

Otto H. Kegel's Beloved Contributions to Sylow Theory

In memory of my adored masterly teacher

Dipl.-Math. Felix F. Flemisch, M.Sc., Bacc.Math.

Mitterweg 4e, 82211 Herrsching a. Ammersee, Bavaria, Germany

Abstract

Let p be a prime. A **p -group** is a group all of whose elements have order a power of p and a **p' -group** is a group all of whose elements have order prime to p , that is, not containing any element of order p . A p -group is finite if and only if its order is a power of p . Every group theorist knows what are well-known as **the three Sylow theorems**: Any finite group G has ① subgroups of order $|G|_p$, where $|G|_p$ is the highest power of p dividing the order $|G|$ of G , which are called **Sylow p -subgroups** and are not only maximal with respect to (w.r.t.) order but also w.r.t. inclusion, whence ② every p -subgroup of G is contained in at least one Sylow p -subgroup, and ③ all the Sylow p -subgroups are **conjugate**, that is, if S_1 and S_2 are Sylow p -subgroups of G , then there exists an element x of G such that $x^{-1}S_1x = S_2$.¹ The set of all Sylow p -subgroups of a group G is denoted by $\text{Syl}_p G$. The theorems and the maximal p -subgroups are named after **Ludvig Sylow**, the great Norwegian mathematician who discovered them and published them in **December 1872** (see [26.] and https://en.wikipedia.org/wiki/Peter_Ludvig_Sylow). A **Sylow p -subgroup** of any group is a p -subgroup, which is maximal w.r.t. inclusion. Every p -subgroup is contained in at least one Sylow p -subgroup. A group **satisfies the Sylow Theorem for the Prime p** or **the Sylow p -Theorem**, if all of its Sylow p -subgroups are conjugate, and it **satisfies the Strong Sylow Theorem for the Prime p** , if each of its subgroups satisfies the Sylow p -Theorem. A **locally finite group** is a group all of whose finitely generated subgroups are finite. **Sylow Theory of Locally Finite Groups** studies when they satisfy the Sylow p -Theorem and when even the Strong Sylow p -Theorem and determines the structure of those groups. A central concept to that end is the **p -uniqueness subgroup** of a locally finite group, which is a finite p -subgroup being contained in a unique Sylow p -subgroup.

Otto H. Kegel has since the swinging sixties of last century again and again showed interest in Sylow Theory and very especially in how to extend it from finite groups to locally finite groups. He summarised findings **up to 1973** by him and by others in the book [22.], which became a standard book on locally finite groups. When the book was

¹ When G is a finite group, P a p -subgroup of G and $S \in \text{Syl}_p G$, then the operation of P by conjugation on $C(G, S) := \{S^x \mid x \in G\}$ has at least one fixed point, that is $(\exists x \in G)(P^x \subseteq S)$, and for $P \in \text{Syl}_p G$ exactly one, which means ④ $|\text{Syl}_p G| = |G : \underline{N}_G S| = |C(G, S)| \equiv 1 \pmod{p}$; hence G satisfies the Strong Sylow Theorem for the Prime p , that means, every subgroup U of G conjugates **transitively** on $\text{Syl}_p U$, and therefore we have the **Fratini argument** for G (and p), that is, if N is a normal subgroup of G and $P \in \text{Syl}_p N$, then $\underline{N}_G P$ covers G/N , that is, $G = N \cdot \underline{N}_G P$. ■

*Corresponding author

Felix F. Flemisch, Mitterweg 4e, 82211 Herrsching a. Ammersee, Bavaria, Germany.
ORCID: <https://orcid.org/0000-0003-1612-8810> 

Received: January 2, 2026; **Revised:** 12 January, 2026, and 23 February 2026;

Accepted: March 14, 2026; **Published:** March 21, 2026

in press, he developed the new paper [11.] on Sylow Theory of Locally Finite Groups and presented it in the lectures during **11 December 1973**. This paper has **two open questions** until today. 13½ years later he presented on **8 June 1987** in four lectures [12.] a summary of results **up to 1987** about Sylow Theory of Locally Finite Groups and extended them beautifully from locally finite and p -soluble groups for $p \neq 2$, according to results by **Brian Hartley** and **Andrew Rae**, to locally finite groups in general for $p \geq 5$. This paper has **ten open questions** until today. The paper at hand presents **Otto H. Kegel's** achievements of and merits for Sylow Theory of Locally Finite Groups and communicates **that it was a "Herzensangelegenheit" (a matter close to one's heart) for him. Otto H. Kegel** ❤️ passed away on his birthday **20 July 2025** at the age of 91. Being in deepest mourning, I miss him dreadfully and will always honour his memory 🌸.

Keywords • p -group • p' -group • Sylow theorems • Sylow p -subgroup • (Strong) Sylow Theorem for the Prime p or (Strong) Sylow p -Theorem • locally finite group • p -uniqueness subgroup • finite p -subgroup singular in a locally finite group • Sylow-separated (ascending) sequence of p -subgroups with its associated sequence of Sylow p -subgroups • (smooth simple straight) split sequence of finite p -perfect subgroups with its associated ascending sequence of subgroups • (proper) Sylow p -intersection • p -blank of G in H

Mathematics Subject Classification (MSC2020)

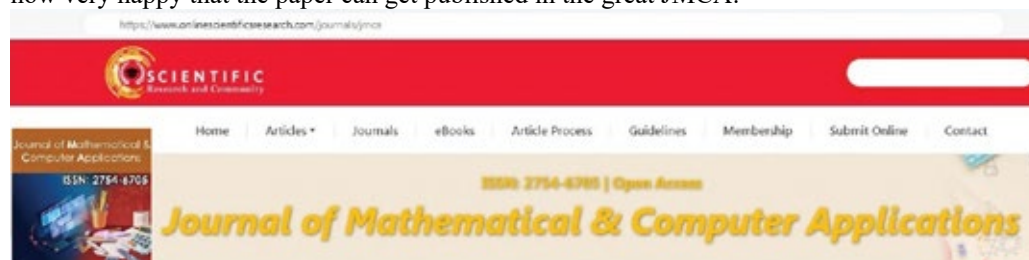
Primary 20D20; Secondary 20F50 • 20D15 • 20D06 • 20D10 • 20E25 • 20D05

Research Funding

This research did not receive any funding.

Note

I tried unsuccessfully to publish this paper inchmeal in the journals **Mathematische Zeitschrift**, **Archiv der Mathematik** and **European Journal of Mathematics**. A common feature of all the three rejects was that they did not state any reason let alone substantial review comments. I am now very happy that the paper can get published in the great JMCA:



1 Introduction

I present references to articles on **Sylow Theory of Locally Finite Groups** by **Otto H. Kegel** and by myself. **First** I present and summarise the twelve *beloved* contributions by **Otto H. Kegel**. **Secondly** I present and summarise the ten *enthusiastic* contributions by myself, which add thorough comments to **Otto H. Kegel's** admirable contributions regarding wide generalisations, solve two of his open issues and state twelve still open issues most of which, however, I solved already in yet unpublished work. **Thirdly** I draw some conclusions from **Otto H. Kegel's** contributions and my contributions thereby suggesting very fascinating topics for future research based upon the twelve to this day open issues of [11.] and [12.]. I almost close with **Acknowledgements** and **30 References**. "Almost" because I add six distinguished historical articles about Sylow Theory: **Sylow's** Norwegian paper of 1867 [25.] with a translation into English, **Sylow's** famous paper of 1872 [26.], **Waterhouse's** paper on the Early Proofs of Sylow's Theorem [27.], and **Scharlau's** German paper on the Discovery of Sylow's Theorems [24.] with an appreciation of his performance and a translation into English.

2 Otto H. Kegel's Beloved Contributions

Otto H. Kegel wrote together with **Bertram A.F. Wehrfritz** a beautiful book about Locally Finite Groups and published it **1973** [22.]. It includes **up to date** results and many references about Sylow Theory by him and by others thereby bridging the gap between **1872** [25.] and **1973**. However, it forgoes **Kegel's** earlier more than 30 ageless contributions in the **1960s** and **1970s**. Those which are related to or are significantly important for Sylow subgroups I cite as well.

2.1 Early Contributions

I cite and summarise the nine of them which are related to or are significantly important for Sylow Theory.

2.1.1 Caractérisation des sous-groupes accessibles d'un groupe fini [13.]

Otto H. Kegel presented this out of the ordinary paper on **29 March 1960** in French in the Séminaire Albert Châtelet et Paul Dubreil as the Talk no. 18. Let G be a group. A subgroup U of G is called **accessible** if it appears in a composition series of G , that is, if there exists a finite series $\{N_i\}_{1 \leq i \leq m}$ of subgroups of G such that $N_1 = U$, N_i is a normal subgroup of N_{i+1} , and $N_m = G$. The subgroup U is a **(D)-subgroup** of the finite group G if for every prime divisor p of $|G|$ and Sylow p -subgroup S of G the intersection $S \cap U$ is a Sylow p -subgroup of U . Every (D)-subgroup is accessible, and when a subgroup U of the finite group G is accessible then for every prime p and Sylow p -subgroup S of G the intersection $U \cap S$ is a Sylow p -subgroup of U . **Kegel** proves further conditions when a subgroup is accessible.

2.1.2 Sylow-Gruppen und Subnormalteiler endlicher Gruppen [14.]

In this paper of **December 1962** **Otto H. Kegel** studies the **π -quasinormal subgroups** U of a finite group G for a set π of prime numbers, which are subgroups where U for each $p \in \pi$ is permutable with each Sylow p -subgroup of G , and **π -subnormal subgroups** U of a finite group G , which are subgroups where for each $p \in \pi$ and every Sylow p -subgroup P of G the group $U \cap P$ is a Sylow p -subgroup of U . Subnormal and π -quasinormal subgroups are π -subnormal. With additional premises **Kegel** proves that the subgroup U is subnormal, if U is π -subnormal for the set π of all prime numbers.

2.1.3 Eine Charakterisierung der Sylowgruppen endlicher Gruppen [15.]

Otto H. Kegel submitted this very sublime paper on **10 June 1965**. He considers a class $\mathcal{K}$ of finite groups which contains with G also every epimorphic image of each subgroup of G , and calls the function f , which assigns to every $G \in \mathcal{K}$ the set $f(G)$ of subgroups of G , a **Sylowfunction** on $\mathcal{K}$ if it has four specified properties, one being that $f(G)$ is a class of conjugated subgroups for every $G \in \mathcal{K}$. An example is for the prime p and the class $\mathcal{E}$ of all finite groups the function p which assigns to every finite group G the set $p(G)$ of all its Sylow p -subgroups. **Kegel** then proves SATZ 1 with a ZUSATZ, SATZ 2 and SATZ 3 for Sylowfunctions: see Zbl 0144.01503.

2.1.4 Über einfache, lokal endliche Gruppen [16.]

This paper **Otto H. Kegel** submitted on **12 March 1966** to **Mathematische Zeitschrift**. It contains his famous “**approximation principle**” for countable simple locally finite groups (see **2.1.5** and **2.2** and **Page 4** of [10.] and the proof in **4.5 Lemma** of [22.] with subsequent **Remark**). For a full summary I refer to the excellent Zbl-review by **Rüdiger Göbel**: see Zbl 0147.27002.

2.1.5 Locally finite versus finite simple groups [17.]

This paper of **May 1968** is a lecture **Otto H. Kegel** gave at a regional conference on finite groups (a symposium on the Theory of Finite Groups) at Harvard University, which had Part I (19 lectures), Part II (seven lectures) and Part III (ten lectures, n° 8 being **Kegel**'s lecture). Based on his famous “**approximation principle**” “**A countably infinite locally finite simple group G has a strictly ascending sequence $\{R_i\}_{i \in \mathbb{N}}$ of finite subgroups of G with $G = \bigcup \{R_i \mid i \in \mathbb{N}\}$ such that for each natural number i there exists a maximal normal subgroup M_{i+1} of R_{i+1} satisfying $M_{i+1} \cap R_i = \langle 1 \rangle$.” whence G is a limit of the approximating sequence $\{R_i / M_i\}_{i \in \mathbb{N}}$ of finite simple groups ordered by “**involvement**” (see **2.1.4** and **2.2**), he reports: • If each of the finite simple groups $\{R_i / M_i\}_{i \in \mathbb{N}}$ is “known”, then either G contains an infinite elementary abelian p -subgroup for every prime p or there is a field F and a natural number n such that G is isomorphic to a subgroup of $GL(n, F)$. • The existence of a non-linear simple locally finite group which for (at least) one prime p has only finite elementary abelian p -subgroups (possibly $\langle 1 \rangle$) entails the existence of a family of finite subgroups $\{R_i\}_{i \in \mathbb{N}}$ such that each of the simple groups $\{R_i / M_i\}_{i \in \mathbb{N}}$ is “new”. Discussing (simple) locally finite groups in this spirit, many questions about finite groups come up.**

2.1.6 Strong finiteness conditions in locally finite groups [18.]

This paper was submitted by **Otto H. Kegel** on **27 March 1970** to **Mathematische Zeitschrift**. **Kegel** himself wrote the following summary: “Eine alte Frage in der Gruppentheorie ist es, ob die Gruppen, die der Minimalbedingung genügen, einen abelschen Normalteiler von endlichem Index haben. Für lokal endliche Gruppen wird diese Frage hier positiv entschieden. [Dieses Resultat wird auch in V. P. Šunkov, Algebra i Logika, Vol. 9, No. 2, 220-248, **March-April 1970** gegeben (see V. P. Shunkov, On the minimality property for locally finite groups, Algebra and Logic, Volume 9, 137–151, **March 1970**, <https://link.springer.com/article/10.1007/BF02218982>)] Wir erhalten dieses Resultat als Spezialfall eines allgemeineren Satzes, der sagt, daß die lokal endliche Gruppe G , in der alle Primuntergruppen der Minimalbedingung genügen, genau dann eine abelsche Untergruppe von endlichem Index hat, wenn die Menge der Zentralisatoren in G als halbgeordnete Menge der Minimalbedingung genügt.” (see Zbl 0195.03804).

2.1.7 Locally finite simple groups [19.]

Otto H. Kegel presented this paper to the Second International Conference on the Theory of Groups (with about 130 participants) held in **August 1973** as the Informal Session C in the Department of Mathematics of the Institute of Advanced Studies of the Australian National University in Canberra. **Kegel** himself wrote the following summary: "In dieser Note wird beschrieben, wie der Fortschritt im Studium "kleiner" lokal endlicher Gruppen von tiefen Klassifikationssätzen in der Theorie endlicher einfacher Gruppen abhängt und wie diese Sätze für unendliche Gruppen nutzbar gemacht werden können. Einige naheliegende Fragen werden formuliert und motiviert." (see Zbl 0292.20028).

2.1.8 Reinhold Baer (1902-1979). Obituary. [20.]

Otto H. Kegel wrote this detailed while very knowledgeable **Obituary** for his adored teacher **Reinhold Baer**, who passed away on **22 October 1979**, and published it in **June 1980**. I was present in the lecture where **Kegel** communicated almost tearfully this sad at heart event.

2.1.9 The structure of locally finite groups with $\min\text{-}p$ [21.]

Otto H. Kegel published this paper in **December 1982**. He discusses the effect of the classification of finite simple groups on locally finite groups with $\min\text{-}p$. Using this classification he shows how to obtain a very strong structural result for locally finite groups satisfying $\min\text{-}p$ for some prime p . Such a group has a unique maximal normal locally p -soluble subgroup $\mathbf{S}_p(G)$. Let $H := G/\mathbf{S}_p(G)$. If $H \neq \langle 1 \rangle$, then H has minimal normal subgroups. Their join $\mathbf{soc}(H)$ is a direct product of finitely many simple groups, and $H/\mathbf{soc}(H)$ has an abelian normal subgroup of finite rank and finite index. The simple groups referred to, if infinite, are actually known to be groups of Lie type over locally finite fields, and this fact plays a central part in the proof. As a direct consequence, if the locally finite group G satisfies $\min\text{-}p$, then the factor group $G/\mathbf{O}_p(G)$ is countable, since a linear simple locally finite group must be countable.

2.2 "Locally Finite Groups", co-authored with Bertram A.F. Wehrfritz [22.]

The book mentions the conjugacy part of the Sylow theorems in the **Introduction** and gives a very profound account of the Sylow Theory in **Section D** "Maximal p -subgroups" of **Chapter 1** with its **Appendix** "Conventional Sylow theory and related ideas" and in **Section A** "A Sylow theory for locally finite groups with $\min\text{-}p$ [that is, each of their p -subgroups satisfies $\min$]" of **Chapter 3**. Instead of studying Sylow p -subgroups and $\mathbf{Syl}_p G$, it studies **maximal p -subgroups** and $\mathbf{Max}_p G$ because of the general absence of a satisfactory theory for $\mathbf{Max}_p G$ along the lines of the theory of Sylow p -subgroups of finite groups. However, this is not true for locally finite groups (see [23.]).

First it collects basic properties of maximal p -subgroups: • The p -subgroup P of the locally finite group G is a maximal p -subgroup if there is a local system Σ of G [a set of subgroups whose union is G and where any two of it lie in a third of it] consisting of finite subgroups such that P reduces into Σ [i.e., for every subgroup $S \in \Sigma$ the intersection $S \cap P$ is a Sylow p -subgroup of the finite group S]. If the local system Σ of the group G consists of finite subgroups only and is linearly ordered by inclusion (whence G is countable), then there is a p -subgroup of G which reduces into Σ . • For a local system Σ of the group G consisting of finite subgroups only denote by $\mathbf{Max}_p \Sigma$ the set of those p -subgroups of G reducing into Σ . • If the local system Σ of the group G consists of finite subgroups only and is linearly ordered by inclusion, then the following three properties of the set $\mathbf{Max}_p \Sigma$ are equivalent: **a** the elements of $\mathbf{Max}_p \Sigma$ are conjugate in G ; **b** $|\mathbf{Max}_p \Sigma| < 2^{\aleph_0}$; **c** the set $\mathbf{Max}_p \Sigma$ is finite. If for some prime p , every countable subgroup of the locally finite group G contains less than $2^{\aleph_0}$ maximal p -subgroups, then in every factor of G the maximal p -subgroups of G are all conjugate. If p is a prime and G is a countable locally finite group, then the maximal p -subgroups of G are all conjugate if and only if $|\mathbf{Max}_p \Sigma| < 2^{\aleph_0}$. • If the locally finite group G contains a finite maximal p -subgroup P , then the maximal p -subgroups of G are all conjugate to P (see also Page 8 f. of [10.]).

Secondly it summarises heroically with almost fifty (!) references the research work **up to 1973** with the sort of result "in such-and-such a group the maximal p -subgroups are all conjugate". For this particularly astonishing overview I refer to Page 26, Page 27 and Page 28 of [22.].

Thirdly it studies **Sylow Theory for locally finite groups with $\min\text{-}p$** . For a prime p and any group, it calls a subgroup P of G a **Sylow p -subgroup of G** if P is a maximal p -subgroup of G and contains an isomorphic copy of every p -subgroup of G . The set of all Sylow p -subgroups of G is denoted by $\mathbf{Syl}_p G$. It proves: • The locally finite group G satisfies $\min\text{-}p$ if and only if some maximal elementary abelian p -subgroup of G is finite. • If G is a locally finite group satisfying $\min\text{-}p$, then G contains Sylow p -subgroups and every finite p -subgroup of G is contained in a Sylow p -subgroup of G . • Let G be a locally finite group satisfying $\min\text{-}p$. If P is a p -subgroup of G and if Q is a Sylow p -subgroup of G then the following properties are equivalent: **a** P is a Sylow p -subgroup of G ; **b** P contains an isomorphic copy of every finite p -subgroup of G ; **c** P and Q are isomorphic p -subgroups of G . • If G is a locally finite group satisfying $\min\text{-}p$, then the p -subgroup P of G is a Sylow p -subgroup of G if and only if P contains a conjugate of every finite p -subgroup of G .

Fourthly it presents in **Chapter 4** “Locally finite simple groups” results related to the study of Sylow subgroups in simple locally finite groups which were previously obtained in **2.1 Early Contributions:**

- An infinite group G is simple if and only if it has a local system consisting of countably infinite simple subgroups of G .
- A countably infinite locally finite simple group G has a strictly ascending sequence $\{R_i\}_{i \in \mathbb{N}}$ of finite subgroups of G with $G = \bigcup \{R_i \mid i \in \mathbb{N}\}$ such that for each natural number i there exists a maximal normal subgroup M_{i+1} of R_{i+1} satisfying $M_{i+1} \cap R_i = \langle 1 \rangle$. Later the terms **Kegel cover** (R_i, M_i) with **Kegel kernels** M_i and **Kegel simple sections** R_i / M_i were introduced.

2.3 Chain conditions and Sylow's theorem in locally finite groups [11.]

Having just published a such detailed account of Sylow Theory **up to 1973** (see 2.2), **Otto H. Kegel** presented on **11 December 1973** and published **1976** this new paper which comes with the new and really excogitated concept of “**Sylow-separated (ascending) sequence of p -subgroups with its associated sequence of Sylow p -subgroups**” and with a new depiction of the concept of “**Sylow p -intersection**”. I described, summarised, annotated and enlarged the paper on Page 7 to Page 10 of [10.] including the MR-review and the Zbl-review on Page 21. This paper has **two open issues**.

2.4 Four lectures on Sylow theory in locally finite groups [12.]

Practically no work on Sylow Theory was done **since 1973** until **Summer was approaching in 1978** when **Otto H. Kegel** proposed for my **Diplomarbeit** – I had just passed the exam for the minor Diplom subject with a “sehr gut” – to try to extend **Brian Hartley's** tremendous result on Sylow Theory of locally p -soluble locally finite groups for $p \neq 2$ to locally finite groups in general, in particular to simple groups. And then a literally yearslong collaboration between the two of us began until I could publish the **Diplomarbeit** on **8 October 1984** which, however, was rather incomplete since I got hopelessly lost in the classification of finite simple groups. Most of my further drafts were completed by **Kegel** himself, who contributed in any case the preponderant part of great ideas, and presented on **9 June 1987**. I described, summarised, annotated and enlarged his paper on Page 2 to Page 6 and Page 13 of [10.] including the MR-review and the Zbl-review on Page 17. This paper has **ten open issues**. **During a large number of personal sessions I was first surprised by and then in admiration of Kegel's very great interest in my (!) research subject which showed me that it was a real and sincere “Herzensangelegenheit” (matter close to one's heart) for him.** This is well-documented in [12.], [9.] and [10.].

3 Felix F. Flemisch's Enthusiastic Contributions

Being retired since **October 2016**, I extra early rediscovered my loving to work for **Mathematics** and particularly for **Group Theory** and resumed the topics of my **Diplomarbeit** of **1984** and of **Otto H. Kegel's** fantastic paper [12.]. This resulted in *enthusiastic* contributions **since 2021** adding thorough comments to **Kegel's** contributions. I summarise them in the following. They end with **twelve open issues** suggesting **fascinating topics for future research**.

3.1 Trilogy about Sylow Theory in Locally Finite Groups [1.]

The books are based on my Diplomarbeit (see 2.4) and continue my paper “Characterising Locally Finite Groups Satisfying the Strong Sylow Theorem for the Prime p ” which appeared in Adv. Group Theory Appl. 13 (**June 2022**) on pp. 13-39 (see [5.]). Since they contain a lot of material which cannot be published in a mathematical journal, they were published as Books on Demand (BoD) (see 3.2 and 3.3). In the following I describe the mathematical subject matter. Regarding the non-mathematical contents, including very beloved dedications to famous or by me beloved persons, see the contained four careful recensions: **Part 1**, Page v; **Part 2**, Page i; **Part 3**, Page i and Page 42.

3.1.1 Part 1 [1.1]

Part 1 “Characterising Locally Finite Groups Satisfying the Strong Sylow Theorem for the Prime p ” of the Trilogy [1.1] is based on the BoD-Book “Characterising locally finite groups satisfying the strong Sylow Theorem for the prime p – Revised edition” (see under ISBN 978-3-7562-3416-5) which in turn has been based on my rather pioneering research paper in Volume 13 of Advances in Group Theory and Applications (AGTA) (see <https://www.advgrouptheory.com/journal/Volumes/13/Flemisch.pdf> and the good Summary in Zbl 1496.20065). The First edition of **Part 1** removes the highlights in **light green** of the Revised edition and adds the albeit very considerably improved Pages from i to vi and Pages from 27 to 34 to the AGTA-paper. In addition, **Part 1** adds the ten new Pages from 35 to 44 to the Revised edition and therefore had to renumber the Pages from xv to xviii into the Pages from 45 to 48. It includes the second paper [12.] of **Otto H. Kegel** about Sylow theory in locally finite groups (see MR981832 and Zbl 0659.20024) as **Appendix 1** and his first paper [11.] on the beautiful subject (see MR414714 and Zbl 0328.20029) as **Appendix 2**. Finally, it calls to mind **Kegel's** fine contribution to the conference **Ischia Group Theory 2016**.

Really most importantly, **Part 1** introduces the fundamental concepts of the (First) Trilogy about Sylow Theory in Locally Finite Groups: locally finite group satisfying the Strong Sylow Theorem for the prime p (or the Strong Sylow p -Theorem); singular (Sylow) p -subgroup; (very) good Sylow p -subgroup; p -uniqueness subgroup; minimal (w.r.t. order) p -unique subgroup; (numerical) Sylow p -invariant a_p ; P -invariant Sylow p -subgroup; P -isomorphic P -orbit.

3.1.2 Part 1 – Second edition [1.2]

The **Second edition of Part 1** introduces happily a uniform page numbering, adds page numbers to the appendices, improves Pages iv and v, Page 22, Pages 25 to 34 and Pages 39, 45, 49, 50, 75, 76, 105 and 106, adds Pages 109 to 112, and adds a two-page **Table of Contents of the Trilogy. Part 1** has vi + 48 + 27 + 31 + 8 = 120 pages and includes 15 references according to the AGTA- paper followed by • a two-page Postscript about Kegel's Theorem/Conjecture on simple locally finite groups with the Strong Sylow Theorem for the prime p (see **Part 2**) and about the (First) Trilogy, by • the section "About the author", by • a Note on Kegel's Theorem/Conjecture, by • a fine section about "Sylow p -intersections and p -uniqueness subgroups", by • the rather illuminating section "Comparison of Kegel's two papers on Sylow theory in locally finite groups", by • the section "Five personal Notes about Mathematics", and finally followed by • the very insight gaining section "Augustin-Louis Cauchy's and Évariste Galois' contributions to Sylow theory in finite groups" describing and summarising a very pioneering follow-up paper. It also adds the section "Mathematical Reviews (MR) (MathSciNet) and zbMATH Open (Zentralblatt MATH)" for the AGTA-paper.

3.1.3 Part 2 [1.3]

Part 2 "About the Strong Sylow Theorem for the Prime p in Simple Locally Finite Groups" of the Trilogy [1.3] is based on **Part 1**. It first gives a profound overview of the structure of simple groups, and in particular of the simple locally finite groups, and reduces their Sylow theory for the prime p to an old (1987) conjecture of **Otto H. Kegel**, contained in his second paper [4.], about the rank- unbounded ones of the known 19 families of finite simple groups: "Let the p -subgroup P be a p -uniqueness subgroup in the finite simple group S which belongs to one of the seven rank- unbounded families. Then the rank of S is bounded in terms of P ."

Part 2 then introduces a new scheme to describe these 19 families, **the family** $\mathcal{T} := \{ \text{abelian}_p, \mathbb{A}^n, A = \text{PSL}_n, B = \text{P}\Omega_{\text{odd } n}, C = \text{PSp}_n, D = \text{P}\Omega_{\text{even } n}^+, {}^2A = \text{PSU}_n, {}^2D = \text{P}\Omega_{\text{even } n}^-, E_6, E_7, E_8, F_4, G_2, {}^2B_2, {}^3D_4, {}^2E_6, {}^2F_4, {}^2G_2, \text{sporadic } \star \}$ **of types** using well-known symbols, defines the rank of each type, and emphasises the rôle of **Kegel covers**. This introductory part presents a unified picture of well-known results with proofs only by reference which is the reason why the title of **Part 2** starts with "About".

Subsequently **Part 2** applies rather **new ideas** to prove the conjecture for the Alternating Groups. A considerably thorough abstract of this quite pioneering approach is presented on **Page ii**.

Thereupon **Part 2** remembers the central rôle played by **Kegel covers** and **$\star$ -sequences**. Finally, it presents a plan how to prove and even how to optimise the conjecture step-by-step or peu à peu by suggesting **a way 1)** and **a way 2)** which leads to further tough conjectures thereby happily unifying *Sylow theory in locally finite simple groups* with *Sylow theory in locally finite and p -soluble groups* being the work by adored professors **Otto H. Kegel** and **Brian Hartley** (see Page 27 of **Part 1**). **Part 2** has iv + 20 = 24 pages and includes 24 references as well as two figures of the very famous classification of the finite simple groups. For any unexplained terminology **Part 2** refers to **Part 1**.

3.1.4 Part 3 [1.4]

The **Part 3** "The Strong Sylow Theorem for the Prime p in Projective Special Linear Locally Finite Groups" of the Trilogy [1.4] continues the program begun in **Part 2** to optimise along **the way 1)** the **Theorem there** about the first type $\Xi = "A^n"$ of infinite families of finite simple groups step-by-step to further types by proving it for the second type $\Xi = "A = \text{PSL}_n"$. It first proves the **Conjecture 2** from **Part 2** about the General Linear Groups over (commutative) locally finite fields, stating that their rank is bounded in terms of their p -uniqueness, and then **breaks down** this deep insight to the Special Linear Groups and to the Projective Special Linear (PSL) Groups over locally finite fields. A thorough abstract of this three-stage-approach with a description of the **new ideas** regarding the proof for the General Linear Groups and with a figure showing the transitions to the Special Linear Groups and the PSL Groups is presented on **Page ii**.

Part 3 closes with suggestions for future research • regarding the five remaining rank-unbounded types (the "Classical Groups") and **the way 2)**, • regarding the (locally) finite and p -soluble groups by announcing sincerely a first proof of **Conjecture 3** from **Part 2**, thereby somehow rounding off the venerable classical Hall-Higman theory, and thirdly • regarding Augustin-Louis Cauchy's and Évariste Galois' very pioneering contributions to the Sylow theory of finite groups showing three very beautiful rectangles/tableaux (see Page 10). These three suggestions culminate in the ambitious announcement of the **Second Trilogy about Sylow Theory in Locally Finite Groups. Part 3** has iv + 44 = 48 pages and includes 32 references followed

by • an insightful Postscript about ► the Alternating Groups, ► the PSL Groups, ► the First Trilogy and ► the 19 families of finite simple groups, and finally followed by • the very beautiful four-page section “A Contribution to the Mathematical Theory of Big Game Hunting”. Its last Page 42 shows the **First Trilogy** as a beauteous triptych (see <https://en.wikipedia.org/wiki/Triptych> and Page 49 of **Part 1** with an inspiring overview of three other triptychs).

3.2 Review of a Trilogy about Sylow Theory in Locally Finite Groups [2.]

This comprehensive review of **15 August 2023** concerns the trilogy about Sylow Theory in Locally Finite Groups which has been published in four books by Books on Demand (BoD), Norderstedt, Germany, namely (see [1.] for an update): **Part 1** – ISBN 978-3-7504-0398-7 (**November 2023**); **Part 1 – Second edition** – ISBN 978-3-7543-6087-3 (**March 2023**); **Part 2** – ISBN 978-3-7568-3892-9 (**December 2022**); **Part 3** – ISBN 978-3-7568-9853-4 (**January 2023**).

3.3 Three Beautiful Books about Sylow Theory in Locally Finite Groups [3.]

The books are based on my Diplomarbeit (see 2.4) and continue my paper “Characterising Locally Finite Groups Satisfying the Strong Sylow Theorem for the Prime p ” which appeared in Adv. Group Theory Appl. 13 (**June 2022**) on pp. 13-39 (see [5.]). Since they contain a lot of material which cannot be published in a mathematical journal, they were published as Books on Demand (BoD) (see 3.1 and 3.2 and <https://www.bod.de/buchshop/> and <https://www.bod.fr/librairie/>).

3.4 Characterising locally finite groups satisfying the strong Sylow Theorem for the prime p – Manuscript on Sylow theory in locally finite groups – Mathematics edition [4.]

The **Mathematics edition** (32 pages) extracts from the full editions (see [1.]) the mathematical content and omits the fair and very beautiful personal dedications and information (*Richard Wagner, Albert Camus, Pablo Picasso, Freiburg i.Br., Herrsching a.A., Marcel Proust, Charles Baudelaire, Bertolt Brecht*) almost entirely. It is line numbered for (Scholarly Peer) Review purposes (but the **twenty-one Footnotes** cannot [and need not] be line numbered). Besides Sylow Theory of Locally Finite Groups (19 pages) the **Mathematics edition** provides novel but ultimately classical proofs of **considerably historic relevance** for the basic theorems of **Lagrange** and **Cauchy** on finite groups (11 pages).

3.5 Characterising Locally Finite Groups Satisfying the Strong Sylow Theorem for the Prime p [5.]

During his lectures to the 1987 Singapore Group Theory Conference **Otto H. Kegel** proposed the following question: “If every subgroup S of the locally finite group G contains a finite p -subgroup which is singular in S , does G then satisfy the strong Sylow Theorem for the prime p ?” In this paper I answer the question in the affirmative. The paper formed an extremely essential part of my German **Diplomarbeit** of 1984 (the “*Charakterisierungssatz*”) (see 2.4), written before I sadly left academia. I present the *Charakterisierungssatz* as Theorem 3.9, and summarise then the result as Theorem 3.10, stating that if G is a locally finite group and p is a prime, then G satisfies the strong Sylow theorem for the prime p if and only if every subgroup S of G contains a finite p -subgroup which is singular in S . Subsequently I present a few novel concepts for Sylow theory of (locally) finite groups to encourage future research. The paper is divided into four sections: Introduction; Good Sylow p -subgroups and p -uniqueness subgroups; Basic theorems of Sylow theory in locally finite groups and our *Charakterisierungssatz*; Novel concepts for Sylow theory in (locally) finite groups.

3.6 The Strong Sylow Theorem for the Prime p in Simple Locally Finite Groups [6.]

This Research Article continues [5.]. I begin with giving a profound overview of the structure of arbitrary simple groups and in particular of the simple locally finite groups and reduce their Sylow theory for the prime p to a quite famous conjecture by Prof. Otto H. Kegel (see [12.], Theorem 2.4: “Let the p -subgroup P be a p -uniqueness subgroup in the finite simple group S which belongs to one of the seven rank-unbounded families. Then the rank of S is bounded in terms of P .”) about the rank-unbounded ones of the 19 well-known families of finite simple groups. I introduce a new scheme to describe the 19 families, the family $\mathcal{T}$ of types, define the rank of each type, and emphasise the great rôle of Kegel covers: Prof. Kegel rediscovered from Prof. Philip Hall that an infinite simple group has a local system consisting of countably infinite simple subgroups (see [12.], Theorem 2.5) (and conversely) and if they are locally finite he discovered ground-breakingly that they have a Kegel cover (see [12.], Theorem 2.6), that is, a nested local system $\{G_n\}$ with maximal normal subgroups $M_n \leq G_n$ such that $G_n \cap M_{n+1} = \langle 1 \rangle$ so that G_n embeds into G_{n+1} / M_{n+1} . This part presents a unified picture of known results all of whose proofs are by reference.

Subsequently I apply new ideas to prove the conjecture for the Alternating Groups.

Thereupon I am remembering Kegel covers and $\star$ -sequences and the classification of simple locally finite groups according to their Kegel covers. Next I suggest a way 1) and a way 2) how to prove and even how to optimise Kegel's conjecture step-by-step or peu à peu which leads to Conjecture 1, Conjecture 2 and Conjecture 3 thereby unifying *Sylow theory in locally finite simple groups* with *Sylow theory in locally finite and p -soluble groups* whose joint study directs very reliably Sylow theory in (locally) finite groups. For any unexplained terminology I allow me to refer to [5.].

I then continue the program begun above to optimise along the way 1) the theorem about the first type $\Xi = "A^n"$ of infinite families of finite simple groups step-by-step to further types by proving it for the second type $\Xi = "A = \text{PSL}_n"$. I apply new ideas to prove Conjecture 2 about the General Linear Groups over locally finite fields, stating that their rank is bounded in terms of their p -uniqueness, and then break down this insight to the Special Linear Groups and to the Projective Special Linear (PSL) Groups over locally finite fields. I close with pretty good suggestions for future research ► regarding the remaining rank-unbounded types (the "Classical Groups") and the way 2), ► regarding (locally) finite and p -soluble groups, and ► regarding Cauchy's and Galois' contributions to Sylow theory in finite groups. I very much hope to enthuse group theorists with these suggestions and I am ready to support and to coordinate all related work.

It follows from our two theorems that simple locally finite groups which satisfy the Strong Sylow Theorem for even one Prime p are linear and hence countable if they have a local system of countable simple subgroups each having a Kegel cover "of alternating type" or "of projective special linear type".

I include the beautiful predecessor Research Article [5.] as the First Appendix for good reasons. This Research Article had been presented as a slideshow in a Talk at IGT 2024 on April 11. I include its 16 slides as the Second Appendix. Slide 1 to Slide 12 had as well been permanently instaled during IGT 2024 as a Permanent Poster. The Research Article consists of the following seventeen beautiful Chapters:

- Sketch of proof for A^n ; • Sketch of proof for $A = \text{PSL}_n$; ① Introduction; ② Proof of Theorem 1;
- ③ About Kegel covers; ④ Planning future research – Part 1; ⑤ Proof of Theorem 2;
- ⑥ Proof of Theorem 3; ⑦ Proof of Theorem 4; ⑧ Planning future research – Part 2;
- ⑨ The First Trilogy and The Second Trilogy and their reviews; • Acknowledgements;
- Postscript, Luciano De Crescenzo, Felix F. Flemisch, Conflicts of Interest, Pablo Picasso's *La Joie de vivre*;
- About the author in Munich, in Freiburg i.Br., in London, in Weiden i.d.OPf., and in Florence in Tuscany in Italy;
- 75 References; • Appendix 1 – Reference [5.] with MR Review and Zbl Review;
- Appendix 2 – Talk by Felix F. Flemisch at Ischia Group Theory 2024.

3.7 The Strong Sylow Theorem for the Prime p in Simple Locally Finite Groups – De Luxe Edition [7.]

This **Research Article** extends the **JMCA Research Article** "The Strong Sylow Theorem for the Prime p in Simple Locally Finite Groups" (see **3.6**) from **71 pages** to **220 pages** by adding **Pages i to viii, -1 to -18, 72 to 266, and ix to x** (see **Page v**).

Pages i to -18 start with this **Abstract** and then honour **Otto H. Kegel's** beautiful paper [12.] thereby explaining its relationship to its main result and to the **71-pages Research Article**, and then commenting on its final considerations. They then give an overview of the **220-pages Research Article**, including the Front Cover and a Table of Contents, and explain in great detail the relationships of the **71-pages Research Article** to JMCA and to the Ischia Group Theory (IGT) 2024 Conference and its upcoming Proceedings, centred around the **Talk** given by myself at the Conference on **April 11, the 100th birthday of Prof. Philip Hall**. They close with a **List of Open Issues** some of which I have solved already in yet unpublished work (see Page 11).

Pages 72 to x start with a dedication to **Helga** (see **Page 15**), continue with the PowerPoint Presentation at IGT 2024, **honour** Ludvig M. Sylow, the discoverer and explorer of Sylow Theory, **recall** that Ischia was twice an Artist Colony, **remember** Philip Hall's and Graham Higman's fundamental paper "On the p -Length of p -Soluble Groups and Reduction Theorems for Burnside's Problem" thereby **explaining** its relationship to the **71-pages Research Article**, **recall** Some Historicals on Group Theory, in particular Philip Hall's handwritten Lecture Notes on Group Theory and **show** all these beautiful Lecture Notes, **show** a considerably reworked presentation of WIKIPEDIA's Classification of finite simple groups, **remember** Prof. Kegel and Prof. Hall at the Mathematisches Forschungsinstitut Oberwolfach (MFO), and finally as the Back Cover **refer** to Philip Hall's Archive at the London Mathematical Society and again to his Lecture Notes, and in the end **close** by showing Who is Felix F. Flemisch ? & Another Abstract of the **71-pages Research Article**.

3.8 Felix F. Flemisch – Happy Birthday and Gratitude Greetings to Professor Otto H. Kegel (July 17, 2025) [8.]

This is the Happy Birthday Postcard which was sent by Felix F. Flemisch on July 17, 2025 to Professor Otto



Kegel (together with tasty treats) on the occasion of his 91th birthday: Unfortunately, Prof. Otto Kegel could not receive it.

3.9 Professor Otto H. Kegel out of Great Gratitude for Opening a New and Grandiose Dimension of Mathematics to Me [9.]

This paper presents my true Happy Birthday Greetings (in German) which I sent per express delivery on **July 17, 2025** to Prof. Kegel together with a Happy Birthday Gift Box with tasty titbits to congratulate him on his 91st birthday wishing “À votre santé et bon appétit!”. But Prof. Kegel could not receive let alone relish them ... ☹️. I added (in English) two slides of my beautiful talk at IGT 2024 and my rather thorough comments with quite a number of improvements on his beautiful and groundbreaking paper “Four lectures on Sylow theory in locally finite groups” (see [12.]). I also added the obituaries of Albert-Ludwigs-University in Freiburg i.Br. and of his family with comments, the English translation taken from **3.8**, reminders to his dedication on the occasion of his 70th birthday in the Archiv der Mathematik, his visit to IGT 2016 and honouring him at IGT 2024.

3.10 Otto H. Kegel's Beautiful Contributions to Sylow Theory in Locally Finite Groups [10.]

Otto H. Kegel published two fundamental papers on Sylow Theory in locally finite groups: see [11.] and [12.]. The paper [10.] summarises them, compares them and above all provides a list of their **Open Issues** which are still open until the present day. To study crucial configurations, **Kegel** developed in [12.] the really quite excogitated concept of the “(smooth simple straight) split sequences of finite p -perfect subgroups with their associated ascending sequences of subgroups” which is related to his equally very fine concept of the “Sylow-separated (ascending) sequences of p -subgroups with associated sequences of Sylow p -subgroups” he had developed already more then ten years earlier in [11.]. When I met him personally in **July 2022**, I tried to find out how he had detected these really ingenious ideas, but woefully was unsuccessful, although I was really very privileged to witness up very close the creation of the idea of [4.] (see [9.]). A scheduled new attempt in **July 2025** (see [9.]) could not be realised ... ☹️. I therefore developed [10.] to honour his so fantastic achievements of Sylow Theory. The paper is thought to be a supplement to **Mahmut Kuzucuoğlu's** beautiful paper [23.] about life and work of **Otto H. Kegel**. Before publishing it in **the JMCA** I failed to publish it in **the journal of AGTA** and in **the journal Archiv der Mathematik** (see Page 22 and Page 23).

4 Conclusions

I present in [9.] and [10.] the following **List of twelve Open Issues**:

- **Open Issue 1:** Does the strong Sylow Theorem for the prime p force the maximum condition for Sylow-separated sequences of p -subgroups?
- **Open Issue 2:** Does the maximum condition for $I_p G$ imply the strong Sylow Theorem for the prime p ?
- **Open Issue 3:** Extend Theorems 2, 3 and 4 of the JMCA-paper [6.] to the remaining four Locally Finite Classical Groups (i.e., the Symplectic Groups, the Unitary Groups, the Orthogonal Groups in char $\neq 2$ and the Orthogonal Groups in char 2).
- **Open Issue 4:** Summarise the work by **B. Hartley** and **A. Rae** regarding λ_p and p^{a_p} and the foregoing work on the classical Hall-Higman theory regarding λ_p and $p^{b_p}, c_p, d_p, p^{c_p}$ and r_p by **P. Hall, G. Higman, A.H.M. Hoare, T.R. Berger, F. Gross, E.G. Bryukhanova** and **A. Turull**.
- **Open Issue 5:** Let p be a prime. Let G be a p -soluble finite group, $\lambda_p(G)$ be its p -length, and $a_p(G)$ be its p -uniqueness (see Page 37 of [5.]). Then (best possible) $\lambda_p(G) \leq a_p(G) + 1$.
- **Open Issue 6:** Deduce the three rectangles/tableaux shown below and use them to prove **Lagrange's** theorem and **Cauchy's** concealed second and third group theorems:

complete right transversal for G in H	the first row consists of <i>all</i> elements z_k of G ($1 \leq k \leq M$) acting on H in the following rows via multiplication from the left by their inverses				correspondence	$\text{set}_H \text{Orbi}(G) := G \setminus H$ of <i>all</i> orbits of H under G acting by left translation
$t_1 := 1 =: z_1$	z_2	z_3	...	z_M	$\leftrightarrow$	$G = {}_1 \text{Orb}(G)$
t_2	$z_2 t_2$	$z_3 t_2$	...	$z_M t_2$	$\leftrightarrow$	$G t_2 = {}_{t_2} \text{Orb}(G)$
t_3	$z_2 t_3$	$z_3 t_3$	...	$z_M t_3$	$\leftrightarrow$	$G t_3 = {}_{t_3} \text{Orb}(G)$
...	...	...	...	...	...	...
t_R	$z_2 t_R$	$z_3 t_R$	...	$z_M t_R$	$\leftrightarrow$	$G t_R = {}_{t_R} \text{Orb}(G)$

rectangle $|G| \times [H:G]$ of elements

set of <i>certain</i> orbits of H under G acting by left translation	the first row consists of <i>all</i> right cosets Gx_1^k of G in H ($0 \leq k \leq p-1$) with the powers of some p -blank x_1 of G in H ; the following rows consist of right cosets of G in H with the powers of left conjugates of x_1				correspondence	$X := \langle x_1 \rangle$; set of <i>all</i> orbits of H under $G \cup X$, the simultaneous actions of G by left translation and of X by right translation
$Gx_1^0 t_1 = G$	Gx_1	Gx_1^2	...	Gx_1^{p-1}	$\leftrightarrow$	cosets $G \langle x_1 \rangle = GX = \text{double coset } G 1 X$
$Gx_2^0 t_2 = G t_2$	$Gx_2 t_2$	$Gx_2^2 t_2$	...	$Gx_2^{p-1} t_2$	$\leftrightarrow$	cosets $G \langle x_2 \rangle t_2 = \text{double coset } G t_2 X$
$Gx_3^0 t_3 = G t_3$	$Gx_3 t_3$	$Gx_3^2 t_3$	...	$Gx_3^{p-1} t_3$	$\leftrightarrow$	cosets $G \langle x_3 \rangle t_3 = \text{double coset } G t_3 X$
...	...	...	...	...	...	...
$Gx_S^0 t_S = G t_S$	$Gx_S t_S$	$Gx_S^2 t_S$	...	$Gx_S^{p-1} t_S$	$\leftrightarrow$	cosets $G \langle x_S \rangle t_S = \text{double coset } G t_S X$

tableau $p \times [H:G] / p$ of cosets

set of <i>certain</i> orbits of H under G acting by left translation	the first row consists of <i>all</i> right cosets Gx_{1c} of G in H ($0 \leq c \leq H _p - 1$) with the elements of some Sylow p -subgroup X of H , all of whose elements of order p are p -blanks of G in H ; the following rows consist of right cosets of G in H with the elements of left conjugates of X				correspondence	$ X = H _p = p^b$; set of <i>all</i> orbits of H under $G \cup X$, the simultaneous actions of G by left translation and of X by right translation
$Gx_{10} t_1 = G$	Gx_{11}	Gx_{12}	...	Gx_{1p^b-1}	$\leftrightarrow$	cosets $G \{x_{1c} 0 \leq c \leq p^b-1\} = GX = \text{double coset } G 1 X$
$Gx_{20} t_2 = G t_2$	$Gx_{21} t_2$	$Gx_{22} t_2$	...	$Gx_{2p^b-1} t_2$	$\leftrightarrow$	cosets $G \{x_{2c} 0 \leq c \leq p^b-1\} t_2 = \text{double coset } G t_2 X$
$Gx_{30} t_3 = G t_3$	$Gx_{31} t_3$	$Gx_{32} t_3$	...	$Gx_{3p^b-1} t_3$	$\leftrightarrow$	cosets $G \{x_{3c} 0 \leq c \leq p^b-1\} t_3 = \text{double coset } G t_3 X$
...	...	...	...	...	...	...
$Gx_{T0} t_T = G t_T$	$Gx_{T1} t_T$	$Gx_{T2} t_T$	...	$Gx_{Tp^b-1} t_T$	$\leftrightarrow$	cosets $G \{x_{Tc} 0 \leq c \leq p^b-1\} t_T = \text{double coset } G t_T X$

rectangle $|H|_p \times [H:G] / |H|_p$ of cosets

- **Open Issue 7:** Deduce **Cauchy's** fundamental theorem of 1812/1815 from $[H:\langle x \rangle] \geq |G|$, if x is a **p -blank of G in H** , that is, an element of H of order p with $x \notin G$.

- **Open Issue 8:** Determine all the (minimal) p -uniqueness subgroups for the known finite simple groups and their natural overgroups, the symmetric and the linear groups, and for the (locally) p -soluble groups, distinguishing $p \geq 5$, $p = 3$ and $p = 2$.
- **Open Issue 9:** Specify for a finite group the relationships of **the properties** of its p -subgroups which are **minimal** (w.r.t. order or w.r.t. inclusion) w.r.t. being contained in a unique **Sylow** p -subgroup to **the properties** (e.g., conjugacy) of its p -subgroups which are **maximal** w.r.t. being contained in a (unique) **Sylow** p -subgroup (i.e., its **Sylow** p -subgroups).
- **Open Issue 10:** Introduce for every prime p a generalised p -length for locally finite groups which is finite if and only if they satisfy the strong **Sylow** Theorem for p .
- **Open Issue 11:** Making a revision of **Kegel's** (3.5) Theorem [12.] thereby relating it to rarely known articles and extending it to $p \geq 3$, extend **Kegel's** (4.4) Theorem [12.] to the case $p = 3$.
- **Open Issue 12:** Summarise **Kegel's** wonderful **Sylow** paper [12.] thereby integrating **first of all** the AGTA-paper (see <https://www.advgrouptheory.com/journal/Volumes/13/Flemisch.pdf>) and then **secondly** the JMCA-paper (see <https://www.onlinescientificresearch.com/articles/the-strong-sylow-theorem-for-the-prime-p-in-simple-locally-finite-groups--de-luxe-edition.pdf>) and then extending **thirdly** his main Theorem (4.4) [12.] to $p = 3$ and $p = 2$ by using the Open Issues 11 and 5.

I solved the following **Open Issues** in unpublished draft and partly German work: **OI 3, OI 4, OI 5, OI 6, OI 7, OI 10** and **OI 11**. The following **Open Issues** are without draft work let alone published work: **OI 1, OI 2, OI 8, OI 9** and **OI 12**. Therefore I gladly suggest the following **fascinating topics for future research**: • Develop (possibly myself) the **Open Issues OI 3, OI 4, OI 5, OI 6, OI 7, OI 10** and **OI 11** to publishable documents thereby using my draft work. ☺ • Develop the **Open Issues OI 1, OI 2, OI 8, OI 9** and **OI 12** to publishable papers thereby using my published work. ☺ I will be happy if this research can be done in **2026**.

Acknowledgements

The author is sincerely very grateful to the known and unknown **referees** for their corrections, suggestions and such friendly adjuvant advice which improved the manuscript quite considerably. He wishes to thank also so very heartfully his truly most fabulous wife **Helga** . Without her tenderest and unconditional support and her love and greatest patience over so many years, this publication would never ever have been born. Most importantly, he is forever and ever grateful to **Prof. Brian Hartley** and to his masterly teacher **Prof. Otto H. Kegel** for their **beautiful** papers which provide really incredible insights and give marvellous pleasure in reading and understanding the magnificent Sylow Theory of both locally p -soluble locally finite groups (for $p \neq 2$) and locally finite groups in general (for $p \geq 5$), specifically the simple ones.

References

1. **FLEMISCH, F.F.:** Trilogy about Sylow Theory in Locally Finite Groups.
- 1.1 **FLEMISCH, F.F.:** Characterising Locally Finite groups satisfying the Strong Sylow theorem for the Prime p – Part 1 of a Trilogy. Norderstedt, Germany: Books on Demand (**March 2023**). ISBN 978-3-7543-6087-3. <https://buchshop.bod.de/characterising-locally-finite-groups-satisfying-the-strong-sylow-theorem-for-the-prime-p-part-1-of-a-trilogy-dipl-math-felix-flemisch-9783754360873>.
- 1.2 **FLEMISCH, F.F.:** Characterising Locally Finite groups satisfying the Strong Sylow theorem for the Prime p – Part 1 of a Trilogy. Second edition. Norderstedt, Germany: Books on Demand (**November 2023**). ISBN 978-3-7568-0801-4. <https://buchshop.bod.de/characterising-locally-finite-groups-satisfying-the-strong-sylow-theorem-for-the-prime-p-part-1-of-a-trilogy-felix-f-flemisch-9783756808014>.

- 1.3 **FLEMISCH, F.F.:** About the Strong Sylow theorem for the Prime p in Simple Locally Finite Groups – Part 2 of a Trilogy. Norderstedt, Germany: Books on Demand (**November 2023**). ISBN 978-3-7543-3642-7. <https://buchshop.bod.de/about-the-strong-sylow-p-theorem-in-simple-locally-finite-groups-part-2-of-a-trilogy-dipl-math-felix-f-flemisch-9783754336427>.
- 1.4 **FLEMISCH, F.F.:** The Strong Sylow theorem for the Prime p in Projective Special Linear Locally Finite Groups – Part 3 of a Trilogy. Norderstedt, Germany: Books on Demand (**April 2023**). ISBN 978-3-7568-9853-4. <https://buchshop.bod.de/the-strong-sylow-theorem-for-the-prime-p-in-projective-special-linear-locally-finite-groups-part-3-of-a-trilogy-dipl-math-felix-f-flemi-9783756898534>.
2. **FLEMISCH, F.F.:** Review of a Trilogy about Sylow Theory in Locally Finite Groups. Contemporary Mathematics, Volume 4, Issue 3 (**April 2023**), 484-487. <https://ojs.wiserpub.com/index.php/CM/issue/view/cm.v4i32023.379-619> and <https://ojs.wiserpub.com/index.php/CM/article/view/2669>.
3. **FLEMISCH, F.F.:** Three Beautiful Books about Sylow Theory in Locally Finite Groups. Journal of Mathematical & Computer Applications (JMCA), Volume 2, Issue 3 (**September 2023**), 1-3. <https://www.onlinescientificresearch.com/journals/jmca/archives/2023/2/3>.
4. **FLEMISCH, F.F.:** Characterising locally finite groups satisfying the strong Sylow Theorem for the prime p – Manuscript on Sylow theory in locally finite groups – Mathematics edition. Norderstedt, Germany: Books on Demand (**September 2021**). ISBN 978-3-7543-4434-7. <https://buchshop.bod.de/characterising-locally-finite-groups-satisfying-the-strong-sylow-theorem-for-the-prime-p-felix-f-flemisch-9783754344347>.
5. **FLEMISCH, F.F.:** Characterising Locally Finite Groups Satisfying the Strong Sylow Theorem for the Prime p . Adv. Group Theory Appl. 13 (**June 2022**), 13-39 (see Zbl 1496.20065 and MR4441631). <https://www.advgrouptheory.com/journal/index.php#vol13>.
6. **FLEMISCH, F.F.:** The Strong Sylow Theorem for the Prime p in Simple Locally Finite Groups. Journal of Mathematical & Computer Applications (JMCA), Volume 4, Issue 1 (**January 2025**), 1-72. <https://www.onlinescientificresearch.com/journals/jmca/archives/2025/4/1>.
7. **FLEMISCH, F.F.:** The Strong Sylow Theorem for the Prime p in Simple Locally Finite Groups – De Luxe Edition. Journal of Mathematical & Computer Applications (JMCA), Volume 4, Issue 3 (**June 2025**), 1-220. <https://www.onlinescientificresearch.com/journals/jmca/archives/2025/4/3>.
8. **FLEMISCH, F.F.:** Felix F. Flemisch – Happy Birthday and Gratitude Greetings to Professor Otto H. Kegel (July 17, 2025) . AGTA – Group Theory Archivum – Historical Documents. <https://www.advgrouptheory.com/GTArchivum/historicals.html> and <https://www.advgrouptheory.com/GTArchivum/Kegel/Felix%20F.%20Flemisch%20%E2%80%93%20Happy%20Birthday%20and%20Gratitude%20Greetings%20to%20Professor%20Otto%20H.%20Kegel%20on%20July%2017,%202025.pdf>.
9. **FLEMISCH, F.F.:** Professor Otto H. Kegel out of Great Gratitude for Opening a New and Grandiose Dimension of Mathematics to Me. Journal of Mathematical & Computer Applications (JMCA), Volume 4, Issue 4 (**August 2025**), 1-18. <https://www.onlinescientificresearch.com/journals/jmca/archives/2025/4/4>.
10. **FLEMISCH, F.F.:** Otto H. Kegel's Beautiful Contributions to Sylow Theory in Locally Finite Groups. Journal of Mathematical & Computer Applications (JMCA), Volume 4, Issue 6 (**November 2025**), 1-24. <https://www.onlinescientificresearch.com/journals/jmca/archives/2025/4/6>.
11. **KEGEL, O.H.:** "Chain conditions and Sylow's theorem in locally finite groups", in: Symposia Mathematica, Volume XVII, Convegno sui Gruppi Infiniti, Istituto Nazionale di Alta Matematica (**INdAM**) 'Francesco Severi', Roma, **11-14 Dicembre 1973**, Academic Press, London & New York (1976), 251-259 (see MR0414714 [MR 54 #2809 by Rüdiger Göbel] and Zbl 0328.20029 [Autorreferat]). ISBN 978-0-12612-217-6. <https://www.altamatematica.it/>.
12. **KEGEL, O.H.:** "Four lectures on Sylow theory in locally finite groups", in: Group Theory – Proceedings of the Singapore Group Theory Conference held at the National University of Singapore, **June 8-19, 1987**, edited by K.N. CHENG and Y.K. LEONG, Walter de Gruyter, Berlin & New York (**January 1989**, reprinted **November 2016**), 3-27 (see MR0981832 [MR 90c:20037 by tough Brian Hartley (March 1990)] and Zbl 0659.20024 [by tough Bernhard Amberg]). ISBN 978-3-11-011366-2. ISBN 978-0-89925-406-7. <https://www.degruyter.com/view/book/9783110848397/10.1515/9783110848397-004.xml>.
13. **KEGEL, O.H.:** Caractérisation des sous-groupes accessibles d'un groupe fini. Séminaire DUBREIL-PISOT (Algèbre et Théorie des Nombres) 13^e année, 1959/60, n° 18, 01-06 (**29 Mars 1960**), https://www.numdam.org/item/SD_1959-1960_13_2_A7_0/, Zbl 0112.26004.
14. **KEGEL, O.H.:** Sylow-Gruppen und Subnormalteiler endlicher Gruppen. Archiv der Mathematik 78, 205-221 (**December 1962**), <https://d-nb.info/1123426201/34>, Zbl 0102.26802, MR0147527 [MR 26 #5042].
15. **KEGEL, O.H.:** Eine Charakterisierung der Sylowgruppen endlicher Gruppen. Rendiconti del Seminario Matematico della Università di Padova 36, n° 1, 122-128 (**10 June 1965**), https://www.numdam.org/item/RSMUP_1966_36_1_122_0/, Zbl 0144.01503, MR 0202823 [MR 34 #2682].
16. **KEGEL, O.H.:** Über einfache, lokal endliche Gruppen. Math. Z. 95, 169-195 (**12 March 1966**), <https://link.springer.com/article/10.1007/BF01111522>, Zbl 0147.27002, MR0204527 [MR 34 #4366].

17. **KEGEL, O.H.:** Locally finite versus finite simple groups. Theory of Finite Groups, Symposium Harvard University **2-4 May 1968**, edited by RICHARD BRAUER and CHIH-HAN SAH, 247-249 (1969), <https://epdf.pub/theory-of-finite-groups.html>, Zbl 0184.04403.
18. **KEGEL, O.H.:** Strong finiteness conditions in locally finite groups. Math. Z. **117**, 309-324 (March 1970), <https://link.springer.com/article/10.1007/BF01109850>, Zbl 0195.03804, MR0306330 [MR 46 #5456].
19. **KEGEL, O.H.:** Locally finite simple groups. Proceedings of the Second International Conference on The Theory of Groups, Dept. of Mathematics, Australian National University, Institute for Advanced Studies, Canberra, **13-24 August 1973**, Lecture Notes in Mathematics **372**, edited by MICHAEL F. NEWMAN, 395-400 (1974), <https://link.springer.com/book/10.1007/978-3-662-21571-5>, Zbl 0292.20028, MR0364460 [MR 51 #714].
20. **KEGEL, O.H.:** Reinhold Baer (1902-1979). Obituary. The Mathematical Intelligencer, Volume **2**, 181-182 (June 1980), <https://link.springer.com/article/10.1007/BF03028598>, Zbl 0446.01022, MR0600225 [MR 82a:01037].
21. **KEGEL, O.H.:** The structure of locally finite groups with min- p . Mathematical Reports – Comptes rendus mathématiques de l'Académie des sciences, Volume **IV**, n° **6**, **Décembre 1982**, 383-386, <https://mathreports.ca/>, Zbl 0506.20025, MR0681198 [MR 83m:20043].
22. **KEGEL, O.H. – WEHRFRITZ B.A.F.:** “Locally Finite Groups”, North-Holland Mathematical Library, Volume **3**, North-Holland Publishing Company [, Ltd.], Amsterdam & London (1973) (see MR0470081 [MR 57 #9848] and Zbl 0259.20001 [by tough Brian Hartley]). ISBN 0-7204-2454-2. American Elsevier Publishing Company, Inc. (1973). ISBN 978-0-444-10406-9. ISBN 0-08-095413-8 (2000, eBook). <https://www.sciencedirect.com/bookseries/north-holland-mathematical-library/vol/3/suppl/C>.
23. **KUZUCUOĞLU, M.:** Otto H. Kegel (1934 – 2025). Adv. Group Theory Appl. **21** (August 2025), 1-9, <https://www.advgrouptheory.com/journal/index.php#vol21>, Zbl 1569.01037, MR4953771.
24. **SCHARLAU, W.:** Die Entdeckung der Sylow-Sätze (The discovery of the Sylow theorems). Historia Mathematica, Volume **15**, Issue **1**, 40-52 (February 1988), <https://www.sciencedirect.com/science/article/pii/0315086088900481>, Zbl 0637.01006 [by Roger L. Cooke], MR0931678 [MR 89f:01041].
25. **SYLOW, L.M.:** Om Systemer af konjugerede Substitutioner, der kunne tilhøre irreduktible Ligninger, hvis Grad er Primtal. Forhandlinger i Videnskabs-Selskabet i Christiania Aar 1867, 105-122, <https://www.biodiversitylibrary.org/bibliography/62508>.
26. **SYLOW, L.M.:** Théorèmes sur les groupes de substitutions. Mathematische Annalen, Volume **5**, Issue **4**, 584–594 (Dezember 1872), <https://link.springer.com/journal/208/volumes-and-issues/5-4>, <https://link.springer.com/article/10.1007/BF01442913>, JFM 04.0056.02 [by Eugen O.E. Netto], MR1509796.
27. **WATERHOUSE, W.C.:** The Early Proofs of Sylow's Theorem. Archive for History of Exact Sciences, Volume **21**, Issue **3**, 279-290 (September 1980), <https://link.springer.com/article/10.1007/BF00327877>, Zbl 0436.01006 [by Frédéric Campana], MR0575718 [MR 82i:01034].



Pablo Picasso – *La Joie de vivre* which shepherds the Trilogy as a flock along all abysses (see the covers of [1.1], [1.2], [1.3], [1.4] and [4.]

Received: 2 January 2026
 Revised: 12 January 2026
 23 February 2026
 Accepted: 14 March 2026
 Published online: 21 March 2026

Copyright: © 2026 Felix F. Flemisch. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Ludvig Sylow and William Waterhouse and Winfried Scharlau

After 13 pages created by myself and thus copyrighted, I finally present six short beauteous articles which were not created by myself but by **Ludvig Sylow** and **William Waterhouse** and **Winfried Scharlau**:

- the “**Om Systemer af konjugerede Substitutioner, der kunne tilhøre irreduktible Ligninger, hvis Grad er Primtal**” by Ludvig M. Sylow (see [25.]), a forerunner of the very famous [26.] [22 pages];
- the translation (by ÜZM GmbH) into English of Ludvig M. Sylow’s article [25.] “**On Systems of Conjugate Substitutions that could belong to irreducible Equations whose Degree is a Prime Number**” [22 pages];
- the very famous “**Théorèmes sur les groupes de substitutions**” by Ludvig M. Sylow (see [26.]) [20 pages];
- the famous “**The Early Proofs of Sylow’s Theorem**” by William C. Waterhouse (see [27.]) [17 pages];
- the equally famous “**Die Entdeckung der Sylow-Sätze**” by Winfried Scharlau (see [24.]) [27 pages];
- the translation (by myself) into English “**The Discovery of the Sylow Theorems**” of Winfried Scharlau’s pioneering article [9 pages] (Copyright © 2026 Felix F. Flemisch).

Ludvig Mejdell Sylow (12 December 1832 until 7 September 1918)
(see https://en.wikipedia.org/wiki/Peter_Ludwig_Sylow)

The discoverer and explorer of Sylow theory



Ludvig M. Sylow
(12 December 1832 until 7 September 1918)
(see https://en.wikipedia.org/wiki/Peter_Ludwig_Sylow and <https://mathshistory.st-andrews.ac.uk/Biographies/Sylow/> and https://en.wikipedia.org/wiki/Sylow_theorems)

Sylow Theorem Part 1
 $|G| = p^k m \quad H \leq G$
 $|H| = p^k$

Sylow Theorem Part 2
 H, K Sylow p -subgroups
 $H = gKg^{-1}$

Sylow Theorem Part 3
 $n_p \equiv 1 \pmod{p} \quad n_p | m$

Monsieur L. Sylow (Frederikssjøen in Norway): *Théorèmes sur les groupes de substitutions*. *Mathematische Annalen* 5, Issue 4 (December 1872), 584-594
(see <https://link.springer.com/journal/208/volumes-and-issues/5-4>).
MR1509796 (no review: see <https://mathscinet.ams.org/mathscinet-getitem?mr=1509796>).
Zbl JFM 04.0056.02 (Eugen O. Netto: see <https://www.zblmath.org/?q=an%3A04.0056.02> and <https://www.zblmath.org/pdf/02718820.pdf>)

In 1904 Ludvig Sylow was admitted to the German order **Pour le Mérite** für Wissenschaften und Künste (see <https://www.orden-pourlemerite.de/mitglieder/peter-ludwig-mejdell-sylow> and https://en.wikipedia.org/wiki/Pour_le_M%C3%A9rite and https://de.wikipedia.org/wiki/Pour_le_M%C3%A9rite and https://commons.wikimedia.org/wiki/Category:Pour_le_M%C3%A9rite).



Winfried Scharlau (12 August 1940 until 26 November 2020)
(see https://en.wikipedia.org/wiki/Winfried_Scharlau)

Die Westfälische Wilhelms-Universität Münster trauert um

Prof. Dr. Winfried Scharlau

der am 26. November 2020 im Alter von 80 Jahren verstorben ist.

Winfried Scharlau wurde am 12. August 1940 in Berlin geboren. Er studierte Mathematik an der Rheinischen Friedrich-Wilhelms-Universität in Bonn und der Columbia University in New York. 1967 promovierte er bei Friedrich Hirzebruch in Bonn mit einer Arbeit aus den Gebieten Zahlentheorie und Algebra. Bereits 1970 wurde er zum Ordentlichen Professor am Mathematischen Institut der Universität Münster ernannt, wo er bis zu seiner Emeritierung im Jahre 2005 forschte und lehrte. Er war äußerst aktiv in seinem Fachbereich und auch mehrfach dessen Dekan. Als Forscher und Lehrer war er sehr erfolgreich. Von seinem Engagement als Mathematiker und als Mensch profitierten Kollegen, Schüler und Studierende gleichermaßen. Er brachte 15 Doktoranden zur Promotion, war Verfasser einer Monographie über Quadratische Formen und weiterer mathematischer Lehrbücher. 1972 war er invited Speaker beim Internationalen Mathematikerkongress in Vancouver. Er war korrespondierendes Mitglied der Akademie der Wissenschaften in Göttingen und 1991/92 Präsident der Deutschen Mathematikervereinigung (DMV).

Er schrieb Biografien der Mathematiker Alexander Grothendieck und Friedrich Hirzebruch sowie mit einem Koautor eine historisch orientierte Einführung in die Zahlentheorie. Ganz außerhalb der Mathematik war er leidenschaftlicher Hobbyfotograf und Ornithologe und Autor zweier literarischer Bücher.

Die Westfälische Wilhelms-Universität und der Fachbereich Mathematik und Informatik werden Winfried Scharlau ein ehrendes Andenken bewahren.

Der Rektor der Westfälischen Wilhelms-Universität
Prof. Dr. Johannes Wessels

Der Dekan des Fachbereichs Mathematik und Informatik
Prof. Dr. Xiaoyi Jiang

Der geschäftsführende Direktor des Mathematischen Instituts
Prof. Dr. Wilhelm Winter

Alle Institutsangehörigen



Wer ist Alexander Grothendieck?
Anarchie, Mathematik, Spiritualität, Einsamkeit
– Eine Biographie von Winfried Scharlau





Deutsche Mathematiker-Vereinigung (<https://www.mathematik.de>)

<https://www.mathematik.de/hochschule-beruf/mathemacher-innen/>

<https://www.mathematik.de/hochschule-beruf/mathemacher-innen/2326-winfried-scharlau>

<https://www.mathematik.de/kontakt-medienbuero>

Winfried Scharlau

Mathemacher des Monats Februar 2017

Winfried Scharlau, ein Doktorsohn von **Friedrich Hirzebruch**, ist in Fachkreisen für seine Arbeiten in der Zahlentheorie bekannt, die an seiner langjährigen Arbeitsstätte, der Universität Münster, entstanden sind, sowie als ehemaliger Präsident der DMV – er leitete den Verein in den Jahren 1991/92. Doch das ist nicht alles: **Scharlau** hat auch zwei Romane geschrieben: **I megali istoria** (die große Geschichte) (siehe <https://www.mathematik.de/lesecke-article/1105-i-megali-istoria>) und **Scharife** (siehe <https://www.mathematik.de/lesecke-article/1011-scharife>) – und bedeutende Mathematiker-Biographien, zum Beispiel über den Braunschweiger Mathematiker **Richard Dedekind** und den geheimnisumwitterten **Alexander Grothendieck** sowie den grandiosen **Ludvig Sylow** (siehe Seite 52 bis Seite 78). Scharlau, seit nunmehr 11 Jahren emeritiert, dient seinem Fach auch heute noch als Biograph. Gerade erschien sein jüngstes Werk bei Springer Spektrum: "Das Glück, Mathematiker zu sein – Friedrich Hirzebruch und seine Zeit". Grund genug, **Winfried Scharlau** zum Mathemacher des Monats zu machen und ihn kurz zu interviewen. **Thomas Vogt** vom DMV-Medienbüro sprach mit ihm.

Nachtrag: Zu unserer großen Trauer erfuhren wir vom Tode Winfried Scharlaus am 26.11.2020. Die DMV trauert um ihr Ehrenmitglied und ihren ehemaligen Präsidenten (1991/92).

Auf welchen mathematischen Teilgebieten haben Sie hauptsächlich geforscht?

Algebra, Zahlentheorie, insbesondere Theorie der quadratischen Formen.

Hatten Sie schon immer ein mathematik-historisches Interesse und wann fingen Sie an, mathematik-historisch zu arbeiten?

Mich haben vor allem Mathematiker interessiert und weniger die Ideengeschichte der Mathematik. Insofern bin ich eigentlich gar kein richtiger Mathematik-Historiker. Mein Interesse begann etwa 1980 mit Arbeiten zu **Dedekind**, an dessen 150. Geburtstag erinnert werden sollte.



Winfried Scharlau in seiner Berliner Wohnung Foto: **Thomas Vogt**

Welche Mathematiker-Persönlichkeiten haben Sie besonders in ihren Bann gezogen?

Cardano, Dedekind, Dirichlet, Grothendieck, Hirzebruch, Tits.

Wollten Sie schon länger eine Biographie über Hirzebruch schreiben, oder war das eine Idee des Verlags?

Ehrlich gesagt, kam mir die Idee am Tag von **Hirzebruchs** Beerdigung, als so viele Menschen aus aller Welt sich um sein Grab versammelten und vielfältige Erinnerungen aus der Vergangenheit wach wurden, die alle diesen großartigen Mathematiker und so wunderbaren Menschen **Hirzebruch** betrafen. Mathe zählt weil – wie **Galilei** gesagt hat – das Buch der Natur in der Sprache der Mathematik geschrieben ist.

Daher auch die Idee nicht nur Hirzebruch, sondern auch seine Zeit vor dem geistigen Auge des Lesers auferstehen zu lassen?

Genau. Das bot sich hier perfekt an. **Hirzebruch** war eben nicht nur ein weltweit wirkender Mathematiker sondern auch – um im Bild zu bleiben – prägend für die Wiederauferstehung der Mathematik in Deutschland in der Zeit nach dem Zweiten Weltkrieg. Er hat dieser als erster nach dem Krieg internationale Sichtbarkeit gegeben.

Wie sind Sie bei der Biographie über Hirzebruch vorgegangen und wie sind Sie an diesen seltenen, teils sehr privat anmutenden, Fotoschatz gekommen?

Die Arbeit verlief ziemlich zufällig. Je nachdem wie ich an Informationen oder Dokumente kommen konnte, mit welchen Personen ich sprechen oder korrespondieren konnte und oft auch, wie mir gerade der Sinn stand, habe ich mal da und mal dort etwas aufgeschrieben und im Verlauf der Arbeit zusammengefügt. Für fast alle Fotos gibt es Quellenangaben. Die meisten wurden mir von **Frau Hirzebruch** zur Verfügung gestellt; viele habe ich im Laufe der Jahrzehnte selbst gemacht; viel schwirrt heutzutage auch im Internet herum. Übrigens habe ich alle Fotos bearbeitet, um ein technisch einigermaßen akzeptables Ergebnis zu erzielen. Das ist nicht immer so gelungen, wie ich es mir gewünscht hätte. Auf dem Gebiet bin ich einfach kein Profi! (lacht)

Haben Sie weitere Biographien geplant oder in Arbeit oder was machen Sie sonst noch so, nun, da Sie emeritiert sind?

Es ist nichts Größeres geplant und wäre wohl auch gar nicht mehr zu schaffen, denn das "nun" in Ihrer Frage muss man etwas modifizieren: ich wurde ja schon vor mehr als 11 Jahren emeritiert. Allerdings habe ich eine große Sammlung von (selbst gemachten) Fotos von Mathematikern, und diese Sammlung würde ich gerne noch ergänzen.

Hier an der Wand hängen aber nur Fotos von Vögeln ...

(lacht) Ja, Vogelbeobachtung und -fotografie ist auch so ein Hobby von mir! Das Buch "Das Glück, Mathematiker zu sein – Friedrich Hirzebruch und seine Zeit" können Sie in der Buchhandlung bestellen oder direkt bei Springer über diesen Link: <https://link.springer.com/book/10.1007/978-3-658-14757-0>.

© 2026 Deutsche Mathematiker-Vereinigung

Winfried Scharlau als Mathemacher der DMV im Monat Februar 2017

https://opc.mfo.de/person_data/ID=7496

Oberwolfach Photo Collection

Total number of photos: 25423

Main

Occasions

Persons

Links

Legal Notice/Impressum

Search

Extended Search

Details for Winfried Scharlau



F. Göke
W. Scharlau
(2018)



W. Scharlau
(2018)



W. Scharlau
(2018)



W. Scharlau
M. Rösner
(2018)



W. Scharlau
W. Scharlau
(2018)



W. Scharlau
(2006)



W. Scharlau
(2006)



W. Scharlau
D. Scharlau
J. McCleary
J. J. Dine
A. Schneider
C. Heusel
S. Shentek
(2009)



W. Scharlau
M. Knöser
(2009)



W. Scharlau
P. Birkhoff
P. Birkhoff
W. Scharlau
(2009)



W. Scharlau
(1990)

For more detailed information please click on the photo.

https://opc.mfo.de/detail/photo_id=12938

Oberwolfach Photo Collection

Total number of photos: 25423

Main

Occasions

Persons

Links

Legal Notice/Impressum

Search

Extended Search

1990



On the Photo:

Scharlau, Winfried

Location: Berkeley

Author: Bergman, George M. (photos provided by Bergman, George M.)

Source: George M. Bergman, Berkeley

Year: 1990

Copyright: George M. Bergman, Berkeley

Photo ID: 12938

[Find related pictures](#)

https://opc.mfo.de/detail/photo_id=27338

Oberwolfach Photo Collection

Total number of photos: 25423

Main

Occasions

Persons

Links

Legal Notice/Impressum

Search

Extended Search

2018



On the Photo:

Scharlau, Winfried (left)

Rückner, Michael (right)

Annotation: Ehrnftagung, March 2018

Location: Paderborn

Author: Scharlau, Dorothee (photos provided by Scharlau, Dorothee)

Source: Winfried Scharlau

Year: 2018

Copyright: Winfried Scharlau

Photo ID: 27338

[Find related pictures](#)

[Correct errors:](#) If you have corrections or additional information on this photo, please send us a message using the following form.

[Are you interested in using this photo?](#)

Winfried Scharlau at the Mathematisches Forschungsinstitut Oberwolfach (MFO)

J Mathe & Comp Appli, 2026

Volume 5(2): 16-136

Om Systemer af konjugerede Substitutioner, der kunne tilhøre irreduktible Ligninger, hvis Grad er Primal

(see <https://www.biodiversitylibrary.org/bibliography/62508> and <https://ia800501.us.archive.org/31/items/mobot31753002493077/mobot31753002493077.pdf>)

https://www.biodiversitylibrary.org/bibliography/62508

Title

Forhandling i Videnskabs-selskabet i Christiania

Title Variants

Alternative: Christiania Videnskabs-selskabs forhandling
Alternative: Forh. Vidensk.-Selsk. Kristiania
Alternative: Forhandling i Videnskabs-selskabet
Alternative: Forhandling i Videnskaps-selskabet i Kristiania
Alternative: Kristiania Videnskaps-selskaps forhandling
Alternative: Videnskaps-selskabet forhandling for ...

Related Titles

Succeeded by: [Avhandling \(Norske videnskaps-akademii i Oslo, II.-Hist.-filos. klasse\)](#)
Succeeded by: [Avhandling utgitt av det Norske videnskaps-akademii i Oslo, I. Matematisk-naturvidenskapelig klasse](#)
Succeeded by: [Avhandling utgitt av det Norske videnskaps-akademii i Oslo, II. Historisk-filosofisk klasse](#)
Succeeded by: [Norske videnskaps-akademii i Oslo. Årbok](#)
Succeeded by: [Norske videnskaps-akademii i Oslo. Årbok](#)
Succeeded by: [Avhandling utgitt av det Norske videnskaps-akademii i Oslo](#)
With: [Oversigt over Videnskabs-selskabets meder](#)

By

[Christiania videnskabs-selskab, I.-Math.-naturv. klasse](#)
[Norske videnskaps-akademii i Oslo](#)
[Christiania videnskabs-selskab, I.-Math.-naturv. klasse](#)

Type

Journal

Cite This Publication

Volumes

- + 1858 >
- + 1859 >
- + 1860 >
- + 1861 >
- + 1862-63 >
- + 1864-65 >
- 1866-67 >

Holding Institution:
Missouri Botanical Garden,
Peter H. Raven Library

Sponsor:
Missouri Botanical Garden

Date Scanned:
02/10/2014

[View Volume](#)

Copyright & Usage:

Copyright Status: Public domain. The BHL considers that this work is no longer under copyright protection.

Download: [All](#) [PDF](#) [OCR](#) [PDI](#)

Peter Ludvig Sylow (1832–1918) entwickelte seine berühmten Sätze über endliche Gruppen zwar schon um 1862–1864, veröffentlichte sie jedoch nicht sofort. Der Durchbruch und die Publikation seiner Ergebnisse in der Fachzeitschrift *Mathematische Annalen* erfolgten erst später, im Jahr 1872.

Obwohl oft von einer Arbeit um 1867 die Rede ist (oft im Kontext von Vorlesungen oder der Entwicklung der Gruppentheorie), gilt:

- Der originale Artikel (Englisch/Französisch): Sylows grundlegende Arbeit ist auf Französisch verfasst und trägt den Titel "Théorèmes sur les groupes de substitutions" (Theoreme über Substitutionsgruppen), erschienen in *Math. Ann.* 5, S. 584–594, 1872.
- Inhalt: Sylow bewies, dass für eine endliche Gruppe G , deren Ordnung durch p^n (wobei p eine Primzahl ist) teilbar ist, eine Untergruppe der Ordnung p^n existiert. Zudem zeigte er, dass alle diese sogenannten Sylow-Untergruppen zueinander konjugiert sind und ihre Anzahl kongruent zu 1 modulo p ist.
- Kontext 1867: Um diese Zeit (Ende der 1860er) war Sylow mit der Arbeit an den Manuskripten und der Vorbereitung seiner Theoreme beschäftigt, stand aber in Kontakt mit Camille Jordan, dessen Werk "Traité des substitutions" (1870) Sylows Ergebnisse teilweise vorwegnahm, was die Publikation verzögerte.

Zusammenfassend: Die bahnbrechenden Ergebnisse wurden von Sylow in den 1860ern erarbeitet, aber die Publikation erfolgte als 10-seitige Abhandlung im Jahr 1872.

Ludwig Sylow (1832–1918) veröffentlichte seine bahnbrechenden Ergebnisse, die als Sylow-Sätze bekannt sind, nicht direkt im Jahr 1867, sondern seine Arbeit begann in dieser Zeit, während der Höhepunkt seiner Veröffentlichungen in den frühen 1870er Jahren lag.

Hier sind die zentralen Fakten zu Sylows Wirken um 1867:

- Der Ursprung (1867): Es handelt sich um die Arbeit "Om Systemer af konjugerede Substitutioner" (Über Systeme konjugierter Substitutionen), die im *Videnskabs-selskabet i Kristiania Forhandling* im Jahr 1867 erschien. In dieser Arbeit untersuchte er die Grundlagen der Gruppentheorie, insbesondere permutierende Untergruppen.
- Die Sylow-Sätze (1872): Die formale, detaillierte Beweisführung seiner drei berühmten Sätze über die Existenz und Konjugiertheit von Untergruppen von Primzahlpotenzordnung (Sylow-Untergruppen) veröffentlichte er später, insbesondere in der Arbeit "Théorèmes sur les groupes de substitutions" in den *Mathematischen Annalen* (1872).
- Historische Bedeutung: Sylows Arbeit um 1867–1872 war eine direkte Weiterentwicklung von Ideen aus Galois' Arbeiten (1820er) und Cauchy's Theorem (1845). Er erweiterte den Satz von Lagrange, indem er bewies, dass eine Gruppe der Ordnung $p^n m$ (wobei p nicht m teilt) immer Untergruppen der Ordnung p^n besitzt.

Obwohl 1867 das Jahr einer seiner frühesten Publikationen zu diesem Thema ist, werden die "Sylow-Sätze" meist mit seinem Hauptwerk von 1872 assoziiert.



Fristaden Christiania (Freetown Christiania, see https://en.wikipedia.org/wiki/Freetown_Christiania)

FORHANDLINGER

I

VIDENSKABS-SELSKABET

I CHRISTIANIA

AAR 1867.

MED 13 LITHOGRAPHEREDE PLADER.

Christiania 1868.

Trykt i Brøgger & Christie's Bogtrykkeri.

I Commission hos Jac. Dybwad.

Indhold.

Foredrag og Afhandlinger.

a. Meddeelte fuldstændigt eller i Udtog:

	Side.
Om Ni-Tallet, af C. A. Holmboe	1—8
En Text-Emendation til Melissi fragmenta, af Lyng	9
Om et nyt Led i Glycocolrækken, af Lindgaard	9—10
— Muskel-Sammentrækning, af C. Boeck	10—11
En Notits om Øen Maaln, af Sexe	12—15
Om Kometer og Stjernesked, af Fearnley	15—16. 25
Emendation til Gaji instt. 2, 181, af Aubert senior	17—18
Om det 22de ægyptiske Dynasti, af Lieblein	18—19
— Echinodermer og Coelenterater, fundne ved Lofoten, af M. Sars	19—23
— to nye Arter Bryozoe, af Danielssen	23—24
— Ruslands ældre Vægtsystem, af Holmboe	25—36
— Haymari Monachi de expugnata Accone liber tetrastichas ed. Riant, (en Text-Emendation), af Monrad	36
— Pythagoreismen, af Lyng	38—44
Ny Fortolkning af et Sted i Platons Phædrus (p. 241 E.), af Monrad	44—49
Fossiler fra Skotlands og Nordamericas Glacial-Formation, af M. Sars	51—58
Oversigt over det meteorologiske Instituts Organisation og Arbejder, af Mohn	58—63
Om Gravhøje, hvori mere end eet Kammer og mere end een Urne er funden, af Holmboe	63—80
— Artsbegrebet i Planteriget, af Schübeler	82
Æsthetisk Bemærkning angaaende Krumningen af Horizontalliniene paa de doriske Templer i Athen, af Monrad	82—90
Om Conglomeraterne i det thronhjemske Skifer-Felt og deres Vidnesbyrd ligeoverfor Omvandlings-Theorien, af Kjerulf	90—95
— russiske Rubel-Barrer, af Holmboe	95—100
— Lysets Indflydelse paa Plantelivet, af Christie	100—105
Discussion over samme Emne	210—212
Om Systemer af conjugerede Substitutioner, der kunne tilhøre irreductible Ligninger, hvis Grad er Primtal, af Sylow	105—122
— en usædvanlig Bevægelse af Havet paa Norges Vestkyst den 7 Mai 1867, af Mohn	123—129
— Anaxagoras's Plads i Philosophiens Historie, af Lyng, samt Medbemærkning, af Monrad	129—135
— de ægyptiske Skarabæers Vægt, af Lieblein	135—139
Bidrag til Legemernes Molekylar-Theorie	140—146, 159—169
Om Flaghougen paa Karmøen og de buddhistiske Tøper i Asien, af Holmboe	146—155
— et geologisk Profil fra Rigsgrænsen over Lyngen til Kvalø, af K. Pettersen	155—158
— Tordenvær i Norge i Sommeren 1867, af Mohn	169—201
— Forskjellen mellem Parmenides og Melissos, af Lyng	202—204
Et nyt Bidrag til Danmarks Reformationshistorie, af L. L. Daae	204—210
Om Finnmarkens Geologi, af T. Dahl	213—222

IV	
b. Uden her meddeelt Udvikling af Indholdet.	
Angaaende den 32te Psalme, af Caspari	9
Om Balænoptera musculus, af G. O. Sars	11
— Begrebet af Christendommen som den absolute Religion, af Monrad	15
— Russisk Laplands geographiske Forholde, af L. K. Daa	19, 139
— Daabs-Spørgsmaalene i den mozarabisk-spanske Kirke, af Caspari	36
— en Sygdom hos Grantræet, af C. Boeck	51
— Nadverens Indstiftelsesords liturgiske Historie, af Caspari	80
— nogle norske Rune-Indskrifter, af Bugge	129
— Karyatiderne paa Erechtheion, af Monrad	202
Blandede Meddelelser.	
Anmerkninger angaaende det forrige Aars trykte Forhandling, af E. S. mark og Sars	16, 36—38
Indvotering af nye Medlemmer	16
Om Selskabets Virksomhed i 1866	49—51
Digt i Anledning af Prinds Oscars Nærværelse, af A. Munch	80—82
Valg paa Selskabets Embedsmænd for 1868	213
Gaver til Selskabets Bibliothek	222—224
Selskabets Medlemmer i 1867	225

https://de.wikipedia.org/wiki/Peter_Ludwig_Mejdell_Sylow


WIKIPEDIA
 Die freie Enzyklopädie

Peter Ludwig Mejdell Sylow

Peter Ludwig Mejdell Sylow, genannt Ludwig bzw. Ludvig Sylow, (* 12. Dezember 1832 in Christiania, heute Oslo; † 7. September 1918 ebenda) war ein norwegischer Mathematiker, der grundlegende Arbeiten zur Gruppentheorie verfasste.

Leben [Bearbeiten | Quelltext bearbeiten]

Sylow war der Sohn von Thomas Edvard von Westen Sylow (1792–1875), einem Hauptmann der Kavallerie und später Kriegsminister der norwegischen Regierung, und von Magdalena Cecilie Cathrine Mejdell (1806–1898), die insgesamt zehn Kinder hatten, von denen Ludvig Sylow der Älteste war.

Sylow besuchte bis 1850 die Kathedralschule in Oslo (damals Christiania) und studierte an der Universität Oslo (damals: Universität Christiania) und gewann 1853 einen Mathematikwettbewerb. 1856 erhielt er seinen Abschluss als Lehrer für Mathematik und Naturwissenschaften. Danach unterrichtete er, da es keine Stellen an der Universität gab, an der Hartvig Nissen Schule in Oslo (einer unabhängigen Mädchenschule, gegründet von Sylows Mathematikprofessor Ole Jacob Broch und dessen Freund Hartvig Nissen) und von 1858 bis 1898 unterrichtete er an der Schule von Fredrikshald (Halden). Als Schullehrer war er weniger erfolgreich, da er hauptsächlich an höherer Mathematik interessiert war und Probleme mit der Disziplin in den Klassen hatte. 1861 besuchte er mit einem Reisestipendium Berlin, wo er mit Leopold Kronecker diskutierte, aber die Vorlesungen von Karl Weierstraß nicht besuchen konnte, da dieser krank war, und Paris, wo er bei Michel Chasles, Joseph Liouville und Jean-Marie Duhamel studierte. Weder in Paris noch in Berlin besuchte er Algebra-Vorlesungen. 1862/63 war er ersatzweise für Broch Dozent an der Universität Christiania, wo er die Galois-theorie unterrichtete. Darin fanden sich noch nicht die nach ihm benannten 1872 veröffentlichten Sätze, aber eine Frage in diesem Zusammenhang (ob es nicht nur zu Primzahlen, die die Ordnung einer Gruppe teilen, Untergruppen gibt, sondern wie es für den Fall von Primzahlpotenzen aussieht). Seine Vorlesungen wurden vom Studenten Sophus Lie besucht. Borch wollte, dass er auch danach Vorlesungen für ihn übernahm, die Schule von Sylow erteilte aber keine Freigabe. Seine ersten Chancen auf eine Universitätsprofessur kam 1869 für die Nachfolge von Borch, die Universität hielt aber eine Stelle in reiner Mathematik für nicht angezeigt und bevorzugte angewandte Mathematiker, so dass der Lehrstuhl an Carl Anton Bjerknes ging. Schließlich erhielt er auf Initiative von Sophus Lie 1898 einen für ihn speziell geschaffenen Lehrstuhl an der Universität Oslo. Obwohl er damals schon 65 Jahre alt war, unterrichtete er 20 Jahre lang an der Universität.

Die drei nach ihm benannten Sylow-Sätze bewies er 1872, er hatte sie aber schon im September 1870 bewiesen. Zuvor hatte Augustin-Louis Cauchy 1845 bewiesen, dass jede endliche Gruppe Untergruppen zu jeder Ordnung hatte, die eine Primzahl war und die Ordnung der Gruppe teilte. Die Sylow-Sätze waren die erste Erweiterung dieses Satzes und eines der ersten wichtigen Ergebnisse der abstrakten Gruppentheorie. Daneben veröffentlichte er über elliptische Funktionen (speziell deren komplexe Multiplikation), angeregt durch die Arbeiten von Niels Henrik Abel und Carl Gustav Jacobi, die er über seinen Mathematikprofessor Ole Jacob Broch kennenlernte. Er war auch an Abels Aufsatz über die Auflösbarkeit von algebraischen Gleichungen durch Radikale interessiert und kam über seinen Professor Carl Anton Bjerknes von dort zur Galois-theorie. Sylow benutzte beim Beweis seiner Sätze, die aus Sylows Analyse der Arbeit von Galois entstanden, Methoden der Galois-theorie (Winfried Scharlau).

In den 1870er Jahren stand er in Briefwechsel mit Julius Peter Christian Petersen.



Sylow

Zusammen mit Sophus Lie gab Sylow zwischen 1873 und 1881 das gesamte Werk von Niels Henrik Abel heraus, wobei viele Arbeiten erstmals publiziert wurden (es gab schon zuvor (1839) eine Ausgabe gesammelter Schriften von Abel von Bernt Michael Holmboe, dem Vorgänger von Broch an der Universität Oslo). Laut Lie hatte Sylow die maßgebliche Arbeit dazu geleistet und die ersten vier Jahre war er dafür von der Schule beurlaubt. Die Arbeit wurde auf Anregung der Norwegischen Akademie der Wissenschaften vom Parlament finanziert. 1902 veröffentlichte er mit Elling Holst den Briefwechsel von Abel. Sylow hatte schon zuvor unveröffentlichte Arbeiten von Abel zur Veröffentlichung an das Crelle'sche Journal in Berlin geschickt, wo der Herausgeber Leopold Kronecker allerdings die Veröffentlichung ablehnte, da er inzwischen selbst die Ergebnisse unabhängig entdeckt hatte. 1902 hielt Sylow den Eröffnungsvortrag zur Zweihundertjahrfeier von Abels Geburt und auf dem dritten skandinavischen Mathematikerkongress 1913 in Oslo stellte er neu entdeckte Dokumente zu Abel vor.

1883 wurde er zum korrespondierenden Mitglied der Göttinger Akademie der Wissenschaften gewählt.^[1] 1894 wurde Sylow Herausgeber der *Acta Mathematica* und erhielt die Ehrendoktorwürde der Universität Kopenhagen.^[2]

Sylow heiratete nie. Sein Charakter wurde als humorvoll und warmherzig beschrieben. In den Sommermonaten war er meist in den Bergen, insbesondere in Kongsvoll zwischen Oslo und Trondheim, zum Wandern und Sammeln von Pflanzen.

https://de.wikipedia.org/wiki/Peter_Ludwig_Meidell_Sylow

Hr. Bjerknes fremlagde følgende af Hr. Sylow indsendte Afhandling: Om Systemer af konjugerede Substitutioner, der kunne tilhøre irreduktible Ligninger, hvis Grad er Primtal.¹

Efter Galois berømte Theori bestaar Betingelsen for, at en rational Funktion af Rødderne i en algebraisk Ligning skal kunne udtrykkes rationalt ved Koefficienterne og andre som bekjendte antagne Størrelser, deri, at Funktionens numeriske Værdi maa forblive den samme, naar man ombytter Rødderne med hinanden paa visse Maader. Disse Ombytninger eller Substitutioner danne, hvad Cauchy har kaldt, et „System af konjugerede Substitutioner“, d. e. hvilkesomhelst to af dem, udførte efter hinanden i en hvilkesomhelst Permutation af Rødderne, frembringe samme Resultat, som om man havde udført en vis tredie af Systemets Substitutioner. Galois tænker sig Systemets Substitutioner definerede ved en „Gruppe“ af Permutationer, som gaa over til hinanden ved Substitutionerne. Ligninger, der under samme Forudsætning have samme System af konjugerede Substitutioner eller samme Gruppe, have saaledes væsentlige Egenskaber fælles og kunne derfor opfattes som en særegen Klasse. Paa den anden Side kan man ogsaa bevise, at der til ethvert givet System af konjugerede Substitutioner findes tilsvarende Ligninger. Det vilde saaledes være en Sag af stor Betydning for de algebraiske Ligningers Theori, om man kunde angive, hvilke Systemer af konjugerede Substitutioner der kunne henhøre til Ligninger af en

¹ Optages i Selskabets Forhandlinger ifølge Bedømmelse afgiven af DHrr. Dr. O. J. Broch og Bjerknes.

given Grad, og især hvilke der henhøre til irreduktible Ligninger. Dette Problem, saavel som andre Problemer, der staa i Forbindelse med dette, er derfor ogsaa bleven behandlet af flere udmærkede Mathematikere, uden at det imidlertid er lykkedes at opløse det.

For de ved Rodtegn opløselige Ligninger har Problemet vist sig at være langt lettere, naar Graden er Primtal, end naar den er et sammensat Tal. Denne Omstændighed gjør det sandsynligt, at et lignende Forhold finder Sted for de ved Rodtegn uopløselige Ligningers Vedkommende. Idet jeg saaledes har indskrænket Undersøgelsen til irreduktible Ligninger af Primtalgrad, er det blandt Andet lykkedes mig at fuldstændiggjøre nogle Resultater, der ere fundne af Mathieu (*Mémoire sur l'étude des fonctions de plusieurs quantités* etc. Liouville's Journal 1861). Da imidlertid den Udvikling, der har ledet mig hertil, tildels er forskjellig fra Mathieu's, har jeg troet at burde fremsætte den i sin Helhed.

I det Følgende skal jeg bruge de samme Betegnelser, som findes anvendte i 3die Udgave af Serret's *Cours d'algèbre supérieure*. Jeg betegner saaledes Ligningens Rødder med samme Bogstav, x , forsynet med Indexer tagne efter Modulen n , idet n betegner Ligningens Grad; en Substitution af Rødderne betegnes ved at angive, hvilken Substitution af disse Indexer den medfører. Naar en Substitution betegnes med et Bogstav, tænker jeg mig dette som et Funktionsmærke, hvorved den ved Substitutionen fremkomne Index udtrykkes ved Hjælp af den oprindelige. Ved Substitutionen φ forstaaes altsaa det Samme som ved Substitutionen $\left(\varphi \atop k\right)$, hvor da $\varphi(k)$ betegner en vis Funktion af saadan Natur, at den, naar k antager Værdierne $0\ 1\ 2\ \dots\ (n-1)$, selv bliver kongruent (mod n) med de samme Tal i en eller anden Orden. Jeg tænker mig fremdeles det System af konjugerede Substitutioner, der tilhører den givne Ligning, defineret ved en Gruppe af Permutationer, for, naar Saadant maatte være fornødent, at kunne tale ligesaavel om de Permutationer, der ved Systemets Substitutioner fremgaa af hinanden, som om Substitutionerne selv.

Schönemann¹ og senere Mathieu² have bevist, at naar en irreduktibel Lignings Grad er et Primtal n , maa det Ligningen tilhørende System af konjugerede Substitutioner indeholde en cirkulær Substitution af de n Rødder. Lad denne være betegnet med θ , og lad Rødderne være betegnede med $x_0 x_1 x_2 \dots x^{n-1}$ i en saadan Orden, at man har

$$\theta = (0\ 1\ 2\ \dots\ (n-1)) \text{ d. e. } \theta = \begin{pmatrix} k+1 \\ k \end{pmatrix};$$

det Ligningen tilhørende System af konjugerede Substitutioner indeholder da ogsaa alle Potenser af θ . For Kortheds Skyld vil jeg benævne en cirkulær Substitution tilligemed dens Potenser et Sæt af cirkulære Substitutioner. Er Ligningen opløselig ved Rodtegn, da indeholder Systemet kun dette ene Sæt; omvendt ved man ogsaa, at hvis det Ligningen tilhørende System af konjugerede Substitutioner kun indeholder et Sæt cirkulære Substitutioner, da er Ligningen opløselig ved Rodtegn. Hvis derfor Ligningen ikke er opløselig ved Rodtegn, maa der i Systemet findes mere end et Sæt cirkulære Substitutioner; der maa altsaa findes en cirkulær Substitution θ' saadan, at man ikke har:

$$\theta' = \theta^a$$

for nogen Værdi af a . Man kan da heller ikke have

$$\theta'^a = \theta^b,$$

med mindre saavel a som b ere divisible med n , hvorved θ'^a og θ^b blive $= 1$, d. e. betegne, at ingen Forandring sker i Røddernes Plads. Thi af $\theta'^a = \theta^b$ følger $\theta'^{ac} = \theta^{bc}$; da nu n er Primtal,

¹ Über die Beziehungen, welche zwischen den Wurzeln irreduktibeler Gleichungen stattfinden etc. i 5te Bind af Denkschriften der math.-naturw. Classe der kaiserlich. Acad. Wien. Schönemann forudsætter, at Ligningens Koefficienter ere rationale Tal; denne Indskrænkning er imidlertid ikke væsentlig for Beviset. Dette Beviis er vistnok et af de væsentligste Fremskridt. Theorien har gjort siden Galois's Død; navnlig er herved for første Gang, saavidt jeg ved, en af de vigtigste Lakuner i Galois's „Memoire sur les conditions de résolubilité des équations par radicaux“ bleven udfyldt, nemlig den i Proposition VIII, hvor der uden Bevis forudsættes, at Gruppen maa indeholde en Cirkelombytning.

² I den ovenfor nævnte Afhandling „Memoire sur l'étude des fonctions de plusieurs quantités“ Liouville's Journal Aar 1861. Pag. 304.

kunde man, hvis ikke $a \equiv 0 \pmod{n}$, sætte $ac \equiv 1 \pmod{n}$ eller $c \equiv \frac{1}{a}$, hvorved man fik

$$\theta^i = \theta^{\frac{b}{a}}$$

hvilket er mod Betingelsen. Ligningens System af konjugerede Substitutioner maa nu indeholde Substitutionen $\theta^{ia} \cdot \theta^r \cdot \theta^{i-a}$, eller for at bruge Betti's Udtryksmaade, den afledede af θ^r ved Hjælp af θ^{ia} ; den er som afledet ligedannet med θ^r , altsaa cirkulær. Man bemærker nu for det Første, at man har

$$\theta^{ia} \cdot \theta^r \cdot \theta^{i-a} = (\theta^{ia} \cdot \theta \cdot \theta^{i-a})^r;$$

de Substitutioner af Formen $\theta^{ia} \cdot \theta^r \cdot \theta^{i-a}$, i hvilke a har samme Værdi, danne altsaa et Sæt af cirkulære Substitutioner, der saaledes kan siges at være afledet af Sættet θ^r ved Hjælp af θ^{ia} . For det Andet ere de n Sæt

$$\theta^r, \theta^i \theta^r \theta^{i-1}, \theta^{i^2} \theta^r \theta^{i-2}, \theta^{i^3} \theta^r \theta^{i-3}, \dots, \theta^{i^{(n-1)}} \theta^r \theta^{i-(n-1)}$$

forskjellige fra hinanden saavel som fra θ^r . Var nemlig

$$\theta^{ia} \cdot \theta^r \cdot \theta^{i-a} = \theta^{is},$$

$$\text{fulgte strax } \theta^r = \theta^{is},$$

hvilket er umuligt. Var derimod

$$\theta^{ia} \cdot \theta^r \cdot \theta^{i-a} = \theta^{ib} \cdot \theta^s \cdot \theta^{i-b},$$

$$\text{fulgte } \theta^r = \theta^{i(b-a)} \theta^s \cdot \theta^{i-(b-a)},$$

$$\text{hvoraf } \theta^{\frac{r}{s}} = \theta^{i(b-a)} \cdot \theta \cdot \theta^{i-(b-a)}.$$

Denne Ligning udsiger, at θ ved Afledning ved Hjælp af $\theta^{i(b-a)}$ gaar over til en af sine Potenser. Men nu ved man, at enhver Substitution, der ved Afledning forandrer $\binom{k+1}{k}$ til en af dens Potenser, selv maa være af Formen $\binom{ck+d}{k}$; denne Substitution er kun cirkulær, hvis $c \equiv 1 \pmod{n}$. Man maatte saaledes have:

$$\theta^{i(b-a)} = \binom{k+d}{k} = \theta^d,$$

men dette er umuligt, naar ikke $b \equiv a$. Det er saaledes bevist, at θ^r og $\theta^{ia} \theta^r \theta^{i-a}$ repræsentere $n+1$ Sæt cirkulære Substitutioner; hvis altsaa Ligningens System af konjugerede Substitutioner indeholder mere end et Sæt cirkulære Substitutioner, da indehol-

der det mindst $n + 1$ Sæt. Indeholder det imidlertid flere end disse, være θ_1 en ny cirkulær Substitution. Systemet indeholder da de n Sæt, der ere udtrykte ved

$$\theta'^a \cdot \theta_1^r \cdot \theta'^{-a};$$

disse ere som ovenfor bevist indbyrdes forskellige og forskellige fra θ'^r . Men de ere ogsaa forskellige fra Sættene $\theta'^a \theta^r \theta'^{-a}$; thi havde man:

$$\theta'^a \theta_1^r \theta'^{-a} = \theta'^b \theta^s \theta'^{-b},$$

$$\text{saa fulgte } \theta_1 = \theta'^{(b-a)} \theta^{\frac{s}{r}} \theta'^{-(b-a)},$$

d. e. θ_1 hørte selv til et af de foregaaende Sæt, hvilket er mod vor Forudsætning. Indeholder saaledes Systemet flere end hine $n + 1$ Sæt, da har det mindst $2n + 1$: har det endnu flere, ser man paa samme Maade, at det mindst har $3n + 1$ o. s. v. Paa denne Maade kan man vedblive at ordne de Systemet tilhørende cirkulære Substitutioner, indtil de ere udtømte; Antallet af de forskellige Sæt maa altsaa være af Formen $np + 1$. De ved Rodtegn opløselige Ligninger ere indbefattede heri, idet de svare til $p = a$.

Hvis θ ved Afledning ved Hjælp af hvilkensomhelst af Systemets Substitutioner gik over til en Potens af sig selv, maatte Systemets Substitutioner som bekjendt alle være af Formen

$$\left(\begin{matrix} ak + b \\ k \end{matrix} \right),$$

og Ligningen hørte til de ved Rodtegn opløselige. Hører den altsaa ikke til disse, maa Systemet indeholde en saadan Substitution φ , at $\varphi\theta\varphi^{-1}$ ikke hører til Sættet θ^r . Da Valget af den cirkulære Substitution, som vi have betegnet med θ' , er ganske vilkaarligt, kunne vi forudsætte:

$$\theta' = \varphi\theta\varphi^{-1}.$$

Sættet θ'^r lader sig da altsaa aflede af Sættet θ^r ved Hjælp af en af Systemets egne Substitutioner; det samme gjælder om Sættene $\theta'^a \theta^r \theta'^{-a}$. Indeholder nu Systemet flere Sæt cirkulære Substitutioner, der kunne afledes af θ^r ved Hjælp af Systemets egne Substitutioner end disse $n + 1$, kunne vi antage at θ_1 har samme Egenskab. Man har da:

$$\theta_1 = \psi \theta \psi^{-1},$$

hvor ψ tilhører Systemet. Heraf følger

$$\theta'^a \theta_1^r \theta'^{-a} = \theta'^a \psi \theta^r \psi^{-1} \theta'^{-a} = (\theta'^a \psi) \theta^r (\theta'^a \psi)^{-1}.$$

Da θ'^a og ψ tilhøre Systemet, maa deres Produkt $\theta'^a \psi$ ogsaa tilhøre Systemet; man ser saaledes, at samtlige Sæt $\theta'^a \theta_1^r \theta'^{-a}$ lade sig aflede af Sættet θ^r ved Systemets egne Substitutioner. Man kan derfor gjentage det foregaaende Ræsonnement og den foregaaende Ordning af de cirkulære Substitutioner, idet man indskrænker sig til de Sæt, der kunne afledes af θ^r ved Substitutioner, der tilhøre Systemet. Antallet af disse Sæt er saaledes ogsaa af Formen $np + 1$. Det skal nedenfor vises, at man herved i Virkeligheden faar alle cirkulære Substitutioner.

Man kan af Sættet θ^r aflede et andet ved Hjælp af hvilken som helst Substitution, der tilhører Systemet; men af disse afledede Sæt kunne flere falde sammen med hinanden, eller med θ^r . For at opnaa en Relation mellem Antallet af Systemets Substitutioner, d. e. Systemets Orden, og Antallet af Sæt af cirkulære Substitutioner, der kunne afledes af θ^r ved Systemets Substitutioner, ville vi undersøge, hvormange af disse sidste kunne give samme afledede Sæt. Lad til den Ende φ og ψ være to hvilken som helst Substitutioner, ved hvilke der af θ^r afledes samme Sæt. Man har da

$$\psi \theta \psi^{-1} = \varphi \theta^a \varphi^{-1},$$

og omvendt er dette tilstrækkeligt, for at de afledede Sæt skulle være identiske. Nu er:

$$\psi \theta \psi^{-1} = (\psi(0) \psi(1) \psi(2) \dots \psi(n-1))$$

$$\varphi \theta^a \varphi^{-1} = (\varphi(0) \varphi(a) \varphi(2a) \dots \varphi(n-1)a).$$

Hvis derfor $\psi(0) = \varphi(ma)$, maa man have:

$$\psi(1) = \varphi((m+1)a), \psi(2) = \varphi((m+2)a), \dots, \psi(k) = \varphi((m+k)a).$$

Sættes altsaa $ma \equiv b \pmod{n}$, bliver

$$\psi(k) = \varphi(ak + b).$$

De Substitutioner, der af $\binom{k+r}{k}$ aflede samme Sæt, som $\binom{\varphi(k)}{k}$, ere altsaa de, der indeholdes i Udtrykket $\binom{\varphi(ak+b)}{k}$, alle disse, og ingen andre. Tilhører nu φ Systemet, saa blive de

Substitutioner i Systemet, der fyldestgjøre den omtalte Betingelse, de samme som de, der ere af Formen $\left(\varphi(ak+b) \atop k\right)$. Men tilhører baade $\left(\varphi(ak+b) \atop k\right)$ og φ Systemet, da gjælder det samme om Produktet $\varphi^{-1} \cdot \left(\varphi(ak+b) \atop k\right)$ eller $\left(ak+b \atop k\right)$; omvendt, hvis φ og $\left(ak+b \atop k\right)$ tilhører Systemet, da er det samme Tilfældet med $\left(\varphi(ak+b) \atop k\right)$. Antallet af hine Substitutioner er derfor lig Antallet af Substitutioner i Systemet, der ere af Formen $\left(ak+b \atop k\right)$.

Da Systemet indeholder Substitutionen $\left(k+1 \atop k\right)$ og dens Potenser, ser man, at Konstanten b kan have alle n Værdier; ligeledes ser man, at hvis Systemet indeholder Substitutionen $\left(ak+b \atop k\right)$ for en Værdi a , da indeholder det ogsaa Substitutionen $\left(ak \atop k\right)$ for samme Værdi, og omvendt. For nærmere at undersøge, hvilke Værdier a kan have, ville vi ved ε betegne en primitiv Rod til Primtallet n og antage, at Systemet indeholder Substitutionen $\left(\varepsilon^{\alpha} \cdot k \atop k\right)$; det indeholder da enhver Potens af denne, altsaa enhver Substitution af Formen $\left(\varepsilon^{\xi \alpha} \cdot k \atop k\right)$. Er nu α' den største fælles Faktor for α og $n-1$, kan man sætte:

$$\xi \alpha \equiv \alpha' \pmod{n-1},$$

hvorved man faar: $\varepsilon^{\xi \alpha} = \varepsilon^{\alpha'} \pmod{n}$;

sættes endvidere $n-1 = \alpha' \cdot \alpha''$,

ser man, at Systemet indeholder følgende Række af α'' Substitutioner:

$$(1) \dots \left(k \atop k\right) \left(\varepsilon^{\alpha'} k \atop k\right) \left(\varepsilon^{2\alpha'} \cdot k \atop k\right) \dots \left(\varepsilon^{(\alpha''-1)\alpha'} \cdot k \atop k\right).$$

Indeholder Systemet flere Substitutioner af Formen $\left(ak \atop k\right)$ end disse, f. Ex. $\left(\varepsilon^{\beta} \cdot k \atop k\right)$, maa det paa samme Maade indeholde en lignende Række af Substitutioner:

$$(2) \dots \left(k \atop k\right) \left(\varepsilon^{\beta'} k \atop k\right) \left(\varepsilon^{2\beta'} \cdot k \atop k\right) \dots \left(\varepsilon^{(\beta''-1)\beta'} \cdot k \atop k\right),$$

hvor β' betegner den største fælles Faktor for β og $n-1$, og hvor

$n-1 = \beta' \cdot \beta''$. Det maa da ogsaa indeholde enhver Substitution af Formen:

$$\left(\begin{smallmatrix} \varepsilon^{\xi\alpha' + \eta\beta'} \cdot k \\ k \end{smallmatrix} \right).$$

Nu kan man altid give ξ og η saadanne Værdier, at

$$\xi\alpha' + \eta\beta' \equiv \zeta\gamma \pmod{n-1},$$

hvor ζ er vilkaarlig og γ betegner den største fælles Faktor for α' og β' . Systemet indeholder altsaa følgende Række af γ' Substitutioner

$$\left(\begin{smallmatrix} k \\ k \end{smallmatrix} \right) \left(\begin{smallmatrix} \varepsilon^{\gamma} \cdot k \\ k \end{smallmatrix} \right) \left(\begin{smallmatrix} \varepsilon^{2\gamma} \cdot k \\ k \end{smallmatrix} \right) \dots \dots \left(\begin{smallmatrix} \varepsilon^{(\gamma'-1)\gamma} \cdot k \\ k \end{smallmatrix} \right), \text{ hvor } \gamma \cdot \gamma' = n-1.$$

Denne Række indeholder alle Substitutioner i (1) og (2). Paa denne Maade kan man vedblive, til man har udtømt alle Systemets Substitutioner af Formen $\left(\begin{smallmatrix} ak \\ k \end{smallmatrix} \right)$. Alle disse Substitutioner ere saaledes Potenser af en eneste Substitution; er deres Antal v , maa v være en Divisor af $n-1$; sættes $n-1 = v \cdot v'$, kunne de skrives saaledes:

$$\left(\begin{smallmatrix} k \\ k \end{smallmatrix} \right) \left(\begin{smallmatrix} \varepsilon^{v'} \cdot k \\ k \end{smallmatrix} \right) \left(\begin{smallmatrix} \varepsilon^{2v'} \cdot k \\ k \end{smallmatrix} \right) \dots \dots \left(\begin{smallmatrix} \varepsilon^{(v-1)v'} \cdot k \\ k \end{smallmatrix} \right).$$

De Værdier, som a kan have, ere altsaa $1, \varepsilon^{v'}, \varepsilon^{2v'} \dots \varepsilon^{(v-1)v'}$, d. e. alle Tal af Formen $a^{v'}$. De Substitutioner af Formen $\left(\begin{smallmatrix} ak+b \\ k \end{smallmatrix} \right)$, som Systemet indeholder, ere altsaa udtrykte ved $\left(\begin{smallmatrix} a^{v'} \cdot k+b \\ k \end{smallmatrix} \right)$, og deres Antal er $n \cdot v$.

Efter hvad ovenfor er sagt, er saaledes Antallet af de Substitutioner i Systemet, ved Hjælp af hvilke man af θ^r kan aflede et givet andet Sæt af cirkulære Substitutioner, lig $n \cdot v$, hvilket ogsaa er Antallet af dem, ved hvilke Sættet θ^r afledes af sig selv. Er nu Antallet af de Sæt, der ved Hjælp af Systemets Substitutioner kunne afledes af θ^r , lig $np+1$, bliver altsaa Systemets Orden lig $(np+1) \cdot n \cdot v$.

Det var tænkeligt, at der gaves flere Sæt cirkulære Substitutioner, end de nævnte $np+1$. Lad derfor θ^r være et Sæt, der ikke kan afledes af θ^r ved nogen af Systemets Substitutioner. Da det er ligegyldigt, hvilken af Systemets cirkulære Substitutioner man betegner med $\left(\begin{smallmatrix} k+1 \\ k \end{smallmatrix} \right)$, gjælder det, som ovenfor er bevist

om θ , ogsaa om ϑ . Hvis Antallet af de Sæt, som ved Systemets Substitutioner kunne afledes af ϑ^r , er lig $np_1 + 1$, og Antallet af de Substitutioner, der ved Afledning forandre ϑ til dens Potenser, er $n\nu_1$; idet ν_1 betegner en Divisor af $n-1$, saa er Gruppens Orden lig $(np_1 + 1) \cdot n \cdot \nu_1$. Man har da

$$(np_1 + 1)n \cdot \nu_1 = (np + 1)n \cdot \nu,$$

$$\text{hvoraf } \nu_1 \equiv \nu \pmod{n}, \text{ d. e. } \nu_1 = \nu,$$

hvilket atter medfører $p_1 = p$. De cirkulære Substitutioner, der ved Systemets Substitutioner kunne afledes af ϑ^r , udgjøre altsaa ligesaamange Sæt, som de, der kunne afledes af θ^r ; jeg tilføier, at de ogsaa ere forskellige fra disse. Thi i modsat Fald maatte man have en Identitet af Formen

$$\varphi\theta^r\varphi^{-1} = \psi\vartheta^s\psi^{-1},$$

hvor φ og ψ tilhøre Systemet. Heraf fulgte

$$\vartheta = \psi^{-1} \cdot \varphi \theta^{\frac{r}{s}} \varphi^{-1} \cdot \psi = (\psi^{-1}\varphi) \cdot \theta^{\frac{r}{s}} (\psi^{-1}\varphi)^{-1},$$

d. e. ϑ lod sig aflede af $\theta^{\frac{r}{s}}$ ved Hjælp af $\psi^{-1} \cdot \varphi$, der tilhører Systemet; men dette strider jo mod Forudsætningen. Gaves der altsaa i Systemet flere end $np + 1$ Sæt cirkulære Substitutioner, maatte der mindst gives $2(np + 1)$. Gaves der flere end disse, ser man paa samme Maade, at der mindst maatte gives $3(np + 1)$. Kort, Antallet af forskellige Sæt maatte være et Multiplum af $np + 1$; lad det hede $m(np + 1)$. Men efter hvad ovenfor er bevist, har man da

$$m(np + 1) \equiv 1 \pmod{n}, \text{ d. e. } m \equiv 1.$$

Man kan altsaa sætte

$$m(np + 1) = (nq + 1)(np + 1).$$

Hvert Sæt indeholder nu $n-1$ cirkulære Substitutioner (idet den identiske Substitution fraregnes); det hele Antal af cirkulære Substitutioner bliver saaledes $(nq + 1)(np + 1)(n-1)$, og dette Tal maa være mindre end det hele Antal af Substitutioner; man har saaledes

$$(nq + 1)(np + 1)(n-1) < (np + 1) \cdot n \cdot \nu.$$

Da nu

$$n-1 \geq \nu$$

følger

$$nq + 1 < n, \text{ d. e. } q = 0.$$

Videnak. Selsk. Forh. 1867.

Der gives altsaa ikke flere Sæt cirkulære Substitutioner, end de, der kunne afledes af θ ved Systemets egne Substitutioner. Man erindre her, at den cirkulære Substitution, der er betegnet med $\binom{k+1}{k}$, er valgt ganske vilkaarligt; hvad der er bevist om denne gjælder altsaa ogsaa om enhver anden. Fremdeles bemærkes, at de ved Rødtegn opløselige Ligninger ere indbefattede i den almindelige Regel, i det de svare til Værdien $p = 0$.

Sammenstilles Alt hvad ovenfor er bevist, saa bestaar det altsaa i Følgende:

Tilhører et System af konjugerede Substitutioner en irreduktibel Ligning af Primtalgraden n , maa dets Orden være et Tal af Formen $(np+1)n \cdot \nu$, hvor ν betegner en Divisor af $n-1$. Antallet af de forskjellige Sæt af cirkulære Substitutioner er $np+1$, og hvert af disse kan ved $n \cdot \nu$ af Systemets Substitutioner afledes af et hvilket som helst andet Sæt. Benævnes Rødderne med samme Bogstav med tilføiede Indexer, tagne efter Modulen n , i en saadan Orden, at en af de cirkulære Substitutioner bliver at betegne med $\binom{k+1}{k}$, saa er ν Antallet af Systemets Substitutioner af Formen $\binom{ak}{k}$.

Er det nu end bevist, at Ordenen af ethvert transitivt System af Primtalgraden n maa være af Formen $(np+1)n \cdot \nu$, saa er det allerede paa Forhaand klart, at der ikke gives Systemer af enhver Orden, der er et Tal af denne Form. Da nemlig Ordenen er en Divisor af $2 \cdot 3 \dots n$, maa $(np+1)\nu$ være Divisor af $2 \cdot 3 \dots (n-1)$. Men end ikke naar denne Betingelse er opfyldt, gives der altid Systemer af Ordenen $(np+1)n \cdot \nu$. Allerede 7de Grad giver her paa flere Exempler.

Saaledes bevises let Følgende: *Man kan ikke have $\nu = 1$, naar man undtager Tilfældet $p = 0$, d. e. de Abelske Ligninger.*

Er $\nu = 1$, har Systemet $(np+1)n$ Substitutioner, og af disse ere de $(np+1)(n-1)$ cirkulære; der gives altsaa kun $np+1$ Substitutioner i Systemet, der ikke ere cirkulære. Men nu maa Antallet af de Substitutioner, der lade en hvilkensomhelst Rod x_k uforandret, ogsaa være $= np+1$; de $np+1$ ikke cirkulære Substitutioner lade altsaa en hvilkensomhelst Rod x_k uforandret. Da

Systemet kun har en saadan, den identiske Substitution, sluttet:
 $np + 1 = 1, p = 0$.

Heraf følger endvidere: Naar $p > 0$, d. e. naar man undtager de ved Rodtegn oploselige Ligninger, og n er af Formen $4h + 3$, kan man ikke have $v = 2$.

Systemet maatte nemlig indeholde Substitutionen $\begin{pmatrix} -k \\ k \end{pmatrix}$ eller

$$(1, n-1) (2, n-2) (3, n-3) \dots \left(\frac{n-1}{2}, \frac{n+1}{2} \right),$$

der er sammensat af et ulige Antal Transpositioner. Men nu har man følgende Sætning.

Naar et System af konjugerede Substitutioner indeholder en Substitution, der er sammensat af et ulige Antal Transpositioner, da er dets Orden et lige Tal; den ene Halvpart af dets Substitutioner er sammensat af et ulige Antal Transpositioner, den anden af et lige Antal, og disse sidste udgjøre et fuldstændigt System af konjugerede Substitutioner.

Ere nemlig de af Systemets Substitutioner, der ere sammensatte af et lige Antal Transpositioner:

$$1. \varphi_1 \varphi_2 \dots \dots \dots, \varphi_{r-1} \dots \dots \dots (a),$$

saa er ogsaa $\varphi_i \varphi_k$ en Substitution, der tilhører Systemet og er sammensat af et lige Antal Transpositioner; den er saaledes indbefattet i (a). Substitutionerne (a) danne altsaa et System af konjugerede Substitutioner. Er endvidere ψ og χ to hvilkesomhelst af det oprindelige Systems Substitutioner, der ere sammensatte af et ulige Antal Transpositioner, saa er aabenbart

$$\psi, \psi\varphi_1, \psi\varphi_2, \dots \dots \dots, \psi\varphi_{r-1} \dots \dots \dots (b)$$

r distinkte Substitutioner af samme Slags. Nu er $\psi^{-1}\chi$ sammensat af et lige Antal Transpositioner, altsaa en af Substitutionerne a. Man har altsaa

$$\psi^{-1}\chi = \varphi_k, \chi = \psi\varphi_k$$

Samtlige det oprindelige Systems Substitutioner ere saaledes indbefattede i (a) og (b); deres Antal er saaledes $2r$.

Gaves der et System af Ordenen $(np+1)n.2$, maatte der ogsaa gives et af Ordenen $(np+1)n$, hvilket kun er muligt, hvis $p = 0$.

Naar man vil gjøre sig et Billede af de cirkulære Substitutioners Forhold ved Afledning, kan man tænke sig Ligningen transformeret til en anden, der er saadan, at der til hvert Sæt cirkulære Substitutioner tilhørende den givne Ligning, svarer en Rod i den transformerede. Da de herved fremkomne transformerede Ligninger desuden i andre Henseender ere af Interesse, skal jeg tale noget nærmere om Sagen. Jeg maa herved støtte mig til nogle Sætninger af den almindelige Theori for de algebraiske Ligninger, som jeg skal hidsætte og forsyne med Beviser, da jeg ikke ved at henvise til noget Sted, hvor de findes udviklede.

1. Lad u være en rational Funktion med bekjendte Koefficienter af Rødderne $x_0 x_1 \dots x_{n-1}$ i en algebraisk Ligning, og lad dens numeriske Værdi være uforandret ved en Substitution θ ; hvis nu en Substitution φ af det Ligningen tilhørende System af konjugerede Substitutioner forandrer u til u' , da er den numeriske Værdi af u' uforandret ved den afledede af θ ved Hjælp af φ .

Er nemlig

$$u = f(x_0 x_1 \dots x_{n-1}) = f(x_{\theta(0)} x_{\theta(1)} \dots x_{\theta(n-1)}),$$

maa denne Relation vedblive at gjælde, om man end udfører Substitutionen φ , altsaa er

$$u' = f(x_{\varphi(0)} x_{\varphi(1)} \dots x_{\varphi(n-1)}) = f(x_{\varphi\theta(0)} x_{\varphi\theta(1)} \dots x_{\varphi\theta(n-1)});$$

Man ser saaledes, at u' er uforandret ved Substitutionen

$$\begin{pmatrix} \varphi\theta(k) \\ \varphi(k) \end{pmatrix} \text{ d. e. ved } \varphi \cdot \theta \cdot \varphi^{-1}.$$

2. Hvis man i Funktionen $u_0 = f(x_0 x_1 \dots x_{n-1})$ udfører det Ligningen tilhørende System af konjugerede Substitutioner, faar man et Antal Funktioner, der er lig Systemets Orden, og hvoraf hver svarer til en Permutation i Ligningens Gruppe; af disse kunne imidlertid flere have samme numeriske Værdi. Hvis nu Antallet af de indbyrdes forskellige Værdier af u_0 er m , og Antallet af de til forskellige Permutationer svarende, der ere lige med u_0 , er μ , saa er Ordenen af det Ligningen tilhørende System af konjugerede Substitutioner lig $m \cdot \mu$.

Har man nemlig

$$u_0 = u_0' = u_0'' = \dots = u_0^{(p-1)}$$

hvor $u_0, u_0', \dots, u_0^{(p-1)}$ svare til forskjellige Permutationer, og antager disse Funktioner ved en vis Ligningen tilhørende Substitution Værdierne $u_1, u_1', \dots, u_1^{(p-1)}$, saa har man

$$u_1 = u_1' = u_1'' = \dots = u_1^{(p-1)}.$$

Antallet af de Permutationer, der give Værdien u_1 , er saaledes mindst lig Antallet af dem, der give u_0 . Paa den anden Side indsees ligeledes, at Antallet af dem, der give u_0 , mindst er lig Antallet af dem, der give u_1 ; følgelig er begge Antal lige store, hvorved Paastanden er retfærdiggjort.

3. Kaldes de indbyrdes forskellige Værdier, som u_0 antager ved det Ligningen tilhørende System af konjugerede Substitutioner $u_0, u_1, \dots, u_{m-1}$, saa ere disse Rødder i en irreduktibel Ligning af Graden m , hvis Koefficienter lade sig udtrykke rationalt ved bekendte Størrelser.

Gaar ved en vis Ligningen tilhørende Substitution $\varphi: u_0, u_1, \dots, u_{m-1}$ over til $u_0', u_1', \dots, u_{m-1}'$, maa disse sidste være indbefattede i de første; paa den anden Side maa de være indbyrdes forskellige; thi af $u_i' = u_k'$ fulgte ved Anvendelse af Substitutionen $\varphi^{-1}: u_i = u_k$, hvilket er mod Forudsætningen. Heraf sluttes at $u_0', u_1', \dots, u_{m-1}'$ ere de samme som $u_0, u_1, \dots, u_{m-1}$ i en eller anden Orden. Da saaledes enhver symmetrisk Funktion af $u_0, u_1, \dots, u_{m-1}$ er uforandret ved alle Ligningen tilhørende Substitutioner, har Ligningen

$$F(u) = (u - u_0)(u - u_1) \dots (u - u_{m-1}) = 0$$

Koefficienter, der lade sig udtrykke rationalt ved de bekendte Størrelser. Irreduktibiliteten af denne Ligning godtgjøres saaledes: Er u_0 Rod i en Ligning $F'(u) = 0$, hvis Koefficienter lade sig udtrykke rationalt ved de bekendte Størrelser, saa følger af Relationen

$$F'(u) = 0 \text{ umiddelbart } F'(u_1) = 0, F'(u_2) = 0, \dots, F'(u_{m-1}) = 0.$$

Da en saadan Ligning altsaa maa være af Graden m i det mindste, er $F(u) = 0$ irreduktibel.

4. Det System af konjugerede Substitutioner, der tilhører Ligningen $F(u) = 0$, bestaar af de Substitutioner af Rødderne

$u_0 u_1 \dots u_{m-1}$, der foraarsages, ved at man i disse Størrelser Udtryk som Funktioner af $x_0 x_1 \dots x_{n-1}$ udfører det den givne Ligning tilhørende System af konjugerede Substitutioner.

Kaldes det sidstnævnte System S og det tilsvarende System af Substitutioner af u 'erne T , saa kan enhver rational Funktion af disse, der er uforandret ved Substitutionerne T , betragtes som en Funktion af x 'erne, der er uforandret ved Substitutionerne S , og kan saaledes udtrykkes rationalt ved de bekjendte Størrelser. En rational Funktion af u 'erne derimod, der forandrer Værdi ved en Substitution, der tilhører T , er en Funktion af x 'erne, der forandres ved den tilsvarende Substitution i S , og kan altsaa ikke udtrykkes rationalt ved bekjendte Størrelser. T er saaledes virkelig det System af konjugerede Substitutioner, der tilhører Ligningen $F(u) = 0$.

Jeg kommer nu tilbage til den omtalte Transformation af den givne Ligning. Lad y betegne en rational Funktion af Rødderne $x_0 x_1 \dots x_{n-1}$, hvis numeriske Værdi er uforandret ved Substitutionerne $\left(\begin{smallmatrix} a^{y'} k + b \\ k \end{smallmatrix} \right)$, men er foranderlig ved alle andre Substitutioner. Dette y bliver da Rod i en irreduktibel Ligning af Graden $\frac{n(np+1)v}{n \cdot v}$ eller $np+1$, hvis Koefficienter ere bekjendte Størrelser. Gaar ved en Substitution φ , der tilhører den oprindelige Lignings System af konjugerede Substitutioner, som jeg for Kortheds Skyld vil bevægne med Bogstavet S , y over til y' , saa er y' uforandret ved enhver Substitution, der indeholdes i Udtrykket $\left(\begin{smallmatrix} \varphi \cdot (a^{y'} k + b) \\ \varphi(k) \end{smallmatrix} \right)$. Paa den anden Side kan y' heller ikke være uforandret ved andre end disse $n \cdot v$ Substitutioner; thi da omvendt y' gaar over til y ved φ^{-1} , vilde deraf følge, at y var uforandret ved flere end $n \cdot v$ Substitutioner. Til hver Værdi af y svarer saaledes et partielt System af konjugerede Substitutioner, der er af Ordenen $n \cdot v$ og er ligedannet med Systemet $\left(\begin{smallmatrix} a^{y'} k + b \\ k \end{smallmatrix} \right)$, og som saaledes indeholder et og kun et af de $np+1$ Sæt cirkulære Substitutioner i S . Da fremdeles ethvert Sæt lader sig aflede af Sættet $\left(\begin{smallmatrix} k + b \\ k \end{smallmatrix} \right)$ ved Substitutioner, der tilhøre S , vil der ogsaa til hvert Sæt svare en

Værdi af y ; som Følge heraf kan heller ikke to forskellige Værdier af y være uforandrede ved det samme Sæt af cirkulære Substitutioner. Ved Afledning ved Hjælp af Substitutionerne i S vil saaledes de $np+1$ Sæt cirkulære Substitutioner gaa over til hinanden paa en Maade, som kan udtrykkes ved de Substitutioner af y 'erne, som foraarsages ved de samme Substitutioner. Disse Substitutioner af y 'erne udgjøre nu netop det System, der tilhører y 'ernes Ligning; lader os for Korthed betegne dette System med Bogstavet T . T indeholder nu høist $(np+1)n$ Substitutioner. Skulde det indeholde færre, maatte S indeholde Substitutioner, der lode alle y 'er uforandrede. Men lader en Substitution af Systemet S den Funktion, som vi fra først af betegnede med y , uforandret, da er den af Formen $\left(a^{y'}k+b\right)$; hvis her $a^{y'} \equiv 1$, er den cirkulær, og efter hvad ovenfor er sagt, vil en saadan ombytte de øvrige y 'er i p Cirkler, hver bestaaende af n . Er derimod ikke $a^{y'} \equiv 1$, lader Substitutionen et x staa; hvis dette er x_0 , er $b \equiv a$. Betegnes for et Øieblik $\left(a^{y'}k\right)$ med φ , og lader $\varphi y'$, svarende til Sættet θ_1^r , uforandret, saa maa man have $\varphi\theta_1\varphi^{-1} = \theta_1^c$, ligesom man har $\varphi\theta\varphi^{-1} = \theta^{a^{y'}}$. Som Følge heraf bliver

$$\varphi\theta\theta_1\theta^{-1}\varphi^{-1} = (\varphi\theta\varphi^{-1}) \cdot (\varphi\theta_1\varphi^{-1}) \cdot (\varphi\theta^{-1}\varphi^{-1}) = \theta^{a^{y'}} \cdot \theta_1^c \cdot \theta^{-a^{y'}}.$$

Da nu ikke $a^{y'} \equiv 1$, er denne cirkulære Substitution ikke af samme Sæt som $\theta\theta_1\theta^{-1}$, følgelig lader φ ikke det til $\theta\theta_1\theta^{-1}$ svarende y uforandret. Da man uden at forandre den cirkulære Substitution $\left(k+1\right)$ kan lade hvilket som helst x betegnes med x_0 , gjælder det samme ogsaa om de øvrige Substitutioner af Formen $\left(a^{y'}k+b\right)$, hvor ikke $a^{y'} \equiv 1$. Det er saaledes bevist, at Systemet T virkelig indeholder $(np+1)n$ Substitutioner.

Som Følge heraf vil Rødderne i den givne Ligning atter kunne udtrykkes som rationale Funktioner af y 'erne. Medregnes nemlig y 'erne blandt de bekjendte Størrelser, vil, som bekjendt, under denne nye Forudsætning den givne Lignings System af konjugerede Substitutioner kun beholde de Substitutioner i S , ved hvilke

y 'erne ere uforandrede, d. e. det vil kun bestaa af den identiske Substitution. Enhver rational Funktion af x 'erne vil altsaa lade sig udtrykke rationalt ved de bekjendte Størrelser, hvortil nu y 'erne regnes.

Ethvert transitivt System af konjugerede Substitutioner af Primtalgraden n og af Ordenen $(np+1) \cdot n$ kan saaledes udledes af et andet transitivt System af samme Orden, men af Graden $np+1$.

Man har vel bekjendte Exempler herpaa; for $n = 5, 7, 11$ gives Systemer, hvor $p = 1$, nemlig af Ordenen $(n+1)n(n-1)$ for $n = 5$, og af Ordenen $(n+1)n \cdot \frac{n-1}{2}$ for $n = 5, 7, 11$, hvoraf de af 5te Grad indeholder, det ene alle mulige Substitutioner, det andet Halvparten; de af 7de og 11te Grad derimod færre. Nu ere virkelig Ligninger, hvortil disse to sidste Systemer høre, først udledede af Ligninger af 8de og 12te Grad, nemlig af de i de elliptiske Funktioners Theori saakaldte Modularligninger, henhørende til Transformationer af 7de og 11te Grad. En nærmere Undersøgelse vil ogsaa vise, at disse Modularligninger virkelig staa i samme Forhold til sine reducerede af 7de og 11te Grad, som ovenfor y 'ernes Ligning til den oprindelige Ligning af Graden n . Ligeledes kan Modularligningen, der tilhører Transformationen af 5te Grad, omdannes til en Ligning af 5te Grad. Nu kan efter Galois (Lettre à M. Auguste Chevalier, Liouvilles Journal 11te Bind 1846) Ligninger af Graden n , hvis System af konjugerede Substitutioner er udtrykt ved

$$\begin{pmatrix} ak+b \\ ck+d \\ k \end{pmatrix}$$

f. Ex. Modularligningerne, kun i de nævnte Tilfælde transformeres til andre Ligninger af Graden n .¹ Gives der altsaa Systemer af konjugerede Substitutioner af Graden n og af Ordenen $(n+1)n$, hvor n er et Primtal høiere end 11, maa disse kunne udledes af andre Systemer af Graden $n+1$, end de, hvis Substitutioner ere af Formen

¹ Denne Del af Galois's Paastand er ikke bevist i Betti's Arbeide om denne Gjenstand (Sopra l'abbassamento etc. Tortolinis Annaler 1853). Jeg skal maaske ved en anden Anledning give Beviset.

$$\binom{ak+b}{ck+d}.$$

Af de ovenfor udviklede Sætninger ere følgende beviste af Mathieu i den oftere omtalte Afhandling. Antallet af Sæt af cirkulære Substitutioner er af Formen $np+1$; kaldes Systemets Orden nr , saa er r divisibel med en vis Faktor af $n-1$; er denne v og $n-1 = v \cdot v'$, indeholder Systemet de nv Substitutioner $\binom{a^{v'}k+b}{k}$; Tallet v er større end 1, og, hvis n er af Formen $4h+3$, ogsaa større end 2; endelig indeholder Systemet mindst $\frac{r}{v}$ Sæt cirkulære Substitutioner, idet et saadant Antal kan afledes af et af dem ved Hjælp af Systemets Substitutioner. Hertil har jeg tilføiet, at ogsaa Antallet af de Sæt, der kunne afledes ved Hjælp af Systemets Substitutioner af et hvilket som helst af dem, er af Formen $np+1$; dette har givet Middel til at bevise, at disse $np+1$ Sæt i Virkeligheden indeholde alle Systemets cirkulære Substitutioner; heraf følger videre, at Systemets Orden er Produktet af de tre Tal, der betegne Graden, Antallet af Sæt af cirkulære Substitutioner, og Antallet af de Substitutioner, der ved Afledning lade et hvilket som helst Sæt uforandret. Det bliver saaledes muligt at angive begge disse sidste Tal uden at kjende andet end Systemets Orden. Jeg skal til Slut anføre et Par Exempler herpaa.

Mathieu har vist, at der gives transitive Systemer af Graden q^r+1 og af Ordenen $(q^r+1)q^r \cdot (q^r+1)\frac{r}{\tau}$, naar q er Primtal og τ en Divisor af r . Er nu $q=2$ og r en Potens af 2, kan det hende, at q^r+1 er Primtal. Man har da

$$n = 2^r + 1; (2^r + 1) \cdot 2^r \cdot (2^r - 1) \frac{r}{\tau} = n(np + 1) \cdot v;$$

heraf følger, da $2^r \cdot (2^r - 1) \equiv 2 \pmod{n}$

$$v = 2 \frac{r}{\tau}, \text{ hvilket er en Divisor af } n-1 \text{ eller } 2^r$$

$$np + 1 = 2^{r-1} \cdot (2^r - 1).$$

Disse Systemer indeholde saaledes $2 \cdot \frac{r}{\tau}$ Substitutioner af Formen $\binom{ak}{k}$, og $2^{r-1}(2^r-1)$ Sæt cirkulære Substitutioner.

Et andet Exempel kan hentes fra Systemer af konjugerede Substitutioner, der ere bekjendte fra de ved Rodtegn opløselige

Ligningers Theori. L d q som f r v re et Primtal, og lader os t nke os en Ligning af Graden $q^r - 1$, hvis R dder adskilles ved r Indexer $i, k, \dots, m$, der antage alle V rdier efter Modulen q , undtagen Kombinationen

$$i \equiv k \equiv l \equiv \dots \equiv m \equiv 0.$$

Lader os endvidere antage, at det Ligningen tilh rende System af konjugerede Substitutioner betaar af de

$$(q^r - 1)(q^r - q)(q^r - q^2) \dots (q^r - q^{r-1})$$

Substitutionen af Formen

$$\left\{ \begin{array}{c} ai + bk + \dots + dm, a_1 i + b_1 k + \dots + d_1 m, \dots, a_{r-1} i + b_{r-1} k + \dots + d_{r-1} m \\ i, k, \dots, m \end{array} \right\}$$

Dennes nu symmetriske Funktioner af de $\frac{q^r - 1}{q - 1}$ Systemer af $q - 1$ R dder, hvis Indexer have samme Forhold til hinanden, saa ere disse Funktioner samtlige uforandrede ved de $q - 1$ Substitutioner af Formen

$$\left\{ \begin{array}{c} ai, ak, \dots, am \\ i, k, \dots, m \end{array} \right\},$$

og ville ved Systemets  vrige Substitutioner kun ombyttes med hinanden. De ere saaledes R dder i en Ligning af Graden $\frac{q^r - 1}{q - 1}$, hvis System af konjugerede Substitutioner bliver af Ordenen $\frac{q^r - 1}{q - 1} (q^r - q)(q^r - q^2) \dots (q^r - q^{r-1})$.

Er nu r et ulige Primtal, kan det hende, at $\frac{q^r - 1}{q - 1}$ er et Primtal. S ttes $\frac{q^r - 1}{q - 1} = n$, ser man let, at q er primitiv Rod i Kongruentsen

$$z^r \equiv 1 \pmod{n},$$

hvoraf f lger, at

$$\frac{z^r - 1}{z - 1} \text{ eller } z^{r-1} + z^{r-2} + \dots + z + 1 \equiv (z - q)(z - q^2)(z - q^3) \dots (z - q^{r-1}).$$

Gj res nu

$$z \equiv q^r \equiv 1,$$

finder man

$$(q^r - q)(q^r - q^2)(q^r - q^3) \dots (q^r - q^{r-1}) \equiv r \pmod{n}.$$

I disse Systemer bliver saaledes $v = r$, hvilket er en Divisor af $n - 1$, og $np \vdots 1 = \frac{q^r - q}{r} (q^r - q^2)(q^r - q^3) \dots (q^r - q^{r-1})$.

On Systems of Conjugate Substitutions that could belong to irreducible Equations whose Degree is a Prime Number

I presented Sylow's original Norwegian paper of 1867 on Page 21 to Page 38. I now owe the Übersetzerzentrale München (ÜZM GmbH) (see <https://uezm.de/>) a rather good translation into English, including corrections by myself regarding all the mathematical symbols, which I can present on Page 43 to Page 60. In the following I summarise this English Paper:

In his **article of 1867** Sylow relates to and comments on works by **Évariste Galois** [*Memoire sur les conditions de résolubilité des équations par radicaux*, Journal de mathématiques pures et appliquées 1re série, tome 11 (1846), p. 381-444; see https://en.wikipedia.org/wiki/%C3%89variste_Galois and https://www.numdam.org/item/JMPA_1846_1_11_381_0.pdf and <https://www.bibliotheque-institutdefrance.fr/sites/default/files/memoire-equations-radicaux-galois-evariste.pdf>], **Augustin-Louis Cauchy** [see https://en.wikipedia.org/wiki/Augustin-Louis_Cauchy], **Émile Léonard Mathieu** [*Mémoire sur l'étude des fonctions de plusieurs quantités, sur la manière de les former et sur les substitutions qui les laissent invariables*, Journal de Mathématiques Pures et Appliquées (1861), 241-323; see https://en.wikipedia.org/wiki/%C3%89mile_L%C3%A9onard_Mathieu and <https://eudml.org/doc/235340>], **Jean-Pierre Serret** [*Cours d'algèbre supérieur*, Gauthier-Villars, Paris, 1877-79; see https://en.wikipedia.org/wiki/Jean-Pierre_Serre and <https://archive.org/details/coursdalgebsuper01serrrich> and <https://archive.org/details/coursdalgebsuper02serrrich>], **Nils Henrik Abel** [*Abel equations*; see https://en.wikipedia.org/wiki/Abel_equation], **Theodor Schönemann** [*Über die Beziehungen, welche zwischen den Wurzeln irreductibeler Gleichungen stattfinden, insbesondere wenn der Grad derselben eine Primzahl ist*, Denkschriften k. k. Akademie der Wissenschaften, Math.-Naturwiss. Klasse (1853); see under https://en.wikipedia.org/wiki/Theodor_Sch%C3%B6nemann and <https://www.biodiversitylibrary.org/item/247907>] and **Enrico Betti** [*Sopra l'abbassamento delle equazioni modulari delle funzioni ellittiche*, Annali di Scienze Matematiche e Fisiche, TOMO QUARTO, (marzo 1853), 81-100, by **Barnaba Tortolini**; see under https://en.wikipedia.org/wiki/Enrico_Betti and <https://www.sba.unifi.it/p589.html> and https://en.wikipedia.org/wiki/Barnaba_Tortolini]. His concern is to describe the systems named in the title and to show how they relate to the works of the quoted distinguished mathematicians. He limits his investigations to irreducible equations of prime degree whence he is not yet investigating prime powers as he did in his excellent **article of 1872**. He frequently uses the binomial coefficients $\binom{n}{k} := (n(n-1)(n-2)\dots(n-k+1)) / (k(k-1)\dots 1) = n! / (k!(n-k)!)$ for pairs of integers $n \geq k \geq 0$ (see https://en.wikipedia.org/wiki/Binomial_coefficient) and says that he has used the same symbols as used in **Serret's** book. He cites **Schönemann's** and **Mathieu's** result that for an irreducible equation of prime degree n the associated system of conjugate substitutions must contain a circular substitution $\binom{k+1}{k}$ of the n roots and relates this to **Galois's** memoir. He then develops on 15 pages his outstanding and hitherto hardly known theory of systems of conjugate substitutions belonging to irreducible equations of prime degree n which precedes his famous **article of 1872**.

nature

[Explore content](#)
[About the journal](#)
[Publish with us](#)
[Subscribe](#)

nature > news > article

News | Published: 20 March 2019

Ludvig Sylow

G. B. M.

Nature 103, 49 (1919) | [Cite this article](#)

752 Accesses | 4 Altmetric | [Metrics](#)

Abstract

THE death of Ludvig Sylow (September 7, 1918), at the age of eighty-five, has removed an eminent mathematician, whose career was in many ways remarkable. Sylow's seventh published paper ("Théorèmes sur les groupes de substitutions") occupies less than ten pages in vol. v. of the *Mathematische Annalen* (1872); this contains the proof of his justly celebrated theorem about groups, which has perhaps done more than any other single proposition to advance our knowledge of groups in general. In spite of this great achievement, Sylow had to earn his living as a secondary-school teacher until he had served a term of forty years. Recognition came at last; he was made professor at Christiania at the age of sixty-five, and filled the chair successfully for twenty years.

<https://www.nature.com/articles/103049a0>



https://pantheon.world/profile/person/Peter_Ludwig_Mejdell_Sylow and https://pantheon.world/de/profile/person/Peter_Ludwig_Mejdell_Sylow



Contents.

Lectures and Treatises.

a. Published in full or in excerpts:

	Page.
Om Ni-Tallet, af C. A. Holmboe	1—8
En Text-Emendation til Melissi fragmenta, af Lyng	9
Om et nyt Led i Glycocolrækken, af Lindgaard	9—10
— Muskel-Sammentrækning, af C. Boeck	10—11
En Notits om Øen Maaln, af Sexe	12—15
Om Kometer og Stjernesked, af Fearnley	15—16. 25
Emendation til Gaji instt. 2, 181, af Aubert senior	17—18
Om det 22de ægyptiske Dynasti, af Lieblein	18—19
— Echinodermer og Coelenterater, fundne ved Lofoten, af M. Sars	19—23
— to nye Arter Bryozoeer, af Danielssen	23—24
— Ruslands ældre Vægtsystem, af Holmboe	25—36
— Haymari Monachi de expugnata Accone liber tetrastichas ed. Riant, (en Text-Emendation, af Monrad	36
— Pythagoreismen, af Lyng	38—44
Ny Fortolkning af et Sted i Platons Phædrus (p. 241 E.), af Monrad	44—49
Fossiler fra Skotlands og Nordamerikas Glacial-Formation, af M. Sars.	51—58
Oversigt over det meteorologiske Instituts Organisation og Arbejder, af Mohn	58—63
Om Gravhøie, hvori mere end eet Kammer og mere end een Urne er funden, af Holmboe	63—80
— Artsbegrebet i Planteriget, af Schübeler	82
Æsthetisk Bemærkning angaaende Krumningen af Horizontallinierne paa de doriske Templer i Athen, af Monrad	82—90
Om Conglomeraterne i det throndhjemske Skifer-Felt og deres Vidnesbyrd ligeoverfor Omvandlings-Theorien, af Kjerulf	90—95
— russiske Rubel-Barrer, af Holmboe	95—100
— Lysets Indflydelse paa Plantelivet, af Christie	100—105
Discussion over samme Emne	210—212
On the system of conjugate substitutions that could yield irreducible equations whose degree is a prime number, by Sylow	105—122
— en usædvanlig Bevægelse af Havet paa Norges Vestkyst den 7 Mai 1867, af Mohn	123—129
— Anaxagoras's Plads i Philosophiens Historie, af Lyng, samt Modbe- mærkning, af Monrad	129—135
— de ægyptiske Skarabæers Vægt, af Lieblein	135—139
Bidrag til Legemernes Molekylar-Theorie	140—146, 159—169
Om Flaghøien paa Karmøen og de buddhistiske Tøper i Asien, af Holmboe	146—155
— et geologisk Profil fra Rigsgrænsen over Lyngen til Kvalø, af K. Petterson	155—158
— Tordenveir i Norge i Sommeren 1867, af Mohn	169—201
— Forskjellen mellem Parmenides og Melissos, af Lyng	202—204
Et nyt Bidrag til Danmarks Reformationshistorie, af L. L. Daac	204—210
Om Finmarkens Geologi, af T. Dahll	213—222

IV

b. Without communicating the development of the content here.

Angaaende den 32te Psalme, af Caspari	9
Om Balænoptera musculus, af G. O. Sars	11
— Begrebet af Christendommen som den absolute Religion, af Mourad	15
— Russisk Laplands geographiske Forholde, af L. K. Daa	19, 139
— Daabs-Spørgsmaalene i den mozarabisk-spanske Kirke, af Caspari	36
— en Sygdom hos Grantræet, af C. Boeck	51
— Nadværens Indstiftelsesords liturgiske Historie, af Caspari	80
— nogle norske Rune-Indskrifter, af Bugge	129
— Karyatiderne paa Erechtheion, af Mourad	202

Miscellaneous Communications.

Anmerkninger angaaende det forrige Aars trykte Forhandling, af E. S. mark og Sars	16, 36—38
Indvotering af nye Medlemmer	16
Om Selskabets Virksomhed i 1866	49—51
Digt i Anledning af Prinds Oscars Nærværelse, af A. Munch	80—82
Vaig paa Selskabets Embedsmænd for 1868	213
Gaver til Selskabets Bibliothek	222—224
Selskabets Medlemmer i 1867	225

WIKIPEDIA

20 years of the free encyclopedia

Peter Ludvig Sylow

Peter Ludvig Mejdell Sylow (/ˈsiːls/) (12 December 1832 – 7 September 1918) was a Norwegian mathematician who proved foundational results in Group Theory.^[1] Sylow processed and further developed the innovative works of mathematicians Niels Henrik Abel and Évariste Galois in Algebra. Sylow theorems and *p*-groups, known as Sylow subgroups, are fundamental in finite groups.^[2] By profession, Sylow was a teacher at the Fredrikshald Latin School (Norwegian: Fredrikshalds lærde og realskole) for 40 years from 1858 to 1898, and then a professor at the University of Oslo for 20 years from 1898 to 1918.^[3] Despite the isolation in Fredrikshald, Sylow was an active member of the mathematical world. He wrote a total of approximately 25 mathematical and biographical works, corresponded with many of the leading mathematicians of the time, and was an able co-editor of *Acta Mathematica* from the journal's start in 1882.^[4] He was also elected into the Norwegian Academy of Science and Letters in 1868, a corresponding member of the Academy of Sciences in Göttingen and the University of Copenhagen awarded him an honorary doctorate in 1894.^{[5][6]}

Early life

Ludvig Sylow was born in Kristiania (now Oslo) on 12 December 1832 to later minister and customs treasurer **Thomas Edvard von Westen Sylow** (1792–1875) and **Magdalene Cecilie Cathrine Mejdell** (1806–98).^{[1][3]} His father had been an officer and a captain in the cavalry, and later he served as the head of the Ministry of the Army between 1848 and 1854.^{[3][6]}

Initially, his father was aware of his son's talent in Mathematics, so he encouraged him to work independently. From home, Sylow learned a sense of duty and hard work but was also taught to be modest and although this was done with the best of intentions, it would become an obstacle for him later in life since it meant that he was happy to spend many years in a more lowly position than he should have had.^{[3][6]}

Career as a mathematician

Education and first steps in mathematics

Abel and the theory of equations

Failure to join a university

Sylow's theorems

Written works

Later career

Ludvig Sylow

Born

Peter Ludvig Mejdell Sylow
12 December 1832
Christiania, Norway

Died

7 September 1918 (aged 85)
Christiania, Norway

Alma mater

University of Christiania

Known for

Sylow theorems

Scientific career

Fields

Mathematics

Personal life

Sylow never married, but was a warm person with a nice sense of humour.^[2] He was an avid lover of being out of doors and often spent summer vacations in the mountains, usually in Kongsvoll, where he studied plants. Kongsvoll is a mountain station providing food and shelter on the route between Oslo and Trondheim, erected when the route was used by pilgrims visiting the shrine of St Olav in Trondheim.^[3]

Death

Sylow died on 7 September 1918, at the age of 85, in Christiania, Norway.^[6]

Honors

- The Crown Prince's Gold Medal (1853)
- The Norwegian Academy of Science and Letters, elected in 1868
- Corresponding member of the Academy of Sciences in Göttingen (1893)
- Editor of *Acta Mathematica* from (1893)
- Honorary doctorate at Copenhagen University (1894)

References

- Birkeland, Bent. "Ludvig Sylow" (https://nbl.srl.no/Ludvig_Sylow). *nbl.srl.no* (in Norwegian).
- O'Connor, John J.; Robertson, Edmund F., "Ludvig Sylow (1832 - 1918)" (<https://mathshistory.st-andrews.ac.uk/Biographies/Sylow.html>), *MacTutor History of Mathematics Archive*, University of St Andrews.
- "885 [Salmonsens konversationsleksikon / Anden Udgave / Bind XXII. Spekulation—Seere]" (<https://runesberg.org/salmonsens/2220907.html>) [885 [Salmonsens's Conversation Lexikon / Second Edition / Volume XXII: Speculation—Seere]], *runesberg.org* (in Danish).
- Brinchmann, Christopher; Daa, Anders; Hammer, K.V., eds. (1912). "Sylow, Peter Ludvig Mejdell" (<https://runesberg.org/foermerhvers/1912/0266.html>). *Hvem er Hvem? Haandbog over samtidige norske mænd og kvinder* (in Norwegian) (1 ed.). Kristiana: Aschehoug.

External links

- Mathews, G.B. (1919). "Ludvig Sylow" (<https://doi.org/10.1038/257103049a0>). *Nature*. **103** (2577): 49. Bibcode:1919Natur.103...49G (<https://doi.org/10.1038/257103049a0>). doi:10.1038/257103049a0 (<https://www.nature.com/articles/257103049a0>).
- Sylow, M.L. (1872). "Théorèmes sur les groupes de substitutions" (<https://zenodo.org/record/2329278>). *Mathematische Annalen*. **5** (4): 584–594. doi:10.1007/BF01442913 (<https://doi.org/10.1007/BF01442913>). S2CID 121928336 (<https://api.semanticscholar.org/CorpusID:121928336>).
- O'Connor, John J.; Robertson, Edmund F., "Peter Ludvig Sylow" (<https://mathshistory.st-andrews.ac.uk/Biographies/Sylow.html>), *MacTutor History of Mathematics Archive*, University of St Andrews.
- Peter Ludvig Sylow (<https://mathgenealogy.org/id.php?id=18234>) at the Mathematics Genealogy Project.

https://en.wikipedia.org/wiki/Peter_Ludvig_Sylow and <https://runesberg.org/foermerhvers/1912/0266.html>

Peter Ludwig Mejdell Sylow



(see <https://mathhistory.st-andrews.ac.uk/Biographies/Sylow/pictdisplay/> and <https://runeberg.org/salmosen/2/22/0907.html> and <https://runeberg.org/salmosen/2/22/0908.html>)

*Mr. B j e r k n e s presented the following paper submitted by Mr. S y l o w :
On Systems of Conjugate Substitutions that could
belong to irreducible Equations whose Degree
is a Prime Number.*¹

According to G a l o i s ' famous theory, the condition for a rational function of the roots of an algebraic equation to be expressed rationally by the coefficients and other known quantities is that the numerical value of the function must remain the same when the roots are interchanged in certain ways. These permutations or s u b s t i t u t i o n s , also called by C a u c h y a "system of conjugate substitutions", i.e. any two of them performed one after the other in any permutation of the roots, produce the same result as if a certain third substitution of the system had been performed. G a l o i s conceives of the substitutions of the system as defined by a "group" of permutations, which are transformed into each other by the substitutions. Equations that, under the same conditions, have the same system of conjugate substitutions or the same group, thus have essential properties in common and could therefore be regarded as a distinct class. On the other hand, it can also be proven that for any given system of conjugate substitutions there are corresponding equations. It would be of great importance to the theory of algebraic equations if one could specify which systems of conjugate substitutions could belong to equations of a given degree,

¹ Included in the Society's Proceedings according to the assessment given by gentlemen Dr. O.J. Broch and Bjerknes.

and especially which ones belong to irreducible equations. This problem, as well as other problems related to it, has therefore also been addressed by several distinguished mathematicians, without, however, succeeding in solving it.

For equations that can be solved by root signs, the problem has proven to be much easier when the degree is a prime number than when it is a composite number. This circumstance makes it likely that a similar relationship applies to equations that can be solved by root signs. Having thus limited my investigation to irreducible equations of prime degree, I have, among other things, succeeded in completing some results found by M a t h i e u (*Mémoire sur l'étude des fonctions de plusieurs quantités* etc. Liouville's Journal 1861). However, since the development that has led me to this point differs in part from M a t h i e u 's, I have thought it appropriate to present it in its entirety.

In the following, I will use the same symbols as those used in the third edition of S e r r e t 's *Cours d'algèbre supérieur*. I thus denote the roots of the equation by the same letter, x , provided with indices taken from the modulus n , where n denotes the degree of the equation; a substitution of the roots is denoted by indicating which substitution of these indices it entails. When a substitution is denoted by a letter, I think of this as a function symbol, whereby the index resulting from the substitution is expressed using the original one. The substitution is thus understood to be the same as in the substitution $\left(\begin{smallmatrix} \varphi(k) \\ k \end{smallmatrix} \right)$, where $\varphi(k)$ denotes a certain function of such a nature that, when k assumes the values $0\ 1\ 2\ \dots\ (n-1)$, it becomes congruent (mod n) with the same numbers in some order. I still think of the system of conjugate substitutions belonging to the given equation, determined by a group of permutations, before, when the substituent must be compatible, to be able to speak as much about/of the permutations that emerge from each other through the substitutions of the system as about/of the substitutions themselves.

S c h ö n e m a n n ¹ and later M a t h i e u ² have proven that when the degree of an irreducible equation is a prime number n , the system of conjugate substitutions associated with the equation must contain a circular substitution of the n roots. Let this be denoted by θ , and let the roots be denoted by $x_0, x_1, x_2, \dots, x_{n-1}$ in such an order that we have

$$\theta = (0 \ 1 \ 2 \ \dots \ (n-1)), \text{ i.e. } \theta = \begin{pmatrix} k+1 \\ k \end{pmatrix};$$

the equation belonging to the system of conjugate substitutions then also contains all powers of θ . For brevity, I will refer to a circular substitution together with its powers as a set of circular substitutions. If the equation is solvable by root signs, then the system contains only this one set; conversely, we also know that if the system of conjugate substitutions associated with the equation contains only one set of circular substitutions, then the equation is solvable by root signs. If, on the other hand, the equation is not solvable by root signs, then there must be more than one set of circular substitutions in the system; that is, there must be a circular substitution θ^i such that we do not have:

$$\theta^i = \theta^a$$

for any value of a . Nor can we have

$$\theta^{ia} = \theta^b,$$

unless both a and b are divisible by n , whereby θ^{ia} and θ^b become $= 1$, i.e. indicating, that no change occurs in the position of the roots. For from $\theta^{ia} = \theta^b$ follows $\theta^{iac} = \theta^{bc}$, since n is now a prime number,

¹ Über die Beziehungen, welche zwischen den Wurzeln irreductibeler Gleichungen stattfinden etc. [On the relationships that occur between the roots of irreducible equations] in the 5th volume of Denkschriften der math.-naturw. Classe der kaiserlich. Acad. Wien. Schönemann assumes that the coefficients of the equation are rational numbers; however, this restriction is not essential for the proof. This proof is undoubtedly one of the most significant advances the theory has made since Galois's death; in particular for the first time, one of the most important solutions in Galois's "Memoire sur les conditions de résolubilité des équations par radicaux" has been completed, namely that in Proposition VIII, where it is assumed, without full proof, that the group must contain a circular permutation.

² In the above-mentioned treatise "Memoire sur l'étude des fonctions de plusieurs quantités" Liouville's Journal Year 1861. Page 304.

one could, if not $a \equiv 0 \pmod{n}$, set $ac \equiv 1 \pmod{n}$ or $c \equiv 1/a$, thereby obtaining

$$\theta^i = \theta^{b/a}$$

which is contrary to the condition. The system of conjugate substitutions in the equation must now contain the substitution $\theta^{ia} \theta^r \theta^{i-a}$, or, to use B e t t i 's expression, the derivative of θ^r using θ^{ia} , which is derived in the same way as θ^r , i.e., circular. First, note that we have

$$\theta^{ia} \theta^r \theta^{i-a} = (\theta^{ia} \theta \theta^{i-a})^r ;$$

the substitutions of the form $\theta^{ia} \theta^r \theta^{i-a}$, in which a has the same value, thus form a set of circular substitutions, which can thus be said to be derived from the set θ^r using θ^{ia} . Secondly, the n sets

$$\theta^r, \theta^i \theta^r \theta^{i-1}, \theta^{i^2} \theta^r \theta^{i-2}, \theta^{i^3} \theta^r \theta^{i-3}, \dots, \theta^{i^{(n-1)}} \theta^r \theta^{i-(n-1)}$$

are different from each other as well as from θ^{ir} . Namely,

$$\text{from } \theta^{ia} \theta^r \theta^{i-a} = \theta^{is}$$

$$\text{immediately followed } \theta^r = \theta^{is},$$

which is impossible. If, on the other hand,

$$\text{from } \theta^{ia} \theta^r \theta^{i-a} = \theta^{ib} \theta^s \theta^{i-b},$$

$$\text{followed } \theta^r = \theta^{i(b-a)} \theta^s \theta^{i-(b-a)},$$

$$\text{then } \theta^{r/s} = \theta^{i(b-a)} \theta \theta^{i-(b-a)}.$$

This equation states that θ , when derived using $\theta^{i(b-a)}$, changes to one of its powers. But now we know that any substitution that, by derivation, changes $\binom{k+1}{k}$ to one of its powers must itself be of the form $\binom{ck+d}{k}$; this substitution is only circular if $c \equiv 1 \pmod{n}$. We must therefore have

$$\theta^{i(b-a)} = \binom{k+d}{k} = \theta^d.$$

but this is impossible when $b \equiv a$. It has thus been proven that θ^{ir} and $\theta^{ia} \theta^r \theta^{i-a}$ represent $n+1$ sets of circular substitutions; if, therefore, the system of conjugate substitutions in the equation contains more than one set of circular substitutions, then it contains

at least $n + 1$ sets. However, if it contains more than these, let θ_1 be a new circular substitution. The system then contains the n sets expressed by

$$\theta^{ia} \theta_1^r \theta^{i-a}$$

which, as proven above, are mutually different and different from θ^{ir} . But they are also different from the sets $\theta^{ia} \theta^r \theta^{i-a}$; for if one had

$$\theta^{ia} \theta_1^r \theta^{i-a} = \theta^{ib} \theta^s \theta^{i-b},$$

then it follows $\theta_1 = \theta^{i(b-a)} \theta^{s/r} \theta^{i-(b-a)}$, i.e. θ_1 itself belonged to one of the preceding sets, which is contrary to our assumption. Thus, if the system contains more than those $n + 1$ sets, then it has at least $2n + 1$; if it has even more, then we see in the same way that it has at least $3n + 1$, and so on. In this way, we can continue to arrange the circular substitutions belonging to the system until they are exhausted; the number of different sets must therefore be of the form $np + 1$. The equations solvable by root signs are included in this, as they correspond to $p = 0$.

If θ , by derivation using any of the substitutions of the system, became a power of itself, then the substitutions of the system must all be of the form

$$\left(\begin{smallmatrix} ak + b \\ k \end{smallmatrix} \right),$$

and the equation would belong to those solvable by root signs. If it does not belong to these, the system must contain a substitution φ such that $\varphi\theta\varphi^{-1}$ does not belong to the set θ^r . Since the choice of the circular substitution, which we have denoted by θ^i , is quite arbitrary, we could assume

$$\theta^l = \varphi\theta\varphi^{-1}.$$

The set θ^{ir} can then be derived from the set θ^r using one of the system's own substitutions; the same applies to the sets $\theta^{ia} \theta^r \theta^{i-a}$. If the system now contains more sets of circular substitutions that could be derived from θ^r using the system's own substitutions than these $n + 1$, we could assume that θ_1 has the same property. We then have

$$\theta_1 = \psi \theta \psi^{-1},$$

where φ belongs to the system. It follows that

$$\theta^{ia} \theta_1^r \theta^{i-a} = \theta^{ia} \psi \theta^r \psi^{-1} \theta^{i-a} = (\theta^{ia} \psi) \theta^r (\theta^{ia} \psi)^{-1}.$$

Since θ^{ia} and ψ belong to the system, their product $\theta^{ia} \psi$ must also belong to the system; but we see that all sets $\theta^{ia} \theta_1^r \theta^{i-a}$ can be derived from the set θ^r by the system's own substitutions. One can therefore repeat the previous reasoning and the previous arrangement of the circular substitutions, limiting oneself to the sets that could be derived from θ^r by substitutions belonging to the system. The number of these sets is thus also of the form $np + 1$. It will be shown below that this actually yields a l l circular substitutions.

One can derive another set from the set θ^r using any substitution belonging to the system; but several of these derived sets could coincide with each other or with θ^r . In order to obtain a relation between the number of substitutions in the system, i.e. the o r d e r of the system, and the number of sets of circular substitutions that could be derived from θ^r by the substitutions of the system, we would examine how many of the latter could give the same derived set. To this end, let φ and ψ be a n y t w o substitutions by which θ^r gives the same set. We then have

$$\psi \theta \psi^{-1} = \varphi \theta^a \varphi^{-1},$$

and conversely, which is sufficient for the derived sets to be identical. Now

$$\begin{aligned} \psi \theta \psi^{-1} &= (\psi(0) \psi(1) \psi(2) \dots \psi(n-1)) \text{ and} \\ \varphi \theta^a \varphi^{-1} &= (\varphi(0) \varphi(a) \varphi(2a) \dots \varphi(n-1)a) \end{aligned}$$

Therefore, if $\psi(0) = \varphi(ma)$, we must have

$$\psi(1) = \varphi((m+1)a), \psi(2) = \varphi((m+2)a), \dots \psi(k) = \varphi((m+k)a).$$

If we set $ma \equiv b \pmod{n}$, we get

$$\psi(k) = \varphi(ak + b).$$

The substitutions that derive the same set as $\binom{k+r}{k}$ from $\binom{\varphi(k)}{k}$ are thus those contained in the expression $\binom{\varphi(ak+b)}{k}$, all of these and no others. If φ now belongs to the system, then they become

substitutions in the system that satisfy the aforementioned condition are the same as those of the form $\left(\begin{smallmatrix} \varphi(ak+b) \\ k \end{smallmatrix} \right)$. However, if both $\left(\begin{smallmatrix} \varphi(ak+b) \\ k \end{smallmatrix} \right)$ and φ belong to the system, then the same applies to the product $\varphi^{-1} \left(\begin{smallmatrix} \varphi(ak+b) \\ k \end{smallmatrix} \right)$ or $\left(\begin{smallmatrix} ak+b \\ k \end{smallmatrix} \right)$; conversely, if φ and $\left(\begin{smallmatrix} ak+b \\ k \end{smallmatrix} \right)$ belong to the system, then the same is true of $\left(\begin{smallmatrix} \varphi(ak+b) \\ k \end{smallmatrix} \right)$. The number of these substitutions is thus equal to the number of substitutions in the system that are of the form $\left(\begin{smallmatrix} ak+b \\ k \end{smallmatrix} \right)$.

Since the system contains the substitution $\left(\begin{smallmatrix} k+1 \\ k \end{smallmatrix} \right)$ and its powers, we see that the constant b can have all n values; similarly, we see that if the system contains the substitution $\left(\begin{smallmatrix} ak+b \\ k \end{smallmatrix} \right)$ for a value a , then it also contains the substitution $\left(\begin{smallmatrix} ak \\ k \end{smallmatrix} \right)$ for the same value, and vice versa. To examine more closely what values a can have, we would denote by ε a primitive root of the prime number n and assume that the system contains the substitution $\left(\begin{smallmatrix} \varepsilon^a k \\ k \end{smallmatrix} \right)$; it then contains every power of this, i.e. every substitution of the form $\left(\begin{smallmatrix} \varepsilon^{\alpha a} k \\ k \end{smallmatrix} \right)$. If α' is now the greatest common factor of α and $n-1$, we can set

$$\xi\alpha \equiv \alpha' \pmod{n-1},$$

whereby we obtain $\varepsilon^{\xi\alpha} \equiv \varepsilon^{\alpha'} \pmod{n}$;

furthermore, if $n-1 = \alpha' \alpha''$, one sees that the system contains the following series of α'' substitutions:

$$(1) \dots \left(\begin{smallmatrix} k \\ k \end{smallmatrix} \right) \left(\begin{smallmatrix} \varepsilon^{\alpha'} k \\ k \end{smallmatrix} \right) \left(\begin{smallmatrix} \varepsilon^{2\alpha'} k \\ k \end{smallmatrix} \right) \dots \left(\begin{smallmatrix} \varepsilon^{(\alpha''-1)\alpha'} k \\ k \end{smallmatrix} \right).$$

If the system contains more substitutions of the form $\left(\begin{smallmatrix} ak \\ k \end{smallmatrix} \right)$ then these, e.g. $\left(\begin{smallmatrix} \varepsilon^{\beta} k \\ k \end{smallmatrix} \right)$, it must contain a similar series of substitutions:

$$(2) \dots \left(\begin{smallmatrix} k \\ k \end{smallmatrix} \right) \left(\begin{smallmatrix} \varepsilon^{\beta'} k \\ k \end{smallmatrix} \right) \dots \left(\begin{smallmatrix} \varepsilon^{(\beta''-1)\beta'} k \\ k \end{smallmatrix} \right),$$

where β' denotes the greatest common factor of β and $n-1$, and where

$n-1 = \beta' \cdot \beta''$. It must also contain every substitution of the form:

$$\begin{pmatrix} \varepsilon^{\zeta\alpha' + \eta\beta'} k \\ k \end{pmatrix}.$$

Now, ζ and η can always be given values such that

$$\zeta \alpha' + \eta \beta' \equiv \zeta \gamma \pmod{n-1},$$

where ζ is arbitrary and γ denotes the greatest common factor of α' and β' . The system therefore contains the following series of γ' substitutions

$$\begin{pmatrix} k \\ k \end{pmatrix} \begin{pmatrix} \varepsilon^\gamma k \\ k \end{pmatrix} \begin{pmatrix} \varepsilon^{2\gamma} k \\ k \end{pmatrix} \dots \begin{pmatrix} \varepsilon^{(\gamma'-1)\gamma} k \\ k \end{pmatrix}, \text{ where } \gamma \cdot \gamma' = n-1.$$

This series contains all substitutions in (1) and (2). In this way, one can continue until all substitutions of the form $\begin{pmatrix} ak \\ k \end{pmatrix}$ in the system have been exhausted. All these substitutions are therefore powers of a single substitution; if their number is v , then v must be a divisor of $n-1$; if $n-1 = v \cdot v'$, they could be written as follows:

$$\begin{pmatrix} k \\ k \end{pmatrix} \begin{pmatrix} \varepsilon^{v'} k \\ k \end{pmatrix} \begin{pmatrix} \varepsilon^{2v'} k \\ k \end{pmatrix} \dots \begin{pmatrix} \varepsilon^{(v-1)v'} k \\ k \end{pmatrix}.$$

The values that a can have are therefore $1 \cdot \varepsilon^{v'} \varepsilon^{2v'} \dots \varepsilon^{(v-1)v'}$, i.e. all numbers of the form $a^{v'}$. The substitutions of the form $\begin{pmatrix} ak+b \\ k \end{pmatrix}$ contained in the system are therefore expressed by $\begin{pmatrix} a^{v'}k+b \\ k \end{pmatrix}$, and their number is $n \cdot v$.

According to what has been said above, the number of substitutions in the system by means of which one can derive a given other set of circular substitutions from θ^r is equal to $n \cdot v$; which is also the number of those by which the set θ^r is derived from itself. If the number of sets that can be derived from θ^r using the substitutions of the system is $np + 1$, then the order of the system is $(np + 1) \cdot n \cdot v$.

It is conceivable that there are more sets of circular substitutions than the ones mentioned $np + 1$. Therefore, let ϑ^r be a set that cannot be derived from θ^r by any of the system's substitutions. Since it does not matter which of the system's circular substitutions is denoted by $\begin{pmatrix} k+1 \\ k \end{pmatrix}$, the following applies, as proven above about θ

also applies to $\mathfrak{g}$. If the number of sets, that could be derived from $\mathfrak{g}^r$ by the substitutions of the system, is equal to $np_1 + 1$, and the number of substitutions, that change $\mathfrak{g}$ to its powers by derivation, is nv_1 , where v_1 denotes a divisor of $n - 1$, then the order of the group is equal to $(np_1 + 1) nv_1$. We then have $(np_1 + 1) nv_1 = (np + 1) nv$ where $v_1 \equiv v \pmod{n}$, i.e. $v_1 = v$, which again implies $p_1 = p$. The circular substitutions that could be derived from $\mathfrak{g}^r$ by the substitutions of the system therefore constitute as many sets as those that could be derived from θ^r ; I add that they are also different from these. For otherwise one would have to have an identity of the form

$$\phi \theta^r \phi^{-1} = \psi \mathfrak{g}^r \psi^{-1},$$

where ϕ and ψ belong to the system. From this it follows that

$$\mathfrak{g} = \psi^{-1} \phi \theta^{r/s} \phi^{-1} \psi = (\psi^{-1} \phi) \theta^{r/s} (\psi^{-1} \phi)^{-1},$$

i.e. $\mathfrak{g}$ could be derived from $\theta^{r/s}$ using $\psi^{-1} \cdot \phi$, which belongs to the system; but this contradicts the assumption. If there were more than $np + 1$ sets of circular substitutions in the system, there would have to be at least $2(np + 1)$. If there were more than these, it can be seen in the same way that there would have to be at least $3(np + 1)$. In short, the number of different sets must be a multiple of $np + 1$; let it be called $m(np + 1)$. But according to what has been proven above, we then have

$$m(np + 1) \equiv 1 \pmod{n}, \text{ i.e. } m \equiv 1.$$

One can therefore set

$$m(np + 1) = (nq + 1)(np + 1).$$

Each set now contains $n-1$ circular substitutions (excluding the identical substitution); the total number of circular substitutions is thus also $m(np + 1)(n-1)$, and this number must be less than the total number of substitutions; we thus have

$$(nq + 1)(np + 1)(n-1) < (np + 1) \cdot n \cdot v.$$

Since $n-1 \geq v$, it follows that $nq + 1 < n$, i.e. $q = 0$.

Therefore, there are no more sets of circular substitutions than those that could be derived from θ^r by the system's own substitutions. It should be noted here that the circular substitution denoted by $\binom{k+1}{k}$ has been chosen quite arbitrarily; what has been proven about this one thus also applies to any other. It should also be noted that the equations solvable by root signs are included in the general rule, as they correspond to the value $p = 0$. Putting together everything that has been proven above, we have the following:

If a system of conjugate substitutions belongs to an irreducible equation of prime degree n , then the order must be a number of the form $(np + 1) \cdot n \cdot v$, where v denotes a divisor of $n-1$. The number of different sets of circular substitutions is $np + 1$, and each of these can be derived from any other set by $n \cdot v$ of the system's substitutions. If the roots are denoted by the same letter with added indices taken from the modulus n , in such an order that one of the circular substitutions is denoted by $\binom{k+1}{k}$, then v is the number of substitutions of the system of the form $\binom{ak}{k}$.

If it is now proven that the order of any transitive system of prime numbers of degree n must be of the form $(np + 1) \cdot n \cdot v$, then it is already clear in advance that there are no systems of any order that are numbers of this form. Since the order is a divisor of $2 \cdot 3 \cdot \dots \cdot n$, $(np + 1) \cdot v$ must be a divisor of $2 \cdot 3 \cdot \dots \cdot (n-1)$. But even when this condition is not fulfilled, there are always systems of order $(np + 1) \cdot n \cdot v$. The 7th degree already provides several examples of this.

Thus, the following is easily proven: *One cannot have $v = 1$, except in the case $p = 0$, i.e. the Abel equations.*

If $v = 1$, the system has $(np + 1) \cdot n$ substitutions, and of these, $(np + 1) \cdot (n-1)$ are circular; thus, there are only $np + 1$ substitutions in the system that are not circular. But now the number of substitutions that leave any root x_k unchanged must also be $= np + 1$; the $np + 1$ non-circular substitutions therefore leave any root x_k unchanged.

Since the system has only one such substitution, the identical substitution, we conclude: $np + 1 = 1, p = 0$.

It further follows that: *When $p > 0$, i.e. when excluding the equations solvable by root signs, and n is of the form $4k + 3$, one cannot have $v = 2$.*

The system must contain the substitution $\begin{pmatrix} -k \\ k \end{pmatrix}$ or

$$(1, n-1) (2, n-2) (3, n-3) \dots ((n-1)/2, (n+1)/2),$$

which is composed of an odd number of transpositions. But now we have the following theorem.

When a system of conjugate substitutions contains a substitution composed of an odd number of transpositions, its order is an even number; one half of its substitutions is composed of an odd number of transpositions, the other of an even number, and the latter constitute a complete system of conjugate substitutions.

Namely, those of the system's substitutions that are composed of an even number of transpositions:

$$1 \cdot \varphi_1 \varphi_2 \dots \varphi_{r-1} \dots (a),$$

then $\varphi_i \varphi_k$ is also a substitution belonging to the system and composed of an even number of transpositions; it is therefore included in (a). The substitutions (a) thus form a system of conjugate substitutions. Furthermore, if ψ and χ are any two of the original system's substitutions that are composed of an odd number of transpositions, then it is obvious that

$$\psi, \psi\varphi_1, \psi\varphi_2, \dots, \psi\varphi_{r-1}, \dots (b)$$

are r distinct substitutions of the same kind. Now $\psi^{-1} \cdot \chi$ is composed of an even number of transpositions, i.e. one of the substitutions a. We therefore have

$$\psi^{-1} \cdot \chi = \varphi_k \text{ and } \chi = \psi \varphi_k.$$

All the substitutions of the original system are thus included in (a) and (b); their number is therefore $2r$.

If there were a system of order $(np + 1) n \cdot 2$, there would also have to be one of order $(np + 1) n$, which is only possible if $p = 0$.

When one wishes to form a picture of the relationship between circular substitutions in derivation, one can imagine the equation transformed into another such that for each set of circular substitutions belonging to the given equation, there corresponds a root in the transformed equation. Since the transformed equations thus obtained are also of interest in other respects, I shall discuss the matter in more detail. I must thus refer to some theorems of the general theory of algebraic equations, which I shall insert and provide with proofs, as I do not know of any place where they are developed.

1. Let u be a rational function with known coefficients of the roots $x_0, x_1, \dots, x_{n-1}$ in an algebraic equation, and let its numerical value remain unchanged by a substitution θ ; if now a substitution φ of the system of conjugate substitutions belonging to the equation changes u to u' , then the numerical value of u' remains unchanged by the derivative of θ using φ .

Namely

$$u = f(x_0 x_1 \dots x_{n-1}) = f(x_{\theta(0)} x_{\theta(1)} \dots x_{\theta(n-1)}),$$

this relation must continue to hold, even if the substitution φ is performed, i.e.

$$u' = f(x_{\varphi(0)} x_{\varphi(1)} \dots x_{\varphi(n-1)}) = f(x_{\varphi\theta(0)} x_{\varphi\theta(1)} \dots x_{\varphi\theta(n-1)}).$$

Thus, we see that u' remains unchanged by the substitution

$$\begin{pmatrix} \varphi\theta(k) \\ \varphi(k) \end{pmatrix}, \text{ i.e. by } \varphi \cdot \theta \cdot \varphi^{-1}.$$

2. If in the function $u_0 = f(x_0 x_1 \dots x_{n-1})$ one performs the system of conjugate substitutions associated with the equation, one obtains a number of functions equal to the order of the system, each of which corresponds to a permutation in the group of the equation; however, several of these could have the same numerical value. If the number of mutually different values of u_0 is m , and the number of different permutations corresponding to u_0 is μ , then the order of the system of conjugate substitutions associated with the equation is equal to $m \cdot \mu$.

Namely, if one has

$$u_0 = u_0' = u_0'' = \dots = u_0^{(\mu-1)}$$

where $u_0, u_0', \dots, u_0^{(\mu-1)}$ correspond to different permutations, and if these functions assume the substitution values $u_1, u_1', \dots, u_1^{(\mu-1)}$ belonging to a certain equation, then we have

$$u_1 = u_1' = u_1'' = \dots = u_1^{(\mu-1)}.$$

The number of permutations, that give the value u_1 , is thus at least equal to the number of those that give u_0 . On the other hand, it is also clear that the number of those that give u_0 is at least equal to the number of those that give u_1 ; so both numbers are equal, thereby justifying the assertion.

3. If we call the mutually different values assumed by u_0 in the system of conjugate substitutions $u_0, u_1, \dots, u_{m-1}$ associated with the equation, then these are roots of an irreducible equation of degree m , whose coefficients can be expressed rationally by known quantities.

If by a certain substitution φ $u_0, u_1, \dots, u_{m-1}$ belonging to the equation, we go over to $u_0', u_1', \dots, u_{m-1}'$, these latter must be included in the former; on the other hand, they must be mutually different; for from $u_i' = u_k'$ it follows, by applying the substitution φ^{-1} , that $u_i = u_k$, which is contrary to the assumption. From this it follows that $u_0', u_1', \dots, u_{m-1}'$ are the same as $u_0, u_1, \dots, u_{m-1}$ in some order. Since symmetric functions of $u_0, u_1, \dots, u_{m-1}$ are unchanged by all substitutions belonging to the equation, the equation

$$F(u) = (u - u_0)(u - u_1) \dots (u - u_{m-1}) = 0$$

has coefficients that can be expressed rationally by the known quantities. The irreducibility of this equation is therefore demonstrated. If u_0 is a root of an equation $F(u) = 0$ whose coefficients can be expressed rationally by the known quantities, then it follows immediately from the relations

$$F'(u) = 0 \text{ that } F'(u_0) = 0, F'(u_1) = 0, F'(u_2) = 0, \dots, F'(u_{m-1}) = 0.$$

Since such an equation must therefore be of degree m at least, $F(u) = 0$ is irreducible.

4. The system of conjugate substitutions belonging to the equation $F(u) = 0$ consists of the substitutions of the roots

$u_0 u_1 \dots u_{m-1}$, which are caused by performing the system of conjugate substitutions belonging to the given equation in the expressions of these quantities as functions of $x_0 x_1 \dots x_{n-1}$.

If the latter system is called S and the corresponding system of substitutions T , then any rational function of these that is unchanged by the substitutions T can be regarded as a function of the x 's that is unchanged by the substitutions S , and can thus be expressed rationally by the known quantities. A rational function of the r 's, on the other hand, which changes value by a substitution belonging to T , is a function of the r 's that changes by the corresponding substitution in S , and so cannot be expressed rationally by known quantities. T is thus really the system of conjugate substitutions belonging to the equation $F(u) = 0$.

I now return to the aforementioned transformation of the given equation. Let y denote a rational function of the roots $x_0 x_1 \dots x_{n-1}$, whose numerical value is unchanged by the substitutions $\left(\begin{smallmatrix} a^v k + b \\ k \end{smallmatrix} \right)$, but is variable by all other substitutions. This y then becomes a root in an irreducible equation of degree $(n(np+1)v)/nv$ or $np+1$, if the coefficients are known quantities.

If by a substitution ϕ belonging to the original system of conjugate substitutions, which for brevity I will denote by the letter S , y is transformed into y' , then y' remains unchanged by any substitution contained in the expression $\left(\begin{smallmatrix} \phi(a^v k + b) \\ \phi(k) \end{smallmatrix} \right)$. On the other hand, y' cannot remain unchanged by substitutions other than these $n \cdot v$ substitutions; for if, conversely, y' is transformed to y by ϕ^{-1} , it would follow that y remained unchanged by more than $n \cdot v$ substitutions. Each value of y thus corresponds to a partial system of conjugate substitutions of order n , which is equal to the system $\left(\begin{smallmatrix} a^v k + b \\ k \end{smallmatrix} \right)$ and thus contains one and only one of the $np+1$ sets of circular substitutions in S . Since every set can be derived from the set $\left(\begin{smallmatrix} k + b \\ k \end{smallmatrix} \right)$ by substitutions belonging to S , there is also a value of y ; as a result, two different values

of y cannot remain unchanged by the same set of circular substitutions. By derivation using the substitutions in S , the $np + 1$ sets of circular substitutions will thus correspond to each other in a way that can be expressed by the substitutions of the r 's caused by the same substitutions. These substitutions of the y 's now constitute precisely the system that belongs to the equation of the y 's; for brevity, let us denote this system by the letter T . T now contains at most $(np + 1) \cdot nv$ substitutions. If it contained fewer, T would have to contain substitutions that left all y 's unchanged. But if a substitution of the system S leaves the function that we initially denoted by y unchanged, then it is of the form $\left(\begin{smallmatrix} a^{v^i}k+b \\ k \end{smallmatrix} \right)$; if here $a^{v^i} \equiv 1$, it is circular, and according to what has been said above, such a substitution will exchange the other y 's in p circles, each consisting of n . If, on the other hand $a^{v^i} \not\equiv 1$, the substitution leaves an x ; if this is x_0 , then $b \equiv 0$. Let us denote $\left(\begin{smallmatrix} a^{v^i}k \\ k \end{smallmatrix} \right)$ by ϕ for a moment, and let $\phi y'$ corresponding to the set θ_1^r remain unchanged, then we must have $\phi \theta_1 \phi^{-1} = \theta_1^c$, just as we have $\phi \theta \phi^{-1} = \theta^{a^{v^i}}$. As a result, we get

$$\phi \theta \theta_1 \theta^{-1} = (\phi \theta \phi^{-1}) (\phi \theta_1 \phi^{-1}) (\phi \theta^{-1} \phi^{-1}) = \theta^{a^{v^i}} \theta_1^c \theta^{a^{v^i}}.$$

Since $a^{v^i} \not\equiv 1$, this circular substitution is not of the same set as $\theta \theta_1 \theta^{-1}$, and consequently ϕ does not leave y , corresponding to $\theta \theta_1 \theta^{-1}$, unchanged. Since, without changing the circular substitution $\left(\begin{smallmatrix} k+1 \\ k \end{smallmatrix} \right)$, any x can be denoted by x_0 , the same applies to the other substitutions of the form $\left(\begin{smallmatrix} a^{v^i}k+b \\ k \end{smallmatrix} \right)$, where $a^{v^i} \not\equiv 1$. So it has been proven that the system T really contains $(np + 1) \cdot n \cdot v$ substitutions.

Now as a result, the roots in the given equation can again be expressed as rational functions of the y 's. If the y 's are included among the known quantities, then, as is well known, under this new assumption, the system of conjugate substitutions in the given equation will retain only those substitutions in S for which

the y 's are unchanged, i.e. it will consist only of the identical substitution. Any rational function of the x 's can therefore be expressed rationally by the known quantities to which the y 's are now counted.

Any transitive system of conjugate substitutions of prime degree n and of order $(np + 1) \cdot n \cdot v$ can thus be derived from another transitive system of the same order, but of degree $np + 1$.

There are well-known examples of this; for $n = 5, 7, 11$, there are systems where $p = 1$, namely of order $(n + 1) n (n-1)$ for $n = 5$, and of order $(n + 1) n \cdot n-1 / 2$ for $n = 5, 7, 11$, of which the 5th degree contains all possible substitutions, the other half; those of the 7th and 11th degrees, on the other hand, fewer. Now, the equations to which these last two systems belong are first derived from equations of the 8th and 12th degrees, namely from the so-called modular equations in the theory of elliptic functions, belonging to transformations of the 7th and 11th degrees. A closer examination will also show that these modular equations really stand in the same relation to their reduced forms of the 7th and 11th degrees as the above equation of the y 's to the original equation of the degree n . Similarly, the modular equation belonging to the transformation of the 5th degree can be converted into an equation of the 5th degree. Now, according to G a l o i s (Lettre à M. Auguste Chevalier, Liouville's Journal, Volume 11, 1846), equations of degree n , whose system of conjugate substitutions is expressed by

$$\left(\frac{ak + b}{ck + d} \right),$$

e.g. modular equations, are transformed into other equations of degree n only in the cases mentioned.¹ If there are systems of conjugate substitutions of degree n and of order $(n + 1) n \cdot v$, where n is a prime number greater than 11, these must be derivable from other systems of degree $n + 1$ than those whose substitutions are of the form

¹ This part of Galois's assertion is not proven in Betti's work on this subject (Sopra l'abbassamento etc. Tortolini's Annaler 1853). I shall give the proof on another occasion.

$$\binom{\frac{ak+b}{ck+d}}{k}.$$

Of the theorems developed above, the following are proven by M a t h i e u in the frequently mentioned treatise. The number of sets of circular substitutions is of the form $np + 1$; if the order of the system is called $n r$, then r is divisible by a certain factor of $n - 1$; if this is v and $n - 1 = v \cdot v'$, the system contains the $n v$ substitutions $\binom{a^v k + b}{k}$. The number v is greater than 1, and, if n is of the form $4h + 3$, also greater than 2; finally, the system contains at least r/v sets of circular substitutions, since such a number can be derived from one of them using the substitutions of the system. To this I have added that the number of sets that could be derived using the substitutions of the system from any of them is of the form $np + 1$; this has provided a means of proving that these $np + 1$ sets in fact contain all the circular substitutions of the system; from this it further follows that the order of the system is the product of the three numbers denoting the degree, the number of sets of circular substitutions, and the number of substitutions that, when derived, leave any set unchanged. It thus becomes possible to specify both of these last numbers without knowing anything other than the order of the system. Finally, I will give a couple of examples of this.

M a t h i e u has shown that there are transitive systems of degree $q^r + 1$ and of order $(q^r + 1) q^r (q^r + 1) r/\tau$, when q is a prime number and q is a divisor of r . If $q = 2$ and r is a power of 2, it may be that $q^r + 1$ is a prime number. We then have

$n = 2^r + 1$ and $(2^r + 1) 2^r (2^r - 1) r/\tau = n (np + 1) \cdot v$,
from which it follows that $2^r (2^r - 1) \equiv 2 \pmod{n}$ and

$$v = 2 r/\tau, \text{ which is a divisor of } n-1 \text{ or } 2^r, \\ \text{and } np + 1 = 2^{r-1} (2^r - 1).$$

These systems thus contain $2 r/\tau$ substitutions of the form $\binom{ak}{k}$ and $2^{r-1} (2^r - 1)$ sets of circular substitutions.

Another example can be found in systems of conjugate substitutions, which are known from those equation theories solvable by root signs.

Let q be a prime number as before, and let us consider an equation of degree $q^r - 1$, whose roots are separated by r indices $i, k, \dots, m$, which assume all values according to the modulus q , except for the combination

$$i \equiv k \equiv l \equiv \dots \equiv m \equiv 0.$$

Let us further assume that the system of conjugate substitutions belonging to the equation consists of the

$$(q^r - 1) (q^r - q) (q^r - q^2) \dots (q^r - q^{r-1})$$

substitutions of the form

$$\left\{ \begin{array}{cccc} ai + bk + \dots + dm, & a_1 i + b_1 k + \dots + d_1 m, & \dots, & a_{r-1} i + b_{r-1} k + \dots + d_{r-1} m \\ i & k & \dots & m \end{array} \right\}.$$

These are now symmetrical functions of the $(q^r - 1)/(q - 1)$ systems of $q - 1$ roots, whose indices have the same relation to each other, so that these functions are all unchanged by the $q - 1$ substitutions of the form

$$\left\{ \begin{array}{cccc} a_i, & a_k, & \dots, & a_m \\ i, & k, & \dots, & m \end{array} \right\}$$

and would only be interchanged with each other by the other substitutions of the system. They are thus roots of an equation of degree $(q^r - 1)/(q - 1)$, whose system of conjugate substitutions is of the order

$$(q^r - 1)/(q - 1) (q^r - q) (q^r - q^2) \dots (q^r - q^{r-1}).$$

If r is an odd prime number, it may be that $(q^r - 1)/(q - 1)$ is a prime number. If $(q^r - 1)/(q - 1) = n$, it is easy to see that q is a primitive root in the congruence $z^r \equiv 1 \pmod{n}$, from which it follows that

$$(z^r - 1)/(z - 1) (z - q) (z - q^2) (z - q^3) \dots (z - q^{r-1}).$$

If we now set $z \equiv q^r \equiv 1$, we find

$$(q^r - q) (q^r - q^2) (q^r - q^3) \dots (q^r - q^{r-1}) \equiv r \pmod{n}.$$

In these systems we have $v = r$, which is a divisor of $n - 1$, and $np + 1 = (q^r - q/r) (q^r - q^2) (q^r - q^3) \dots (q^r - q^{r-1}).$

Théorèmes sur les groupes de substitutions

Théorèmes sur les groupes de substitutions | Mathematische Annalen | Springer Nature Link

SPRINGER NATURE Link

 Account

 Menu

 Search

 Cart

Home Mathematische Annalen Article

Théorèmes sur les groupes de substitutions

Published: December 1872

Volume 5, pages 584–594, (1872) Cite this article

Access provided by Nationallizenz periodicals archive

Download PDF 



Mathematische Annalen

Aims and scope

Submit manuscript

M. L. Sylow

 406 Accesses  73 Citations  3 Altmetric [Explore all metrics](#) →

[Download](#) to read the full article text

Author information

Authors and Affiliations

Frederiksiiald en Norvege, Norvege

M.L. Sylow

Rights and permissions

[Reprints and permissions](#)

About this article

Cite this article

Sylow, M.L. Théorèmes sur les groupes de substitutions. *Math. Ann.* 5, 584–594 (1872).

<https://doi.org/10.1007/BF01442913>

Issue date

December 1872

DOI

<https://doi.org/10.1007/BF01442913>

Share this article

Anyone you share the following link with will be able to read this content:

[Get shareable link](#)

Provided by the Springer Nature SharedIt content – sharing initiative

MATHEMATISCHE ANNALEN

HERAUSGEGEBEN

VON

A. CLEBSCH UND **C. NEUMANN**,
PROFESSOR IN GÖTTINGEN. PROFESSOR IN LEIPZIG.

V. Band.



LEIPZIG,
DRUCK UND VERLAG VON B. G. TEUBNER.
1872.

Inhalt des fünften Bandes.

(In alphabetischer Ordnung, abgesehen von einer an das Ende dieses Verzeichnisses gesetzten Preisaufgabe.)

	Seite
Du Bois-Reymond , in Freiburg i. Br. Summation der Reihe mit dem Glieder $\frac{p \sin pu}{h^2 + p^2}$	399
Brill , in Darmstadt. Ueber Elimination aus einem gewissen System von Gleichungen	378
————— Note über die Gleichung der auf einer Ebene abbildbaren Flächen	401
Cantor , in Halle a. d. S. Ueber die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen	123
————— Algebraische Notiz	133
Cayley , in Cambridge. On a theorem in Covariants	625
————— On the Non-Euclidian Geometry	630
Clebsch , in Göttingen. Ueber die geradlinigen Flächen vom Geschlechte $p = 0$	1
————— Ueber die ebene Abbildung einer Fläche dritter Ordnung	419
————— Ueber zwei Erzeugungsarten der ebenen Curven dritter Ordnung	422
————— Ueber eine Fundamentalaufgabe der Invariantentheorie	427
————— Ueber die Complexflächen und die Singularitätenflächen der Complexen	435
v. Drach , in Marburg. Ueber das vollständige Fünfeck und gewisse durch dasselbe bestimmte Kegelschnitte.	404
Durège , in Prag. Ueber die Curve 3 ^{ter} Ordnung, welche den geometrischen Ort der Brennpunkte einer Kegelschnittschaar bildet	83
Eckhardt , in Reichenbach im Voigtland. Beiträge zur analytischen Geo- metrie des Raumes, insbesondere zur Theorie der Flächen 3 ^{ten} Grades mit 4 Doppelpunkten und der Steiner'schen Flächen, sowie zur Lehre von den Raumcurven	30
Enneper , in Göttingen. Bemerkungen über die Enveloppe einer Fläche. .	304
Ermakoff , in Heidelberg. Ueber die Cylinderfunctionen	639
Gordan , in Giessen. Ueber Combinanten	95
————— Ueber das Pentaeder der Flächen dritter Ordnung	341
————— Ueber die simultanen Invarianten binärer Formen	595
Gundelfinger , in Tübingen. Ueber die Wendepunktdreiseite einer Curve dritter Ordnung	442
Klein , in Göttingen. Ueber Liniengeometrie und metrische Geometrie . .	257
————— Ueber gewisse in der Liniengeometrie auftretende Differential- gleichungen	278

	Seite
König, in Pest. Ueber die Darstellung von Functionen durch unendliche Reihen	310
Korkine, à St. Petersbourg. Sur les formes quadratiques positives quaternaires. (Zus. mit G. Zolotareff)	581
Lie, in Christiania. Ueber Complexe, insbesondere Linien- und Kugelcomplexe, mit Anwendung auf die Theorie partieller Differential-Gleichungen . .	145
Mareks †. Bestimmung der Ordnung und Classe der Krümmungsmittelpunktfäche einer Fläche n^{ter} Ordnung	27
Mayer, in Leipzig. Ueber unbeschränkt integrable Systeme von linearen totalen Differentialgleichungen und die simultane Integration linearer partieller Differentialgleichungen	448
Mehler, in Elbing. Ueber die Darstellung einer willkürlichen Function zweier Variablen durch Cylinderfunctionen	135
—— Notiz über die Dirichlet'schen Integralausdrücke für die Kugelfunction $P^*(\cos \vartheta)$ und über eine analoge Integralform für die Cylinderfunction $J(x)$	141
Neumann, in Leipzig. Ueber die Elementargesetze der Kräfte elektrodynamischen Ursprungs	602
Noether, in Heidelberg. Zur Theorie der eindeutigen Ebenentransformationen	635
Schröter, in Breslau. Ueber eine besondere Curve 3^{ter} Ordnung und eine einfache Erzeugungsart der allgemeinen Curve 3^{ter} Ordnung	50
Sylow, à Frederikshald en Norvege. Théorèmes sur les groupes de substitutions	584
Von der Mühl, in Leipzig. Ueber die Reflexion und Brechung des Lichtes an der Grenze unkrystallinischer Medien	471
Zolotareff, à St. Petersbourg. Sur la méthode d'intégration de M. Tschébychef	560
—— Sur les formes quadratiques positives quaternaires. (Zus. mit A. Korkine)	581
—————	
Preisaufrage der Beneke'schen Stiftung für das Jahr 1874, gestellt von der philosophischen Honorenfacultät der Universität Göttingen	397

MATHEMATISCHE ANNALEN

HERAUSGEGEBEN

VON

A. CLEBSCH UND **C. NEUMANN**,
PROFESSOR IN GÖTTINGEN. PROFESSOR IN LEIPZIG.

V. Band. 4. Heft.



LEIPZIG,
DRUCK UND VERLAG VON B. G. TEUBNER.
1872.

I N H A L T.

	Seite
Ueber die Reflexion und Brechung des Lichtes an der Grenze unkrystallinischer Medien. (Fortsetzung.) Von Karl Von der Mühl in Leipzig .	513
Sur la méthode d'intégration de M. Tchébychef. Par G. Zolotareff à St. Petersbourg	560
Sur les formes quadratiques positives quaternaires. Par A. Korkine et G. Zolotareff	581
Théorèmes sur les groupes de substitutions. Par M. L. Sylow à Frederikshald en Norvege	584
Ueber die simultanen Invarianten binärer Formen. Von Paul Gordan in Giessen	595
Ueber die Elementargesetze der Kräfte elektrodynamischen Ursprungs. Von Carl Neumann in Leipzig	602
On a theorem in Covariants. By A. Cayley, Cambridge	625
On the Non-Euclidian Geometry. By A. Cayley, Cambridge	630
Zur Theorie der eindeutigen Ebenentransformationen. Von M. Noether in Heidelberg	635
Ueber die Cylinderfunction. Von W. Ernakoff in Heidelberg	639

Verantwortliche Redaction: A. Clebsch und C. Neumann.



Mathematische Annalen

Publishing model
Hybrid

Bavarian State Library **Great news! Funding is available for open access publishing.**
[Explore open access funding](#) [Change institution](#)



Volume 5, Issue 4
December 1872

11 articles in this issue

Ueber die Reflexion und Brechung des Lichtes auf der Grenze unkrystallinischer Medien. (Fortsetzung)

Karl Von der Mühl

OriginalPaper | Pages: 513 - 559

Sur la méthode d'intégration de M. Tchébychef

G. Zolotareff

OriginalPape | Pages: 560 - 580

Verbesserung

Legacy | Pages: 580 - 580

Sur les formes quadratiques positives quaternaires

A. Korkine & G. Zolotareff

BriefCommunication | Pages: 581 - 583

Théorèmes sur les groupes de substitutions

M. L. Sylow

OriginalPaper | Pages: 584 - 594

Ueber die simultanen Invarianten binärer Formen

Paul Gordan

OriginalPaper | Pages: 595 - 601

Ueber die Elementargesetze der Kräfte elektrodynamischen Ursprungs

Carl Neumann

OriginalPaper | Pages: 602 - 624

On a theorem in covariants

A. Cayley

OriginalPaper | Pages: 625 - 629

On the Non-Euclidian geometry

Cayley

OriginalPaper | Pages: 630 - 634

Zur Theorie der eindeutigen Ebenentransformationen

M. Noether

OriginalPaper | Pages: 635 - 639

Ueber die Cylinderfunction

W. Ermakoff

BriefCommunication | Pages: 639 - 640

Théorèmes sur les groupes de substitutions.

Par M. L. SYLOW à FREDERIKSHALD en NORVEGE.

On sait que si l'ordre d'un groupe de substitutions est divisible par le nombre premier n , le groupe contient toujours une substitution d'ordre n . Ce théorème important est contenu dans un autre plus général que voici: „Si l'ordre d'un groupe est divisible par n^α , n étant premier, le groupe contient un faisceau partiel d'ordre n^α “. La démonstration même du théorème fournit quelques autres propriétés générales des groupes de substitutions. J'y ajouterai encore quelques propositions moins générales qui s'y rattachent ou qui en écoulent, dont quelques unes pourtant sont déjà connues par un travail de M. E. Mathieu.

Les notations et les termes employés sont ceux de M. C. Jordan.

1. Si G est un groupe de substitutions dont l'ordre N est divisible par le nombre premier n , on sait que G contient une substitution d'ordre n , mais nous pouvons supposer plus généralement qu'il contienne un groupe g d'ordre n^α , dont par conséquent chaque substitution est d'un ordre diviseur de n^α . Nous désignerons les substitutions de g par

$$1 \ \theta_1 \ \theta_2 \ \dots$$

tandis que les substitutions de G en général seront désignées par

$$1 \ \psi_1 \ \psi_2 \ \dots$$

Enfin nous supposerons que G ne contient aucun groupe partiel dont l'ordre est une puissance de n supérieure à n^α . Or G contient toujours des substitutions permutable à g , savoir les substitutions de ce dernier elles-mêmes, mais il est possible qu'il en contient un nombre plus grand; en tous cas ces substitutions forment un groupe γ , qui contient g , et dont l'ordre sera désigné par $n^\alpha \nu$; ce nombre est à son tour un diviseur de N ; nous pouvons donc faire:

$$N = n^\alpha \nu h.$$

Les substitutions du groupe γ seront désignées par

$$1 \ \varphi_1 \ \varphi_2 \ \dots$$

Les θ sont donc comprises parmi les φ , ainsi que celles-ci parmi les ψ .

Cela posé, nous allons d'abord démontrer que le nombre ν doit être premier à n . Soient $x_0 x_1 x_2 \dots$ les lettres que le groupe G permute entre elles, et soit y_0 une fonction rationnelle des x , invariable par les substitutions de g mais variable par toute autre substitution. Cette fonction prend par les substitutions de γ les ν valeurs différentes

$$y_0 y_1 y_2 \dots y_{\nu-1}.$$

Chacune de ces fonctions est invariable par les substitutions de g mais variable par toute autre substitution. En effet, si y_1 se déduit de y_0 par la substitution φ_1 , y_1 est invariable par le groupe transformé de g par φ_1 , mais variable par toute autre substitution; mais φ_1 étant permutable à g , le groupe transformé se confond avec g . Or si l'on opère dans les y les substitutions de γ , on aura entre ces quantités un groupe γ' nécessairement transitif et isomorphe à γ . Pour en avoir l'ordre il faut diviser celui de γ par le nombre des substitutions φ qui n'altèrent aucune des y , c'est-à-dire par n^α . L'ordre de γ' est donc ν . Si maintenant ν était divisible par n , γ' devrait contenir une substitution d'ordre n ; une substitution correspondante φ_1 de γ devrait remplir la condition

$$\varphi_1^n = \theta_a.$$

Mais puisque φ_1 est permutable à g , on voit que dans ce cas les substitutions $\theta_a \varphi_1^n$ formeraient un groupe d'ordre $n^{\alpha+1}$ contenu dans G . Cela étant contraire à l'hypothèse, on conclut que ν est premier à n .

Notons ici que les θ sont les seules substitutions de γ dont les ordres sont des puissances de n . En effet, si φ_1 est une substitution de γ étrangère à g , les substitutions $\theta_a \varphi_1^n$ forment un groupe dont l'ordre est égal à $n^\alpha m$, m désignant l'exposant de la puissance la moins élevée de φ_1 qui appartient à g . Or on voit sans peine que les seules puissances de φ_1 qui appartiennent à g sont celles dont les exposants sont des multiples de m , d'où il suit immédiatement que m est un diviseur de l'ordre de φ_1 . Si donc l'ordre de φ_1 était une puissance de n , on aurait $m = n^\beta$, ce qui est impossible, le groupe des $\theta_a \varphi_1^n$ ne pouvant être d'ordre $n^{\alpha+\beta}$.

Le nombre h n'est pas non plus divisible par n . Pour le faire voir imaginons une fonction rationnelle des x invariable par les substitutions de γ , mais variable par toute autre substitution. Soit z_0 cette fonction, et représentons par

$$z_0 z_1 z_2 \dots z_{h-1}$$

les h valeurs qu'elle prend par les substitutions de G . Effectuons dans les z les substitutions de g ; par cela z_0 ne varie pas, mais chacune des autres z prend un nombre de valeurs qui est un diviseur de l'ordre de g , c'est-à-dire une puissance de n . Cette puissance ne peut se réduire à l'unité; si par exemple z_1 était invariable par g

et que z_1 se déduise de z_0 par la substitution ψ_1 , z_0 devrait être invariable par le groupe transformé de g par ψ_1^{-1} ; or, le seul groupe d'ordre n^a contenu dans γ étant g , ψ_1^{-1} devrait être permutable à g , ce qui n'a pas lieu. Si donc on partage les fonctions $z_1 \dots z_{k-1}$ en systèmes, en réunissant ensemble celles qui se permutent entre elles par les substitutions de g , le nombre de fonctions contenues dans chaque système sera une puissance de n . Par conséquent le nombre h est de la forme $np + 1$. L'ordre de g égale donc la plus grande puissance de n qui divise l'ordre de G . Les résultats obtenus se résument ainsi:

Théorème I. Si n^a désigne la plus grande puissance du nombre premier n qui divise l'ordre du groupe G , ce groupe contient un autre g de l'ordre n^a ; si de plus n^av désigne l'ordre du plus grand groupe contenu dans G dont les substitutions sont permutables à g , l'ordre de G sera de la forme $n^av (np + 1)$.

2. Évidemment g n'est pas le seul groupe d'ordre n^a contenu dans G , excepté seulement le cas $p = 0$. Mais on pourrait demander si G en contient d'autres que g et ses transformés par les substitutions de G . Voilà ce que nous allons rechercher. Soit g' un groupe d'ordre n^a contenu dans G mais différent de g , et soient

$$1 \theta'_1 \theta'_2 \dots$$

ses substitutions. Effectuons ces substitutions dans les fonctions z , et réunissons en systèmes celles qui par cela s'échangent entre elles. Comme nous l'avons déjà dit, le nombre des fonctions contenues dans chaque système doit être un diviseur de n^a ; on doit donc avoir une égalité de la forme

$$np + 1 = n^a + n^b + n^c + \dots$$

$n^a, n^b, n^c \dots$ désignant le nombre des fonctions contenues dans les divers systèmes. Mais cela exige qu'au moins un des exposants $a b c \dots$ soit nul; en d'autres termes, il faut qu'au moins une des fonctions z soit invariable par toutes les substitutions de g' . Soit z_k cette fonction, et supposons qu'elle se déduise de z_0 par la substitution ψ_k . On z_k n'est invariable que par les substitutions $\psi_k^{-1} \varphi_a \psi_k$; de plus $\psi_k^{-1} \varphi_a \psi_k$ est semblable à φ_a , et parmi les φ_a il n'y a que les θ dont les ordres sont des puissances de n . Il faut donc qu'on ait

$$\theta'_b = \psi_k^{-1} \theta_a \psi_k$$

pour toutes les valeurs de b . Le groupe g' est donc le transformé de g par ψ_k .

Si d'ailleurs on remplace ψ_k par $\varphi_r \psi_k$, on a évidemment le même groupe transformé. De l'autre côté ψ_k ne peut être remplacée que par $\varphi_r \psi_k$. En effet, si l'on a

$$\psi_l^{-1} \theta_a \psi_l = \psi_k^{-1} \theta_b \psi_k$$

pour toute valeur de a , il s'ensuit

$$\psi_k \psi_l^{-1} \theta_a \psi_l \psi_k^{-1} = \theta_b$$

d'où l'on conclut

$$\psi_l \psi_k^{-1} = \varphi_r$$

ou

$$\psi_l = \varphi_r \psi_k.$$

On peut donc énoncer ce théorème:

Théorème II. Tout étant posé comme au théorème précédent, le groupe G contient précisément $np + 1$ groupes distincts d'ordre n^a ; on les obtient tous en transformant l'un quelconque d'entre eux par les substitutions de G , tout groupe étant donné par $n^a v$ transformantes distinctes.

Par un raisonnement analogue on voit que tout groupe contenu dans G d'ordre n^b , b étant moindre que a , est le transformé d'un groupe contenu dans g par une substitution de G , et qu'il y a au moins $n^a v$ manières de l'obtenir par transformation. Il est en effet possible qu'il y en ait plus, puisque de la relation

$$\psi_k \psi_l^{-1} \theta_a \psi_l \psi_k^{-1} = \theta_b$$

on ne peut conclure

$$\psi_l \psi_k^{-1} = \varphi_r$$

à moins qu'elle n'ait lieu pour toute valeur de a .

3. Nous allons maintenant nous occuper du groupe g . Formons les transformées des substitutions $1\theta, \theta_2, \dots$ par une d'elles; comme par cela on ne fait que les reproduire dans un autre ordre, on a une substitution entre les substitutions θ elles mêmes. Si on les transforme successivement par toutes les substitutions de g , on a un groupe de substitutions; cela résulte en effet immédiatement de l'identité:

$$\theta_b^{-1} \theta_a^{-1} \theta_r \theta_a \theta_b = (\theta_a \theta_b)^{-1} \theta_r (\theta_a \theta_b).$$

Le groupe entre les θ qu'on obtient de cette manière est nécessairement intransitif, la substitution identique au moins étant invariable par les transformations; mais il y a aussi d'autres substitutions invariables, comme nous allons voir. En effet on peut réunir en systèmes celles des substitutions qui s'échangent entre elles par les transformations; cela fait, les transformations produiront un groupe transitif entre les substitutions de chaque système. Or le nombre de substitutions θ contenues dans un système est un diviseur de l'ordre du groupe correspondant; mais on voit par un raisonnement familier que l'ordre de ce groupe est égal à n^a divisé par le nombre des transformations qui ne font varier aucune des substitutions du système considéré. Ainsi donc le nombre de substitutions contenues dans chaque système est une puissance de n . La substitution identique étant invariable, on doit avoir une égalité de la forme

$$n^a = 1 + n^a + n^b + \dots$$

où $1n^an^b \dots$ sont les nombres des substitutions des divers systèmes. Cela exige qu'au moins $n - 1$ des exposants $ab \dots$ soient nuls. Il y a donc dans le groupe g au moins n substitutions, y comprise la substitution identique, qui sont invariables; en d'autres termes il y a dans g au moins n substitutions échangeables à toutes les substitutions du groupe.

Or puisque, deux substitutions étant échangeables, leurs puissances le sont également, il y aura toujours parmi les substitutions échangeables à toutes les autres une substitution d'ordre n . Soit θ_0 cette substitution, et soit y_0 une fonction rationnelle des x , invariable par θ_0^i mais variable par toute autre substitution, et représentons par

$$y_0 \ y_1 \ y_2 \ \dots$$

les n^{a-1} valeurs qu'elle prend par les substitutions de g . En effectuant dans les y les substitutions de g on aura entre ces fonctions un groupe isomorphe à g , dont l'ordre est évidemment n^{a-1} . En vertu de ce qui vient d'être démontré ce groupe doit contenir une substitution d'ordre n échangeable à toutes les substitutions du groupe. Soit maintenant θ_1 une substitution correspondante de g . Effectuée n fois de suite θ_1 doit ramener toutes les y à leurs places primitives, donc

$$\theta_1^n = \theta_0^a.$$

De plus, si ϑ désigne une substitution quelconque de g , θ_1 doit produire entre les y la même substitution que sa transformée par ϑ , c'est-à-dire, on a

$$\vartheta^{-1} \theta_1 \vartheta = \theta_0^b \theta_1.$$

Les substitutions $\theta_0^i \theta_1^k$ constituent évidemment un groupe d'ordre n^2 . Si maintenant on forme une fonction rationnelle des x invariable par les $\theta_0^i \theta_1^k$, mais variable par toute autre substitution, et qu'on raisonne sur cette fonction, comme nous avons raisonné sur y_0 , on voit que g doit contenir une substitution θ_2 qui remplit les conditions

$$\theta_2^n = \theta_0^c \theta_1^d$$

$$\vartheta^{-1} \theta_2 \vartheta = \theta_0^e \theta_1^f \theta_2.$$

En continuant ainsi on démontre le théorème suivant:

Théorème III. Si l'ordre d'un groupe est n^a , n étant premier, une substitution quelconque ϑ du groupe peut être exprimée par la formule

$$\begin{aligned} \vartheta &= \theta_0^i \theta_1^k \theta_2^l \dots \theta_{a-1}^r \\ \text{où} \quad \theta_0^n &= 1 \\ \theta_1^n &= \theta_0^a \\ \theta_2^n &= \theta_0^b \theta_1^c \\ \theta_3^n &= \theta_0^d \theta_1^e \theta_2^f \\ &\dots \end{aligned}$$

et où l'on a

$$\begin{aligned}\vartheta^{-1} \theta_0 \vartheta &= \theta_0 \\ \vartheta^{-1} \theta_1 \vartheta &= \theta_0^{\beta} \theta_1 \\ \vartheta^{-1} \theta_2 \vartheta &= \theta_0^{\gamma} \theta_1^{\delta} \theta_2 \\ \vartheta^{-1} \theta_3 \vartheta &= \theta_0^{\epsilon} \theta_1^{\zeta} \theta_2^{\eta} \theta_3 \\ &\dots \dots \dots\end{aligned}$$

On voit que les facteurs de composition du groupe sont tous égaux à n , nous pouvons donc énoncer comme corollaire la proposition suivante :

Si l'ordre d'une équation algébrique est une puissance d'un nombre premier, l'équation est résoluble par radicaux.

Supposons que le groupe g soit transitif et que le nombre des lettres soit égal à n^{β} . Dans ce cas la substitution que nous avons nommée θ_0 est régulière, c'est-à-dire qu'elle déplace toutes les lettres, et que toutes ces cycles en contiennent un même nombre; car autrement elle ne serait pas évidemment échangeable à toutes les substitutions du groupe. De plus le groupe sera imprimitif; en effet les substitutions remplaceront les lettres contenues dans un même cycle de θ_0 par des lettres d'un même cycle. Donc l'équation le partagera par la résolution d'une équation de degré $n^{\beta}-1$ en $n^{\beta}-1$ équations de degré n . Évidemment les groupes de ces dernières équations, ainsi que celui de l'équation auxiliaire, ne contiendront que des substitutions dont les ordres sont des puissances de n ; les équations de degré n seront par suite abéliennes. Donc :

Théorème IV. Si le degré d'une équation irréductible est n^{β} , n étant premier, et que l'ordre de son groupe soit également une puissance de n , l'une quelconque de ses racines se déterminera par une suite de β équations abéliennes de degré n .

Pour le cas $n = 2$ cette dernière proposition a été démontrée par M. J. Petersen (Om de Ligninger, der kunne løses ved Kvadratrods etc. Kjöbenhavn 1871).

Ces résultats peuvent même être généralisés. En effet, si l'ordre du groupe d'une équation est égal à $n^{\alpha}m$, m étant moindre que n , on a, en employant le théorème I, $p = 0$, $m = v$. Par suite toutes les substitutions du groupe sont permutables au groupe partiel que nous avons désigné par g . Le groupe se réduit donc à g , si l'on adjoint les fonctions que nous avons désignées par $y_0 y_1 \dots$, et qui sont les racines d'une équation dont l'ordre et le degré sont égaux à m . Si donc l'équation auxiliaire est résoluble par radicaux, l'équation donnée l'est également. De là s'ensuit comme conséquence immédiate :

Théorème V. Si l'ordre d'une équation algébrique est

$$n^{\alpha} n_1^{\alpha_1} n_2^{\alpha_2} n_3^{\alpha_3} \dots,$$

$n, n_1, n_2, n_3 \dots$ étant premiers, si de plus on a

$$n > n_1^{\alpha_1} n_2^{\alpha_2} n_3^{\alpha_3} \dots$$

$$n_1 > n_2^{\alpha_2} n_3^{\alpha_3} \dots$$

$$n_2 > n_3^{\alpha_3} \dots$$

l'équation est résoluble par radicaux.

4. De ce qui précède on tire aussi une démonstration simple du théorème de M. E. Mathieu: *Tout groupe transitif entre n^α lettres, n désignant un nombre premier, contient une substitution régulière d'ordre n .* (Voir le journal de M. Liouville 1861.)

Soit G un groupe transitif de degré $n^\alpha m$, et soit N son ordre. Or N est divisible par $n^\alpha m$; faisons donc

$$N = n^{\alpha+\beta} m N',$$

N' étant supposé premier à n ; soit de plus G' le groupe d'ordre $n^\beta N'$ qui contient les substitutions de G qui ne déplacent pas x_0 . Maintenant G contient un groupe g d'ordre $n^{\alpha+\beta}$, et les substitutions de ce dernier qui ne déplacent pas x_0 forment un groupe g' , dont nous désignerons l'ordre par n^γ . Or g' est évidemment contenu dans G' , donc on a

$$\gamma \leq \beta.$$

Mais si l'on désigne par r le nombre des places qui sont successivement occupées par x_0 , quand on effectue toutes les substitutions de g , on a, comme on sait,

$$r n^\gamma = n^{\alpha+\beta}$$

$$\text{donc} \quad r \geq n^\alpha.$$

Le nombre r est nécessairement une puissance de n ; d'ailleurs ce qui vient d'être démontré pour x_0 a aussi lieu pour chacune des x . Donc chaque lettre prend par le groupe g un nombre de places qui est une puissance de n égale ou supérieure à n^α .

Si maintenant on suppose $m = 1$, on voit que g doit être transitif. Cela étant, g doit contenir une substitution régulière comme nous l'avons déjà dit. Le théorème est donc démontré.

Il y a un autre cas où l'on peut également démontrer l'existence de substitutions régulières. Supposons en effet $\alpha = 1$ avec $m < n$. Puisque $n^2 > mn$, on conclut que chaque lettre prend par les substitutions de g précisément n places différentes. Si donc m réunit dans un même système les lettres qui s'échangent entre elles, on aura m systèmes de n lettres chacun. Soit maintenant c un cycle d'une substitution de g , c représentera une substitution circulaire des n lettres d'un même système. Or si une autre substitution de g fait subir aux mêmes lettres un déplacement, ce déplacement ne sera autre chose qu'une puissance de c , car dans le cas contraire on pourrait des deux substitutions dériver une troisième qui ne soit pas d'ordre n . Soit donc θ une substitution de g , on a

$$\theta = c_1 c_2 \dots c_r$$

c_k désignant une substitution circulaire entre les lettres du $k^{\text{ième}}$ système. Si maintenant $r < m$, le groupe g doit contenir une substitution θ_1 qui permute les lettres du $(r+1)^{\text{ième}}$ système, et d'après ce qui vient d'être dit on a

$$\theta_1 = c_1^\delta c_2^\varepsilon \dots c_r^\xi c_{r+1} c_{r+2} \dots c_s,$$

les nombres $\delta \varepsilon \dots \xi$ pouvant être nuls. On en tire

$$\theta^p \theta_1 = c_1^{p+\delta} c_2^{p+\varepsilon} \dots c_r^{p+\xi} c_{r+1} c_{r+2} \dots c_s.$$

Or, puisque le nombre des systèmes est inférieur à n , on peut déterminer p de sorte qu'aucun des nombres $p + \delta, p + \varepsilon, \dots p + \xi$ ne soit égal à zéro. On obtient ainsi une substitution ayant $r + s$ cycles. Si $r + s < m$, on déterminera de la même manière une substitution de g qui a plus de $r + s$ cycles; en continuant ainsi on finira par trouver une substitution régulière.

Théorème VI. Une groupe transitif entre nm lettres, n étant premier, et $m < n$, contient une substitution régulière d'ordre n .

En vertu de ces deux théorèmes tout groupe transitif entre un nombre de lettres moindre de 12 contient des substitutions régulières. Mais déjà pour le degré 12 il existe des groupes transitifs qui en sont dépourvus. Ainsi les substitutions du groupe dérivé de

$$\begin{aligned}\theta_0 &= (x_0 x_1 x_2) (x_3 x_4 x_5) (x_6 x_7 x_8) \\ \theta_1 &= (x_3 x_4 x_5) (x_6 x_8 x_7) (x_9 x_{10} x_{11}) \\ \varphi &= (x_0 x_3 x_6 x_9 x_1 x_4 x_5 x_{11}) (x_2 x_5 x_7 x_{10})\end{aligned}$$

sont semblables les unes à θ_0 , les autres aux puissances de φ . Un autre exemple est le groupe dérivé de $\theta_0 \theta_1$ et des substitutions suivantes

$$\begin{aligned}(x_0 x_3 x_1 x_4) (x_2 x_5) (x_6 x_9 x_7 x_{11}) (x_8 x_{10}) \\ (x_0 x_7 x_1 x_6) (x_2 x_8) (x_3 x_9 x_4 x_{11}) (x_5 x_{10}).\end{aligned}$$

Ces deux groupes sont d'ordre 72, et caractérisent des équations résolubles par radicaux.

5. Considérons maintenant les groupes transitifs de degré premier. Soit n le degré, N l'ordre du groupe. Puisque N est divisible par n mais non divisible par n^2 , on a

$$N = nv (np + 1)$$

Supposons les lettres rangées dans un ordre tel qu'une substitution circulaire du groupe est exprimée par

$$\theta = |k \ k + 1|;$$

alors les substitutions permutables au groupe dérivé de θ sont de la forme

$$|k \ ak + b|$$

Or nv est égal à l'ordre de ce dernier groupe, donc v est égal au nombre des substitutions du groupe donné qui sont de la forme $|k \ ak|$; v est donc un diviseur de $n - 1$. On a donc ce théorème:

Théorème VII. L'ordre d'un groupe transitif entre un nombre premier de lettres est de la forme $nv (np + 1)$, où n est le degré, $np + 1$ le nombre des substitutions régulières essentiellement différentes, c'est-à-dire, qui ne sont pas des puissances les unes des autres, et où v est le nombre des substitutions de la forme $|k \ ak|$, une substitution circulaire quelconque étant désignée par $|k \ k + 1|$.

Ces résultats sont en partie connus par les recherches de M. E. Mathieu, qui a démontré que le nombre des substitutions circulaires essentiellement différentes est de la forme $np + 1$, et qu'il y en a au moins $\frac{N}{nv}$, un tel nombre pouvant être déduit des $|k \ k + b|$ en les transformant par les substitutions du groupe. Ce qu'il faut ajouter aux propositions de M. Mathieu pour avoir le théorème ci-dessus c'est donc que toutes les substitutions circulaires peuvent être déduites de la manière mentionnée, un point sur lequel M. Mathieu semble avoir conservé des doutes.

Qu'on se rappelle ici ces deux propositions également dues à M. E. Mathieu:

- 1) Si $p > 0$, v ne peut être égal à 1.
- 2) Si $p > 0$, et que n soit de la forme $4h + 3$, v ne peut être égal à 2.

Étant donné l'ordre N d'un groupe transitif entre n lettres, notre théorème permet de déterminer le nombre des substitutions circulaires et le nombre des substitutions permutable au groupe dérivé d'une substitution circulaire. En effet v , étant moindre que n , est complètement déterminé par la congruence

$$\frac{N}{n} \equiv v \pmod{n};$$

et puis on a

$$np + 1 = \frac{N}{nv}.$$

Prenons pour exemple le groupe du degré $\frac{q^r - 1}{q - 1}$, q étant un nombre premier, que l'on peut déduire du groupe linéaire à r indices. Si r est un nombre premier impair, il peut arriver que $\frac{q^r - 1}{q - 1}$ est un nombre premier. Faisons donc

$$n = \frac{q^r - 1}{q - 1}$$

$$N = \frac{q^r - 1}{q - 1} (q^r - q) (q^r - q^2) \dots (q^r - q^{r-1}).$$

Or on voit aisément que q est une racine primitive de la congruence

$$z^r \equiv 1 \pmod{n};$$

par suite on a

$$z^{r-1} + z^{r-2} + \dots + z + 1 \equiv (z - q)(z - q^2) \dots (z - q^{r-1}).$$

Si maintenant on fait

$$z \equiv q^r \equiv 1,$$

on obtient

$$(q^r - q)(q^r - q^2) \dots (q^r - q^{r-1}) \equiv r.$$

c'est-à-dire

$$\frac{N}{n} \equiv r$$

Si donc on choisit les indices de sorte qu'une substitution circulaire est représentée par $|k \ k+1|$, le groupe contiendra r substitutions de la forme $|k \ q^i k|$; le nombre des substitutions circulaires essentiellement différentes sera $\frac{q^r - q}{r} (q^r - q^2) \dots (q^r - q^{r-1})$.

La formule $N = nv(np + 1)$ réduit considérablement le nombre des diviseurs du produit $2 \cdot 3 \dots n$ propres à désigner l'ordre d'un groupe transitif. Si par exemple on fait $n = 7$, v doit être égal à 6 ou à 3, excepté pour les équations résolubles par radicaux. Mais s'il existe un groupe d'ordre $7(7p + 1)6$, il y en a aussi un d'ordre $7(7p + 1)3$ contenant celles des substitutions du premier groupe qui équivalent à un nombre pair de transpositions. Pour avoir les valeurs de $7p + 1$ il suffit donc d'examiner le cas $n = 3$; donc $7p + 1$ doit être un diviseur du nombre $2 \cdot 5 \cdot 4 \cdot 3$, et par conséquent égal à un des nombres $1, 2^3, 5 \cdot 3, 5 \cdot 3 \cdot 2^3$, dont le troisième doit être rejeté, puisqu'il n'y a pas de groupe d'ordre $5 \cdot 3$ entre 6 lettres. Pour $n = 11$ il n'y aura que 15 cas à examiner etc.

Examinons maintenant la composition des groupes en question. Soient donc G et H deux groupes transitifs, et soit G contenu dans H et permutable à ses substitutions. Soit de plus $n(np + 1)v$ l'ordre de G , et désignons par $\theta_0 \theta_1 \dots \theta_{np}$ ses substitutions circulaires essentiellement différentes. G contient donc les $np + 1$ groupes d'ordre n : $\theta_0^r, \theta_1^r, \dots, \theta_{np}^r$. Si l'on transforme ces groupes par une substitution circulaire quelconque de H , qui sera désignée par θ' , on doit les reproduire dans un autre ordre; on a donc une substitution entre les $np + 1$ groupes. Mais on voit sans peine que si un groupe θ_i^r n'est pas invariable par la transformation, il doit faire partie d'un cycle de n groupes. Donc au moins un des groupes est invariable par la transformation. Si nous supposons que c'est θ_0^r , ce groupe est permutable à θ' , d'où l'on conclut

$$\theta' = \theta_0^s.$$

En effet, si l'on choisit les indices de sorte que

$$\theta_0 = |k \ k + 1|,$$

il n'y a parmi les $n(n-1)$ substitutions $|k \ ak + b|$, seules permutable à θ_0 , que les $|k \ k + b|$ qui sont d'ordre n . Toutes les substitutions circulaires de H font donc partie de G .

Réciproquement, si G et H contiennent les mêmes substitutions circulaires et que H contienne G , H est composé avec G . Soit toujours $n(np+1) \nu$ l'ordre de G , celui de H sera $n(np+1) \nu \nu_1$, ν_1 étant un diviseur de $\frac{n-1}{\nu}$. Les substitutions de la forme $|k \ ak|$ contenues dans H sont les puissances d'une seule d'entre elles; désignons celle-là par φ ; celles qui appartiennent à G seront par conséquent les puissances de φ^{ν_1} . Or il est facile à voir que H dérive des substitutions $\theta_0 \theta_1 \dots \theta_{np} \varphi$. En effet le groupe dérivé de ces substitutions est contenu dans H ; de l'autre côté son ordre ne peut être moindre que $n(np+1) \nu \nu_1$, puisqu'il a $np+1$ substitutions circulaires et $\nu \nu_1$ substitutions $|k \ ak|$. De même G dérive des substitutions $\theta_0 \theta_1 \dots \theta_{np} \varphi^{\nu_1}$. G est donc permutable aux substitutions de H , s'il est permutable à φ . Or cela a lieu, car premièrement les transformées de $\theta_0 \theta_1 \dots \theta_{np}$ par φ sont des substitutions circulaires appartenant à H et par suite à G ; secondement φ^{ν_1} est échangeable à φ .

Ainsi nous avons démontré le théorème suivant:

Théorème VIII. Pour qu'un groupe transitif de degré premier soit composé avec un groupe partiel, il faut et il suffit que le second groupe possède toutes les substitutions circulaires du premier.

Soit donnée une équation dont le groupe est H . Si l'on forme une fonction des racines invariable par les substitutions de G , mais variable par toute autre substitution, elle sera évidemment racine d'une équation abélienne de degré ν_1 . En adjoignant cette fonction on réduit le groupe de l'équation à G .

Si donc une équation irréductible de degré n est composée, elle devient simple par l'adjonction de la racine d'une équation abélienne, dont le degré est un diviseur de $n-1$.

En supposant $p=0$, on retombe sur une propriété connue des équations résolubles par radicaux.

Sylow, L.

Theorems on the theory of substitutions. (Théorèmes sur les groupes de substitutions.)

(French) JFM 04.0056.02

Clebsch Ann. V, 584-594 (1872).

Bezeichnet n^a die höchste Potenz der Primzahl n , welche die Ordnung von G theilt, so enthält diese Gruppe eine andere von der Ordnung n^a . Hieran schliessen sich ähnliche Theoreme über enthaltene Gruppen. Wenn die Ordnung einer algebraischen Gleichung $= n^a n_1^a n_2^a \dots$ ist, wobei $n, n_1, n_2, \dots$ Primzahlen sind, und $n > n_1 + n_2 + \dots$, $n_1 > n_2 + \dots$ ist, so ist die Gleichung durch Wurzeln lösbar. Es folgt eine Untersuchung der wichtigsten Eigenschaften transitiver Gruppen.

Reviewer: Netto, Dr. (Berlin)

<https://zbmath.org/04.0056.02> and <https://zbmath.org/pdf/02718820.pdf>

The Early Proofs of Sylow's Theorem

Articles | Volume 21 | Archive for History of Exact Sciences

SPRINGER NATURE Link

 Account

[Home](#) [Archive for History of Exact Sciences](#) [Articles](#)



Archive for History of Exact Sciences

Publishing model: Hybrid

Great news! Funding is available for open access publishing.
Bavarian State Library [Explore open access funding](#) [Change institution](#)

Articles

Filter by Volume

Volume 21 (1980)



Sort by Date published

☒ Old to new

Showing 1–14 of 14 articles

[Chu Shih-chieh's Suan-hsüeh ch'i-meng \(introduction to mathematical studies\)](#)

OriginalPaper Pages: 1 – 31

[On the emergence of probability](#)

OriginalPaper Pages: 33 – 53

[Physics in the shadow of mathematics: The Göttingen electron-theory seminar of 1905](#)

OriginalPaper Pages: 55 – 89

[Newton's "Achromatic" dispersion law: Theoretical background and experimental evidence](#)

OriginalPaper Pages: 91 – 128

<https://link.springer.com/journal/407/articles?filter-by-volume=21&sortBy=oldestFirst>

1/2

Articles | Volume 21 | Archive for History of Exact Sciences

The Gibbs-Wilbraham phenomenon: An episode in fourier analysis

OriginalPaper Pages: 129 – 160

Heaviside's operational calculus and the attempts to rigorise it

OriginalPaper Pages: 161 – 200

Aristotele e l'incommensurabilità

OriginalPaper Pages: 201 – 228

The problem of coincidences

OriginalPaper Pages: 229 – 244

Optics and the theory of the punctiform ether

OriginalPaper Pages: 245 – 278

The early proofs of Sylow's theorem

OriginalPaper Pages: 279 – 290

Hipparchus's determination of the length of the tropical year and the rate of precession

OriginalPaper Pages: 291 – 309

Experimental investigations of double refraction from Huygens to Malus

OriginalPaper Pages: 311 – 373

Olinde Rodrigues' paper of 1840 on transformation groups

OriginalPaper Pages: 375 – 385

A postscript to my article "Riemann, Betti and the Birth of Topology"

Legacy Pages: 387 – 387

Volume 21, Issue 3 | Archive for History of Exact Sciences

SPRINGER NATURE Link

 Account

Home Archive for History of Exact Sciences
Volume 21, Issue 3

Volumes and Issues



Archive for History of Exact Sciences

Publishing model: Hybrid

Great news! Funding is available for open access publishing.
Bavarian State Library Explore open access fundingChange institution



Volume 21, Issue 3 September 1980

4 articles in this issue

Aristotele e l'incommensurabilità

OriginalPaper Pages: 201 – 228

The problem of coincidences

OriginalPaper Pages: 229 – 244

Optics and the theory of the punctiform ether

OriginalPaper Pages: 245 – 278

The early proofs of Sylow's theorem

OriginalPaper Pages: 279 – 290

<https://link.springer.com/journal/407/volumes-and-issues/21-3>

[Home](#) [Archive for History of Exact Sciences](#) [Article](#)

The early proofs of Sylow's theorem

Published: September 1980

Volume 21, pages 279–290, (1980) [Cite this article](#)

Access provided by Nationallizenz periodicals archive

[Download PDF](#) 



[Archive for History of Exact Sciences](#)

[Aims and scope](#)

[Submit manuscript](#)

[William C. Waterhouse](#)



476 Accesses



14 Citations



11 Altmetric



1 Mention

[Explore all metrics](#)

[Download](#) to read the full article text

Author information

Authors and Affiliations

Department of Mathematics, The Pennsylvania State University, University Park
William C. Waterhouse

Additional information

Communicated by B.L. VAN DER WAERDEN

Rights and permissions

[Reprints and permissions](#)

About this article

Cite this article

Waterhouse, W.C. The early proofs of Sylow's theorem. *ArchRational Mech.* 21, 279–290 (1980). <https://doi.org/10.1007/BF00327877>

Received 10 September 1979

Issue date September 1980

DOI

<https://doi.org/10.1007/BF00327877>

Share this article

Anyone you share the following link with will be able to read this content:

[Get shareable link](#)

Provided by the Springer Nature SharedIt content sharing initiative

Keywords

[Early Proof](#)

Waterhouse, William C.

The early proofs of Sylow's theorem. (English) Zbl 0436.01006

Arch. Hist. Exact Sci. 21, 279-290 (1979).

Waterhouse, William C.:

01006

The early proofs of Sylow's theorem.

Arch. Hist. Exact Sci. 21, 279-290 (1979).

Cette étude a pour objet l'analyse des diverses démonstrations établies pour le théorème de Sylow dans les premiers quinze ans après sa découverte, en 1872. On sait que, par son cours sur la théorie des groupes de substitution L. Sylow, professeur à l'Université Cristiania de Norvège, fut un des mathématiciens qui ont contribué à la diffusion et au développement de l'oeuvre de Galois. Le présent article nous fait assister ainsi à un des plus intéressants épisodes concernant la théorie des groupes, il y a un siècle. Fl.T. Câmpan.

The Early Proofs of Sylow's Theorem

WILLIAM C. WATERHOUSE

Communicated by B.L. VAN DER WAERDEN

1. Introduction

The early history of SYLOW's theorem is surprisingly unfamiliar. A recent bulky history of mathematics, for instance, recounts that "Having arrived at the abstract notion of a group, the mathematicians turned to proving theorems about abstract groups that were suggested by known results for concrete cases. Thus Frobenius proved Sylow's theorem for finite abstract groups."¹ Now a moment's thought shows that this in itself is not much of an accomplishment: any finite group can be realized as a group of permutations (CAYLEY's theorem), and so SYLOW's theorem for permutation groups implies the abstract result. The reader then wonders whether FROBENIUS somehow did not know CAYLEY's theorem. But a glance at the paper in question² shows that FROBENIUS not only mentioned that result but had included it in one of his own earlier publications. Obviously more careful analysis is needed to grasp what FROBENIUS was actually doing.

The specific purpose of this paper is precisely to analyze the various different proofs that were given for SYLOW's theorem in the first fifteen years after its discovery. This is of interest in itself, since the theorem is still basic, and the major lines of argument now known all turn out to have been discovered in some form by that time. But also, by tracing this single theorem through a crucial period in the development of group theory, we will see more generally how the introduction of new ideas throws new light on the same result. Indeed, we almost have a case study in levels and use of abstraction. Some of the authors still thought of changes of variable in polynomials, others applied group-theoretic reasoning to permutation groups, and finally FROBENIUS himself made serious use of abstract groups. In addition to the advance, the continuity in this development will also be illuminated, since we will see techniques equivalent to the construction of coset actions and quotient groups used in proofs before these concepts were formulated explicitly.

¹ M. KLINE, *Mathematical Thought from Ancient to Modern Times* (Oxford, 1972), p. 1141.

² *J. reine angew. Math.* **100** (1887), 179-181. See § 6 below.

2. Sylow's Proof

It was in 1872 that L. SYLOW (1832–1918)³ published the paper which keeps his name alive.⁴ Our subject is the first theorem in it: if G is a finite group whose order $|G|$ is divisible by a prime p , then G contains a subgroup of index prime to p which has p -power order.⁵ SYLOW's own proof, not very well known nowadays, is as follows.

Let P be a p -power subgroup of maximal order. Let N be its normalizer. If p divides the order of N/P , then by CAUCHY's theorem N/P contains an element of order p , and a corresponding element of N adjoined to P gives a larger p -power subgroup. Hence $|N/P|$ must be prime to p . Similarly, any element of p -power order in N lies in P , since otherwise it together with P would give a larger p -power subgroup.

Now let P act by translation on the cosets of N in G . If gN is fixed, then $gPg^{-1} \subseteq N$, whence $gPg^{-1} = P$ since no other p -power elements lie in N . Hence by definition g is in N , and $gN = N$. Every other orbit has then a cardinality divisible by p , so $|G:N|$ is congruent to 1 modulo p . In particular it is prime to p , so $|G:P| = |G:N||N:P|$ is prime to p , Q.E.D.

Technically, this proof is interesting for the crucial role of the normalizer N (which SYLOW introduces, though he invents no name for it); this is the beginning of the study of " p -local" group structure. But historically more interesting (and making the proof much harder to read) is the fact that SYLOW does not explicitly have the concept of action on cosets. What appears in its place is a theorem of CAUCHY which is hardly remembered now: If H is any group of substitutions of n variables, then there is a function of those variables left invariant by the substitutions in H and by no other substitutions.⁶ One can see how this is used by examining a more literal version of the second half of SYLOW's proof.

³ For biographical information on SYLOW, see H.B. KRAGEMO, Nord. Math. Tids. **15** (1933), 73–99.

⁴ "Théorèmes sur les groupes de substitutions," Math. Ann. **5** (1872), 584–594.

⁵ I will preserve this notation throughout the paper and silently substitute it for the various symbols used by the different authors.

⁶ CAUCHY's proof was an explicit construction. Let $s = ax + by + cz + \dots$ be a linear function of the variables where the coefficients are unequal and have nonzero sum. Let Ω be the product of s and its images under the substitutions in H . If s' is the image of s under a substitution leaving Ω unchanged, then the equation $s' = 0$ implies $\Omega = 0$ and hence implies $s'' = 0$ for some image s'' of s under a substitution in H . As the sum of the coefficients is nonzero, this implies $s' = s''$. As all coefficients are distinct, the substitutions must be the same, and the original substitution is in H . ("Sur le nombre des valeurs égales ou inégales que peut acquérir une fonction de n variables indépendantes, quand on permute ces variables entre elles d'une manière quelconque," C.R. Acad. Sci. XXI (1845), 777 et seq. = Œuvres I, 9, no. 303, pp. 337–9). The original connection with solution of equations is clear from CAUCHY's statement of the theorem, which says only that there is a function of the variables taking each value exactly $|H|$ times. The theorem and its proof are reproduced in the treatises of JORDAN and SERRET.

"Let $x_0, x_1, x_2, \dots$ be the letters which the group G permutes among themselves... Let us consider a rational function of the x unchanged by the substitutions in N but changed by every other substitution. Let z_0 be this function, and let us represent by

$$z_0 z_1 z_2 \dots z_{h-1}$$

the h values that it assumes under the substitutions of G . Let us carry out in the z the substitutions of P ; by this z_0 is unchanged, but each of the other z assumes a number of values which is a divisor of the order of P , that is, a power of p . This power cannot reduce to unity; if for instance z_1 were unchanged by P and z_1 is derived from z_0 by the substitution ψ_1 , z_0 would have to be unchanged by the group conjugate to P under ψ_1^{-1} ; but as the only group of order p^n contained in N is P , ψ_1^{-1} would have to be permutable with P , which is not the case. Therefore if one partitions the functions $z_1 \dots z_{h-1}$ into systems, bringing together those that are permuted among each other by the substitutions of P , the number of functions contained in each system will be a power of p . Consequently the number h is of the form $np + 1$."

SYLOW of course also has no explicit concept of quotient group. In the first part of the proof he takes a function y_1 invariant only under the substitutions in P , lets $y_1 \dots y_v$ be the values it assumes under the substitutions in N , and shows that performing these substitutions on the y gives a group N' of substitutions which is a homomorphic image of N with $|N'| = v = |N:P|$.

Needless to say, "group" for SYLOW meant an explicit group of substitutions, though as we saw one can present his proof for abstract groups merely by using coset actions in place of actions on certain functions. But there is a further technical point not yet brought out. SYLOW's proof uses the weaker result of CAUCHY that G contains an element of order p . This result is itself nontrivial, and we must now look back at it.

3. Cauchy's Theorem

Someone giving SYLOW's proof today would probably establish CAUCHY's theorem by induction, using the partition into conjugacy classes and reducing ultimately to Abelian groups.⁷ But this argument was not known before FROBENIUS (see § 6). CAUCHY's original proof (1845) is explicitly tied to substitution groups, and his nine-page argument involves two lemmas of substance in themselves.⁸ As late as 1878 NETTO could begin a paper with the remark that the proof of CAUCHY's theorem was as recondite as that of LAGRANGE's theorem was simple.⁹ Formally it is a part of SYLOW's proof, and

⁷ After writing this, I found that such a approach is indeed adopted in J.J. ROTMAN, *The Theory of Groups* (Boston, 1965).

⁸ "Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières et des systèmes de substitutions conjuguées," *C.R. Acad. Sci.* XXI (1845), 835 *et seq.* = *Œuvres* I, 9, no. 304, pp. 349–358.

⁹ See § 5.

its method of argument also became important later, so it must be sketched here.

The first lemma is the explicit construction of a "SYLOW subgroup" in the full symmetric group. CAUCHY's procedure for this is the one still familiar. That is, he separates the elements into p -tuples (discarding any left over) and takes a cyclic permutation of each p -tuple; then he separates the p -tuples into sets of p and permutes these in p -cycles, and so on. An explicit computation shows that the highest power of p dividing $n!$ is exactly the order of this group.¹⁰

The second lemma in CAUCHY's proof runs as follows. Take two groups G and M inside the symmetric group, and list off the cosets aM of M . Assume now that no nontrivial element of G is conjugate to any element of M . Then for any fixed v one can show that the elements $\{gv|g \in G\}$ lie in different cosets of M . Furthermore, if w is not in those cosets, the elements gw lie in cosets distinct not only from each other but also from those of the gv . Continuing this process, we eventually exhaust all cosets of M and have them gathered into $|G|$ -tuples. Thus the index of M is a multiple of $|G|$.

Finally now suppose $|G|$ is divisible by p , and take M to be the previously constructed p -group. The index of M is prime to p and thus not divisible by $|G|$. Hence the assumption in the second lemma cannot hold. That is, G must contain a nontrivial conjugate of an element in M . Such elements are of p -power order, and hence G contains an element of order p .

One can see why the theorem was thought to be difficult, and CAUCHY himself soon took the first step toward a better understanding of it. In a later paper in the same series¹¹ he extended the lemma to show that if I is the collection of substitutions conjugating a nontrivial element of G into M , then $n! - |I|$ is a multiple of $|G| \cdot |M|$. To do this he tabulated the products $\{gvm|g \in G, m \in M\}$, showing that for v not in I these are all distinct and the substitutions outside I are partitioned into such sets. This is the first appearance of double cosets. But CAUCHY had no occasion to examine the cases where the products are not all distinct, and the impulse for that came from an entirely different area of mathematics.

4. The Cauchy-Frobenius Proof

Let G be a subgroup of the symmetric group S_n . Take the subgroup M of S_n constructed by CAUCHY, and let $S_n = \cup Gs_i M$ be the double coset decomposition. Each $|Gs_i M|$ is a multiple of $|M|$, and in fact $|Gs_i M| = |M| \cdot |G|/|P_i|$ where $P_i = G \cap s_i^{-1} M s_i$. Then $|S_n|/|M| = \sum |G|/|P_i|$ is prime to p by the con-

¹⁰ The original paper has a minor slip: CAUCHY was overhasty in treating the wreath product, and wrote that all elements in the group had order p . The error is put right in the version published in the *Exercices* = *Œuvres* II, 13, pp. 171-282 (see pp. 221-235).

¹¹ "Note sur un théorème fondamental relatif à deux systèmes de substitutions conjuguées," C.R. Acad. Sci. XXII (1846), 630 *et seq.* = *Œuvres* I, 10, no. 327, pp. 65-68.

struction of M , so some term is prime to p . But that means the p -group P_i has index in G prime to p , and SYLOW's theorem is proved.¹²

This proof is a natural extension of CAUCHY's argument, and when we recall that SYLOW's own proof needed CAUCHY's theorem, we see that this approach is definitely shorter overall. By 1909 G.A. MILLER could comment in passing that "Cauchy used a method which required only slight changes to yield an easy proof."¹³ But in fact the crucial concept of double coset arose rather from deep work in number theory.

In 1880 KRONECKER published an announcement of a major theorem relating the factorization of an integer polynomial to the number of roots it has modulo all primes.¹⁴ He also briefly stated a related result: Let F be an irreducible integer polynomial of prime degree p with solvable splitting field of degree pd . If D_k is the density of the primes q for which F has k roots modulo q , then $D_1 = 1 - (1/d)$ and $D_2 = \dots = D_{p-1} = 0$ and $D_p = 1/pd$. These relations caught the attention of FROBENIUS. They are closely connected with double cosets inside the GALOIS group of the splitting field,¹⁵ and FROBENIUS says explicitly that it was this study that led him to double cosets.

DEDEKIND independently came across double cosets in his study of the same problem. He did not publish his work until 1894,¹⁶ and FROBENIUS waited until after that to publish the number-theoretic part of his results.¹⁷ But in the mean time he wrote up the other part as a paper devoted specifically to double cosets and their applications in group theory.¹⁸ The paper presumes an abstract notion of finite group, begins its exposition with the definition of double cosets as classes for a certain "congruence" relation, derives various counting relations

¹² One could replace S_n by any group for which SYLOW's theorem is known. Some modern authors using this argument embed G in $n \times n$ invertible matrices over the field with p elements, where simple counting shows the strict upper triangular group is a SYLOW subgroup.

¹³ "Extensions of two theorems due to Cauchy," Bull. Amer. Math. Soc. **16** (1909), 510–513 = Works III, 138–140. In his later note "History of the theory of groups to 1900" (Works I, 427–467), his memory actually misled him into saying that "Sylow recognized that the method employed by A.C. Cauchy to prove the given result could readily be extended so as to prove the general theorem." (p. 449)

¹⁴ "Über die Irreducibilität von Gleichungen," Berlin Monatsberichte 1880, 155–162 = Werke II, 85–93. "Let $F(x)$ be an integer polynomial, and for every prime p let v_p be the number of (equal or unequal) roots of the congruence $F(x) \equiv 0 \pmod{p}$. Then the limiting value of $\sum v_p p^{-1-\omega}$ for infinitely small positive ω is equal to $\log(1/\omega)$ multiplied by the number of irreducible factors of $F(x)$."

¹⁵ The two subgroups involved are the decomposition group for a prime ideal over q and the subgroup fixing a root of F .

¹⁶ "Zur Theorie der Ideale," Göttingen Nachrichten (Math.-phys. Klasse) 1894, 272–277 = Werke II, 43–48.

¹⁷ "Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und der Substitutionen seiner Gruppe," Berlin Sitzungsberichte 1896, 689–703 = Abhandlungen II, 719–733. This is the paper defining the FROBENIUS automorphism and proving the FROBENIUS density theorem.

¹⁸ "Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul," J. reine angew. Math. **101** (1887), 273–299 = Abhandlungen II, 304–330.

involving them, and as first application proves the SYLOW theorems. In style and approach FROBENIUS is completely modern, and the presentation at the start of this section is quite faithful to his.

5. Netto's Proof

The modern style of FROBENIUS' argument is clearly brought out when we compare it with a related proof published nine years earlier by E. NETTO (1846–1919).¹⁹ Omitting the introduction, I translate it here, noting that $|G|$ is called k .

“Let φ now be a function of the n elements $x_1, \dots, x_n$ which remains unchanged for all substitutions in G and only for these; then for all possible substitutions of the quantities x the function φ will assume altogether $n!/k$ different values $\varphi_1, \varphi_{s_1}, \varphi_{s_2}, \dots$, where say φ_{s_1} arises from φ by application of the substitution s_1 . — If now p^f is the highest power of p that divides $n!$, one can construct a group H of order p^f on the n quantities x . Let ψ be a function unchanged only for the group H ; among the possible choices of φ and ψ let φ_1 and ψ_1 be chosen so that the order p^α of the group Γ_1 that leaves both these functions unchanged is as large as possible.

“If further a and b are indeterminate constants, $a\varphi_1 + b\psi_1$ will assume $n!/p^\alpha$ different values for the substitutions of the x among themselves, since it remains unchanged only for the p^α substitutions of Γ_1 which belong simultaneously to the groups G_1 and H_1 . If now among the $(n!/k)(n!/p^f)$ possible values $a\varphi_\lambda + b\psi_\mu$ ($\lambda = 1 \dots n!/k$; $\mu = 1 \dots n!/p^f$) there are some different from those obtained from $a\varphi_1 + b\psi_1$, e.g. $a\varphi_{s_1} + b\psi_{s_2}$, then $a\varphi_{s_1 s_1^{-1}} + b\psi_{s_2 s_1^{-1}} = a\varphi_1 + b\psi_t$, also does not occur among them. This function $a\varphi_1 + b\psi_t$ yields $n!/p^\beta$ values for the substitutions of the x , where p^β is the order of the group that leaves φ_1 and ψ_t both unchanged. By assumption $\beta \leq \alpha$. If there are still more $a\varphi_\lambda + b\psi_\mu$ besides these $(n!/p^\alpha) + (n!/p^\beta)$ expressions, one can continue in the same way; and since obviously none of the expressions can be repeated, one gets

$$\frac{n!}{k} \cdot \frac{n!}{p^f} = \frac{n!}{p^\alpha} + \frac{n!}{p^\beta} + \dots = \frac{n!}{p^\alpha} \cdot s$$

where s is an integer, since necessarily $p^\alpha \geq p^\beta, p^\gamma, \dots$. But this equation yields

$$p^\alpha \cdot n! = p^f \cdot k \cdot s.$$

The highest power of p that occurs on the left side is $p^{\alpha+f}$, and hence k can be divisible at most by p^α . On the other hand, k must be divisible at least by p^α by Lagrange's theorem; it follows from this that $k = p^\alpha \cdot \kappa$ where κ is relatively prime to p .”

¹⁹ “Neuer Beweis eines Fundamentaltheorems aus der Theorie der Substitutionen-lehre,” *Math. Ann.* 13 (1878), 249–250. The only convenient source of biographical information on NETTO is the article by BIERMANN in the *Dict. Sci. Biog.*

FROBENIUS rather modestly wrote that “apart from the simplification gained by the abstract form of expression, the [double-coset] proof is identical with that” given by NETTO. The counting in NETTO's argument is a bit more complicated, but certainly the proofs are closely related. Like SYLOW, NETTO uses functions with prescribed stabilizer instead of cosets, and the “indeterminate constants” serve to keep the two actions apart, so that in modern terms the proof uses the action of S_n on $S_n/G \times S_n/H$. Each orbit contains an element of the form (eG, tH) , and its stabilizer is $G \cap t^{-1}Ht$, the same as for the $(G \times H)$ -action with double cosets as orbits.

In speaking of the abstract form of his proof, FROBENIUS here does not mean to contrast abstract groups with substitution groups. The double coset proof takes place in S_n and would have been perfectly comprehensible to CAUCHY. He means rather that his argument (like CAUCHY's) *deals with* substitution groups rather than functions on which they act; it is “group-theoretic”. H. WUSSING has emphasized the importance of such group-theoretic thinking in the growth of abstract group theory,²⁰ and this is a good example, because NETTO obviously still thought much more in terms of polynomials.

This style of thought is evident in NETTO's first book on substitutions, *The Theory of Substitutions and its Application to Algebra*.²¹ The title itself shows that “algebra” still meant equations and polynomials, and one part of the preface deserves careful attention. NETTO grants that if one can “free the foundations and development from all assumptions not absolutely necessary, the generality of the objects with which it works makes possible its application in many different areas.” But by treating only “application to a definitely prescribed and strictly limited area” one gets “freedom from everything superfluous and heightened usefulness, in place of a generality which is absent but not missed.” These ideas are so familiar that it is a shock to read on and find that NETTO does not at all intend to contrast abstract groups with groups of substitutions.²² It is rather substitution groups themselves that NETTO considers abstract in comparison with the original idea of substitutions as explicit changes of variable.²³ He indeed goes on to say that using polynomials from the beginning gives “a comprehensible foundation for the ‘operating with operators’ which is substitution theory.”

One of the traditional advantages of abstraction is that it reveals common features. NETTO saw no relation between his argument and CAUCHY's. His opening comment on CAUCHY's theorem was already cited in § 3. He goes on to quote the S_n construction lemma (which is used in his proof), but he describes the other lemma only vaguely as “investigating the relationship between two groups that contain no conjugate substitutions.” His argument in fact virtually

²⁰ H. WUSSING, *Die Genesis des abstrakten Gruppenbegriffs* (Berlin, 1969).

²¹ *Substitutionstheorie und ihre Anwendung auf die Algebra* (Leipzig, 1882).

²² This point is missed by WUSSING (*op. cit.* pp. 176–178). It is true that NETTO gives KRONECKER's abstract treatment of finite Abelian groups, but he does little more than reproduce it; he does not call such systems of objects “groups”, nor does he deal with similarly abstract systems in the rest of his book.

²³ We still preserve the old terminology in calculus courses when we speak of “integration by substitution”.

contains a proof of that lemma²⁴, but the relationship was not yet within his grasp.²⁵ FROBENIUS, by contrast, not only recognized that his proof was extremely close to NETTO's but also carefully recorded which cases of the double-coset counting had been found by CAUCHY.

6. The Frobenius Class-Equation Proof

About the same time as the double-coset work, FROBENIUS wrote a paper containing an essentially different proof of SYLOW's theorem.²⁶ Unlike all the proofs discussed so far, it does not require previous construction of the SYLOW subgroup of S_n . One can hear a new tone in the way FROBENIUS describes this:

"Since the symmetric group, which is introduced into all these proofs, is totally alien to the content of Sylow's theorem, I have tried to find a new derivation of it in which the Cauchy lemma is not used."

Obviously the man who wrote this did not think that groups were by definition groups of substitutions inside S_n . This is made explicit a few lines later:

"The elements of every finite group can be interpreted as substitutions (this Journal 86, p. 230).^[27] Nevertheless, considering the theorem to be proved, I specifically do not want to assume this interpretation in what follows."

FROBENIUS thereupon gives an abstract definition of a finite group.²⁸ To understand the role of abstraction here, we must look at the actual proof.

The first step is to prove CAUCHY's theorem for a finite Abelian group Z . If p divides $|Z|$, list the elements g_i of Z , let n_i be the order of g_i , and consider $\prod g_i^{r_i}$ for $0 \leq r_i < n_i$. This represents each element in Z the same number of times, so $|Z|$ divides $\prod (n_i)$. Hence p divides some n_j , and $g_j^{n_j/p}$ has order p , as desired.²⁹

²⁴ Suppose G and H are any two subgroups of S_n with $G \cap t^{-1}Ht$ trivial for all t . Then in NETTO's construction each orbit of functions has $n!$ elements, so $n!$ divides $|S_n : G| \cdot |S_n : H|$. Hence $|G| \cdot |H|$ divides $n!$.

²⁵ NETTO's later book *Gruppen- und Substitutionentheorie* (Leipzig, 1908), which is strongly influenced by FROBENIUS, treats abstract groups and is group-theoretic throughout.

²⁶ "Neuer Beweis des Sylowschen Satzes," *J. reine angew. Math.* **100** (1887), 179–181 = *Abhandlungen II*, 301–303.

²⁷ FROBENIUS & STICKELBERGER, "Über Gruppen von vertauschbaren Elementen," *J. reine angew. Math.* **86** (1879), 217–262 = FROBENIUS, *Abhandlungen I*, 545–590.

²⁸ As he says, the definition is modelled on that of KRONECKER for finite Abelian groups.

²⁹ FROBENIUS mentions here a place in his paper with STICKELBERGER (above, note 27) where this argument is used in a more general context. The result also follows immediately from the structure theory of finite Abelian groups, which itself is presented in FROBENIUS & STICKELBERGER. But obviously FROBENIUS wanted to give a simple argument to make his proof of SYLOW's theorem self-contained.

Now the proof of SYLOW's theorem goes by induction on $|G|$. Let Z be the center of G , and assume first that p divides $|Z|$. Let $\langle g \rangle$ be a subgroup of Z of order p , and form $G/\langle g \rangle$. By induction this has a SYLOW subgroup, and its inverse image is a SYLOW subgroup of G . Now assume that p does not divide $|Z|$, and partition the group into its conjugacy classes. The number of classes with just one element is $|Z|$, prime to p . Since $|G|$ is divisible by p , some larger class also has order prime to p . The centralizer of an element in it then is a smaller group involving the same power of p , and by induction it contains a SYLOW subgroup.³⁰

There is no need to dilate on the attractiveness of this argument, which quickly became standard;³¹ it is quite short and avoids the preliminary construction. WUSSING is quite wrong in attributing publication of the paper merely to a desire for abstract presentation.³² FROBENIUS indeed stresses abstract groups, but this is not just a personal preference: they are needed to make the proof work. At one step, as we saw, he identifies elements in G which differ by a power of a central element g . He explicitly points out that after this identification the postulates still hold, and *therefore he can apply the induction hypothesis* to this quotient. In this paper abstraction not only makes the proof clearer, it actually makes it work.

Theoretically it would be possible to construct a substitution group playing the role of the quotient. SYLOW we saw did something of this sort. But psychologically this simple argument seems much more likely to occur to someone who thinks of groups with abstract elements, and in fact we have good confirmation of this. W. BURNSIDE later discovered the same proof independently,³³ and his introductory remarks emphasize abstract groups even more than FROBENIUS did:

"Now, since every group of finite order can be represented as a permutation-group, there can be no objection to the validity of the proofs above referred to [i.e., SYLOW and NETTO]; but from the point of view of right method they leave something to be desired. A theorem so fundamental in the theory, which also from its statement is independent of the infinite variety

³⁰ FROBENIUS notes that this use of conjugacy classes was suggested by SYLOW's proof that a p -group has nontrivial center.

³¹ It is given, for instance, in NETTO's book (note 25 above), in H. WEBER, *Lehrbuch der Algebra*, vol. 2 (Braunschweig, 1889), and in R. FRICKE, *Lehrbuch der Algebra*, vol. I (Braunschweig, 1924).

³² *Op. cit.* pp. 182–3: "Citing the theorem that every finite group can be represented as a permutation group, he admits that the problem is essentially solved and the theorem also holds for groups in general. But Frobenius wants to obtain the theorem in question abstractly." The misinterpretation mentioned at the start of the paper is of course much worse.

³³ "Notes on the theory of groups of finite order," *Proc. London Math. Soc.* **25** (1894), 9–18. In his argument he forgets to mention the Abelian case with which the induction must start, but a full version is given in his book, *Theory of Groups of Finite Order* (Cambridge, 1897), pp. 91–92. By then he had also come across the article by FROBENIUS.

of forms in which a group can be presented, should not depend for its proof on the properties of a very special mode of representation."

7. Dedekind's Proof of Cauchy's Theorem

We should pause here to observe a similar use of abstract groups much earlier, though it did not reach as far as SYLOW's theorem. In the period 1855–1858 DEDEKIND did a little work on group theory.³⁴ His results were not published at the time, had no contemporary influence, and are not discussed by WUSSING. But they included a rediscovery of CAUCHY's theorem³⁵ with the following proof.

Assume inductively that the theorem is known for all groups of smaller order than G . If any proper subgroup of G has order divisible by p , then by induction it contains an element of order p . Assume therefore that this does not happen. If now K is any nontrivial normal subgroup, then the group of classes G/K has order divisible by p and hence contains a class of order p . An element g in G representing that class must have order divisible by p , so some power of g has order p . We may thus assume that G has no nontrivial normal subgroups.

Let K be a cyclic subgroup. Its normalizer now must be a proper subgroup, and so has order prime to p . Hence the number of conjugates of K is divisible by p . Now each cyclic subgroup of order d contains $\varphi(d)$ generators (elements of order d), so if there are $\psi(d)$ such subgroups in G we have

$$|G| = \sum \psi(d) \varphi(d) = 1 + \sum_{d > 1} \psi(d) \varphi(d).$$

But since $|G|$ and all $\psi(d)$ are divisible by p , this is impossible.

By a similar counting argument DEDEKIND also showed that a p -group has a normal subgroup of order p . These strange but ingenious proofs, which of course were never polished for publication, are obviously modelled on GAUSS' counting argument for the existence of primitive roots.³⁶ For our purposes the significant feature is that passage to quotients is used freely in the induction.³⁷ It is almost unnecessary to add that DEDEKIND's groups consist not of substitutions but of unspecified "objects".

³⁴ DEDEKIND, Werke II, 419. The dates are given in a letter of 1895 to FROBENIUS.

³⁵ Werke III, 442–443. Obviously DEDEKIND was not previously acquainted with the result, since the sheet is headed "Theorem(?)", followed by "Attempted Proof."

³⁶ Disquisitiones Arithmeticae § 52–55.

³⁷ This is probably also influenced by study of GAUSS. Like KRONECKER and FROBENIUS, DEDEKIND had number-theoretic training and interests, and knew GAUSS' use of congruences and classes of quadratic forms. We may recall that FROBENIUS used GAUSS' word "congruence" for the double-coset relation.

8. Capelli's Forgotten Proof

The Italian mathematician ALFREDO CAPELLI (1855–1910)³⁸ published his thesis³⁹ in 1878, six years after SYLOW's paper appeared. His only sources appear to be SERRET and JORDAN and a course given from JORDAN's book by BATTAGLINI. There are several different sections. In one, for instance, he extends the concept of homomorphism and analyzes those many-to-many correspondences between two groups that respect multiplication. In another he essentially constructs quotients G/N using the same function-permutation approach as SYLOW did, and he shows that any transitive action can be matched up with an action on functions constructed by the CAUCHY method. Section IV is headed "A new theorem relative to an arbitrary group of substitutions. — Cauchy's theorem follows as a corollary." Here CAPELLI rediscovered SYLOW's theorem with a quite different proof.

The first and crucial step in the proof is to take the transitive action of G on $|G|$ variables $x_1, \dots, x_{pv}$ and form the function

$$f = x_1 x_2 \dots x_p + x_{p+1} \dots x_{2p} + \dots + x_{1+(p-1)p} \dots x_{pv},$$

together with all the different f which arise in this way from all possible renumberings of the variables.⁴⁰ The number of different functions is $|G|!/(p!)^{|G|/p}(|G|/p)!$, which is prime to p (the denominator includes all those factors in the numerator divisible by p), and G permutes the functions *via* its action on the x_i .

Suppose first some f is left fixed by G . Then the variables $y_1 = x_1 \dots x_p, \dots, y_v = x_{1+(p-1)p} \dots x_{pv}$ are permuted transitively among themselves by G ; we repeat the process with these variables and continue inductively. "In the most exceptional case," we can continue thus dividing the number of variables by p until the number is prime to p . Then the elements in G fixing some one of these variables will form our desired subgroup. "But in general" we will have to stop before this. The functions constructed at that stage will fall into nontrivial orbits, at least one of which must have order prime to p . Then the stabilizer of a function in such an orbit is a proper subgroup involving the same power of p , and the theorem follows by induction.

I have slightly simplified the original (ten-page) presentation by using non-faithful group actions where CAPELLI each time introduces the substitution group to which G maps, but the essence of the proof is here. The end of the argument is similar to the later FROBENIUS induction, but obviously the basic idea in the proof is to find *a priori* a reasonable action of G on a set of cardinality prime to p . And this is a very good idea indeed.

³⁸ There is an obituary of CAPELLI by G. TORELLI, *Giornale di Mat.* (3) **1** (1910), 5–15.

³⁹ "Sopra l'isomorfismo dei gruppi di sostituzioni," *Giornale di Mat.* **16** (1878), 32–87.

⁴⁰ Set-theoretically, one would say that he is considering all partitions of G into p -element subsets.

The *Fortschritte* review (by NETTO) did not discuss this method of proof, and almost the only later reference to it is by G.A. MILLER. In his 1915 paper "A new proof of Sylow's theorem"⁴¹ he remarks that "among the later proofs those by A. Capelli, E. Netto and G. Frobenius are most noteworthy from the standpoint of originality and simplicity." The comment is appropriate enough, because MILLER's proof is a somewhat more polished version of the same basic idea. The set he uses is all the permutations of the elements which involve only p -cycles and move p^b elements, where $p^b \leq |G| < p^{b+1}$. This proof was adopted in a couple of American texts,⁴² but did not become generally known. It was only in 1959 that WIELANDT independently found his brilliantly polished proof⁴³ using the action of G on the collection of subsets that have order equal to the highest power of p dividing $|G|$.

Though CAPELLI's basic idea is good, there is one curiosity in the presentation that illustrates how unfamiliar group actions still were. As was mentioned earlier, one part of the thesis is devoted to showing how every transitive group action can be matched up with one constructed from a subgroup by the CAUCHY method. Section VI, using a counting argument similar to the proof in Section IV, proves that a p -group has a chain of subgroups $P \supset P_1 \supset \dots \supset P_n = \{e\}$ with P_i normal in P_{i-1} of index p . And CAPELLI explicitly remarks that having a fixed function f in his original construction means that the group action on the x_i is imprimitive. But he did not think of combining these facts to see that the chain of subgroups corresponds to a fixed function at each stage in his proof of SYLOW's theorem. What he calls the "general" case is impossible, and only his "most exceptional" case actually occurs.

In CAPELLI's paper, the functions corresponding to P_i in the CAUCHY lemma need not be the same as the y_i he meets in the SYLOW theorem construction. The relation between them does not strike the eye as much as it would if both were expressed intrinsically in terms of cosets. Thus we see here once again what we have already observed: greater understanding of SYLOW's theorem went hand in hand with the more intrinsic, abstract grasp of groups in general.

This work was supported in part by the U.S. National Science Foundation.

⁴¹ Ann. of Math. **16** (1915), 169–171 = Works III, 435–437.

⁴² MILLER, BLICHFELDT & DICKSON, *Theory and Applications of Finite Groups* (New York, 1916 and 1938); and R.D. CARMICHAEL, *Introduction to the Theory of Groups of Finite Order* (Boston, 1937).

⁴³ "Ein Beweis für die Existenz von Sylowgruppen," Arch. Math. **10** (1959), 401–402.

Department of Mathematics
The Pennsylvania State University
University Park

(Received September 10, 1979)



WILLIAM CHARLES WATERHOUSE
(31 December 1941 until 26 June 2016)
(see https://en.wikipedia.org/wiki/William_C._Waterhouse
and <https://camws.org/node/1051>
and [https://www.legacy.com/us/obituaries/centredaily/
name/william-waterhouse-obituary?id=16790379](https://www.legacy.com/us/obituaries/centredaily/name/william-waterhouse-obituary?id=16790379))

Die Entdeckung der Sylow-Sätze

Die Entdeckung der Sylow-Sätze - ScienceDirect



Historia Mathematica
Volume 15, Issue 1, February 1988, Pages 40-52

Die Entdeckung der Sylow-Sätze

Herrn H. Wussing Zum 60. Geburtstag, am 15. Oktober 1987 Gewidmet

Winfried Scharlau

Show more

Outline | Share | Cite

[https://doi.org/10.1016/0315-0860\(88\)90048-1](https://doi.org/10.1016/0315-0860(88)90048-1)

Get rights and content

Under an Elsevier user license

Open archive

Abstract

The paper describes Sylow's discovery of the theorems named after him. He was led to this discovery by his study of Galois' work, in particular of Galois' criterion for the solvability of equations of prime degree. It is explained how Sylow used methods from Galois theory in his proofs. The paper also discusses relevant correspondence between Sylow, Jordan, and Petersen.

Zusammenfassung

<https://www.sciencedirect.com/science/article/pii/0315086088900481?via%3Dihub>

1/10

Die Entdeckung der Sylow-Sätze - ScienceDirect

Diese Arbeit behandelt Sylows Entdeckung der Sätze, die nach ihm benannt sind. Er gelangte zu ihnen durch seine Beschäftigung mit Galois' Arbeiten über die Auflösbarkeit von Gleichungen vom Primzahlgrad. Es wird beschrieben, wie Sylow im Beweis seiner Sätze Methoden aus der Galois-Theorie benutzt. Es wird weiterhin auf die diesbezügliche Korrespondenz zwischen Sylow, Jordan und Petersen eingegangen.

Résumé

Cet article traite de la découverte par Sylow du théorème qui porte depuis son nom. Il a trouvé ce théorème en étudiant les travaux de Galois sur la résolubilité des équations dont le degré est un nombre premier. On y indique comment Sylow utilise dans sa démonstration les méthodes de la théorie de Galois. De plus, on étudie dans cet article la correspondance à ce propos entre Sylow, Jordan et Petersen.

< Previous

Next >

MSC

01 A55

Schlüsselwörter

Ludvig Sylow; Sylow theorems; Galois theory; group theory

<https://www.sciencedirect.com/science/article/pii/0315086088900481?via%3Dihub>

2/10

développement naturel de vos beaux théorèmes, dont j'ai été le premier, si je ne me trompe à prédire l'importance future. Ils m'ont inspiré à votre égard une amitié intellectuelle qui m'a fait me réjouir à la vue de votre écriture. [7]

Die Geschichte einer mathematischen Theorie ist vor allem die Geschichte der zentralen Sätze und tiefen Ergebnisse dieser Theorie. Entsprechend verdienen die Sylow-Sätze besondere Aufmerksamkeit im Rahmen einer allgemeineren Geschichte der Gruppentheorie. Es ist das Verdienst von Waterhouse [1980], erstmals eine solche Untersuchung vorgelegt zu haben, der von der mathematischen Substanz her nur wenig hinzuzufügen ist und die vor allem eine umfassende Darstellung verschiedener—heute z. T. fast vergessener—Beweisvarianten enthält. Die vorliegende Note—die als Ergänzung zu der Arbeit von Waterhouse angesehen werden kann—beschäftigt sich mehr mit der historischen Seite der Entdeckung der Sylow-Sätze. Während Waterhouse die Zeit nach der ersten Veröffentlichung der Sylow-Sätze im Jahre 1872 behandelt, geht es uns vor allem um die Zeit vor 1872. Es wird der Frage nachgegangen, wie Sylow zu der Problemstellung seiner Sätze gekommen ist, welche Hilfsmittel und Methoden es zur Verfügung hatte, ob und gegebenenfalls welche Anregungen er von Zeitgenossen erhielt, wie er selbst seine Sätze einschätzte, welche Hoffnungen und Erwartungen er mit ihnen verband, wie sie sich vielleicht in ein umfassenderes "Forschungsprogramm" einordnen lassen.

Diese Fragen können nicht alle ganz eindeutig und vollständig beantwortet werden, aber es läßt sich doch folgendes feststellen:

1. Sylow ist ganz offensichtlich von der Theorie der algebraischen Gleichungen und der Galois-Theorie zur Gruppentheorie gekommen und nicht—was auch denkbar wäre—von einer abstrakteren Theorie der Permutations-Gruppen im Sinne Cauchys (1789–1857). Darüber hinaus war für ihn Gruppentheorie noch praktisch ein Teil der Galois-Theorie, gewissermaßen angewandte Galois-Theorie, und er verwandte galois-theoretische Konstruktionen und Schlüsse an Stellen, die später rein gruppentheoretisch behandelt wurden. Seine ersten beiden Hauptsätze (Existenz, Anzahl und Konjugiertheit der p -Sylow-Gruppen) hat er in unmittelbarem Anschluß an ein Ergebnis von Galois (1811–1832) zunächst in einem sehr speziellen Fall (nämlich p -Sylow-Gruppen einer Untergruppe der S_n) gefunden und anschließend verallgemeinert. Bei dieser Verallgemeinerung könnte

2 von 13

<https://www.sciencedirect.com/science/article/pii/S0315086088900481?via%3Dihub>

3/10

 [View PDF](#)

[Recommended articles](#)

Referenzen

[Bourbaki and Deutsche Übersetzung, 1971](#) [Literatur](#)

N Bourbaki

Éléments d'histoire des mathématiques

Hermann, Paris (1965)

[Google Scholar](#)

Deutsche Übersetzung

Elemente der Mathematikgeschichte (1971)

Göttingen

[Cauchy et al., 1896](#) [A.L Cauchy](#)

Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières et des systèmes de substitution conjuguées

Comptes Rendus hebdomadaires des Séances de l'Académie des Sciences, 21 (1845), pp. 835-852

[Google Scholar](#)

A.L Cauchy

Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières et des systèmes de substitutions conjuguées

Comptes Rendus hebdomadaires des Séances de l'Académie des Sciences, 21 (1845), pp. 895-902

[Google Scholar](#)

A.L Cauchy

<https://www.sciencedirect.com/science/article/pii/S0315086088900481?via%3Dihub>

4/10

Die Entdeckung der Sylow-Sätze - ScienceDirect

Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières et des systèmes de substitutions conjuguées

Comptes Rendus hebdomadaires des Séances de l'Académie des Sciences, 21 (1845), pp. 931-933

[Google Scholar](#) »

A.L. Cauchy

Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières et des systèmes de substitutions conjuguées

Comptes Rendus hebdomadaires des Séances de l'Académie des Sciences, 21 (1845), pp. 972-987

[Google Scholar](#) »

A.L. Cauchy

Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières et des systèmes de substitutions conjuguées

Comptes Rendus hebdomadaires des Séances de l'Académie des Sciences, 21 (1845), pp. 1025-1041

[Google Scholar](#) »

Zitiert wird nach

Oeuvres, vol. 9, Gauthier-Villars, Paris (1896), pp. 342-358

I^{re} Série

Cayley and Cayley, 1896 A Cayley

Desiderata and suggestions

American Journal of Mathematics, 1 (1878), pp. 50-52

[View in Scopus](#) » [Google Scholar](#) »

A Cayley

Abgedruckt in

Mathematical papers, vol. 10, The Univ. Press, Cambridge (1896), pp. 401-403

<https://www.sciencedirect.com/science/article/pii/S0315086088900481?via%3Dihub>

5/10

Die Entdeckung der Sylow-Sätze - ScienceDirect

Dedekind, 1932 R Dedekind

Aus den Gruppen-Studien (1855–1858)

R Fricke, E Noether, O Ore (Eds.), Gesammelte Mathematische Werke, vol. 3, Vieweg, Braunschweig (1932), pp. 439-446

[Google Scholar](#) »

Dedekind, 1981 R Dedekind

Eine Vorlesung über Algebra

W Scharlau (Ed.), Richard Dedekind 1831/1981, Vieweg, Braunschweig/Wiesbaden (1981)

[Google Scholar](#) »

Deutsche, 1985 J Dieudonné (Ed.), Abrégé d'histoire des mathématiques 1700–1900, Hermann, Paris (1978)

Übersetzung Deutsche

Geschichte der Mathematik 1700–1900 (1985)

Braunschweig/Wiesbaden

[Google Scholar](#) »

Galois, 1962 E Galois

R Bourgne, J.P. Azra (Eds.), Ecrits et mémoires mathématiques, Gauthier-Villars, Paris (1962)

[Google Scholar](#) »

Huppert, 1967 B Huppert

Endliche Gruppen, vol. 1, Springer, Berlin/Heidelberg/New York (1967)

Jordan and Jordan, 1961 C Jordan

Sur la limite de transitivité des groupes non alternés

Bulletin de la Société mathématique de France, 1 (1873), pp. 40-71

[Google Scholar](#) »

C Jordan

<https://www.sciencedirect.com/science/article/pii/S0315086088900481?via%3Dihub>

6/10

Die Entdeckung der Sylow-Sätze - ScienceDirect

Wieder abgedruckt in

J Dieudonné (Ed.), Oeuvres, vol. 1, Gauthier-Villars, Paris (1961), pp. 365-396

Jordan, 1961 C Jordan

J Dieudonné (Ed.), Oeuvres, vol. 1, Gauthier-Villars, Paris (1961)

Kragemo, 1933 H.B Kragemo

Ludvig Sylow

Norsk Matematisk Tidsskrift, 15 (1933), pp. 73-99

[Google Scholar »](#)

Kronecker and Kronecker, 1929 L Kronecker

Über die algebraisch auflösbaren Gleichungen

Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin vom Jahre 1853 (1853), pp. 365-374

[Google Scholar »](#)

L Kronecker

Wieder abgedruckt in

K Hensel (Ed.), Werke, vol. 4, Teubner, Leipzig/Berlin (1929), pp. 3-11

Lagrange and Lagrange, 1869 J.L Lagrange

1770/71

Réflexions sur la résolution algébrique des équations, Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin (1770), pp. 134-215

[Google Scholar »](#)

J.L Lagrange

1770/71

Réflexions sur la résolution algébrique des équations, Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin (1771), pp. 138-253

<https://www.sciencedirect.com/science/article/pii/S0315086088900481?via%3Dihub>

7/10

Die Entdeckung der Sylow-Sätze - ScienceDirect

[Google Scholar »](#)

Zitiert wird nach

Oeuvres, vol. 3, Gauthier-Villars, Paris (1869), pp. 203-421

Petersen, 1878 J Petersen

Theorie der algebraischen Gleichungen

Høst u. Sohn, Kopenhagen (1878)

[Google Scholar »](#)

Skolem, 1922 Th Skolem

Bericht über die nachgelassenen Schriften L. Sylows

Videnskabs-selskabet i Kristiania (1922)

Matematisk-Naturvidenskapelig Klasse. Skrifter No. 18. Kristiania

[Google Scholar »](#)

Sylow, 1867 L Sylow

Om Systemer af konjugerede Substitutioner...

Videnskabs-selskabet i Kristiania Forhandling (1867), pp. 105-122

[Google Scholar »](#)

Sylow, 1872 L Sylow

Théorèmes sur les groupes de substitutions

Mathematische Annalen, 5 (1872), pp. 584-594

[View in Scopus »](#) [Google Scholar »](#)

Sylow, 1888 L Sylow

Sur les groupes transitifs dont le degré est le carré d'un nombre premier

Acta mathematica, 11 (1888), pp. 201-256

[Google Scholar »](#)

<https://www.sciencedirect.com/science/article/pii/S0315086088900481?via%3Dihub>

8/10

Die Entdeckung der Sylow-Sätze - ScienceDirect

Waterhouse, 1980 W Waterhouse

The early proofs of Sylow's theorem

Archive for History of Exact Sciences, 21 (1980), pp. 279-290

[View in Scopus »](#) [Google Scholar »](#)

Wußing and Wußing, 1984 H Wußing

Die Genesis des abstrakten Gruppenbegriffs

VEB Deutscher Verlag der Wissenschaften, Berlin (1969)

[Google Scholar »](#)

H Wußing

Amerikanische Übersetzung

The Genesis of the Abstract Group Concept, VEB Deutscher Verlag der Wissenschaften, Cambridge, MA/London (1984)

Abe Shenitzer, translator, with the editorial assistance of Hardy Grant

[Google Scholar »](#)

Cited by (3)

The mathematical life of Cauchy's group theorem

2004, Historia Mathematica

Citation Excerpt :

...That "class-equation" proof of Frobenius became standard, so much so that subsequent textbooks on group theory, since Sylow's theorems have far more mathematical consequence than Cauchy's theorem, typically relegated the latter to a footnote. Scharlau [1988, 49] warns us of the danger of an overemphasis on the mutual incomprehension between the permutation-theoretic view of groups and the abstract view; nevertheless, Wussing's picture of a reworking of permutation-theoretic results within the framework of the abstract group theory [Wussing, 1984, 243–244] goes far to answer Waterhouse's [1980, 279] question of what Frobenius was up to when in 1884 he reproved Sylow's theorem. Thomas Hawkins [1981] adds

<https://www.sciencedirect.com/science/article/pii/S0315086088900481?via%3Dihub>

9/10

Die Entdeckung der Sylow-Sätze - ScienceDirect

explanatory power when he displays Frobenius as a member of the "Berlin School" of mathematics, producing proofs in algebra without appeal to "generic" argument.17...

[Show abstract ▾](#)

The Development and Understanding of the Concept of Quotient Group

1993, Historia Mathematica

[Show abstract ▾](#)

Julius Petersen 1839–1910 a biography

1992, Discrete Mathematics

Copyright © 1988 Published by Elsevier Inc.



All content on this site: Copyright © 2026 Elsevier B.V., its licensors, and contributors. All rights are reserved, including those for text and data mining, AI training, and similar technologies. For all open access content, the relevant licensing terms apply.



<https://www.sciencedirect.com/science/article/pii/S0315086088900481?via%3Dihub>

10/10

HISTORIA MATHEMATICA

Founded by KENNETH O. MAY

International journal of history of mathematics

مجلة دولية لتاريخ العلوم الرياضية

Revue internationale d'histoire des mathématiques

Международный Журнал по истории математики

Internationale Zeitschrift für Geschichte der Mathematik

国 際 雜 誌 : 数 学 史

GIORNALE INTERNAZIONALE DI STORIA DELLA MATEMATICA

गणित के इतिहास की एक अन्तर्राष्ट्रीय पत्रिका

Revista internacional de historia de las matemáticas

国际数学史杂志

Volume 15 · 1988



ACADEMIC PRESS, INC.

Harcourt Brace Jovanovich, Publishers

San Diego New York Boston

London Sydney Tokyo Toronto

Copyright © 1988 by Academic Press, Inc.

All rights reserved

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the copyright owner.

The appearance of the code at the bottom of the first page of an article in this journal indicates the copyright owner's consent that copies of the article may be made for personal or internal use, or for the personal or internal use of specific clients. This consent is given on the condition, however, that the copier pay the stated per copy fee through the Copyright Clearance Center, Inc. (27 Congress Street, Salem, Massachusetts 01970), for copying beyond that permitted by Sections 107 or 108 of the U.S. Copyright Law. This consent does not extend to other kinds of copying, such as copying for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. Copy fees for pre-1988 articles are as shown on the article title pages; if no fee code appears on the title page, the copy fee is the same as for current articles.

0315-0860/88 \$3.00

MADE IN THE UNITED STATES OF AMERICA

Bayrische
Staatsbibliothek
München

CONTENTS OF VOLUME 15

NUMBER 1, FEBRUARY 1988

A. D. ALEKSANDROV, S. S. DEMIDOV, A. T. GRIGORYAN, G. P. MATVIEVSKAYA, S. S. SIRAZHDINOV, AND A. P. YUSHKEVICH. Boris A. Rozenfeld: On the 70th Anniversary of His Birth	1
J. DHOMBRES ET M. PENSIVY. Esprit de rigueur et présentation mathématique au XVIII ^{ème} siècle: le cas d'une démonstration d'Aepinus	9
VICTOR E. THOREN. Prosthaphaeresis Revisited	32
WINFRIED SCHARLAU. Die Entdeckung der Sylow-Sätze	40
MARGHERITA BENZI. Un "Probabilista Neoclassico": Francesco Paolo Cantelli	53
CHRISTOPH J. SCRIBA. Who Is It?	73
MEETINGS—ANNOUNCEMENT	
Summer School and Conference on Mathematical Logic	75
MEETINGS—REPORTS	
ANGELO GUERRAGGIO. Italian Mathematics between the Two World Wars (1920–1940)	76
R. C. GUPTA. National Seminar on the Scientific Heritage of India	77
FRITZ NAGEL. 1687/1987: Der Ausbau des Calculus durch Leibniz und die Brüder Bernoulli	81
MICHAEL OTTE. Symposium on "'Style' as a Category of the History and Philosophy of Science"	83
The Fourth International Symposium on the History of Arabic Science	84
NEWS AND NOTICES	
BERND BEKEMEIER. Research Group on the History of Mathematical Textbooks (GRIMM)	85
REVIEWS	
ROBIN E. RIDER. <i>The History of Mathematics from Antiquity to the Present: A Selective Bibliography</i> . Edited by Joseph W. Dauben	87
EBERHARD KNOBLOCH. <i>En lisant le mémoire de Seidel de 1847</i> . Par Pierre Dugac	88
ABSTRACTS	90
NOTES ON CONTRIBUTORS	98
PAPERS TO APPEAR IN FORTHCOMING ISSUES	100

NUMBER 2, MAY 1988

ERWIN NEUENSCHWANDER. A Brief Report on a Number of Recently Discovered Sets of Notes on Riemann's Lectures and on the Transmission of the Riemann <i>Nachlass</i>	101
HANS GEORG KNAPP. Zahl als Zeichen—Zur "Technisierung" der Arithmetik im Mittelalter	114
SHEN KANGSHENG. Mutual-Subtraction Algorithm and Its Applications in Ancient China	135
SOURCES	
Neugebauer Microform Index of the Exact Sciences	148
MEETING—ANNOUNCEMENT	
Colloque "Condorcet"	149

MEETINGS—REPORTS

2nd School of All Poland of the History of Mathematics. Mathematics of the 19th Century. May 25–29, 1987, Międzyzdroje	151
WALTER PURKERT. 28. Tagung zur Geschichte der Mathematik. Mathematisches Forschungsinstitut Oberwolfach, 27.4–2.5. 1987	152
First Seminar on the Scientific Tradition of Brescia. Francesco Lana Terzi (1631–1687): La scuola gesuitica e la scienza moderna. October 8, 1987	164
IVOR GRATTAN-GUINNESS. Mathematics, Mechanics, and Astronomy. Newton (1687). Lagrange (1788), Poincaré (1889). September 17–20, 1987	165
Franco–Italian Colloquy <i>Ars Analytica</i> . September 28–October 2, 1987	170

PROJECT

MARCO PANZA. Le débat sur les fondements du calcul différentiel en France dans la seconde moitié du XVIIIe siècle: L'hypothèse réductionniste et la naissance de l'algèbre opératoire	172
---	-----

REVIEWS

Y. TZVI LANGERMANN. Ptolemy's <i>Almagest</i> . Translated and annotated by G. T. Toomer. .	174
ALBERT C. LEWIS. <i>Alfred North Whitehead: The Man and His Work. Volume I: 1861–1910.</i> By Victor Lowe	176
MICHIO YANO. <i>Science and Technology in Medieval India—A Bibliography of Source Materials in Sanskrit, Arabic and Persian.</i> By A. Rahman	179
JEREMY GRAY. <i>Über die Entstehung von David Hilberts "Grundlagen der Geometrie".</i> By M.-M. Toepell	181
DAVID PINGREE. <i>The Śulbasūtras of Baudhāyana, Āpastamba, Kātyāyana and Mānava with Text, English Translation and Commentary.</i> By S. N. Sen and A. K. Bag.	183
IVO SCHNEIDER. <i>Statistics in Britain, 1865–1930: The Social Construction of Scientific Knowledge.</i> By Donald A. MacKenzie	185

ABSTRACTS	188
-----------------	-----

ERRATUM

Volume 14, Number 1, February 1987: Sabetai Unguru, review of <i>Coloured Quadrangles, a Guide to the Tenth Book of Euclid's "Elements,"</i> pp. 67–70	195
--	-----

NOTES ON CONTRIBUTORS	196
-----------------------------	-----

PAPERS TO APPEAR IN FORTHCOMING ISSUES	198
--	-----

ACKNOWLEDGMENT	199
----------------------	-----

NUMBER 3, AUGUST 1988

MARCIA ASCHER. Graphs in Cultures: A Study in Ethnomathematics	201
JOHN L. GREENBERG. Breaking a "Vicious Circle": Unscrambling A.-C. Clairaut's Iterative Method of 1743	228
RAFFAELLA FRANCI. Antonio de' Mazzinghi: An Algebraist of the 14th Century	240
BERND J. ARNOLD. Das Kontinuitätsprogramm zwischen Cantor und der Nonstandard-Analysis	250

NOTE

ROBERT INEICHEN. Dante-Kommentare und die Vorgeschichte der Stochastik	264
--	-----

SOURCES

IRVING H. ANELLIS. Some Unpublished Papers of Jean van Heijenoort	270
NICHOLAS A. VONNEUMAN. Biography of John von Neumann	274

MEETINGS—ANNOUNCEMENT

- C. J. SCRIBA. 18th International Congress on the History of Science..... 275

MEETINGS—REPORTS

- LI ZHAOHUA AND LIU DUN. The Second National Chinese Conference for History of Mathematics 275
- YOSHIMASA MICHIAKI. The International Symposium on the History and Education of Mathematics Using Chinese Characters (ISHM) 278
- LAWRENCE SHIRLEY. Second Pan-African Congress of Mathematicians..... 280
- JOSÉ FRANCISCO RODRIGUES. Anastácio da Cunha (1744–1787), o matemático e o poeta... 281
- Journées d'Histoire des Sciences. La Mathématisation (1780–1830). 11–12 Mars 1988..... 282
- LUIS SARAIVA. Portuguese Seminar of History of Mathematics 283
- NORBERT KNOCH. History of Algebra. Workshop, June 25–27, 1987, Essen..... 283

NEWS AND NOTICES

- Teaching and the History of Mathematics 285

REVIEWS

- JEAN DHOMBRES. *Leonhard Euler 1707–1783: Beiträge zu Leben und Werk.* 287
- IGNACIO ANGELELLI. *Life and Works of Giuseppe Peano.* Edited by Hubert Kennedy 289

- ABSTRACTS..... 291

- NOTES ON CONTRIBUTORS 295

- PAPERS TO APPEAR IN FORTHCOMING ISSUES..... 298

NUMBER 4, NOVEMBER 1988

- REINHARD SIEGMUND-SCHULTZE. Der Beweis des Weierstraßschen Approximationssatzes 1885 vor dem Hintergrund der Entwicklung der Fourieranalysis 299

- CATHERINE JAMI. Western Influence and Chinese Tradition in an Eighteenth Century Chinese Mathematical Work 311

- TONY CRILLY. The Decline of Cayley's Invariant Theory (1863–1895)..... 332

- A. I. DALE. On Bayes' Theorem and the Inverse Bernoulli Theorem 348

NOTE

- JAMES J. TATTERSALL. Who Put the "C" in A.-T. Vandermonde? 361

SOURCES

- DAVID C. ARNEY. Resources in the History of Mathematics at the United States Military Academy 368

MEETINGS—ANNOUNCEMENT

- International Symposium on Cauchy and the French Mathematical World..... 370

MEETINGS—REPORTS

- Colloque-atelier (CIRM Luminy 6–10 Juillet 1987). Physique et analyse de Newton à Gauss 371
- JIM RITTER. History of Fractions or Fractions of a History..... 372
- JEAN DHOMBRES. La France scientifique et technique: Les années 1816–1824. Journée de la société française d'histoire des sciences et des techniques, Conservatoire des arts et métiers, Paris, 7 Mai 1988 375

PROJECTS

VICTOR S. ALBIS AND LUIS C. ARBOLEDA. Newton's <i>Principia</i> in Latin America	376
DAVID C. ARNEY, ROBERT L. BALL, WARREN C. CHELLMAN, WILLIAM E. EBEL, JR., AND MARTIN L. VOZZO. History of the Department of Mathematics of the United States Military Academy	379

EDUCATION

MIRIAM P. COONEY. A Seminar on Women and Mathematics	380
--	-----

REVIEWS

FRANK J. SWETZ. <i>Native American Mathematics</i> . Edited by Michael P. Closs	384
JOAN L. RICHARDS. <i>Mathematical Perspectives: Essays on Mathematics and Its Historical Development</i> . Edited by Joseph W. Dauben	386
L. PEARCE WILLIAMS. <i>Intellectual Master of Nature: Theoretical Physics from Ohm to Einstein</i> . Vol. 1, <i>The Torch of Mathematics 1800–1870</i> ; Vol. 2, <i>The Now Mighty Theoretical Physics 1870–1925</i> . By Christa Jungnickel and Russell McCormmach	389
RONALD CALINGER. <i>Philosophie als Analysis: Studien zur Entwicklung philosophischer Analysiskonzeptionen unter den Einfluss mathematischer Methoden-Modelle im 17. und frühen 18. Jahrhundert</i> . By Hans-Jürgen Engfer	392

ERRATUM

Volume 14, Number 2, May 1987: Lorraine Daston, review of <i>Siméon-Denis Poisson et la science de son temps</i> , pp. 198–200	396
--	-----

ABSTRACTS	397
-----------------	-----

NOTES ON CONTRIBUTORS	402
-----------------------------	-----

PAPERS TO APPEAR IN FORTHCOMING ISSUES	405
--	-----

INDEX OF AUTHORS OF ARTICLES AND REVIEWS IN VOLUME 15	406
---	-----

INDEX OF AUTHORS OF PUBLICATIONS REVIEWED AND ABSTRACTED IN VOLUME 15	407
---	-----

HISTORIA MATHEMATICA

Vol. 15, No. 1, pp. 1–100/February 1988

Abstracts 15.1.1–15.1.77

Founded by KENNETH O. MAY

International journal of history of mathematics

مجلة دولية لتاريخ العلوم الرياضية

Revue internationale d'histoire des mathématiques

Международный Журнал по истории математики

Internationale Zeitschrift für Geschichte der Mathematik

国际雜誌：数学史

GIORNALE INTERNAZIONALE DI STORIA DELLA MATEMATICA

गणित के इतिहास की एक अन्तर्राष्ट्रीय पत्रिका

Revista internacional de historia de las matemáticas

国际数学史杂志



ACADEMIC PRESS, INC.

Harcourt Brace Jovanovich, Publishers

San Diego New York Boston

London Sydney Tokyo Toronto

HISTORIA MATHEMATICA

A publication of the International Commission on the History of Mathematics of the Division of the History of Science of the International Union of the History and Philosophy of Science.

Editor: Eberhard Knobloch, Technische Universität Berlin

Managing Editor: Helena Pycior, University of Wisconsin, Milwaukee

Book Review Editor: Judy V. Grabiner, California State University, Dominguez Hills

For Russian-language publications: Esther R. Phillips, Herbert H. Lehman College,
The City University of New York

Abstracts Editor: Albert C. Lewis, McMaster University, Ontario, Canada

Associate Editors:

John L. Berggren, Department of Mathematics, Simon Fraser University, Burnaby, B.C. V5A 1S6, Canada

H. J. M. Bos, Mathematisch Instituut, Rijksuniversiteit Utrecht, Budapestlaan 6, Utrecht, The Netherlands

I. Bernard Cohen, Department of the History of Science, Harvard University, Science Center 235, Cambridge, Massachusetts 02138

J. G. Dhombres, Institut de Mathématiques, Université de Nantes, 2 Chemin de la Houssinière, 44072 Nantes Cédex, France

Jöran Friberg, Department of Mathematics, Chalmers University of Technology and University of Göteborg, Sven Hultins gata 6, S-412 96 Göteborg, Sweden

Ivor Grattan-Guinness, Middlesex Polytechnic, Queensway, Enfield, Middlesex EN3 4SF, England

Jeremy Gray, Faculty of Mathematics, The Open University, Milton Keynes MK7 6AA, England

E. S. Kennedy, 37 Wiggins Street, Princeton, New Jersey 08540

L. Y. Lam, Department of Mathematics, National University of Singapore, Singapore

F. A. Medvedev, Institute of the History of Science and Technology, Staropanski 1/5, Moscow K-2, USSR

Herbert Mehrtens, Jenaer Strasse 6, 1000 Berlin 31, Germany

David Pingree, Department of History of Mathematics, Brown University, Box 1900, Providence, Rhode Island 02912

Ivo Schneider, Institut für Geschichte der Naturwissenschaften der Universität München, Deutsches Museum, D-8000 Munich 26, FRG

Hans Wussing, Karl-Sudhoff-Institut, Karl-Marx-Universität, Talstrasse 33, DDR-701 Leipzig, DDR

A. P. Yushkevich, Institute of the History of Science and Technology, Staropansky 1/5, Moscow K-2, USSR

Sponsors:

Académie Internationale d'Histoire des Sciences, American Mathematical Society, Association of Teachers of Mathematics (Great Britain), British Society for the History of Mathematics, Canadian Mathematical Congress, Canadian Society for the History and Philosophy of Science, Deutsche Mathematiker-Vereinigung, Fibonacci Association, History of Science Society, Indian Mathematical Society, The Institute of Mathematical Statistics, London Mathematical Society, Mathematical Association of America, The Mathematical Association (Great Britain), National Council of Teachers of Mathematics, La Société Mathématique de France. *Historia Mathematica* is the official journal of the Canadian Society for History and Philosophy of Mathematics/Société Canadienne d'Histoire et de Philosophie des Mathématiques.

HISTORIA MATHEMATICA 15 (1988), 40–52

Die Entdeckung der Sylow-Sätze

WINFRIED SCHARLAU

Mathematisches Institut der Universität Münster, Einsteinstr. 62, D-4400 Münster, Germany

HERRN H. WUSSING ZUM 60. GEBURTSTAG, AM 15. OKTOBER 1987 GEWIDMET

The paper describes Sylow's discovery of the theorems named after him. He was led to this discovery by his study of Galois' work, in particular of Galois' criterion for the solvability of equations of prime degree. It is explained how Sylow used methods from Galois theory in his proofs. The paper also discusses relevant correspondence between Sylow, Jordan, and Petersen. © 1988 Academic Press, Inc.

Diese Arbeit behandelt Sylows Entdeckung der Sätze, die nach ihm benannt sind. Er gelangte zu ihnen durch seine Beschäftigung mit Galois' Arbeiten über die Auflösbarkeit von Gleichungen vom Primzahlgrad. Es wird beschrieben, wie Sylow im Beweis seiner Sätze Methoden aus der Galois-Theorie benutzt. Es wird weiterhin auf die diesbezügliche Korrespondenz zwischen Sylow, Jordan und Petersen eingegangen. © 1988 Academic Press, Inc.

Cet article traite de la découverte par Sylow du théorème qui porte depuis son nom. Il a trouvé ce théorème en étudiant les travaux de Galois sur la résolubilité des équations dont le degré est un nombre premier. On y indique comment Sylow utilise dans sa démonstration les méthodes de la théorie de Galois. De plus, on étudie dans cet article la correspondance à ce propos entre Sylow, Jordan et Petersen. © 1988 Academic Press, Inc.

AMS 1980 subject classification: 01A55.

KEY WORDS: Ludvig Sylow, Sylow theorems, Galois theory, group theory.

1. EINLEITUNG UND ZUSAMMENFASSUNG

Diese Arbeit beschäftigt sich mit der Entdeckung der Sylow-Sätze, die ungefähr in das Jahr 1870 fällt. Sie behandelt damit ein wichtiges Ereignis der frühen Geschichte der Gruppentheorie und schließt unmittelbar an eine Arbeit von Waterhouse [1980] an. Für eine knappe, aber sehr prägnante und die wesentlichen Punkte deutlich hervorhebende Darstellung der Geschichte der Gruppentheorie in dem hier interessierenden Zeitraum wird auf Dieudonné [1978, Kapitel 3.4.1] verwiesen, für eine außerordentlich gründliche Diskussion vieler Einzelheiten und Zusammenhänge auf das bekannte Buch von Wußing [1969].

Weil es in wenigen Zeilen geschehen kann (selten genug bei einem historischen Thema), soll zunächst an die Aussagen der Sylow-Sätze erinnert werden: Es sei G eine endliche Gruppe der Ordnung $n = p^k m$ wobei p eine Primzahl und m kein Vielfaches von p ist. Dann enthält G eine Untergruppe P der Ordnung p^k (eine p -Sylow-Gruppe). Je zwei solche Untergruppen P_1, P_2 sind konjugiert, d.h. es existiert $g \in G$ mit $P_2 = gP_1g^{-1}$. Die Anzahl der p -Sylow-Gruppen ist einerseits ein

Teiler von n , andererseits von der Form $p^k + 1$. Schließlich ist jede Gruppe P der Ordnung p^k auflösbar, genauer es existiert eine Folge von Normalteilern $P_1 \subset \dots \subset P_k = P$ mit $|P_i| = p^i$.

Die zentrale Bedeutung dieser—vielleicht technisch und abstrakt erscheinenden—Sätze für die Theorie endlicher Gruppen kann hier nicht erläutert werden. Es muß genügen festzustellen, daß mit ihnen der Grundstein für die gesamte Strukturtheorie endlicher Gruppen gelegt ist [1]. Ihre fundamentale Wichtigkeit wurde auch von dem führenden Gruppentheoretiker des vorigen Jahrhunderts, C. Jordan (1838–1922), sofort erkannt. In [Jordan 1873, 40], einer Arbeit, die erste Anwendungen enthält, schreibt er:

Cette proposition mérite assurément par sa simplicité, sa netteté et sa généralité, d'être considérée comme fondamentale; et nous ne doutons pas qu'elle ne donne lieu à d'importantes conséquences.

Dieses Urteil brauchte Jordan nie zu revidieren; noch im Juli 1907 schrieb er an den inzwischen 75-jährigen L. Sylow (1832–1918) inzwischen auf eine fast vierzig-jährige persönliche und wissenschaftliche Bekanntschaft zurückblickend:

Vous me parlez à la fin de votre lettre des nombreux travaux dont la théorie des groupes a fait l'objet dans ces derniers temps; . . . Et ces travaux devraient vous plaire, n'étant que le développement naturel de vos beaux théorèmes, dont j'ai été le premier, si je me ne trompe à prédire l'importance future. Ils m'ont inspiré à votre égard une amitié intellectuelle qui m'a fait me réjouir à la vue de votre écriture. [2]

Die Geschichte einer mathematischen Theorie ist vor allem die Geschichte der zentralen Sätze und tiefen Ergebnisse dieser Theorie. Entsprechend verdienen die Sylow-Sätze besondere Aufmerksamkeit im Rahmen einer allgemeineren Geschichte der Gruppentheorie. Es ist das Verdienst von Waterhouse [1980], erstmals eine solche Untersuchung vorgelegt zu haben, der von der mathematischen Substanz her nur wenig hinzuzufügen ist und die vor allem eine umfassende Darstellung verschiedener—heute z. T. fast vergessener—Beweisvarianten enthält. Die vorliegende Note—die als Ergänzung zu der Arbeit von Waterhouse angesehen werden kann—beschäftigt sich mehr mit der historischen Seite der Entdeckung der Sylow-Sätze. Während Waterhouse die Zeit nach der ersten Veröffentlichung der Sylow-Sätze im Jahre 1872 behandelt, geht es uns vor allem um die Zeit vor 1872. Es wird der Frage nachgegangen, wie Sylow zu der Problemstellung seiner Sätze gekommen ist, welche Hilfsmittel und Methoden er zur Verfügung hatte, ob und gegebenenfalls welche Anregungen er von Zeitgenossen erhielt, wie er selbst seine Sätze einschätzte, welche Hoffnungen und Erwartungen er mit ihnen verband, wie sie sich vielleicht in ein umfassenderes “Forschungsprogramm” einordnen lassen.

Diese Fragen können nicht alle ganz eindeutig und vollständig beantwortet werden, aber es läßt sich doch folgendes feststellen:

1. Sylow ist ganz offensichtlich von der Theorie der algebraischen Gleichungen und der Galois-Theorie zur Gruppentheorie gekommen und nicht—was auch denkbar wäre—von einer abstrakteren Theorie der Permutations-Gruppen im

Sinne Cauchys (1789–1857). Darüber hinaus war für ihn Gruppentheorie noch praktisch ein Teil der Galois-Theorie, gewissermaßen angewandte Galois-Theorie, und er verwandte galois-theoretische Konstruktionen und Schlüsse an Stellen, die später rein gruppentheoretisch behandelt wurden. Seine ersten beiden Hauptsätze (Existenz, Anzahl und Konjugiertheit der p -Sylow-Gruppen) hat er in unmittelbarem Anschluß an ein Ergebnis von Galois (1811–1832) zunächst in einem sehr speziellen Fall (nämlich p -Sylow-Gruppen einer Untergruppe der S_p) gefunden und anschließend verallgemeinert. Bei dieser Verallgemeinerung könnte Cauchys bekannter Satz (Existenz eines Elementes der Ordnung p in einer Gruppe mit durch p teilbarer Ordnung), der auch im Beweis benutzt wird, eine Rolle gespielt haben [Cauchy 1845].

2. Sylow ist zwar ganz unabhängig von anderen Autoren zu der Entdeckung seiner Sätze gekommen, aber die Gruppentheorie hatte zu dieser Zeit ein Entwicklungsstadium erreicht, daß strukturelle Fragen dieser Art nahelagen und die Zeit für die Entdeckung der Sylow-Sätze reif war. Schon bei Galois und Dedekind (1831–1916) finden sich in lange Zeit unveröffentlicht gebliebenen Manuskripten Teilaussagen der Sylow-Sätze. Weiterhin war etwa gleichzeitig mit Sylow der dänische Mathematiker J. Petersen (1839–1910) [3] im Zusammenhang mit Konstruktionsproblemen auf das Problem der Auflösbarkeit der 2-Gruppen gestoßen. Über diesen Fragenkreis existiert eine Korrespondenz zwischen Sylow und Petersen aus den Jahren 1870/71.

3. Wenn auch—wie gerade gesagt—die Zeit für die Untersuchung der inneren Struktur der endlichen Gruppen gekommen war, so rückten diese Probleme doch nicht sofort in das Zentrum des Interesses der Gruppentheoretiker. Das eigentlich zentrale Problem der Gruppentheorie im ganzen 19. Jahrhundert seit Cauchy und Galois war das Klassifikationsproblem oder, genauer und sinnvoller, das Problem der Klassifikation transitiver Permutationsgruppen, wobei von vornherein naheliegend war, nach Ordnung, Grad und Transitivitätsgrad vorzugehen. Wesentliche Beiträge stammten vor allem von Jordan [1961] und E. Mathieu (1835–1890) [4]. Wie aus seinem Nachlaß und dem Briefwechsel mit Jordan ersichtlich ist, stand dieses Problem auch bei Sylow im Vordergrund des Interesses. Auf die Sylow-Sätze stieß er vielleicht eher beiläufig. Er versuchte, sie sofort auf dieses Problem anzuwenden, und in seinen Briefen klingt etwas Enttäuschung an, daß sie bei der Bearbeitung des Klassifikationsproblems sich nicht von durchschlagendem Nutzen erwiesen.

2. DAS ERBE GALOIS'

Unsere heutige (Lehrbuch-) Literatur suggeriert insofern ein etwas unzutreffendes Bild, als man den Eindruck gewinnen könnte, daß Galois' Hauptleistung darin bestand, das gefunden zu haben, was wir heute Galois-Theorie nennen. Dies ist nur sehr eingeschränkt richtig: ein Kernpunkt der Galois-Theorie, nämlich die Bedeutung der Gruppen für die Behandlung algebraischer Gleichungen, war schon vorher im Prinzip bekannt. Insbesondere war J. J. Lagrange (1736–1813) in seiner großen Arbeit zu diesem Thema schon dem "Hauptsatz der Galois-Theo-

rie" sehr nahe gekommen—und zwar nicht nur im "generischen Fall" unbestimmter Koeffizienten der betrachteten algebraischen Gleichung, sondern im allgemeinen [Lagrange 1770/71, insbesondere Artikel 104]. Auch hatte er die prinzipielle Bedeutung der Gruppentheorie für dieses Problem erkannt. Vielleicht würde es zu weit gehen zu behaupten, daß Lagrange den Hauptsatz der Galois-Theorie schon kannte, aber er hatte zweifellos klare und richtige Vorstellungen davon, in welcher Richtung die Theorie der algebraischen Gleichungen zu entwickeln sei [5]. Die eigentliche Leistung von Galois besteht darin, daß er schon weit über "abstrakte Galois-Theorie" hinausgeht und, angeregt von dem Problem der Auflösung algebraischer Gleichungen durch Radikale, mit einer eingehenden Untersuchung der Struktur endlicher Gruppen beginnt. Zu diesem Zweck—und das ist sicher eine seiner beeindruckendsten Ideen—erfindet er die Theorie der endlichen Körper, um nämlich durch Darstellung der Gruppe in einer passenden linearen Gruppe über einem endlichen Körper Auflösbarkeitsaussagen zu gewinnen. Damit ist mit einem Schlage ein weites Spektrum gruppentheoretischer Probleme und Konzepte angesprochen: die Untersuchung der inneren Struktur endlicher Gruppen, das Problem der Bestimmung auflösbarer Gruppen, die Beschreibung von Gruppen als lineare Gruppen über endlichen Körpern und damit eine erste Idee einer allgemeinen Darstellungstheorie, etwas spezieller und konkreter dann die Bestimmung der auflösbaren Untergruppen affiner oder projektiver linearer Gruppen, und, weil Galois-Gruppen als transitive Permutationsgruppen operieren, die Untersuchung transitiver Gruppen nach Ordnung, Grad und Transitivitätsgrad. Auf diesem Gebiet ist Galois praktisch ohne Vorgänger und aus dem Nichts heraus zu Ergebnissen gekommen, von denen Bourbaki [1971, 70] noch hundert Jahre später sagen konnte, daß sie "zu den scharfsinnigsten der Theorie zählen". Galois selbst hat die Bedeutung und Tragweite dieser Zusammenhänge selbst hervorgehoben, als er schrieb:

C'est surtout dans la théorie des permutations, ou l'on a sans cesse besoin de varier la forme des indices, que la considération des racines imaginaires des congruences paraît indispensable. Elle donne un moyen simple et facile de reconnaître dans quel cas une équation primitive est soluble par radicaux, comme je vais essayer d'en donner en deux mots une idée. [Galois 1962, 125]

Eines der bemerkenswertesten Einzelergebnisse Galois' war sein Kriterium für die Auflösbarkeit irreduzibler Gleichungen vom Primzahlgrad, das sich rein gleichungstheoretisch formulieren ließ (in heutiger Sprechweise: $p(x) = 0$ ist auflösbar durch Radikale genau dann, wenn der Zerfällungskörper durch je zwei beliebige Wurzeln erzeugt wird). Vergleiche die Bemerkung:

Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que deux quelconques des racines étant connus, les autres s'en déduisent rationnellement. [Galois 1962, 69]

Bekanntlich hat Galois weder Zeit gehabt noch sich die Zeit genommen, sein algebraisches und gruppentheoretisches Programm auszuführen. Es kann aber kein Zweifel bestehen, daß er mehr gewußt hat, als sich in seinen Aufzeichnungen

oder gar seinen Publikationen findet. So kann auch kaum verwundern, daß er offenbar den wesentlichen Teil der Sylow-Sätze gekannt hat, wie sich aus einer unveröffentlichten Randbemerkung ergibt, auf die wohl als erster Dieudonné [1978, 117] hingewiesen hat. Es heißt dort [Galois 1962, 72]:

Théorème. Si le nombre des permutations d'un groupe est divisible par p^n (p étant premier), le group aura pour diviseur un groupe de p^n permutations.

Es ist müßig, darüber zu spekulieren, ob Galois diesen Satz wirklich bewiesen oder nur erraten hatte. Sicher hatte er die Fähigkeiten und Mittel zum Beweis. Andererseits ist zu bedenken, daß der Satz, so wie er formuliert ist, fast die Auflösbarkeit der p -Gruppen mit einschließt. Da sein Hauptziel gerade Auflösbarkeitskriterien waren, wäre es dann eigentlich naheliegend gewesen, ihn auch in diesem Zusammenhang zu erwähnen.

Es ist oben gesagt worden, daß Galois' Werk für jeden Mathematiker dieser Generation eine Herausforderung darstellen mußte. Einer, der diese Herausforderung (in später beiseite gelegten Untersuchungen) annahm, war Dedekind [1932; 1981]. Es ist nicht notwendig, darauf noch einmal näher einzugehen. Was die Gruppentheorie betrifft, sollen nur drei Feststellungen gemacht werden: 1) Für einen Mathematiker vom Range Dedekinds bestanden um die Jahrhundertmitte keine grundsätzlichen Schwierigkeiten mehr, eine abstrakte Gruppentheorie zu konzipieren und mit einer Ausarbeitung zu beginnen, 2) als eines der ersten Probleme stellte sich das Klassifikationsproblem [Dedekind 1932, 439; Cayley 1878], 3) ausgehend von Cauchys schon erwähntem Satz scheint eine Untersuchung der inneren Struktur der endlichen Gruppen immer in Richtung auf die Sylow-Sätze zu verlaufen: Dedekind zeigt, daß eine p -Gruppe ein nicht-triviales Zentrum hat; da er den Begriff der Faktorgruppe kannte, hätte er daraus ohne weiteres die Auflösbarkeit der p -Gruppen folgern können [6, 7].

Überhaupt kann man feststellen, daß die Galois-Theorie in den fünfziger und sechziger Jahren recht schnell bekannt wurde; eine größere Zahl von Mathematikern in verschiedenen Ländern beschäftigten sich mit ihr, darunter auch weniger bekannte oder solche, die an abgelegenen Orten wirkten, wie Sylow selbst oder der schon erwähnte Petersen.

3. SYLOWS WEG ZU DEN SYLOW-SÄTZEN

Aus der vorhandenen Literatur und einigen weniger bekannten Arbeiten Sylows, seinem Nachlaß und seinem Briefwechsel läßt sich rekonstruieren, wann und wie Sylow zu seinen gruppentheoretischen Untersuchungen gekommen ist. Wir stützen uns vor allem auf den von Kragemo [1933] verfaßten Lebenslauf, auf Sylows eigene Arbeiten [1867] und [1872] und auf den im Nachlaß befindlichen Briefwechsel mit Jordan und Petersen [8].

Von Kragemo erfahren wir zunächst, daß Sylow sich schon während seines Lehramtsstudiums mit der Theorie der Gleichungen beschäftigt hat, und daß er sich von ca. 1856 an, angeregt durch seinen Lehrer C. A. Bjerknes (1825–1903), intensiv mit Abels (1802–1829) z. T. fragmentarischen Untersuchungen über al-

gebraische Gleichungen beschäftigt hat. Unabhängig von Kronecker (1823–1891) gelang es ihm, ein Fragment von Abel zu vervollständigen. 1860 reichte er diese Arbeit bei Crelles Journal ein; die Arbeit wurde aber von Kronecker abgelehnt. 1861 erhielt er ein Stipendium, reiste nach Berlin, Leipzig und Paris, "um die Bekanntschaft der bedeutendsten Mathematiker zu machen und die Theorie der Gleichungen und die Theorie der Gruppen zu studieren". Spätestens zu dieser Zeit muß er auch begonnen haben, sich intensiver mit Galois zu beschäftigen, dessen Arbeiten in Serrets Cours d'algèbre supérieure allgemein bekannt geworden waren. Schon im Frühjahr 1863 hielt Sylow eine Vorlesung über Galois-Theorie, zu deren Hörern auch Lie (1842–1899) gehörte.

Einige Jahre später publiziert er dann seine erste selbständige Arbeit [Sylow 1867] über Gruppentheorie, die der Sache nach genau zwischen Galois' schon erwähnter Arbeit über irreduzible Gleichungen vom Primzahlgrad und seiner eigenen späteren Arbeit über die Sylow-Sätze steht. Sylow beweist nämlich in dieser Arbeit die Aussagen der Sylow-Sätze im Spezialfall einer Untergruppe der symmetrischen Gruppe S_n vom Primzahlgrad n für diese Primzahl n . Ausgangspunkt dieser Untersuchung war offensichtlich die naheliegende Frage nach den möglichen Ordnungen der Gruppe einer irreduziblen Gleichung vom Primzahlgrad. Er schreibt diese Ordnung in der Form $n(np + 1)\nu$ (wobei ν also der Index einer n -Sylow-Gruppe in ihrem Normalisator und $np + 1$ der Index dieses Normalisators ist); es verdient hervorgehoben zu werden, daß er auch in seiner späteren Arbeit genau diese Bezeichnungen verwendet. Damit liegt die Vermutung nahe, daß die berühmte Arbeit von 1872 unmittelbar aus diesen Untersuchungen erwachsen ist.

Dies wird durch den Briefwechsel mit Petersen bestätigt, der Ende der sechziger Jahre an seiner Dissertation über Konstruktionen mit Zirkel und Lineal arbeitete. Er versuchte, die in diesem Zusammenhang zentrale Frage zu lösen, welche algebraischen Gleichungen die Koordinaten von konstruierbaren Punkten erfüllen müssen. Er war schon ungefähr zu der richtigen Vermutung gekommen, deren gruppentheoretischer Kern besagt, daß die Galois-Gruppe eine 2-Gruppe sein muß. Da er das Problem jedoch nicht vollständig lösen konnte, wandte er sich in einem Brief vom 19.7.1870 an Sylow mit der Bitte um Auskunft, ob Galois etwas zu dieser Frage gesagt hätte. Sylow antwortete daraufhin in einem Brief vom 17.9.70 unter anderem folgendes [9]:

Aus Ihrem Brief schließe ich, daß es nur einen Punkt gibt (nämlich 5) für welchen Ihnen der Beweis noch fehlt. Ich glaube, hierüber versichern zu können, daß es sich wirklich so verhält, wie Sie vermuten. Wenn sich eine irreduzible algebraische Gleichung vom Grad 2^n mit Quadratwurzelzeichen auflösen läßt, dann kann jede Wurzel durch n Quadratwurzeln rational ausgedrückt werden, so daß jede Kombination der Vorzeichen dieser Wurzeln eine neue Wurzel der Gleichung gibt. Ausgehend von einem Satz der Substitutionentheorie, den ich schon längere Zeit gekannt, aber noch nicht veröffentlicht habe, bin ich imstande, dies zu beweisen. Ich habe in diesem Winter den ersten Entwurf einer Abhandlung, wo dieser Satz unter anderen bewiesen werden soll, ausgearbeitet. Da ich aber während der letzten zwei Jahre die ausländischen Zeitschriften nicht ordentlich verfolgt habe, habe ich sie zur Seite gelegt, weil ich erst feststellen will, ob jemand anders in der letzten Zeit dieselben Dinge

bewiesen hat. Hiermit bin ich jetzt beschäftigt, und wenn ich nach Frederikshald zurückkomme, wird es vermutlich meine erste Arbeit sein, diese Abhandlung fertig zu machen. Wenn ich von den Resultaten dieser Abhandlung ausgehen kann, wird der Beweis für Punkt 5) in Ihrem Brief einfach sein. Es wird ein Spezialfall eines allgemeinen Theorems über Gleichungen vom Grad p^n sein, deren Auflösung auf die sukzessive Lösung von n "abelschen" Gleichungen vom Grad p reduziert werden kann.

Sylow drückt sich weder hier noch in folgenden Briefen völlig eindeutig über die von ihm entdeckten Sätze aus; es hört sich aber ganz so an, als ob er die Sylow-Sätze zu diesem Zeitpunkt schon einige Zeit lang gekannt und bewiesen hatte. Er gibt auch keine Andeutung einer Beweismethode und überläßt es insbesondere Petersen, den Fall $p = 2$ selbst zu erledigen. In seiner Veröffentlichung von 1872 weist er auf Petersens Arbeit hin, ohne anzudeuten, daß er diesen Satz schon früher und unabhängig von Petersen gekannt hat.

4. GRUPPENTHEORIE ALS GALOIS-THEORIE

Sylow ist also unzweifelhaft von der Theorie algebraischer Gleichungen und Galois-Theorie zur Gruppentheorie gekommen. Es soll jetzt diskutiert werden, welche Konsequenzen sich aus diesem Ansatz ergaben und wie die Beweise von Sylows Sätzen vor diesem Hintergrund zu lesen sind. In diesem Zusammenhang ist als erstes festzustellen, daß allen Mathematikern dieser Generation offenbar die Tatsache geläufig war, daß jede Permutationsgruppe als Galois-Gruppe realisiert werden kann, und daß man sich somit bei der Untersuchung beliebiger Gruppen auf Galois-Gruppen beschränken kann [10]. Ein besonders eindrucksvoller Beleg dafür findet sich in einem Algebra-Lehrbuch aus dieser Zeit, das von dem schon mehrfach erwähnten Petersen verfaßt worden war. Dort heißt es [Petersen 1878, 325]:

Der obenstehende Beweis zeigt, dass keine anderen transitiven Gruppen von der Ordnung p^n ($n > 1$) existieren als imprimitive. Der Beweis setzt freilich voraus, dass es eine Gleichung giebt, welche die gegebene Gruppe hat. Indessen entspricht jeder Gruppe eine Gleichung, nämlich die allgemeine Gleichung vom Grade der Gruppe, wenn man dieser eine Function der Wurzeln, die durch die Substitutionen der Gruppe und nicht durch andere Substitutionen unverändert bleibt, adjungiert denkt.

Kürzer und lakonischer könnte man wohl auch heute nicht die übliche Konstruktion einer Gruppe als Galois-Gruppe abhandeln, und man wird annehmen können, daß dieser Gedankengang allgemein bekannt war, wenn er so knapp beschrieben wurde. Auch Sylow [1867] schreibt zu Beginn seiner erwähnten Arbeit ohne nähere Ausführungen:

Auf der anderen Seite kann man auch beweisen, daß zu jedem gegebenen System von konjugierten Substitutionen [d.h. zu jeder Gruppe] eine entsprechende Gleichung existiert.

Wie noch ausgeführt werden wird, machte er in seiner Arbeit über die Sylow-Sätze von dieser Tatsache implizit Gebrauch. Schließlich ging Kronecker schon einen Schritt weiter, indem er nämlich bereits 1853 das Problem aufwarf, welche Gruppen eigentlich als Galois-Gruppen über $\mathbb{Q}$ realisiert werden können, wobei

die Realisierbarkeit über einem passenden Körper mit unbestimmten Elementen für ihn wohl selbstverständlich war:

Ja, man konnte eigentlich gar nicht wissen, ob . . . überhaupt noch irgend welche Gleichungen existieren, welche die gegebenen Auflösbarkeits-Bedingungen erfüllen. Noch weniger konnte man solche Gleichungen bilden. . . . [Kronecker 1853, 3]

Es ist durchaus amüsant zu verfolgen, wie Sylow und auch Petersen von der Realisierung einer beliebigen Gruppe als Galois-Gruppe Gebrauch machen. Sieht man sich die heutigen Beweise der Sylow-Sätze an, so ist ein Kernpunkt immer, eine geeignete Operation der Gruppe anzugeben. Vom Standpunkt der Galois-Theorie ist nichts einfacher und natürlicher als das: die Galois-Gruppe operiert eben auf den Wurzeln der Gleichung bzw. den Konjugierten irgendeines passenden Elementes. Auch kann man in der Sprache der Galois-Theorie die abstrakt-gruppentheoretische Konstruktion der Faktorgruppe nach einem Normalteiler umgehen: diese ist einfach die Galois-Gruppe des entsprechenden Normalkörpers. In ähnlicher Weise braucht man auch keine Nebenklassen nach einer Untergruppe; diese werden ebenfalls durch Konjugierte eines passenden Körperelementes ersetzt. Nach diesen Vorbemerkungen liest sich der Beweis von Sylows erstem Satz dann in ganz natürlicher Weise wie folgt [vgl. Waterhouse 1980]: Es sei G die Galois-Gruppe der Körpererweiterung L/K , ferner P eine maximale Untergruppe von p -Potenzordnung, N ihr Normalisator und F der Fixkörper von N . Wegen der Maximalität von P enthält N/P keine Elemente von p -Potenzordnung, und nach dem Satz von Cauchy ist $|N/P|$ teilerfremd zu p . Es sei jetzt $x = x_1$ primitives Element von F mit Konjugierten $x_1, \dots, x_h$. Wir betrachten die Operation von P auf den x_i . Trivialerweise wird x_1 festgelassen. Dies kann aber für kein anderes $x_i = gx_1$, $g \in G$, gelten, denn aus $Pgx_1 = gx_1$ folgt $g^{-1}Pgx_1 = x_1$, also $g^{-1}Pg \subset N$. Dann gilt aber sogar $g^{-1}Pg = P$, denn alle Elemente von p -Potenzordnung von N liegen schon in P . Es folgt $g \in N$, also $x_i = x_1$. Die Menge $\{x_1, \dots, x_n\}$ zerfällt also unter der Operation der p -Gruppe P in Bahnen, von denen nur eine 1-elementig ist. Es folgt $h \equiv 1 \pmod{p}$ und damit der erste Sylow-Satz.

In ganz ähnlicher Weise geht Petersen in seinem Lehrbuch beim Beweis der Auflösbarkeit der p -Gruppen vor. Wie wir in dem oben angeführten Zitat gesehen haben, hebt er diesen Ansatz auch ganz ausdrücklich hervor. Es ergibt sich dann eine etwas andere Aussage und ein anderer Beweis als heute üblich für diesen Satz; sein eigentliches Anliegen ist ein Satz über die Auflösung algebraischer Gleichungen, den er so formuliert:

Die notwendige und ausreichende Bedingung dafür, dass eine Gleichung mit Hilfe von Abelschen Gleichungen p^{ten} Grades aufgelöst werden kann, besteht darin, dass die Ordnung ihrer Gruppe eine Potenz von p ist. Ihr Grad ist dann auch eine Potenz von p .

In heutiger Terminologie beweist Petersen folgendes: Ist G eine p -Gruppe und H eine Untergruppe, so existiert eine Folge von Untergruppen $G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_k = H$, so daß H_{i+1} normal vom Index p in H_i ist. Sein galois-theoretischer Beweis verläuft in heutiger Ausdrucksweise folgendermaßen: Sei G die

Galois-Gruppe von L/K und F der Fixkörper von H mit einem primitiven Element x . Wir betrachten die Operation von H auf den Konjugierten von x . Da x festgelassen wird, müssen wenigstens $(p - 1)$ Konjugierte $x_2, \dots, x_p$ auch festgelassen werden, liegen also in F . Es gibt ein $\sigma \in G$ mit $\sigma x_1 = x_2$, also $\sigma F = F$. Also ist σ ein nicht-trivialer Automorphismus von F , etwa der Ordnung p^r . Es sei F_1 der Fixkörper von σ^{p^r-1} und $H_1 \supset H$ die zugehörige Galois-Gruppe. Dies Verfahren wird dann fortgesetzt.

Es ist interessant, zum Vergleich einen Blick auf Sylows eigenen Beweis dieses Satzes zu werfen: In seinem ersten und wesentlichen Teil ist es genau der bis heute übliche; G operiert durch Konjugation auf sich selbst, und man stellt fest, daß das Zentrum nicht-trivial ist. Weil er den Begriff der Faktorgruppe nicht kennt oder nicht benutzen will, kommt Sylow anschließend auf seine galois-theoretische Betrachtungsweise zurück, um die Induktion zu Ende zu führen.

Mit diesen Beispielen sollte hinreichend deutlich geworden sein, wie eng in dem betrachteten Zeitraum die Gruppentheorie noch mit der Galois-Theorie zusammenhing und wie die genannten Mathematiker von gleichungstheoretischen Fragestellungen ausgingen. Es sollte jedoch noch auf einen Punkt in diesem Zusammenhang eingegangen werden, nämlich die wesentliche Rolle, die der Satz vom primitiven Element in den diskutierten Beweisen spielte. Bei Sylow wird er in folgender Form gebraucht: Ist H eine Untergruppe der vollen Permutationsgruppe von m Unbestimmten, so existiert eine rationale Funktion in diesen Unbestimmten, die genau unter den Substitutionen aus H invariant bleibt. Diese Funktion ist also ein primitives Element des Fixkörpers von H (auf dem rationalen Funktionenkörper in den m Unbestimmten operierend gedacht) über dem Körper der symmetrischen Funktionen. Es verdient hervorgehoben zu werden, daß dieser Satz (oder eng verwandte) einer der Kernpunkte beim Aufbau der Galois-Theorie war; er hängt ja auch mit dem Hauptsatz der Galois-Theorie eng zusammen. Er spielte eine wesentliche Rolle bei Galois selbst [Galois 1962, 47 ff.] als auch in späteren Darstellungen der Galois-Theorie [Dedekind 1981, 81]. Insofern wurde er von Sylow (und auch Petersen) wie selbstverständlich benutzt [12].

5. GRUPPENTHEORIE IN DER GENERATION NACH GALOIS

Es würde über die Fragestellung dieses Aufsatzes hinausgehen zu versuchen, eine vollständige Darstellung der Hauptentwicklungstendenzen in der Gruppentheorie nach Galois zu geben. Es soll darauf nur so weit eingegangen werden, daß deutlich gemacht werden kann, wie Sylows Arbeiten sich in diese Tendenzen einpassen. Insgesamt ergibt sich ein Bild von bemerkenswerter Einheitlichkeit. Sowohl Cauchys Theorie der Permutationsgruppen als auch die Galois-Theorie (die die abstrakte Gruppentheorie um Begriffe wie Normalteiler, Faktorgruppe, auflösbare Gruppe etc. bereichert hat) führen in natürlicher Weise zu der Untersuchung (transitiver) Gruppenoperationen. Dieses Problem steht, wie schon in der Einleitung hervorgehoben, (neben dem der Untersuchung linearer Gruppen) ganz cindeutig im Vordergrund des Interesses.

Es ist meines Erachtens nicht angebracht, den Gegensatz zwischen abstrakter

Gruppentheorie und Theorie der Permutationsgruppen in dieser Zeit überzubetonen. Es scheint vielmehr, daß das Konzept einer abstrakten Gruppentheorie den Mathematikern dieser Generation durchaus gegenwärtig war und den (oft unausgesprochenen) Hintergrund ihrer Arbeiten bildete. Zumindestens Cayley [1878] und Dedekind [1981] hatten auch schon in den fünfziger Jahren ganz explizit eine abstrakte Gruppentheorie konzipiert. Beide stellen in diesem Zusammenhang auch das Problem der Klassifikation aller (endlichen) Gruppen als zentrale Frage auf. Andererseits ist der Satz von Cayley, daß jede abstrakte Gruppe als Permutationsgruppe realisiert werden kann, eine solche Trivialität, daß er sicher ebenso allgemein bekannt war wie die Identität der Begriffe Permutationsgruppe und Galois-Gruppe. Es gab also für die Gruppentheoretiker dieser Zeit—insbesondere soweit sie an konkreten Fortschritten in dieser Theorie und nicht wie Dedekind an abstrakter Algebra interessiert waren—kaum einen Anlaß, scharf zwischen abstrakten Gruppen, Permutationsgruppen und Galois-Gruppen zu unterscheiden. Schließlich ist auch vom rein mathematischen Standpunkt die Untersuchung der Permutationsgruppen naheliegender und erfolversprechender als abstrakte Gruppentheorie. Stellt man sich z. B. das naheliegende Problem der Bestimmung mehrfach transitiver Gruppen, wie es Mathieu und Jordan getan haben, so kommt man bald zu tiefen Ergebnissen und schwierigen Problemen, die auch heute noch nicht gelöst sind.

Aus allen vorhandenen Dokumenten ergibt sich ganz eindeutig, daß Fragen dieser Art es waren, die auch Sylow sein ganzes Leben lang beschäftigt haben und die sein mathematisches Werk geprägt haben. Es ist schon ausgeführt worden, wie er sich im Anschluß an Galois die Frage nach den Untergruppen der S_p gestellt hat, und wie er dadurch zu seinen Theoremen gekommen ist. Diese Sätze versucht er noch in derselben Arbeit von 1872, auf Probleme über transitive Gruppenoperationen anzuwenden, wobei er Resultate von Mathieu verallgemeinerte [Sylow 1872, Théorème VI, VII und VIII]. An Jordan schreibt er um diese Zeit über seine weiteren Absichten:

Je me suis proposé le problème de trouver toutes les groupes de degré n et d'ordre $(n + 1)n \cdot v$, mais je n'ai encore pu le résoudre. . . . L'insuffisance des mes efforts pour résoudre ce problème ayant un peu rebaisé l'opinion que je m'étais d'abord formée sur l'utilité de mon théorème. . . . Quand vous me honorez d'une seconde lettre, je vous prie Monsieur de vouloir bien me dire si l'on a fait l'énumération des groupes transitifs pour des degrés plus grands de 7, et où cela est imprimé. . . . (Brief vom 20.8.1872)

Je vais maintenant m'occuper du nombre p dans l'égalité $0 = n^p v(np + 1)$ et de la forme des groupes d'ordre n^p (Brief vom 6.12.1872)

Dans le temps évlée depuis ma dernière lettre je me suis principalement occupé des groupes d'ordre n^p , en me bornant pour le moment aux groupes transitifs. . . . (Brief vom 8.2.1873)

Jordan seinerseits wendet, unmittelbar nachdem er bei seinem Besuch in Christiania (Oslo) von Sylows Sätzen erfahren hatte, diese—ganz im Sinne des beschriebenen “Forschungsprogrammes”—an, um Abschätzungen für den höchstmöglichen Transitivitätsgrad einer Permutationsgruppe zu erhalten. Mit Unter-

suchungen dieses Problems hatte er sich schon früher in mehreren Noten beschäftigt [Jordan 1961]. Um diese Fragestellung geht es hauptsächlich in seinen Briefen an Sylow aus dieser Zeit; er publiziert diese Resultate in [1873] und hebt in der Einleitung die Bedeutung von Sylows Ergebnissen hervor (vgl. das Zitat in Abschnitt 1).

Sylow selbst hat nur noch einmal [1888] eine größere gruppentheoretische Arbeit publiziert, die wohl viel früher entstanden war und sich unmittelbar an frühere Untersuchungen von Galois, Jordan und ihm selbst anschließt. Hatte er in der Arbeit [1867] transitive Gruppen vom Grad p untersucht, so geht es in dieser Arbeit um transitive Gruppen vom Grad p^2 . Er bestimmt weitgehend vollständig in diesem Fall die Struktur der möglichen p -Sylow-Gruppen, ihrer Normalisatoren und die möglichen Ordnungen dieser Gruppen. Galois und Jordan hatten sich mit den auflösbaren Gruppen dieser Art beschäftigt, über die Galois eine Vermutung geäußert hatte, die von Jordan berichtigt, vervollständigt und bewiesen worden war. Sylow erweitert diese Untersuchungen also auf nicht-auflösbare Gruppen. Aus seinem unveröffentlichten Nachlaß [vgl. Skolem 1922] ist ersichtlich, daß er sich auch intensiv mit höheren Graden, insbesondere dem Fall p^3 , aber auch zusammengesetzten Graden wie $2p$ beschäftigt hat. Zu abschließenden Resultaten und Publikationen ist er aber nicht mehr gekommen.

Sylow wirkte als Gymnasiallehrer im abgelegenen Frederikshald weitab von allen Zentren mathematischer Aktivität, und er klagte oft in seinen Briefen über seine völlige Isolierung. Wohl deshalb und auch wegen anderer zeitraubender Verpflichtungen (Abel-Ausgabe, Mitherausgabe der *Acta Mathematica*) hat er nur einmal eine bahnbrechende Arbeit veröffentlicht. Seine wirkliche Originalität und mathematische Kraft ist deshalb nur schwer abzuschätzen. In seinem gruppen- und galois-theoretischen Werk hat er sich jedenfalls mit zentralen Problemen beschäftigt. Es bleibt sein Verdienst, eines der Hauptergebnisse der Strukturtheorie endlicher Gruppen entdeckt zu haben, auch wenn diese Entdeckung um diese Zeit fast als historische Notwendigkeit erscheint.

FUSSNOTEN

1. Z. B. heißt es in Hupperts umfangreichem Handbuch [1967, 35]: Die Sätze 7.3 bis 7.6 [das sind die Sylow-Sätze] sind von grundlegender Bedeutung für die Theorie der endlichen Gruppen. Wir werden sie immer wieder verwenden, und ein nicht geringer Teil unserer Arbeit wird die Suche nach Ausdehnungen dieser Sätze sein.

2. Die Briefe Jordans an Sylow werden mit dem Nachlaß Sylows in der Universitätsbibliothek Oslo aufbewahrt. Ich danke T. Gulliksen für die Beschaffung von Fotokopien und der Universitätsbibliothek für die Genehmigung zur auszugsweisen Veröffentlichung.

3. J. Petersen war offenbar ein guter und kenntnisreicher Mathematiker, der eine Reihe ausgezeichnete Lehrbücher verfaßt hat. Eine wissenschaftliche Biographie über ihn, die seine Beziehungen zu anderen Mathematikern beschreibt und etwas Licht auf den Entwicklungsstand der Mathematik in den skandinavischen Ländern wirft, wäre wünschenswert.

4. Im Sinne der These, daß die Geschichtsschreibung einer mathematischen Theorie sich vor allem mit den tiefen Resultaten befassen sollte, wäre eine Untersuchung über Mathieus bemerkenswertes Werk, insbesondere seine Entdeckung der nach ihm benannten einfachen Gruppen, höchst wün-

schenswert. Hier ist ein Vorgriff auf eine Entwicklung zu sehen, die erst fast 100 Jahre später wirklich aktuell wurde.

5. Bei Lagrange [1770/71, 403] heißt es: *Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire; tout se réduit, comme on voit, à une espèce de calcul de combinaisons, par lequel on trouve à priori les résultats auxquels on doit s'attendre.*

6. Galois, Dedekind und Sylow erwähnen alle drei im Zusammenhang mit den Sylow-Sätzen zunächst den Satz von Cauchy.

7. Dedekinds gruppentheoretische Studien werden in Wußings grundlegender Untersuchung [1969] nicht erwähnt; auch der hier diskutierte Problemkreis wird nur stiefmütterlich behandelt. Insgesamt erscheinen einige Korrekturen an dem von Wussing gezeichneten Bild notwendig: 1.) Die Idee einer abstrakten Gruppentheorie schien schon lange, bevor sie explizit formuliert wurde, den Gruppentheoretikern durchaus gegenwärtig gewesen zu sein, und half ihnen, Ordnung und Struktur in ihre Untersuchungen zu bringen. 2.) Zumindest die Theorie endlicher Gruppen hat sich überwiegend wohl doch aus der Galois-Theorie entwickelt. Eine ausführliche Diskussion ist hier nicht möglich.

8. Der Briefwechsel Petersen-Sylow wird an der Universität Oslo aufbewahrt; vgl. Fußnote 2. Die Briefe von Sylow an Jordan befinden sich in der Bibliothèque centrale de l'école polytechnique in Palaiseau. Ich danke Frau Cl. Billoux für freundliche Unterstützung bei der Beschaffung der Briefe.

9. Ich danke J. Høyrup für Hilfe bei der Entzifferung und Übersetzung dieser Briefe.

10. In diesem Zusammenhang ist es wohl eher nebensächlich, ob und wie weit der abstrakte Gruppenbegriff und die Darstellung abstrakter Gruppen als Permutationsgruppen bekannt war.

11. Dieses Buch, dessen dänische Originalausgabe ein Jahr früher erschienen war, ist ein bemerkenswert klares, verständliches und vollständiges Lehrbuch der Algebra, weit besser als Serrets und vermutlich eines der besten vor Webers Algebra. Es verdiente, etwas besser bekannt zu sein.

12. In diesem Zusammenhang meine ich, daß Waterhouse [1980, 280] sich etwas mißverständlich ausdrückt, wenn er schreibt:

But historically more interesting (and making the proof much harder to read) is the fact that Sylow does not explicitly have the concept of action on cosets. What appears in its place is a theorem of Cauchy which is hardly remembered now: If H is any group of substitutions of n variables, then there is a function of those variables left invariant by the substitutions in H and by no other substitutions.

Es geht im wesentlichen einfach um den Satz vom primitiven Element!

LITERATUR

- Bourbaki, N. 1965. *Eléments d'histoire des mathématiques*. Paris: Hermann. Deutsche Übersetzung: *Elemente der Mathematikgeschichte*. Göttingen: Vandenhoeck u. Ruprecht, 1971.
- Cauchy, A. L. 1845. Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières et des systèmes de substitutions conjuguées. *Comptes Rendus hebdomadaires des Séances de l'Académie des Sciences* 21, 835–852, 895–902, 931–933, 972–987, 1025–1041. Zitiert wird nach: *Oeuvres*, I^{re} Série, vol. 9, 342–358. Paris: Gauthier-Villars, 1896.
- Cayley, A. 1878. Desiderata and suggestions. *American Journal of Mathematics* 1, 50–52. Abgedruckt in: *Mathematical papers*, vol. 10, pp. 401–403. Cambridge: The Univ. Press, 1896.
- Dedekind, R. 1932. Aus den Gruppen-Studien (1855–1858). In *Gesammelte Mathematische Werke*, R. Fricke, E. Noether, O. Ore, Hrsgg., vol. 3, pp. 439–446. Braunschweig: Vieweg.
- 1981. Eine Vorlesung über Algebra. In *Richard Dedekind 1831/1981*, W. Scharlau, Hrsg. Braunschweig/Wiesbaden: Vieweg.
- Dicudonné, J. (Hrsg.) 1978. *Abrégé d'histoire des mathématiques 1700–1900*. Paris: Hermann.

- Deutsche Übersetzung: *Geschichte der Mathematik 1700–1900*. Braunschweig/Wiesbaden: Vieweg, 1985.
- Galois, E. 1962. *Ecrits et mémoires mathématiques*, R. Bourgne und J. P. Azra, Hrsgg. Paris: Gauthier-Villars.
- Huppert, B. 1967. *Endliche Gruppen*, vol. 1. Berlin/Heidelberg/New York: Springer.
- Jordan, C. 1873. Sur la limite de transitivité des groupes non alternés. *Bulletin de la Société mathématique de France* **1**, 40–71. Wieder abgedruckt in: *Oeuvres*, J. Dieudonné, Hrsg., vol. 1, pp. 365–396. Paris: Gauthier-Villars, 1961.
- 1961. *Oeuvres*, J. Dieudonné, Hrsg., vol. 1. Paris: Gauthier-Villars.
- Kragemo, H. B. 1933. Ludvig Sylow. *Norsk Matematisk Tidsskrift* **15**, 73–99.
- Kronecker, L. 1853. Über die algebraisch auflösbaren Gleichungen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* vom Jahre 1853, 365–374. Wieder abgedruckt in *Werke*, K. Hensel, Hrsg., vol. 4, pp. 3–11. Leipzig/Berlin: Teubner, 1929.
- Lagrange, J. L. 1770/71. Réflexions sur la résolution algébrique des équations. *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin* 1770, 134–215 und 1771, 138–253. Zitiert wird nach: *Oeuvres*, vol. 3, pp. 203–421. Paris: Gauthier-Villars, 1869.
- Petersen, J. 1878. *Theorie der algebraischen Gleichungen*. Kopenhagen: Höst u. Sohn.
- Skolem, Th. 1922. Bericht über die nachgelassenen Schriften L. Sylows. *Videnskabs-selskabet i Kristiania*. Matematisk-Naturvidenskapelig Klasse. Skrifter No. 18. Kristiania.
- Sylow, L. 1867. Om Systemer af konjugerede Substitutioner. . . . *Videnskabs-selskabet i Kristiania Forhandlinger*, 105–122.
- 1872. Théorèmes sur les groupes de substitutions. *Mathematische Annalen* **5**, 584–594.
- 1888. Sur les groupes transitifs dont le degré est le carré d'un nombre premier. *Acta mathematica* **11**, 201–256.
- Waterhouse, W. 1980. The early proofs of Sylow's theorem. *Archive for History of Exact Sciences* **21**, 279–290.
- Wußing, H. 1969. *Die Genesis des abstrakten Gruppenbegriffs*. Berlin: VEB Deutscher Verlag der Wissenschaften. Amerikanische Übersetzung: *The Genesis of the Abstract Group Concept*, Abe Shenitzer, translator, with the editorial assistance of Hardy Grant. Cambridge, MA/London: MIT Press, 1984.

<https://zbmath.org/0637.01006>

Scharlau, Winfried

The discovery of the Sylow theorems. (Die Entdeckung der Sylow-Sätze.) (German) Zbl 0637.01006

Hist. Math. **15**, No. 1, 40-52 (1988).

The author notes the discovery of Dieudonné that Galois had asserted the essence of the Sylow theorems in a marginal note. According to the author, it was Dedekind who took up the challenge in Galois' legacy. The basis of the author's thesis is that there were no essential barricades to the development of an abstract group theory after 1850, that Cauchy's theorem pointed in the direction of a classification of finite groups which would necessarily lead to the Sylow theorems; and that Dedekind, knowing that a p -group has a non-trivial center, could have deduced the solvability of p -groups directly.

The author traces the route followed by Sylow from his studies, while a student of Bjerknes, of Abel's incomplete works on algebraic equations, through his first publication (in 1867) of a theorem intermediate between that of Galois and the full Sylow theorems, to a letter of 19 September 1870, in which he indicates that he is in possession of the full theorem, though he applies it only for $p = 2$ and gives no proof. Sylow's statement of the theorem is in terms of Galois groups rather than abstract groups, for reasons the author makes clear in the subsequent section.

Reviewer: Roger L. Cooke (Burlington)

https://mathscinet.ams.org/mathscinet/relay-station?mr=0931678

 Home Resources Reviewers Free Tools Support Help Pages

American Mathematical Society

MR0931678 (89f:01041)

Scharlau, Winfried
Die Entdeckung der Sylow-Sätze. [The discovery of the Sylow theorems]
Historia Math. **15** (1988), no. 1, 40–52.

Classifications
01A55 - History of mathematics in the 19th century
20-03 - History of group theory

 Article

89f:01041 01A55 20-03

Scharlau, Winfried (D-MUNS)

Die Entdeckung der Sylow-Sätze. (English and French summaries)
[The discovery of the Sylow theorems]

Historia Math. **15** (1988), no. 1, 40–52.

The author evokes primarily the works of Sylow that antedate 1872—the date of the first publication of Sylow's famous theorems—and proposes to provide answers to the following questions: How did Sylow arrive at the formulation of his theorems, what were the mathematical techniques at his disposal, what was the influence of his contemporaries, and what hopes did Sylow have for his work?

The author points out that this article may be considered to be a complement to a paper by W. Waterhouse [Arch. Hist. Exact Sci. **21** (1979/80), no. 3, 279–290; MR 82i:01034].

Sylow undertook his research at a time when the works of Galois were already very widely known, and the author shows us to what extent Galois's legacy had a determining influence on Sylow's thinking, which would lead him from the theory of algebraic equations to the formulation of his renowned theorems (derived from his research on the subgroups of permutation groups).

Relying also on Sylow's correspondence with some of his illustrious contemporaries (Petersen, Jordan), the author underlines the fact that abstract group theory was implicit in the works of most mathematicians of that era who had an interest in groups, even if they actually did not feel the need to make a distinction among abstract groups, permutation groups and Galois groups.

Jean-Luc Steffan (Strasbourg)

The Discovery of the Sylow Theorems

HISTORIA MATHEMATICA 15 (1988), 40–52

The Discovery of the Sylow Theorems

WINFRIED SCHARLAU

Mathematical Institute of the University of Münster, Einsteinstr. 62, D-4400 Münster, Germany

DEDICATED TO MR. H. WUSSING ON HIS SIXTIETH BIRTHDAY, OCTOBER 15, 1987

The paper describes Sylow's discovery of the theorems named after him. He was led to this discovery by his study of Galois' work, in particular Galois' criterion for the solvability of equations of prime degree. It is explained how Sylow used methods from Galois theory in his proofs. The paper also discusses relevant correspondence between Sylow, Jordan, and Petersen. © 1988 Academic Press, Inc.

Diese Arbeit behandelt Sylows Entdeckung der Sätze, die nach ihm benannt sind. Er gelangte zu ihnen durch seine Beschäftigung mit Galois' Arbeiten über die Auflösbarkeit von Gleichungen vom Primzahlgrad. Es wird beschrieben, wie Sylow im Beweis seiner Sätze Methoden aus der Galois-Theorie benutzt. Es wird weiterhin auf die diesbezügliche Korrespondenz zwischen Sylow, Jordan und Petersen eingegangen. © 1988 Academic Press, Inc.

Cet article traite de la découverte par Sylow du théorème qui porte depuis son nom. Il a trouvé ce théorème en étudiant les travaux de Galois sur la résolubilité des équations dont le degré est un nombre premier. On y indique comment Sylow utilise dans sa démonstration les méthodes de la théorie de Galois. De plus, on étudie dans cet article la correspondance à ce propos entre Sylow, Jordan et Petersen. © 1988 Academic Press, Inc.

AMS 1980 subject classification: 01A55.

KEY WORDS: Ludvig Sylow, Sylow theorems, Galois theory, group theory.

1. INTRODUCTION AND SUMMARY

This paper deals with the discovery of the Sylow theorems, which occurred around 1870. It thus addresses an important event in the early history of group theory and directly follows a paper by Waterhouse [1980]. For a concise yet highly succinct presentation of the history of group theory during the period under consideration, highlighting the essential points, see Dieudonné [1978, Chapter 3.4.1], for an exceptionally thorough discussion of many details and interrelationships, see the well-known book by Wussing [1969].

Because it can be done in just a few lines (rare enough for a historical topic), let us first recall the statements of the Sylow theorems: Let G be a finite group of order $n = p^k m$, where p is a prime number and m is not a multiple of p . Then G contains a subgroup P of order p^k (a p -Sylow group). Any two such subgroups P_1, P_2 are conjugate, i.e., there exists a $g \in G$ such that $P_2 = gP_1g^{-1}$. The number of p -Sylow groups is, on the one hand, a divisor of n , and on the other hand, of the form $pk + 1$. Finally, every group P of order p^k is solvable; more precisely, there exists a sequence of normal subgroups $P_1 \subseteq \dots \subseteq P_k = P$ such that $|P_i| = p^i$.

0315-0860/88 \$3.00

Copyright © 1988 by Academic Press, Inc.
All rights of reproduction in any form reserved.

The central importance of these—perhaps seemingly technical and abstract—theorems for the theory of finite groups cannot be explained here. It must suffice to state that they lay the foundation for the entire structural theory of finite groups [1]. Their fundamental importance was also immediately recognised by the leading group theorist of the previous century, C. Jordan (1838–1922). In [Jordan 1873, 40], a paper containing initial applications, he writes:

Cette proposition mérite assurément par sa simplicité, sa netteté et sa généralité, d'être considérée comme fondamentale; et nous ne doutons pas qu'elle ne donne lieu à d'importantes conséquences.

Jordan never had to revise this judgment; in July 1907 he wrote to the now 75-year-old L. Sylow (1832–1918), now looking back on almost forty years of personal and scientific acquaintance:

Vous me parlez à la fin de votre lettre des nombreux travaux dont la théorie des groupes a fait l'objet dans ces derniers temps: ... Et ces travaux devraient vous plaire, n'étant que le développement naturel de vos beaux théorèmes, dont j'ai été le premier, et je me trompe à prédire l'importance future. Ils m'ont inspiré à votre égard une amitié intellectuelle qui m'a fait me réjouir à la vue de votre écriture. [2]

The history of a mathematical theory is above all the history of that theory's central theorems and profound results. Accordingly, the Sylow theorems deserve special attention within the framework of a more general history of group theory. It is to Waterhouse's credit [1980] that such an investigation was first presented, to which little can be added in terms of mathematical substance and which, above all, contains a comprehensive presentation of various—now partly almost forgotten—proof variants. This note—which can be seen as a supplement to Waterhouse's work—is more concerned with the historical aspect of the discovery of the Sylow theorems. While Waterhouse deals with the period after the first publication of Sylow's theorems in 1872, our focus is primarily on the period before 1872. We will investigate how Sylow arrived at the problem posed by his theorems, what tools and methods were available to him, whether and, if so, what suggestions he received from contemporaries, how he himself assessed his theorems, what hopes and expectations he associated with them, and how they might be integrated into a broader “research program”.

These questions cannot all be answered completely and unambiguously, but the following can nevertheless be established:

1. Sylow quite obviously arrived at group theory from the theory of algebraic equations and Galois theory, and not—as would also be conceivable—from a more abstract theory of permutation groups in the sense of Cauchy (1789–1857). Moreover, for him group theory was still practically a part of Galois theory, in a sense applied Galois theory, and he used Galois-theoretical constructions and inferences in places that were later treated purely from a group-theoretical perspective. He derived his first two main theorems (existence, number, and conjugation of p -Sylow groups) directly from a result by Galois (1811–1832), initially in a very specific case (namely, p -Sylow groups of a subgroup of S_p) and subsequently generalized them. Cauchy's well-known theorem (existence of an element of order p in a group with order divisible by p), which is also used in the proof, may have played a role in this generalisation [Cauchy 1845].

2. Although Sylow arrived at the discovery of his theorems entirely independently of other authors, group theory had reached a stage of development at that time where structural questions of this kind were obvious and the time was ripe for the discovery of Sylow's theorems. Even in manuscripts by Galois and Dedekind (1831–1916), which remained unpublished for a long time, partial statements of Sylow's theorems can be found. Furthermore, around the same time as Sylow, the Danish mathematician J. Petersen (1839–1910) [3] encountered the problem of the solvability of 2-groups in connection with construction problems. A correspondence between Sylow and Petersen on this topic exists from the years 1870/71.

3. Although—as just mentioned—the time had come for the investigation of the internal structure of finite groups, these problems did not immediately move to the center of interest of group theorists. The truly central problem of group theory throughout the 19th century, since Cauchy and Galois, was the classification problem, or, more precisely and meaningfully, the problem of classifying transitive permutation groups. From the outset, it seemed obvious to

proceed according to order, degree and degree of transitivity. Significant contributions came primarily from Jordan [1961] and E. Mathieu (1835–1890) [4]. As is evident from his papers and correspondence with Jordan, this problem was also of paramount interest to Sylow. He may have come across Sylow's theorems rather incidentally. He attempted to apply them immediately to this problem, and his letters reveal a certain disappointment that they did not prove of decisive use in addressing the classification problem.

2. GALOIS' LEGACY

Our current (textbook) literature suggests a somewhat inaccurate picture, as one might get the impression that Galois's main achievement was discovering what we now call Galois theory. This is only partially true: a key aspect of Galois theory, namely the importance of groups for the treatment of algebraic equations, was already known in principle. In particular, J. L. Lagrange (1736–1813) had already addressed the "Fundamental Theorem of Galois Theory" in his major work on this topic. Lagrange came very close to the fundamental theorem of Galois theory—not only in the "generic case" of indeterminate coefficients of the algebraic equation under consideration, but in general [Lagrange 1770/71, especially Article 104]. He had also recognized the fundamental importance of group theory for this problem. Perhaps it would be going too far to claim that Lagrange already knew the fundamental theorem of Galois theory, but he undoubtedly had clear and correct ideas about the direction in which the theory of algebraic equations should be developed [5]. Galois's real achievement lies in the fact that he goes far beyond "abstract Galois theory" and, prompted by the problem of solving algebraic equations by radicals, begins a thorough investigation of the structure of finite groups. To this end—and this is certainly one of his most impressive ideas—he invents the theory of finite fields, namely, to obtain solvability statements by representing the group in a suitable linear group over a finite field. At once, a wide spectrum of group-theoretical problems and concepts is addressed: the investigation of the internal structure of finite groups, the problem of determining solvable groups, the description of groups as linear groups over finite fields and thus a first idea of a general theory of representation, somewhat more specifically and concretely then the determination of the solvable subgroups of affine or projective linear groups, and, because Galois groups operate as transitive permutation groups, the investigation of transitive groups with respect to order, degree and degree of transitivity. In this area, Galois arrived at results practically without predecessors and out of thin air, results which Bourbaki [1971, 70] could still say a hundred years later were "among the most insightful in the theory." Galois himself emphasised the significance and scope of these connections when he wrote:

C'est surtout dans la théorie des permutations, où l'on a sans cesse besoin de varier la forme des indices, que la considération des racines imaginaires des congruences paraît indispensable. Elle donne un moyen simple et facile de reconnaître dans quel cas une équation primitive est soluble par radicaux, comme je vais essayer d'en donner en deux mots une idée. [Galois 1962, 125]

One of Galois's most remarkable individual results was his criterion for the solvability of irreducible equations of prime degree, which could be formulated purely in terms of equation theory (in modern terms: $p(x) = 0$ is solvable by radicals if and only if the splitting field is generated by any two roots). Compare the remark:

Pour qu'une équation irréductible de degré premier soit soluble par radicaux, il faut et il suffit que deux quelconques des racines étant connus, les autres s'en déduisent rationnellement. [Galois 1962, 69]

As is well known, Galois neither had the time nor took the time to carry out his algebraic and group-theoretical program. However, there can be no doubt that he knew more than what he revealed in his writings or even in his publications. It is thus hardly surprising that he apparently knew the essential part of the Sylow theorems, as can be seen from an unpublished marginal note, which was probably first pointed out by Dieudonné [1978, 117]. It reads there [Galois 1962, 72]:

Théorème. Si le nombre des permutations d'un groupe est divisible par p (p étant premier), le groupe aura pour diviseur un groupe de p permutations.

It is pointless to speculate whether Galois actually proved this theorem or merely guessed at it. He certainly had the skills and means to prove it. On the other hand, it must be considered that the theorem, as it is formulated, almost implies the solvability of the p -groups. Since his main goal was precisely resolvability criteria, it would have been natural to mention him in this context as well.

It has been stated above that Galois' work must have posed a challenge for every mathematician of that generation. One who accepted this challenge (in investigations later set aside) was Dedekind [1932; 1981]. It is not necessary to elaborate on this further. Regarding group theory, only three observations should be made: 1) For a mathematician of Dedekind's caliber, there were no longer any fundamental difficulties around the middle of the century in conceiving an abstract group theory and beginning to develop it; 2) One of the first problems that arose was the classification problem [Dedekind 1932, 439; Cayley 1878]; 3) Starting from Cauchy's theorem already mentioned, an investigation of the internal structure of finite groups always seems to lead in the direction of the Sylow theorems: Dedekind shows that a p -group has a non-trivial center; since he knew the concept of the factor group, he could easily have deduced the solvability of p -groups from this [6, 7].

In general, it can be observed that Galois theory became known quite quickly in the 1850s and 1860s; a large number of mathematicians in various countries worked on it, including lesser-known ones or those working in remote locations, such as Sylow himself or Petersen, already mentioned.

3. SYLOW'S PATH TO THE SYLOW THEOREMS

From the existing literature and some of Sylow's lesser-known works, his papers, and his correspondence, it is possible to reconstruct when and how Sylow arrived at his group-theoretical investigations. We rely primarily on the curriculum vitae written by Kragemo [1933], on Sylow's own works [1867] and [1872], and on the correspondence with Jordan and Petersen found in his estate [8].

From Kragemo we learn first that Sylow had already been studying the theory of equations during his teacher training, and that from about 1856 onward, encouraged by his teacher C. A. Bjerknes (1825–1903), he intensively studied Abel's (1802–1829) partly fragmentary investigations on algebraic equations. Independently of Kronecker (1823–1891), he succeeded in completing a fragment by Abel. In 1860, he submitted this work to Crelle's Journal; however, it was rejected by Kronecker. In 1861, he received a scholarship and traveled to Berlin, Leipzig, and Paris "to make the acquaintance of the most important mathematicians and to study the theory of equations and the theory of groups." At this time at the latest, he must also have begun to study Galois more intensively, whose work had become widely known in Serret's *Cours d'algebre supérieure*. As early as spring 1863, Sylow gave a lecture on Galois theory, which was attended by Lie (1842–1899).

A few years later, he published his first independent work [Sylow 1867] on group theory, which, in essence, lies precisely between Galois's aforementioned work on irreducible equations of prime degree and his own later work on the Sylow theorems. In this work, Sylow proves the statements of the Sylow theorems in the special case of a subgroup of the symmetric group S_n of prime degree n for this prime number n . The starting point of this investigation was evidently the obvious question of the possible orders of the group of an irreducible equation of prime degree. He writes this order in the form $n(np + 1)v$ (where v is the index of an n -Sylow group in its normaliser and $np + 1$ is the index of this normaliser); it is worth emphasising that he uses precisely these notations in his later work as well. This strongly suggests that the famous work of 1872 arose directly from these investigations.

This is confirmed by the correspondence with Petersen, who was working on his dissertation on constructions with compass and straightedge at the end of the 1860s. He was attempting to solve the central question in this context which algebraic equations must be satisfied by the coordinates of constructible points? He had already arrived at the correct conjecture, the group-theoretical core of which states that the Galois group must be a 2-group. However, since he could not completely solve the problem, he wrote to Sylow on July 19, 1870, asking whether Galois had said anything about this question. Sylow replied in a letter dated September 17, 1870, stating, among other things, the following [9]:

Aus Ihrem Brief schließe ich, daß es nur einen Punkt gibt (nämlich 5) für welchen Ihnen der Beweis noch fehlt. Ich glaube, hierüber versichern zu können, daß es sich wirklich so verhält, wie Sie vermuten. Wenn sich eine irreduzible algebraische Gleichung vom Grad 2^n mit Quadratwurzelzeichen auflösen läßt, dann kann jede Wurzel durch n Quadratwurzeln rational ausgedrückt werden, so daß jede Kombination der Vorzeichen dieser Wurzeln eine neue Wurzel der Gleichung gibt. Ausgehend von einem Satz der Substitutionentheorie, den ich schon längere Zeit gekannt, aber noch nicht veröffentlicht habe, bin ich imstande, dies zu beweisen. Ich habe in diesem Winter den ersten Entwurf einer Abhandlung, wo dieser Satz unter anderen bewiesen werden soll, ausgearbeitet. Da ich aber während der letzten zwei Jahre die ausländischen Zeitschriften nicht ordentlich verfolgt habe, habe ich sie zur Seite gelegt, weil ich erst feststellen will, ob jemand anders in der letzten Zeit dieselben Dinge bewiesen hat. Hiermit bin ich jetzt beschäftigt, und wenn ich nach Frederikshald zurückkomme, wird es vermutlich meine erste Arbeit sein, diese Abhandlung fertig zu machen. Wenn ich von den Resultaten dieser Abhandlung ausgehen kann, wird der Beweis für Punkt 5) in Ihrem Brief einfach sein. Es wird ein Spezialfall eines allgemeinen Theorems über Gleichungen vom Grad p^n sein, deren Auflösung auf die sukzessive Lösung von n "abelschen" Gleichungen vom Grad p reduziert werden kann.

Sylow does not express himself completely unambiguously about the theorems he discovered, either here or in subsequent letters; however, it sounds very much as if he had already known and proven the Sylow theorems for some time at this point. He also gives no indication of a proof method and, in particular, leaves it to Petersen to work out the case $p = 2$ himself. In his 1872 publication, he refers to Petersen's work without indicating that he had known this theorem earlier and independently of Petersen.

4. GROUP THEORY AS GALOIS THEORY

Sylow undoubtedly arrived at group theory from the theory of algebraic equations and Galois theory. We will now discuss the consequences of this approach and how the proofs of Sylow's theorems should be read in this context. First, it should be noted that all mathematicians of this generation were apparently familiar with the fact that every permutation group can be realized as a Galois group, and that one can therefore restrict oneself to Galois groups when investigating arbitrary groups [10]. A particularly impressive piece of evidence for this can be found in an algebra textbook from this period, written by Petersen, whom we have already mentioned several times [11]. There it states [Petersen 1878, 325]:

Der obenstehende Beweis zeigt, dass keine anderen transitiven Gruppen von der Ordnung p^n ($n > 1$) existieren als imprimitive. Der Beweis setzt freilich voraus, daß es eine Gleichung giebt, welche die gegebene Gruppe hat. Indessen entspricht jeder Gruppe eine Gleichung, nämlich die allgemeine Gleichung vom Grade der Gruppe, wenn man dieser eine Function der Wurzeln, die durch die Substitutionen der Gruppe und nicht durch andere Substitutionen unverändert bleibt, adjungiert denkt.

Even today, one could hardly treat the usual construction of a group as a Galois group more concisely and laconically, and one can assume that this line of reasoning was generally known if it was described so succinctly. Sylow [1867] also writes at the beginning of his aforementioned work, without further elaboration:

Auf der anderen Seite kann man auch beweisen, daß zu jedem gegebenen System von konjugierten Substitutionen [d.h. zu jeder Gruppe] eine entsprechende Gleichung existiert.

As will be explained later, he made implicit use of this fact in his work on the Sylow theorems. Finally, Kronecker went a step further by raising the problem as early as 1853 of which groups could actually be realized as Galois groups via $\mathbb{Q}$, whereby the realizability over a suitable field with indeterminate elements was probably self-evident to him:

Ja, man konnte eigentlich gar nicht wissen, ob ... überhaupt noch irgend welche Gleichungen existiren, welche die gegebenen Auflösbarkeits-Bedingungen erfüllen. Noch weniger konnte man solche Gleichungen bilden. ... [Kronecker 1853, 3]

It is quite amusing to follow how Sylow and also Petersen make use of the realisation of an arbitrary group as a Galois group. If one looks at the modern proofs of the Sylow theorems, a key point is always to specify a suitable operation of the group. From the standpoint of Galois theory, nothing is simpler and more natural than this: the Galois group simply operates on the roots of the equation or the conjugates of some suitable element. In the language of Galois theory, one can also circumvent the abstract group-theoretic construction of the quotient group by a normal subgroup: this is simply the Galois group of the corresponding normal field. Similarly, one does not need cosets by a subgroup; these are also replaced by conjugates of a suitable field element. After these preliminary remarks, the proof of Sylow's first theorem then reads quite naturally as follows [cf. Waterhouse 1980]: Let G be the Galois group of the field extension L/K , furthermore P a maximal subgroup of p -power order, N its normaliser, and F the fixed field of N . Because of the maximality of P , N/P contains no elements of p -power order, and by Cauchy's theorem, N/P is coprime to p . Now let $x = x_1$ be a primitive element of N with conjugates $x_2, \dots, x_h$. We consider the operation of P on the x_i . Trivially, x_1 is fixed. However, this cannot hold for any other $x_i = gx_1$, $g \in G$, because from $Pgx_1 = gx_1$ follows that $g^{-1}Pg x_1 = x_1$ whence $g^{-1}Pg \subset N$. Then, however, even $g^{-1}Pg = P$ holds, since all elements of p -power order of N are already in P . It follows that $g \in N$, so $x_i = x_1$. The set $\{x_1, \dots, x_h\}$ thus splits under the operation of the p -group P into orbits, of which only one is a singleton. It follows that $h \equiv 1 \pmod{p}$ and therefore the first Sylow theorem.

Petersen proceeds in a very similar way in his textbook when proving the solvability of p -groups. As we saw in the quotation above, he also explicitly emphasises this approach. This results in a somewhat different statement and a different proof than is customary today for this theorem; his actual concern is a theorem about the solution of algebraic equations, which he formulates as follows:

Die nothwendige und ausreichende Bedingung dafür, daß eine Gleichung mit Hülfe von Abelschen Gleichungen p^{ten} Grades aufgelöst werden kann, besteht darin, daß die Ordnung ihrer Gruppe eine Potenz von p ist. Ihr Grad ist dann auch eine Potenz von p .

In modern terminology, Petersen proves the following: If G is a p -group and H a subgroup, then there exists a sequence of subgroups $G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_k = H$, such that H_{i+1} is normal to the index p in H_i . His Galois-theoretical proof proceeds in modern terms as follows: Let G be the Galois group of L/K and F be the fixed field of H with a primitive element x . We consider the operation of H on the conjugates of x . Since x is fixed, at least $(p - 1)$ conjugates $x_2, \dots, x_p$ must also be fixed, and thus lie in F . There exists a $\sigma \in G$ such that $\sigma x_1 = x_2$, i.e., $\sigma F = F$. Therefore, σ is a non-trivial automorphism of F , say of order p^r . Let F_1 be the fixed field of $\sigma^{p^{r-1}}$ and $H_1 \supset H$ the corresponding Galois group. This procedure is then continued.

It is interesting to take a look at Sylow's own proof of this theorem for comparison: In its first and essential part, it is exactly the one still in use today; G operates on itself by conjugation, and it is found that the center is non-trivial. Because he does not know or does not want to use the concept of the factor group, Sylow subsequently returns to his Galois-theoretical approach to complete the induction.

With these examples, it should have become sufficiently clear how closely group theory was still related to the period under consideration. Galois theory and how the aforementioned mathematicians proceeded from questions of equational theory. However, one point in this context should be addressed further, namely the essential role that the primitive element theorem played in the proofs discussed. Sylow uses it in the following form: If H is a subgroup of the full permutation group of m indeterminates, then there exists a rational function in these indeterminates that remains invariant precisely under the substitutions from H .

This function is thus a primitive element of the fixed field of H (conceived as operating on the rational function field in the m indeterminates) over the field of symmetric functions. It deserves emphasis that this theorem (or closely related ones) was one of the key points in the construction of Galois theory; indeed, it is closely related to the fundamental theorem of Galois theory. It played an essential role for Galois himself [Galois 1962, 47 ff.] as well as in later presentations of the Galois theory [Dedekind 1981, 81]. In this respect, it was used by Sylow (and also Petersen) as a matter of course [12].

5. GROUP THEORY IN THE GENERATION AFTER GALOIS

It would go beyond the scope of this essay to attempt a complete account of the main developmental trends in group theory after Galois. It will only be addressed to the extent necessary to demonstrate how Sylow's work fits into these trends. Overall, a picture of remarkable uniformity emerges. Both Cauchy's theory of permutation groups and Galois theory (which enriched abstract group theory with concepts such as normal subgroups, factor groups, solvable groups, etc.) naturally lead to the study of (transitive) group operations. This problem, as already emphasized in the introduction, is (along with the study of linear groups) clearly at the forefront of interest.

In my opinion, it is inappropriate to overemphasize the contrast between abstract group theory and the theory of permutation groups during this period. Rather, it seems that the concept of an abstract group theory was quite present for mathematicians of this generation and formed the (often unspoken) background of their work. At least Cayley [1878] and Dedekind [1981] had already explicitly conceived of an abstract group theory in the 1850s. In this context, both also posed the problem of classifying all (finite) groups as a central question. On the other hand, Cayley's theorem that every abstract group can be realized as a permutation group is such a triviality that it was surely as widely known as the identity of the terms permutation group and Galois group. Thus, for the group theorists of this time—especially insofar as they were interested in concrete advances in this theory and not, like Dedekind, in abstract algebra—there was hardly any reason to sharply distinguish between abstract groups, permutation groups, and Galois groups. Finally, from a purely mathematical standpoint, the investigation of permutation groups is more obvious and promising than abstract group theory. If one poses, for example, the obvious problem of determining multiply transitive groups, as Mathieu and Jordan did, one soon arrives at profound results and difficult problems that remain unsolved even today.

All available documents clearly show that questions of this kind occupied Sylow throughout his life and shaped his mathematical work. It has already been explained how, following Galois, he posed the question of the subgroups of S_p and how he thereby arrived at his theorems. In the same work of 1872, he attempts to apply these theorems to problems concerning transitive group operations, generalizing results from Mathieu [Sylow 1872, Théorème VI, VII and VIII]. At this time he wrote to Jordan about his future intentions:

Je me suis proposé le problème de trouver toutes les groupes de degré n et d'ordre $(n+1)n^v$, mais je n'ai encore pu le résoudre.... L'insuffisance des mes efforts pour résoudre ce problème ayant un peu rebaisé l'opinion que je m'étais d'abord formée sur l'utilité de mon théorème.... Quand vous me honorez d'une seconde lettre, je vous prie Monsieur de vouloir bien me dire si l'on a fait l'énumération des groupes transitifs pour des degrés plus grands de 7, et où cela est imprimé. ... (lettre of août 20, 1872)

Je vais maintenant m'occuper du nombre p dans l'égalité $0 = n^v(np+1)$ et de la forme des groupes d'ordre n^v (lettre of décembre 6, 1872)

Dans le temps évalée depuis ma dernière lettre je me suis principalement occupé des groupes d'ordre n^v , en me bornant pour le moment aux groupes transitifs. ... (lettre of février 8, 1873)

Jordan, for his part, immediately after learning of Sylow's theorems during his visit to Christiania (Oslo), applies them—entirely in keeping with the described “research program”—

to obtain estimates for the highest possible degree of transitivity of a permutation group. He had already dealt with investigations of this problem earlier in several notes [Jordan 1961]. This question is the main subject of his letters to Sylow from this period; he publishes these results in [1873] and emphasizes in the His letters to Sylow from this period primarily revolve around this question; he published these results in [1873] and, in the introduction, emphasized the significance of Sylow's findings (see the quotation in Section 1).

Sylow himself published only one more major work on group theory [1888], which was likely written much earlier and directly follows previous investigations by Galois, Jordan, and himself. While he had investigated transitive groups of degree p in his work [1867], this work deals with transitive groups of degree p^2 . In this case, he largely determines the structure of the possible p -Sylow groups, their normalizers, and the possible orders of these groups. Galois and Jordan had studied solvable groups of this kind, about which Galois had formulated a conjecture that was subsequently corrected, completed, and proven by Jordan. Sylow thus extended these investigations to non-solvable groups. His unpublished papers [cf. Skolem 1922] reveal that he also intensively studied higher degrees, particularly the case of p^3 , but also composite degrees such as $2p$. However, he never achieved any conclusive results or published his work.

Sylow worked as a secondary school teacher in the remote town of Frederikshald, far removed from any centers of mathematical activity, and he often complained in his letters about his complete isolation. Probably for this reason, and also due to other time-consuming commitments (editing Abel's works and co-editing *Acta Mathematica*), he published only one groundbreaking work. His true originality and mathematical power are therefore difficult to assess. In his work on group and Galois theory, he certainly addressed central problems. His achievement lies in having discovered one of the main results of the structure theory of finite groups, even if this discovery at that time seemed almost a historical necessity.

FOOTNOTES

1. For example, Huppert's comprehensive handbook [1967, 35] states: The Theorems 7.3 to 7.6 [these are the Sylow theorems] are of fundamental importance for the theory of finite groups. We will use them again and again, and a considerable part of our work will be the search for extensions of these theorems.

2. Jordan's letters to Sylow are kept with Sylow's estate in the Oslo University Library. I thank T. Gulliksen for providing photocopies and the University Library for permission to publish excerpts.

3. J. Petersen was evidently a skilled and knowledgeable mathematician who authored a number of excellent textbooks. A scholarly biography of him, describing his relationships with other mathematicians and shedding some light on the state of mathematical development in the Scandinavian countries, would be desirable.

4. In line with the thesis that the historiography of a mathematical theory should primarily focus on its profound results, an investigation into Mathieu's remarkable work, especially his discovery of the simple groups named after him, would be highly desirable. Here we see a foreshadowing of a development that only became truly relevant almost 100 years later.

5. Lagrange [1770/71, 4031] states: "Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire; tout se réduit, comme on voit, à une espèce de calcul de combinaisons, par lequel on trouve à priori les résultats auxquels on doit s'attendre."

6. Galois, Dedekind, and Sylow all first mention Cauchy's theorem in connection with Sylow's theorems.

7. Dedekind's group-theoretical studies are not mentioned in Wußing's fundamental study [1969]; also the problem area discussed here is only treated as an orphan. Overall, several corrections to the picture painted by Wußing seem necessary: 1.) The idea of an abstract group theory appears to have been quite present in the minds of group theorists long before it was explicitly formulated, and it helped them to bring order and structure to their investigations. 2.) At least the theory of finite groups likely did, in fact, develop predominantly from Galois theory. A detailed discussion is not possible here.

8. The Petersen-Sylow correspondence is kept at the University of Oslo; see footnote 2. Sylow's letters to Jordan are located in the Bibliothèque centrale de l'école polytechnique in Palaiseau. I thank Ms. Cl. Billoux for her kind assistance in obtaining the letters.

9. I thank J. Høyrup for his help in deciphering and translating these letters.

10. In this context, it is probably rather irrelevant whether and to what extent the abstract concept of groups and the representation of abstract groups as permutation groups were known.

11. This book, whose Danish original edition appeared a year earlier, is a remarkably clear, understandable, and complete textbook of algebra, far superior to Serret's and probably one of the best before Weber's *Algebra*. It deserves to be better known.

12. In this context, I think that Waterhouse [1980, 280] expresses himself somewhat misleadingly when he writes:

But historically more interesting (and making the proof much harder to read) is the fact that Sylow does not explicitly have the concept of action on cosets. What appears in its place is a theorem of Cauchy which is hardly remembered now: If H is any group of substitutions of n variables, then there is a function of those variables left invariant by the substitutions in H and by no other substitutions.

Essentially it's simply a matter of the primitive element theorem!

LITERATURE

- Bourbaki, N. 1965.** *Eléments d'histoire des mathématiques*. Paris: Hermann. Deutsche Übersetzung: *Elemente der Mathematikgeschichte*. Göttingen: Vandenhoeck u. Ruprecht, 1971.
- Cauchy, A. L. 1845.** Mémoire sur diverses propriétés remarquables des substitutions régulières ou irrégulières et des systèmes de substitutions conjuguées. *Comptes Rendus hebdomadaires des Séances de l'Académie des Sciences* **21**, 835-852, 895-902, 931-933, 972-987, 1025-1041. Zitiert wird nach: *Oeuvres*, I^{re} Série, vol. 9, 342-358. Paris: Gauthier-Villars, 1896.
- Cayley, A. 1878.** Desiderata and suggestions. *American Journal of Mathematics* **1**, 50-52. Abgedruckt in: *Mathematical Papers*, vol. 10, pp. 401-403. Cambridge: The University Press, 1896.
- Dedekind, R. 1932.** Aus den Gruppen-Studien (1855-1858). In *Gesammelte Mathematische Werke*, R. Fricke, E. Noether, O. Ore, Hrsgg., vol. 3, pp. 439-446. Braunschweig: Vieweg.
- **1981.** Eine Vorlesung über Algebra. In *Richard Dedekind 1831/1981*, W. Scharlau, Hrsg. Braunschweig/Wiesbaden: Vieweg.
- Dieudonné, J. (Hrsg.) 1978.** *Abrégé d'histoire des mathématiques 1700-1900*. Paris: Hermann.
- Deutsche Übersetzung: *Geschichte der Mathematik 1700-1900*. Braunschweig/Wiesbaden: Vieweg, 1985.
- Galois, E. 1962.** *Ecrits et mémoires mathématiques*, R. Bourgne und J. P. Azra, Hrsgg. Paris: Gauthier-Villars.
- Huppert, B. 1967.** *Endliche Gruppen*, vol. 1. Berlin/Heidelberg/New York: Springer.
- Jordan, C. 1873.** Sur la limite de transitivité des groupes non alternés. *Bulletin de la Société mathématique de France* **1**, 40-71.
- Wieder abgedruckt in: *Oeuvres*, J. Dieudonné, Hrsg., vol. 1, pp. 365-396. Paris: Gauthier-Villars, 1961.
- **1961.** *Oeuvres*, J. Dieudonné, Hrsg., vol. 1. Paris: Gauthier-Villars.
- Kragemo, H. B. 1933.** Ludvig Sylow. *Norsk Matematisk Tidsskrift* **15**, 73-99.
- Kronecker, L. 1853.** Über die algebraisch auflösbaren Gleichungen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin vom Jahre 1853*, 365-374. Wieder abgedruckt in *Werke*, K. Hensel, Hrsg., vol. 4, pp. 3-11. Leipzig/Berlin: Teubner, 1929.
- Lagrange, J. L. 1770/71.** Réflexions sur la résolution algébrique des équations. *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin* **1770**, 134-215 und **1771**, 138-253.
- Zitiert wird nach: *Oeuvres*, vol. 3, pp. 203-421. Paris: Gauthier-Villars, 1869.
- Petersen, J. 1878.** *Theorie der algebraischen Gleichungen*. Kopenhagen: Höst u. Sohn.
- Skolem, Th. 1922.** Bericht über die nachgelassenen Schriften L. Sylows. *Videnskabs-selskabet i Kristiania*. Matematisk-Naturvidenskapelig Klasse. Skrifter No. 18. Kristiania.
- Sylow, L. 1867.** Om Systemer af konjugerede Substitutioner. ... *Videnskabs-selskabet i Kristiania Forhandling*, 105-122.
- **1872.** Théorèmes sur les groupes de substitutions. *Mathematische Annalen* **5**, 584-594.
- **1888.** Sur les groupes transitifs dont le degré est le carré d'un nombre premier. *Acta mathematica* **11**, 201-256.
- Waterhouse, W. 1980.** The early proofs of Sylow's theorem. *Archive for History of Exact Sciences* **21**, 279-290.
- Wußing, H. 1969.** *The genesis of the abstract group concept*. Berlin: VEB Deutscher Verlag der Wissenschaften.
- Amerikanische Übersetzung: *The Genesis of the Abstract Group Concept*, Abe Shenitzer, translator, with the editorial assistance of Hardy Grant. Cambridge, MA/London: MIT Press, 1984.

Copyright © 2026 Felix F. Flemisch

https://encyclopediaofmath.org/wiki/Sylow_theorems

Sylow theorems

Three theorems on maximal p -subgroups in a finite group, proved by L. Sylow [1] and playing a major role in the theory of finite groups. Sometimes the union of all three theorems is called **Sylow's theorem**.

Let G be a finite group of order $p^n s$, where p is a prime number not dividing s . Then the following theorems hold.

Sylow's first theorem: G contains subgroups of order p^i for all $i = 1, \dots, m$; moreover, each subgroup of order p^{i-1} is a normal subgroup in at least one subgroup of order p^i . This theorem implies, in particular, the following important results: there is in G a Sylow subgroup of order p^m ; any p -subgroup of G is contained in some Sylow p -subgroup of order p^m ; the index of a Sylow p -subgroup is not divisible by p ; if $G = P$ is a group of order p^n , then any of its proper subgroups is contained in some maximal subgroup of order p^{n-1} and all maximal subgroups of P are normal.

Sylow's second theorem: All Sylow p -subgroups of a finite group are conjugate.

For infinite groups the analogous result is, in general, false.

Sylow's third theorem: The number of Sylow p -subgroups of a finite group divides the order of the group and is congruent to one modulo p .

For arbitrary sets π of prime numbers, analogous theorems have been obtained only for finite solvable groups (see **Hall subgroup**). For non-solvable groups the situation is different. For example, in the alternating group A_5 of degree 5, for $\pi = \{2, 3\}$ there is a Sylow π -subgroup S of order 6 whose index is divisible by a number from π . In addition, in A_5 there is a Sylow π -subgroup isomorphic to A_4 and not conjugate with S . The number of Sylow π -subgroups in A_5 does not divide the order of A_5 .

References

- [1] L. Sylow, "Théorèmes sur les groupes de substitutions", *Math. Ann.* **5** (1872), pp. 584-594, Zbl 04.0056.02
- [2] M. Hall, "Group theory", Macmillan (1959)

Dedication to Professor Otto H. Kegel

This paper is dedicated to sadly late **Professor Dr. Otto Helmut Kegel** and especially to his contributions to Sylow Theory: see Pages 2 to 9. It is drawing challenging conclusions for future research work from **Otto H. Kegel's** grandiose contributions: see Pages 9 to 11.



It is a great honour to commemorate **Otto H. Kegel** through some photographs:

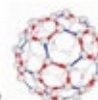


Professor Dr. Otto H. Kegel giving one of his fascinating lectures on Group Theory, e.g. at the MFO (see https://opc.mfo.de/detail?photo_id=23960 and <https://opc.mfo.de/search?term=Kegel>), with an outlook to challenging and very beautiful research topics thereby offering his genuine careful supervision ☺.



Prof. Kegel, wie er lebt und glücklich lebt, auf einem Spaziergang in Freiburg im Breisgau

Prof. Kegel, that's him all over, his happy spotting image, on a cosy stroll in Freiburg im Breisgau



Long live Group Theory and in particular Sylow Theory of Locally Finite Groups!

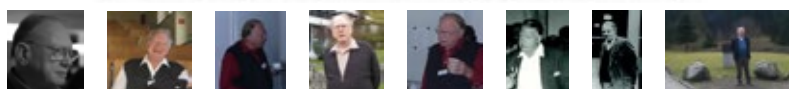


Otto H. Kegel (Ischia, 2016) • courtesy of Nikolay Aleksandrovich Vavilov (see <https://www.advgrouptheory.com/GTArchivum/Pictures/gtphotos/OttoKegel.jpg>)

The Mathematical Institute in Freiburg im Breisgau



This is the **Mathematical Institute** at **Albert-Ludwigs-University in Freiburg im Breisgau** in Germany where from 1975 until 1999 **Prof. Kegel** occupied his chair, gave **beautiful** lectures and seminars, invited researchers over researchers, and hosted students in the morning offering a **cup of coffee** (or two) thereby doing careful supervision work and suggesting fascinating research topics.



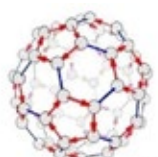
Otto H. Kegel (Mathematisches Forschungsinstitut Oberwolfach (MFO), 2010) • courtesy of Renate Schmid (see https://opc.mfo.de/detail?photo_id=12425)

Table of Contents

Otto H. Kegel's Beloved Contributions to Sylow Theory

In memory of my adored masterly teacher

Abstract	1
Keywords	2
Mathematics Subject Classification (MSC2020)	2
1 Introduction	2
2 Otto H. Kegel's Beloved Contributions	2
2.1 Early Contributions	2
2.1.1 Caractérisation des sous-groupes accessibles d'un groupe fini [13.]	3
2.1.2 Sylow-Gruppen und Subnormalteiler endlicher Gruppen [14.]	3
2.1.3 Eine Charakterisierung der Sylowgruppen endlicher Gruppen [15.]	3
2.1.4 Über einfache, lokal endliche Gruppen [16.]	3
2.1.5 Locally finite versus finite simple groups [17.]	3
2.1.6 Strong finiteness conditions in locally finite groups [18.]	3
2.1.7 Locally finite simple groups [19.]	4
2.1.8 Reinhold Baer (1902-1979). Obituary. [20.]	4
2.1.9 The structure of locally finite groups with $\min-p$ [21.]	4
2.2 "Locally Finite Groups", co-authored with Bertram A.F. Wehrfritz [22.]	4
2.3 Chain conditions and Sylow's theorem in locally finite groups [11.]	5
2.4 Four lectures on Sylow theory in locally finite groups [12.]	5
3 Felix F. Flemisch's Enthusiastic Contributions	5
3.1 Trilogy about Sylow Theory in Locally Finite Groups [1.]	5
3.1.1 Part 1 [1.1]	5
3.1.2 Part 1 – Second edition [1.2]	6
3.1.3 Part 2 [1.3]	6
3.1.4 Part 3 [1.4]	6
3.2 Review of a Trilogy about Sylow Theory in Locally Finite Groups [2.]	7
3.3 Three Beautiful Books about Sylow Theory in Locally Finite Groups [3.]	7
3.4 Characterising locally finite groups satisfying the strong Sylow Theorem for the prime p – Manuscript on Sylow theory in locally finite groups – Mathematics edition [4.]	7
3.5 Characterising Locally Finite Groups Satisfying the Strong Sylow Theorem for the Prime p [5.]	7
3.6 The Strong Sylow Theorem for the Prime p in Simple Locally Finite Groups [6.]	7
3.7 The Strong Sylow Theorem for the Prime p in Simple Locally Finite Groups – De Luxe Edition [7.]	8
3.8 Felix F. Flemisch – Happy Birthday and Gratitude Greetings to Professor Otto H. Kegel (July 17, 2025) [8.]	9
3.9 Professor Otto H. Kegel out of Great Gratitude for Opening a New and Grandiose Dimension of Mathematics to Me [9.]	9
3.10 Otto H. Kegel's Beautiful Contributions to Sylow Theory in Locally Finite Groups [10.]	9
4 Conclusions	9
Acknowledgements	11
References	11
Pablo Picasso – <i>La Joie de vivre</i> which shepherds the Trilogy as a flock along all abysses	13
Ludvig Sylow and William Waterhouse and Winfried Scharlau	14
Om Systemer af konjugerede Substitutioner, der kunne tilhøre irreduktible Ligninger, hvis Grad er Primtal	17
On Systems of Conjugate Substitutions that could belong to irreducible Equations whose Degree is a Prime Number	39
Théorèmes sur les groupes de substitutions	61
The Early Proofs of Sylow's Theorem	81
Die Entdeckung der Sylow-Sätze	98
The Discovery of the Sylow Theorems	125
Dedication to Professor Otto H. Kegel	134
Table of Contents	135



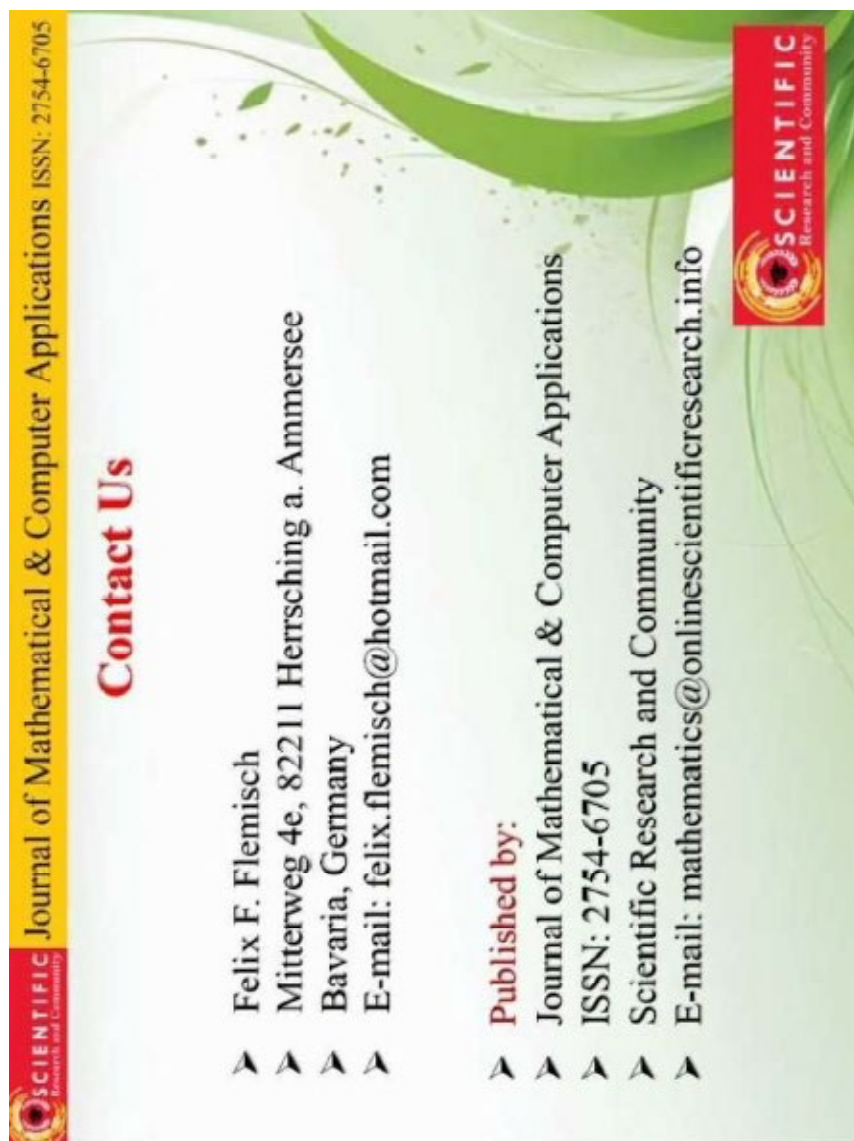
Alternating group A^5



L'amour immortel, éternel et infini



Contact Us: the Author (felix.flemisch@hotmail.com) **and the Journal** (mathematics@onlinescientificresearch.info)



SCIENTIFIC
Research and Community

Journal of Mathematical & Computer Applications ISSN: 2754-6705

Contact Us

- Felix F. Flemisch
- Mitterweg 4e, 82211 Herrsching a. Ammersee
- Bavaria, Germany
- E-mail: felix.flemisch@hotmail.com

Published by:

- Journal of Mathematical & Computer Applications
- ISSN: 2754-6705
- Scientific Research and Community
- E-mail: mathematics@onlinescientificresearch.info

SCIENTIFIC
Research and Community

J Mathe & Comp Appli, 2026 | <https://www.onlinescientificresearch.com/journals/jmca> and <https://www.onlinescientificresearch.com/journals/jmca/archive>