Третя частина.

Рішимі рівнаня.

XI. Рішимі рівнаня первого степеня.

§. 98. Остатне твердженє попереднього розділу вказує, як можна зредукувати проблєм розвязки альґебраічних рівнань. Іменно, коли степень рівнаня є зложений

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\nu^{\alpha_\nu},$$

($p_1, p_2, \ldots, p_\nu$ перві числа, ріжні між собою), то розвязку рівнаня степеня n можна звести до ряду рівнань степенів $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_\nu^{\alpha_\nu}$, — отже ми маємо займити ся типовим проблємом: знайти і розвязати рішимі рівнаня степеня p^ν, де p є числом первим.

Коли рівнанє

$$f(x) = 0 \qquad (1)$$

є рішиме, то його ґрупа G називаєть ся теж рішима; вона мусить сповнювати ось такі вимоги: 1) мусить бути перехідна, бо в противнім разї рівнанє було би зведиме; 2) мусить бути первісна, бо приймаємо, що рівнанє має найпростїйшу форму, отже не можна його вважати результатом елімінації, вказаної в §. 90; 3) мусить мати ряд зложеня о первих показчиках. Отсей ряд складаєть ся з таких членів, що кождий з них є найбільшою (визначною) підґрупою попереднього; кожда ґрупа є перемінна аж по субституції слїдуючого члена, а остатня ґрупа є зовсїм перемінна, т. зн. Абелева.

§. 97. Найпростїйший є той випадок, що $\alpha = 1$, отже $n = p$, т. зн. степень рівнаня є первий. Ми бачили, що корінї такого рівнаня можемо представити при помочи невимірностий

$$\left.\begin{aligned} V_\nu^{p_\nu} &= F_\nu(R), \\ V_{\nu-1}^{p_{\nu-1}} &= F_{\nu-1}(R;\ V_\nu), \\ & \\ V_1^{p} &= F_1(R;\ V_\nu, V_{\nu-1}, \ldots, V_2) \end{aligned}\right\} \qquad (2)$$

в формі:

$$\left.\begin{aligned} x_1 &= G_0 + V_1 + G_1 V_1^2 + \ldots + G^{p-1} V_1^{p-1}, \\ x_2 &= G_0 + \omega V_1 + G_2 \omega^2 V_1^2 + \ldots + G_{p-1} \omega^{p-1} V_1^{p-1}, \\ & \\ x_p &= G_0 + \omega^{p-1} V_1 + G_2 \omega^{2(p-1)} V_1^2 + \ldots + G_{p-1} \omega^{(p-1)^2} V_1^{p-1}, \end{aligned}\right\} \quad (3)$$

де ω є p-тим корінем з одиниці.

Заступаючи кожду з невимірностий V величинами $\omega^{\mu} V$, одержимо замість V_1 вираженє $G_{\mu}\omega^{k\mu} V_1^{\mu}$; примінюючи те до корінів рівнаня побачимо, що така переміна переводить тільки один корінь в другий, отже цілости системи (3) не може змінити. З того слідує, що всї такі субституції, які викликують згадану зміну, належать до ґрупи G рівнаня (1).

Ужиймо такої субституції, яка переводить V_1 в ωV_1, т. є

$$| \; V_1 \quad \omega V_1 \; | \; ; \tag{4}$$

вона переведе x_1 в x_k, x_2 в $x_{k+1}, \ldots$, x_p в $_{k+p-1}$, отже є рівнозначна з субституцією

$$| \; x_{\mu} \quad x_{\mu+k-1} \; | \; (mod. \; p), \tag{4a}$$

Беручи самі показчики незвісних, можемо написати ту субституцію в такій найпростїйшій формі:

$$g = | \; z \quad z + 1 \; | \; , \tag{5}$$

бо кожду иншу субституцію виду (4a) можемо представити як степень субституції g. Субституція (5) є циклїчна; ми назвали її також аритметичною. Її періода дає циклїчну ґрупу порядку p, якої не можна вже розложити на підґрупи; назвім ту підґрупу M; вона пересуває всї корінї рівнаня. Вона є також переміна, отже буде стояти в ряді зложеня ґрупи G на остатнім місці перед 1. З того слідує, що кожда рішима ґрупа степеня p мусить містити в собі циклїчну ґрупу як підґрупу.

§. 100. Шукаймо дальших субституцій ґрупи G. Можемо се робити на два способи; 1) або шукати субституції, які не пересувають всїх корінів, тільки деякі, 2) або брати під розвагу функції, що належать до ґрупи M, і їх ріжні вартости.

Субституції g пересувають всї корінї рівнаня (1). Шукаймо тепер таких субституцій, які змінюють $p - 1$ корінїв, а один лишають незмінний. Приймім, що якась переміна в V не змінює коріня x_{α}, а всї другі корінї пересуває, отже $x_{\alpha+1}$ переводить впр. в $x_{\alpha+\beta}$ ($\beta = | = 1$). Се значить, що коли

$$V_1 \text{ переходить в } G_{\mu}\omega^{k\mu} V_1^{\mu}, \text{ то}$$

$$\omega^{\alpha-1} V \text{ перейде в } G_{\mu}\omega^{k\mu+\alpha-1} V_1^{\mu},$$

а з того виходило би, що вираженє на x_{α} мусїло би містити в собі член $G_{\mu}(\omega^{\alpha-1} V_1)^{\mu}$, який переходить в инший член того самого коріня, т. є в $G_{\mu}\omega^{k\mu+\alpha-1} V_2^{\mu}$. Порівнуючи виложники при ω, маємо:

$$k_\mu + \alpha - 1 \equiv \mu(\alpha - 1) \ (mod.\ p.),$$

або

$$k_\mu \equiv (\mu - 1)(\alpha - 1) \ (mod.\ p.) \qquad (6)$$

Та сама переміна переведе $x_{\alpha+1}$ в $x_{\alpha+\beta}$, отже дають:

$$G_\mu \omega^{k+\alpha} V_{1\mu} = G_\mu \omega^{\mu(\alpha+\beta-1)} \ V_1{}^\mu,$$

т. зн.

$$k\mu + \alpha \equiv \mu(\alpha + \beta - 1) \ mod.\ p) \qquad (7).$$

З обох тих конґруенцій виходить:

$$\beta\mu \equiv 1 (mod.\ p.),$$

і

$$k \equiv (\alpha - 1)(1 - \beta) \ (mod.\ p). \qquad (8)$$

Рівної переміни мусить зазнати кождий инший корінь; нпр. x_γ перейде в таке x_δ, що член

$$\omega^{\gamma-1} V_1 \text{ перейде в } G_\mu \omega^{k\mu+\gamma-1} V_1{}^\mu = G_\mu \omega^{\mu(\delta-1)} V_1{}^\mu;$$

вставивши тут вартість на k, одержимо:

$$k\mu + \gamma - 1 \equiv \mu(\alpha - 1)(1-\beta) + \gamma - 1 \equiv \mu[(\alpha - 1)(1 - \beta) + \beta(\gamma - 1)] \equiv$$
$$\mu[(\alpha - 1) + \beta(\gamma - \alpha)] \ mod.\ p.),$$

а се має давати $\mu(\delta - 1)$, отже

$$\delta \equiv \alpha(1 - \beta) + \beta\gamma. \qquad (mod.\ p.) \qquad (9)$$

Ту субституцію можемо написати так;

$$t_0 = | \ \gamma \quad \beta\gamma + \alpha(1 - \beta) \ | \ ;$$

помноживши її знаною вже субституцією $g^{-\alpha(1-\beta)}$, одержимо

$$t = | \ \gamma \quad \beta\gamma \ | \ ;$$

β може приймати всї вартости від 1 до $p - 1$; 0 і p є виключені, бо такі субституції не мали би значіня. Можемо проте написати на місцї β первісний корінь з числа p; тодї субституція t матиме можливо найпростїйшу форму:

$$t = | \ z \quad \varrho z \ | \ ; \qquad (10)$$

Її порядок є $p - 1$. Вона змінює $p - 1$ коріньів: $x_1, x_2, \ldots, x_{p-1}$, а корінь x_p лишає незмінений.

101. Коли-б ми хотїли шукати дальше таких субституцій, які лишають більше ніж один корінь незмінений, то переконаємо ся, що такі субституції лишають всї корінї незмінені. Приймім, що якась субституція не змінює корінів x_α і x_β; тодї побіч реляції (6) мусить істнувати ще анальоґічна

$$k\mu \equiv (\mu - 1)(\beta - 1) \ (mod.\ p). \qquad (6a)$$

Вони обі мусять істнувати рівночасно; $\alpha \neq \beta$. З того слїдує: $\mu = 1$, $k = 0$, т. зн., що та субституція **переводить** V_1 **в себе само, отже не перемінює нї одного коріня в инший.** Так само заховували-б ся субституції, що не змінюють трьох, чотирох etc. корінів.

Инакших субституцій не можна брати під увагу, бо вони вже змінювали би **вартости** поодиноких корінїв. Отже ґрупа G складаєть ся з аритметичних і ґеометричних субституцій (5) і (10), т. зн. є **метациклїчна** порядку $(p-1)p$. Длятого то називаємо рішимі рівнаня первого степеня також **метациклїчними**; те означене перенесемо опісля на рівнаня зложених степенїв.

Метациклїчна ґрупа G є дїйсно **рішима**, т. зн. сповнює вимоги §. 98. Вона є перехідна і первісна, бо неможливий є подїл p корінів на системи. Її ряд зложеня має самі перві показчики, а про се переконуємо ся так:

Найнизша ґрупа в ряді зложеня є M порядку p. Розложім число $p-1$ на перві чинники,

$$p-1 = k_1 k_2 \ldots k_\nu\,; \tag{11}$$

числа $k_1, k_2, \ldots, k_\nu$ можуть бути рівні або ріжні. Утворім тепер частинну ґрупу з субституцій

$$t_\nu = t^{\frac{p-1}{k_\nu}} = \left| z \quad \varrho^{\frac{p-1}{k_\nu}} z \right| \tag{12}$$

і з M; назвім ту ґрупу G_ν. Вона буде попереджувати ґрупу в ряді зложеня, бо її субституції є перемінні аж по g:

$$g^{-1} t_\nu g = | z+1 \quad z | \; \left| z \quad \varrho^{\frac{p-1}{k_\nu}} z \right| \; | z \quad z+1 | = \left| z+1 \quad \varrho^{\frac{p-1}{k_\nu}} z + 1 \right|$$

$$= \left| z \quad \varrho^{\frac{p-1}{k_\nu}} z + 1 - \varrho^{\frac{p-1}{k_\nu}} \right| = t_\nu g'\,;$$

$$t^{-1} t_\nu t = | \varrho z \quad z | \,.\, \left| z \quad \varrho^{\frac{p-1}{k_\nu}} z \right| \; | z \quad \varrho z | = \left| \varrho z \quad \varrho^{\frac{p-1}{k_\nu}+1} z \right| = \left| z \quad \varrho^{\frac{p-1}{k_\nu}} z \right| = t_\nu.$$

Порядок ґрупи $G_{\nu-1}$ є добутком з порядкових чисел складових субституцій; порядок субституції t_ν є k_ν, бо $t_\nu^{k_\nu} = 1$, отже порядок ґрупи $G_{\nu-1}$ є $r_{\nu-1} = k_\nu \,.\, p$.

Показчик ґруп $G_{\nu-1}$ і M є k_ν, отже перве число.

Тепер творимо дальшу частинну ґрупу з попередньої і з нової субституції

$$t_{\nu-1} = t^{\frac{p-1}{k_\nu k_{\nu-1}}} = \left| z \quad \varrho^{\frac{p-1}{k_\nu k_{\nu-1}}} z \right| \tag{13}$$

порядку $k_\nu k_{\nu-1}$, бо $t_{\nu-1}{}^{k_{\nu-1}} = t_\nu$, $t_{\nu-1}{}^{k_{\nu-1}} = t_\nu{}^{k_\nu} = 1$. Ґрупа $G_{\nu-2} = \{G_{\nu-1}, t_{\nu-1}\}$ буде стояти в рядї зложеня перед $G_{\nu-2}$; її порядок буде $r_{\nu-1}, = k_{\nu-1}\ k_\nu\ p$, а показчик $k_{\nu-1}$, отже знов перве число.

Поступаючи так дальше, творимо ґрупи:

$$G_{\nu-3} = \{G_{\nu-2}, t_{\nu-2}\};\ t_{\nu-2} = t^{\overline{k_\nu k_\nu k_{\nu-1} k_{\nu-2}}^{\,p-1}};\ r_{\nu-3} = k_{\nu-2} . k_{\nu-1} . k_\nu . p;$$

$$G_{\nu-4} = \{G_{\nu-3}, t_{\nu-3}\};\ t_{\nu-3} = t^{\overline{k_\nu k_{\nu-1} k_{\nu-2} k_{\nu-3}}^{\,p-1}};\ r_{\nu-4} = k_{\nu-3} . k_{\nu-2} . k_{\nu-1} . k_\nu p;$$

$$G_1 = \{G_2, t_2\};\ t_2 = t^{\overline{k_\nu k_{\nu-1} \ldots k_2}^{\,p-1}};\ r_1 = k_2\ k_3 \ldots k_\nu\ p:$$

$$G_0 = \{G_1, t_1\};\ t_1 = t \qquad ;\ r_0 = k_1 k_2 \ldots k_\nu p = p\ (p-1)$$

Остатня ґрупа є нашою ґрупою G, отже її ряд зложеня виглядає так:

$$G,\ G_1,\ G_2, \qquad G_{\nu-1},\ M,\ 1, \tag{14}$$

а ряд показчиків є

$$k_1,\ k_2,\ k_3, \qquad .,\ k_\nu,\ p,$$

отже ґрупа G є рішима.

§. 102. Між коріннями рішимого рівнаня первого степеня панує реляція, що двома довільними коріннями можна представити всї инші. Бо коли до обсягу R долучимо два корінї, нпр. x_α і x_β, то ґрупа G зредукує ся до тої підґрупи, яка не змінює тих двох корінїв, т. є до 1. Огже по тім долученю є вже знана кожда функція тих двох корінїв; всї инші корінї будуть вимірними функціями в обсягу $(R;\ x_\alpha,\ x_\beta)$:

$$x_k = \psi_k\ (x_\alpha,\ x_\beta)\ (k = 1,\ 2, \qquad .,\ p). \tag{15}$$

Навпаки, коли між коріннями панує така реляція, то рівнане є рішиме: α і β мусять бути два довільні корінї. З того слїдує, що ґрупа G того рівнаня є перехідна; вона не має крім 1 инших субституцій, які не змінювали-б α і β. Отже ґрупа, яка змінює всї елементи, має $p-1$ субституцій, а є вона циклїчна, бо в противнім разї деякі її степенї не змінювали би всіх елементів. Та циклїчна ґрупа є утворена з періоди субституції

$$g = |\ z \quad z+1\ |$$

Поза тим є в G $p-1$ таких субституцій, які пересувають тільки $p-1$ елементів; приймім, що субституція t не змінює елемента x_p, отже мусить бути $t^{-1}st = s^\alpha$, т. зн., що t викликує таку зміну:

$$\begin{pmatrix} x_1 & x_2 & & x_p \\ x_\alpha & x_{2\alpha} . & & x_p \end{pmatrix}$$

Такою субституцією є

$$t = | u \quad au$$

Отже ґрупа G є ідентична з нашою рішимою ґрупою.

Рівнаня первого степеня, які мають ту прикмету, що кождий з корінїв можна представити як вимірну функцію двох котрих небудь инших, називають ся рівнанями Galois*). Кожде рішиме рівнане первого степеня є рівнанем Galois. Рівнаня Абеля є спеціяльним родом тих рівнань.

Коли в обсягу R є два корінї рівнаня (1), нпр. x_α і x_β дійсні, то з (15) слїдує, що всї инші корінї мусять бути дійсні. Коли-ж маємо до дїла з одним сполученим (мнимим) корінем, нпр. x_α, то одержимо всї злучені корінї з виїмком одного. Отже рівнане первого степеня має або один або всї корінї дійсні.

§. 104. Тепер займемо ся розвязкою рівнаня первого степеня. Утворім ресольвенту Lagrange'а для рівнаня (1):

$$\xi = x_1 + \omega^2 x_3 + \ldots + \omega^{p-1} x_p;$$

для субституції g вона перейде в $\xi\omega^{-1}$, отже циклїчна функція $\xi^p = \varphi_1$ буде незмінна для аритметичної ґрупи M. Инші субституції ґрупи G переведуть φ_1 в спряжені вартости: $\varphi_1, \varphi_2, \varphi_3, \quad \varphi_k$. Виконуючи серед функцій φ субституції ґрупи G на коріннях x, одержимо такі переміни вартостий φ, які дадуть ґрупу Γ, ізоморфну з ґрупою G; вона буде належати до рівнаня

$$F(\varphi) = \prod_{i=1}^{k} (\varphi - \varphi_i) = 0. \qquad (16)$$

Рівнане (16) є циклїчне, бо Γ є циклїчною ґрупою. Коли уложимо субституції ґрупи G в таблицю

$$\begin{array}{llll} 1, \; g, \; g^2, \; g^3, & & & g^{p-1}, \\ t, \; gt, \; g^2t, \; g^3t, & & & g^{p-1}t, \\ t^2, \; gt^2, \; g^2t^2, \; g^3t^2, & & & g^{p-1}t^2, \end{array}$$

то до кождого рядка буде належати одна вартість функції φ:

$$\varphi_1 = \varphi, \; (\varphi)_t = \varphi_2, \; (\varphi)_{t_2} = \varphi_3, \quad ., \; (\varphi)_{t^{k-1}} = \varphi_k. \qquad (17)$$

*) Netto, Substitutionentheorie, стр. 226.

Субституції ґрупи Γ можуть пересувати величини φ тільки циклїчно, бо субституції $t^{\lambda}g^{\alpha}$ мають для всіх λ форму $g^{\alpha\varrho^{\lambda}}t^{\lambda}$, отже ряд функцій

$$\varphi_{t^{\beta}g^{\alpha}},\ \varphi t^{\beta+1}g^{\alpha}, \qquad , \varphi t^{k\beta-1}g^{\alpha}$$

є ідентичний з рядом

$$\varphi_{\alpha},\ \varphi_{\beta-1} \qquad , \varphi_{k\beta-1} = \varphi_{\beta-1},$$

т. зн., що ґрупа Γ є дійсно циклїчна. Проте розвязка рівнаня степеня p зводить ся до розвязки двох рівнань:

1. циклїчного степеня $p-1$ або $\frac{p-1}{\sigma}$, де σ є дїльником числа $p-1$, і

2. циклїчного степеня p.

§. 104. Розходить ся нам ще о означене форми, яку мають мати коріні рішимого рівнаня степеня p. Напишім ті коріні в такій формі:

$$\left.\begin{aligned}
x_1 &= G_0 + \sqrt[p]{R_1} + \sqrt[p]{R_2} + \sqrt[p]{R_3} + \ldots + \sqrt[p]{R_{p-1}},\\
x_2 &= G_0 + \omega\sqrt[p]{R_1} + \omega^{\varrho}\sqrt[p]{R_2} + \omega^{\varrho^2}\sqrt[p]{R_3} + \ldots + \omega^{\varrho^{p-1}}\sqrt[p]{R_{p-1}}\\
x_3 &= G_0 + \omega^2\sqrt[p]{R_1} + \omega^{2\varrho}\sqrt[p]{R_2} + \omega^{2\varrho^2}\sqrt[p]{R_3} + \ldots + \omega^{2\varrho^{p-1}}\sqrt[p]{R_{p-1}},\\
&\ldots\\
x_p &= G_0\, \omega^{p-1}\sqrt[p]{R_1} + \omega^{(p-1)\varrho}\sqrt[p]{R_2} + \omega^{(p-1)\varrho^2}\sqrt[p]{R_3} + \ldots + \omega^{(p-1)\varrho^{p-1}}\sqrt[p]{R_{p-1}},
\end{aligned}\right\}(18)$$

де $\sqrt[p]{R_i}$ мають такі значіня:

$$\sqrt[p]{R_1} = V_1,\ \sqrt[p]{R_2} = G_{\varrho}V_1^{\varrho}, \sqrt[p]{R_3} = G_{\varrho_2}V_1^{\varrho^2}$$

взагалї

$$\sqrt[p]{R_{\lambda}} = G_{\varrho^{\lambda-1}}V_1^{\varrho^{\lambda-1}} \quad (\lambda = 1,\ 2, \qquad p \quad 1). \qquad (19)$$

З (18) слїдує:

$$\left.\begin{aligned}
\sqrt[p]{R_1} &= \frac{1}{p}\left[x_1 + \omega^{-1}x_2 + \omega^{-2}x_3 + \ldots + \omega x_p\right].\\
\sqrt[p]{R_2} &= \frac{1}{p}\left[r_1 + \omega^{-\varrho}x_2 + \omega^{-2\varrho}x_3 + \ldots + \omega^{\varrho}x_p\right],\\
\sqrt[p]{R_3} &= \frac{1}{p}\left[x_1 + \omega^{-\varrho^2}x_2 + \omega^{-2\varrho^2}x_3 + \ldots + \omega^{\varrho^2}x_p\right],
\end{aligned}\right\}\quad(20)$$

отже взагалі:

$$\sqrt[p]{R_\lambda}=\frac{1}{p}\left[x_1+\omega^{-\varrho^{\lambda-1}}x_2+\omega^{-2\varrho^{\lambda-1}}x_3+\ldots+\omega^{\varrho^{\lambda-1}}x_p\right]. \quad (20')$$

Субституція g переводить $\sqrt[p]{R_\lambda}$ в $\omega^{\varrho^{\lambda-1}}\sqrt[p]{R_\lambda}$, отже зовсім не зміняє величин $R_1, R_2, \ldots R_{p-1}$; вони є проте циклічними функціями корінів $x_1, x_2, \ldots, x_p$. Зате субституція

$$t^{-1}=|z \quad \varrho^{-1}z|=|z \quad \varrho^{p-2}z| \quad (21)$$

переводить кожде $\sqrt[p]{R_\lambda}$ в $\omega^{-\varrho^{\lambda}+\varrho^{\lambda-1}}\sqrt[p]{R_{\lambda+1}}$, отже пересуває циклічно величини R_λ.

§. 105. Утворім тепер функцію *).

$$Q=\sqrt[p]{R_1}\sqrt[p]{R_{p-1}}+\sqrt[p]{R_2}\sqrt[p]{R_{p-2}}+\sqrt[p]{R_3}\sqrt[p]{R_{p-3}}+\ldots+\sqrt[p]{R_{\frac{p-1}{2}}}\sqrt[p]{R_{\frac{p+1}{2}}}. \quad (22)$$

Отся функція належить до ґрупи G, бо кожда субституція переведе $\sqrt[p]{R_1}$ в $\omega\sqrt[p]{R_1}$, а $\sqrt[p]{R_{p-1}}$ в $\omega^{-1}\sqrt[p]{R_{p-1}}$, т. зн. не змінить добутка $\sqrt[p]{R_1}\sqrt[p]{R_{p-1}}$; так само не змінить вона всіх инших додайників суми Q. — Подібно субституція t^{-1} переведе в себе циклїчно додайники тої суми. Звідси слїдує, що функція Q є вимірна в сочинниках рівнаня (1). Отсю функцію можемо дїйсно обчислити.

Маємо:

$$\sqrt[p]{R_1}=\frac{1}{p}\left[x_1+\omega^{-1}x_2+\omega^{-2}x_3+\ldots+\omega^{-(k-1)}x_k+\ldots+\omega^{-(l-1)}x_l+\ldots+x_p\right]$$

$$\sqrt[p]{R_{p-1}}=\frac{1}{p}\left[x_1+\omega x_2+\omega^2x_3+\ldots+\omega^{k-1}x_k+\ldots+\omega^{l-1}x_l+\ldots+\omega^{p-1}x_p\right].$$

Ті рівнаня множимо одно другим. Наперед множимо члени так, як вони стоять під собою, а опісля збираємо добутки о рівних показчиках в суми. Впровадьмо скорочене:

$$\omega^k+\omega^l=(k,\ l);$$

тепер маємо:

$$\begin{aligned}p^2\sqrt[p]{R_1}\sqrt[p]{R_{p-1}}=\Sigma x_i^2&+(1,-1)x_1x_2+(2,-2)x_1x_3+\ldots+(p-1,\ 1-p)x_1\ x_p\\&+(1,-1)x_2x_3+\ldots+(p-2,\ 2-p)\ x_2\ x_p\\&+\ldots\\&+(1,-1)x_{p-1}x_p,\ x_2\ x_p\end{aligned}$$

*) J. Dolbnia, Sur la forme plus précise des racines des équations algébriques resolubles par radicaux. — Darboux Bull. des sc. math. (2). XVIII/1. 1894. стр. 132.

т. зн.

$$\sqrt[p]{R_1}\sqrt[p]{R_{p-1}}=\frac{1}{p^2}\left[\Sigma x_i{}^2+\Sigma(k-l,\ l-k)x_k x_l\right]\ (k\equiv|\equiv l\ (mod.\ p).\quad (23)$$

Виконаймо на тім рівнаню субституцію t^{-1}; вона переведе ліву сторону в другий член суми Q. t^{-2} переведе її в третій член і т. д., а на правій стороні повстануть такі зміни:

$$\left.\begin{aligned}
\sqrt[p]{R_1}\sqrt[p]{R_{p-1}}&=\frac{1}{p^2}\left[\Sigma x_i{}^2+\Sigma(k-l,\ l-k)x_k x_l\right],\\
\sqrt[p]{R_2}\sqrt[p]{R_{p-2}}&=\frac{1}{p^2}\left[\Sigma x_i{}^2+\Sigma(k\ \ l,\ l\ \ k)\,x_{k\varrho^{p-2}}x_{l\varrho^{p-2}}\right]\\
\sqrt[p]{R_3}\sqrt[p]{R_{p-3}}&=\frac{1}{p^2}\left[\Sigma x_i{}^2+\Sigma(k-l\ \ l-k)\,x_{k\varrho^{p-3}}x_{l\varrho^{p-3}}\right]\\
&\ \ \vdots\\
\sqrt[p]{R_{\frac{p-1}{2}}}\sqrt[p]{R_{\frac{p+1}{2}}}&=\frac{1}{p^2}\left[\Sigma x_i{}^2+\Sigma(k-l,\ l-k)x_{k\varrho^{\frac{p+1}{2}}}x_{l\varrho^{\frac{p+1}{2}}}\right]
\end{aligned}\right\}\quad(24)$$

Додаймо всї ті вираженя:

$$Q=\frac{p-1}{2p^2}\sum x_i{}^2+\frac{1}{p^2}\sum(k-l,\ l-k)\sum_{\lambda=1}^{\frac{p-1}{2}}x_{k\varrho^{p-\lambda}}x_{l\varrho^{p-\lambda}}.\quad(25)$$

Сочинники рівних добутків $x_k x_l$ не можуть бути рівні; коли-б сочинники при $(m,-m)$ в членах

$$\sqrt[p]{R_\alpha}\sqrt[p]{R_{p-\alpha}}\ \text{ і }\ \sqrt[p]{R_\beta}\sqrt[p]{R_{p-\beta}}$$

були рівні, т. зн.

$$x_\alpha x_{\alpha-m\varrho^{1-\alpha}}=x x_{\alpha\ \alpha-m\varrho^{1-\beta+\alpha}},$$

то з того виходило би $\beta\equiv 2\alpha$ $(mod.\ p)$, а се неможливе, коли $\alpha\leqq\frac{p-1}{2}$, $\beta\leqq\frac{p-1}{2}$.

Так само неможлива рівність сочинників при $(k-l,\ l-k)$, т. зн., Неможлива реляція

$$x_{k\varrho^{p-\lambda}}x_{l\varrho^{p-\lambda}}=x_{(k+m)\varrho^{p-\mu}}x_{(l+m)\varrho^{p-\mu}},\ (m=|=0).$$

Тут можливі такі дві евентуальности:

$$\left.\begin{aligned}1.\ k\varrho^{p-\lambda}&\equiv(k+m)\varrho^{p-\mu},\\ l\varrho^{p-\lambda}&\equiv(l+m)\varrho^{p-\mu},\end{aligned}\right\}\ (mod.\ p.);$$

З них виходило би

$$(k-l)\ \varrho^{p-\lambda} \equiv (k-l)\varrho^{p-\mu}\ (mod.\ p\ ),$$

т. зн. мусіло би бути $\lambda \equiv \mu$ $(mod.\ p-1)$, а се не можливе.

$$\left.\begin{array}{l} 2.\ k\varrho^{p-\lambda} \equiv (l+m)\varrho^{p-\mu} \\ l\varrho^{p-\lambda} \equiv (k+m)\varrho^{p-\mu} \end{array}\right\} (mod\ p.),$$

або $\varrho^{\lambda} + \varrho^{\mu} \equiv 0$ $(mod.\ p.)$, т. зн. $\varrho^{\lambda} \equiv p - \varrho^{\mu}$, а се також неможливе на основі дефініції величини Q. З того слідує, що всї сочинники в сумах (25) є ріжні поміж собою.

Обчислїм тепер суму сочинників кождого члена $x_k x_l$

$$\Sigma(k-l,\ l-k) = (1,-1) + (2,-2) + \ldots + \left(\frac{p-1}{2}, \frac{p+1}{2}\right) = -1,$$

отже

$$Q = \frac{p\ \ 1}{2p^2}\sum x_i^{\,2} - \frac{1}{p^2}\sum x_k x_l, \tag{26}$$

т. зн., що Q є величиною, вимірною в сочинниках рівнаня (1). Звідси слїдує, що при помочи величини Q можемо представити вимірно корінї рівнаня (1).

§. 106. Творім тепер дальше такі функції при помочи величини ε, даної рівнанем:

$$\varepsilon^{\frac{p-1}{2}} = 1\,;$$

$$\left.\begin{array}{l}
Q_1 = \left(\sqrt[p]{R_1}\sqrt[p]{R_{p-1}} + \varepsilon\sqrt[p]{R_2}\sqrt[p]{R_{p-2}} + \varepsilon^2\sqrt[p]{R_3}\sqrt[p]{R_{p-3}} + \ldots\right. \\
\qquad\qquad \left. + \varepsilon^{\frac{p-1}{2}}\sqrt[p]{R_{\frac{p-1}{2}}}\sqrt[p]{R_{\frac{p+1}{2}}}\right)^{\frac{p-1}{2}}, \\
Q_2 = \left(\sqrt[p]{R_1}\sqrt[p]{R_{p-1}} + \varepsilon^2\sqrt[p]{R_2}\sqrt[p]{R_{p-2}} + \varepsilon^4\sqrt[p]{R_3}\sqrt[p]{R_{p-3}} + \ldots\right. \\
\qquad\qquad \left. + \varepsilon^{\frac{p-5}{2}}\sqrt[p]{R_{\frac{p-1}{2}}}\sqrt[p]{R_{\frac{p+1}{2}}}\right)^{\frac{p-1}{2}}, \\
\\
Q_{\frac{p-3}{2}} = \left(\sqrt[p]{R_1}\sqrt[p]{R_{p-1}} + \varepsilon^{\frac{p-3}{2}}\sqrt[p]{R_2}\sqrt[p]{R_{p-2}} + \varepsilon^{\frac{p-5}{2}}\sqrt[p]{R_3}\sqrt[p]{R_{p-1}} + \ldots\right. \\
\qquad\qquad \left. + \varepsilon\sqrt[p]{R_{\frac{p-1}{2}}}\sqrt[p]{R_{\frac{p+1}{2}}}\right)^{\frac{p-1}{2}};
\end{array}\right\} \tag{27}$$

всї вони незмінні для ґрупи G, бо субституція g не змінить зовсїм додайників тих сум, а t^{-1} пересуне їх тільки циклїчно серед тої самої суми, так що надчисельні сочинники ε^i відпадуть при степенованю. З того слїдує, що всї ті величини Q_i можна представити вимірно величиною $Q = c$.

Доберім до тих рівнань ще

$$a = \sqrt[p]{R_1}\sqrt[p]{R_{p-1}} + \sqrt[p]{R_2}\sqrt[p]{R_{p-2}} + \ldots + \sqrt[p]{R_{\frac{p-1}{2}}}\sqrt[p]{R_{\frac{p+1}{2}}}$$

і розвяжім їх як лінїйну систему рівнань з огляду на добутки величин R, то се дасть:

$$\left.\begin{aligned}
\sqrt[p]{R_1}\sqrt[p]{R_{p-1}} &= \frac{2}{p-1}\left(a + \sqrt[\frac{p-1}{2}]{Q_1} + \sqrt[\frac{p-1}{2}]{Q_2} + \ldots + \sqrt[\frac{p-1}{2}]{Q_{\frac{p-3}{2}}}\right)\\
\sqrt[p]{R_2}\sqrt[p]{R_{p-2}} &= \frac{2}{p-1}\left(a + \varepsilon^{-1}\sqrt[\frac{p-1}{2}]{Q_1} + \varepsilon^{-}\sqrt[\frac{p-1}{2}]{Q_2} + \ldots \varepsilon^{-\frac{p-}{2}}\sqrt[\frac{3p-1}{2}]{Q_{\frac{p-1}{2}}}\right),\\
\sqrt[p]{R_{\frac{p-1}{2}}}\sqrt[p]{R_{\frac{p-1}{2}}} &= \frac{2}{p-1}\left(a + \varepsilon^{-p\cdots}\sqrt{Q_1} + {}^{-\frac{\cdots}{2}}\sqrt{Q_2} + \ldots + {}^{\cdot 1}\sqrt[\frac{p-1}{2}]{Q_{\frac{p-3}{2}}}\right)
\end{aligned}\right\} \quad (28)$$

Вираженя Q_i є вимірними функціями величини a.

§ 107. Тепер треба ще обчислити добутки $\sqrt[p]{R_\lambda}\sqrt[p]{R_{p-\lambda}}$.

Сума

$$b = (R_1 + R_{p-1}) + (R_2 + R_{p-2}) + \ldots + (R_{\frac{p-1}{2}} + R_{\frac{p+1}{2}}) \qquad (29)$$

є функцією, яка належить також до ґрупи G, отже є знаною величиною. Так само функції

$$L_i = \left[(R_1 + R_{p-1}) + \varepsilon^i(R_2 + R_{p-2}) + \ldots + \varepsilon^{\frac{p-1}{2}i}(R_{\frac{p-1}{2}} + R_{\frac{p+1}{2}})\right]^{\frac{p-1}{2}} \quad (30)$$

$$\left(i = 1,\ 2, \ldots, \frac{p-3}{2}\right)$$

мають G за ґрупу, отже є вимірними функціями величини b. З (29) і (30) маємо:

$$R_1+R_{p-1}=\frac{2}{p-1}\left(b+\sqrt[\frac{p-1}{2}]{L_1}+\varepsilon-\lambda\sqrt[\frac{p-1}{2}]{L_2}+\ldots\varepsilon^{\frac{p-3}{2}}\sqrt[\frac{p-1}{2}]{L_{\frac{p-1}{2}}}\right)$$

взагалї:

$$R_\lambda+R_{p-\lambda}=\frac{2}{p-1}\left(b+\varepsilon_-\sqrt[\frac{p-1}{2}]{L_1}+\varepsilon-\lambda\sqrt[\frac{p-1}{2}]{L_2}\ldots+\varepsilon^{-}+\sqrt[\frac{p-1}{2}]{L_{\frac{b-3}{2}}}\right), \quad (31a)$$

$$\left(\lambda=1,\ 2,\ \ldots,\frac{p-1}{2}\right).$$

З (28) і (30) обчисляємо чергою R_1 і R_{p-1}, і R_2 і R_{p-2} і т. д.

Оба перші рівнаня дадуть R_1+R_{p-1} і R_2 R_{p-1}, отже ті величини знаходимо як корінї квадратного рівнаня:

$$t^2-\frac{2}{p-1}\left(b+\sqrt[\frac{p-1}{2}]{L_1}\sqrt[\frac{p-1}{2}]{L_1}+\ldots+\sqrt[\frac{p-1}{2}]{L_{\frac{p-3}{2}}}\right)t+\left(\frac{2}{p-1}\right)^p\left(a+\sqrt[\frac{p-1}{2}]{Q_1}+\ldots\right.$$

$$\left.+\sqrt[\frac{p-1}{2}]{Q_{\frac{p-3}{2}}}\right)^p=0, \quad (31)$$

отже:

$$\left.\begin{aligned}
&R_1=\frac{1}{p-1}\left(b+\sqrt[\frac{p-1}{2}]{L_1}+\sqrt[\frac{p-1}{2}]{L_2}+\ldots\right)+\\
&+\ldots+\sqrt{\frac{1}{(p-1)^2}\sqrt[\frac{p-1}{2}]{L_1}+\sqrt[\frac{p-1}{2}]{L_2}+\ldots-\left(\frac{2}{p-1}\right)^p\left(a+\sqrt[\frac{p-1}{2}]{Q_1}+\ldots+\right)}\\
&R_{p-1}=\frac{1}{p-1}\left(b+\sqrt[\frac{p-1}{2}]{L_1}\sqrt[\frac{p-1}{2}]{}+\ldots\right),\\
&-\sqrt{\frac{1}{(p-1)^2}\left(b+\sqrt[\frac{p-1}{2}]{L_2}+\sqrt[\frac{p-1}{2}]{L_2}+\ldots\right)-\left(\frac{2}{p-1}\right)^p\left(a+\sqrt[\frac{p-1}{2}]{Q_1}+\ldots\right)^n}
\end{aligned}\right\}(32)$$

На тій самій дорозї обчислимо всі инші R. Знаючи вже всї R, вертаємо до x, і таким чином маємо розвязане рівнанє (1).

XII. Рішимі рівнаня степеня p^2.

§. 108. Другою квестією в загальнім проблємі розвязки рівнань v_1 є рішимі рівнаня і ґрупи степеня p^2.

Нехай буде дане рішиме рівнане первісне степеня p^2

$$f(x) = 0 \qquad (1)$$

з ґрупою G. Ґрупа G є зложена, а остатнім членом її ряду мусить бути аритметична Абелева ґрупа M, утворена з субституцій

$$g = | h, k \quad h + \alpha, k + \beta \quad | \quad (mod.\ p), \qquad (2)$$

які можемо представити як добутки з односторонних аритметичних субституцій

$$g = g_1^{\alpha} g_2^{\beta}, \quad (\alpha, \beta = 0\ 1, \quad ., p-1) \qquad (3)$$

де

$$\left.\begin{array}{l} g_1 = | h, k\ h+1, k |, \\ g_2 = | g, k\ h, k+1 |. \end{array}\right\} \qquad (3a)$$

Прочі субституції ґрупи G є ґеометричні, бо тільки ті субституції можуть бути перемінні з ґрупою M. Щоби се доказати, покажемо, що тільки субституції лінійної ґрупи (§. 43) можуть трансформувати аритметичну ґрупу саму в себе.

Найзагальнійша лінійна субституція степеня p^2 має форму

$$u = | h, k \quad ah + bk + \alpha, ch + dh + \beta | (mod.\ p). \qquad (4)$$

Тепер шукаємо такої субституції τ, щоби було

$$\tau^{-1} M\tau = M, \qquad (5)$$

як того вимагає наше твердженє. Кожду субституцію показчиків h, k можемо представити як функцію тих величин, уживаючи до тої цїли інтерполяційного взору Lagrange'a:*)

$$\tau = | h, k \quad \varphi(h, k), \psi(h, k) | \qquad (6)$$

Ґрупа M складається з субституцій g, отже рівнане (5) можемо написати також так:

$$\tau^{-1}g\tau = \tau^{-1}g_1^{\alpha}\tau . \tau^{-1}g_2^{\beta}\tau = (\tau^{-1}g_1\tau)^{\alpha} . (\tau^{-1}g_2\tau)^{\beta} = g' \qquad (5a)$$

т. зн., маємо знайти таке τ, щоби $\tau^{-1}g_1\tau$ і $\tau^{-1}g_2\tau$ були опять аритметичними субституціями:

$$\left.\begin{array}{l} \tau_1 = \tau^{-1}g_1\ \tau = g_1^{\gamma} g_2^{\delta} \\ \tau_2 = \tau^{-1}g_2\ \tau = g_1^{\varepsilon} g_2^{\zeta}. \end{array}\right\} \qquad (7)$$

---

*) Netto, Algebra, II. стр. 329.

Субституція τ^{-1} переводить $\varphi\ (h,\ k)$ в h_1, субституція g_1 переводить h в $h+1$, а τ переводить h в $\varphi\ (h,\ k)$, отже $h+1$ перейде в $\varphi\ (h+1,\ k)$, т, зн., що під впливом τ_1 перейде $\varphi\ (h,\ k)$ в $\varphi(h+1,\ k)$; подібно τ_2 переведе $\psi\ (h,\ k)$ в $\psi\ (h,\ k+1)$.

Коли τ_1 і τ_2 мають бути аритметичними субституціями, то кождий показчик, представлений функціями φ і ψ, мусить збільшити ся о якесь стале число:

$$\left.\begin{array}{l|l} \varphi(h+1,\ k)=\varphi(h,\ k)+a', & \psi(h+1,\ k)=\psi(h,\ k)+c'. \\ \varphi(h,k+1)=\varphi(h,\ k)+b', & \psi(h,\ k+1)=\psi(h,\ k)+d'. \end{array}\right\}$$

Приймаючи, що

$$\varphi\ (0,\ 0)=m,\ \psi(0,\ 0)=n,$$

одержимо, коли будемо збеншувати показчики h і k чергою о 1:

$$\varphi(h,\ k)=a'h+b'k+m,$$
$$\psi(h,\ k)=c'h+d'k+n,$$

отже субституція τ є лінїйна. Наше твердженє є проте доказане, З того слїдує, що рішима ґрупа G є або лїнїйною ґрупою, або підґрупою лїнїйної ґрупи.

§. 109. Рішимі ґрупи висших (т. є зложених) степенїв називає Weber*) рівно-ж метациклїчними. Вони ріжнять ся тим від метациклїчних ґруп першого степеня, що тамті є ідентичні з лїнїйними ґрупами степеня p, а тут можуть бути метациклїчні ґрупи тільки їх підґрупами.

Метациклїчні ґрупи степеня p^2 перший сконструував C. Jordan**); він виказав, що є три типи таких ґруп. Його метода лежить в тім, що перше зводить ся лінїйні субституції до найпростїйшої форми (канонїчної, Jordan; нормальної, Netto), а опісля добирається до Абелевої ґрупи M такі субституції, які є з собою переміннї по субституції попередньої ґрупи. Таким чином доходить Jordan вкінці до своєї найзагальнїйшої ґрупи.

Найпростїйша форма лїнїйних — а саме ґеометричних — субституцій є та, що така субституція переводить кожду функцію показчиків в її многократь ***).

*) Weber, Algebra I, стр. 647.

**) C. Jordan, Sur la résolution algèbrique des équations du degré p^2 (p—un premier impair) Liouville's Journal, (2):XIII. 1868, стр. 111—135. — Netto, Algebra II, стр. 444.

***) C. Jordan, Traité de substitutions et des équations algèbriques, Paris 1870, стр. 114.

Нормальна форма субституції

$$t = | h, k \quad ah + bk, ch + dk | \quad (mod.\ p) \tag{8}$$

переведе функцію

$$\varphi(h, k) = mh + nk \tag{9}$$

в її многократь

$$\varrho\varphi = \varrho(mh + nk);$$

t переводить φ в

$$\varphi_t = m(ah + bk) + n(ch + dk) = \varrho\varphi,$$

отже величини m, n і ϱ мусять сповнювати отсї конґруенції

$$\left.\begin{array}{r} m(a-\varrho) + nc \equiv 0 \\ mb + n(d-\varrho) \equiv 0 \end{array}\right\} \ (mod.\ p) \tag{10}$$

Елїмінуючи звідси m і n, одержуємо т. зв. **характеристичну конґруенцію** (Jordan)

$$\begin{vmatrix} a-\varrho, & c \\ b, & d-\varrho \end{vmatrix} \equiv 0 \quad (mod.\ p), \tag{11}$$

яка має три ріжні можливі розвязки, в міру того, чи її діскрімінанта

$$D = (a+d)^2 - 4(ad - bc) = (a-d)^2 + 4bc \tag{12}$$

є через p подїльна, є квадратним останком або не-останком ($mod.\ p$). Перша евентуальність дає два рівні корінї конґруенції (11), друга два ріжні корінї, дійсні, а третя два спряжені корінї.

§. 110. **Перша можливість.** $D \equiv 0$ ($mod.\ p$). Тодї конґруенція (11) має одну розвязку ϱ, т. зн., що істнує тільки **одна** така функція φ показчиків, яка переходить в $\varrho\varphi$ під впливом субституції t; другої такої функції нема. Пишучи ту функцію на місцї показчика h, одержимо

$$t = | \varphi, \psi \quad \varrho\varphi, \psi_1 + \psi_2 |$$

одначе за φ і ψ можемо написати h і k:

$$t = | h, k \quad \varrho h, ch + dk |,$$

т. зн. маємо $a = \varrho$, $b = 0$. Вставивши ті вартости в (12), одержуємо: $(\varrho - d)^2 \equiv 0$ ($mod.\ p$), отже $d = \varrho$, проте **перша нормальна форма субституції** t є

$$t = | h, k \quad \varrho h, ch + \varrho k | \tag{13}$$

Друга можливість. D є квадратним останком ($mod.\ p$), т. зн. конґруенція

$$z^2 \equiv D \ (mod.\ p)$$

є рішима в цїлих числах. Тодї істнують дві дійсні розвязки конґруенції (11) $\varrho_1 = a$, $\varrho_2 = b$, так що можемо написати

$$t = | \, h, \; k \quad ah, \; bk \, | \; ; \tag{14}$$

се **друга нормальна форма субституції** t.

Третя можливість. D є квадратним не-останком $(mod.\ p)$, т. зн. конґруенція $z^2 \equiv D \ (mod.\ p)$ не є рішима; тоді маємо дві спряжені розвязки, так що в (14) можемо написати:

$$a = a_1 + b_1 j,$$
$$b = a_1 - b_1 j,$$

де $j^2 \equiv e \ (mod.\ p)$; e — не-останок $(mod.\ p)$. Порівнуючи в субституції (14) дійсні і мнимі части з собою, одержимо як **третю нормальну форму** субституцію

$$t = | \, h, \; k \quad ah + bek, \; bh + ak \, | \, . \tag{15}$$

§. 111. Тепер шукаємо ряду зложеня для ґрупи G, яка має складати ся з субституцій g і нормальних форм субституції t. Остатнім членом ряду буде Абелева ґрупа M порядку p^2. Дальшим членом L буде така ґрупа, яка побіч M буде містити в собі самі перемінні субституції t. Отся ґрупа мусить **напевно** складати ся з субституцій форми

$$s_a = | \, h, \; k \quad ah, \; ak \, | \; (a = 1, \; 2, \; \ldots, \; p - 1) \; ; \tag{16}$$

ті субституції можна назвати **рівнобічними** (gleichseitig). Крім них може та ґрупа мати ще инші субституції, загальнїйшої форми t.

Ще висший член одержимо, коли до згаданої ґрупи L доберемо такі субституції, які з собою перемінні тільки по субституції попередньої ґрупи. Таким чином вичерпаємо цїлу ґрупу.

Шукаючи ґрупи L, мусимо розріжнити дві можливости:

1. субституціям t не накладаємо нїякого обмеженя (можливість A);

2. за субституції t беремо тільки рівнобічні s_a (можливість $Б$).

Можливість А.

§. 112. **Перша нормальна форма.** Субституція

$$t = | \, h, \; k \quad \varrho h, \; ch + \varrho k \, | \tag{12}$$

має бути перемінна з кождою иншою субституцією форми

$$\tau = | \, h, \; k \quad \alpha h + \beta k, \; \gamma h + \delta k \, | \, ,$$

т. зн. має бути

$$t\tau = \tau t.$$

Звідси слїдує: $\beta = 0$, отже

$$\tau = | \, h, \; k \quad \alpha h, \; \gamma h + \delta k \, | \, . \tag{17}$$

Возьмім субституцію σ з висшої ґрупи K,

$$\sigma = | h, k \quad mh + nk, qh + rk | ,$$

то вона мусить трансформувати субституцію t в якесь τ, бо $K^{-1}LK = L$, т. зн. $\tau\sigma = \sigma\tau$. Звідси слїдує: $n = 0$, отже

$$\sigma = | h, k \quad mh, qh + rk | .$$

Бачимо, що всї субституції ґрупи G мають форму τ. Така ґрупа є, правда, метациклїчна, але **не є первісна**, бо можна корінї x_{hk} рівнаня (1) роздїлити на p кляс по p членів так, що перші показчики будуть в кождій клясї рівні. Тодї субституції t не будуть могли роздїлити тих кляс, отже ґрупа G є непервісна.

§. 116. **Друга нормальна форма.** Возьмім субституцію

$$t = | h, k \quad ah, bk | , \qquad (14)$$

яка має бути перемінна з кождою иншою ґеометричною

$$\tau = | h, k \quad ah + \beta k, \gamma h + \delta k | .$$

З $t\tau = \tau t$ слїдує $a\beta = b\beta$ і $a\gamma = b\gamma$. a і b є ріжні від 0, бо детермінанта субституції мусить бути $\equiv | \equiv 0$; отже мусять бути $\beta = 0$, $\gamma = 0$, т. зн., що субституція τ є тої форми, що t.

Субституція σ з ґрупи K мусить трансформувати кожде t в якесь τ; беручи знов

$$\sigma = | h, k \quad mh + nk, qh + rk | ,$$

одержуємо з $t\sigma = \sigma\tau$:

$$am = \alpha m, \; bq = \alpha q ; \; an = \delta n, \; br = \delta r.$$

Ті вимоги можна сповнити двома ріжними способами:

$$1. \; n = 0, \; q = 0 ; \; 2. \; m = 0, \; r = 0.$$

Перший спосіб дає

$$\sigma_1 = | h, k \quad mh, rk | , \qquad (18)$$

субституцію форми t, другий

$$\sigma_2 = | h, h \quad nk, qh | ;$$

ту другу субституцію можна звести до простїйшої форми, комбінуючи її з відповідним σ_1:

$$\sigma_1^{-1} = | h, k \quad qh, nk |^{-1} = | qh, nk \quad h, k | ;$$

се дає:

$$\sigma_3 = | h, k \quad k, h | . \qquad (19)$$

Таку субституцію, яка тільки переставлює показчики, можна назвати **транспонуючою** (transponierende Subst.).

Тими субституціями вичерпали ми цїлу ґрупу G. **Маємо отже перший тип загальних, первісних, метациклїчних ґруп степеня p^2; назвемо їх ґрупами G_I.** Ґрупа G_I складає ся з таких субституцій:

$g = g_1^{\alpha} g_2^{\beta}$ $(\alpha, \beta = 0, 1, \ldots, p-1)$; порядок p^2;

$\sigma_1 = | h, k \quad ah, bk |$ $(a, b = 1, 2, \ldots, p-1)$; порядок $(p-1)^2$;

$\sigma_2 = | h, k \quad k, h |$; порядок 2;

отже порядок ґрупи G_{I} є

$$r_{\mathrm{I}} = 2(p-1)^2 p^2. \qquad (20)$$

§. 114. **Третя нормальна форма.** Вибираємо найвигіднійшу форму субституції t

$$t = | h, k \quad ah + bek, bh + ak |; \qquad (15)$$

перемінна з нею субституція τ має таку саму форму

$$\tau = | h, k \quad \alpha h + \beta ek, \beta h + \alpha k |,$$

а субституція σ з висшої ґрупи K

$$\sigma_1 = | h, k \quad mh + nek, nh + mk | \qquad (21)$$

або

$$\sigma_2 = | h, k \quad k, -h |. \qquad (22)$$

Порядок субституції σ_1 є p^2-1, бо зі всіх можливих комбінацій m і n треба виключити $m = n = 0$.

Тут маємо отже **другий тип** шуканих ґруп, G_{II}. Вони складають ся з

$g = g_1^{\alpha} g_2^{\beta}$ $(\alpha, \beta = 0, 1, 2, \ldots, p-1)$; порядок p^2;

$\sigma_1 = | h, k \quad ah + bek, bh + ak |$ $(a, b = 0, 1, 2, \ldots, p-1)$, $a = b = 0$ виключене: e — не-останок $(mod.\ p)$); порядок p^2-1;

$\sigma_2 = | h, k \quad k, -h |$; порядок 2;

отже

$$r_{\mathrm{II}} = 2(p^2-1)\, p^2. \qquad (23)$$

Можливість Б.

§. 115. Тут маємо шукати таких ґруп K, яких субституції є з собою перемінні по субституції форми s, отже таких t і τ, що

$$t\tau = \tau t \,.\, s_1; \qquad (24)$$

ґрупа L складаєть ся з самих s.

Перша нормальна форма дає також непервісні ґрупи, бо з виїмком субституцій s всї инші мають вид (13).

§. 116. **Друга і третя форма** ведуть до того самого типу, бо ріжниця між ними обома виступає що йно у висшім членї ряду зложеня, понад K. Тому можемо взяти

$$t = | h, k \quad ah, bk |, \qquad (14)$$

де a і b є дїйсні або спряжені (мнимі) числа. Приймаючи знов

$$\tau = | h, k \quad ah + \beta k, \gamma h + \delta k | ,$$

одержуємо з реляції (24).

$$a\alpha = a\alpha l, \; a\beta = b\beta l; \; b\gamma = a\gamma l, \; b\delta = b\delta l.$$

Се веде знов до двох можливостий:

1. $\beta = 0$, $\gamma = 0$, $\alpha\delta \neq 0$; 2. $\alpha = 0$, $\delta = 0$, $\beta\gamma \neq 0$;
перша можливість дає $l = 1$ — т. зн., що t і τ належали би до чисто перемінної ґрупи; друга дає $a = bl$, $b = al$, отже $l^2 = 1$, $l = \pm 1$; тільки вартість $l = -1$ є придатна, а з неї маємо: $\alpha = 0$, $\delta = 0$, $b = -a$. Відповідно до того є:

$$t = | h, k \quad ak, -ak | = | h, k \; ah, ak | \quad | h, k \; h, -k | ,$$

або в найпростійшій формі

$$t = | h, k \quad h, -k | . \qquad (25).$$

Дальше є

$$\tau = | h, k \quad \beta k, \gamma h | ,$$

приймаючи детермінанту тої субституції ± 1, маємо $\beta = \gamma = 1$, і

$$\tau = | h, k \quad k, h | . \qquad (26)$$

§. 117. Одначе ті субституції не вичерпують ще цілої ґрупи G. Є ще такі субституції, які стоять поза ґрупою К. Назвім одну таку субституцію

$$v = | h, k \quad Ah + Bk, Ch + Dk | , \qquad (27)$$

то вона мусить бути з субституціями t і τ перемінна аж по рівнобічні субституції s_i. Пригляньмо ся ближше тим обставинам.

Впровадимо на хвилю такі означеня: T за одну з субституцій t або τ, $[T]$ за яку небудь їх комбінацію (отже t або τ само, або $t\tau$; бо вже квадрат котрої небудь з них дає 1). Зі всїх можливих комбінацій, які одержали-б ми з трансформації субституцією v, задержимо тільки ті, в яких ліва сторона рівнаня

$$v^{-1} T v = [T]. \; s_\pi \qquad (28)$$

не приходить ще в ґрупі K; всї инші комбінації відкидаємо. Мусимо тут розріжнити такі можливости:

1. По обох сторонах рівнаня (28) є таке саме T, отже або t, або τ. Порівнуючи сочинники при h і k, маємо $AC = 0$, $BD = 0$; з огляду на те, що детермінанта субституції v

$$\begin{vmatrix} A & B \\ C & D \end{vmatrix}$$

має бути перва супроти модулу p, мусить бути або $A = 0$, $D = 0$, $BC \neq 0$, або $B = 0$, $C = 0$, $AD \neq 0$. Обі можливости дають на правій стороні $T.s_\pi$; така субституція приходить вже в K, отже ту комбінацію треба виключити.

2. Так само мусимо виключити ще й ту можливість, що v трансформує оба T в те саме $[T]$. s_π — розуміеть ся, показчик π може мати ріжні вартости. В такім разї мусіла-б субституція v трансформувати добуток $t\tau$ в $t\tau.\, s_1$, або в $\tau.\, s_1'$, або в s_1'', отже була би перемінна з $t\tau$ аж по s_1.

3. Остають ще тільки такі випадки, що v трансформує одно T в $T_1.s_\pi$, а друге T в $t\tau.s_{\pi'}$; тодї v^2 мусить трансормувати перше T в $t\tau.\, s_\varphi$, а друге T в $T_2.\, s_{\varphi'}$, і навпаки. Тут треба ще розріжнити, чи перше T є ідентичне з T_1 — а очивидно друге T з T_2 —, чи ні. *Ті дві можливости дають одинокі нові субституції, яких ще нема в ґрупі* K. Їх можна написати так:

$$v_1^{-1} t v_1 = \tau s_\alpha, \qquad v_2^{-1} t v_2 = t\tau s_\gamma,$$
$$v_1^{-1} \tau v_1 = t\tau s_\beta; \qquad v_2^{-1} \tau v_2 = t s \delta,$$

або в вигіднїйшій формі

$$t v_1 = v_1 \tau s \alpha, \qquad t v_2 = t\tau s \gamma,$$
$$\tau v_1 = v_1 t\tau s_\beta; \qquad \tau v_2 = v_2 t s \gamma. \tag{29}$$

Обчислимо тепер v_1 і v_2.

§. 118. Приймім, що шукані субституції є такі:

$$\left.\begin{aligned} v_1 &= |\, h,\ k \quad Ah + Bk,\ Ch + Dk \,|\,, \\ v_2 &= |\, h,\ k \quad \mathrm{A}h + \mathrm{B}k,\ \Gamma h + \Delta k \,|\,. \end{aligned}\right\} \tag{30}$$

З (29) одержуємо такі системи лїнійних рівнань:

$$\left.\begin{aligned} &A = \alpha B,\ B = \alpha A;\ C = -\alpha D,\ D = \alpha C; \\ &C = -\beta B,\ D = \beta A;\ A = -\beta D = \beta C; \end{aligned}\right\} \tag{31}$$

і

$$\left.\begin{aligned} &\mathrm{A} = -\gamma \mathrm{B},\ \mathrm{B} = \gamma \mathrm{A};\ \Gamma = \gamma\Delta,\ \Delta = -\gamma\Gamma; \\ &\Gamma = \delta \mathrm{A},\ \Delta = -\delta \mathrm{B};\ \mathrm{A} = \delta\Gamma,\ \mathrm{B} = -\delta\Delta. \end{aligned}\right\} \tag{32}$$

Ні одна з тих величин не може бути зером, бо тодї субституції або не мали би значіня, або належали би до иншої ґрупи, або врештї вели би до непервісних ґруп.

З (31) і (32) слїдує в першій мірі

$$\alpha^2 = 1,\ \beta^2 = -1,\ \gamma^2 = -1,\ \delta^2 = 1; \tag{33}$$

оба середнї рівнаня треба радше вважати конґруенціями з модулом p, отже вони є тодї рішимі, коли $p \equiv 1\ (mod.\ 4)$, а нерішимі, коли $p \equiv -1\ (mod.\ 4)$. Назвім j корінь конґруенції

$$j^2 \equiv -1 (mod.\ 4), \tag{34}$$

і шукаймо, коли вона має дїйсну, а коли мниму розвязку.

§. 119. *Перша можливість.* (Форма $\mathfrak{A}$). $p \equiv 1\ (mod.\ 4)$. Конґруенцію (34) можна розвязати в дїйсних числах, отже $\beta = j$. З двовартісного $\alpha = \pm 1$ (33) маємо дві такі системи розвязок для (31):

$$1.\ A = +B,\ C = -D;\ 2.\ A = -B,\ C = +D;$$

але що вони обі виходять на одно, бо треба в данім разї переставити тільки показчики, беремо $A = B$ і $C = -D$, і маємо дальше $C = -jB$, $D = jA$. Заступаючи ще тільки в v_1 показчик k величиною λk і ввзначуючи λ з конґруенції
$\lambda\gamma \equiv 1\ (mod.\ p)$ маємо

$$v_1 = |\ h,\ k \quad A(h+h),\ A(h-k)\ |\ ;$$

чинник A можемо вилучити при помочи субституції s_A, отже найпростїйша форма буде

$$v_1 = |\ h,\ k \quad h+k,\ h-k\ | \qquad (35)$$

Подібно обчислюємо v_2:

$$v_2 = |\ h,\ k \quad h-jk,\ h+jk\ |\ . \qquad (36)$$

Таким чином одержуємо третїй тип (форму $\mathfrak{A}$) шуканих ґруп, $\mathfrak{G}_{III}\mathfrak{A}$. В їх склад входять:

$$g = g_1^{\alpha} g_2^{\beta},\ (\alpha,\ \beta = 0,\ 1,\ \ldots,\ p-1);\ \text{порядок}\ p^2 - 1;$$
$$s_a = |\ h,\ k \quad ah,\ ak\ |\ ,\ (a = 1,\ 2,\ \ldots,\ p-1);\ \text{порядок}\ p-1;$$
$$s = |\ h,\ k \quad h, -k\ |\ ;\ \text{порядок}\ 2;$$
$$\tau = |\ h,\ k\ k,\ h\ |\ ;\ \text{порядок}\ 2;$$
$$v_1 = |\ h,\ k\ h+k,\ h-k\ |\ ;\ \text{порядок}\ 2;$$
$$v_2 = |\ h,\ k\ h-jk,\ h+jk\ |\ ;\ j^2 \equiv -1\ (mod.\ p);\ \text{порядок}\ 3;$$

отже

$$r_{III}\mathfrak{A} = 3.2.2.2.(p-1).\ p^2 = 24\ (p-1)\ p^2. \qquad (37)$$

§. 120. **Друга можливість** (Форма $\mathfrak{B}$). $p \equiv -1\ (mod.\ 4)$. З огляду на те, що конґруенція (34) не має дійсних корінів, представляємо субституції t і τ в иншій формі. До того надаєть ся найлїпше третя нормальна форма у видї

$$t = |\ h, k \quad (m+nj)h,\ (m-nj)k\ |\ ; \qquad (38)$$

тут також і показчики є злученими числами:

$$h = h' + k'j,\ k = h' - k'j;$$

се дає

$$t = |\ h,\ k\ mh - nk,\ nk + mk\ |\ . \qquad (38a)$$

Субституція τ з ґрупи K

$$\tau = |\ h,\ k\ \mu h + \nu k,\ \xi h + \pi k\ |$$

є з t перемінна аж по s_l

$$t\tau = \tau.s_l,$$

а звідси слїдує:

$$\left.\begin{array}{l|l} m\mu - n\xi = \lambda(m\mu + n\nu), & m\xi + n\mu = \lambda\,(m\xi + n\pi), \\ m\nu - n\pi = \lambda(-n\mu + m\nu); & m\pi + n\nu = \lambda(-n\xi + m\pi). \end{array}\right\} \qquad (39)$$

Отся система є однородна й лінійна у величинах μ, ν, ξ, π, отже її детермінанта мусить бути зером:

$$\begin{vmatrix} (1-\lambda)\,m, & -\lambda n, & -n, & 0 \\ \lambda n, & (1-\lambda)m, & 0, & -n \\ n, & 0, & (1-\lambda)m, & -\lambda n \\ 0, & n, & \lambda n, & (1-\lambda)m \end{vmatrix} = 0.$$

З неї одержуємо рівнане для λ, m, n. Її вартість є:

$$[(1-\lambda)((1-\lambda)m^2 + (1+\lambda)n^2)]^2 = 0; \qquad (40)$$

се можливе тільки так, що або $1-\lambda = 0$, або виражене в грубшій скобці є 0. Перше не має значіня, друге дає $m = 0$, і або $n = 0$, або $\lambda = -1$; $n = 0$ є неможливе, отже зістає тільки $\lambda = -1$. Звідси дістаємо

$$t = \mid h, k \quad nh, -nk \mid$$

або в найпростійшій формі

$$t = \mid h, k \quad h, -k \mid ; \qquad (41)$$

подібно маємо, з огляду на те, що $\xi = \nu$, $\pi = -\mu$,

$$\tau = \mid h, k \quad \mu h + \nu k, \ \nu h - \mu k \mid \qquad (42)$$

§. 121. Реляції (29) можемо тут примінити без застережена. З них маємо

$$C = \alpha(A\mu + B\nu),\ D = -\alpha(A\nu - B\mu);\ A = -\alpha(C\mu + D\nu),\ B = \alpha\,(C\nu - D\mu);$$

$$A\mu + C\nu = \beta(A\nu - B\mu),\ B\mu + D\nu = -\beta(A\mu + B\nu);$$

$$A\nu - C\alpha = \beta\,(C\nu - D\mu),\ B\nu - D\mu = -\beta\,(C\mu + D\nu); \qquad (43)$$

і

$$\Gamma = \gamma(\mathrm{A}\nu - \mathrm{B}\mu),\ \Delta = -\gamma(\mathrm{A}\mu + \mathrm{B}\nu);\ \mathrm{A} = -\gamma(\Gamma\nu - \Delta\mu),$$

$$B = \gamma\,(\Gamma\mu + \Delta\nu); \qquad (44)$$

$$\mathrm{A}\mu + \Gamma\nu = -\mathrm{B}\delta,\ \mathrm{A}\nu - \Gamma\mu = -\delta\Delta;\ \mathrm{B}\mu + \Delta\nu = \mathrm{A}\delta,\ \mathrm{B}\nu - \Delta\mu = \Gamma\delta.$$

З тих двох систем маємо насамперед:

$$\alpha^2(\mu^2 + \nu^2) \equiv -1 \ (mod\ p). \qquad (45)$$

Отся конґруенція є все рішима для $p \equiv -1$ $(mod.\ 4)$, коли тільки поставимо $\alpha^2 = 1$, т. зн. $\alpha = -1$ ($\alpha = +1$ мусимо виключити). Нехай μ, ν буде довільною парою чисел, яка сповняє конґруенцію (45), то ті два числа можна поставити в субституції τ; отже тепер μ і ν не є вже довільними числами, тільки вони звязані реляцією (45).

Рівнаня (43) дають

$$v_1 = \mid h, k \quad \mu k + (\nu + 1)k,\ (\nu - 1)h - \mu k \mid ;\ \text{порядок } 2; \qquad (46)$$

з (44) маємо

$$v_2 = | \, h, \, k \quad -(1+\mu\nu)h+(\mu-\nu^2)\,k, \; (\nu+\mu^2)\,h+(\mu\nu-\mu+\nu)k \, | \, ;$$

порядок 3. (47)

Таким чином доходимо до третього типу (форма $\mathfrak{B}$) $G_{\mathrm{III}\mathfrak{B}}$ шуканих ґруп:

$$g = g_1^{\alpha} g_2^{\beta}; \text{ порядок } p^2;$$

$$s_a = | \, h, \, k \;\; ah, \, ak \, | \, , \; (a = 1, 2, \;\; ., \, p-1); \text{ порядок } p-1;$$

$$t = | \, h, \, k \;\; k, \, -h \, | \; ; \text{ порядок } 2;$$

$$\left.\begin{array}{c} \tau = | \, h, \, k \;\; \mu k + \nu k, \; \nu h - \mu k \, | \; ; \text{ порядок } 2; \\ v_1 = | \, h, \, k \;\; \mu h + (\nu+1)k, \; (\nu-1)h - \mu k \, | \; ; \text{ порядок } 2; \\ v_2 = | \, h, \, k \;\; -(1+\mu\nu)h + (\mu-\nu^2)k, \; (\nu+\mu^2)h + (\mu\nu-\mu+\nu)k \, | \; ; \\ \text{порядок } 3; \end{array}\right\} \mu^2+\nu^2 \equiv -1 \; (mod. \; p)$$

порядок ґрупи є рівно-ж

$$r_{\mathrm{III}\mathfrak{B}} = 24 \; (p-1)p^2.$$

§. 122. Субституції тої ґрупи τ_1, v_1 і v_2 містять в собі довільну пару розвязок конґруенції (45); длятого мусимо ще доказати, що довільність в виборі чисел μ і ν не спричинює зміни ґрупи $G_{\mathrm{III}}\;\mathfrak{B}$, т. зн., що дві субституції, утворені з двох ріжних пар розвязок, μ_1, ν_1; μ_2, ν_2 можна представити взаїмно як добутки з инших субституцій тої самої ґрупи, независимих від конґруенції (45).

Тут є дві можливости:

1. Конґруенція має тільки одну пару розвязок, $| \, a \, |$ і $| \, b \, |$; з тих чисел можна утворити вісїм комбінацій:

$$\mu = \pm a, \quad \text{і} \quad \mu = \pm b,$$
$$\nu = \pm b; \quad \quad \nu = \pm a.$$

Всї ті комбінації дають ту саму субституцію, а ріжнять ся тільки в показчику субституції форми s. Перемінїм μ і ν з $-\mu$ і $-\nu$, або числа μ і ν з собою, і введїм скорочене:

$$\tau = | \, h, \, k \;\; \mu h + \nu k, \; \nu h - \mu k \, | = (\mu, \, \nu).$$

Тоді є:

$$\tau' = (-\mu, \, \nu) = \tau. \, s_i, \text{ де } i = \mu^2 - \nu^2,$$
$$\tau'' = (\mu, -\nu) = \tau'. \, s_{-1};$$
$$\tau''' = (-\mu, -\nu) = \tau. \, s_{-1};$$

а так само

$$\tau_1 = (\nu, \, \mu) = \tau. \, s_l, \; l = -2\mu\nu.$$

2. Конґруенція має дві ріжні пари розвязок:

$$\mu_1^2 + \nu_1^2 \equiv -1 \; (mod. \; p),$$
$$\mu_2^2 + \nu_2^2 \equiv -1 \; (mod. \; p).$$

Коли $\tau_1 = (\mu_1, \nu_1)$ і $\tau_2 = (\mu_2, \nu_2)$, то

$$\tau_2 = \tau_1 . u; \quad u = (a, b),$$

де

$$a = -\mu_1\mu_2 - \nu_1\nu_2$$
$$b = \mu_1\nu_2 - \mu_2\nu_1,$$

отже також

$$a^2 + b^2 \equiv -1 \pmod{p}.$$

XIII. Метациклїчні ґрупи степеня p^2.

§. 123. Вишукавши ґрупи степеня p^2, мусимо переконати ся, чи вони відповідають своїй цїли, т. зн., чи є 1. первісні, 2. загальні, 3. метациклїчні.

Ґрупи G_{I}, G_{II}, G_{III} є первісні, бо нї одна з них не має прикмети, спільної всїм непервісним ґрупам, а іменно:

Непервісна лїнїйна ґрупа може мати тільки такі субституції, які переводять дїйсні функції показчиків в їх многократи*).

Доказ. Нехай буде G первісною лїнїйною ґрупою. Елементи, які вона має переставлювати, можна подїлити на кляси, яких не розриває нїяка субституція з G. Ті субституції можуть або тільки пересувати елементи в нутрі одної кляси, або перемінювати кляси поміж собою. Назвім ті кляси (r'), (r''), (r'''), . ., а елементи кождої з них r_1', r_2', . . .; r_1'', r_2'', . . .; r_1''', r_2''' . . .; . . .

Субституції g є перехідні у всїх елементах; нехай

$$g' = | h, k \quad h + \alpha', k + \beta' | \qquad (1)$$

переводить елемент r_1' в r'_q серед тої самої кляси, то вона не розірве кляси (r'). Можемо доказати, що g' не розірве взагалї нї одної кляси.

Нехай буде (r'') другою клясою елементів; поміж субституціями g мусить бути одна така

$$g'' = | h, k \quad h + \alpha'', k + \beta'' | , \qquad (2)$$

яка переводить кожде r_i' в r_i''; отже вона переведе цїлу систему (r') в (r''). Субституція g' може пересувати елементи (r') тільки поміж собою, отже

$$g''^{-1} \, g' \, g''$$

може пересувати тільки елементи (r''). Субституції g' і g'' є перемінні, отже $g''^{-1} \, g' \, g'' = g'$ буде пересувати елементи (r'') і взагалї в кождій клясї (r). З того слїдує, що така субституція не розриває нї одної кляси.

Ту прикмету може мати тільки субституція g' і її степенї; всї инші субституції, нпр.

*) Jordan, Sur les équations du dégré p^2, стр. 128.

$$g_1 = | h, k \quad h+\alpha_1, k+\beta_1 |, \qquad (3)$$

можуть тільки переміщувати кляси. Конечною і достаточною умовою, щоби субституція g_1 не була степенню субституції g', є те, що конґруенції

$$\left.\begin{aligned} m\alpha' &\equiv \alpha_1 \\ m\beta' &\equiv \beta_1 \end{aligned}\right\} (mod.\ p) \qquad (4)$$

не можуть істнувати рівночасно, коли приймемо

$$\alpha'\beta_1 - \alpha_1\beta' \equiv|\equiv 0 \ (mod.\ p); \qquad (4a)$$

m ціле число, $< p$.

Отже ґрупа G складаєть ся з двох родів субституцій g:

1. з g', які переставляють елементи тільки в нутрі поодиноких кляс;

2. з g_1, які пересувають кляси поміж собою.

Инакших субституцій нема в G, бо кляси як такі мусять оставати нерозірвані.

Субституції g' і g_1 є переміннї, отже ґрупа G є Абелева; кожда її субституція має форму

$$g = g'^{\eta} g_1^{\vartheta} \qquad (5)$$

Тепер шукаймо таких двох функцій показчиків, щоби g' збільшувало першу з них о s, а другої не змінювало, а g_1 навпаки. Нехай ті функції будуть

$$\left.\begin{aligned} h_1 &= mh + nk, \\ k_1 &= qh + rk, \end{aligned}\right\} \qquad (6)$$

тоді мусять істнувати таки пари конґруенцій:

$$\left.\begin{aligned} m\alpha' + n\beta' &\equiv 1, \\ m\alpha_1 + n\beta_1 &\equiv 0; \end{aligned}\right\} (mod.\ p) \qquad (7a)$$

$$\left.\begin{aligned} q\alpha' + r\beta' &\equiv 0, \\ q\alpha_1 + r\beta_1 &\equiv 1; \end{aligned}\right\} (mod.\ p). \qquad (7b)$$

ті конґруенції є все рішимі, бо їх детермінанта (4a) не є 0.

Впроваджуючи ті нові показчики, маємо:

$$\begin{aligned} g' &= | h, k \quad h+1, k |, \\ g_1 &= | h, k \quad h, k+1 |; \end{aligned} \qquad (8)$$

показчики h_1 і k_1 заступили ми старими h і k, бо се виходить на одно.

Кожда инша субституція з G,

$$t = | h, k \quad ah + bk, ch + dk |,$$

трансформує

$$\left.\begin{array}{lll} g' & \text{в} & g'^{\frac{d}{\Delta}} g_1^{-\frac{c}{\Delta}}, \\ g_1 & \text{в} & g'^{-\frac{b}{\Delta}} g_1^{\frac{a}{\Delta}}; \end{array}\right\} \quad (\Delta = ad - bc \not\equiv 0)$$

трансформовані субститудії мають ті самі прикмети що первісні, отже мусить бути $b=0$, $c=0$, т. зн.

$$t = | h, k \quad ah, dk | . \tag{9}$$

Отся субституція множить кожду дійсну функцію показчиків (6) сталим чинником; наше твердженє є проте доказане.

§. 124. Ґрупи степеня p^2 мають такі субституції, які не сповнюють наведених тут умов.

1. Ґрупа G_I має в собі субституцію

$$\sigma_2 = | h, k \quad k, h | ,$$

яка не є форми (9).

2. Так само в ґрупі G_{II} є субституція

$$\sigma_1 = | h\ k,\ ah + bke,\ bh + ak | ,$$

яка не допускає такого добору функцій h_1 і k_1, тим більше, що тут маємо до діла зі злученими величинами.

3. Субституції v_1 і v_2 в обох своїх формах є занадто скомплїковані, щоби могли виконувати таку просту переміну.

Таким чином ми доказали, що наші ґрупи не можуть бути непервісні.

§. 125. Тепер займаємо ся питанем, коли ґрупи G є загальні і ріжні поміж собою.

I. Твердженє. Кожда ґрупа G_I для $p=3$ і $p=5$ містить ся в G_{III}; так само кожда ґрупа G_{II} для $p=3$.

Доказ. 1. G_I; $p=3$. Субституція

$$u = | h, k \quad h+k, h-k | \tag{11}$$

є перемінна з ґрупою G_I, отже $\{G_I, u\}$ творить загальнїйшу метациклїчну ґрупу, яка містить ся в $G_{III}8$; $u = \tau$.

2. G_I; $p=5$. Комбінуючи ґрупу G_I з

$$\left.\begin{array}{r} u_1 = | h, k \quad h, -k | , \\ u_1 = | h, k \quad h+k, -2h+2k | , \end{array}\right\} \tag{11}$$

одержимо метациклїчну ґрупу, загальнїйшу від G_I, яка є підґрупою третього типу G_{III}; $u_1 = ts_2$, $u_2 = v_1 ts_2$.

3. G_{II}; $p=3$. Для $p=3$ є $e=-1$, отже

$$\left.\begin{array}{r} \sigma_1 = | h, k \quad ah - bk, bh + ak | , \\ a^2 + b^2 \not\equiv 0 \ (mod. p). \end{array}\right\}$$

Утворивши ґрупу $\{G_{II}, u\}$, де

$$u = | \, h, \; k \quad \alpha h + \beta k, \; \beta h - \alpha k \, | \, , \tag{12}$$

а α і β сповнюють умову

$$(\alpha^2 + \beta^2)(a^2 + b^2) + 1 \equiv\!\mid\!\equiv 0 \; (mod.\; 3), \tag{13}$$

загальнїйшу ґрупу, яка містить в $G_{III}\vartheta$; $u = \sigma_1^{-1}\tau$.

§. 126. Отсе ті одиноко можливі виїмки, що наші ґрупи є підґрупами ґруп инших типів.

II. Твердженє. *Ґрупа* G_I *є загальна для* $p > 5$, G_{II} *для* $p > 3$, G_{III} *все.*

Доказ. Крітерією загальности є те, що порядок ґрупи мусить бути многократою порядку кождої підґрупи. Коли отся крітерія не вистарчає, доказуватимемо твердженє безпосередно.

1. G_I не може містити ся в G_{II}, бо

$$\frac{r_{II}}{r_I} = \frac{2(p^2-1)p^2}{2(p-1)^2p^2} = \frac{p+1}{p-1}$$

не може бути цїлим числом, коли $p > 3$.

2. Так само G_{III} не може містити ся в G_I, бо

$$\frac{r_I}{r_{II}} = \frac{p-1}{p+1}$$

ніколи не є цїлим числом.

Дальше слїдують безпосередні докази.

1. G_I не може містити ся в G_{III}, бо в G_I містить ся субституція форми σ_1

$$\sigma_1 = | \, h, \; k \quad \varrho h, \; k \, | \, , \tag{14}$$

де ϱ є первісний корінь $(mod.\; p)$, яка не змінює рівно p корінів, а саме тих, яких перший показчик є p. Кожда инша субституція, яка має ту саму прикмету, є комбінацією того σ_1 з

$$g_2 = | \, h, \; k \quad h, \; k+1 \, | \, ,$$

т. зн.

$$\sigma = \sigma_1 g_2{}^{\lambda} = | \, h, \; k \quad \varrho h, \; k + \lambda \, | \, . \tag{15}$$

r-та степень тої субституції є

$$\sigma^r = | \, h, \; k \quad \varrho^r h, \; k + \lambda r \, | \, ; \tag{16}$$

вона мусить зіставляти без зміни ті самі корінї, в числї p, що σ_1 і σ. Те можливе тільки тодї, коли $\beta = 0$ і $\varrho^r \equiv 1$ $(mod.\; p)$; з того бачимо, що тільки субституція σ_1 і її степенї дають бажану переставку. Твердженє Fermat'а дає: $r = m(p-1)$.

Означім якусь субституцію з ґеометричної ґрупи третього типу u і шукаймо тих степений субституцій u, які є перемінні з τ (т. є з t або τ) аж по s_1:

$$Tu^{\mu} = u^{\mu} T, s_1 ; \tag{17}$$

легко провірити, що $\mu \leqq 4$. Кожда субституція, перемінна з τ, має форму

$$s_a = | h, k \quad ah, a k | ,$$

отже $u^\mu = s_a$.

Коли-б субституція σ_2 містила ся в G_{III}, то одна з її степеней мусїла-б бути перемінна з T, т. зн. мусїла-б мати форму s; воно можливе тільки для $\mu = r$. Звідси виходить суперечність: r є многократю числа $p-1$, а μ є що найбільше 4, отже для $p > 5$ ґрупа G_I не може містити ся в G_{III}.

2. G_{II} не може містити ся в G_{III}, бо коли u є субституцією з G_{III}, то u^r $(r \leqq 4)$ редукує ся на

$$u' = | h, k \quad ah + \alpha, bk + \beta | ; \tag{18}$$

$(p-1)$-ша степень тої субституції редукує ся на

$$\begin{aligned} u'' = | h, k \quad & a^{p-1} h + (a^{p-1} + a^{p-2} + \ldots + 1)\, \alpha, b^{p-1} k + (b^{p-1} + b^{p-2} + \ldots + 1)\, \beta | \\ = & | h, k \quad h + \alpha, k + \beta | \end{aligned} \tag{19}$$

а p-та степень тої субституції є $\equiv 1$.

G_{II} має субституцію σ_2 порядку $p^2 - 1$; отже всї ті її степені, які редукують ся на 1, мають порядок $c(p^2-1)$; коли-б σ_1 містило ся в G_{III}, то

$$\frac{r(p-1)p}{c(p^2-1)} = \frac{rp}{c(p+1)}$$

мусїло-б бути цїлим числом; p і $p+1$ є супроти себе перві, отже r мусїло би бути многократю числа $p+1$, а се неможливе для $r \leqq 4$, $p > 3$.

§. 127. Остає ще тільки виказати, що ґрупа G_{III} є загальна.

1. G_{III} не може містити ся в G_I. Возьмім субституції

$$\left.\begin{aligned} u' &= | h, k \quad ah + \alpha, bk + \beta | , \\ u'' &= | h, k \quad ak + \alpha, bh + \beta | , \end{aligned}\right\} \tag{20}$$

яких квадрати є

$$\left.\begin{aligned} u'^2 &= | h, k \quad a^2 h + (a+1)\alpha, b^2 k + (b+1)\beta | , \\ u''^2 &= | h, k \quad abh + (a\beta + \alpha), abk + (b\alpha + \beta) | . \end{aligned}\right\} \tag{21}$$

Обі ті субституції є в G_I: $u' = \sigma_1 g$, $u'' = \sigma_1 \sigma_2 g$, отже і субституція

$$w = u'^{-2} u''^{-2} u'^2 u''^2 \tag{22}$$

містить ся в G_{III}; вона редукує ся на

$$w = | h, k \quad h + \eta, k + \vartheta | , \tag{23}$$

де η і ϑ дані рівнанями

$$\left.\begin{aligned} a^2 b \eta &\equiv (a^2 - 1)\beta - (a+1)(b-1)\alpha , \\ a b^2 \vartheta &\equiv (b^2 - 1)\alpha - (b+1)(a-1)\beta . \end{aligned}\right\} \tag{24}$$

Порядок субституції w є p або 1; те друге є тодї, коли $\eta=0$, $\vartheta=0$.

2. G_{II} містить в собі подібну субституцію як G_{I} з тою ріжницею, що тут є показчики числами сполученими; w має також і тут порядок p або 1.

3. G_{III} не може містити в собі такої субституції порядку p або 1. Возьмім v_2 за u', а $v_2 t$ за u'', то се дасть:

$$w=v_2^{-2}(v_2t)^{-2}v_2^{2}(v_2t)^{2}=t\tau \tag{22}$$

отже субституцію порядку 4 ($=\!|\!=p$, $=\!|\!=1$).

Таким чином ми вичерпали всї можливости і виказали, що виймаючи G_{I} для 3 і 5, і G_{II} для 3 всї типи ґруп є загальні, т. є. не можна одного з них переводити в другий. З тих доказів бачимо також, що всї ті типи є поміж собою ріжні.

§. 128. Тепер уставимо ряди зложеня для наших ґруп. Коли нам вдасть ся розложити ті ґрупи так, щоби їх показчики були первими числами, то се буде доказом, що ґрупи є метациклічні. Побачимо, що се справдї можливе.

Всї три типи ґруп мають спільну визначну підґрупу M порядку p^2, яка переставляє оба показчики корінів; субституції тої ґрупи можна представити як добуток двох односторонних субституцій

$$g=g_1^{\alpha}g_2^{\beta}(\alpha,\ \beta=0,\ 1,\dots,\ p-1) \tag{25}$$

Порядок ґрупи M є p^2; приймаючи $\beta=0$, одержимо Абелеву ґрупу N, зложену з односторонних субституцій g_1. Таким чином маємо вже кінцеву частину ряду зложеня для G з відповідним рядом показчиків

$$\begin{matrix} M, & & N, & & 1, \\ & p, & & p. & \end{matrix} \tag{26}$$

Та частина ряду зложеня є для всїх трьох ґруп спільна. Від тепер мусимо розкладати кождий тип з окрема.

§. 129. В першім типі маємо таку зложену субституцію

$$\sigma_1=|\ h,\ k\quad ah,\ bk\ | \tag{27}$$

яку можемо опять розложити на дві односторонні

$$s=|\ h,\ k\quad ah,\ k\ |,$$
$$t=|\ h,\ k\quad h,\ bk\ |;$$

найпростїйша форма тих субституцій буде, коли за a і за b положимо ϱ, первісний корінь числа p:

$$\left.\begin{aligned} s&=|\ h,\ k\quad \varrho h,\ k\ |, \\ t&=|\ h,\ k\quad h,\ \varrho k\ |, \end{aligned}\right\} \tag{28}$$

отже

$$\sigma_1 = s^a t^b \ (a, b = 0\ 1, 2, \ldots, p-2). \tag{29}$$

Держимо ся тут зовсїм такої самої методи, як при метациклїчних ґрупах степеня p; розкладаємо $p-1$ на перві чинники

$$p - 1 = k_1 k_2 \qquad k_\nu \tag{30}$$

і творимо субституції

$$\left.\begin{array}{l} s_\nu = s^{\frac{p-1}{k_\nu}}, \\ t_\nu = t^{\frac{p-1}{k_\nu}}; \end{array}\right\} \tag{31}$$

їх порядки є однакові, k_ν. До ґрупи порядку M добираємо субституцію t_ν і одержуємо ґрупу L''_ν порядку $k_\nu . p^2$; її показчик з огляду на M є k_ν. Добираючи до L''_ν ще s_ν, одержуємо ґрупу L'_ν порядку $k_{\nu-1}{}^2\ p^2$, з показчиком k_ν.

Тепер творимо знов субституції

$$\left.\begin{array}{l} s_{\nu-1} = s^{\frac{p-1}{k_\nu k_{\nu-1}}}, \\ t_{\nu-1} = t^{\frac{p-1}{k_\nu k_{\nu-1}}}; \end{array}\right\} \tag{32}$$

їх $k_{\nu-1}$-ті степені містять ся вже в L'_ν і L''_ν, отже їх порядок є $k_{\nu-1}$. При їх помочи творимо дальше ґрупи $L''_{\nu-1}$ і $L'_{\nu-1}$ порядків $k_{\nu-1}\ k_\nu{}^2 p^2$ і $k_{\nu-1}{}^2 k_\nu{}^2 p^2$ з показчиками $k_{\nu-1}$ і $k_{\nu-1}$. Так поступаємо все дальше, аж врештї з субституціями

$$\left.\begin{array}{l} s_1 = s^{\frac{p-1}{k_\nu \cdots k_1}} = s \\ t_1 = t^{\frac{p-1}{k_\nu \cdots k_1}} = t \end{array}\right\} \tag{33}$$

вичерпаємо всї субституції σ_1 і одержимо ґрупу L'_1.

Зістала ще тільки транспонуюча субституція σ_2 порядку 2, яку добираємо до L'_1 як найвисший член ґрупи G_{I}. Отже наш ряд зложеня з рядом відповідних показчиків виглядає так:

$$\begin{array}{l} G_{\mathrm{I}},\ L'_1,\ L_1'',\ L'_2,\ L''_2, \quad .,\ L'_\nu,\ L''_\nu,\ M,\ N,\ 1, \\ \quad 2,\ k_1,\ \ k_1,\ k_2,\ \ k_2 \quad\ .,\ k_\nu,\ k_\nu,\ p,\ p. \end{array} \tag{34}$$

Всї показчики є первими числами, отже G_{I} **метациклїчною ґрупою.**

§. 130. Зовсїм подібно поступаємо при **третїм** **типі**. Тут маємо субституцію

$$s_\alpha = |\ h, k \quad ah, ak\ |, \tag{35}$$

яку ми назвали **рівнобічною**. Напишім за a опять ϱ, то одержимо найпростїйшу її форму

$$s_\varrho = s = | h, k \quad \varrho h, \varrho k | , \tag{36}$$

отже

$$s_\alpha = s^\alpha \ (\alpha = 0, 1, \quad ., p-2). \tag{37}$$

За вихідну точку беремо субституцію $s^{\frac{p-1}{k_\nu}}$
і творимо чергою такі субституції:

$$\left.\begin{array}{l} s_\nu = s^{\frac{p-1}{k_\nu}}, \\ s_{\nu-1} = s^{\frac{p-1}{k_\nu k_{\nu-1}}} \\ \quad . \\ s_1 = s^{\frac{p-1}{k_\nu \ldots k_1}} = s \end{array}\right\} \tag{38}$$

порядків k_ν, $k_{\nu-1}$, . ., k_1. З них творимо ґрупи комбінуючи їх по черзї з ґрупою M. Се дає: L_ν, $L_{\nu-1}$, . ., L_1, ґрупи порядків $k_\nu p^2$, $k_{\nu-1}\, k_\nu p^2$, . ., $k_1 k_2 \quad k_\nu p^2 = (p-1)\, p^2$, показчиками будуть числа k_ν, $k_{\nu-1}$, ., k_1.

Вичерпавши всї субституції s_a, маємо ще чотири инші t, τ, v_1, v_2, яких форма залежить від числа p. В формі $\mathfrak{A}$ $(p = 4n+1)$ маємо:

$$t^2 = 1,\ \tau^2 = 1,\ v_1^{\,2} = s_2,\ v_1^{\,3} = s_{2(1+j)},$$

отже v_1 і v_2 переходять в другій, згл. третїй степені в якесь s.

В формі $\mathfrak{B}$ $(p = 4n-1)$ є

$$t^2 = s_{-1},\ \tau^2 = s_{-1},\ v_1^{\,2} = s_2,\ v_2^{\,3} = s_m,$$

отже всї чотири субституції переходять в s. Звідси маємо таку конструкцію ряду: добираючи t до L_1, одержуємо K; далї добираємо τ і маємо J, а вкінцї v_1 і v_2 і маємо H і і G_{III}. Порядки тих ґруп є такі: $(K) = 2(p-1)p^2$, $(J) = 4(p-1)p^2$, $(H) = 8(p-1)p^2$ або $12(p-1)p^2$, $(G_{\text{III}}) = 24(p-1)p^2$. Отже ряди зложеня і показчиків для G_{III} є:

$$\left.\begin{array}{l} G_{\text{III}},\ H,\ J,\ K,\ L_1,\ L_2, \quad .,\ L_\nu,\ M_1,\ N_1,\ 1. \\ (2,\ 3),\ (2,\ 2)\ k_1,\ k_2, \quad .,\ k_\nu,\ p,\ p. \end{array}\right\} \tag{39}$$

Числа, замкнені в скобках, значать, що пари субституцій v_1 і v_2, t і τ можемо добирати в довільнім порядку.

§. 134. В **другім типі** поступаємо трохи инакше, а то тому, що тут σ_1 має більше скомплїковану будову. Коли

$$\sigma_1 = | h, k \quad ah + bek,\ bh + ak | ,\ e \text{ — не-останок } (mod.\ p), \tag{40}$$

тодї шукаємо такої лїнїйної однородної функції показчиків

$$\varphi = mh + nk,$$

яка під впливом σ_1 зміняла би ся в свою многократь. Анальоґічно як при вишукуваню нормальної форми маємо тут такі конґруенції:

$$\left.\begin{array}{l} ma + nb \equiv m\varrho, \\ mbe + na \equiv n\varrho \end{array}\right\} (mod.\ p), \tag{41}$$

з яких визначуємо ϱ

$$\begin{vmatrix} a - \varrho, & b \\ be, & a - \varrho \end{vmatrix} \equiv 0\ (mod.\ p),$$

т. зн.

$$\varrho^2 - 2a\varrho + a^2 - b^2 e \equiv 0\ (mod.\ p) \tag{42}$$

Звідси слїдує;

$$\varrho \equiv a \pm b\sqrt{e}\ (mod.\ p);$$

ϱ має дві вартости, ϱ_1 і ϱ_2; вони є дїйснї або злучені відповідно до того, чи e є додатне, чи відємне. В такім разї можна представити σ_1 простійше так:

$$t = |\ h,\ k \quad \varrho_1 h,\ \varrho_2 k\ |\ , \tag{44}$$

де

$$\left.\begin{array}{l} \varrho_1 \equiv a + b\sqrt{e} \\ \varrho_2 \equiv a - b\sqrt{e} \end{array}\right\} (mod\ \ p) \tag{45}$$

Тепер йде розклад подібно як перше. Порядок субституції t є $p^2 - 1$, бо з поміж можливих p^2 комбінацій чисел a і b мусимо виключити $a = 0$, $b = 0$.

$p^2 - 1$ є все подїльне через 8; тому в рядї показчиків буде число 2 приходити три (або більше) разів. Длятого мусимо шукати таких субституцій t_1, t_2, t_3, щоби було:

$$t_1^{\,2} = 1,\ \ t_2^{\,2} = t \text{ або} = 1;\ \ t_3^{\,2} = t_2^{\,q}\ (q = 0,\ 1,\ 2). \tag{46}$$

Коли

$$t_1 = |\ h\ \ k \quad \lambda_1 h,\ \mu_1 k\ |\ ,$$

то мусить бути $\lambda_1^{\,2} \equiv 1$, $\mu_1^{\,2} \equiv 1$ $(mod.\ p)$, т. зн. мусить істнувати така пара конґруенцій:

$$\left.\begin{array}{l} a^2 + b^2 e \equiv 1, \\ 2ab\sqrt{e} \equiv 0. \end{array}\ (mod.\ p).\right\} \tag{47}$$

Розвязку тих конґруенцій називаємо a_1, b_1. Дальше мусить бути

$$t_2 = |\ h,\ k \quad \lambda_2 h,\ \mu_2 k\ \ |$$

таке, щоби було $\lambda_2^{\,2} \equiv 1$, $\mu_2^{\,2} \equiv 1$ $(mod.\ p)$, або $\lambda^2_2 \equiv \lambda_1$, $\mu_2^{\,2} \equiv \mu_1$ $(mod. p)$. В першім разї беремо ту саму розвязку, що в (47), в другім творимо нові конґруенції

$$\left.\begin{array}{l} a_2 + b^2 e \equiv a_1, \\ 2ab\sqrt{e} \equiv b_1\ ; \end{array}\right\} (mod.\ p) \tag{48}$$

їх розвязка нехай буде a_2, b_2. Тепер визначуємо так само t_3, т. є або 1). $\lambda_3^{\,2} \equiv 1$, $\mu_3^{\,2} \equiv 1$; або 2). $\lambda_3^{\,2} \equiv \lambda_1$, $\mu_3^{\,2} \equiv \mu_1$; або 3). $\lambda_3^{\,2} \equiv \lambda_2$, $\mu_3^{\,2} \equiv \mu_2$. Третя можливість дасть нову пару конґруенцій, яка буде мати розвязку a_3, b_3.

На подібній дорозї обчисляємо дальші су туції, розкладаючи число p^2-1 на перві чинники:

$$p^2 - 1 = l_1 l_2 \ldots l_\mu \tag{49}$$

добираємо такі субституції τ_μ, $\tau_{\mu-1}$, . ., τ_1, щоби їх l_μ-та, $l_{\mu-1}$, -та, . ., l_1-та степень містила ся в попередній. До кождої із них будемо мусїли розвязати одну пару конґруенцій.

Тепер укладаємо ряд для G_{II}; беремо чергою субституції τ_μ, $\tau_{\mu-1}$, . ., τ_1 і комбінуємо їх все з попередньою ґрупою, так що одержимо ряд ґруп L_μ (степень $l_\mu\, p^2$), $L_{\mu-1}$ (степень $l_{\mu-1}\, l_\mu\, p^2$), . ., L_1 (степень $l_1 l_2 \ldots l_\mu p^2 = (p^2-1)\, p^2$); показчики будуть тут l_μ, $l_{\mu-1}$, , l_1.

Вкінцї добираємо ще σ_2 і маємо вже повну ґрупу G_{II} з рядами зложеня і показчиків.

$$\left.\begin{array}{l} G_{II},\ L_1,\ L_2,\ \ldots,\ L_\mu,\ M,\ N,\ 1 \\ \quad 2,\ l_1,\ l_2,\ \quad\quad l_\mu,\ p,\ p. \end{array}\right\} \tag{50}$$

Субституції τ, які виступають в невимірній або й злученій формі, можна привести назад до вимірного виду.

§. 132. Визначенє ряду зложеня для ґруп G подає заразом дорогу, як треба вести розвязку рівнаня степеня p^2. Приймім, що дане рівнанє

$$f(x) = 0 \tag{51}$$

має сочинники з обсягу (R). Той обсяг розширюємо так, що долучуємо до нього по одному кореневи рівнань первих степенів, так що поміж тими степенями будуть всї числа з ряду показчиків, з виїмком двох остатнїх. Через те ґрупа редукує ся постепенно аж до M; коли назвемо сей розширений обсяг (R'), то рівнанє, яке має ґрупу M, є Абелевим рівнанем степеня p^2. Отсе рівнанє можна розвязати зовсїм, розвязуючи два Абелеві рівнаня степеня p.

Нехай буде

$$F(y) = 0 \tag{52}$$

тим Абелевим рівнанем степеня p^2, якого сочинники належать до обсягу (R'). Називаючи його корінї y_{hk}, творимо при помочи ω, первісного p-того кореня з одиницї, функції:

$$\left.\begin{array}{l} Y_1 = y_{11} + y_{21} + \ldots + y_{p1}, \\ Y_2 = y_{12} + y_{22} + \ldots + y_{p2}, \\ \\ Y\ = y_1 + y_{2p} + \ldots + y_{pp}, \end{array}\right\} \tag{53}$$

$$\left.\begin{aligned} U_1 &= Y_1 + \omega Y_2 + \omega^2 Y_3 + \qquad + \omega^{p-1} Y_p, \\ U_2 &= Y_1 + \omega^2 Y_2 + \omega^4 Y_3 + \qquad + \omega^{2(p-1)} Y_p, \\ &\cdot \qquad\qquad\qquad\qquad\qquad \cdot \\ U_{p-1} &= Y_1 + \omega^{p-1} Y_2 + \omega^{2(p-1)} Y_3 + \ldots + \omega^{(p-1)^2} Y_p; \end{aligned}\right\} \quad (54)$$

до них долучуємо ще вимірну величину

$$U_0 = Y_1 + Y_2 + Y_3 + \ldots + Y_p = a. \qquad (54a)$$

Через те розпадають ся корінї на p кляс неперві́сности по p членів; субституції g_1 пересувають елементи в нутрі поодиноких рядків (53), а g_2 рядки поміж собою. Виконуючи ті субституції на (54), переконаємо ся, що g_1 не змінює тих функцій, а g_2 переводить U_i в $\varepsilon^{-i}\, U_i$. Звідси слїдує, що функції U_i^p належать до ґрупи M; тому можна їх виразити вимірно одною з них.

З рівнань (54) і (54a) маємо

$$Y_i = \frac{1}{p}\left[a + \sum_{n=1}^{p-1} \omega^{-in}\, U_n\right]; \qquad (55)$$

U_n^p є величиною в обсягу (R',ω), нпр. $= u_n$, отже для обчисленя функцій Y_i мусимо витягнути p-тий корінь з величин u_n, які можна означити вимірно:

$$Y_i = \frac{1}{p}\left[a + \sum_{n=1}^{p-1} \omega^{-in} \sqrt[p]{u_n}\right]. \qquad (55a)$$

Отсе вираженє має p^2 вартостий, а Y може мати тільки p ріжних вартостий; щоби усунути злишню многозначність, творимо такі функції

$$\varphi_\lambda = U_\lambda \cdot U_1^{p-\lambda} \; (\lambda = 1, 2, \quad ., p-1); \qquad (56)$$

для $\lambda = 0$ є $\varphi_0 = U_0 \,.\, U_1^p = a u_1$, отже вимірна величина. Кожде φ_λ можна представити одним з них, бо вони всї належать до тої самої ґрупи, т. є до M: анї g_1, анї g_2 не змінюють φ_λ. З того слїдує:

$$U_\lambda = \frac{\varphi_\lambda}{U_1^p} \cdot U_1^\lambda = \frac{\varphi_\lambda}{u_1} \,.\, U_1^\lambda; \qquad (57)$$

специяльно є

$$U_1 = \frac{\varphi_1}{u_1} \,.\, U_1,$$

т. зн.

$$\varphi_1 = u_1.$$

Всї инші φ_λ є вимірними функціями одного φ, нпр. φ_1

$$\varphi_\lambda = \chi_\lambda(u_1) \,.\, u_1,$$

так що (е дає:

$$U_\lambda = \chi_\lambda(u_1) \,.\, U_1^\lambda.$$

Вставивши се в (55a), маємо

$$Y_i = \frac{1}{p}\left[a + \sum_{n=1}^{p-1} \omega^{-in} \chi_n(u_1) \left(\sqrt[p]{u_1}\right)^n\right] \tag{58}$$

Тут маємо вираженє, яке може приймати p вартостей для $i = 1$, 2, ., p; одержимо його, добуваючи p-тий корінь з величини u_1, вимірної в обсягу (R', ω). Таким чином ми визначили p корінїв Абелевого рівнаня степеня p

$$\Phi(Y) = \prod_{i=1}^{p} (Y - Y_i) = 0 \tag{59}$$

§. 133. Хотячи перейти до самих корінїв y, мусимо звернути увагу на те, що з одної кляси непервісности до другої переходимо через субституції g_2; отже ґрупа N, зложена з субституцій g_2, є ґрупою тих поодиноких кляс. З того бачимо, що треба нам обчислити тільки елементи з одної кляси, а всї прочі одержимо при помочи субституцій g_2.

До обсягу (R', ω) долучуємо ще одну невимірність ζ, первісний p^2-ий корінь з одиниці, і творимо функції з елементів першої кляси:

$$\left.\begin{aligned}
Y_1 &= y_{11} + y_{21} + y_{31} + \ldots + y_{p1}, \\
\xi_1' &= y_{11} + \zeta y_{21} + \zeta^2 y_{31} + \ldots + \zeta^{p-1} y_{p1}, \\
\xi_2' &= y_{11} + \zeta^2 y_{21} + \zeta^4 y_{31} + \ldots + \zeta^{2(p-1)} y_{p1}, \\
&\ldots \\
\xi'_{p-1} &= y_{11} + \zeta^{p-1} y_{21} + \zeta^{2(p-1)} y_{31} + \ldots + \zeta^{(p-1)^2} y_{p1}
\end{aligned}\right\} \tag{60}$$

Ґрупа N переводить ξ'_i в $\zeta^{-i}\xi'_i$; отже коли напишемо $\xi'^{p^2}_i = w'_i$, одержимо нові величини, вимірні в (R', ζ), які належать до ґрупи N і дають ся виразити одною з них. З (60) маємо

$$y_{i1} = \frac{1}{p}\left[Y_1 + \sum_{m=1}^{p-1} \zeta^{-im} \xi'_m\right]; \tag{61}$$

злишнї вартости виражень під коренем ξ'_m вилучуємо при помочи функції

$$\psi'_\lambda = \xi'_\lambda \cdot \xi_1^{p^2-\lambda},$$

яка належить до ґрупи N, т. зн.

$$\xi'_\lambda = \frac{\psi'_\lambda}{\xi'^{p^2}_1} \cdot \xi_1'^\lambda = \omega'_\lambda(w_1') \cdot \xi_1'^\lambda \tag{62}$$

Се дає

$$y_{i1} = \frac{1}{p}\left[Y_1 + \sum_{m=1}^{p-1} \zeta^{-im} \omega'_m(w_1') \left(\sqrt[p^2]{w_1'}\right)^m\right]. \tag{63}$$

Отсе вираженє має для $i = 1, 2, \quad p$ знов p вартостий. Субституція g_2 веде до

$$y_{i2} = \frac{1}{p}\left[Y_2 + \sum_{m=1}^{p-1} \zeta^{-im} \omega''_m(w_1'') \left(\sqrt[p^2]{(w_1'')} \right)^m \right] \tag{64}$$

Тут маємо під корінем вншу функцію, а саме w_1''. Ті обі функції, w_1' і w_1'', дають ся представити одна другою вимірно, а так само кожда инша $w_1^{(j)}$

$$w_1^{(j)} = \vartheta_j(w_1'), \tag{65}$$

отже спеціяьною $w_1' = \vartheta_1(w_1')$. Рівно-ж величини ω''_m, $\omega'''_m \ldots$, можна представити функцією ω'_m, так що се дає

$$\omega_m^{(j)}(w_1^{(j)}) = \tilde{\omega}_m^{(j)}(w_1'). \tag{66}$$

Вставивши те в (64), маємо

$$y_{i2} = \frac{1}{p}\left[Y_2 + \sum_{m=1}^{p-1} \zeta^{\,\cdot}\, \tilde{\omega}''_m(w_1') \left(\sqrt[p^2]{\zeta_2(w_1')} \right)^m \right]$$

і загально

$$y_{ij} = \frac{1}{p}\left[Y_j + \sum_{m=1}^{p-1} \zeta^{-im} \tilde{\omega}^{(j)}_m(w_1') \left(\sqrt[p^2]{\zeta_j(w_1')} \right)^m \right] \tag{67}$$

Комбінуючи се з вираженєм на Y_j (58), одержимо вкінці корінь рівнаня (52):

$$y_{ij} = \frac{1}{p^2}\left[a + \sum_{n=1}^{p-1} \omega^{-jn} \chi_n(u_1) \left(\sqrt[p]{u_1} \right)^n + p \sum_{m=1}^{p-1} \zeta^{\,im} \tilde{\omega}^{(j)}_m(w_1') \left(\sqrt[p^2]{\zeta_j(w_1')} \right)^m \right] \tag{68}$$

Тут маємо функцію о p^2 вартостях. Її одержимо, коли добудемо p-тий корінь з величини u_1 з обсягу (R',ω): дальше при помочи того коріня визначимо величину w_1' і її вимірні функції $\zeta_j(w_1')$ в обсягу (R', ζ), а вкінці з тих фунцій добудемо p-тий корінь.

Се ще не є одначе найзагальнїйше вираженє, яке може приймати p^2. Коли розходить ся о найзагальнійшу p^2-вартісну функцію, тоді мусимо узглядните ті всї „приготовлюючі“ долученя, які привели первісний обсяг вимірности (R) до (R'). При помочи корінїв тих помічних рівнань знаходимо коріні первісного рівнаня $f(x) = 0$. Таким чином наш проблем рішений вповні.

XIV. Закінченє.

§. 134. Описану тут методу Jordan'а для рівнань степеня p^2 можемо примінити до всїх рішимих рівнань степеня p^α, $\alpha > 2$.

Рішиме рівнане степеня p^α буде мати в ряді зложеня своеї ґрупи **Абелеву підґрупу** M порядку p^α, яку творять субституції

$$g = | \; h_i \quad h_i + \alpha_i \; | \; (i = 1, 2, \ldots, \alpha); \qquad (1)$$

їх представимо як добуток α односторонних субституцій

$$g = g_1^{a_1} \, g_2^{a_2} \ldots g_\alpha^{a_\alpha}. \qquad (2)$$

Потім означимо **нормальні форми** ґеометричних субституцій по припису Jordan'a*), а опісля будемо з них будувати метациклїчні ґрупи.

Нормальні форми субституцій степеня p^α знайдемо, розвязуючи конґруенцію

$$\begin{vmatrix} a_{11} - \varrho, & a_{12}, & \ldots & a_{1\alpha} \\ a_{21}, & a_{22} - \varrho, & \ldots & a_{2\alpha} \\ \ldots & & & \\ a_{\alpha 1}, & a_{\alpha 2}, & \ldots, & a_{\alpha\alpha} - \varrho \end{vmatrix} \equiv 0, \; (mod.\ p) \; (3)$$

якої детермінанта

$$D = \begin{vmatrix} a_{11}, & a_{12}, & \ldots & a_{1\alpha} \\ a_{21}, & a_{22}, & \ldots, & a_{2\alpha} \\ \ldots & & & \\ a_{\alpha 1}, & a_{\alpha 2}, & \ldots & a_{\alpha\alpha} \end{vmatrix} \qquad (4)$$

не є зером. Отся конґруенція має взагалї n корінїв; вони можуть бути або дійсні, або злучені. Тепер розбираємо, які є можливі комбінації рівних, дійсних або злучених спряжених розвязок. Так нпр. для $\alpha = 3$ маємо конґруенцію

$$\varrho^3 - (a_{11} + a_{22} + a_{33}) \varrho^2 + (A_{11} + A_{22} + A_{33}) \; \varrho - D \equiv 0 \; (mod.\ p); \quad (5)$$

A_{11}, A_{22}, A_{33} є мінорами, приналежними до елементів a_{11}, a_{22}, a_{23}. В тім разї можливі такі комбінації розвязок:

1. всї три корінї дїйсні, рівні;
2. всї три корінї дїйсні, — два з них рівні, третїй відмінний;
3. всї три корінї дійсні, всї ріжні;
4. один корінь дійсний, два другі злучені, спряжені.

Обі перші можливости дадуть мабуть непервісні ґрупи; бо коли істнує тільки одна або дві такі функції, які перемінять ся під впливом тих субституцій в свої многократи, то можна буде знайти елементи, яких вони не змінять; нпр. 1. дасть нормальну форму

$$t = | \; h, \; k, \; l \quad \varrho h, \; a_{21} h + a_{22} k + a_{23} l, \; a_{31} h + a_{32} k + a_{33} l \; |,$$

яка не змінить елементів, котрі будуть мати перший показчик $= p$; в разї 2. буде нормальна форма

---

*) C. Jordan, Traité etc., стр. 114.

$$t = | h,\ k,\ l \quad \varrho_1 h,\ \varrho_2 k,\ a_{31}h + a_{32}k + a_{33}l \,|\,,$$

яка не змінить елементів x_{ppi} $(i = 1, 2, \ldots, p)$. Тільки 3.

$$t = | h,\ k,\ l \quad \varrho_1 h,\ \varrho_2 k,\ \varrho_3 l \,|$$

і 4.

$$t = | h,\ k,\ l \quad \varrho_1 h,\ (\varrho_2 + \varrho_3\, j)k,\ (\varrho_2 - \varrho_3\, j)l \,|$$

будуть могли дати первісні ґрупи.

Проблемом рівнань степеня p^3 займемо ся другим разом.

ДОДАТОК.

(Доповнене до рівнань четвертого степеня, §§. 56—60).

На стр. 54 подано хибно методу, яку подає Vogt, Leçons, стр. 94sqq., під назвою методи Euler'a. З огляду на теоретичну й практичну вартість тої методи подаємо її в цілости.

В рівнаню четвертого степеня, зведенім до найвигіднїйшої форми,

$$y^4 - py^2 - qy + r = 0, \tag{1}$$

кладемо

$$y = \sqrt{u_1} + \sqrt{u_2} + \sqrt{u_3}. \tag{2}$$

Закладаючи

$$u_1 + u_2 + u_3 = \gamma_1,$$
$$u_1u_2 + u_2u_3 + u_3u_1 = \gamma_2$$
$$u_1u_2u_3 = \gamma_3,$$

одержимо через подвійне квадроване реляції (2)

$$y^2 = \gamma_1 + 2\left(\sqrt{u_1u_2} + \sqrt{u_2u_3} + \sqrt{u_3u_1}\right),$$

$$y^4 - 2\gamma_1 y^2 + \gamma_1{}^2 = 4\left(\gamma_2 + 2\sqrt{\gamma_3}\cdot y\right),$$

або

$$y^4 - 2\gamma_1 y^2 - 8\sqrt{\gamma_3}\cdot y + (\gamma_1{}^2 - 4\gamma_2) = 0; \tag{3}$$

з порівнаня сочинників при (1) і (3) одержуємо

$$\gamma_1 = \frac{p}{2},$$

$$\gamma_2 = \frac{p^2}{16} - \frac{r}{4},$$

$$\gamma_3 = \frac{q^2}{64}.$$

Величини γ_1, γ_2, γ_3 є основними симетричними функціями величин u_1, u_2, u_3, які одержимо, розвязуючи кубічне рівнане

$$u^3 - \gamma_1 u^2 + \gamma_2 u - \gamma_3 = 0,$$

т. є

$$u^3 - \frac{p}{2}u^2 + \left(\frac{p^2}{16} - \frac{r}{4}\right)u - \frac{q^2}{64} = 0, \qquad (4)$$

рівнане, яке вповні покриває ся з кубічною ресольвентою в методї д. Цвойдзїньского (стр. 56), так що ся остатня метода являєть ся тільки дуже простою (а корисною для рахунку) модіфікацією методи Euler'а.

Термінольоґічний додаток*).

Абелеве рівнанє Abel'sche Gleichung.
альтернуючий alternierend.
визначна підґрупа ausgezeichnete Untergruppe; Normalteiler.
виконувати субституцію eine Substitution ausüben.
*вимірний (виміримий) rational.
головний ряд (зложеня) Haupt(kompositions)reihe.
двостороння субституція zweiseitige Substitution.
долученє Adjunktion.
доповняюча ґрупа komplementäre Gruppe.
допускати субституцію eine Substitution gestatten.
ізоморфний isomorph.
*квадратний (квадратовий) quadratisch.
кляса непервісности Imprimitivitätssystem.
комплексія Komplexion.
корінь з одиницї Einheitswurzel.
*лїнїйний (лїнїовий) linear.
метациклїчний metazyklisch.
многовартісний mehrwertig.
многостепенний mehrstufig; meroëdrisch.
найбільша (визначна) підґрупа ausgezeichnete Maximaluntergruppe; Maximalnormalteiler.
*невимірність (невиміримість) Irrationalität.
незмінна підґрупа invariante Untergruppe.
не-останок Nichtrest.
непервісний imprimitiv.

---

*) Подані тут такі терміни, яких нема в „Матеріялах до математичної термінольоґії" ВП. Дра В. Левицького (Збірник т. VIII/2), або які пропонував би я ввести замість поданих Дром В. Левицьким; ті остатні зазначені звіздкою (*), а в скобцї містить ся їх давня назва.

неперéхідний intransitiv.
*обсяг вимірности (вимірности) Rationalitätsbereich.
одностепенний einstufig; holoëdrisch.
одностороння субституція einseitige Substitution.
оператор Operator.
*первісний (первичний) primitiv.
*перекрій (переріз) Durchschnitt.
перемінний kommutativ.
*періода (fem., не masc.) Periode.
підґрупа Untergruppe.
побічна ґрупа Nebengruppe.
поодинокий einfach.
похідний abgeleitet.
правильний regelmässig, regulär.
природний обсяг вимірности natürlicher Rationalitätsbereich.
*ресольвента (розвязник) Resolvente.
рівнане ресольвенти Resolventengleichung.
рішимий auflösbar.
рішимість Auflösbarkeit.
роздїлене Verteilung.
розширити erweitern.
ряд (Абелевого рівнаня) Rang.
ряд зложеня Reihe der Zusammensetzung, Kompositionsreihe.
*система (fem. не masc.). System.
складовий konstituierend.
спряжені роди konjugierte Gattungen.
транспонуюча субституція transponierende Substitution.
чисельний numerisch.
циклїчний zyklisch.

ПОКАЗЧИК.

(Цифри означують сторони).

А) Річи.

Б) Імена.

RÉSUMÉ.

An der Theorie der algebraischen Gleichungen hat sich die ganze heutige Algebra ausgebildet; die Theorie der Gleichungen bedient sich nunmehr eines der mächtigsten Hilfsmittel der modernen Mathematik — der Substitutionengruppen.

In der vorliegenden Arbeit werden die Grundzüge derjenigen Disziplin geschildert, die unter dem Namen: „Galois'sche Gleichungstheorie" bekannt ist. In der ersten Abteilung werden die Grundlagen für die Theorie gewonnen: die Substitutionen und deren Gruppen. Es werden die vier Haupteigenschaften derselben untersucht (Transitivität und Intransitivität, Primitivität und Imprimitivität, Isomorphismus, Einfachheit und Zusammensetzung), sowie wird der Einfluss der Gruppen auf algebraische Funktionen besprochen. Mit einem Abschnitt über spezielle (zyklische und metazyklische) Gruppen- und Funktionen wird dieser Teil der Arbeit abgeschlossen.

Die zweite Abteilung bringt die eigentliche Theorie der Gleichungen dar. Nach einer kurzen Behandlung der quadratischen, kubischen und biquadratischen Gleichungen wird das Problem der algebraischen Auflösung der Gleichungen höherer Grade vor Augen gestellt, woraus erhellt, dass allgemeine Gleichungen vom höheren als dem vierten Grade algebraisch nicht lösbar sind. In den zwei folgenden Abschnitten werden specielle Klassen von Gleichungen: Kreisteilungs- und Abel'sche Gleichungen behandelt, und zuletzt die Gruppe einer auflösbaren Gleichung untersucht; hieraus ergeben sich notwendige und hinreichende Kriterien für die Auflösbarkeit der Gleichungen.

Die dritte Abteilung ist spezielleren Untersuchungen gewidmet; es wird dargetan, dass die Lösung einer Gleichung zusammengesetzten Grades auf diejenige mehrerer Gleichungen von Primzahlpotenzgraden p^α reduziert werden kann. Wir stellen also ein typisches Problem auf, eine primitive Gleichung vom Grade p^α zu lösen.

Für $\alpha = 1$ haben wir mit einer Gleichung vom Primzahlgrad zu tun, deren Lösung wir Abel, Galois und in neuesten Zeit Herrn Weber verdanken; in der vorliegenden Arbeit wurde aber einer wenig bekannten, aber doch präzisen und durchsichtigen Methode des Herrn J. Dolbnia Platz gegeben.

Für $\alpha = 2$ haben wir Gleichungen vom Grade p^2. Metazyklische Gruppen vom Grade p^2 hat Herr C. Jordan aufgestellt: er fand drei Typen derselben, indem er die homogenen linearen (geometrischen) Substitutionen von zwei Indices

$$t = | \; h, k \quad ah + bk, \; ch + dk \; |$$

auf Normalformen brachte, die aus der charakteristischen Kongruenz

$$\begin{vmatrix} a-\varrho, & b \\ c, & d-\varrho \end{vmatrix} \equiv 0 \; (mod. \; p)$$

zu entnehmen sind. Diese Kongruenz hat eine reelle, zwei reelle oder zwei konjugiert komplexe Wurzeln, und diesen drei Möglichkeiten entsprechen die drei Normalformen von t, durch welche jede Funktion der Indices in eines ihrer Vielfachen verwandelt wird. Die genannten drei Gruppentypen sind:

Erster Typus: Die Gruppe G_{I} besteht aus der Kombination der arithmetischen Substitutionen g *), mit den geometrischen der Form

$$\sigma_1 = | \; h, k \quad ah, bk \; | \quad (a, b = 1, 2, \ldots, p-1),$$

und

$$\sigma_2 = | \; h, k \quad k, h \; |$$

Ihre Ordnung ist $2 \, (p-1)^2 \, p^2$.

Zweiter Typus: G_{II} besitzt neben den arithmetischen Substitutionen g solche geometrische:

$$\sigma_1 = | \; h, k \quad ah + bek, \; bh + ak \; |, \; e\text{- Nichtrest } (mod. \; p);$$

$$(a, b = 0, 1, 2, \ldots, p-1; \; a = b = 0 \text{ ausgeschlossen});$$

$$\sigma_2 = | \; h, k \quad h, -k \; | ;$$

ihre Ordnung ist $2 \, (p^2-1) \, p^2$.

Im dritten Typus haben wir zwei Formen zu unterscheiden:

Form $\mathfrak{A}$ für $p \equiv 1 \; (mod. \; 4)$. Ausser den g haben wir noch

$$s = | \; h, k \quad \varrho h, \varrho k \; |, \; (\varrho \text{ — primitive Wurzel von } p);$$

$$t = | \; h, k \quad h, -k \; |,$$

$$\tau = | \; h, k \quad k, h \; | ;$$

$$v_1 = | \; h, k \quad h + k, \; h - k \; | ;$$

$$v_2 = | \; h, k \quad h - jk, \; h + jk \; |,$$

worin j eine Wurzel der Kongruenz

$$j^2 \equiv -1 \; (mod. \; \mathrm{p})$$

bedeutet.

Form $\mathfrak{B}$ für $p \equiv 3 \; (mod. \; 4)$ besitzt ausser den g und s auch noch

$$t = | \; h, k \quad k, -h \; | ;$$

$$\tau = | \; h, k \quad \mu h + \nu k, \; \nu k - \mu k \; | ;$$

*) Arithmetische Substitutionen des Grades p^2,

$$g = | \; h, k \quad h + \alpha, \; k + \beta \; | \quad (\alpha, \beta = 0, 1, \ldots, p-1),$$

können als Kombinationen sog. einseitiger Substitutionen gedacht werden, die nur einen einzigen Index um 1 vermehren,

$$g_1 = | \; h, k \quad h + 1, k \; |, \text{ bzw. } g_2 = | \; h, k \quad h, k + 1 \; |,$$

so dass $g = g_1{}^{\alpha} \, g_2{}^{\beta}$ $(\alpha, \beta = 0, 1, 2, \ldots, p-1)$ ist.

$$v_1 = | h, k \quad \mu h + (\nu + 1)k, (\nu - 1)h - \mu k | ;$$
$$v_2 = | h, k'' - (1 + \mu\nu)h + (\mu - \nu^2)k, (\nu + \mu^2)h + (\mu\nu - \mu + \nu) k | ,$$
worin die Zahlen μ und ν durch die Relation
$$\mu^2 + \nu^2 + 1 \equiv 0 \ (mod.\ p)$$
mit einander verbunden sind.

Die Ordnung des dritten Gruppentypus ist in beiden Formen dieselbe, u. z. $24(p-1)p^2$.

Alle diese Gruppen sind, wie es sich zeigt, primitiv und allgemein, ausgenommen die Fälle $p = 3$ für G_{I} und $G_{\mathrm{I}'}$, und $p = 5$ für G_{I}. Dass diese Gruppen metazyklisch sind, erhellt aus der Aufstellung ihrer Kompositionsreihe, deren sämtliche Indices Primzahlen sind.

Bei der Auflösung einer primitiven Gleichung vom Grade p^2, deren Koeffizienten Zahlen des natürlichen Rationalitätsbereiches (R) sind, wird folgender Weg eingeschlagen: Durch „vorbereitende" Adjunktionen von Irrationalitäten, deren Grade die Indices der Kompositionsreihe von G sind, kommt man durch allmähliche Reduktion der Gruppe auf eine Abel'sche Gleichung vom Grade p^2
$$F(y) = 0,$$
der ein erweiterter Bereich (R') zugrundeliegt. Durch Adjunktion zweier weiteren Irrationalitäten, einer p-ten und einer p^2-ten primitiven Einheitswurzel (was eigentlich auf eine einzige Adjunktion auskommt), wird diese Gleichung vollständig gelöst. Um die x zu finden, muss man noch Rückschritte durch „vorbereitende" Gleichungen machen.

Zuletzt wird die Methode skizziert, wie das Problem der Gleichungen p^α für $\alpha > 2$ zu behandeln wäre; den Fall $\alpha = 3$ behält sich Verf. einer späteren Gelegenheit vor.