

# Początki teorii grup skończonych

Witold WIEŚŁAW, Wrocław

## 0. Wstęp

Praca jest kontynuacją części pierwszej (Więśław [1995]), w której omówione zostały podstawowe pojęcia algebry na tle ich historycznego rozwoju.

Obecnie skoncentruję się jedynie na pojęciu grupy – podstawowym pojęciu algebry. Poniżej prześledzone zostaną główne etapy w rozwoju tego pojęcia oraz najważniejsze osiągnięcia tej teorii, wraz ze wskazaniem odpowiednich źródeł.

Newcóm (por. Miller [1914–15]) pisał w 1893 roku:

*The mathematics of the twenty-first century may be very different from our own; perhaps the schoolboy will begin algebra with the theory of substitution groups, as he might now but for inherited habits.*

A oto jak o rozwoju teorii grup pisał van Vleck [1916].

*In the last half of the nineteenth century the same problem [afforded by the equation of the  $n$ th degree] eventuated in the theory of groups which has become the foundation of mathematical classification (many kinds of geometries and number fields have come to be distinguished). [...] For many reasons the last quarter of the nineteenth century might be termed the group period, from which we have only in part emerged. I need not tell you how necessary it became to explore geometry and analysis under the guidance of the group concept. Yet there are reservations which must be made in designating this quarter century as the group period.*

## 1. Początki teorii grup omówiłem w pierwszej części (Więśław, [1995]).

Przypomnę tu jedynie najważniejsze fakty.

Za okres wstępny w rozwoju pojęcia grupy należy uznać lata 1770–1846, tj. okres od pierwszych wyników Lagrange’a dotyczących permutacji (Lagrange [1770]), aż do ukazania się „Exercices” Cauchy’ego (Cauchy [1844]). Cauchy dowodzi podstawowych twierdzeń o grupach permutacji (Dahan [1980]). Jego dowody są jednakże ogólne i łatwo można przenieść je na przypadek dowolnych grup skończonych. Permutacje pojawiły się u Lagrange’a w związku z próbami algebraicznego rozwiązania ogólnego równania stopnia  $n$ , tj. z próbami zredukowania tego zadania do rozwiązania skończenia wielu równań dwumiennych, tj. równań postaci  $x^N - a = 0$ . Lagrange badał funkcje wymierne pierwiastków danego wielomianu stopnia  $n$  i liczbę wartości, które przyjmuje funkcja wymierna, jeżeli permutować pierwiastki tego wielomianu, tzn. liczył dla ilu permutacji  $g \in S_n$ ,  $w(x_1, \dots, x_n) = w(x_{g(1)}, \dots, x_{g(n)})$ , gdzie  $x_1, \dots, x_n$  są pierwiastkami danego wielomianu  $f$ . Zastosowanie permutacji okazało się pożyteczne: Ruffini [1799] zdołał udowodnić, że ogólne równanie stopnia większego niż 4 nie jest rozwiązywalne algebraicznie, tj. zgodnie z aktualną terminologią, nie jest rozwiązywalne przez pierwiastniki. W dowodzie swojego twierdzenia Ruffini wykorzystał fakt, że  $A_n$  jest grupą generowaną przez cykle długości 3 i dla  $n \geq 5$  jest grupą prostą, choć ten ostatni fakt wykorzystany był implícite.

Podobnie rozumował Abel podając w 1826 dowód niemożliwości rozwiązania przez pierwiastniki ogólnego równania stopnia 5.

W 1815 Cauchy badał dalsze własności permutacji, podając od razu zastosowania do wyznaczników.

Teoria przemennych grup skończonych ma swoje początki u Eulera i Gaussa, w związku z ich badaniami teorioliczbowymi nad resztami potęgowymi, jak też w związku z teorią klas binarnych form kwadratowych o współczynnikach całkowitych. Ich dowody były jednak *ad hoc* i mimo, że często można je bez trudu przenieść na przypadek ogólny, to jednak nie były to twierdzenia z teorii grup, ale z teorii liczb. Niewątpliwie jednak metody dowodu były teoriogrupowe.

## 2. Pochodzenie podstawowych terminów

Formalnie rzecz biorąc termin *grupa* wystąpił po raz pierwszy u Galois, jednak raczej w znaczeniu zbioru, aniżeli grupy, bowiem terminu tego używał Galois na oznaczenie warstwy. Galois odnotowuje podstawowe własności grupy  $S_n$  permutacji  $n$  elementów i zapewne dlatego bywa uważany za twórcę pojęcia grupy.

Formalną definicję grupy podał po raz pierwszy Cayley [1854a], [1854b]. W pracy [1854a] Cayley wprowadził zapis grupy za pomocą tabelki działań i podał przykłady grup: grupa macierzy nieosobliwych  $n \times n$  (loc. cit. str. 127), grupa klas binarnych form kwadratowych o współczynnikach całkowitych (loc. cit. str. 126). W pracy [1854b] pojawia się idea pojęcia podgrupy i sposób wyszukiwania podgrup na podstawie tabelki działań. W definicjach podanych przez Cayleya nie występuje jednak ani pojęcie przemienności, ani łączności, jako własności działania grupowego. Jak pisze Miller [1928] (str. 224): *The fact that technical terms for these fundamental laws were introduced so long after these laws were explicitly used throws light on the relation between the use of technical terms and the concepts involved therein.* Jest to opinia nieprawdziwa. Wszystkie z wymienionych tu pojęć pojawiły się w XIX wieku i miały własne nazwy. Niektóre terminy miały po kilka równoległych nazw. Servois [1814] pisał na str. 101 pracy poświęconej superpozycji funkcji: *Quand  $f, \xi, \varphi, \dots$  étant commutatives entre elles,  $k, m, n, \dots$  sont des nombres positifs, on a*

$$f^n f^m z = f^m f^n z \quad (17).$$

Natomiast Hamilton [1853] pisał (loc. cit. str. 114): *distributive character of the multiplication of ordinary algebraic quantities (real or imaginary) extends to [...], so that*

$$Q(Q' + Q'') = QQ' + QQ'', \&c.,$$

*yet the commutative character is lost, and we cannot generally write for the new as for the old imaginaries,  $QQ' = Q'Q$ . ... may be called the associative character of the operation, which may have for its type the formula*

$$Q \cdot Q'Q'' \cdot Q'''Q^{IV} = QQ' \cdot Q''Q'''Q^{IV},$$

*thus we have, generally,  $Q \cdot Q'Q'' = QQ' \cdot Q''$ .*

Terminy: rząd grupy (the group is of the order  $n$ ), element neutralny (unity) wprowadził Cayley [1854a].

Pojęcie przemienności występowało u różnych autorów pod różnymi nazwami. Wspomniany już Hamilton [1854] używał nazwy *commutative*. Netto [1874], Frobenius i Stickelberger [1879] elementy komutujące nazywali przestawialnymi (*a und b einander vertauschbar*). Termin *abelowa* na określenie grupy przemiennej pojawił się u Webera [1882]. Zapewne wystąpił już wcześniej w tym znaczeniu, ale nie potrafimy tego potwierdzić.

Frobenius i Stickelberger [1879] wprowadzili pojęcie bazy grupy, określając tym terminem minimalny (skończony) zbiór generatorów grupy (abelowej). Przez analogię do teorii liczb rząd elementu  $g$  nazywali wykładnikiem, do którego należy  $g$  (*der Exponent zu welchem  $g$  gehört*). Liczbę elementów bazy nazwali rangą grupy. Grupę nazwali elementarną (*Eine Gruppe heisst elementar*), gdy jest rangi 1, tzn. gdy jest cykliczna. Generator grupy, przez analogię do teorii liczb, nazwali elementem pierwotnym. Terminy te w większości nie przyjęły się. Np. Remak [1911] pisał już o grupie przemiennej. Weber [1882] używa już terminu *rząd elementu* (*der Grad des Elements*).

Warstwy grupy skończonej względem jej podgrupy występują już u Galois, Bettiego i innych. Frobenius [1887] cytuje Kroneckera jako twórcę pojęcia kongruencji w grupie:  *$A \equiv B \pmod{G}$ : Elemente  $A$  und  $B$  sind äquivalent oder congruent in Bezug auf eine Gruppe  $G$ .*

Intuicyjne pojęcie grupy wolnej, choć nie nazwane, wprowadził Dyck [1882]: grupa wolna o generatorach  $A_1, \dots, A_m$ , nieskończonego rzędu (*unsere*

*Operationen  $A_i$  keine Perioden besitzen und ausserdem gegenseitig durch keine Relation verbunden sind).*

Pojęcie grupy ilorazowej oraz termin (*the quotient group*) pojawia się u Cayleya [1893] i Younga [1893], a wcześniej u Höldera [1887].

### 3. Aksjomatyczne definicje grupy

Jak już wspomnieliśmy, pierwszą formalną definicję grupy podał Cayley [1854a], str. 40 ([1878a], str. 126 (123); [1878b], str. 51 (324 lub str. 401)). Jego definicja była mało precyzyjna i odnosiła się do grup skończonych. Np. w jego definicji nie postuluje się łączności, chociaż implicite łączność operacji jest później wykorzystywana. W pełni poprawną definicję podał Kronecker [1870], str. 882. Grupą Kronecker nazywa skończony zbiór elementów  $Q', Q'', Q''', \dots$  z działaniem  $f$ , zwanym operacją, takim, że

- 1°  $f(Q', Q'') = f(Q'', Q')$ ,
- 2°  $f(Q', f(Q'', Q''')) = f(f(Q', Q''), Q''')$ .

Jeżeli funkcja  $f$  spełnia warunek:

$$Q'' \neq Q''' \text{ implikuje } f(Q', Q'') \neq f(Q', Q'''),$$

to pisze się  $QQ'$  zamiast  $f(Q, Q')$ . Tyle definicja Kroneckera. Jordan [1867a], [1867b], [1870] definiował grupę jako skończony zbiór permutacji zamknięty względem superpozycji.

Frobenius [1886] definiował grupę jako zbiór z łącznym działaniem  $(A, B) \rightarrow AB$  takim, że  $AB = AC \Rightarrow B = C$  &  $AB = CB \Rightarrow A = C$ .

Natomiast u Webera ([1893], [1899]) znajdujemy następującą definicję:

- A. W zbiorze  $G$  określone jest działanie:  $(a, b) \rightarrow ab$ ,
- B. działanie jest łączne:  $\forall a, b, c \in G, a(bc) = (ab)c$ ,
- C. 1)  $ab = ab' \Rightarrow b = b'$   
2)  $ab = a'b \Rightarrow a = a'$
- D. 1)  $\forall a, c \in G \exists b \in G, ab = c$   
2)  $\forall b, c \in G \exists a \in G, ab = c$ .
- E. W przypadku grup abelowych:  $ab = ba$ .

Weber zauważa, że jeżeli  $G$  jest zbiorem skończonym, to  $A \& B \& C \Rightarrow D$ .

Burnside [1897] definiował grupę jako zbiór funkcji zamknięty względem superpozycji i odwracania funkcji.

Dalszego uproszczenia definicji Webera dokonał Pierpont ([1900–01], str. 47), zastępując warunki C i D odpowiednio przez

- C'. *There exists a unique element 1, called the identity, such that  $a1 = 1a = a$  for every element  $a$ .*
- D'. *For every element  $a$  there exists an element  $a^{-1}$ , called the inverse of  $a$ , such that  $aa^{-1} = a^{-1}a = 1$ .*

Nieco słabszej definicji używał Moore ([1902], [1905]). Postulował on łączność, istnienie jedności lewostronnej, istnienie jedności prawostronnej, oraz istnienie takiej jedności prawostronnej, względem której każdy element posiada lewostronny odwrotny.

Huntington [1905] definiował grupę następująco:

1. wykonalność mnożenia  $(a, b) \rightarrow ab$ .
2. łączność mnożenia:  $a(ab) = (ab)c$  dla dowolnych  $a, b, c$ .
3. istnienie elementu  $i$ , takiego że  $ii = i$ .

4.  $xx = x, yy = y \Rightarrow x = y$  (element  $i$  jest jedyny).
5. jeżeli istnieje jedyne  $i$  takie, że  $ii = i$ , to  $ia = a$  dla każdego  $a$ , lub też  $ai = a$  dla każdego  $a$ .
6. jeżeli istnieje jedyne  $i$  takie, że  $ii = i$ , to dla każdego  $a$  istnieje  $a_r$  takie, że  $aa_r = i$ , lub też istnieje  $a_l$ ,  $a_la = i$ .
7. (dla grup przemiennych)  $ab = ba$  dla każdego  $a, b$ .
- N. (dla grup skończonych) liczba elementów w zbiorze jest równa  $n$  dla pewnego  $n \in \mathbb{N}$ .

Dickson ([1905a], [1905b]) analizując dotychczasowe definicje grupy użył pojęcia półgrupy (Dickson [1905b]) pochodzącego od Séguiera [1904]: półgrupą nazywa zbiór z działaniem łącznym  $(a, b) \rightarrow a \circ b$  spełniającym obustronne prawo skreśleń;

1.  $a \circ x = a \circ x' \Rightarrow x = x'$
2.  $x \circ a = x' \circ a \Rightarrow x = x'$ .

Dickson [1905b] zauważył, że skończona półgrupa jest grupą, ale nie na odwrót.

Slater [1961] zdefiniował grupę  $G$  jako zbiór z dwoma działaniami: binarnym  $(a, b) \rightarrow ab$  i unarnym  $a \rightarrow a'$ , które spełniają jedyny aksjomat:

$$S. \forall a, b, c, d, f \in G, (ab)c = (ad)f \Rightarrow b = d(fc').$$

#### 4. Opis grup małego rzędu

Jak już było powiedziane wcześniej, za początek abstrakcyjnej teorii grup uznać można pracę Cayleya [1854a]. W pracy tej, oprócz konkretnych przykładów grup, podany jest opis (nieizomorficznych) grup rzędu 4 i 6. W pracy [1859] Cayley pisze: *The following is, I believe, a complete enumeration of the groups of 8:*

- I.  $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7$  ( $\alpha^8 = 1$ ).
- II.  $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3$  ( $\alpha^4 = 1, \beta^2 = 1, \alpha\beta = \beta\alpha$ ).
- III.  $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3$  ( $\alpha^4 = 1, \beta^2 = 1, \alpha\beta = \beta\alpha^2$ ).
- IV.  $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3$  ( $\alpha^4 = 1, \beta^2 = \alpha, \alpha\beta = \beta\alpha$ ).
- V.  $1, \alpha, \beta, \beta\alpha, \gamma, \gamma\alpha, \gamma\beta, \gamma\beta\alpha$  ( $\alpha^2 = 1, \beta^2 = 1, \gamma^2 = 1, \alpha\beta = \beta\alpha, \alpha\gamma = \gamma\alpha, \beta\gamma = \gamma\beta$ ).

Cayley dowodzi, że są to grupy parami nieizomorficzne (really distinct groups). Brak dowodu, że to są jedyne grupy rzędu 8. Nietrudno jednak wywnioskować ten fakt z jego pracy.

O trudnościach związanych z rozwojem abstrakcyjnej teorii grup świadczy fakt, że w pracy [1854a] Cayley stwierdził, że istnieją dokładnie dwie grupy rzędu 6, a już w pracy [1878b] (str. 51) (Collected ..., str. 402/403) pisał: *if  $n = 6$  there are three groups, a group  $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$  ( $\alpha^6 = 1$ ), and two groups  $1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2$  ( $\alpha^2 = 1, \beta^3 = 1$ ), viz. in the first of these  $\alpha\beta = \beta\alpha$ , while in the other of them (that mentioned above) we have  $\alpha\beta = \beta\alpha, \alpha\beta^2 = \beta\alpha$* . Wskazuje to na powolny rozwój abstrakcyjnej teorii grup. Kempe [1886] w rozdziale „Groups containing from one to twelve units” (str. 37–43) opisał grupy rzędu 1 do 12. Praca zawiera błąd: Kempe podał niekompletny dowód dla  $n = 8$ . Dla  $n = 12$  podał pięć grup, w tym jedną błędnie, a jedną pominał.

Poprawny opis wszystkich grup rzędu 2–12 zawiera praca Cayleya [1889].

#### 5. Twierdzenie Lagrange’a i twierdzenia Sylowa

Lagrange [1770] sformułował twierdzenie, że rząd podgrupy grupy  $S_n$  permutacji  $n$  elementów dzieli  $n!$ . Zadawałający dowód podał Abbati [1803] w liście z dnia 30 września 1802, adresowanym do Ruffiniego. Udowodnił mianowicie, że grupę  $G$  można rozbić na (równoliczne) podzbiory względem dowolnej podgrupy  $H$  i to

w ten sposób, że zbiory te są parami rozłączne, a jednym z nich jest  $H$ . Dowiódł on także prawdziwości twierdzenia sformułowanego przez Lagrange'a dla cyklicznych podgrup grupy skończonej. Ogólną wersję cytowanego twierdzenia można znaleźć w dziele Galois [1832], jednak brak tam dowodu (Carmichael [1920–21]). Pierwsza ogólna wersja tzw. twierdzenia Lagrange'a udowodniona została w pracy Jordana [1869], a następnie w jego książce [1870]. Terminu *Twierdzenie Lagrange'a* użył już Peterson w swojej książce [1877]. Termin ten stał się popularny dzięki niemieckiemu tłumaczeniu jego książki (1878). Miller [1922] uważa termin za poprawny, gdyż był używany przez kilku ważnych autorów, m.in. przez Millera, Blichfeldta, Dicksona [1916].

Częściowe odwrócenie twierdzenia Lagrange'a udowodnił Cauchy [1844] (tom III, str. 250): jeżeli liczba pierwsza  $p$  dzieli rząd grupy (permutacji)  $G$ , to istnieje podgrupa rzędu  $p$  w  $G$ .

Pierwszymi głębokimi wynikami teorii grup były twierdzenia Sylowa [1872], [1888]:

**I Twierdzenie Sylowa.** Jeżeli  $G$  jest grupą rzędu  $n$ ,  $p$  – liczbą pierwszą, a  $\alpha$  maksymalnym wykładnikiem, z jakim  $p$  dzieli  $n$ , to istnieje podgrupa  $H$  grupy  $G$ , rzędu  $p^\alpha$ .

**II. Twierdzenie Sylowa.** Liczba  $N$  podgrup  $H$  z twierdzenia I daje resztę 1 z dzielenia przez  $p$ . Ponadto podgrupy te są parami sprzężone.

Z twierdzeń tych wyprowadził Sylow ważny wówczas wniosek (Th. IV): jeżeli  $f$  jest wielomianem nieprzywiedlnym stopnia  $p^\alpha$ , a jego grupa Galois ma rząd  $p^\beta$ , to równanie  $f = 0$  jest rozwiązywalne przez pierwiastniki (redukuje się do równań abelowych).

Wkrótce nowe dowody twierdzeń Sylowa podali: Capelli [1878], Netto [1882] i Frobenius [1886].

Capelli zapewne nie znał wyniku Sylowa – nie cytuje pracy Sylowa. Był świeżo po studiach i mógł nie znać nowych prac. Capelli dowodzi, że istnieją  $p$ -grupy Sylowa (tzn. dowodzi I Twierdzenia Sylowa), oraz że są one parami sprzężone (loc. cit. str. 65–66).

Wynik Sylowa początkowo nie był doceniany. Netto zrecenzował jego pracę w "Jahrbuch über die Fortschritte der Mathematik" w ośmiu zaledwie liniach! Natomiast specjalny przypadek podstawowego wyniku Sylowa nie został wymieniony przez Netto we wspomnianej recenzji. Wynik ten został przypisany mu w recenzji F. Meyera (Jahrbuch ... 20 (1894), str. 139; vide: Miller [1920–21]).

## 6. Opis grup specjalnego rzędu

W ślad za rezultatami Cayleya i Kempego pojawiły się ogólniejsze wyniki opisujące grupy specjalnego rzędu. Np. Netto [1882] (str. 133) sklasyfikował grupy rzędu  $p^2$  i  $pq$  ( $p, q$  – liczby pierwsze,  $p \neq q$ ).

Grupy rzędu  $p^3$ ,  $pq^2$ ,  $pqr$  i  $p^4$  ( $p, q, r \in P$  – zbiór liczb pierwszych) opisał Hölder [1893]. Mimo, że cytuje on twierdzenia Sylowa, to jednak robi z nich bardzo mały użytek. Hölder w dowodzie korzysta z twierdzenia, że każda grupa rzędu  $p^\alpha$  ( $\alpha > 3$ ) zawiera podgrupę abelową rzędu  $p^3$ . Miller [1920–21] zwracał się do niego w tej sprawie wskazując, że można użyć twierdzeń Sylowa, aby skrócić dowód o około 30 stron. Hölder wołał jednak opublikować bezpośredni dowód tego faktu dla grup rzędu  $p^4$ . Cytował siebie i Frobeniusa, choć powinien był wykorzystać twierdzenie Sylowa.

Young [1893] opisał niektóre grupy rzędu  $p^\alpha$  ( $p \in P$ ), a Cole [1893] wszystkie grupy rzędu  $pqr$  ( $p, q, r \in P$ ).

Bagnera [1898] i Bender [1928] opisali grupy rzędu  $p^5$  ( $p \in P$ ). Weisner [1925] wyliczył liczbę  $p$ -grup Sylowa w grupie  $S_n$ . Jeżeli  $m = v_p(n!)$  jest maksymalnym

wykładnikiem, z jakim wchodzi  $p$  w rozkładzie  $n!$  na czynniki pierwsze, a

$$n = a_0 + a_1p + \dots + a_kp^k$$

jest rozkładem  $n$  w bazie przy podstawie  $p$ , to liczba  $p$ -grup Sylowa (rzędu  $p^m$ ) w  $S_n$  jest równa

$$\frac{n!}{a_0!a_1!\dots a_k!p^m(p-1)^m}.$$

Jeżeli  $p > 2$ , to tak samo jest dla  $A_n$  (grupy permutacji parzystych).

## 7. Izomorfizm i homomorfizm. Grupa ilorazowa

Idea izomorfizmu grup pochodzi od Cauchy'ego (C. R. Acad. Sci. Paris 21 (1845), str. 1363 & 1401). Cauchy używa terminu *ta sama grupa*. Taką samą intuicją posługiwał się Cayley, nazywając grupy nieizomorficzne *really distinct groups*. Formalną definicję izomorfizmu podał Jordan [1870] (str. 56), definiując  $a : 1$  izomorfizm, tj. homomorfizm, którego jądro ma  $a$  elementów. Capelli [1878] uogólnił to pojęcie, definiując  $a : b$  izomorfizm.

Grupa  $\Gamma$  jest izomorficzna z grupą  $G$  (wg. Capelliego), jeżeli istnieje funkcja  $F : G \xrightarrow{\text{na}} \Gamma$  taka, że  $f(gg') = f(g)f(g')$  dla dowolnej pary elementów  $g, g' \in G$ . Jeżeli  $\text{Ker}(f) \neq 1$ , to jest to *l'isomorfismo meriedrico*; w przeciwnym wypadku *l'isomorfismo oloedrico*. Termin ten był w użyciu przez pewien czas i przetrwał do końca stulecia (Moore [1895]).

Dyck [1882] pisał o grupie wolnej o  $m$  generatorach (loc. cit. str. 5): *Damit werden alle holoedrisch isomorphen Gruppen in eine einzige Gruppe begriffen*.

Definicja Capelliego w niezmienionej postaci znalazła się w książce Burnside'a [1897], w takiej samej postaci w obu jej wydaniach: z 1897 i 1911:

19. *Definition. Let  $G$  and  $G'$  be two groups of equal order. If a correspondence can be established between the operations of  $G$  and  $G'$ , so that to every operation of  $G$  there corresponds a single operation of  $G'$  and to every operation of  $G'$  there corresponds a single operation of  $G$ , while to the product  $AB$  of any two operations of  $G$  there corresponds the product  $A'B'$  of the corresponding operations of  $G'$ , the groups  $G$  and  $G'$  are said to be simply isomorphic* (loc. cit. str. 21/22, I & II Edition).

28. *When a correspondence can be established between the operations of a group  $G$  and the operations of a group  $G'$ , whose order is smaller than the order of  $G$ , such that to each operations  $S$  of  $G$  there corresponds a single operation  $S'$  of  $G'$ , while to the operation  $S_pS_q$  there corresponds the operation  $S'_pS'_q$  the group  $G$  is said to be multiply isomorphic with the group  $G'$*  (loc. cit. str. 35/36, I & II Edition).

Oprócz pojęcia homomorfizmu (multiply isomorphism) i izomorfizmu (simple isomorphism) w użyciu było też pojęcie automorfizmu (isomorphism of the group with itself).

Mathewson [1916] tak pisał o pojęciu izomorfizmu: *The importance of the idea of simple isomorphism between two groups lies in the fact that abstractly two such groups have the same properties; that is, both are simple or both composite, abelian or non-abelian etc.* Uściśla ta wypowiedź krótki komentarz Burnside'a (loc. cit., str. 21/22): *Two simply isomorphic groups are, abstractly considered, identical*.

Miller [1902] zaczął używać terminu *holomorphism* na określenie *multiple isomorphism*. Wprowadza też pojęcie automorfizmu wewnętrznego (cogradient or inner isomorphism) i zewnętrznego (contragradient or outer).

Do roku 1916 opublikowano co najmniej 40 artykułów poświęconych pojęciom izomorfizmu i homomorfizmu (Mathewson [1916]).

Implicite pojęciem warstwy elementu względem podgrupy posługiwał się już Abbati [1803]. Kongruencjami i rozbiciem grupy na warstwy względem dwóch dowolnych podgrup zajmował się Frobenius [1887]. Pojęcie grupy

ilorazowej stworzył Hölder [1887]. Pojęciem tym posługiwali się: Young [1893] i Cayley [1893]. Cayley [1893] używał już terminu grupa ilorazowa (the quotient  $G/H$ ). Twierdzenie o izomorfizmie (tj. związek  $G/\text{Ker } f \simeq H$ , gdzie  $f$  jest homomorfizmem odwzorowującym  $G$  na  $H$ ) pojawiło się u Burnside'a [1897], jednak w mało czytelnej postaci.

## 8. Skończone grupy abelowe i ich opis

Teoria skończonych grup przemennych ma swoje początki u Eulera i Gaussa, w związku z ich teoriolicebowymi badaniami nad resztami potęgowymi.

Gauss [1801] znalazł rozkład grupy klas binarnych form kwadratowych na składniki prymarne, których rzędy są parami względnie pierwsze. Schering [1869] udowodnił, że grupa ta rozkłada się na składniki elementarne, których rzędy dzielą się kolejno. Każdy taki rozkład jest dobrze zdefiniowany.

Frobenius i Stickelberger [1879] zajęli się grupą moltiplikatywną modulo  $M$ , tj. grupą  $G = (Z/MZ)^\times$ . Wszystkie rozpatrywane przez nich grupy są podgrupami  $G$ . Wprowadzili pojęcie bazy skończonej grupy abelowej, jako minimalny zbiór generatorów tej grupy. Moc bazy nazwali rangą grupy (der Rang). Grupę  $G$  nazwali elementarną, gdy jest rangi 1, tzn. gdy jest cykliczna. Terminologia przez nich przyjęta jest pochodzenia teoriolicebowego. Rząd elementu  $A$  grupy  $G$  nazywają wykładnikiem, do którego należy  $A$  (der Exponent zu welchem  $A$  gehört), a generator grupy  $G$  (w przypadku, gdy jest cykliczna) – elementem pierwotnym (ein primitives Element der Gruppe). Wprowadzają pojęcie iloczynu kompleksowego dwóch podgrup  $A$  i  $B$ :

$$AB = \{ab : a \in A \text{ \& } b \in B\}.$$

W pracy (loc. cit.) dowodzą, że każda skończona grupa abelowa jest produktem swoich składników prymarnych i rozkład ten jest jednoznaczny. Mimo wspomnianego ograniczenia do grupy  $G$ , dowody twierdzeń przeprowadzone są w ogólnym przypadku.

Heffter [1898] uprościł i uściślił wynik Frobeniusa i Stickelbergera [1879]. Używa on już terminu *grupa abelowa* (Abelsche oder commutative Gruppe). Zbiór elementów  $g_1, \dots, g_v$  nazywa bazą grupy (abelowej)  $A$ , jeżeli każdy element  $g_j$  jest skończonego rzędu  $n_j$ , a każdy element grupy  $A$  ma jednoznaczne przedstawienie w postaci

$$g_1^{\alpha_1} g_2^{\alpha_2} \dots g_v^{\alpha_v},$$

gdzie  $0 \leq \alpha_j < n_j$  dla  $j = 1, 2, \dots, v$ .

Jeżeli  $n_{k+1}$  dzieli  $n_k$  dla każdego  $k$ , to bazę  $\{g_1, \dots, g_v\}$  nazywa bazą zredukowaną (reducirte Basis), a liczby  $n_1, \dots, n_v$  – niezmiennikami grupy  $A$ . Dowodzi, że każda skończona grupa abelowa posiada bazę zredukowaną.

## 9. Twierdzenie o rozkładzie dla grup skończonych

Początków pojęcia produktu prostego grup należy szukać w pracach poświęconych strukturze skończonych grup abelowych, a więc w szczególnym przypadku grupy klas binarnych form kwadratowych o współczynnikach całkowitych u Gaussa [1801] i Scheringa [1869], a w przypadku grupy moltiplikatywnej pierścienia reszt modulo  $M$  u Frobeniusa i Stickelbergera [1878]; w ogólnym przypadku dla grup abelowych skończonych – u Hefftera [1898].

Pojęcie produktu jest w tym czasie rozpatrywane jako produkt wewnętrzny – Frobenius i Stickelberger mówią o rozkładzie grupy abelowej na produkt.

Produkt prosty w ogólnym przypadku zdefiniował MacLagan-Wedderburn [1909]. Grupa  $H$  jest produktem prostym grupy  $A$  i  $B$ :

$$H = A \times B \Leftrightarrow \forall a \in A \forall b \in B, ab = ba \text{ \& } A \cap B = E.$$

MacLagan-Wedderburn udowodnił w cytowanej pracy, że każda grupa skończona rozkłada się w produkt prosty grup nierozkładalnych. Lukę w dowodzie

Wedderburna usunął dopiero Remak [1924]. Natomiast w swojej dysertacji Remak [1911] zajął się zagadnieniem jednoznaczności w rozkładzie grupy na produkt prosty czynników nierozkładalnych, opisany przez Wedderburna [1909]. Remak nazywa dwie podgrupy  $A, B$  grupy  $H$  centralnie izomorficznymi, jeżeli istnieje taki izomorfizm  $f: A \rightarrow B$ , że  $af(a)^{-1} \in Z(H)$  (centrum  $H$ ) dla każdego  $a \in A$ , tzn. jeżeli  $A/Z(H) = B/Z(H)$ . W szczególności, dla  $A = B = H$  definiuje centralny automorfizm, a następnie dowodzi twierdzenia o jednoznaczności rozkładu: *Hauptsatz: Ist eine Gruppe auf zweierlei Art in direkte unzerlegbare Faktoren zerlegt, so sind die Faktoren den beiden Zerlegung paarweise einander zentral isomorph.*

Remak dowodzi podstawowych własności produktu prostego; wyprowadza też podstawowe twierdzenie skończonych grup abelowych, tzn. twierdzenie Frobeniusa i Stickelbergera (loc. cit. str. 298): *Unter den kommutativen Gruppen sind alle zyklischen Gruppen von Primzahlpotenzordnung und nur diese direkt unzerlegbar. Jede kommutative Gruppe kann also als direktes Produkt von zyklischen Gruppen von Primzahlordnung dargestellt werden.*

Inny, bezpośredni dowód tego twierdzenia podał Remak w pracy [1912]. Twierdzenie Wedderburna o rozkładzie udowodnił też Schmidt [1912]. Dowód ten można znaleźć w książce Speisera [1923]. Miller [1912] zwrócił uwagę na znaczenie grup nierozkładalnych: *among the indivisible groups the simple groups occupy the most important place.*"

## 10. Grupy proste

Pojęcie grupy prostej znane było Galois; zaanonsował on prostotę grupy  $A_5$ . Terminem *permutacja prosta* (permutazione semplice) posługiwał się Ruffini [1799] na określenie grupy cyklicznej.

Pojęcie grupy prostej wprowadził Jordan [1869] (str. 142). Natomiast Tenner [1888] używał terminu *simple group* na określenie grupy cyklicznej rzędu  $p^n$  ( $p$  – liczba pierwsza).

Mathieu [1861] odkrył dwie grupy proste sporadyczne  $M_{11}, M_{12}$ , a następnie (Mathieu [1873]) grupy  $M_{22}, M_{23}$  i  $M_{24}$ . Grupa  $M_{12}$  jest grupą rzędu  $95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$ , która działa pięciokrotnie tranzytywnie na zbiorze 12-elementowym, a  $M_{24}$  jest grupą rzędu  $244\,823\,040 = 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$  też działającą 5-krotnie tranzytywnie na zbiorze 24-elementowym. Stabilizatorami dowolnego elementu są w nich odpowiednio  $M_{11}$  rzędu  $7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$  i  $M_{23}$  rzędu  $10\,200\,960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ , działające 4-krotnie tranzytywnie na zbiorze 11 i 23-elementowym. Stabilizatorem punktu w  $M_{23}$  jest piąta grupa Mathieu,  $M_{22}$  rzędu  $443\,520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ , działająca 3-krotnie tranzytywnie na zbiorze 22-elementowym.

Termin sporadyczna grupa prosta (sporadic simple group) pochodzi od Burnside'a [1897]. Już w XIX wieku wiadano, że grupy Mathieu nie należą do żadnej nieskończonej rodziny grup prostych takich, jak grupy alternujące  $A_n$  ( $n \geq 5$ ), czy też  $\text{PSL}(n, \mathbb{F}_q)$  (z wyjątkiem  $n = 2$  i  $q = 2, 3$ ).

Nieco wcześniej odkryte zostały nowe serie grup prostych. Kronecker i Mathieu odkryli niezależnie, że grupa  $\text{PSL}(2, \mathbb{F}_7)$  rzędu 168 jest prosta. Co prawda praca Mathieu ukazała się wcześniej, bo w 1858, a praca Kroneckera rok później, jednakże Kronecker uzyskał ten wynik kilka miesięcy wcześniej (Miller [1922], str. 326). Brioschi [1859] błędnie stwierdził, że istnieją dwie grupy macierzowe nad  $\mathbb{F}_7$  rzędu 168. Dopiero Jordan udowodnił, że jest tylko jedna taka grupa:  $\text{PSL}(2, \mathbb{F}_7)$ . Jak już wspominaliśmy wcześniej, Galois [1832] wiedział, że  $A_5$  jest grupą prostą i 60 jest najmniejszym złożonym rzędem grupy prostej, jednak jego dowód nie jest znany. Dopiero Hölder [1892] udowodnił to twierdzenie, uogólniając je równocześnie. Wykazał mianowicie, że jeżeli rząd grupy prostej nie przekracza 200 i grupa ta jest nieprzemieniana, to jest ona izomorficzna z  $A_5$  lub z  $\text{PSL}(2, \mathbb{F}_7)$ . Dowód wykorzystuje II Twierdzenie Sylowa. Cole [1892] opisał wszystkie grupy proste rzędu  $n$ ,  $201 \leq n \leq 500$ , a następnie wszystkie grupy

proste rzędu  $\leq 600$  (Cole [1893]). Burnside [1897] zwrócił uwagę (str. 379), że nie jest znana żadna grupa prosta złożonego nieparzystego rzędu. Zagadnienie to badali Miller, Burnside i Frobenius. Rietz [1904] udowodnił, że grupa prosta złożonego i nieparzystego rzędu ma co najmniej 243 elementy.

Ling i Miller [1900] udowodnili, że nie ma nieprzemiennych grup prostych rzędu  $n$  dla  $1092 \leq n \leq 2001$ .

Siceloff [1912] wyznaczył wszystkie grupy proste rzędu  $n$  dla  $2001 \leq n \leq 3640$ , a Cole 1924 – rzędu  $\leq 6232$ .

Zagadnieniem opisu skończonych grup prostych zajmowali się także: Blichfeldt [1910], Dickson [1900a], [1900b], Vavasaur [1899] i inni.

Vavasaur [1899] badał grupę  $GL(3, \mathbb{F}_p)$  i jej podgrupy. Dickson [1900a] badał grupy liniowe nad ciałami skończonymi. W szczególności udowodnił prostotę grup  $PSL(n, \mathbb{F}_q)$  (z wyjątkiem  $n = 2$  i  $q = 2, 3$ ). W pracy [1900b] Dickson badał podgrupy grupy Mathieu.

Schur [1905] zajmował się przemiennymi grupami macierzy. Wymiarem (die Ordnung) grupy macierzowej  $G$  nazwał wymiar przestrzeni liniowej generowanej przez  $G$ . Udowodnił następujące twierdzenie:

Jeżeli  $G$  jest przemienną grupą macierzy nieosobliwych  $n \times n$ , to  $G = C_n \times D$ , gdzie  $C_n = \{aI : a \neq 0\}$ ,  $I$  – macierz jednostkowa, a  $D$  jest grupą torsyjną i  $\dim D = [\frac{1}{4}n^2]$ .

Na koniec warto zauważyć, że następną sporadyczną grupą prostą odkrył Janko w 1965. Świadczy to dobitnie o trudnościach, jakie napotymano w opisie grup prostych.

## 11. Grupy rozwiązalne

Pojęcie grupy rozwiązalnej pochodzi od Jordana [1867a] (także: Oeuvres, vol. I, (14), 93–104). Jordan pisze: *Définitions. – Un groupe de substitutions sera dit résoluble s'il caractérise une équation résoluble par radicaux.* (loc. cit., str. 93). Zatem grupa jest rozwiązalna, gdy jest grupą Galois wielomianu, którego pierwiastki wyrażają się przez pierwiastniki nad ciałem współczynników tego wielomianu, tzn. nad najmniejszym ciałem, które zawiera współczynniki tego wielomianu.

W pracy Jordana [1867b] (Oeuvres, vol. I, (18), 109–157) podana jest charakterystyka grup rozwiązalnych (Th. IV): grupa  $G$  jest rozwiązalna, wtedy i tylko wtedy, gdy istnieje ciąg podgrup

$$G \supseteq G_1 \supseteq G_2 \supseteq \dots, \text{ taki że } G_i < G$$

i  $G'_i$  (komutant  $G_i$ )  $< G_{i+1}$  dla każdego  $i$ .

Tematyką tą zajmował się także Netto [1874], używając jednak nieco odmiennej terminologii. Jeżeli  $a^{-1}ga \in G$  dla każdego  $g \in G$ , to element  $a$  komutuje z grupą  $G$  (so nennen wir  $G$  permutabel zu  $a$ ). Zauważa, że wówczas komutator  $[a, g] = aga^{-1}g^{-1} \in G$ . Natomiast elementy grupy  $G$  komutują z elementami  $H$  z dokładnością do grupy  $K$ , gdy  $[g, h] \in K$  dla każdego  $g \in G$  i  $h \in H$ . Grupa jest *zusammengesetzt*, jeżeli zawiera dzielnik normalny. Netto używa ciągów niezmienniczych, podobnie jak Jordan, a następnie dowodzi, że grupa skończona jest rozwiązalna, wtedy i tylko wtedy, gdy istnieje ciąg kompozycyjny o czynnikach cyklicznych rzędu pierwszego. Formułuje to następująco:

### §9. Galoischen Criterium:

*Lehrsatz 1. Damit eine Gleichung durch Wurzeln lösbar sei, ist es nothwendig und hinreichend, dass ihre Gruppe aus einer Reihe von Substitutionen*

*1, s, t, ..., k, i, h, g abgeleitet werden kann, welche so beschaffen sind, dass*

*1° jede mit der aus den vorhergehenden Substitutionen gebildeten Gruppe permutabel ist;*

*2° dass die niedrigste Potenz jeder neuen Substitution, welche schon in der vorhergehenden Gruppe enthalten ist, von Primzahlgrade sei.*

Hölder [1892] (Lehrsatz IV) dowodzi, że grupa rzędu  $pqr$  ( $p, q, r \in \mathbb{P}$ ) jest rozwiązalna. Zauważa, że prosta grupa tranzytywna permutacji  $m$  elementów, zawierająca cykl długości 3 jest grupą  $A_m$ . Korzystając z udowodnionego faktu, że  $A_5$  i  $\text{PSL}(2, \mathbb{F}_7)$  są jedynymi nieprzemiennymi grupami prostymi rzędu  $\leq 200$ , wyprowadza fakt, że grupa  $G$  rzędu  $n$ ,  $n \leq 200$ ,  $n \neq 60, 120, 168, 180$ , jest rozwiązalna.

Całą serię wyników o grupach rozwiązalnych opublikował Frobenius [1893b], [1895a], [1895b]. W pracy [1893b] dowodzi m.in., że każda grupa rzędu  $p_1 \dots p_n$  ( $p_i$  – różne liczby pierwsze) jest rozwiązalna, a w pracy [1895b] pokazuje, że każda grupa rzędu  $p^\alpha q$  jest rozwiązalna ( $p, q \in \mathbb{P}$ ).

Blichfeldt [1910] dowiódł np. (Cor.4), że każda grupa rzędu  $p^a q^b r$ , gdzie  $p, q, r$  są różnymi liczbami pierwszymi,  $a \leq p^2 - 1$ , jest rozwiązalna. Podstawowym środkiem dowodowym wspomnianych twierdzeń są różne wersje i wzmocnienia twierdzeń Sylowa. Dopiero jednak stworzona przez Frobeniusa, a następnie rozwinięta przez Schura teoria reprezentacji grup pozwoliła na osiągnięcie jakościowo różnych wyników. Np. pozwoliła dowieść, że każda grupa rzędu  $p^a q^b$  ( $p, q \in \mathbb{P}$ ) jest rozwiązalna (tzw.  $p^a q^b$  theorem). Dopiero w latach siedemdziesiątych został znaleziony elementarny dowód tego twierdzenia, nie korzystający z teorii reprezentacji.

Badając skończone grupy rozwiąalne Dickson [1905a] udowodnił następujące twierdzenie:

*5. Theorem. Let  $n = p_1^{\alpha_1} \dots p_v^{\alpha_v}$ , where  $p_1, \dots, p_v$  are distinct primes, and each  $\alpha_j > 0$ . The necessary and sufficient conditions that all existing groups of order  $n$  shall be abelian are:*

- (i) each  $\alpha_j \leq 2$ ;
- (ii) no  $p_j^{\alpha_j} - 1$  is divisible by one of the primes  $p_1, \dots, p_v$ .

Twierdzenie to zostało ponownie odkryte w 1974 (Rodrigues).

Do dziś nie jest znana charakteryzacja tych liczb naturalnych  $n$  takich, że każda grupa rzędu  $n$  jest rozwiązalna.

## 12. Początki teorii reprezentacji grup

Charakterami grup posługiwał się już Gauss, a w pełni świadomie Dirichlet. Natomiast pojęcie reprezentacji grupy, jak też głębokie wyniki tej teorii zawdzięczamy głównie G. Frobeniusowi i I. Schurowi, a także R. Dedekindowi. Nie będziemy tu jednak omawiać historii tych zagadnień, gdyż jest ona szczegółowo opisana (Hawkins [1971], [1972], [1974]). W zagadnienia te wprowadza też Józefiak [1988].

Naszkiecowany w poprzednich rozdziałach zarys historii teorii grup skończonych uzupełnimy kilkoma uwagami o związkach teorii liczb z teorią grup skończonych.

## 13. Zastosowania teorii grup w teorii liczb

Ważne wyniki i pojęcia teorii grup, takie jak generowanie, cykliczność, rozkład na produkt prosty etc. powstały w związku z badaniami w teorii liczb. Frobenius stwierdził krótko w [1893]: *pojęcie grupy, które zostało wprowadzone do matematyki przez Gaussa i Galois, zdobyło w obecnych czasach podstawowe znaczenie dla całej naszej nauki. Duża część teorii liczb jest jedynie teorią grup abelowych.*

Na przełomie XIX i XX wieku ukazało się kilka prac, które wskazywały na korzyści wynikające ze stosowania teorii grup w teorii liczb. Obszerne opracowanie tego tematu podał Zsigmondy [1896]. Miller [1905] zauważa, że jeśli  $d_1, d_2, \dots, d_\lambda$  są rzędami podgrup cyklicznych grupy rzędu  $g$ , to

$$g = \varphi(d_1) + \dots + \varphi(d_\lambda),$$

gdzie  $\varphi$  oznacza funkcję Eulera. Wyprowadza stąd, że dla  $m = m_1 m_2$ ,  $(m_1, m_2) = 1$ ,  $\mathbb{C}_m \simeq \mathbb{C}_{m_1} \times \mathbb{C}_{m_2}$ , co daje mnożliwość funkcji  $\varphi$ , tzn.  $\varphi(m) = \varphi(m_1)\varphi(m_2)$ .

Smosarski [1910] stosuje proste własności grup skończonych do badania grupy mnożliwościowej  $\mathbb{F}_p^\times$  ciała  $\mathbb{F}_p$  reszt modulo  $p$ .

Miller [1913–14] korzystając z faktu, że  $S_{m+1} < \text{Aut}(\mathbb{C}_p^m)$  zauważa, że

$$(p^m - 1)(p^m - p) \dots (p^m - p^{m-1}) \equiv 0 \pmod{(m+1)!}.$$

Wiele ważnych wyników dotyczących własności skończonych grup macierzowych nad ciałem skończonym uzyskał Dickson.

Wyniki te można uważać za wyniki z teorii liczb.

## Bibliografia

Abbati, P.

[1803] *Lettera di Pietro Abbati Modenese al socio Paolo Ruffini da questo presentata il dì 16 dicembre 1802*, Mem. Mat. Fis. Soc. Ital. 10, No 2 (1803), 385–409.

Bagnera, G.

[1898] *La composizione dei Gruppi finiti il cui grado è la quinta potenza di un numero primo*, Annali di Matematica Pura ed Applicata, ser. III, 1 (1898), 137–228.

Bender, H.A.

[1928a] *A determination of groups of order  $p^5$* , Annals of Mathematics 29 (1928), 61–72.

[1928b] *On groups of order  $p^m$ ,  $p$  being an odd prime number, which contain an abelian subgroup of order  $p^{m-1}$* , ibidem 29 (1928), 88–94.

Blichfeldt, H.F.

[1910] *Theorems on simple groups*, Trans. Amer. Math. Soc. 11 (1910), 1–14.

Brioschi, L.

[1859] Annali di Matematica 2 (1859).

[1883] *Sulla risolvente di Lagrange per le equazioni di grado primo risolubili per radicali*, ibidem, ser. II, 11 (1883), 255–283.

Burkhardt, H.

[1894] *Paolo Ruffini e i primordii della teoria dei gruppi*, ibidem ser. II, 22 (1894), 175–212.

Burnside, W.

[1897] *Theory of groups of finite order*, Cambridge: at the University Press, 1897. (pp. 1–388).

[1911] *Second Edition*, 1911. (1–512 pp.)

Capelli, A.

[1878] *Sopra l'isomorfismo dei gruppi di sostituzioni*, Giornale di Matematiche 16 (1878), 32–87.

Carmichael, R.D.

[1920–21] Bull. Amer. Math. Soc. 27 (1920–21), 471–475.

Cauchy, A.L.

[1815] *Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme*, Journal de l'Ecole Polytechnique 17<sup>e</sup> Cahier, T. X, 1815. (Oeuvres de Cauchy, 2<sup>e</sup> s. T. I, 64–90).

[1844] *Le Mémoire sur les Arrangements que l'on peut former avec des lettres données et sur les permutations ou substitutions à l'aide desquelles on passe d'un arrangement à un autre*. Exercices d'analyse et de physique mathématique, Tome III, Paris 1844. (Oeuvres de Cauchy, 2<sup>e</sup> s., T. XIII, 171–282).

Cayley, A.

[1854a] *On the theory of groups, as depending on the symbolic equation  $\Theta^n = 1$* , Philosophical Magazine 7 (1854), 40–47. (The Collected Mathematical Papers of Arthur Cayley, vol. II, No 125, 123–130).

[1854b] *On the theory of groups, as depending on the symbolic equation  $\Theta^n = 1$* . -Second part, Philosophical Magazine 7 (1854), (The Collected ..., vol. II, No 126, 131–132).

[1859] *On the theory of groups as depending on the symbolic equation  $\Theta^n = 1$* . Third part, Philosophical Magazine 18 (1859), 34–37. (The Collected ..., vol. IV, No 243, 88–91).

- [1878a] *On the theory of groups*, Proc. London Math. Soc. 9 (1878), 126–133. (The Collected ..., vol. X, 690, 324–330).
- [1878b] *The theory of groups*, Amer. J. Math. 1 (1878), 50–52. (The Collected ..., vol. X, 694, No. 1, 401–403).
- [1878c] *The theory of groups; graphical representation*, American Journal of Mathematics 1 (1878), 174–176, (The Collected ..., vol. X, 694 (Desiderata and Suggestions) No. 2, 403–405).
- [1889] *On the theory of groups*, Amer. J. Math. 11 (1889), 139–157. (The Collected ..., vol. XII, 887, 639–656).
- [1893] *Note on the so-called quotient  $G/H$  in the theory of groups*, Amer. J. Math. 15 (1893), 387–388. (The Collected ..., vol. XIII, No 934, 336–337).
- Cole, F.N.
- [1892] *Simple groups from order 201 to order 500*, Amer. J. Math. 14 (1892), 378–388.
- [1893] *Simple groups as far as order 660*, Amer. J. Math. 15 (1893), 303–315.
- [1924] *On simple groups of low order*, Bull. Amer. Math. Soc. 30 (1924), 489–492.
- Cole, F.N.; Glover, J.W.
- [1893] *On groups whose orders are products of three prime factors*, Amer. J. Math. 15 (1893), 191–220.
- Dahan, A.
- [1980] *Les travaux de Cauchy sur les substitutions. Étude de son approche du concept de grupe*, Archive History Exact Sci. 23 (1980), No 4, 279–319.
- Dickson, L.E.
- [1900a] *Canonical form of a linear homogeneous substitution in a Galois field*, Amer. J. Math. 22 (1900), 121–137.
- [1900b] *Certain subgroups of the Betti–Mathieu group*, ibidem 22 (1900), 49–54.
- [1901a] *The theory of linear groups in an arbitrary field*, Trans. Amer. Math. Soc. 2 (1901), 363–394.
- [1901b] *Linear Groups (with an Exposition of the Galois Field Theory)*, Teubner, Leipzig, 1901. pp. 1–311.
- [1901c] *A class of groups in an arbitrary realm connected with the configuration of the 27 lines on a cubic surface*, Quaterly J. Pure and Applied Math. 33 (1901), 145–173.
- [1905a] *Definitions of a group and a field by independent postulates*, Trans. Amer. Math. Soc. 6 (1905), 198–204.
- [1905b] *On semi-group and the general isomorphism between infinite groups*, ibidem 6 (1905), 205–208.
- [1905c] *A new system of simple groups*, Math. Annalen 60 (1905), 137–150.
- [1908] *A class of groups in an arbitrary realm connected with the configuration of the 27 lines on a cubic surface II*, Quaterly J. Pure and Applied Math. 39 (1908), 205–209.
- [1919] *History of the theory of numbers*, 1919.
- Dyck, W.
- [1882] *Gruppentheoretische Studien*, Math. Annalen 20 (1882), 1–44.
- Frobenius, G.
- [1886] *Neuer Beweis des Sylowschen Satzes*, J. Reine Anew. Math. 100 (1886), 179–181.
- [1887] *Ueber die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul*, ibidem 101 (1887), 273–299.
- [1893a] *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin 1893*, str. 627.
- [1893b] *Über auflösbare Gruppen*, ibidem XXIII (1893), 337–345.
- [1895a] *Über auflösbare Gruppen II*, ibidem XLVI (1895), 1027–1044.
- [1895b] *Über auflösbare Gruppen*, ibidem X (1895), 163–194. Frobenius, G., Stickelberger, L.
- [1879] *Ueber Gruppen von vertauschbaren Elementen*, J. Reine Angew. Math. 86 (1879), 217–262.
- Gauss, C.F.
- [1801] *Démonstration de quelques théorèmes concernant les périodes des classes des formes binaires du second degré (1801)* (Werke, Bd. II, Göttingen, 1876 266–268).
- Galois, E.
- [1832] *Écrits et mémoires mathématiques*, Édition critique intégrale, par R. Bourgne et J.P. Azra, Gauthier-Villars, Paris 1962.
- Hamilton, W.R.
- [1843] *On a new species of Imaginary Quantities connected with the Theory of Quaternions (1843)*, Proceedings Royal Irish Academy 2 (1844), 424–434.

- [1853] *Preface to 'Lectures on Quaternions'*, Dublin 1853. (The Mathematical Papers of Sir William Rowan Hamilton, vol.III, Algebra; Edited for the Royal Irish Academy by H.Halberstam and R.E.Ingram, Cambridge University Press, 1967, 111–116).
- Hawkins, T.
- [1971] *The origins of the theory of group characters*, Archive History Exact Sci. 7 (1971), 142–170.
- [1972] *Hypercomplex numbers, Lie groups and the creation of group representation theory*, ibidem 8 (1972), 243–287.
- [1974] *New lights on Frobenius creation of the theory of group characters*, ibidem 12 (1974), 217–243.
- Heffter, L.
- [1898] *Über Abelsche Gruppen*, J. Reine Angew. Math. 119 (1898), 261–266.
- Hölder, O.
- [1889] *Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen*, Math. Annalen 34 (1889), 26–56.
- [1892] *Die einfachen Gruppen im ersten und zweiten Hundert der Ordnungszahlen*, ibidem 40 (1892), 55–88.
- [1893] *Die Gruppen der Ordnungen  $p^3, pq^2, p^4$* , ibidem 43 (1893), 301–412.
- [1895a] *Die Gruppen mit quadratfreier Ordnungszahl*, Nachr. Göttingen 1895, 211–229.
- [1895b] *Bildung zusammengesetzter Gruppen*, Math. Annalen 46 (1895), 321–422.
- Huntington, E.V.
- [1903] *Definitions of a field by sets of independent postulates*, Trans. Amer. Math. Soc. 4 (1903), 31–37.
- [1905] *Note on the definitions of abstract groups and of fields by sets of independent postulates*, ibidem 6 (1905), 181–197.
- Jordan, C.
- [1867a] *Mémoire sur la résolution algébrique des équations*, C.R. Acad. Sci. Paris 64 (1867), 269–272; 586–590; 1179–1183. (Oeuvres de C.Jordan, Gauthier-Villars, Paris, 1961, t.I, (14), 93–104).
- [1867b] *Mémoire sur la résolution algébrique des équations*, J. de Math. 12 (1867), 109–157. (Oeuvres, t.I, (18), 109–157).
- [1869] *Commentaire sur Galois*, Math. Annalen 1 (1869), 142–160. (Oeuvres, t.I, (32), 211–230).
- [1870] *Traité des substitutions et des équations algébriques*, Paris 1870.
- [1871] *Mémoire sur la résolution des équations algébriques les unes par les autres*, J. Mathématique, 2 sér., 16 (1871), 1–20.
- Józefiak, T.
- [1988] *Początki teorii reprezentacji grup skończonych. Teoria charakterów Frobeniusa*, Materiały z II Ogólnopolskiej Szkoły Historii Matematyki, Uniwersytet Szczeciński, Szczecin, 1988, 67–83.
- Kempe
- [1886] *Memoir on the theory of mathematical form*, Phil. Trans. 177 (1886), 1–70.
- Kronecker, L.
- [1870] *Auseinandersetzung einiger Eigenschaften der Klassenzahl idealer Complexen Zahlen*, Monatsberichte der Königl. Preuss. Akademie der Wiss. zu Berlin (1870), Berlin 1871, 271–282.
- Lagrange, J.L.
- [1770] *Réflexions sur la résolution algébrique des équations*, Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin, années 1770 et 1771. (Oeuvres, III, 205–421).
- MacLagan-Wedderburn, J.H.
- [1909] *On the direct product in the theory of finite groups*, Annals of Math., 2 ser. 10 (1909).
- Mathewson, L.C.
- [1916] *Theorems on the group of isomorphisms of certain groups*, Amer. J. Math. 38 (1916), 19–44.
- Maschke, H.
- [1896] *The representation of finite groups, especially of the rotation groups of the regular bodies of three- and four-dimensional space, by Cayley's color diagrams*, Amer. J. Math. 18 (1896), 156–194.
- Mathieu, E.
- [1861] *Mémoire sur l'étude des fonctions de plusieurs quantités*, J. Math. Pures Appl., sér. 2, 6 (1861), 241–243.

- [1873] *Sur la fonction cinq fois transitive de 24 quantités*, ibidem 18 (1873), 25–46.
- Miller, G.A.
- [1901a] *O pewnym twierdzeniu elementarnym w teorii grup podstawień*, Prace Matematyczno-Fizyczne 12 (1901), 136–138.
- [1901b] *Holomorphisms and primitive roots*, Bull. Amer. Math. Soc. 7 (1901), 350–354.
- [1902a] *On the group of isomorphisms of an abelian group*, Prace Matematyczno-Fizyczne 13 (1902), 155–158.
- [1902b] *Second report on recent progress in the theory of groups of finite order and A fundamental theorem with respect to transitive substitution groups*, Bull. Amer. Math. Soc. 9 (1902).
- [1904] *On the number of sets of conjugate elements (o liczbie układów podgrup sprzężonych)*, Prace Matematyczno-Fizyczne 15 (1904), 87–90.
- [1905] *Some relations between number theory and group theory*, Amer. J. Math. 27 (1905), 315–322.
- [1911] *On the use of the co-sets of a group*, Trans. Amer. Math. Soc. 12 (1911), 326–334.
- [1912] *Infinite systems of indivisible groups*, ibidem 13 (1912), 419–433.
- [1913–14] *A theorem in number theory proved by isomorphisms of special abelian group*, Tohoku Mathematical Journal 4 (1913–14), 105–106.
- [1914–15] *Remarks on the bearing of the theory of groups*, ibidem 6 (1914–15), 73–78.
- [1920–21] *Group theory reviews in the Jahrbuch über die Fortschritte der Mathematik*, Bull. Amer. Math. Soc. 27 (1920–21), 459–462.
- [1922] *Contradictions in the literature of group theory*, Amer. Math. Monthly 29 (1922), 319–328.
- [1928] *Definitions of abstract groups*, Annals of Math., 2<sup>d</sup> ser. 29 (1928), 223–228.
- Miller, G.A.; Blichfeldt, H.F.; Dickson, L.E.
- [1916] *Finite groups*, 1916.
- Moore, E.H.
- [1895] *The group of holodric transformation into itself of a given group*, Bull. Amer. Math. Soc. 1 (1895), 61–66.
- [1902] *A definition of abstract group*, ibidem 6 (1905), 179–180.
- Miller, G.A.; Ling, G.H.
- [1900] *Proof that there is on simple group whose order lies between 1092 and 2001*, Amer. J. Math. 22 (1900), 13–26.
- Netto, E.
- [1874] *Zur Theorie der zusammengesetzten Gruppen*, J. Reine Angew. Math. 78 (1874), 81–92.
- [1878] *Neuer Beweis eines Fundamnetaltheorems aus der Theorie der Substitutionslehre*, Math. Annalen 13 (1878), 249–250.
- [1882] *Die Substitutionentheorie und ihre Anwendung auf die Algebra*, Leipzig 1882.
- Newcomb, S.
- [1893] *Modern mathematical thought*, Bull. Amer. Math. Soc. 3 (1893).
- Novy, L.
- [1966] *K voprosu o vznikenii sistematičeskich issledovanij po teorii grupp*, Istoriko-matematičeskije issledovanija, vypusk XVII (1966), 31–56.
- [1973] *Origins of modern algebra*, Academia, Prague 1973.
- Petersen, J.
- [1877] *De algebraiske Ligningers Theori*, 1877.
- [1878] *Theorie der algebraischen Gleichungen*, 1878.
- Pierpont, J.
- [1900–01] *Galois' theory of algebraic equations. Part II. Irrational resolvents*, Annals of Math., ser 2., 2 (1900–01).
- Remak, R.
- [1911] *Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren*, J. Reine Angew. Math. 139 (1911), 293–308.
- [1912] *Über die Zerlegung der kommutativen Gruppen in zyklische teilerfremde Faktoren*, ibidem 141 (1912), 245–250.
- [1924] *Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren*, ibidem 153 (1924), 131–140.
- Rietz, H.L.
- [1904] *On primitive groups of odd order*, Amer. J. Math. 26 (1904), 1–30.
- Rodrigues, N.C.
- [1974] *Entiers  $n$  tels que tout groupe d'ordre  $n$  soit abélien*, C. R. Acad. Sci. Paris 278 (1974), A211–A214.

- Ruffini, P.  
[1799] *Teoria generale delle equazioni in cui si dimostra impossibile la soluzione algebrica delle equazioni generali di grado superiore al quattro*, Bologna 1799. Opere matematiche, Ed. E. Bortolotti, vol. I, Palermo (1915).
- Schering, E.  
[1869] *Die Fundametal-Classen der zusammensetzbaren arithmetischen Formen*, Göttinger Abhandlungen 14 (1869), 3–13.
- Schmidt, O.J.  
[1912] *Über die Zerlegung endlicher Gruppen in direkte unzerlegbare Faktoren*, Izvestija Kievskogo Un-ta, 1912, 1–6.  
[1913] *Sur les produits directs*, Bull. Soc. Math. France 41 (1913), 161–164.
- Schur, I.  
[1905] *Zur Theorie der vertauschbaren Matrizen*, J. Reine Angew. Math. 130 (1905), 66–76. Séguier, J.A. De  
[1904] *Théorie des groupes finis. Eléments de la théorie des groupes abstraits*, Paris 1904.
- Servois, F.J.  
[1814] *Essai sur un nouveau mode d'exposition des principes du calcul différentiel*, Annales de Mathématiques Pures et Appliquées 5 (1814), 93–141.
- Siceloff, L.P.  
[1912] *Simple groups from order 2001 to order 3640*, Amer. J. Math. 34 (1912), 361–372.
- Slater, M.  
[1961] *A single postulate for groups*, Amer. Math. Monthly 68 (1961), 346–347.
- Smosarski, W.  
[1910] *Teorya reszt w oświeetleniu teoryi grup*, Sprawozdania z posiedzeń, Rok V (1910), Dodatek do "Wiadomości matematycznych", 105–115.
- Speiser, A.  
[1923] *Theorie der Gruppen endlicher Ordnung*, Berlin 1923.
- Sylow, M.L.  
[1872] *Théorèmes sur les groupes de substitutions*, Math. Annalen 5 (1872), 584–594.  
[1888] *Sur les groupes transitifs dont le degré est le carré, d'un nombre premier*, Acta Mathematica 11 (1888), 201–256.
- Tanner, H.W.  
[1888] Proc. London Math. Soc. 20 (1888).
- Vavasseur, M.R. Le  
[1899] *Étude du groupe des isomorphismes de  $(G)^3$* , Annales Scientifiques de l'École Normale Supérieure, sér. III, 16 (1899), 377–394.
- Vleck, E.B. van  
[1916] *Current tendencies of mathematical research*, Bull. Amer. Math. Soc. 23 (1916), 1–13.
- Weber, H.  
[1882] *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Math. Annalen 20 (1882), 301–329.  
[1893] *Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie*, Math. Annalen 43 (1893), 521–549.
- Weisner, L.  
[1925] *On the Sylow subgroups of the symmetric and alternating groups*, Amer. J. Math. 47 (1925), 121–124.
- Więśław, W.  
[1995] *Drogi i manowce początków algebry*, Matematyka, Społeczeństwo, Nauczanie Numer 15 (VII 1995), 16–26.
- Wussing, H.  
[1966] *O genezisie abstraknogo ponjatja grupy*, Istoriko-matematičeskije issledovanija, vypusk XVII (1966), 11–30.  
[1969] *Die Genesis des abstrakten Gruppenbegriffes*, VEB Verlag, Berlin 1969.
- Young, J.W.A.  
[1893] *On the determination of groups whose order is a power of a prime*, Amer. J. Math. 15 (1893), No 2, 124–178.
- Zsigmondy, K.  
[1896] *Beiträge zur Theorie Abel'scher Gruppen und ihrer Anwendung auf die Zahlentheorie*, Monatshefte für Mathematik und Physik 7 (1896), 185–289.