Доклады Академии Наук СССР
1939. Том XXIV, № 1

МАТЕМАТИКА

В. И. ГРОШЕВ

О ЧИСЛЕ ЭЛЕМЕНТОВ ГРУППЫ, СТЕПЕНЬ КОТОРЫХ ПРИНАДЛЕЖИТ ПРОИЗВОЛЬНОМУ МНОЖЕСТВУ ЭЛЕМЕНТОВ

(Представлено академиком О. Ю. Шмидтом 8 V 1939)

В 1925 г. Л. Вейснер в работе «On the number of elements of a group which have a power in a given conjugate set» (1) доказал следующую теорему:

«Пусть m — порядок элемента в классе сопряженных элементов $\mathfrak{M}$ группы $\mathfrak{G}$. Число элементов группы, какая-нибудь степень которых принадлежит классу сопряженных элементов $\mathfrak{M}$, кратно наибольшему делителю порядка группы, взаимно простому с m».

Приведенная теорема может быть получена как частный случай из весьма общей теоремы, установленной в 1938 г. П. Е. Дюбюком в работе «О фундаментальной теореме Фробениуса» (2). Эта теорема формулируется так:

«Пусть m—наименьшее кратное порядков элементов, принадлежащих инвариантному комплексу $\mathfrak{M}$ группы $\mathfrak{G}$. Пусть n—делитель порядка группы $\mathfrak{G}$, кратный числу m. Число элементов группы, n-ая степень которых принадлежит произвольному инвариантному комплексу $\mathfrak{A}$ и какая-нибудь степень которых пранадлежит инвариантному комплексу $\mathfrak{M}$, кратно наибольшему делителю n, взаимно простому с m».

Если положить в частности в только что приведенной теореме n равным порядку группы $\mathfrak{G}$ и принять инвариантный комплекс $\mathfrak{A}$ равным единице, то получаем из нее как следствие такое обобщение теоремы Л. Вейснера:

Пусть m—наименьшее кратное порядков элементов, принадлежащих инвариантному комплексу $\mathfrak{M}$ группы $\mathfrak{G}$. Число элементов группы, какая-нибудь степень которых входит в инвариантный комплекс $\mathfrak{M}$, кратно наибольшему делителю порядка группы, взаимно простому с m.

В настоящей работе будет доказано предложение, обобщающее как теорему Вейснера, так и формулированное нами следствие из теоремы П. Е. Дюбюка. Метод, которым мы будем пользоваться при доказательстве, был развит П. Е. Дюбюком частично в цитированной выше работе и частично в другой его работе, а именно: «Теорема, содержащая в себе теоремы Фробениуса, Вейснера и Туркина о числе элементов данного порядка в группе» (3).

Теорема 1. *Пусть m—наименьшее кратное порядков элементов, принадлежащих произвольной системе элементов $\mathfrak{M}$ группы $\mathfrak{G}$, и $\mathfrak{N}$ —*

нормализатор системы $\mathfrak{M}$. *Число элементов группы* $\mathfrak{G}$, *какая-нибудь степень которых входит в систему* $\mathfrak{M}$, *кратно наибольшему делителю порядка нормализатора* $\mathfrak{N}$, *взаимно простому с* m.

Доказательство. Согласно формулировке теоремы определению подлежит число элементов X группы $\mathfrak{G}$, удовлетворяющих условию

$$X^{\alpha} \subseteq \mathfrak{M}, \tag{1}$$

где α может быть каким-угодно числом. Пусть l будет наибольший делитель порядка группы $\mathfrak{G}$, взаимно простой с m. Обозначим X^l через Z:

$$X^l = Z \tag{2}$$

и заменим условие (1) соотношением

$$Z^{\beta} \subseteq \mathfrak{M}, \tag{3}$$

где β может быть каким-угодно числом.

Нетрудно видеть, что равенство (2) вместе с соотношением (3) эквивалентно условию (1). Действительно, если элемент X_1 удовлетворяет условию (1), то, определяя число δ из сравнения

$$l\delta \equiv 1 \pmod{m},$$

очевидно будем иметь, что

$$X_1^{\alpha l \delta} \subseteq \mathfrak{M}.$$

Переписывая же теперь последнее соотношение в виде

$$Z_1 = X_1^l,$$
$$Z_1^{\alpha\delta} \subseteq \mathfrak{M},$$

заключаем отсюда, что элемент X_1 удовлетворяет равенству (2) и условию (3). Обратно, если некоторый элемент X удовлетворяет равенству (2) и условию (3), то следовательно βl-ая степень его принадлежит системе $\mathfrak{M}$, т. е. рассматриваемый элемент удовлетворяет условию (1), если принять α равным βl.

Итак, вместо условия (1) рассмотрим равенство (2) и соотношение (3).

Если существует некоторый элемент X_1, для которого выполняются поставленные требования, то должны иметь место следующие равенства:

$$X_1^l = Z_1, \tag{4}$$
$$Z_1^{\beta} = M_1, \tag{5}$$

где элемент M_1 принадлежит системе $\mathfrak{M}$.

Порядок нормализатора $\mathfrak{N}$ системы $\mathfrak{M}$ обозначим через n и пусть элемент Z_1 имеет нормализатором группу $\mathfrak{H}_1$ порядка h_1. Пусть далее группа $\mathfrak{N}_1$ порядка n_1 будет пересечением групп $\mathfrak{N}$ и $\mathfrak{H}_1$. Образуем полную систему вычетов

$$N_1 = 1,\ N_2, \ldots;\ N_k$$

группы $\mathfrak{N}$ относительно ее подгруппы $\mathfrak{N}_1$. Все элементы

$$Z_i = N_i^{-1} Z_1 N_i \ (i = 1, 2, \ldots, k) \tag{6}$$

различны и удовлетворяют условию (3). Для каждого элемента из системы (6) уравнение

$$X^l = Z_i$$

имеет одно и то же число решений, кратное общему наибольшему делителю $D(l, h_1)$ чисел l и h_1.

Общее число элементов группы $\mathfrak{G}$, удовлетворяющих одному из уравнений

$$X^l = Z_i \quad (i = 1, 2, \ldots, k),$$

будет поэтому кратно произведению

$$kD(l, h_1),$$

и все эти элементы удовлетворяют уравнению (2) и условию (3). Так как k есть индекс подгруппы $\mathfrak{N}_1$ относительно группы $\mathfrak{N}$, то

$$kn_1 = n. \tag{7}$$

Но $\mathfrak{N}_1$ является также подгруппой группы $\mathfrak{H}_1$, и поэтому n_1 есть делитель h_1, вследствие чего $D(l, h_1)$ делится на $D(l, n_1)$. Таким образом искомое число решений делится на произведение

$$kD(l, n_1),$$

которое в свою очередь, принимая во внимание (7), кратно общему наибольшему делителю $D(l, n)$ чисел l и n. Отсюда заключаем, что если для данного числа β имеется элемент X_1, удовлетворяющий условиям (2) и (3), то этот элемент порождает в группе $\mathfrak{G}$ систему решений уравнений (2) и (3) при данном значении β, и число элементов этой системы кратно $D(l, n)$. Если найдется другой элемент X_2, не вошедший в предидущую систему и удовлетворяющий уравнению (3) при дополнительном равенстве (2) для того же значения β, то аналогичным способом построим для него систему решений, число элементов которой также будет кратно $D(l, n)$. Продолжая этот процесс, наконец получим все элементы группы $\mathfrak{G}$, которые при данном значении β удовлетворяют условиям (2) и (3), причем число этих элементов будет попрежнему кратно $D(l, n)$. Все предыдущие рассуждения справедливы для произвольного значения β, следовательно общее число решений, удовлетворяющих условиям (2) и (3) для всевозможных значений β, будет кратно $D(l, n)$, если только среди них не могут оказаться равные между собою. Но если два решения X и X' совпадают, то $Z = X^l$ и $Z' = X'^l$ будут равны между собой, и системы решений, порождаемые элементами X и X', будут очевидно состоять из одних и тех же элементов.

Сделаем еще несколько замечаний к следующей интересной теореме, которая доказана в работе П. Е. Дюбюка, указанной нами ([3]):

«Пусть a—порядок элемента в классе $\mathfrak{A}$ группы $\mathfrak{G}$ и m—порядок всех элементов в произвольной системе элементов $\mathfrak{M}$ группы $\mathfrak{G}$. Пусть далее n—делитель порядка группы, кратный m. Если a и m взаимно просты, то число элементов группы $\mathfrak{G}$, n-ая степень которых принадлежит классу $\mathfrak{A}$ и какая-нибудь степень которых входит в систему $\mathfrak{M}$, кратно $\varphi(m)$».

Прежде всего в приведенной теореме не обязательно вводить условие, что n есть делитель порядка группы, так как оно было введено в формулировку теоремы повидимому только потому, что такое же условие входит в нижеследующую вспомогательную теорему ([4]), которой автор пользовался в процессе доказательства:

«Пусть m и n—делители порядка группы и пусть n кратно m. Число элементов группы, порядок которых есть делитель n и какая-нибудь степень которых принадлежит произвольной системе элементов $\mathfrak{M}$ порядка m, кратно $\varphi(m)$».

В доказательстве же этой последней теоремы указанное выше условие нигде не используется, вследствие чего как она, так и интересующая

нас теорема будут справедливы и при отсутствии требования, что n есть делитель порядка группы.

Второе замечание состоит в том, что вместо класса сопряженных элементов можно рассматривать инвариантный комплекс элементов группы. Действительно, пусть инвариантный комплекс $\mathfrak{A}$ состоит из k классов сопряженных элементов $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k$. Число решений, удовлетворяющих условиям

$$\left.\begin{array}{l} X^n \subseteq \mathfrak{A}_i \\ X^\alpha \subseteq \mathfrak{M}, \end{array}\right\} \quad (1 \leqslant i \leqslant n), \tag{10}$$

где α может быть каким-угодно числом, на основании теоремы П. Е. Дюбюка кратно $\varphi(m)$.

Сумма всех решений для различных $\mathfrak{A}_i\,(1 \leqslant i \leqslant k)$ также будет кратна $\varphi(m)$. Действительно, очевидно не может существовать таких решений, которые удовлетворяют одновременно двум или более парам условий типа (10). Учитывая сделанные замечания, можно высказать такую теорему:

Теорема 2. *Пусть a — наименьшее кратное порядков элементов комплекса $\mathfrak{A}$ группы $\mathfrak{G}$ и m—порядок всех элементов в произвольной системе элементов $\mathfrak{M}$ группы $\mathfrak{G}$. Пусть далее n кратно m. Если a и m взаимно просты, то число элементов группы $\mathfrak{G}$, n-ая степень которых принадлежит инвариантному комплексу $\mathfrak{A}$ и какая-нибудь степень которых входит в систему $\mathfrak{M}$, кратно $\varphi(m)$.*

Поступило
9 V 1939.

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Weissner, Bull. of the Amer. Math. Soc., **31**, 492—496 (1925). [2] П. Е. Дюбюк, ДАН, XXI, № 4 (1938). [3] П. Е. Дюбюк, ДАН, XX, № 7—8 (1938). [4] П. Е. Дюбюк, Математ. сборник, **2(44)**, 6, 1247—1253 (1937).