrak{H}}.$$

VII. Если модуль сравнения $\mathfrak{H}$ — нормальный делитель группы, то из

$$\begin{gathered} \mathfrak{S}_1 \equiv \mathfrak{T}_1 \pmod{\mathfrak{H}}, \\ \mathfrak{S}_2 \equiv \mathfrak{T}_2 \pmod{\mathfrak{H}} \end{gathered}$$

следует:

$$\mathfrak{S}_1\mathfrak{S}_2 \equiv \mathfrak{T}_1\mathfrak{T}_2 \pmod{\mathfrak{H}}.$$

Действительно любой элемент S_1 системы $\mathfrak{S}_1$ может быть представлен в виде $S_1 = H_1T_1$, где H_1 — некоторый элемент $\mathfrak{H}$, T_1 — некоторый элемент $\mathfrak{T}_1$ и любой элемент S_2 системы $\mathfrak{S}_2$ в виде $S_2 = H_2T_2$ (H_2 — некоторый элемент $\mathfrak{H}$, T_2 — некоторый элемент $\mathfrak{T}_2$). Очевидно, что

$$S_1S_2 = H_1T_1H_2T_2 = H_1T_1H_2T_1^{-1}T_1T_2 = HH'T_1T_2 = H''T_1T_2,$$

где H' и H'' — элементы группы $\mathfrak{H}$.

VIII. Если модуль сравнения $\mathfrak{H}$ — нормальный делитель группы и $\mathfrak{T}$ — произвольная система элементов, принадлежащих $\mathfrak{G}$, то из

$$\mathfrak{S} \equiv \mathfrak{S}' \pmod{\mathfrak{H}}$$

следует, что

$$\mathfrak{T}\mathfrak{S} \equiv \mathfrak{T}\mathfrak{S}' \pmod{\mathfrak{H}}.$$

Действительно, если $S = HS'$, то $TS = THS' = THT^{-1}TS' = H'TS'$ (здесь S принадлежит $\mathfrak{S}$, S' входит в $\mathfrak{S}'$, H и H' — элементы $\mathfrak{H}$ и T — элемент системы $\mathfrak{T}$).

§ 2. Докажем сначала одну вспомогательную теорему, используемую далее при выводе признаков непростоты группы.

Теорема 1. *Пусть $\mathfrak{G}$ — группа, $\mathfrak{S}$ — система элементов из $\mathfrak{G}$, $\mathfrak{H}$ — подгруппа группы $\mathfrak{G}$. Совокупность $\mathfrak{F}$ элементов X группы $\mathfrak{G}$, удовлетворяющих условию*

$$\mathfrak{S}X \equiv \mathfrak{S} \pmod{\mathfrak{H}}, \tag{1}$$

есть группа. Если $\mathfrak{H}\mathfrak{S}$ не совпадает с $\mathfrak{G}$, то $\mathfrak{F}$ не *совпадает с $\mathfrak{G}$.*

Доказательство. Пусть X_1 и X_2 — элементы группы $\mathfrak{G}$, удовлетворяющие условию (1), так что

$$\mathfrak{S}X_1 \equiv \mathfrak{S} \pmod{\mathfrak{H}}, \tag{2}$$
$$\mathfrak{S}X_2 \equiv \mathfrak{S} \pmod{\mathfrak{H}}. \tag{3}$$

Из (2) по свойству VI § 1 вытекает:

$$\mathfrak{S}X_1X_2 \equiv \mathfrak{S}X_2 \pmod{\mathfrak{H}},$$

далее по свойству III заключаем:

$$\mathfrak{S}X_1X_2 \equiv \mathfrak{S} \pmod{\mathfrak{H}}$$

и элемент X_1X_2 принадлежит совокупности $\mathfrak{F}$. Единица очевидно также принадлежит $\mathfrak{F}$ и остается только доказать, что если

$$\mathfrak{S}X \equiv \mathfrak{S} \pmod{\mathfrak{H}}, \tag{4}$$

то и

$$\mathfrak{S}X^{-1} \equiv \mathfrak{S} \pmod{\mathfrak{H}}. \tag{5}$$

Однако это очевидно, так как из (4) следует

$$\mathfrak{S} \equiv \mathfrak{S}X^{-1} \pmod{\mathfrak{H}},$$

а это сравнение по свойству II равносильно (5).

Покажем теперь, что если $\mathfrak{H}\mathfrak{S}$ не совпадает с $\mathfrak{G}$, то $\mathfrak{F}$ не может совпасть с $\mathfrak{G}$. Действительно, если бы $\mathfrak{F}$ совпадало с $\mathfrak{G}$, то и $\mathfrak{S}\mathfrak{F}$ совпадало бы с $\mathfrak{G}$, и из $\mathfrak{H}\mathfrak{S} \geqslant \mathfrak{S}\mathfrak{F}$ вытекало бы вопреки условию, что $\mathfrak{H}\mathfrak{S} = \mathfrak{G}$. Опираясь на теорему 1, докажем теперь следующую теорему:

Теорема 2. *Пусть $\mathfrak{G}$ — некоторая группа, $\mathfrak{H}$ — ее подгруппа, $\mathfrak{A}$ — инвариантный комплекс элементов группы $\mathfrak{G}$, $\mathfrak{S}$ и $\mathfrak{S}'$ — две системы элементов из $\mathfrak{G}$.*

Если для любого элемента A инвариантного комплекса $\mathfrak{A}$

$$\mathfrak{S}A \equiv \mathfrak{S}' \pmod{\mathfrak{H}}$$

и

$$\mathfrak{H}\mathfrak{S} \subset \mathfrak{G},$$

то группа $\mathfrak{G}$ имеет нормальный делитель.

Доказательство. Пусть инвариантный комплекс $\mathfrak{A}$ состоит из элементов

$$A_1, A_2, A_3 \ldots$$

По условию теоремы будем иметь

$$\mathfrak{S}A_1 \equiv \mathfrak{S}' \pmod{\mathfrak{H}}, \tag{6}$$
$$\mathfrak{S}A_2 \equiv \mathfrak{S}' \pmod{\mathfrak{H}} \tag{7}$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$

По свойству V отсюда вытекает:

$$\mathfrak{S}\mathfrak{A} \equiv \mathfrak{S}' \pmod{\mathfrak{H}}.$$

По свойству VI имеем далее:

$$\mathfrak{S}\mathfrak{A}\mathfrak{A}^{-1} \equiv \mathfrak{S}'\mathfrak{A}^{-1} \pmod{\mathfrak{H}}, \tag{8}$$

где $\mathfrak{A}^{-1}$—инвариантный комплекс элементов, состоящий из элементов, обратных элементам комплекса $\mathfrak{A}$.

С другой стороны, из равенства (6), (7), следует:

$$\mathfrak{S} \equiv \mathfrak{S}'A_1^{-1} \pmod{\mathfrak{H}},$$
$$\mathfrak{S} \equiv \mathfrak{S}'A_2^{-1} \pmod{\mathfrak{H}}$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$

откуда:

$$\mathfrak{S} \equiv \mathfrak{S}'\mathfrak{A}^{-1} \pmod{\mathfrak{H}}.$$

По свойству II это равносильно сравнению

$$\mathfrak{S}'\mathfrak{A}^{-1} \equiv \mathfrak{S} \pmod{\mathfrak{H}}. \tag{9}$$

Сопоставляя (8) и (9) и имея в виду свойство III, приходим к выводу, что $\mathfrak{S}\mathfrak{A}\mathfrak{A}^{-1} \equiv \mathfrak{S} \pmod{\mathfrak{H}}$.

По теореме 1 инвариантный комплекс элементов $\mathfrak{A}\mathfrak{A}^{-1}$ должен входить в действительную подгруппу $\mathfrak{F}$ группы $\mathfrak{G}$ и следовательно порождать нормальный делитель группы $\mathfrak{G}$.

Положив в частности в условии теоремы 2 $\mathfrak{H} = 1$, получаем такой результат:

Теорема 3. *Пусть $\mathfrak{G}$ — некоторая группа, $\mathfrak{H}$ — ее подгруппа, $\mathfrak{A}$ — инвариантный комплекс элементов группы $\mathfrak{G}$, $\mathfrak{S}$ и $\mathfrak{S}'$ — две системы элементов из $\mathfrak{G}$. Если для любого элемента A инвариантного комплекса $\mathfrak{A}$*

$$\mathfrak{S}A = \mathfrak{S}'$$

и

$$\mathfrak{S} \subset \mathfrak{G},$$

то группа $\mathfrak{G}$ имеет нормальный делитель.

Теорема 3 содержит в свою очередь, как частный случай, следующее предложение, доказанное А. А. Кулаковым и А. П. Дицманом.

Пусть $\mathfrak{S}$ и $\mathfrak{S}'$—две системы, содержащие одно и то же конечное число различных элементов группы $\mathfrak{G}$ и не совпадающие с $\mathfrak{G}$.

Пусть $\mathfrak{A}$ — некоторый инвариантный комплекс элементов группы $\mathfrak{G}$, содержащий по крайней мере один отличный от единицы элемент.

Если произведение $\mathfrak{S}\mathfrak{A}$ содержит только элементы системы $\mathfrak{S}'$, то $\mathfrak{G}$ — не простая группа.

Легко видеть в самом деле, что цитированное предложение представляет собой теорему 3 для частного случая, когда системы $\mathfrak{S}$ и $\mathfrak{S}'$ содержат конечное число элементов.

В самом деле, из условия равенства числа элементов систем $\mathfrak{S}$ и $\mathfrak{S}'$ и из условия, что произведение $\mathfrak{S}\mathfrak{A}$ содержит только элементы системы $\mathfrak{S}'$, вытекает, что для любого элемента A инвариантного комплекса $\mathfrak{A}$ имеет место равенство

$$\mathfrak{S}A = \mathfrak{S}',$$

т. е. предпосылка теоремы 3 в данном случае выполняется.

В заключение приношу благодарность проф. В. К. Туркину, под руководством которого работа была выполнена.

Поступило
17 VIII 1939