Метациклїчні рівнаня і їх ґрупи.

(Über metazyklische Gleichungen und deren Gruppen).

НАПИСАВ

Микола Чайковський.

Теорія альґебраїчних рівнань, се та частина альґебри, на якій і при якій розвинула ся цїла альґебра. Викликана потребами практичного житя (розвязка рівнань), дала вона почин до введеня дробів, відємних, невимірних та злучених чисел. З неї взяла початок теорія визначників і теорія форм.

Рівнаня чотирох перших степенів розвязано розмірно скоро; квадратні рівнаня знали вже Пітаґорейцї, з кубовими рівнанями стрічаємо ся при звіснім проблємі подвоєня куба (Плято, Менехм, 4. стол. пер. Хр.), а розвязку двоквадратного рівнаня завдячуємо Ферровн († 1526 — оголошена друком 1545), Карданови (1501—1576), Тарталїї (1501—1557) і Ферарієви (1522—1565). Перед рівнанєм пятого степеня задержували ся найвизначнїйші математики того часу і слїдуючих столїть, стрічаючися з непоборимими трудностями.

Lagrange (1736—1813) змагав ся розвязувати ті рівнаня і рівнаня висших степенів при помочи ресольвент (1771), але дійшов до переконаня, що рівнанє, від якого залежить ресольвента, є висшого степеня нїж дане рівнанє, отже тою методою не можна дійти до розвязки. В тім часї виринула квестія, чи рівнаня висших степенїв є взагалї рішимі; підніс її 1799 р. італїйський математик Ruffini відносно 5-го степеня, але не довів до нїякого вислїду. Тодї працювали математики над спеціяльними клясами рішимих рівнань; найповажнїйшу теорію сотворив Gauss (1777—1855) для рівнаня поділу кола („Disquisitiones arithmeticae“, VII, 1801); він перший подав також доказ, що кожде альґебраічне рівнане має бодай один корінь з обсяґу злучених чисел (основне твердженє альґебри, 1799).

Абель (1802—1820) знайшов доказ, що загальне рівнане пятого степеня не є альґебраічно рішиме (1824), а два роки опісля (1826) доказав те саме для рівнань висших степенів. Йому завдячуємо також відкритє одної спеціяльної кляси рішимих рівнань (1829), званих Абелевими. Сучасний йому Galois (1812—1832) подав умови, коли рівнане висшого степеня може бути рішиме; своєї теорії він не викінчив, подав тільки її загальний начерк — в передодні своєї смерти.

Galois опер ся на теорії ґруп, якої початки подав Cauchy (1789—1857) в своїх викладах на політехніці в Парижі („Exercices d' analyse“). Від тої хвилї стає теорія ґруп підвалиною теорії альґебраічних рівнань; на ній опирають ся всякі дальші досліди, ведені Kronecker'ом (1823—1891) і Камілем Jordan'ом (ур. 1838), двома найважнїйшими піонїрами теорії Galois. Перший з них подає свої вислїди в розвідках, поміщуваних в „Monatsberichte der Berliner Akademie“ почавши від 1853 р., а кінчить їх величавим твором „Grundzüge einer arithmetischen Theorie der algebraischen Grössen“ (Crelle's Journal, 1882), в якім зібрані результати його довголїтнїх дослідів Другий коментує від 1867 р. Galois'a („Mémoire sur la résolution algèbrique des équations“, Liouville's Journal, 1867; „Sur la résolution algèbrique des équations primitives de degré p^2“, ibid. 1868, і „Commentaire sur Galois“, Mathematische Annalen I, 1868) і подає дуже основну теорію ґруп і рівнань („Traité des substitutions et des équations algèbriqués“, 1870).

Побіч тих двох математиків заслужили ся ще для теорії рівнань Netto (ур. 1846) своїми творами, Weber (ур. 1842) першою строгою розвязкою рівнань першого степеня, Mertens (ур. 1840), Hölder, Wiman і богато инших. Нинї теорія рівнань являєть ся величавою будівлею, замкненою в собі, яка до своїх результатів потрібує тільки деяких дослїдів з теорії чисел (конґруенцій, степенних останків і т. д.). На жаль, зістає та теорія тільки теорією; вже Kronecker висказав ся раз принагідно, що такі рівнаня, про які говорить ся в теорії, не істнують в дїйсности.

Нашим змаганем буде, представити в головних начерках теорію Galois, доповнену пізнїйшими дослідниками. В першій части подаємо основи, потрібні до теорії рівнань (теорію ґруп), в другій властиву теорію рівнань, а в третій приміненє тої теориї до ріжних типів рішимих рівнань: при рівнанях степеня p^2 подані деякі наші власні розсліди. — Жерелами, якими ми користували ся, були переважно твори Netto'на, Weber'a, Jordan'а й ин.; всї вони цитовані у відповідних місцях.

Тернопіль, вересень—падолист 1910.

Перша частина.

Основи.

I. Пермутациї і субституциї.

§. 1. Маємо даних n яких небудь елементів (предметів або річий), які означуємо

$$x_1, x_2, x_3, \qquad x_n,$$

або тільки самими їх показчиками (індексами)

$$1, 2, 3, \qquad n.$$

Тим елементам не накладаємо нїякого иншого обмеженя, тільки те, що вони мають бути між собою ріжні; о їх величину не ходить нам зовсім.

Уґрупуймо їх в такім порядку:

$$1, 2, 3, \qquad n;$$

таке уґрупованє елементів за кождим разом називаємо комплексією. Коли-б ми їх за другим разом уставили инакше нпр. в ряд

$$a_1, a_2, a_3, \qquad a_n,$$

так що всї елементи з другого ряду мають рівні собі елементи в першім рядї, то перехід з першого ряду до другого вимагає виконаня якоїсь пермутациї (переставленя) тих елементів. Пермутацію означуємо так:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & & n \\ a_1 & a_2 & a_3 & & a_n \end{pmatrix};$$

значить, що на місце елемента i прийде инший a_i, визначений докладно і однозначно. Елементи a_i є, як сказано, ті самі, що елементи i, отже коли заступимо $n-1$ елементів i $n-1$ елементами a_i, то тим самим знаємо вже однозначно і n-тий елемент. Нпр. маємо дані елементи

$$1,\ 2,\ 3,\ 4,\ 5$$

в тім самім порядку, що природний ряд чисел. Друга комплексія тих самих елементів нехай буде

$$2,\ 4,\ 3,\ 5,\ 1\ ;$$

перехід з першого упорядкованя до другого вимагає пермутації

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}.$$

Коли знаємо, що елемент 1 маємо заступити елементом 2, 2 елементом 4, 3 собою самим, 4 елементом 5, — то тим самим вже знаємо, що позісталий елемент 5 мусимо заступити позісталим з другого ряду т. є 1.

Пермутація, яка не зміняє порядку елементів, називаеть ся **ідентична пермутація**, а означуємо її одинкою

$$1 = \begin{pmatrix} 1 & 2 & 3 & & n \\ 1 & 2 & 3 & & n \end{pmatrix}.$$

§. 2. Коли комплексію

$$1,\ 2,\ 3, \qquad n$$

перевести в

$$a_1,\ a_2,\ a_3, \qquad a_n,$$

то ту другу комплексію можемо при помочи пермутації

$$\pi' = \begin{pmatrix} a_1 & a_2 & a_3 & & .\,a_n \\ b_1 & b_2 & b_3 & & .\,b_n \end{pmatrix}$$

перевести знов в иншу комплексію, а саме в

$$b_1,\ b_2,\ b_3 \qquad b_n;$$

та комплексія буде містити ті самі елементи, що дві перші. Отже, щоби з першої комплексії перейти в третю, треба виконати дві пермутації π і π'. Символїчно зазначуємо се як добуток: пермутація $\pi\pi'$ переводить першу комплексію в третю

$$\pi\pi' = \begin{pmatrix} 1 & 2 & 3 & & n \\ b_1 & b_2 & b_3 & & b_n \end{pmatrix}.$$

Таке виконуванє двох пермутацій по черзї називаємо **множенєм пермутацій**. — Подібно можемо ще далї перейти до четвертої комплексії

$$c_1,\ c_2,\ c_3, \qquad c_n$$

(c_1, c_2, c_n є все ті самі елементи, що 1, 2, n, тільки в иншім порядку) при помочи пермутації

$$\pi'' = \begin{pmatrix} b_1 & b_2 & & b_n \\ c_1 & c_2 & & c_n \end{pmatrix},$$

так що

$$\pi\pi'\pi'' = \begin{pmatrix} 1 & 2 & 3 & & n \\ c_1 & c_2 & c_3 & & c_n \end{pmatrix};$$

загально при помочи m пермутації дійдемо врешті до

$$m_1,\ m_2,\ m_3, \qquad m_n.$$

Множене пермутацій виконуємо або чергою, т. є до добутка двох перших примінюємо третю, до тоі комплексії четверту і т. д., — або можемо відступити від того порядку в той спосіб, що перше скомбінуємо з собою які небудь пермутації з середини, а опісля ту вислідну пермутацію вважатимемо одним членом добутка і примінимо її як таку в дотичнім місці, нпр.

$$\pi\pi'\pi'' = (\pi\pi')\pi'' = \pi(\pi'\pi'')$$

З того слідує, що множенє пермутацій підлягає законови сполучуваня (асоціяції); закон переміни (коммутації) не має тут такого значіня, як при звичайнім множеню. Бачимо се на примірі:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix},\ \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}.$$

Другу пермутацію можемо написати також ще так:

$$\pi_2 = \begin{pmatrix} 2 & 4 & 3 & 5 & 1 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix},$$

бо в ній так само, як в горішній формі сказано, 1 заступимо 4, 2 заступимо 3, 3–1, 4–5, а 5–2.

Їх добутки є:

$$\pi_1\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 4 & 3 & 5 & 1 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix},$$

$$\pi_2\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} \begin{pmatrix} 4 & 3 & 1 & 5 & 2 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}, —$$

отже два зовсім відмінні результати.

Виїмкові випадки, де добуток пермутацій не залежить від порядку, в якім пермутації виконуємо, будуть нас займати опісля; се т. зв. перемінні (kommutative, vertauschbare) пермутації.

§. 3. Добуток двох однакових пермутацій означуємо аналоґічно до множеня як степень: $\pi\pi = \pi^2$. Нпр.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix},$$

$$\pi^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 4 & 3 & 5 & 1 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}.$$

Подібно означуємо також третю, четверту n-ту степень даної пермутації, π^3, π^4, π^n, нпр.

$$\pi^3 = \pi^2 . \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 4 & 5 & 3 & 1 & 2 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix},$$

$$\pi^5 = \pi^3 . \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} \begin{pmatrix} 5 & 1 & 3 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = 1,$$

$$\pi^5 = n^4 . \pi = 1 . \pi = \pi, \text{ і т. д.}$$

Скількість всїх можливих уґруповань n елементів є $n!$, отже не є безконечно велика; длятого ряд степений мусить містити в собі і ідентичну пермутацію. Нехай буде

$$\pi^m = 1,$$

то маємо: $\pi^{m+1} = \pi^m . \pi = 1 . \pi = \pi$, $\pi^{m+2} = \pi^2$, ., $\pi^{m+n} = \pi^n$ і т. д., отже ряд степений пермутації π повторюють ся періодично по m членах:

$$\pi, \pi^2, \quad ., \pi^{m-1}; \pi^m = 1.$$

Сей ряд називаємо **періодою** (Periode) пермутації π, а виложник m її **порядком** (Ordnung).

Врештї називаємо скількість елементів, яка приходить в данїй комплексії, її **степенем** (Grad). Коли m є порядком, а n степенем пермутації π, то m і n стоять до себе в реляції

$$m \leqq n,$$

а то з тої причини, що:

1. Коли π не переводить **кождий** елемент в инший, то що йно по n повторенях верне той елемент на своє місце; скорше вернути не може, бо π за кождим разом посуває його на инше місце, отже в тім разї є $m = n$.

2. Коли π не переводить одного або більше (k) елементів в инші (в нашім остатнім примірі елемент 3), то наша пермутація відносить ся тільки до $n-k$ елементів, пересуваючи їх за кождим разом; длятого по $n-k$ повторенях вернуть всї вони на своє місце, отже $m = n - k$, т. зн. $m < n$.

3. Коли-б було $m > n$, то кождий з елементів перейшов би всї місця ще перед m-тим повторенем, отже m не могло би називати ся порядком пермутації. З того виходить, що $m \leqq n$.

§. 4. Коли

$$\pi^m = 1,$$

то з рівнаня

$$\pi^\alpha = \pi^\beta$$

виходить

$$\alpha \equiv \beta \pmod m$$

т. є

$$\alpha = \beta + km,$$

бо

$$\pi^{\alpha} = \pi^{\beta + km} = \pi^{\beta}\, \pi^{km} = \pi^{\beta} (\pi^{m})^{k} = \pi^{\beta}.$$

Після того можемо все в виложнику степеня пермутації опустити многократь числа m. Звідси бачимо, що можна написати також так:

$$\pi^{m-1} = \pi^{-1},$$

отже π^{-1} буде означувати таку пермутацію, яка множена першим степенем пермутації π дасть 1, бо:

$$\pi^{-1} . \pi = \pi^{m-1} . \pi = \pi^{m} = 1.$$

Взагалї π^{-k} означує таку пермутацію, яка множена пермутацією π^{k} дасть 1. Пермутацію π^{-k} називаємо **відворотною** (reziprok) до π^{k}, анальоґічно до звичайного множеня: a^{-k} і a^{k} є відворотні числа, бо $a^{-k} . a^{k} = 1$.

§. 5. Якунебудь пермутацію виконуємо так, що кождий елемент заступаємо котримось иншим по даному припису. Сей припис називаємо загально **субституцією** (підставленем). Субституція або подає кождий елемент з окрема з його заступником, — і тодї вона є рівнозначна з пермутацією, — або вказує тільки на правило, по якому треба поодинокі елементи перемінювати. Тодї пишемо так:

$$\sigma = (i,\ a_i),$$

т. зн., що елемент i заступаємо в загалї елементом a_i, — або також можемо се написати у видї функції

$$\sigma = \mid z \quad \varphi(z) \mid, \ (z = 1, 2 \quad n)$$

де z і $\varphi(z)$ можуть приймати тільки вартости 1, 2, $\quad n$.

Взагалї є субституція рівнозначна з пермутацією; ріжниця лежить в тім, що субституція подає припис переставлюваня, а пермутація означає саму операцію переставлюваня *).

§. 6. Субституцію називаємо **циклїчною** (коловою, cyklisch) або **циклем** (Zyklus), коли вона містить в собі припис, що кождий елемент заступаємо слїдуючим, а остатнїй першим. Циклїчну субституцію пишемо так:

---

*) Деякі автори відріжняють дуже точно пермутації і субституції (впр. Weber) инші (Netto) уживають тільки назви субституція, рівнозначно з понятєм пермутації.

$$c=(1\ 2\ 3 \qquad n);$$

вона рівнозначна з пермутацією

$$\pi=\begin{pmatrix}1 & 2 & 3 & & \overline{n-} & n\\ 2 & 3 & 4 & & n & 1\end{pmatrix}.$$

Циклїчна субституція n елементів має періоду о n членах так, що $s^n=1$, а всї попереднї степенї є ріжні від n. Се видко з того, що в циклю є кождий член заступлений слїдуючим, а нї один собою самим, отже треба ту саму субституцію повторити n разів, щоби кождий член, перейшовши всї місця, вернув на первісне. Тому то є циклї такими субституціями, в яких степень є рівний порядкови.

Назва циклїчної субституції походить звідси, що коли би ми обвід кола поділили на n рівних частий і в точках подїлу написали чергою елементи 1, 2, 3, n, то обертаючи коло о кут $\frac{2\pi}{n}$ накрили-б ми елемент 1 елементом 2, 2 елементом 3 і т. д., а остатній n першим. З того видко, що цикль можемо зачинати від котрогонебудь елемента (гл. §. 2).

§. 7. Кожду пермутацію можна заміняти на циклїчну, і то так, що розложимо її на один або більше циклів. Робимо се так:

Нехай буде дана пермутація

$$\pi=\begin{pmatrix}1 & 2 & 3 & & n\\ a_1 & a_2 & a_3 .. & & a_n\end{pmatrix}.$$

На початку циклю пишемо елемент 1, а побіч нього a_1; се значить, що на місце 1 прийде a_1. Тепер шукаємо, який елемент стоїть під a_1; коли тим елементом є 1, то замикаємо цикль; коли-ж той елемент a_e є ріжний від 1, то виписуємо його побіч a_1 і шукаємо знов того, що стоїть під a_e. Коли там знайдемо 1, замикаємо цикль; в противнім разї шукаємо дальшого елементу, що стоїть під виписаним на останку. Натрафивши врештї на 1, замикаємо цикль; се мусить конечно колись стати ся, бо 1 мусить прийти на місце котрогось з прочих елементів.

Коли ми тим чином вичерпали всї елементи, тодї вважаємо нашу задачу покінченою. Коли-ж нї, беремо один з тих елементів, яких в циклю ще нема, і зачинаємо від нього новий цикль. Сей другий цикль мусить також скінчити ся, а і скількість циклів взагалї є скінчена, бо елементи не є данї в безконечнім числї.

Один елемент не може повторяти ся в двох циклях, бо тодї сей елемент з другого циклю потягнув би за собою котрийсь елемент з першого, а тим самим і цїлий перший цикль знайшов би ся в другім, а се неможливе, бо в другім циклю по припасови помістили ми ті елементи, яких нема в першім.

Нпр. розложити на циклї

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 3 & 7 & 6 & 4 & 9 & 8 & 2 & 1 & 0 \end{pmatrix}.$$

Зачинаємо від 0; під ним стоїть 5, отже пишемо початок (05. Елемент 5 має бути заступлений елементом 9, а 9 елементом 0, т. є тим, від якого ми цикль зачинали. Маємо проте перший цикль,

$$(0\ 5\ 9).$$

Тепер беремо один з тих елементів, яких в тім циклю нема, нпр. 1, і бачимо, що 1 заступлений 3, 3—6, 6—8, а 8 знова 1; проте другий цикль буде (1 3 6 8). Трегий цикль зачнім від 2 2 — 7, 7 — 2, кінець: (2 7). Бракує ще 4 4 заступлене само собою, отже (4). Проте маємо:

$$\pi = (0\ 5\ 9)\ (1\ 3\ 6\ 8)\ (2\ 7)\ (4).$$

Одночленний цикль можемо опустити, бо він не змінює нїчого в данім комплексї. Поодинокі циклї є перемінні, бо вони не мають спільних елементів; длятого нам байдуже, котрі з елементів будемо перше переставляти.

Загально пишемо:

$$\pi = c_1\ c_2 \qquad c_\lambda,$$

де c_1, c_2, $\qquad c_\lambda$ є поодинокими циклями. Порядок субституциї π є найменшою спільною многократю степенїв поодиноких циклїв. Нехай n_1 буде степень цикля c_1, n_2 степень цикля c_2, $\qquad n_\lambda$ степень цикля c_λ, а v найменша спільна многократь чисел $n_1, n_2, \ldots n_\lambda$, то

$$\pi^v = (c_1{}^v)(c_2{}^v) \qquad .(c_\lambda{}^v).$$

а що кожде $c_i{}^v = c_i{}^{n_i \frac{v}{n_i}} = 1$ (бо $\frac{v}{n_i}$ є ціле число), то і $\pi^v = 1$.

В нашім примірі є v (2, 3, 4) = 12, отже $\pi^{12} = 1$.

Субституція називаєть ся **правильною** (regelmässig), коли всї її циклї мають рівну скількість елементів; тодї порядок цїлої субституції є рівний порядкови складових циклїв.

Дві субституції називають ся **подібні** (ähnlich), коли обі мають циклї тих самих порядків; порядки двох подібних субституцій є собі рівні.

§. 8. Коли хочемо обчислити квадрат цикля, то перескакуємо все один елемент і переходимо до слідуючого, бо квадрат є рівнозначний з пересуненем кождого елемента о два місця. При третій степені перескакуємо о два місця, при k-тій о $k-1$ елементів. Результат того такий, що при $(n-1)$шій степені йдуть по першім елементі всї инші в противнім порядку нїж первісно.

Коли k є дільником числа n, то k-та степень цикля розпадаєть ся на k циклїв по $\frac{n}{k}$ елементів, бо посуваючи ся від 1 все о k місць по $\frac{n}{k}$ кроках прийдемо знова до 1. Нпр. маємо цикль:

$$c = (1\ 2\ 3\ 4\ 5\ 6);$$

в нїм є:

$$c^2 = (1\ 3\ 5)\ (2\ 4\ 6),$$
$$c^3 = (1\ 4)\ (2\ 5)\ (3\ 6).$$

Цикль зложений з двох елементів, називаємо **транспозиціє ю** (переміщенем)

$$\tau = (1\ 2);$$

його квадрат є 1, бо посунувши ся від 1 о два місця, вернемо до 1. З тоЇ самоЇ причини є:

$$\tau^{-1} = \tau.$$

§. 9. Кождий цикль можна дальше розкладати на циклї низших степенїв. Робимо се так; коли a, b, c, $\ldots$ n, є елементами даного циклю

$$c = (1\ 2 \quad\ldots\quad a \quad\ldots\quad b \quad\ldots\quad c \quad\ldots\quad n),$$

тодї творимо

$$c_1 = (1\ 2 \quad\ldots\quad a),$$
$$c_2 = (1\ \overline{a+1} \quad\ldots\quad b),$$
$$c_3 = (1\ \overline{b+1} \quad\ldots\quad c),$$
$$\ldots$$
$$c_\mu = (1\ \overline{m+1} \quad\ldots\quad n)$$

і маємо

$$c = c_1\ c_2\ c_3 \quad\ldots\quad c_\mu,$$

бо при множеню циклїв кінцевий елемент першого, a, заступаємо початковим 1, а той елементом $\overline{a+1}$ з другого цикля і т. д. Треба завважати, що добуток тих циклїв не є перемінний, як в §. 8, бо ті циклї мають один спільний елемент, 1.

Спеціяльно можемо розложити кожду циклїчну субституцію на $n-1$ транспозицій:

$$(1\ 2\ 3\ \ldots\ n) = (1\ 2)\ (1\ 3)\ \ldots\ (1\ n).$$

§. 10. Нехай буде дана субституція

$$\pi = c_1\ c_2\ \ldots\ c_n.$$

Обчислїм такий добуток:

$$\varrho = k^{-1}\ \pi k,$$

де

$$k = k_1\ k_2\ \ldots\ k_m.$$

Передовсїм маємо ідентично:

$$\varrho = k^{-1}\ \pi k = (k^{-1}\ c_1\ k)\ (k^{-1}\ c_2 k)\ \ldots\ (k^{-1}\ c_n\ k)\ ;$$

з того бачимо, що бажаний добуток одержимо, творячи анальоґічні добутки для кождого із складових циклїв.

Добуток

$$\varrho = k^{-1}\ \pi k$$

називаєть ся трансформованою, (transformierte) перетвореною субституцією з π при помочи k. Трансформацію виконуємо так, що в кождім поодинокім циклю виконуємо зміну, приписану в k.

Нпр. маємо трансформувати

$$\pi = (1\ 2\ 3\ 4\ 5)$$

при помочи

$$k = (3\ 6\ 7)$$

отже виконати множенє

$$\varrho = k^{-1}\ \pi k = (3\ 6\ 7)^{-1}\ (1\ 2\ 3\ 4\ 5)\ (3\ 6\ 7),$$

а що

$$(3\ 6\ 7)^{-1} = (3\ 6\ 7)^2 = (3\ 7\ 6), \text{ то}$$

$$\varrho = (3\ 7\ 6)\ (1\ 2\ 3\ 4\ 5)\ (3\ 6\ 7) = (1\ 2\ 6\ 4\ 5).$$

Ужаваючи поданого правила, щоби в π виконати зміну по приписам k, одержимо рівно-ж

$$\varrho = (1\ 2\ 6\ 4\ 5),$$

бо k каже заступити елемент 3 елементом 6, 6 елементом 7, а 7 елементом 3; 6 і 7 відпадуть, бо їх нема в π, і звідси маємо такий самий результат.

II. Ґрупи.

§. 11. Нехай ряд

$$A, B, C, D, \quad ., E \qquad (1)$$

представляє які небудь елементи: можуть се бути числа, операції, субституції, рухи і т. д. — називаємо їх загально **о п е р а т о р а м и***). Коли ті оператори відповідають таким вимогам, що

1. комбінація двох яких небудь операторів є знов оператором з того самого ряду (комбінацію операторів значимо символїчно їх добутком), $AB = C$;

2. комбіноване більшої скількости ніж двох операторів не противить ся законови злучуваня

$$ABC = (AB)C = A(BC);$$

3. з $AC = BC$, згл. $CA = BA$ виходить однозначно

$$A = B,$$

тодї кажемо, що ряд операторів (1) творить **ґ р у п у** (Gruppe).

Ґрупа може бути **с к і н ч е н а** або **б е з к о н е ч н а**, відповідно до того, чи скількість операторів є скінчена, чи безконечна.

Понятє ґрупи має в математицї велике значінє і часте примінене. Розріжнюємо: ґрупи рухів, ґрупи трансформацій, а також ґрупи субституцій або пермутацій. Той остатнїй рід ґруп має примінене в теорії альґебраїчних рівнань, отже в нашій працї займемо ся тільки ґрупами субституцій.

В склад такої ґрупи входять проте тільки такі субституції, які скомбіновані з собою дають один із членів тої ґрупи. Скількість субституцій в ґрупі називаємо **п о р я д к о м** ґрупи, а скількість всїх елементів **с т е п е н е м** ґрупи. Порядок ґрупи є найменшою спільною многократю порядків поодиноких субституцій.

Кожда ґрупа мусить містити в собі всї степенї тої самої субституції, бо кожду субституцію можемо комбінувати з нею самою, а коли той процедер повторимо кілька разів, то одержимо всї степенї тої субституції. Так само і ідентична субституція є складовою частиною кождої ґрупи, бо повторюючи якусь субституцію тільки разів, кілько виносить її порядок, одержуємо 1.

На означенє ґрупи, зложеної з операторів 1, A, B, C, $\quad E$, пишемо:

$$G = [1, A, B, C, \quad .., E].$$

---

*) **Netto**, Gruppen- und Substitutionentheorie, Sammlung Schubert, Leipzig 1908, стр. 2.

§. 12. Перше питане, яке займе нас в теорії ґруп, буде очивидно, які ґрупи можна утворити з n елементів

$$1, 2, 3, \quad ., n.$$

Длятого рішім перше питане, кілько є можливих всїх пермутацій з n елементів.

Елємент 1 можемо ставити на всїх n місцях; тодї зістає для прочих $n-1$ елементів тільки $n-1$ місць до переставлюваня. Другий елємент, 2, може вже займити тільки одно з позісталих $n-1$ місць. Отже елєменти 1 і 2 можуть бути комбіновані з собою на $n(n-1)$ способів. Тепер вже зістає тільки $n-2$ місць для елєментів 3, 4, . ., n; отже елємент 3 може стояти на $n-2$ місцях, а се дає $n(n-1)(n-2)$ ріжних комбінацій з елементами 1 і 2.

Так сходимо по одному елементови аж до остатнього. З того бачимо, що n елєментів дає $n! = 1 . 2 . 3 \quad n$ ріжних комбінацій.

Отсе число є максімальною границею для порядку ґрупи. В тих n операторах містять ся всї можливі комбінації з n елємевтів, навіть ті субституції, які переставляють менше ніж n елєментів.

§. 13. Ґрупа порядку $n!$ є найбільшою зі всїх ґруп, які можна утворити з n елєментів. Се т. зв. **симетрична ґрупа** (symmetrische Gruppe).

Крім неї є ще можливі й инші ґрупи з тих самих елементів.. Нпр. періода циклїчної субституції

$$c = (1 \ 2 \quad n)$$

творить ґрупу, бо кожде

$$c^k c^\lambda = c^{k+\lambda} = c^\mu$$

належить до періоди субституції v. Се т. зв. **циклїчна ґрупа** (zyklische Gruppe); вона характеристична тим, що її порядок (скількість членів в періоді) рівний степеневи (скількости елєментів). — Всї її субституції містять ся в симетричній ґрупі, бо-ж симетрична ґрупа обіймає **всї можливі** субституції, утворені з n елементів. Длятого кажемо, що циклїчна ґрупа **містить ся** в симетричній, або що вона є **підґрупою** (Untergruppe) симетричної. Взагалї кожда можлива ґрупа містить ся в симетричній.

Кожда ґрупа може містити в собі також ще менші від неї підґрупи; кожда ґрупа мусить містити в собі підґрупу, зложену з ідентичної субституції (се також ґрупа, бо 1 комбіноване з собою дає все 1); отсю остатню ґрупу називаємо **ідентичною ґрупою** (identische Gruppe) і значимо її також 1.

Ґрупа, що не містить в собі инших підґруп, крім ідентичної, називаеть ся **поодинокою** (einfach); в противнім разї є ґрупа **зложена** (zusammengesetzt).

§. 14. *До порядків ґруп і підґруп відносять ся*

I. Твердженє (*Cauchy*). *Порядок кождої підґрупи* **є дїльником порядку ґрупи, в якій вона містить ся.**

Доказ. Нехай дана ґрупа G обіймає підґрупу H, зложену з субституцій

$$1,\ h_1,\ h_2, \quad h_\mu, \tag{2}$$

отже порядок ґрупи H є μ. Возьмім яку небудь субституцію з G, якої нема в H, нпр. g_1, і утворім ряд

$$g_1,\ g_1 h, g_1 h_2, \quad .,\ g_1 h_\mu; \tag{3}$$

всї елементи того ряду є ріжні від елементів ряду (1). Коли ми ще не вичерпали всїх субституцій з G, беремо котру небудь з позісталих, нпр. g_2, і творимо знов подібний ряд, і т. д., аж вичерпають ся всї оператори з G. Таким чином одержимо слїдуючу таблицю:

$$\left.\begin{array}{l} 1,\ h_1,\ h_2, \qquad h_\mu; \\ g_1,\ g_1 h_1,\ g_1 h_2. \qquad .,\ g_1\ h_\mu; \\ g_2,\ g_2 h_1,\ g_2 h_2. \qquad .,\ g_2\ h_\mu; \\ \\ g_{\nu-1},\ g_{\nu-1} h_1,\ g_{\nu-1} h_2, \ldots, g_{\nu-1} h_\mu. \end{array}\right\} \tag{4}$$

Отся таблиця містить в собі як раз всї субституції з G. З неї слїдує безпосередно наше твердженє: коли r є порядком ґрупи G, то

$$r = \mu\nu,$$

отже

$$\mu = \frac{r}{\nu}. \tag{5}$$

Квот $\nu = \frac{r}{\mu}$ з порядків ґруп G і H називаємо **показчиком ґрупи** H **в віднесеню до** G (Index von H in Bezug auf G).

Таке роздїлюванє ґрупи G на рядки таблиці (4) називаємо **роздїленєм ґрупи** G **при помочи підґрупи** H (Verteilung von G mittelst H; Mertens); його значимо так:

$$G = (H,\ g_1 H,\ g_2 H. \quad .,\ g_{r-1}\ H) \tag{6}$$

або за Weber'ом (Algebra I. стр. 544) символїчно

$$G = H + g_1 H + g_2 H + \quad + g_{r-1} H; \tag{7}$$

члени тої суми називає він **системою побічних ґруп** до H (System der Nebengruppen zu H).

§. 15. З поміж всїх ґруп з n елементів виріжнюють ся т. зв. **альтернуюча ґрупа** (alternierende Gruppe). Вона складаєть ся зі всїх тих субституцій, які можна розложити на **паристу скількість транспозицій**, а що скількість транспозицій є о 1 менше ніж степень даної субституції (гл. §. 9), то альтернуюча ґрупа зложена зі всїх тих субституцій, що містять в собі непаристу скількість елементів. Ті субституції називаємо **субституціями першого рода**, а субституції, що мають паристу скількість елементів, **субституціями другого рода**.

II. Твердженє. **Субституції першого рода творять ґрупу, субституції другого рода не творять ґрупи.**

Доказ. Коли скомбінуємо дві субституції першого рода, отже дві паристі скількости транспозицій, одержимо паристу скількість транспозицій, т. є знова оператор першого рода. Коли-ж помножимо дві субституції другого рода, одержимо субституцію з паристою скількістю транспозицій, отже вийдемо поза межі комплексу субституцій другого рода.

Ґрупою субституцій першого рода є альтернуюча ґрупа, а її порядок є $\frac{1}{2}\, n!$, бо коли яку небудь з її субституцій скомбінуємо з одною транспозицією, одержимо субституцію другого рода; отже кождій субституції з ґрупи відповідає одна і тільки одна субституція другого рода, а що обі кляси мають разом $n!$ субституцій, то на альтернуючу ґрупу випадає половина з того, т. є $\frac{1}{2}\, n!$

§. 16. Нехай буде дана ґрупа G порядку m

$$G = [1,\ g_1,\ g_2, \qquad g_{m-1}],$$

а в нїй нехай містить ся підґрупа H порядку μ

$$H = [1,\ h_1,\ h_2. \qquad h_{\mu-1}].$$

Трансформуймо кожду субституцію з H кождою субституцією з G; тодї одержимо цїлий ряд ріжних від себе ґруп:

$$\left.\begin{array}{llll} 1, & h_1, & h_2, & h_{\mu-1}; \\ 1, & g_1^{-1} h_1 g_1, & g_1^{-1} h_2 g_1, & .,\ g_1^{-1} h_{\mu-1} g_1; \\ 1, & g_2^{-1} h_1 g_2, & h_2^{-1} h_2 g_2, & .,\ g_2^{-1} h_{\mu-1} g_2; \\ & & & \end{array}\right\} \tag{8}$$

Се є дійсно ґрупи, бо кожда комбінація двох субституцій з одного рядка мусить стояти знова в тім самім рядку, нпр.
$(g_i^{-1} h_\alpha g_i)(g_i^{-1} h_\beta g_i) = g_i^{-1} h_\alpha (g_i g_i^{-1}) h_\beta g_i = g_i^{-1} h_\alpha h_\beta g_i = g_i^{-1} h_\gamma g_i$.

Що в двох рядках не можуть стояти однакові субституції, бачимо з того, що коли-б ми мали

$$g_i^{-1} h_\alpha g_i = g_j^{-1} h_\beta g_j,$$

то помноживши то рівнанє з лівої сторони субституцією g_i, а з правої субституцією g_i^{-1} одержали-б ми:

$$h_\alpha = (g_i g_j^{-1})\, h_\beta\, (g_j g_i^{-1});$$

отже або було би $i = j$, т. є обі субституції походили би з того самого рядка, а крім того мусїли би бути $\alpha = \beta$ т. є обі субституції були би ідентичні, — або для $i \neq j$ мусїла би субституція $g_j g_i^{-1}$ трансформувати кожде h з H в одну з субституцій таки з тої самої ґрупи, а се неможливе.

Ґрупи, що стоять в рядках таблицї (8), називають ся трансформованими з H при помочи субституцій з G (Transformierte von H mit Hilfe der Substitutionen von G. Їх означуємо так:

$$H,\ g^{-1} H g_1,\ g_2^{-1} H g_2,$$

Тих ґруп не може бути більше від m; зате може їх бути менше, бо деякі з них можуть бути між собою рівні.

Нехай між ними буде ϱ ріжних:

$$H,\ g_1^{-1} H g_1,\ g_2^{-1} H g_2, \quad \ldots,\ g_{\varrho-1}^{-1} H g_{\varrho-1}; \qquad (9)$$

всї ті ґрупи з ряду (9) називають ся спряжені (konjugiert) з ґрупою H. Коли вони всї ідентичні, тоді H називаємо визначною або незмінною підґрупою (ausgezeichnete, invariante Untergruppe). Визначна підґрупа є перемінна з субституціями ґрупи G.

§. 17. Нехай будуть дані дві ґрупи G_1 і G_2. Коли вони мають які спільні субституції, то ті субституції творять знова ґрупу R, звану найбільшою спільною мірою (grösster gemeinsch. Teiler; Jordan, Netto, Mertens) або перекроєм (Durchschnitt; Study, Weber) ґруп G_1 і G_2. R є дійсно ґрупою, бо всї її субституції

$$1,\ r_1,\ r_2, \quad r_{\varrho-1},$$

а так само і всї їх комбінації $r_\alpha r_\beta$, приходять в обох ґрупах G_1, G_2.

Порядок перекрою двох ґруп є найбільшою спільною мірою порядків обох ґруп, бо ϱ мусить містити ся в m_1 і m_2, а R обіймає всі субституції, спільні обом ґрупам.

Так само говоримо про перекрій більшої скількости ґруп.

§. 18. Коли в двох даних субституцій

$$g, h$$

хочемо утворити ґрупу, то мусимо кождий член з періоди субституції g комбінувати з кождим членом періоди h, подібно як при множеню многочленів. Нехай будуть m_1, m_2 степені періодів субституцій g і h, а $v(m_1, m_2)$ означає їх найменшу спільну многократь, то порядок тої зложеної ґрупи буде $v(m_1, m_2)$.

Субституції g, h називають ся **складовими** (konstituierende) субституціями ґрупи

$$K = \{g, h\};\text{*)} \tag{10}$$

то значить, що в ґрупі K поміщені всї можливі комбінації тих субституцій, які стоять в скобках. Ґрупа K називаєть ся **похідною** (abgeleitete) **ґрупою операторів** g і h (Mertens).

Подібно можемо утворити похідну ґрупу з кількох субституцій $g, h, \ldots, r$, а означимо її

$$K = \{g, h, \ldots, r\};$$

її порядок є $v(m_1, m_2, \ldots, m_r)$, т. зн. є найменшою спільною многократю порядків складових субституцій.

Похідна ґрупа даних субституцій істнує все; в остаточнім разї буде нею симетрична ґрупа, утворена зі всїх елементів, які входять в склад даних субституцій.

§. 19. Кожда субституція з ґрупи $\{g, h\}$ має вигляд:

$$g^\alpha h^\beta \; (\alpha = 1, 2, \ldots m_1;\ \beta = 1, 2, \ldots m_2).$$

Розуміеть ся, що в тій ґрупі мусять бути також субституції тої форми:

$$h^\gamma g^\delta.$$

III. Твердженє. Все дадуть ся дібрати такі чотири виложники: $\alpha, \beta, \gamma, \delta$, що буде сповнена рівність:

$$g^\alpha h^\beta = h^\gamma g^\delta. \tag{11}$$

Доказ (по части за Netto'ном**). Субституції g і h є лиш виїмково перемінні, отже реляція $gh = hg$ не обовязує все.

Нехай буде $gh \neq hg$, тодї можемо знайти такий виложник λ, що буде сповнена реляція

$$gh = h^\lambda g.$$

*) Netto. Substitutionentheorie und ihre Anwendungen auf die Algebra, Leipzig, (Teubner) 1882. стр 39, 40 (нота).

**) op. cit. стр. 37. sqq.

Що таке λ дїйсно істнує, виходить з реляції, ідентичної з попереднім рівнанем

$$h^{\lambda} = ghg^{-1},$$

т. зн., що h^{λ} є трансформованою субституцією з h при помочи g^{-1}, отже таке λ дасть ся все знайти. Тому приймаємо ту рівність за доказану. Тодї є:

1. для $\beta = \alpha$:

$$\begin{aligned} g^{\alpha} h^{\alpha} &= g^{\alpha-1}.gh.h^{\alpha-1} = g^{\alpha-1}.h^{\lambda} g.h^{\alpha-1} = g^{\alpha-2}.gh.h^{\lambda-1}.gh.h^{\alpha-2} \\ &= g^{\alpha-2}.h^{\lambda} g.h^{\lambda-1}.h^{\lambda} g.h^{\alpha-2} = g^{\alpha-3}.gh.h^{\lambda-1}.gh.h^{\lambda-2}.h^{\lambda}.gh.h^{\alpha-3} \\ &= g^{\alpha-3}.gh.h^{\lambda-1}.gh.h^{2(\lambda-1)}.gh.h^{\alpha-3} = . \\ &= g^{\alpha-i}.gh.h^{\lambda-1}.gh.h^{2(\lambda-1)}.gh \qquad h^{(i-1)(\gamma-1)} gh.h^{\alpha-i} = \\ &= g.gh.h^{\lambda-1}.gh.h^{2(\lambda-1)}.gh \qquad h^{(\alpha-2)(\lambda-1)}.gh.h \\ &= gh.h^{\lambda-1}.gh.h^{2(\lambda-1)}.gh \ldots h^{(\alpha-1)(\lambda-1)} gh = h^{\lambda} gh.h^{\lambda-1}.gh \ldots h^{\alpha(\lambda-1)} g \\ &= \ldots = h^{\gamma} g^{\delta}; \end{aligned}$$

2. для $\beta > \alpha$:

$$g^{\alpha} h^{\beta} = g^{\alpha} h^{\alpha}.h^{\beta-\alpha} = h^{\gamma} g^{\delta}.h^{\beta-\alpha} = h^{\gamma}.g^{\delta} h^{\delta}.h^{\beta-\alpha-\delta} = \ldots = h^{\varepsilon} g^{\zeta};$$

3. для $\beta < \alpha$ змінять тільки g і h свої ролї.

З того слїдує, що в формі $g^{\alpha} h^{\beta}$ містять ся всї субституції ґрупи $\{g, h\}$. — Подібно виказуємо, що кожду субституцію з ґрупи $\{g, h, \quad k\}$ можна представити в формі $g^{\alpha} h^{\beta} \quad k^{\lambda}$.

§. 20. Коли субституції g і h є з собою перемінні,

$$gh = hg, \tag{12}$$

ґрупа $\{g, h\}$ називаєть ся перемінною (kommutative) або Абелевою (Abel'sche Gruppe)*).

З реляції (12) слїдує

$$h = g^{-1} hg, \quad g = h^{-1} gh,$$

т. зн., що кожда субституція Абелевої ґрупи трансформує кожду иншу субституцію тої ґрупи в неї саму.

Кожда підґрупа Абелевої ґрупи є визначна, бо всї її субституції трансформують ся кождою субституцією Абелевої ґрупи в себе самих, отже всї спряжені ґрупи є ідентичні.

---

*) Weber, Algebra, Bd. I. Braunschweig 1898, стр. 517; Netto, Algebra, Bd. II. Leipzig (Teubner) 1900, стр. 539. — Деякі автори уживають назви „Абелева ґрупа" в иншім значіню; пор. Pascal, Repertorium d. höh. Math. Bd. I. Leipzig (Teubner) 1900 стр. 37.

§ 21. **IV. Твердженє.** Кожду субституцію Абелевої ґрупи G можна представити в формі

$$s = s_1^{\alpha_1} s_2^{\alpha_2} s_3^{\alpha_3} \qquad s_\nu^{\alpha_\nu}, \tag{13}$$

де s_1, s_2, ., s_ν є перемінними субституціями, а виложники є менші від порядків тих субституцій. Порядок Абелевої ґрупи є добутком з порядків субституцій s

$$r = a_1 a_2 \qquad a_\nu. \tag{14}$$

Доказ. 1. В формі (13) можемо представити кождий елемент Абелевої ґрупи. Елемент s_λ одержимо, кладучи всі $\alpha_i = 0$, з виїмком α_λ, яке кладемо $= 1$; кождий инший елемент одержимо через відповідну комбінацію виложників.

2. Коли субституції s_1, s_2, ., s_ν ріжні, то в формі (13) можемо представити кождий елемент Абелевої ґрупи тільки один раз, згл. рівну скількість разів. Бо коли елемент 1 представимо так:

$$1 = s_1^{h1} s_2^{h2} \qquad s_\nu^{h\nu}, \tag{15}$$

то s не змінить ся, коли ми в (14) виложники α_1, α_2, . α_ν заступимо сумами $\alpha_1 + h_1$, $\alpha_2 + h_2$, ., $\alpha_\nu + h_\nu$. Приймім, що представленє (14) можливе на k способів; форма (11) подасть нам кождий елемент ґрупи G що найменше k разів.

Коли-б знова s можна було представити такими двома рядами виложників: α_1, α_1, ., α_ν; β_1, β_2, ., β_ν, то будемо мати очивидно:

$$1 = s_1^{\beta_1 - \alpha_1} s_2^{\beta_2 - \alpha_2} \qquad s_\nu^{\beta_\nu - \alpha_\nu},$$

а звідси слїдує: $\beta_1 = \alpha_1 + h_1$, $\beta_2 = \alpha_2 + h_2$, ., $\beta_\nu = \alpha_\nu + h_\nu$, т. зн., коли-б ми мали дві ріжні форми для того самого елемента, то виложники тих форм могли би ріжнити ся тільки о h_λ; ми приймили, що є k можливих способів для представленя (14), отже форма (13) не може давати нам жадного елементу більше разів ніж k.

3. З того слїдує: $nk = a_1 a_2$. a_ν, а що $k = 1$ (бо реляція (15) тільки тодї можлива, коли кождий елемент буде $= 1$), то тим самим доказана і реляція (13).

4. Коли ϱ є дїльником числа ν, то в G мусить бути субституція порядку ϱ, бо одно з чисел a_1, a_2, a_ν в (13) мусить бути подїльне через ϱ, нпр. $a_k = k\varrho$: тодї субституція s_k^k буде порядку ϱ, бо $(s_k^k)^\varrho = 1$.

Коли m є найменшою спільною многократю чисел $a_1, a_2, \ldots a_r$, то в групі G мусить приходити субституція

$$s' = s_1 s_2 \quad s_\nu$$

порядку m, бо ми можемо написати:

$$(s')^m = (s_1 s_2 \quad s_\nu)^m = s_1^m s_2^m \quad s_\nu^m = 1.$$

отже порядок субституції s' є дійсно m.

5. Коли $\varrho = gh$ (g і h зглядно перві), то група G обіймає рівно g елементів σ, яких порядок є дїльником числа h, так що кождий елемент групи g можна представити в видї

$$s = \sigma\tau. \text{*)} \tag{16}$$

Бо коли g і h є зглядно перві числа, то можна знайти все такі два числа x і y, які сповнять рівнане

$$gx + hy = 1;$$

всї елементи σ, яких порядок є дїльником числа g, творять очивидно групу Σ, а так само всї елементи τ творять групу T. Візьмім тепер елемент s з G, то будемо мати:

$$s = s^{gx} s^{hy}$$

(бо сума виложників $=1$); а що $(s^{hy})^g = 1$, то субституція s^{hy} містить ся в групі Σ, а з тої самої причини s^{gx} містить ся в T. Звідси слїдує, що s має дійсно форму (16).

З того бачимо, що кожду субституцію групи G можемо представити спершу як добуток двох субституцій, яких порядки є дїльниками чисел g і h. Коли далї числа g і h дадуть ся розложити на зглядно перві чинники, то кожду з субституцій σ і τ можна дальше представити як добуток двох субституцій ріжних порядків і т. д., аж врештї дійдемо до форми (13). Треба тепер ще тільки виказати, що форма (13) істнує дійсно, коли порядок групи є степенем первого числа: $r = p^k$. Коли-б те не було можливе, то ми не могли би утворити добутка (16), отже мусимо доказати можливість реляції

$$s = \sigma^\alpha \tag{17}$$

в разї $r = p^k$. Возьмім за σ таку субституцію, якої порядок a є можливо найвисший; a мусить бути очивидно степению числа p, а степені всїх субституцій s подїльниками числа a. Періода субституції σ

$$1, \sigma, \sigma^2, \quad ., \sigma^{a-1} \tag{18}$$

складаєть ся з самих ріжних субституцій. Коли сей ряд вичерпує цїлу Абелеву групу порядку p^k, наше твердженє доказане; коли-ж

*) Weber, Algebra II. стр. 40.

нї, беремо одну з позісталих субституцій τ. Кожда з тих субституцій τ мусить мати такий виложник h, щоби τ^h містило ся в ряді (17); в остаточнім разї є h порядком субституції τ $\tau^h = 1$. Нехай буде b найменшим таким числом h, тодї маємо

$$\tau^b = \sigma^\lambda;$$

b мусить бути дїльником числа a, отже також степеню числа p, а заразом і дїльником числа λ. Положім $a = qb + b'$, то

$$\tau^a = \sigma^{\lambda q}.\ \tau^{b'} = 1,$$

отже $\tau^{b'} = \sigma^{-\lambda q}$, т. зн. $b' = 0$, бо $b' < b$, а b має ту прикмету, що є найменшим з виложників, для яких τ^b містить ся в рядї (17). Звідси маємо дальше

$$\sigma^a = \tau^{\lambda q},$$

а що $q = \frac{a}{b}$, то $\frac{\lambda a}{b}$ мусить бути многократю числа a, отже b мусить містити ся в λ.

6. Приймаючи за α і β ряди чисел

$$\alpha = 0, 1, 2, \ldots, a - 1; \beta = 0, 1, 2 \ldots, b - 1,$$

можемо кожду субституцію s написати в формі

$$s = \sigma^\alpha \tau^\beta. \tag{19}$$

Коли ми тою формою не вичерпали всїх субституцій Абелевої ґрупи, продовжуємо наше розумоване. Таким чином буде наше твердженє доказане.

III. Головні прикмети ґруп.

§. 23. **Дефініції**. 1) Ґрупу G називаємо переходною (transitiv), коли її субституції переводять кождий з елементів в кождий инший.

2). Ґрупа, яка не має тої прикмети, називаєть ся неперехідною (intransitiv); в такім разї можна всї елементи подїлити на кляси так, що ґрупа буде переводити елементи тільки серед тої самої кляси, а нїколи елементів з одної кляси в другу. Нпр. ґрупа

$$G_1 = [1, (12)(34), (13)(24), (14)(23)]$$

є перехідна, бо її кождий елемент можна поставити на кожде місце, зате ґрупа

$$G_2 = [1, (12)(34)]$$

є неперехідна, бо не має субституції, яка могла би перевести 1 і 2 в 3 і 4; отже 1, 2 і 3, 4 є тими клясами елементів.

3). Перехідна ґрупа є непервісна (imprimitiv), коли її елемента можна поділити на такі кляси о рівнім числї членів, що субституції ґрупи або переставляють елемента в нутрі кождої кляси або тільки пересувають кляси поміж собою. Ті кляси елементів називаємо клясами непервісности (Imprimitivitätssysteme). Порядок непервісної ґрупи є добутком з числа кляс і числа елементів в кождій клясї; отже ґрупа, якої порядок є числом первим, не може бути непервісна.

4). Коли такий поділ елементів на кляси неможливий, ґрупа називаєть ся первісною (primitiv).

§. 24. Дві ґрупи

$$G=[1, g_1, g_2, \ldots, g_{m-1}],$$
$$\Gamma=[1, \gamma_1, \gamma_2, \ldots, \gamma_{\mu}-1]$$

називають ся ізоморфними (isomorph), коли стоять до себе в такім відношеню: до кождої субституції з G належить одна або більше субституцій з Γ так, що добуткови двох субституцій з G буде відповідати добуток двох приналежних субституцій з Γ.

Ґрупи можуть бути одностепенно ізоморфні (einstufig, holoëdrisch isomorph), коли кождій субституції з G відповідає одна тільки субституція з Γ, — або многостепенно (mehrstufig, meroëdrisch) ізоморфні, коли одній субституції з G відповідає більше субституцій з Γ; многостепенний ізоморфізм є односторонний або взаїмний в міру того, чи тільки ґрупа G є многостепенно ізоморфна супроти Γ, а Γ супроти G тільки одностепенно, чи і навпаки.

При многостепеннім ізоморфізмі творять ті субституції з Γ, які відповідають одній з субституцій в G, ґрупу Δ, бо добуток яких небудь з поміж них буде також відповідати тій самій субституції з G.

§. 25. Ми назвали ґрупу зложеною, коли вона містила в собі яку небудь підґрупу, ріжну від 1. Тепер мусимо змодифікувати ту дефініцію так, що ґрупа є тоді зложена, коли містить в собі визначну підґрупу; инакше назвемо ґрупу поодинокою.

Коли в G містить ся визначна підґрупа H того рода, що нема вже нїякої висшої ґрупи K, яка була би визначною підґрупою для G і містила в собі заразом H як визначну підґрупу, тодї H називаєть ся найбільшою визначною підґрупою ґрупи G (ausgezeichnete Maximaluntergruppe, Netto; Maximalnormalteiler, Weber). Ми будемо уживати коротшої назви: **найбільша підґрупа**.

Утворім найбільшу підґрупу H для G і шукаймо, чи ґрупа H не має зі своєї черги якої найбільшої підґрупи. Коли така ґрупа істнує, беремо її за основу до дальшого шуканя, аж врешті дійдемо до такої ґрупи M, яка не має вже ніякої найбільшої підґрупи крім 1. Тоді маємо ряд ґруп

$$G,\ H,\ K, \quad .,\ M,\ 1, \tag{1}$$

званий **рядом зложеня для ґрупи** G (Kompositionsreihe, Reihe der Zusammensetzung von G) або коротко **рядом ґрупи** G.

Назвім порядки поодиноких членів того ряду

$$r,\ r_1,\ r_2, \quad .,\ r_{\mu-1},\ 1, \tag{2}$$

тоді показчики слідуючих по собі членів ряду є цілими числами λ (твердженє Cauchy, §. 14)

$$\frac{r}{r_1}=e_1, \frac{r_1}{r_2}=e_2, \ldots, \frac{r_{\mu-2}}{r_{\mu-1}}=e_{\mu-1},\ r_{\mu-1}=e_\mu, \tag{3}$$

а їх добуток є рівний порядкови ґрупи G

$$r=e_1e_2 \qquad e_{\mu-1}e_\mu. \tag{4}$$

Числа $e_1,\ e_2, \quad .,\ e_\mu$ називаємо **показчиками ряду ґрупи** G або **чисельними чинниками зложеня для ґрупи** G (numerische Kompositionsfaktoren von G).

Ряд зложеня відзначає ся тим, що кождий його член є найбільшою підґрупою попереднього, отже є переміннй з ним, $GH=HG$, т. зн. $G^{-1}HG=H$. Довільна субституція з G трансформує субституцію h з H в якусь иншу субституцію з H: $g^{-1}hg=h'$, отже $hg=gh'$.

§. 26. **I. Твердженє. Ряд ґрупи G відзначає ся тим, що кождий член того ряду є ґрупою перемінною аж по субституції слїдуючої ґрупи.**

Доказ. Нехай в ряді ґрупи G по K слїдує L; назвім k субституцію з K, l субституцію з L, а σ нехай буде також субституцією з K, якої нема в L; тоді можемо написати:

$$k=l\sigma^\lambda, \tag{5}$$

т. зн. довільну субституцію з K одержимо, комбінуючи з l таку субституцію, якої нема в L. Возьмім дві субституції з K

$$k_\alpha=l_\alpha\sigma^\alpha,\ k_\beta=l_\beta\sigma^\beta$$

і творім добутки (§. 19)

$$k_\alpha k_\beta = l_\alpha \sigma^\alpha l_\beta \sigma^\beta = l_\alpha (\sigma^\alpha l_\beta \sigma^{-\alpha}) . \sigma^{\beta+\alpha} = l_\alpha l_\gamma \sigma^{\alpha+\beta} = l_\gamma \sigma^{\alpha+\beta};$$

$$k_\beta k_\alpha = l_\beta \sigma^\beta l_\alpha \sigma^\alpha = l^\beta (\sigma_\beta l_\alpha \sigma^{-\beta}) . \sigma^{\alpha+\beta} = l_\beta l_\varepsilon \sigma^{\alpha+\beta} = l_\zeta \sigma^{\alpha+\beta};$$

звідси слїдує

$$k_\alpha k_\beta = k_\beta k_\alpha . l_\mu. \tag{6}$$

Ту прикмету ґрупи K висказуємо так, що її субституції є **перемінні аж по субституції ґрупи** L (bis auf Substitutionen von L vertauschbar). Те саме відносить ся до кождої ґрупи в рядї зложеня, отже наше твердженє доказане.

§. 27. **II. Твердженє. Одна ґрупа може мати кілька ріжних рядів зложеня; в кождім ряді будуть приходити ті самі показчики і що найбільше будуть ріжнити ся тільки упорядкованем.**

Доказ.*) Нехай будуть можливі такі два ряди ґрупи G:

1). $G, G_1, G_2, G_3, \ldots$; порядки: $r, r_1 = \frac{r}{e_1}, r_2 = \frac{r_1}{e_2}. r_3 = \frac{r_2}{e_3}, \ldots$;

2). $G, G_1', G_2' G_3', \ldots$; порядки: $r \ r_1' = \frac{r}{e_1'}, r_2' = \frac{r_1'}{e_2'}, r_3' = \frac{r_2'}{e_3'}, \ldots$;

в обох разах є:

$$e_1 e_2 e_3 \quad . = r \text{ і } e_1' e_2' e_3' \quad = r.$$

Утворім ґрупу Γ, яка буде перекроєм ґрупи G_1 і G_1'; її порядок ϱ буде дїльником чисел r_1 і r_1': $\varrho = \frac{r}{k} = \frac{r_1}{k'}$. Назвім σ_α субституції ґрупи Γ; тодї можемо уложити для ґруп G_1 і G_1' такі роздїленя:

$$\begin{array}{ll}
\sigma_1 = 1, \ \sigma_2, \ \sigma_3, \qquad \sigma_\varrho; & \sigma_1 = 1, \ \sigma_2, \ \sigma_3. \qquad \sigma_\varrho; \\
s_1 \sigma_1, s_1 \sigma_2, s_1 \sigma_3, \ldots, s_1 \sigma_\varrho; & s_1' \sigma_1, s_1' \sigma_2, s_1' \sigma_3 \ \ldots, s_1 \sigma_\varrho; \\
 & \\
s_k \sigma_1, s_k \sigma_2, s_k \sigma_2, \ldots, s_k \sigma_\varrho; & s_{k'}' \sigma_1. s_{k'}' \sigma_2, s_{k'}' \sigma_3, \ldots, s_{k'}' \sigma_\varrho.
\end{array}$$

Таким чином можемо представити всї субституції обох ґруп в видї:

$$t_\alpha = s_\beta \sigma_\gamma, \text{ згл. } t_\alpha' = s_\beta' \sigma_\gamma.$$

Утворім тепер субституцію

$$\tau = t_a^{-1} t_b'^{-1} t_a t_b';$$

вона буде належати до ґрупи Γ, бо є спільна обом ґрупам: в видї $^{-1}(t_b^{-1} t_a t_b)$ належить до G_1, а в видї $(t_a^{-1} t_b^{-1} t_a) t_b$ до G_1'. Та

*) Netto, Substitutionentheorie, стр. 87.

сама субституція належить рівно-ж до ґрупи $\{G_1, G_1'\} = \mathfrak{G}$; та ґрупа є перемінна з G і містить ся в G. Вона є більша від G_1 і від G_1', отже є ідентична з G.

Порядки ґруп G_1 і G_1' є $r_1 = \frac{r}{e_1}$ і $r_1' = \frac{r}{e_1'}$; порядок ґрупи G є r, а що $r_1 = \varrho k$; $r_1' = \varrho k'$ отже

$$r = \varrho k e_1 = \varrho k' e_1', \text{ то}$$
$$k' = e_1, \; k = e_1'.$$

Звідси бачимо, що ґрупа Γ має порядок $\varrho = \frac{r_1}{e_1'} = \frac{r_1'}{e_1} = \frac{r}{e_1 e_1'}$; вона мусить стояти в ряді ґрупи G, бо є найбільшою підґрупою G_1 і G_1'.

Таким чином можемо написати такі ряди для G:

3). G, G_1, Γ, Δ, порядки: $r, r_1 = \frac{r}{e_1}, r_2' = \frac{r_1}{e_1'}$,.

4). G, G_1', Γ, Δ, порядки: $r, r_1' = \frac{r}{e_1'}, r_2 = \frac{r_1}{e_1}$,

звідси слідує, що ряди 1) і 2) мають в перших трьох членах ті самі показчики, що 3) і 4) разом. Дальший доказ лежить в тім, що творимо ряди;

5). $G, G_1, G_2, \mathfrak{G}$, порядки: $r, r_1 = \frac{r}{e_1}, r_2 = \frac{r_1}{e_2'}, r_3'' = \frac{r_2}{e_2'}, \ldots$;

6). $G, G_1, \Gamma, \mathfrak{G}$, .; порадки: $r, r_1 = \frac{r}{e_1}, r_2' = \frac{r_1'}{e_2'}, r_3'' = \frac{r_2'}{e_2}, \ldots$;

попереднє розумоване зачинаємо від члена G_1, і так поступаємо аж до кінця. З того слідує остаточно також, що й скільквість членів в кождім ряді є однакова.

§. 28. Netto*) впроваджує ще т. зв. головний ряд (Hauptreihe) зложеня ґрупи G, або коротко: головний ряд. Повстає він так, що з ряду зложеня ґрупи задержуємо тільки ті члени, які є перемінні з ґрупою G.

Ряд зложеня є взагалї обширнїйший від головного ряду; нехай буде головний ряд:

$$G, H, J, \qquad M, 1 \tag{7}$$

---

*) Substitutionentheorie, стр. 92; Weber, Algebra II. стр. 31.

тодї між кождими двома його числами будуть стояти ґрупи, які належатимуть до ряду зложеня, нпр. між H і J нехай стоїть

$$H_1, H_2, \quad ., H^{\nu-1}. \tag{8}$$

З дефініциї виходить, що H є перемінне з G; так само J, але члени ряду (22). Длятого коли будемо ґрупу H_2 трансформувати субституціями з G, одержимо цїлий ряд подібних і ізоморфних ґруп

$$H_1, H_1', H_1'', \quad .;$$

показчик всїх тих ґруп з огляду на H буде однаковий, нпр. q.

Утворім перекрої ґруп H_1 і H_1'; H_1 і H_1''; H_1 і H_1'''; . .; і поставмо їх в ряд (22) по H_1. Будуть се знова ізоморфні і подібні ґрупи о тім самім показчику q. Коли істнує тільки одна така ґрупа, то вона є членом головного ряду, J, а її показчик з огляду на H є q^2.

Коли-ж тих перекроїв є більше, творимо дальше перекрої ґруп H_1, H_1, H_1'' і т. д.; вони будуть мати знова такий самий показчик q.

По ν кроях дійдемо врештї до J; показчик ґрупи J з огляду на H буде q^ν; той показчик буде належати вже до головного ряду (21).

Звідси слїдує

III. Твердженє. Коли ряд ґрупи G є обширнійший від головного ряду, то члени, які стоять між двома по собі слїдуючими ґрупами головного ряду, мають ті самі показчики.

Тільки такі ґрупи можуть мати головний ряд, яких порядок має в собі деякі або всї рівні чинники ґрупи, які стоять перед J побіч себе (не по собі), $H_{\nu-1}$, $H'_{\nu-1}$, $H''_{\nu-1}$, ., є перемінні, а скомбіновані з собою дають ґрупу H:

$$H = \{H_{\nu-1}. H'_{\nu-1}, H''_{\nu-1}, \quad .\}. \tag{9}$$

IV. Твердженє. Остатня ґрупа головного ряду складаеть ся з одної або більше подібних ґруп, які не мають перекрою більшого від 1, і є Абелевою ґрупою.

Виходить се з того, що субституції кождої з тих ґруп мусять бути перемінні з собою аж по субституції слїдуючого члена, а що ним є 1, то ті субституції є перемінні.

§. 29. Шукаймо ряду зложеня для симетричної ґрупи G. Безпосередно бачимо, що другим членом того ряду буде альтернуюча ґрупа. Коли степень ґрупи $n > 4$, тоді з альтернуючою ґрупою кінчить ся ряд симетричної ґрупи, бо альтернуюча ґрупа є поодинока для $n > 4$.

До того результату доходимо при помочи таких тверджень:

I. Перехідна ґрупа, яка містить в собі одну яку-небудь транспозицію, є ідентична з симетричною.

Приймім, що тою транспозицією є (12). В разї перехідности ґрупи мусять містити ся в нїй всї такі субституції, які переводять котрий небудь елемент, нпр. 1, в кождий инакший, отже мусить істнувати такий ряд транспозицій:

$$(12),\ (13),\ (14),\ \ldots,\ (1n).$$

Комбінуючи ті транспозиції на всї можливі способи, одержимо симетричну ґрупу.

II. Перехідна ґрупа, яка містить в собі один тричленний цикль, є ідентична з альтернуючою або з симетричною ґрупою.

З огляду на перехідність ґрупи мусить в нїй поруч циклю (123) істнувати такий ряд циклїв

$$(124),\ (125),\ \ldots,\ (12n);$$

кождий з тих циклїв можна розложити на дві транспозиції

$$(12k) = (12)(1k),$$

а добуток таких двох циклїв також на дві транспозиції або стягнути на один тричленний цикль:

$$(12k)(12l) = (12)(1k)(12)(1l) = (1k)(1l) = (\ kl),$$

отже все одержуємо субституції першої кляси. В такім разї маємо альтернуючу ґрупу. Коли-ж в ґрупі містить ся ще одна поодинока транспозиція (ab), то одержимо субституцію другої кляси, комбінуючи її з тричленним циклем, отже наша ґрупа складаєть ся зі всїх субституцій обох кляс, т. зн. є симетрична.

III. Альтернуюча ґрупа висшого степеня нїж четвертий є поодинока*).

Приймім, що альтернуюча ґрупа H не є поодинока, тільки що по нїй слїдує в рядї симетричної ґрупи G ще инша, K, отже K мусить бути найбільшою підґрупою для H.

---

*) Доказ гл. Weber, Algebra I. стр. 649.

Нехай K містить в собі субституцію k; коли один з тричленних циклів ґрупи H назвемо c, то K мусить містити в собі субституцію

$$c^{-1}kc,$$

бо K є найбільша підґрупа для H, отже також і субституцію

$$\lambda = k^{-1}c^{-1}kc.$$

Розберім, які форми може мати λ; се залежить від форми субституції k.

1. k містить в собі один більше нїж тричленний цикль:

$$k = (1\ 2\ 3 \qquad m).$$

Возьмім $c = (1\ 2\ 3)$; утворім λ:

$$\lambda = (1\ 2\ 4)$$

отже в K приходить один тричленний цикль; K є ідентичне з альтернуючою ґрупою.

2. k має два тричленні циклї $(1\ 2\ 3)$, $(4\ 5\ 6)$. Приймім $c = (1\ 3\ 4)$, тодї $\lambda = (1\ 2\ 5\ 3\ 4) \quad . . ;$ K має проте одну субституцію другої кляси, отже не може бути підґрупою для H.

3. k має транспозицію і тричленний цикль $(1\ 2\ 3)\ (4\ 5)$. Беручи $c = (1\ 2\ 4)$, маємо $\lambda = (1\ 2\ 5\ 3\ 4)$, — анальоґічно як в 2.

4. k має дві транспозиції $(1\ 2)\ (3\ 4)$. Коли $n > 4$, то в ґрупі мусить бути крім 1, 2, 3, 4 ще бодай один елємент, нпр. 5. Тодї кладемо $c = (1\ 2\ 5)$, а звідси $\lambda = (1\ 5\ 2) \quad .$, як в 1.

5. k має три транспозиції $(1\ 2)\ (3\ 4)\ (5\ 6)$. Беремо $c = (1\ 3\ 5)$; звідси є $\lambda = (1\ 3\ 5)\ (2\ 6\ 4) \qquad$ отже в K містить ся субституція, яка має два тричленні циклї, як в 2.

Инші комбінації дво-, три- і більше членних циклів неможливі. З того виходить, що K є ідентичне з H, отже **альтернуюча ґрупа є поодинока**. — Отсе є причиною, що загальних рівнань степеня вписшого як четвертий не можна альґебраїчно розвязувати.

§. 30. Евентуальність 4. вказує, що коли $n = 4$, то альтернуюча ґрупа є зложена, іменно її найбільша підґрупа буде містити субституцію $k = (1\ 2)\ (3\ 4)$. Шукаймо тої підґрупи.

Коли k є субституцією шуканої ґрупи K, то вона мусить містити в собі також всї трансформовані з K при помочи инших субституцій k з ґрупи H. Возьмім $h_1 = (1\ 2\ 3)$, тодї

$$h_1^{-1}\,k\,h_1 = (1\ 2\ 3)^{-1}\,(1\ 2)\ (3\ 4)\ (1\ 2\ 3) = (1\ 3\ 2)\ (1\ 2)\ (3\ 4)\ (1\ 2\ 3) = (1\ 4)\ (2\ 3),$$

дальше возьмім $h_2 = (1\ 2\ 4)$, отже

$$h_2^{-1} k h_2 = (1\ 3)\ (2\ 4).$$

Дальші тричленні циклі не дадуть вже ніяких нових субституцій для K, бо кождий з них можемо зложити з h_1 і h_2:

$$h_3 = (2\ 3\ 4) = (\ 1\ 2\ 3)\ (1\ 4\ 2) = h_1 h_2^2,$$

$$h_4 = (1\ 3\ 4) = (1\ 2\ 4)\ (2\ 3\ 4) = h_2 h_1\ h_2^2.$$

Таким чином вичерпані вже всі субституції, і K складаєть ся з:

$$1,\ k_1 = k, k_2 = h_1^{-1} k h_1, k_3 = h_2^{-1} k h_2.$$

Шукаймо дальше найбільшої підґрупи L для K. Коли вона має в собі одну транспозицію, нпр. $l = (12)$, то мусить мати всі трансформовані з l при помочи всїх k:

$$k_1^{-1} l k_1 = ((12)\,(34))^{-1}(12)((12)(24)) = (34)^{-1}(12)^{-1}(12)(12)(34)$$
$$= (34)^{-1}(12)(34) = (12) = l_1;$$

$$k_2^{-1} l k_2 = ((14)(23))^{-1}(12)((14)(23)) = (23)^{-1}(14)^{-1}(12)(14)(23)$$
$$= (23)^{-1}((14)^{-1}(12)(14))(23) = (23)^{-1}(24)(23) = (34) = l_2:$$

$$k_3^{-1} l k_3 = ((13)(24))^{-1}(12)((13)(24)) = (24)^{-1}((13)^{-1}(12)(13))(24)$$
$$= (24)^{-1}(23)(24) = (34) = l_3;$$

отже L складаєть ся з 1, (12), (34), (12)(34),

Коли-б ми взяли замість (12) иншу транспозицію, нпр. (13), то одержали би зовсїм відмінну ґрупу L_2, зложену з (13) і (24), а беручу (14), одержали-б L_3, зложену з (14) і (23).

Кожда з ґруп L є вже поодинока.

Загалом виглядає ряд зложеня симетричної ґрупи G так:

1). $G,\ H,\ K,\ L_1,\ 1$;

2). $G,\ H,\ K,\ L_2,\ 1$;

3). $G,\ H,\ K,\ L_3,\ 1$.

Ті три ряди ріжнять ся тільки передостатнїми членами. Кожда з тих ґруп складаєть ся з таких субституцій:

$G = [1;$ (12), (13), (14), (24), (34); (123), (124), (134), (234), (132), (142), (243); (1234), (13)(24), (1432); (1243), (14)(23), (1342); (1324), (12)(34), (1423)$]$;

$H = [1;$ (123), (124), (134), (234), (132), (142), (143), (243); (12)(34), (13)(24), (14)(23)$]$;

$K = [1,$ (12)(14), (13)(24), (14)(23)$]$;

$L_1 = [1,$ (12)(34)$]$; $L_2 = [1,$ (13)(24)$]$; $L_3 = [1,$ (14)(23)$]$.

Порядки тих ґруп є: $(G) = 4! = 24$; $(H) = \frac{4!}{2} = 12$; $(K) = 4$, $(L_1, L_2, L_3) = 2$. Ряд порядків виглядає так:

$$24, 12, 4, 2, 1,$$

а ряд чинників зложеня:

$$2, 3, 2, 2.$$

§. 31. Дотепер вважали ми показчики ряду зложеня звичайними числами; звідси їх назва: чисельні чинники зложеня ґруп. За приводом Hölder'a*) можемо одначе надати їм значінє ґруп.

Розділїм ґрупу G при помочи визначної підґрупи H (§. 14). отже одержимо ряд:

$$G = (H, g_1 H, g_2 H). \tag{10}$$

Побічні ґрупи можемо дальше вважати елементами, з яких можна утворити нову ґрупу; отже та нова ґрупа буде складати ся не з субституції, але з ґруп. Що система (2) творить дїйсно ґрупу, переконуємо ся примінюючи крітерії ґруп (§. 11).

1. Маючи два елементи з системи (2), творимо новий з тої самої системи; нпр. з $g_\alpha H$ і $g_\beta H$ творимо

$$g_\alpha H g_\beta H = g_\alpha g_\beta H H = g_\alpha g_\beta H = g_\gamma H$$

бо $H g_\beta = g_\beta H$ (визначна підґрупа є перемінна з елементами головної), а $HH = H$ (очивидно).

2. Закон асоціяції справджуєть ся:

$$g_\alpha H . g_\beta H g_\gamma H = g_\alpha g_\beta g_\gamma H = g_\alpha H . g_\alpha g_\gamma H = g_\alpha g_\beta H . g_\gamma H.$$

3. З

$$g_\alpha H g_\beta H = g_\beta H . g_\gamma H$$

слїдує однозначно:

$$g_\alpha H = g_\beta H,$$

бо

$$g_\alpha g_\gamma H = g_\beta g_\gamma H,$$

а множачи обі сторони відворотністю елемента $g_\gamma H$, маємо

$$g_\alpha = g_\beta,$$

отже і

$$g_\alpha H = g_\beta H.$$

---

*) Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen. Mathematische Annalen, Bd. XXXIV, 1889. стр. 29—56. — Пор. також Weber, Algebra II. §. 4.

З того бачимо. що система елементів в (10) є дійсно ґрупою. **Ту ґрупу** називаємо доповняючою ґрупою до G в віднесеню до H (komplementäre Gruppe zu G in Bezug auf H) і означуємо її:

$$G/H;$$

в тім означеню містять ся деяка анальоґія звичайного діленя з наведеною тут операцією.

Порядок ґрупи G/H є рівний ν, отже рівний показчикови ґрупи G з огляду на H. Звідси анальоґія поміж чинниками зложеня а доповняючими ґрупами.

IV. Ґрупи в віднесеню до альґебраічних функцій.

§. 32. Переставляючи в якійсь альґебраічній функції поміж собою змінні, одержуємо взагалі иншу вартість, ніж мала первісна функція. З тої точки погляду ділимо функції на одновартісні (einwertig) і многовартісні (mehrwertig). Коли при всїх можливих переставленях змінних функція буде мати m ріжних вартостий, називаємо її m-вартісною (m-wertig).

Переставлюване змінних відбуваєть ся при помочи субституцій; субституція дає тут приписи, в який спосіб має відбути ся те переставлене. Виконуючи між змінними функції F переставлене, приписане субституцією σ, кажемо, що ми ужили субституції σ до функції F (die Substitution σ auf F anwenden) або виконали субституцію на функції (die S. ausüben).

Означім функцію n елементів

$$x_1, x_2, \quad ., x_n$$

знаком $\varphi(x_1, x_2, \ldots, x_n)$; тоді ужиге субституції σ на φ означимо так

$$[\varphi(x_1, x_2, x_3, \quad ., x_n)]\sigma \text{ або } \varphi\sigma(x_1, x_2, x_3, \quad . x_n). \qquad (1)$$

Після того можемо означити первісну вартість тої функції знаком $\varphi_1(x_1, x_2, x_3, \quad ., x_n)$; се значить, що на функції φ виконали ми ідентичну субституцію 1.

Нпр. нехай буде дана функція чотирох елементів

$$\varphi = x_1x_2 + x_3x_4;$$

виконаймо на нїй всї субституції симетричної ґрупи чотирох елементів.

Одержимо з того три ріжні вартости:

$$\varphi_1 = x_1x_2 + x_3x_4,$$
$$\varphi_2 = x_1x_3 + x_2x_4,$$
$$\varphi_3 = x_1x_4 + x_2x_3;$$

инших вартостий та функція не може приймати. Нпр. при субституціях: (12), (34), (13)(24), (14)(32) і т. д. її вартість не може змінити ся, отже φ є тривартістна функція.

Коли якась субституція не змінює вартости функції, тоді кажемо, що **функція φ допускає субституцію σ** (die Funktion φ gestattet die Substitution σ). Всї субституції, які допускає дана функція, творять ґрупу, бо коли кожда з окрема не змінить вартости функції, то й їх комбінація не зможе змінити вартости. Ґрупу всїх тих субституцій називаємо **ґрупою функції φ** (die Gruppe der Funktion φ, або die zur Funktion φ gehörige Gruppe).

Нпр. ґрупа функції $\varphi_1 = x_1x_2 + x_3x_4$ складаєть ся з таких субституцій:

$$\Gamma_1 = [1, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)];$$

добираючи до Γ_1 транспозицію (23), одержимо ґрупу $\Gamma_2 = (23)\,\Gamma_1$, яка не змінює функції $\varphi_2 = x_1x_3 + x_2x_4$, а через дібране (24) одержимо $\Gamma_3 = (24)\,\Gamma_1$ ґрупу функції $\varphi_3 = x_1x_4 + x_2x_3$.

Кожда з тих ґруп є осьмого порядку.

§. 33. Функція n змінних може мати найбільше $n!$ вартостий; тоді кожда субституція з яких небудь елементів змінить її вартість, отже ґрупою $n!$-вартісної функції є ідентична субституція 1. — Навпаки така функція, яка має тільки одну вартість, має симетричну ґрупу, бо ніодна з субституцій не може змінити її вартости. Така функція називаєть ся **симетричною** (symmetrisch). Симетричними функціями є нпр. сума або добуток n змінних; сочинники рівнаня є симетричними функціями корінїв і т. д.

Двовартісна функція називаєть ся **альтернуючою функцією**, бо її ґрупа є альтернуюча. Альтернуючою функцією є нпр. квадратний корінь з т. зв. **діскрімінанти** т. є виражене

$$\sqrt{\Delta} = \Pi(x_i - x_j),\ i \neq j. \tag{2}$$

Кожду альтернуючу функцію можна представити в формі

$$\varphi = S_1 \pm S_2 \sqrt{\Delta}, \tag{3}$$

де S_1 і S_2 є симетричними функціями даних елементів, а $\sqrt{\Delta}$ є дво-

вартісний; се зазначуємо при помочи знаку $\pm$. Назвім обі вартости функції φ_1 і φ_2, тодї маємо:

$$\varphi_1 + \varphi_2 = 2S_1,$$
$$\varphi_1 - \varphi_2 = 2S_2\sqrt{\Delta},$$

отже їх сума є симетрична, а ріжниця альтернуюча.

§. 34. **I. Тверджене**. Ґрупа ϱ-вартісної функції n змінних є порядку

$$\nu = \frac{n!}{\varrho}.$$

Доказ. Назвім ϱ вартостий функції φ:

$$\varphi_1, \varphi_2, \quad ., \varphi_\varrho,$$

а її ґрупу G_1; вона нехай має ν субституцій

$$\sigma_1 = 1, \sigma_2, \sigma_3, \quad ., \sigma_\nu.$$

Ґрупа G_1 є підґрупою симетричної S, отже ν є дїльником числа $n!$; вона має ϱ—1 побічних ґруп, які переводять φ_1 чергою в $\varphi_2, \varphi_3, \quad ., \varphi_\varrho$. Кожда побічна ґрупа має той сам порядок, отже:

$$\nu = \frac{n!}{\varrho} \tag{4}$$

або

$$n! = \nu\varrho. \tag{4'}$$

В нашім примірі було $\nu = 8$, $\varrho = 3$, отже $\nu\varrho = 24 = 4!$

§. 35. Про функції, які мають ту саму ґрупу Γ, говоримо, що вони належать до рода ґрупи Γ (die zur Gattung von Γ gehörigen Funktionen). Скільність вартостий одної функції називаємо порядком рода ґрупи Γ, а знова всї ті вартости називаємо спряженими родами або спряженими вартостями (konjugierte Gattungen, Werte; Kronecker, Netto).

II. Тверджене. Функції одного рода можна представити раціонально при помочи якої небудь з поміж них.

Доказ. Нехай будуть дані дві функції, φ і ψ, які належать до рода ґрупи Γ, степеня n, порядку ν; вони мають $\varrho = \frac{n!}{\nu}$ ріжних вартостий, які одержимо, виконуючи на одній з них субституції, що не належать до Γ. Тим вартостям функцій φ і ψ, які одержуємо при помочи тої самої субституції, даймо однакові показчики, отже одержимо такі два ряди ріжних функцій:

$$\begin{aligned} &\varphi_1,\ \varphi_2,\ \varphi_3, \quad ., \varphi_\nu: \\ &\psi_1,\ \psi_2,\ \psi_3, \quad ., \psi_\varrho. \end{aligned} \tag{5}$$

Напишім тепер функцію:

$$\Phi_\lambda = \varphi_1\psi_1{}^\lambda + \varphi_2\psi_2{}^\lambda + \qquad \varphi_\varrho\psi_\varrho{}^\lambda \tag{6}$$

де λ може приймати ріжні цілочисельні вартости. Функція Φ_λ є з огляду на всі φ і ψ симетрична, бо переставляючи якінебудь φ, мусимо так само переставити і відповідні ψ.

Надаваймо виложникови λ вартости 0, 1, $\qquad \varrho-1$; таким чином одержимо систему ϱ лїнійних рівнань для φ:

$$\left.\begin{array}{llllll} \varphi_1 & +\varphi_2 & +\varphi_3 & + & +\varphi_\varrho & =\Phi_0 \\ \varphi_1\psi_1 & +\varphi_2\psi_2 & +\varphi_3\psi_3 & + & +\varphi_\varrho\psi_\varrho & =\Phi_1 \\ \varphi_1\psi_1{}^2 & +\varphi_2\psi_2{}^2 & +\varphi_3\psi_3{}^2 & + & +\varphi_\varrho\psi_\varrho{}^2 & =\Phi_2 \\ & & & & & \\ \varphi_1\psi_1{}^{\varrho-1} & +\varphi_2\psi_2{}^{\varrho-1} & +\varphi_3\psi_3{}^{\varrho-1} & + & +\varphi_\varrho\psi_\varrho{}^{\varrho-1} & =\Phi_{\varrho-1} \end{array}\right\} \tag{7}$$

Розвяжім ту систему для φ_1

$$\varphi_1 = \left|\begin{array}{lll} \Phi_0, & 1, & 1 \\ \Phi_1, & \psi_2, & \psi_\varrho \\ \Phi_2, & \psi_2{}^2, & \psi_\varrho{}^2 \\ & & \\ \Phi_{\varrho-1}, & \psi_2{}^{\varrho-1} & \psi_{\varrho-1} \end{array}\right| : \left|\begin{array}{lll} 1, & 1, & 1 \\ \psi_1, & \psi_2, & ., \psi_\nu \\ \psi_1{}^2, & \psi_2{}^2, & \psi_\varrho{}^2 \\ & & \\ \psi_1{}^{\varrho-1} & \psi_2{}^{\varrho-1}, & ., \psi_\varrho{}^{\varrho-1} \end{array}\right| \tag{8}$$

Знаменник того вираженя є коренем дїскрімінанти функцій $\psi_1, \psi_2, \quad ., \psi_\varrho$; розширім чисельник і знаменник тою дїскрімінантою, то одержимо в знаменнику $\Delta(\psi)$, отже симетричну функцію, а в чисельнику кождим разом цїлу функцію

$$\varphi_1 = \frac{G_1(\Phi.\psi)}{\Delta(\psi)}. \tag{9}$$

Виконуючи на тій функції ту субституцію, яка переводить φ_1 в φ_2, одержимо в чисельнику якусь иншу функцію $G_2(\Phi;\psi)$; G_2 є ріжне від G_1, бо розвязуючи систему (7) для φ_2 ужиємо вартости φ_1 замість φ_2, а крім того ще детермінанта, яка стоїть в чисельнику як чинник, змінить знак. Переходячи на лївій стороні до $\varphi_3, \varphi_4, \qquad \varphi_\varrho$, одержимо на правій ріжні від себе функції $G_3, G_4, \quad ., G_\varrho$; отже загально:

$$\varphi_i = \frac{G_i(\Phi; \psi)}{\Delta(\psi)}, \ (i = 1, 2, \quad ., \varrho). \qquad (10)$$

Отже наше тверджене доказане.

§. 36. **III. Тверджене** (відвернене II. твердженя). **Всї функції, які можна раціонально представити одною з них, належать до того самого рода.**

Доказ. З заложеня маємо для двох функцій, φ і ψ:

$$\varphi = R_1(\psi); \ \psi = R_2(\varphi).$$

φ є незмінне для всїх тих субституцій, які змінюють ψ, а так само ψ незмінне для ґрупи функції φ. Всї инші субституції, які змінять ψ, мусять змінити і φ, і навпаки, отже наше тверджене доказане.

§. 37. **IV. Тверджене. Ріжні вартости функції φ є коріними рівнаня ϱ-того степеня, якого сочинниками є симетричні функції змінних.**

Доказ. З φ_1, φ_2, ., φ_ϱ і неозначеної величини φ можемо утворити таке рівнане

$$F(\varphi) = (\varphi - \varphi_1)(\varphi - \varphi_2)\ldots(\varphi - \varphi_\varrho) = \varphi^\varrho + A_1\varphi^{\varrho-1} + \ldots + A_\varrho = 0; \ (11)$$

величини A_1, A_2, A_ϱ є симетричними функціями величин φ, отже і змінних x_1, x_2, ., x_n.

Нпр. з функції $\varphi = x_1x_2 + x_3x_4$ одержували ми три вартости, а творячи з них рівнане (10), одержуємо:

$$\varphi^3 - c_2\varphi^2 + (c_1c_3 - 4c_4)\varphi - (c_1{}^2c_4 - 4c_2c_4 + c_3{}^2) = 0,$$

де c_1, c_2, c_3, c_4 є елементарними симетричними функціями величин x_1, x_2, x_3, x_4, т. є

$$c_1 = x_2 + x_2 + x_3 + x_4,$$
$$c_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4,$$
$$c_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4,$$
$$c_4 = x_1x_2x_3x_4.$$

§. 38. **V. Тверджене. Істнує все така функція, якою можна раціонально представити довільну скількість даних функцій; та функція є лїнїйною функцією даних.**

Доказ. Нехай будуть дані функції φ; ψ, χ, . . .; α, β, γ, означують довільні параметри. Тодї можемо написати:

$$\omega = \alpha\varphi + \beta\psi + \gamma\chi +$$

Ґрупа функції ω містить всі ті субституції, які не змінюють функцій φ, ψ, χ, рівночасно, отже є перекроєм ґруп функцій φ, ψ, χ, тому то можна ω виразити лїнійно тими функціями.

Коли перекрій ґруп функцій φ, ψ, χ, є ідентичною ґрупою, тодї ω має $n!$ вартостий; функцією ω можна виразити кожду з даних функцій. В такім разї називаєть ся функція ω функцією Galois*).

V. Циклїчні й метациклїчні функції.

§. 39. Періоди n-членного цикля

$$g = (123\ldots n)$$

є ґрупою n-того степеня і n-того порядку. Субституції тої ґрупи можемо писати також в такій формі:

$$g = | z \quad z+1 | \ (\mathrm{mod.}\ n), \tag{1}$$

т. зн., що субституція g посуне кождий показчик о 1; остатнїй показчик заступить вона першим. На се вказує означенє (mod. n), бо воно значить, що ми не беремо повних вартостий величини $z+1$, тільки все той останок, який лишить ся по відділеню всїх цїлочисельних многократий величини n.

Квадрат субституції g посуне кождий показчик о два місця, т. є

$$g^2 = | z \quad z+2 | \ (\mathrm{mod.}\ n)$$

взагалї

$$g^k = | z \quad z+k | \ (\mathrm{mod.}\ n);$$

ті всї означеня містять ся в формулцї (1).

Ґрупа субституцій g називаєть ся циклїчною ґрупою (zyklische Gruppe), а належна до неї функція циклїчною функцією. Коли за n приймемо перве число p, тодї кожда субституція циклїчної ґрупи буде мати тільки один цикль, а циклїчна функція буде

$$\varphi = (x_1 + \omega x_2 + \omega^2 x_3 + \cdot \quad \cdot + \omega^{p-1} x_p)^p, \tag{2}$$

де ω є первісним p-тим коренем з одиниці. Що φ є дійсно циклїчною функцією, бачимо з того, що за ужитєм субституції g_α переходить φ в

$$(\varphi)_{g^\alpha} = (x_{\alpha+1} + \omega x_{\alpha+2} + \cdot \quad \cdot + \omega^{p-1} x_{\alpha+p})^p$$
$$= \omega^{\alpha p}(x_1 + \omega x_2 + \quad \cdot + \omega^{p-1} x_p)^p = \varphi,$$

бо $\omega^p = 1$, отже зовсїм не змінить ся.

---

*) Vogt, Leçons sur la résolution algèbrique des équations, Paris 1895, стр. 23.

§. 40. Коли $n = pq$, де p і q є перві числа, тоді можемо всї змінні представити так, що вони мають по два показчики, отже можемо їх уложити в прямокутник:

$$\left.\begin{array}{l} x_{11},\ x_{12},\ x_{13}, \qquad ., \ x_{1q}, \\ x_{21},\ x_{22},\ x_{23}, \qquad ., \ x_{2q}, \\ \\ x_{p1},\ x_{p2},\ x_{p3}, \qquad .; \ x_{pq}; \end{array}\right\} \quad (3)$$

репрезентанта тої системи означуємо x_{hk}. Щоби зазначити, що субституція g буде змінювати оба показчики, пишемо так:

$$g = | \, h, \, k \quad h + \alpha, \; k + \beta \, | \; (\text{mod.}\ p;\ \text{mod.} q); \qquad (4)$$

т. зн., що c замінить перший показчик h на $h + \alpha$ (mod. p), а другий k на $k + \beta$ (mod. q). Субституцію (4) можна назвати двосторонною (zweiseitig). Коли субституція змінює тільки один показчик, т. є коли $\beta = 0$ або $\alpha = 0$, назвемо її односторонною (einseitig). Порядок двосторонної субституції є $n = pq$, односторонної p або q, в міру того, чи $\beta = 0$, чи $\alpha = 0$. Коли $\beta = 0$, субституція g змінює тільки перші показчики, отже пересуває змінні x_{hk} тільки в прямовісних рядках таблиці (3); таку субституцію назвемо g_1 і зазначимо її як (1); для $\alpha = 0$ будемо мати субституцію g_2, яка пересуває тільки кожду змінну серед того самого поземого рядка. Супроти того можемо кожду двосторонну субституцію представити при помочи двох односторонних

$$g = g_1{}^{\alpha} g_2{}^{\beta} \begin{pmatrix} \alpha = 0, \ 1, & ., \ p-1 \\ \beta = 0, \ 1, & ., \ q-1 \end{pmatrix}. \qquad (5)$$

Субституції g_1 і g_2 є очивидно перемінні, бо обсяги їх ділання є зовсїм инакші: g_1 пересуває перші показчики, g_2 другі, отже нам байдуже, чи ми змінимо перше той чи другий показчик; ґрупа субституцій g є проте Абелева, а звідси форма (5) (§. 21).

Ґрупа субститутуцій g_1 є непервісна, бо всї її субституції g_1 переставлюють тільки елементи серед того самого прямовісного рядка або прямовісні рядки між собою; клясу непервісности становлять тут за кождим разом елементи

$$x_{1k},\ x_{2k},\ x_{3k}, \qquad ., \ x_{pk} \ (k = 1,\ 2, \qquad ., \ q).$$

Так само ґрупа субституцій g_2 є непервісна; клясами непервісности є елементи:

$$x_{h1},\ x_{h2},\ x_{h3}, \qquad ., \ x_{hq} \ (h = 1,\ 2, \qquad ., \ p).$$

Коли $p=q$, маємо p^2 елементів, а таблиця (3) стає квадратом

$$\left.\begin{matrix} x_{11}, & x_{12}, & \ldots, & x_{1p}, \\ x_{21}, & x_{22}, & \ldots, & x_{2p}, \\ \vdots \\ x_{p1}, & x_{p2}, & \ldots, & x_{pp}; \end{matrix}\right\} \quad (3')$$

тоді субституція (4) має тільки один модул

$$g = | h, k \quad h+\alpha, k+\beta | \text{ (mod. } p). \qquad (4')$$

§. 41. Коли n складаєть ся з більшої скількости первих чинників (однакових або ні), $n=pq \ldots r$, можемо елементам x надати тільки показчиків, кілько є в n первих чинників

$$x_{hk \ldots l};$$

в такім разї кожду субституцію, яка буде циклічно пересувати ті показчики, напишемо в формі

$$g = | h, k, \ldots, l \quad h+\alpha, k+\beta, \ldots, l+\gamma | \text{ (mod. } p\text{; mod. } q\text{; mod. } r) \quad (6)$$

або приймаючи

$$n = p_1 p_2 \ldots p_\nu,$$

$$g = | h_i \quad h_i + \alpha_i | \text{ (mod. } p_i\text{; } i = 1, 2, \ldots, \nu), \quad (6')$$

а означуючи субституцію, яка посуває λ-тий показчик о 1, а всї прочі лишає без зміни, g_λ — маємо

$$g = g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_\nu^{\alpha_\nu} (\alpha_i = 0, 1, 2, \ldots, k-1; i = 1, 2, \ldots, \nu) \quad (5')$$

Порядок субституції (5') є $p_1 p_2 \ldots p_\nu = n$.

Субституції (4) і (6) називаємо **зложеними циклїчними**.

Коли $p_1 = p_2 = \ldots = p_\nu$, отже $n = p^\nu$, субституція g називаєть ся **аритметичною** (aritmetisch) **порядку** p^ν, а ґрупа, утворена з тих субституцій, **аритметичною***).

Ми бачили, що порядок циклїчної ґрупи (1) був p, отже рівний степеневи ґрупи; так само порядок аритметичної ґрупи буде p^ν, отже рівний її степеневи, бо добір показчиків α_i в (5) допускає p^ν комбінацій.

§. 42. Анальоґічно до циклїчних функцій, можемо творити **зложені циклїчні функції**. До тої цїли потрібуємо двох або більшої скількости первісних корінів з одиниці, p_1-ого, ω_1, p_2-ого, ω_2, $\ldots$, p_ν-ого, ω_ν. При їх помочи творимо прості циклїчні функції таких елементів, яких всі показчики з виїмком першого є однакові, нпр. для $n = p_1 p_2$:

---

*) Отсю назву впровадив Cauchy, Exercices d' Analyse III. стр. 232.

$$\left.\begin{array}{l}\varphi_1=(x_{11}+\omega_1 x_{21}+\omega_1{}^2 x_{31}+\ldots+\omega_1{}^{p-1}x_{p_1 1})^{p_1},\\ \varphi_2=(x_{12}+\omega_1 x_{22}+\omega_1{}^2 x_{32}+\ldots+\omega_1{}^{p-1}x_{p_2 2})^{p_1},\\ \cdot\\ \varphi_{p_2}=(x_{1p_2}+\omega_1 x_{2p_2}+\omega_1{}^2 q_{3p_2}+\ldots+\omega_1{}^{p-1}x_{p_1 p_2})^{p_1};\end{array}\right\}\quad(7)$$

ґрупа кождої з тих функцій обіймає тільки такі субституції, які не змінюють других показчиків, отже g_1.

Тепер творимо циклічну функцію величин φ_λ; їх є p_2, отже мусимо до того ужити коріня ω_2

$$\psi=(\varphi_1+\omega_2\varphi_2+\omega_2{}^2\varphi_3+\ldots+\omega_2{}^{p-1}\varphi_{p_2})^{p_2}; \qquad (8)$$

до тої функції належить така ґрупа, яка пересуває циклічно величини φ, отже ґрупа субституцій g_2. Величини φ є незмінні для ґрупи g_1, отже ціла ґрупа, утворена з субституцій

$$g=g_1{}^{\alpha_1}g_2{}^{\alpha_2}(\alpha_1=0,\ 1,\ 2,\ldots,\ p_1-1;\ \alpha_2=0,\ 1,\ 2,\ldots,\ p_2-1)\ (5'')$$

не може змінювати функції ψ; проте зложена циклічна ґрупа є ґрупою функції ψ.

Коли маємо більше первих чинників в n, творимо нові циклічні функції при помочи корінів $\omega_3, \ldots, \omega_\nu$.

§. 43. Циклічні субституції пересувають кождий з показчиків о одно або більше місць, отже не лишають ні одного елємента без зміни. Шукаймо тепер такої субституції, яка переводить кождий з показчиків в його многократь; для $n=p$ будемо мати

$$t=|z\ \ az|\ (\mathrm{mod.}\ p). \qquad (9)$$

Що ті субституції творять ґрупу, виходить з їх комбінації

$$t_a t_b=|z\ \ az|.|z\ \ bz|=|z\ \ abz|=t_{ab};$$

порядок тої ґрупи є $p-1$, бо за a можна класти всї числа від 1 до $p-1$; вартість $a=0$, а так само $a=p$, не має значіня.

Ґрупа субституції t є перемінна, бо

$$t_a t_b=t_{ab}=t_{ba}=t_b t_a.$$

Комбінуючи ґрупу субституцій g з ґрупою субституції t, одержуємо ґрупу порядку $p(p-1)$, якої кожду субституцію можна представити в формі

$$s=|z\ \ az+b|\ (a=1,\ 2,\ \ldots,\ p-1;\ b=0,\ 1,\ \ldots,\ p-1). \quad (10)$$

Отсю ґрупу називаємо лїнїйною (linear; Jordan) або метациклїчною ((metazyklisch; Kronecker).

Трансформуючи яку небудь циклїчну субституцію субституцією лїнїйної ґрупи, одержимо иншу циклїчну субституцію

$$s^{-1}gs = g', \tag{11}$$

або

$$gs = sg'; \tag{12}$$

з огляду на те, що g і g' є субституції циклічної ґрупи, можемо написати:

$$GS = SG; \tag{13}$$

тут означує G циклїчну ґрупу, а S лїнїйну. З того бачимо, що **лїнїйна ґрупа є перемінна з циклїчною.** З рівнаня (11) виходить дальше, що **циклїчна ґрупа є визначною підґрупою лїнїйноï.**

§. 44. Функція, яка належить до ґрупи S, називаєть ся **метациклїчна.** Її можемо утворити так: при помочи ω творимо просту циклїчну функцію

$$\varphi = (x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{p-1} x_p)^p \tag{2}$$

яка позваляє на всї субституцї g, але під впливом t переходить в

$$(\varphi)_t = (x_a + \omega x_{2a} + \omega^2 x_{3a} + \ldots + \omega^{p-1} x_{pa})^p;$$

показчики при незвісних мусимо скорочувати для (mod. p); приймім, що

$$ka \equiv 1 \pmod{p},$$

тодї маємо:

$$x_a + \omega x_{2a} + \ldots + \omega^{p-1} x_{pa} = \omega^{k-1}(x_1 + \omega x_{1+a} + \omega^2 x_{1+2a} + \ldots + \omega^{p-1} x_{1-a}),$$

а звідси

$$(\varphi)_t = \varphi_a = (x_1 + \omega x_{1+a} + \omega_2 x_{1+2a} + \ldots + \omega^{p-1} x_{1-a})^p;$$

кладучи за a вартости: 1, 2, ... $p-1$, одержимо ряд функцій

$$\left.\begin{aligned}
\varphi_1 &= (x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{p-1} x_p)^p,\\
\varphi_2 &= (x_1 + \omega x_3 + \omega^2 x_5 + \ldots + \omega^{p-1} x_{2p-1})^p,\\
\varphi_3 &= (x_1 + \omega x_4 + \omega^2 x_7 + \ldots + \omega^{p-1} x_{3p-2})^p,\\
&\ldots\\
\varphi_{p-1} &= (x_1 + \omega x_p + \omega^2 x_{2p-1} + \ldots + \omega^{p-1} x_{p+1})^p,
\end{aligned}\right\} \tag{14}$$

симетрична функція тих величин буде вже незмінна для всїх субституцій t, бо буде переводити тільки кожде φ в инше.

Отже функція

$$\Phi = (\varphi - \varphi_1)(\varphi - \varphi_2) \ldots (\varphi - \varphi_{p-1})$$

є метациклїчною функцією.

§. 45. Подібно як перше, можемо і тут творити лінїйні ґрупи для зложених степенїв. Обмежимо ся тільки до того випадку, де $n = p^m$. В такім разї має субституція t вигляд:

$$t = | h,k,\ldots,l \quad a_1 h + a_2 k + \ldots + a_m l, b_1 h + b_2 k + \ldots + b_m l, \ldots,$$
$$c_1 h + c_2 k + \ldots c_m l \mid (\text{mod. } p) \qquad (16)$$

можемо її назвати **однородною лінїйною субституцією**, бо вона заступає кождий показчик однородною лінїйною функцією всїх инших. Cauchy називає її **ґеометричною субституцією** (geometrische S.).

Твердженє. Щоби вираженє t представляло (ґеометричну) субституцію, є конечне і вистарчаюче, щоби визначник, утворений з сочинників при показчиках, був зглядно первий до модулу p.

$$\varDelta = \begin{vmatrix} a_1 & a_2 & & a_m \\ b_1 & b_2 & & b_m \\ & & & \\ c_1 & c_2 & & c_m \end{vmatrix} \equiv|\equiv 0 \ (\text{mod. } p). \quad (17)$$

Доказ. Коли t має представляти субституцію, тодї мусить істнувати система рівнань

$$\left.\begin{aligned} a_1 h + a_2 k + \ldots + a_m l &\equiv h' \\ b_1 h + b_2 k + \ldots + b_m l &\equiv k', \\ & \\ c_1 h + c_2 k + \ldots + c_m l &\equiv l' \end{aligned}\right\} (\text{mod. } p), \qquad (18)$$

отже буде:

$$t = | h,k \ldots,l \quad h',k',\ldots,l' \mid \ (\text{mod. } p)$$

і навпаки:

$$t^{-1} = | h', k',\ldots,l \qquad h k,\ldots l \mid (\text{mod. } p).$$

Щоби з t можна перейти до t^{-1} при помочи рівнань (18), мусить бути визначник (17) зглядно первий до модулу p, бо тодї система (18) не мала би нїякого значіня.

§. 46. Скомбінувавши ґеометричні субституції з аритметичними, одержуємо **повну лінїйну ґрупу степеня** p^m (volle lineare Gruppe або lineare Kongruenzgruppe).

Її порядок є

$$(p^m - 1)\ (p^m - p)\ (p^m - p^2) \qquad (p^m - p^{m-1})^*).$$

*) Пор Netto, Substitutionentheorie, стр. 155.

Повна лінїйна ґрупа є перемінна з аритметичною. З того виходить, що аритметична ґрупа є визначною підґрупою повної лїнїйної.

Повна лїнїйна ґрупа степеня p^2 складаєть ся з двох родів субституцій:

$$\left.\begin{array}{l} g = | \, h\,k \quad h+a,\ k+\beta \, | \,, \\ t = | \, h,k \quad ah+bk,\ ch+dk \, | \end{array}\right\} (\text{mod. } p). \quad (19)$$

Та ґрупа містить в собі як підґрупу т. зв. метациклїчну ґрупу степеня p^2, якою займемо ся в дальшій части нашої працї.

Друга частина.

Теорія рівнань.

VI. Альґебраічні рівнаня.

§. 47. **Альґебраічне рівнане називаємо рішимим** (auflösbar), **коли його можна розвязати в альґебраічнім змислї, т. є представити його корінї як альґебраічні функції сочинників. Що розвязка рівнаня істнує все, виходить з основного твердженя альґебри, яке каже, що кожде рівнане, якого сочинники є дїйсними або сполученими числами, має один корінь з обсягу дїйсних або сполучених чисел, а тим самим як раз стільки корінїв, кілько одиниць є в степеню рівнаня***).

Помимо того не вміємо розвязати кождого даного рівнаня в альґебраічнім значіню; можемо радше сказати, що рішимі рівнаня є виїмками з поміж усїх, які-б ми могли утворити зі всїх можливих дїйсних і злучених чисел.

Теорія ґруп дає спромогу вибирати з поміж всїх рівнань рішимі.

*) Доказ основного твердженя альґебри не належить сюди, тільки до теорії функцій. Гл. нпр. Gauss, Vier Beweise für die Zerlegung ganzer alg. Funktionen in reelle Faktoren ersten und zweiten Grades. Ostwald's Klassiker der exakt. Wiss. Leipzig, 1898.