Доклады Академии Наук СССР
1938. Том XXI, № 4

МАТЕМАТИКА

П. Е. ДЮБЮК

О ФУНДАМЕНТАЛЬНОЙ ТЕОРЕМЕ ФРОБЕНИУСА

(Представлено академиком О. Ю. Шмидтом 22 IX 1938)

В работе автора «Теорема, содержащая в себе теоремы Фробениуса, Вейснера и Туркина о числе элементов данного порядка в группе», предварительное сообщение о которой опубликовано в текущем году (1), доказывается следующее предложение:

«Пусть m — порядок элемента в классе сопряженных элементов $\mathfrak{M}$ группы $\mathfrak{G}$. Пусть далее n — делитель порядка группы, кратный числу m. Число элементов группы $\mathfrak{G}$, n-я степень которых принадлежит произвольному классу сопряженных элементов $\mathfrak{A}$ и какая-нибудь степень которых входит в класс $\mathfrak{M}$, кратно наибольшему делителю n, взаимно простому с m».

В настоящей работе мы доказываем следующую более общую теорему:

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-я степень которых принадлежит произвольному инвариантному комплексу $\mathfrak{A}$ и какая-нибудь степень которых принадлежит инвариантному комплексу $\mathfrak{M}$, кратно наибольшему делителю n, взаимно простому с m.

Если в частности в условии теоремы инвариантные комплексы $\mathfrak{A}$ и $\mathfrak{M}$ принять за классы сопряженных элементов, то мы получим цитированное выше предложение. Тем самым приведенная теорема содержит как частные случаи теоремы Фробениуса (2) и Вейснера (3).

Далее доказываемая теорема содержит как частный случай теорему В. К. Туркина (4). Для получения последней достаточно в условии нашей теоремы принять, что инвариантный комплекс $\mathfrak{M}$ исчерпывает все элементы группы $\mathfrak{G}$, порядок которых равен m, и положить одновременно инвариантный комплекс $\mathfrak{A}$ равным единице.

При выводе настоящей теоремы мы используем только фундаментальную теорему Фробениуса и не опираемся на теорему Л. Вейснера. Таким образом приводимое здесь доказательство теоремы дает также новый вывод теоремы Л. Вейснера.

Доказательство. При доказательстве теоремы очевидно достаточно ограничиться случаем, когда инвариантный комплекс $\mathfrak{A}$ есть класс сопряженных элементов группы $\mathfrak{G}$. Выведем прежде всего следующее вспомогательное предложение.

Лемма. *Пусть $m_1, m_2, \ldots, m_k$ — порядки элементов в классах сопряженных элементов (соответственно) $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_k$ группы $\mathfrak{G}$. Пусть*

m — наименьшее кратное чисел $m_1, m_2, \ldots, m_k$, а n — делитель порядка группы, кратный числу m. Число элементов группы, n-я степень которых принадлежит произвольному классу сопряженных элементов $\mathfrak{A}$, какая-нибудь степень которых входит в класс $\mathfrak{M}_1$, какая-нибудь другая степень входит в класс $\mathfrak{M}_2$ и т. д., наконец, какая-нибудь степень которых входит в класс $\mathfrak{M}_k$, кратно наибольшему делителю n, взаимно простому с m.

Нашей задачей является определение числа элементов группы, удовлетворяющих одновременно следующим условиям:

$$X^n \subseteq \mathfrak{A}, \tag{1}$$

$$X^{\alpha_i} \subseteq \mathfrak{M}_i, \quad (i=1, 2, \ldots, k), \tag{2}$$

где числа α_i могут нами быть выбраны как угодно.

Порядок некоторого элемента X, удовлетворяющего условиям (1) и (2), обозначим через bm', где b — наибольший делитель bm', взаимно простой с m. Применяя известную теорему, мы можем положить теперь $X = X_1X'$, причем элементы X_1 и X' перестановочны и порядки их равны соответственно m' и b. Заметим для дальнейшего, что

$$X'^{\alpha_i} = 1, \quad (\alpha_i = 1, 2, \ldots, k)$$

и значит

$$X_1^{\alpha_i} \subseteq \mathfrak{M}_i, \quad (\alpha_i = 1, 2, \ldots, k).$$

Теперь положим $n = lm''$, где l — наибольший делитель n, взаимно простой с m. Мы можем считать, что все α_i делятся на l. В самом деле, если какое-нибудь из чисел α_i не делится на l, то мы определим x из сравнения $lx \equiv 1 \pmod{m'}$ и заменим α_i через $\alpha_i lx$, так как

$$X^{\alpha_i lx} = X_1^{\alpha_i lx} X'^{\alpha_i lx} = X_1^{\alpha_i lx} = X_1^{\alpha_i} \subseteq \mathfrak{M}_i.$$

Условия (1) и (2) могут быть теперь заменены следующими:

$$X^l = Z, \tag{3}$$

$$Z^{m_2} \subseteq \mathfrak{A}, \tag{4}$$

$$Z^{\beta_i} \subseteq \mathfrak{M}_i, \quad (i=1, 2, \ldots, k), \tag{5}$$

где числа β_i могут быть нами выбраны как угодно.

В самом деле, если какой-нибудь элемент X удовлетворяет условиям (1) и (2), то он будет также удовлетворять равенству (3) при дополнительных условиях (4) и (5).

Обратно, если X удовлетворяет равенству (3) при дополнительных условиях (4) и (5), то X будет также удовлетворять условиям (1) и (2).

Обозначим элементы Z, удовлетворяющие условиям (4) и (5), через

$$Z_1, Z_2, \ldots, Z_\sigma.$$

Будем определять число элементов X, удовлетворяющих одному из условий:

$$X^l = Z_1, \; X^l = Z_2, \ldots, X^l = Z_\sigma.$$

Совокупность элементов $Z_1, Z_2, \ldots, Z_\sigma$ представляет собой, как легко видеть из условий (4) и (5), инвариантный комплекс элементов группы $\mathfrak{G}$. Число элементов X, удовлетворяющих поставленным условиям, будет поэтому, на основании теоремы Фробениуса, кратно l. Лемма таким образом доказана.

Воспользуемся теперь для доказательства теоремы методом эратосфенова решета, примененным в аналогичном случае В. К. Туркиным в цитированной выше работе ([4]), а также автором в работе «La généralisation du théorème de Turkin» ([5]).

Нашей задачей является теперь определение числа элементов, удовлетворяющих условиям:

$$X^n \subseteq \mathfrak{A}, \tag{6}$$

$$X^\alpha \subseteq \mathfrak{M}, \tag{7}$$

где α может быть выбрано нами как угодно.

Здесь, как уже отмечалось выше, $\mathfrak{A}$ без ущерба для общности можно считать классом сопряженных элементов.

С другой стороны, инвариантный комплекс $\mathfrak{M}$ мы будем считать состоящим из k классов сопряженных элементов $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_k$, причем порядки элементов этих классов будем обозначать, как и при выводе леммы, через $m_1, m_2, \ldots, m_k$. Нас будет интересовать следовательно число элементов, n-я степень которых принадлежит классу $\mathfrak{A}$ и какая-нибудь степень которых принадлежит по крайней мере одному из классов $\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_k$.

Введем следующее обозначение: наибольший делитель числа n, взаимно простой с m_i, будем обозначать через n_i; наибольший делитель числа n, взаимно простой с произведением $m_i m_j$, будем обозначать через $n_{ij} = n_{ji}$ и так далее. Наконец наибольший делитель числа n, взаимно простой с произведением $m_1 m_2 \ldots m_k$, иначе говоря, с числом m, обозначим через $n_{12\ldots k}$. Число элементов, удовлетворяющих условию (6) и одному из условий

$$X^{\alpha_i} \subseteq \mathfrak{M}_i \tag{8}$$

(здесь α_i может быть выбрано как угодно, а i — одно из чисел $1, 2, \ldots, k$), кратно на основании леммы n_i.

Обозначим это число через $\lambda_i n_i$, где λ_i — некоторое целое число. Число элементов, удовлетворяющих поставленным условиям (6) и (7), будет очевидно меньше, чем

$$\sum_{i=1}^{k} \lambda_i n_i,$$

за счет элементов, удовлетворяющих одновременно условию (6) и двум или более из условий (8). Число таких элементов равно

$$\frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{k} \mu_{ij} n_{ij}, \tag{9}$$

где μ_{ij} — целые числа, причем $\mu_{ij} = \mu_{ji}$ для $i \neq j$ и $\mu_{ij} = 0$, если $i = j$.

Разность

$$\sum_{i=1}^{k} \lambda_i n_i - \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{k} \mu_{ij} n_{ij}$$

будет очевидно меньше интересующего нас числа элементов, удовлетворяющих условиям (6) и (7). Дело в том, что некоторые элементы учтены в сумме (9) два или более раз. Это именно те элементы, которые помимо условия (6) удовлетворяют также по крайней мере трем из условий (8).

Продолжая тот же процесс далее, приходим в конце концов к выводу, что число элементов, удовлетворяющих условиям теоремы, выражается суммой:

$$\sum_{i=1}^{k} \lambda_i n_i - \frac{1}{2} \sum_{i=1}^{k} \sum_{j=1}^{k} \mu_{ij} n_{ij} + \ldots \pm \nu n_{12 \ldots k}, \tag{10}$$

где ν — некоторое целое число.

Легко видеть, что всякий элемент группы, удовлетворяющий условиям теоремы, учитывается в сумме (10) один и только один раз. Если например элемент удовлетворяет условию (6) и s из условий (8), то он учитывается

$$C_s^1 - C_s^2 + C_s^3 - \ldots \pm C_s^s = 1 - (i-1)^s = 1$$

раз.

Замечаем наконец, что все члены суммы (10) делятся на наибольший делитель n, взаимно простой с m.

Теорема таким образом доказана.

Институт математики.
Московский гос. университет.

Поступило
27 IX 1938.

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] П. Е. Дюбюк, ДАН, XX, № 7 (1938). [2] Frobenius, Sitzungsber. d. Berl. Akad., 987 (1903). [3] Weissner, Bull. of the Amer. Mathemat. Soc., **31**, 492—496 (1925). [4] В. К. Туркин, C. R. Acad. Sci. de Paris, 1059—1061 (1931). [5] П. Е. Дюбюк, Матем. сб., **1** (43), 4, 603—605 (1936).