Приложенiе теоремы Зилова къ симметрической группѣ.

А. А. Радцигъ.

Одна изъ основныхъ теоремъ теорiи подстановокъ есть теорема *Лагранжа*, по которой порядокъ каждой подгруппы какой либо группы подстановокъ есть дѣлитель порядка послѣдней *).

Коши показалъ **), обратно, что группа, порядокъ которой дѣлится на простое число p, заключаетъ подстановку этого порядка (т. е. содержитъ подгруппу этого порядка).

Эта теорема была обобщена и значительно дополнена *Зиловымъ* ***). Онъ нашелъ, что группа $\mathfrak{S}$, порядокъ которой s дѣлится на какое-либо простое число p въ степени α, содержитъ подгруппы порядка p^α. Подгруппы порядка p^f, гдѣ f — наивысшая степень p, на которую дѣлится s, *подобны* (semblables, ähnlich) другъ другу, т. е. получаются изъ одной чрезъ *преобразованiе* (Transformation) элементами $\mathfrak{S}$. Число N *различныхъ* группъ порядка p^f удовлетворяетъ сравненiю

$$N \equiv 1 \pmod{p} \quad \ldots \ldots \quad (1)$$

Порядокъ группы $\mathfrak{H}$, состоящей изъ элементовъ $\mathfrak{S}$, перемѣщаемыхъ съ одной изъ группъ $\mathfrak{G}$ порядка p^f, есть

$$h = p^f v \ldots \ldots \ldots \ldots \quad (2)$$

гдѣ v не зависитъ отъ выбора группы $\mathfrak{G}$).

Между s, N и h существуетъ зависимость

$$s = Nh \ldots \ldots \ldots \ldots \quad (3)$$

---

*) См. напр. *Serret*, Cours d'Algèbre supérieure, § 425, *Netto*, Substitutionentheorie § 43.

**) Exercices d'Analyse et de Physique mathématique, T. III.

***) *Sylow*, Théorémes sur les groupes de substitutions, Mathematische Annalen, B. V. Теорема эта изложена у *Netto*: „Substitutionentheorie", §§ 48, 121.

Теорема Зилова даетъ возможность во многихъ случаяхъ изучить строеніе группы, зная только *порядокъ* послѣдней, и потому представляетъ большую важность для теоріи группъ *), въ особенности при современной, совершенно абстрактной, постановкѣ въ ней вопросовъ **). Не смотря на большое значеніе теоремы Зилова, существуетъ мало изслѣдованій *извѣстныхъ* группъ, исходящихъ изъ ея точки зрѣнія.

Въ моей диссертаціи: „Die Anwendung des Sylow'schen Satzes auf die symmetrische und die alternirende Gruppe", Berlin 1895, я сдѣлалъ такое изслѣдованіе для симметрической и знакоперемѣнной группъ. Въ настоящемъ сообщеніи я хочу изложить часть результатовъ, полученныхъ мною, именно приложеніе теоремы Зилова къ симметрической группѣ, которой *степень* (т. е. число буквъ, надъ которыми производятся ея подстановки—„*Grad der Gruppe* по Нетто), есть степень простого числа — p^n. Изучивъ этотъ случай, не трудно, какъ показано въ § 3-мъ вышеупомянутой диссертаціи, изслѣдовать и общій случай группы произвольной степени. Я ограничусь, притомъ, сообщеніемъ только одной изъ методъ, послужившихъ мнѣ для рѣшенія поставленныхъ вопросовъ, именно той, при которой основаніемъ изслѣдованія служитъ *аналитическое изображеніе подстановокъ* (§ 2-ой диссертаціи; другая метода, пользующаяся *описаніемъ* составленія группы $\mathfrak{G}$, изложена въ § 1-мъ).

Извѣстно, что наивысшая степень простого числа p, дѣлящая $m!$, выражается такъ:

$$f=\left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\,.\,.\,.\,.\,.\,.\,.\,.\,. \tag{4}$$

гдѣ вообще $[a]$ означаетъ наибольшее цѣлое число, заключающееся въ a (обозначеніе Кронекера). По теоремѣ Зилова, симметрическая группа порядка $p^n!$ содержитъ подгруппу $\mathfrak{G}$ порядка p^f. Наша задача будетъ состоять прежде всего въ аналитическомъ изображеніи этой группы.

Когда число буквъ, входящихъ въ подстановки группы, есть p^n, буквы эти можно получить, какъ извѣстно ***), снабдивъ какую-ни-

---

*) Кромѣ доказательства Зилова, этой теоремѣ были посвящены многіе другіе труды:

E. Netto. Neuer Beweis eines Fundamentaltheorems aus der Theorie der Substitutionenlehre. Mathematische Annalen, B. 13.

G. Frobenius. Neuer Beweis des Sylow'schen Satzes. Crelle's Journal, B. 100.

G. Frobenius. Ueber die Congruenz nach einem aus 2 endlichen Gruppen gebildeten Doppelmodul. Crelle's Journal, B. 101.

**) Прекрасное (но нѣсколько сжатое) изложеніе основаній такой абстрактной теоріи представляетъ статья Фробеніуса:

G. Frobenius. Ueber endliche Gruppen. Sitzungsberichte der Königl. Pr. Academie der Wissenschaften zu Berlin 21 Februer 1895.

***) См. напр. *Netto*, Substitutionentheorie, § 136. Другой пріемъ обозначенія и аналитическаго изображенія подстановокъ изложенъ у *Serret* въ Cours d'Algébre supérieure, § 478.

будь одну букву u и n индексами: x_1, $x_2 \cdots x_n$ и придавая этимъ индексамъ, независимо другъ отъ друга, всѣ цѣлыя значенія отъ 0 до $p-1$ [или вообще значенія полной системы остатковъ (mod. p)]. Тогда всякая подстановка группы можетъ быть изображена выраженіемъ вида:

$$|x_1, x_2, \cdots x_n \;\; \psi_1(x_1, \cdots x_n), \; \psi_2(x_1, \cdots x_n), \cdots \; \psi_n(x_1, \cdots x_n)|,$$

что означаетъ замѣну x_i черезъ $\psi_i(x_1, \cdots x_n)$, гдѣ $\psi_i(x_1, \cdots x_n)$—надлежащимъ образомъ выбранная функція входящихъ въ нее перемѣнныхъ.

Не трудно видѣть, что и обратно, для того, чтобы выраженіе вышеприведеннаго рода изображало подстановку, необходимо и достаточно, чтобы p^n различнымъ системамъ величинъ $x_1, \cdots x_n$ соотвѣтствовало такое же число различныхъ относительно модуля p значеній функцій $\psi_1, \cdots \psi_n$.

Предположивъ функціи $\psi_1, \cdots \psi_n$ раціональными, цѣлыли и съ цѣлыми коэффиціентами [степень ихъ относительно каждой изъ перемѣнныхъ можно предположить, на основаніи теоремы Fermat'a, не выше $(p-1)$-ой], можно было бы искать болѣе точныхъ условій, которымъ должны удовлетворять эти функціи для того, чтобы изображать подстановку. Однако, задача эта представляетъ громадныя затрудненія и до сихъ поръ болѣе подробно изслѣдованъ только случай $n=1$ *) и случай *линейныхъ подстановокъ* **) вида:

$$s = |x_1, \cdots x_n \;\; a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n, \cdots, a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n|.$$

Было показано, что выраженіе это изображаетъ подстановку всегда, когда опредѣлитель

$$\begin{vmatrix} a_{11} a_{12} \cdots a_{1n} \\ \cdots\cdots \\ \cdots\cdots \\ a_{n1} a_{n2} \cdots a_{nn} \end{vmatrix}$$

не дѣлится на p, и найдено число различныхъ подстановокъ этого рода (т. е. порядокъ группы, ими образуемой):

$$r = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

Аналитическое изображеніе нашей группы порядка p^f, гдѣ

---

*) См. напр. *Serret*. Cours d'Algébre supérieure, §§ 474—478 и 485—488.

**) См. *Netto*. Substitutionentheorie, §§ 137—143. Подробную теорію этихъ подстановокъ можно найти въ книгѣ *C. Jordan*: Traité des substitutions et des équations algébriques.

$$f = p^{p^{n-1}+p^{n-2}+\ldots+p+1} \ldots\ldots\ldots\ldots (5)$$

получается на основаніи слѣдующихъ теоремъ:

I. Выраженіе

$$|x_1, \ldots x_n\, x_1 + \varphi_1(x_2, \ldots x_n), x_2 + \varphi_2(x_3, \ldots x_n), \ldots x_{n-1} + \varphi_{n-1}(x_n), x_n + \alpha|, (6)$$

гдѣ $\varphi_1, \ldots \varphi_{n-1}$ — цѣлыя раціональныя функціи соотвѣтственныхъ перемѣнныхъ съ цѣлыми коэффиціентами (степени не выше $p-1$-ой относительно каждой изъ перемѣнныхъ), а α — цѣлое число, изображаетъ подстановку при произвольныхъ коэффиціентахъ функцій φ и произвольномъ α.

Чтобы доказать это, надо только показать, что двумъ различнымъ системамъ величинъ $x_1, \ldots x_n$ и $x'_1, \ldots x'_n$ соотвѣтствуютъ двѣ различныя системы значеній функцій:

$$x_1 + \varphi_1(x_2, \ldots x_n), \ldots x_{n-1} + \varphi_{n-1}(x_n), x_n + \alpha.$$

Положимъ, что

$$x'_n \equiv x_n, \; x'_{n-1} \equiv x_{n-1}, \ldots x'_{i+1} \equiv x_{i+1} \; (\mathrm{mod.}\, p),$$

но что x'_i не сравнимо съ x_i по модулю p. Тогда получимъ:

$$x'_n + \alpha \equiv x_n + \alpha$$

$$x'_{n-1} + \varphi_{n-1}(x'_n) \equiv x_{n-1} + \varphi_{n-1}(x_n)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$x'_{i+1} + \varphi_{i+1}(x'_{i+2} \ldots x'_n) \equiv x_{i+1} + \varphi_{i+1}(x_{i+2} \ldots x_n).$$

Но

$$x'_i + \varphi_i(x'_{i+1}, \ldots x'_n)$$

не будетъ сравнимо съ

$$x_i + \varphi_i(x_{i+1}, \ldots x_n)$$

по модулю p, такъ какъ

$$\varphi_i(x'_{i+1}, \ldots x'_n) \equiv \varphi_i(x_{i+1}, \ldots x_n) \; (\mathrm{mod.}\, p),$$

а

$$x'_i \text{ не } \equiv x_i \; (\mathrm{mod.}\, p).$$

II. Произведеніе двухъ подстановокъ вида (6):

$$s_1 = | x_1 \dots x_n \, x_1 + \varphi_1(x_2 \dots x_n), \dots x_n + \alpha |$$

и

$$s_2 = | x_1 \dots x_n \, x_1 + \varphi_1^{(1)}(x_2 \dots x_n). \ . x_n + \alpha^{(1)} |$$

есть подстановка того же типа.

Въ самомъ дѣлѣ:

$$s_1 s_2 = \left| \begin{array}{l} x_1 \;\; x_1 + \varphi_1(x_2, \dots x_n) + \varphi_1^{(1)}[x_2 + \varphi_2(x_3 \dots x_n), \dots x_n + \alpha] \\ x_2 \;\; x_2 + \varphi_2(x_3, \dots x_n) + \varphi_2^{(1)}[x_3 + \varphi_3(x_4 \dots x_n), \dots x_n + \alpha] \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ x_{n-1} \;\; x_{n-1} + \varphi_{n-1}(x_n) + \varphi_{n-1}^{(1)}[x_n + \alpha] \\ x_n \;\; x_n + \alpha + \alpha^{(1)} \end{array} \right|$$

т. е.

$$s_1 s_2 = | x_1 \dots x_n \, x_1 + \psi_1(x_2 \dots x_n), x_2 + \psi_2(x_3, \dots x_n), \dots x_{n-1} + \psi_{n-1}(x_n), x_n + \beta |$$

что и тр. док.

III. Двѣ подстановки вида (6) будутъ тождественны только тогда когда всѣ коэффиціенты всѣхъ функцій φ въ одной сравнимы по модулю p съ соотвѣтственными коэффиціентами въ другой.

Теорема эта можетъ быть легче всего доказана при помощи такой леммы:

Если имѣемъ цѣлую раціональную функцію перемѣнныхъ $x_1, x_2, \dots x_m$ съ цѣлыми коэффиціентами, которые не всѣ дѣлятся на p, степени n_i относительно $x_i (i = 1, \dots m)$, при чемъ $n_i \leqq p - 1$, то, придавая всѣмъ перемѣннымъ, независимо другъ отъ друга, значенія $0 . 1, \dots p - 1$, получимъ по крайней мѣрѣ

$$(p - n_1)(p - n_2) \dots (p - n_m)$$

системъ значеній перемѣнныхъ, для которыхъ функція не дѣлится на p *).

Наша функція имѣетъ видъ:

$$\varphi(x_1, \dots x_m) = \sum_{\alpha_m=0}^{\alpha_m=n_m} \dots \sum_{\alpha_1=0}^{\alpha_1=n_1} C_{\alpha_1 \dots \alpha_m} x_1^{\alpha_1} \dots x_m^{\alpha_m} .$$

*) Теорема эта представляетъ простое обобщеніе теоремы Lagrange'a относительно сравненій по простому модулю.

Пусть $C_{\alpha_1'\ldots\alpha'_m}$ будетъ коэффиціентъ, не дѣлящійся на p. Расположимъ въ φ члены слѣдующимъ образомъ:

$$\varphi(x_1,\cdots x_m)=\left(\sum_{\alpha_1=0}^{\alpha_1=n_1} C_{\alpha_1\alpha'_2\ldots\alpha'_m}x_1^{\alpha_1}\right)x_1^{\alpha_2'}\cdots x_m^{\alpha'm}+R(x_1\cdots x_m)$$

гдѣ $R(x_1\cdots x_m)$ заключаетъ всѣ члены φ за исключеньемъ отдѣленной суммы. Изъ извѣстной теоремы Лагранжа для сравненій по простому модулю слѣдуетъ, что можно найти по крайней мѣрѣ $p-n_1$ значеній x_1 не сравнимыхъ между собою по модулю p, для которыхъ

$$\sum_{\alpha_1=0}^{\alpha_1=n_1} C_{\alpha_1\alpha'_2\ldots\alpha'_n}x_1^{\alpha_1}$$

не будетъ дѣлиться на p.

Взявъ одно изъ этихъ значеній для x_1 и подставивъ его въ φ, получимъ функцію отъ $(m-1)$ перемѣнныхъ, въ которой по крайней мѣрѣ одинъ коэффиціентъ (при $x_2^{\alpha'_2}\cdots x_m^{\alpha'_m}$) не дѣлится на p. Очевидно, можно примѣнить къ полученной функціи то же разсужденіе, какъ и къ φ и продолжать этотъ процессъ до тѣхъ поръ, пока не придемъ къ функціи отъ одной перемѣнной x_m, къ которой непосредственно приложима теорема Лагранжа.

Изъ этихъ соображеній очевидна справедливость доказываемой леммы.

Если въ подстановкахъ:

$$s_1=|\,x_1\cdots x_n\, x_1+\varphi_1(x_2\cdots x_n),\cdots x_i+\varphi_i(x_{i+1},\cdots x_n),\cdots x_n+\alpha\,|$$

и

$$s_2=|\,x_1\cdots x_n\, x_1+\varphi_1^{(1)}(x_2\cdots x_n),\cdots x_i+\varphi_i^{(1)}(x_{i+1},\cdots x_n),\cdots x_n+\alpha\,|$$

какіе-либо соотвѣтственные коэффиценты въ функціяхъ φ_i и $\varphi_i^{(1)}$ не сравнимы между собою (mod. p), то разность

$$\varphi_i(x_{i+1}\cdots x_n)-\varphi_i^{(1)}(x_{i+1},\cdots x_n)$$

заключаетъ по крайней мѣрѣ одинъ коэффиціентъ, не дѣлящійся на p; значитъ эта разность, по только что доказанной леммѣ, не можетъ равняться нулю для всѣхъ системъ величинъ $x_1,\cdots x_n$, т. е. подстановки s_1 и s_2 различны, что и тр. док.

Функція $\varphi_{n-i}(x_{n-i+1},\cdots x_n)$, входящая въ подстановку вида (6), имѣетъ видъ:

$$\varphi_{n-i}=\sum_{\alpha_n=0}^{\alpha_n=p-1}\cdots\sum_{\alpha_{n-i+1}=0}^{\alpha_{n-i+1}=p-1} C_{\alpha_{n-i+1},\ldots\alpha_n}x_{n-i+1}^{\alpha_{n-i+1}}\cdots x_n^{\alpha_n}.$$

Число коэффиціентовъ въ ней есть p^i. Если придавать каждому изъ коэффиціентовъ, независимо отъ остальныхъ, значенія $0, 1, \ldots p-1$, то получимъ:

$$p^{p^i}$$

различныхъ функцій. Дѣлая это для $i = 1, 2, \ldots n-1$, получимъ, по теоремѣ III,

$$p^{p^{n-1}+p^{n-2}+\ldots+p+1}$$

различныхъ подстановокъ, образовывающихъ, по теоремѣ II, группу.

Такъ какъ, по теоремѣ Зилова, группы подстановокъ изъ p^n буквъ порядка

$$p^{p^{n-1}+p^{n-2}+\ldots+p+1}$$

подобны между собою, то найденное нами выраженіе

$$s = | x_1 \ldots x_n \; x_1 + \varphi_1(x_2, \ldots x_n), x_2 + \varphi_2(x_3 \ldots x_n), \ldots x_n + \alpha |$$

и есть искомое аналитическое изображеніе подстановокъ группы $\mathfrak{G}$ *).

Всѣ подстановки этой группы могутъ быть составлены, комбинируя слѣдующія:

$$\left.\begin{aligned} s_{1,\alpha_2,\ldots\alpha_n} &= | x_1 \ldots x_n \; x_1 + x_2^{\alpha_2} \ldots x_n^{\alpha_n}, x_2, \ldots x_n | \\ s_{2,\alpha_3,\ldots\alpha_n} &= | x_1 \ldots x_n \; x_1, x_2 + x_3^{\alpha_3} \ldots x_n^{\alpha_n}, x_3, \ldots x_n | \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_{n-1,\alpha_n} &= | x_1 \ldots x_n \; x_1, \ldots x_{m-1} + x_n^{\alpha_n}, x_n | \\ s_n &= | x_1, \ldots x_n \; x_1, \ldots x_{n-1}, x_n + 1 | \\ (\alpha_2, \ldots \alpha_n &= 0, 1, \ldots p-1). \end{aligned}\right\} \ldots \quad (7)$$

Всякая подстановка s группы $\mathfrak{G}$ можетъ быть только единственнымъ образомъ представлена выраженіемъ вида:

$$s = s_n^{i_n} \prod_{\alpha_2,\ldots\alpha_n} s_{1,\alpha_2,\ldots\alpha_n}^{i_{1\alpha_2\ldots\alpha_n}} \, s_{2,\alpha_3,\ldots\alpha_n}^{i_{2\alpha_3\ldots\alpha_n}} \ldots s_{n-1,\alpha_n}^{i_{n-1\alpha_n}} \quad \ldots\ldots\ldots (8)$$

---

*) Для случая $n=2$ это изображеніе дано Зиловымъ въ статьѣ: „Sur les groupes transitifs dont le degré est le carré d'un nombre premier"; Acta mathematica, T. 11.

Группа $\mathfrak{G}$ заключаетъ, какъ извѣстно *), среди своихъ подгруппъ всѣ типы группъ порядковъ p^α ($\alpha \leqq p^{n-1}+p^{n-2}+\ldots+p+1$).

Поэтому выраженія вида:

$$|\,x_1,\ldots x_n\; x_1+\varphi_1(x_2,\ldots x_n),\ldots x_n+\alpha\,|$$

изображаютъ всякую группу порядка p^α и степени p^n ($\alpha \leqq p^{n-1}+p^{n-2}+ +\ldots+p+1$). Въ этихъ группахъ должна быть взята извѣстная часть функцій φ.

Такъ, напримѣръ, одною изъ подгруппъ группы $\mathfrak{G}$ является *группа ариѳметическихъ подстановокъ*, изображаемыхъ выраженіями вида:

$$|\,x_1,\ldots x_n\; x_1+\alpha_1,\; x_2+\alpha_2,\ldots x_n+\alpha_n\,|\;.\;.\;.\;.\;.\;.\;(9)$$

гдѣ $\alpha_1\ldots\alpha_n$ — какія либо изъ чиселъ $0, 1, \ldots p-1$ (порядокъ этой группы равенъ ея степени $=p^n$).

Подстановки вида:

$$|\,x_2,\ldots x_n\; x_1+f_1(x_2\ldots x_n),\, x_2+f_2(x_3\ldots x_n),\ldots x_{n-1}+f_{n-1}(x_n),\, x_n\,|\;(10)$$

гдѣ функціи f такія же, какъ φ, *только не заключаютъ постояннаго члена* тоже образовываютъ группу $\mathfrak{G}'$.

Всѣ подстановки ея не мѣняютъ буквы $u_{0,0,\ldots 0}$. (Не трудно показать, что, назвавъ группу ариѳметическихъ подстановокъ чрезъ $\mathfrak{A}$, получимъ:

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

— $\mathfrak{G}$ есть „*произведеніе*“ $\mathfrak{A}$ и $\mathfrak{G}'$, или „*наименьшее кратное*“ ихъ **).

Въ вышеназванной диссертаціи моей показано, что изображеніе группы $\mathfrak{G}$ можетъ быть получено, взявъ вмѣсто *степеней факторіели*. Тамъ найдены (стр. 19 и слѣд.), съ помощью послѣднихъ, выраженія для подстановокъ, служившихъ прежде для описанія группы $\mathfrak{G}$ (у *Netto* въ „Substitutionentheorie“, § 39, у *Jordan*'а въ „Traité des Substitutions“—§ 41).

Опредѣленіе группы $\mathfrak{H}$ подстановокъ, перемѣщаемыхъ съ $\mathfrak{G}$.

Самымъ простымъ путемъ для построенія этой группы былъ бы слѣдующій:

Положивъ

$$t=|\,x_1,\ldots x_n\;\psi_1(x_1\ldots x_n),\ldots\psi_n(x_1\ldots x_n)\,|$$

и взявъ

$$s=|\,x_1,\ldots x_n\; x_1+\varphi_1(x_2\ldots x_n),\ldots x_n+\alpha\,|,$$

---

*) См. *Netto*, Substitutionentheorie, § 49.

**) Термины проф. Фробеніуса. См. *G. Frobenius*. Ueber endliche Gruppen. Sitzungsberichte der Königl. Pr. Academie der Wissenschaften, 21 Februar 1895.

надо было бы составить

$$t^{-1}st$$

и положить это выраженіе равнымъ нѣкоторой подстановкѣ изъ группы $\mathfrak{G}$

$$s_1 = | x_1, \ldots x_n \; x_1 + \theta_1(x_2 \ldots x_n), \ldots x_n + \alpha |.$$

Отсюда можно было бы найти извѣстныя условія для функцій ψ, входящихъ въ t.

Путь этотъ ведетъ, однако, къ слишкомъ длиннымъ вычисленіямъ (даже если брать за s простѣйшія подстановки группы $\mathfrak{G}$). Эти вычисленія могутъ быть значительно сокращены съ помощью слѣдующихъ теоремъ изъ общей теоріи подстановокъ:

I. Положимъ, что группа $\mathfrak{C}$ состоитъ изъ подстановокъ, перемѣщаемыхъ съ группой $\mathfrak{A}$ и $\mathfrak{B}$ есть подгруппа $\mathfrak{A}$, образованная всѣми подстановками $\mathfrak{A}$, перемѣщаемыми со всѣми подстановками $\mathfrak{A}$. Тогда группа $\mathfrak{B}$ перемѣщаема со всѣми подстановками группы $\mathfrak{C}$ *).

Назовемъ чрезъ A какую-либо подстановку изъ группы $\mathfrak{A}$, чрезъ B какую-либо подстановку группы $\mathfrak{B}$ и чрезъ C группы $\mathfrak{C}$. По предположенію

$$AB = BA$$

для всякихъ подстановокъ A и B. Отсюда получаемъ чрезъ *преобразованіе* (Transformation) обѣихъ частей подстановкой C:

$$C^{-1}ABC = C^{-1}BAC$$

или

$$C^{-1}ACC^{-1}BC = C^{-1}BCC^{-1}AC.$$

Подстановка $C^{-1}BC$ принадлежитъ группѣ $\mathfrak{A}$ (такъ какъ B принадлежитъ группѣ $\mathfrak{A}$, а $\mathfrak{C}$ состоитъ изъ подстановокъ, перемѣщаемыхъ съ $\mathfrak{A}$).

Если брать за A всѣ подстановки группы $\mathfrak{A}$, то выраженіе $C^{-1}AC$ проходитъ значенія всѣхъ подстановокъ группы $\mathfrak{A}$. Поэтому найденное равенство показываетъ, что подстановка $C^{-1}BC$ тоже принадлежатъ къ числу подстановокъ $\mathfrak{A}$, перемѣщаемыхъ со всѣми подстановками $\mathfrak{A}$, т. е. къ группѣ $\mathfrak{B}$; а значитъ группа $\mathfrak{B}$ перемѣщаема со всѣми подстановками $\mathfrak{C}$, что и тр. док.

Обобщеніемъ этой теоремы является слѣдующая:

II. Положимъ, что имѣемъ 4 группы: $\mathfrak{D}$, $\mathfrak{C}$, $\mathfrak{B}$ и $\mathfrak{A}$, изъ которыхъ каждая послѣдующая есть подгруппа предъидущихъ. Предположимъ, что группы $\mathfrak{A}$ и $\mathfrak{B}$ перемѣщаемы со всѣми подстановками $\mathfrak{D}$. Пусть $\mathfrak{C}$ есть

---

*) Теорема эта употребляется (безъ доказательства) въ статьѣ Зилова: „Sur les groupes transitifs dont le dégré est le carré d'un nombre premier"; Acta mathematica, T. 11.

группа, образованная всѣми подстановками $\mathfrak{D}$, перемѣщаемыми съ подстановками $\mathfrak{B}$ „до подстановокъ" $\mathfrak{A}$ *). Тогда группа $\mathfrak{C}$ будетъ перемѣщаема съ подстановками $\mathfrak{D}$.

По опредѣленію перемѣщаемости „до подстановокъ" извѣстной группы, имѣемъ:

$$CB = BCA$$

гдѣ C, B и A какія-либо изъ подстановокъ соотвѣтственныхъ группъ $\mathfrak{C}$, $\mathfrak{B}$ и $\mathfrak{A}$.

Преобразовывая это равенство какой-либо подстановкой D изъ $\mathfrak{D}$, получимъ:

$$D^{-1}CBD = D^{-1}BCAD$$

или

$$(D^{-1}CD)(D^{-1}BD) = (D^{-1}BD)(D^{-1}CD)(D^{-1}AD) =$$
$$= (D^{-1}BD)(D^{-1}CD)A'$$

такъ какъ, по предположенію, группа $\mathfrak{A}$ перемѣщаема съ подстановками группы $\mathfrak{C}$. Выраженіе $D^{-1}BD$ проходитъ, съ измѣненіемъ B, значенія всѣхъ подстановокъ группы $\mathfrak{B}$. Найденное равенство показываетъ, что подстановка $D^{-1}CD$ (принадлежащая къ $\mathfrak{D}$), перемѣщаема съ подстановками группы $\mathfrak{B}$ до подстановокъ изъ $\mathfrak{A}$. Отсюда слѣдуетъ, что $D^{-1}CD$ принадлежитъ $\mathfrak{C}$, т. е. что группа $\mathfrak{C}$ перемѣщаема съ подстановками D, что и тр. док.

Въ нашей группѣ $\mathfrak{G}$ подстановки, перемѣщаемыя со всѣми подстановками ея, будутъ слѣдующія:

$$|x_1, \ldots x_n \; x_1 + \alpha, x_2, \ldots x_n|,$$
$$(\alpha = 0.1, \ldots p - 1).$$

---

*) Если $\mathfrak{A}$ есть подгруппа $\mathfrak{B}$ и $\mathfrak{B}$ подгруппа $\mathfrak{C}$, то говорятъ, что подстановки группы $\mathfrak{C}$ перемѣщаемы со всѣми подстановками $\mathfrak{B}$ до подстановокъ $\mathfrak{A}$, когда для всякой подстановки B изъ $\mathfrak{B}$ и для всякой подстановки C изъ $\mathfrak{C}$ исполнено условіе:

$$BC = CBA,$$

гдѣ A есть нѣкоторая подстановка группы $\mathfrak{A}$. Не трудно видѣть, что подстановки C удовлетворяющія этому условію, образовываютъ группу; изъ равенствъ:

$$BC = CBA \text{ и } BC' = C'BA'$$

слѣдуетъ:

$$B(CC') = CBAC' = CBC'A'' = CC'BA'A'' = (CC')BA''',$$

т. е. и CC' перемѣщаема съ B до подстановки изъ $\mathfrak{A}$.

Въ самомъ дѣлѣ, группа $\mathfrak{G}$ содержитъ въ себѣ группу ариѳметическихъ подстановокъ. Значитъ подстановки, перемѣщаемыя со всѣми подстановками $\mathfrak{G}$, заключаются среди такихъ:

$$s = |x_1, \dots x_n \, x_1 + a_{12}x_2 + \dots + a_{1n}x_n + \alpha_1, x_2 + a_{23}x_3 +$$
$$+ \dots + a_{2n}x_n + \alpha_2, \dots x_n + \alpha_n|.$$

Сравнивая выраженія:

$$s.|x_1, \dots x_n \, x_1, \dots x_i + \beta_i, \dots x_n| =$$
$$= |x_1, \dots x_i, \dots x_n \, x_1 + a_{12}x_2 + \dots + a_{1n}x_n + \alpha_1, \dots x_i + a_{ii+1}x_{i+1} +$$
$$+ \dots + \alpha_i + \beta_i, \dots x_n + \alpha_n|$$

и

$$|x_1 \dots x_n \, x_1, \dots x_i + \beta_i, \dots x_n|.s =$$
$$= |x_1, \dots x_i, \dots x_n \, x_1 + a_{12}x_2 + \dots + a_{1n}x_n + \alpha_1 + a_{1i}\beta_i, \dots$$
$$\dots x_i + a_{ii+1}x_{i+1} + \dots + \alpha_i + \beta_i, \dots x_n + \alpha_n|,$$
$$(i = 2, 3, \dots n),$$

легко убѣдиться, что всѣ коэффиціенты

$$a_{ik} \begin{pmatrix} i = 1, 2, \dots n \\ k = 2, 3, \dots n \end{pmatrix}$$

должны быть равны нулю. Для перемѣщаемости съ подстановками

$$|x_1, \dots x_n \, x_1 + x_2, x_2, \dots x_n|$$
$$|x_1, \dots x_n \, x_1 + x_3, x_2, \dots x_n|$$
$$\dots\dots\dots\dots\dots$$

числа

$$\alpha_i \, (i = 2, 3, \dots n)$$

должны равняться нулю. Подстановки

$$|x_1, \dots x_n \, x_1 + \alpha_1, x_2, \dots x_n| \quad \dots\dots\dots (11)$$

дѣйствительно перемѣщаемы со всѣми подстановками группы $\mathfrak{G}$. Назовемъ группу, ими образовываемую, черезъ $\mathfrak{G}_1$. Пусть

$$H = |x_1, \dots x_n \, f_1(x_1, \dots x_n), \dots f_n(x_1 \dots x_n)|$$

будетъ какая-либо подстановка группы $\mathfrak{H}$. Составимъ

$$H^{-1}.\left| x_1, \dots x_n\, x_1 + 1, x_2, \dots x_n \right|.H.$$

По первой изъ только что доказанныхъ леммъ будетъ

$$H^{-1}\left| x_1 \dots x_n x_1 + 1, x_2, \dots x_n \right| H = \left| x_1, x_2, \dots x_n x_1 + \alpha, x_2, \dots x_n \right|.$$

Отсюда получаются сравненія:

$$f_1(x_1+1, x_2, \dots x_n) - f_1(x_1, \dots x_n) \equiv \alpha \,(\mathrm{mod.}\, p),$$

$$f_i(x_1+1, x_2, \dots x_n) - f_i(x_1, \dots x_n) \equiv 0 \,(\mathrm{mod.}\, p),$$

$$(i = 2, 3, \dots n).$$

Изъ этихъ сравненій можно заключить, что x_1 входитъ въ f_1 линейно и съ постояннымъ коэффиціентомъ и вовсе не входитъ въ остальныя функціи $f_i, (i=2, \dots n)$.

Значитъ, подстановки группы $\mathfrak{H}$ имѣютъ видъ:

$$H = \left| x_1, \dots x_n a_1 x_1 + f_1^{(1)}(x_2, \dots x_n), f_2(x_2 \dots x_n), \dots f_n(x_2 \dots x_n) \right|.$$

Подстановки такого вида перемѣщаемы съ подгруппой $\mathfrak{G}_2$ группы $\mathfrak{G}$, образованной подстановками вида:

$$G_2 = \left| x_1 \dots x_n x_1 + \varphi_1(x_2 \dots x_n), x_2, \dots x_n \right| \;.\;.\;.\;.\;. \quad (12)$$

гдѣ за φ_1 берутся всѣ функціи, различныя относительно модуля p. Въ самомъ дѣлѣ, имѣемъ:

$$\left| x_1, \dots x_n x_1 + \varphi_1(x_2 \dots x_n), x_2, \dots x_n \right| H = \left| x_1, \dots x_n\, x_1 + f_1(x_2 \dots x_n) + \right.$$
$$\left. + \varphi_1(x_2 \dots x_n), x_2 + f_2(x_3 \dots x_n), \dots x_n + f_n(x_2, \dots x_n) \right|$$

и

$$H.\left| x_1, \dots x_n\, x_1 + \varphi_1(x_2 \dots x_n), x_2, \dots x_n \right| = \left| x_1, \dots x_n\, x_1 + f_1(x_2 \dots x_n) + \right.$$
$$+ \varphi_1[x_2 + f_2(x_2 \dots x_n), \dots x_n + f_n(x_2 \dots x_n)], x_2 + f_2(x_2 \dots x_n), \dots$$
$$\left. \dots x_n + f_n(x_2, \dots x_n) \right| =$$
$$= \left| x_1, \dots x_n\, x_1 + f_1(x_2 \dots x_n) + \varphi_1(x_2, \dots x_n), x_2 + f_2(x_3 \dots x_n), \dots \right.$$
$$\left. \dots x_n + f_n(x_2 \dots x_n) \right| \cdot \left| x_1 \dots x_n\, x_1 + \psi_1(x_2 \dots x_n), x_2 \dots x_n \right|,$$

гдѣ

$$\psi_1(x_2 \dots x_n) = \varphi_1[x_2 + f_2(x_2 \dots x_n), \dots x_n + f_n(x_2 \dots x_n)] - \varphi_1(x_2 \dots x_n).$$

Изъ этихъ равенствъ слѣдуетъ:

$$HG_2 = G_2 HG_2',$$

т. е.

$$H^{-1} G_2 H = G_2'',$$

что и доказываетъ перемѣщаемость подстановокъ H съ групой $\mathfrak{G}_2$.

Съ другой стороны, не трудно убѣдиться, что група $\mathfrak{G}_3$ подстановокъ вида

$$G_3 = |\, x_1, \ldots x_n \; x_1 + \varphi_1(x_2 \ldots x_n),\, x_2 + \alpha,\, x_3 \ldots x_n \,| \quad . \quad . \quad (13)$$

гдѣ за φ_1 берутся всѣ функціи, различныя относительно модуля p, а за α числа $0, 1, \ldots p-1$, есть група, образованная подстановками $\mathfrak{G}$, перемѣщаемыми со всѣми подстановками $\mathfrak{G}$ до подстановокъ групы $\mathfrak{G}_2$.

Поэтому групы $\mathfrak{H}, \mathfrak{G}, \mathfrak{G}_3, \mathfrak{G}_2$ удовлетворяютъ условіямъ леммы II, т. е. група $\mathfrak{G}_3$ должна быть перемѣщаема съ подстановками $\mathfrak{H}$.

Взявъ подстановку

$$G_3' = |\, x_1, \ldots x_n \; x_1,\, x_2 + 1,\, x_3, \ldots x_n \,|$$

и составивъ

$$H^{-1} G_3' H,$$

получимъ, на основаніи только что найденнаго, сравненія:

$$f_2(x_2 + 1, x_3, \ldots x_n) - f_2(x_2, \ldots x_n) \equiv \alpha \,(\mathrm{mod.}\, p),$$

$$f_i(x_2 + 1, x_3, \ldots x_n) - f_i(x_2, \ldots x_n) \equiv 0 \,(\mathrm{mod.}\, p),$$

$$(i = 3, 4, \ldots n),$$

изъ которыхъ, какъ и раньше, найдемъ что x_2 можетъ входить въ f_2 только линейно и съ постояннымъ коеффиціентомъ, и что оно не входитъ въ остальныя $f_i, (i = 3, \ldots n)$, т. е. что подстановки групы $\mathfrak{H}$ имѣютъ видъ

$$H_1 = |\, x_1, \ldots x_n \; a_1 x_1 + f_1^{(1)}(x_2, \ldots x_n),\, a_2 x_2 + \\ + f_2^{(1)}(x_3, \ldots x_n),\, f_3(x_3 \ldots x_n), \ldots f_n(x_3 \ldots x_n) \,|.$$

Подстановки этого вида перемѣщаемы съ подгрупной $\mathfrak{G}_4$ групы $\mathfrak{G}$ состоящей изъ подстановокъ вида:

$$G_4 = |\, x_1, \ldots x_n \; x_1 + \varphi_1(x_2 \ldots x_n),\, x_2 + \varphi_2(x_3 \ldots x_n),\, x_3, \ldots x_n \,| \quad . \quad (14)$$

гдѣ за φ_1 и φ_2 берутся всѣ различныя относительно модуля p функціи соотвѣтственныхъ перемѣнныхъ (перемѣщаемость эта доказывается совершенно такъ же, какъ для $\mathfrak{G}_2$).

Не трудно найти, что группа $\mathfrak{G}_5$, составленная изъ подстановокъ

$$G_5 = |x_1, \ldots x_n\, x_1 + \varphi_1(x_2 \ldots x_n), x_2 + \varphi_2(x_3, \ldots x_n), x_3 + \alpha, x_4, \ldots x_n| \quad (15)$$

есть группа подстановокъ $\mathfrak{G}$, перемѣщаемыхъ со всѣми подстановками $\mathfrak{G}$ до подстановокъ группы $\mathfrak{G}_4$. Примѣняя къ $\mathfrak{H}$, $\mathfrak{G}$, $\mathfrak{G}_5$, $\mathfrak{G}_4$ нашу лемму II, найдемъ, подобно предъидущему, что f_3 содержитъ x_3 линейно съ постояннымъ коеффиціентомъ и что функціи $f_i\,(i = 4, \ldots n)$ не содержатъ x_3.

Заключеніемъ отъ $k-1$ къ k докажемъ, что подстановки $\mathfrak{H}$ имѣютъ видъ *):

$$H = |x_1, \ldots x_n a_1 x_1 + \Phi_1(x_2, \ldots x_n), a_2 x_2 + \Phi_2(x_3 \ldots x_n), \ldots a_n x_n + \alpha|. \quad (16)$$

Такая подстановка есть произведеніе подстановки изъ группы $\mathfrak{G}$ и подстановки вида

$$H' = |x_1, \ldots x_n\, a_1 x_1, \ldots a_n x_n| \quad \ldots \ldots \ldots (17)$$

По теоремѣ относительно линейныхъ подстановокъ, приведенной въ началѣ сообщенія, выраженіе это изображаетъ подстановку при

$$a_i = 1, 2, \ldots p-1, \; (i = 1, 2, \ldots n). \quad \ldots \ldots \ldots (18)$$

Такимъ образомъ получимъ $(p-1)^n$ подстановокъ H', образовывающихъ группу $\mathfrak{H}'$. Комбинируя каждую изъ этихъ подстановокъ съ каждой изъ подстановокъ группы $\mathfrak{G}$, получимъ

$$h = p^{p^{n-1}+p^{n-2}+\ldots+p+1}(p-1)^n \quad \ldots \ldots \ldots (19)$$

различныхъ подстановокъ, образовывающихъ группу $\mathfrak{H}$ (группа $\mathfrak{H}$ есть *произведеніе* или „наименьшее краткое" группъ $\mathfrak{G}$ и $\mathfrak{H}'$).

Число различныхъ группъ $\mathfrak{G}$, заключенныхъ въ симметрической группѣ степени p^n, найдется изъ формулы (3):

$$N = \frac{p^n!}{p^{p^{n-1}+p^{n-2}+\ldots+p+1}(p-1)^n} \quad \ldots \ldots \ldots (20)$$

---

*) Въ диссертаціи моей сдѣлано подробное изслѣдованіе группы $\mathfrak{G}$ относительно перемѣщаемости подстановокъ ея подгруппъ, уясняющее нахожденіе группы $\mathfrak{H}$. Руководящей мыслью этого изслѣдованія служилъ принципъ классификаціи группъ, высказанный Joung'омъ въ статьѣ: „On the Determination of the Groups whose Order is a Power of a Prime". American Journal of the Mathematics 1893.

Не трудно показать, что число это дѣйствительно сравнимо съ единицей по модулю p. Членъ не дѣлящійся на p въ выраженіи для N (по раздѣленіи на знаменателя) есть

$$(p-1)^{p^{n-1}+p^{n-2}+\dots+p+1-n}\left[(p-2)!\right]^{p^{n-1}+p^{n-2}+\dots+p+1}.$$

Но изъ теоремы Вильсона слѣдуетъ, что

$$(p-2)! \equiv +1 \,(\mathrm{mod.}\, p)\,,$$

а число

$$p^{n-1}+p^{n-2}+\dots+p+1-n$$

есть четное для всякаго нечетнаго p. Поэтому для нечетнаго p

$$N \equiv +1 \,(\mathrm{mod.}\, p)$$

(для $p=2$ это очевидно).
