Ludvig Sylow's Lectures on Algebraic Equations and Substitutions, Christiania (Oslo), 1862: An Introduction and a Summary

Bent Birkeland*

Institute of Mathematics, University of Oslo, Postboks 1053, Blindern, N-0316 Oslo, Norway

In 1862–1863 Ludvig Sylow (1832–1918) gave a course on Galois theory at the University of Oslo. His notes for that course have now been published (in Norwegian). They give a good account of their subject as it was seen at that time, and they show that Sylow in 1862 had posed himself the problem which later was to lead him to the famous “Sylow theorems” on the existence of subgroups of a given order in a finite group (published 1872). This course was also the young Sophus Lie’s first introduction to the theory of groups. The present article gives an introduction to Sylow’s notes, and a summary of them in English.

AMS 1991 classification: 01A55, 12F10, 13B05.
KEY WORDS: Sylow, Galois theory, groups, algebraic equations.

THE LECTURES

Galois theory was first presented to a Norwegian audience as early as the academic year 1862–1863, in Oslo (at that time called Christiania). The lecturer was Ludvig Sylow, on leave of absence from his job as teacher in the small city of Halden (then called Frederikshald). In the audience was then 20-year-old Sophus Lie. This must have been his first contact with the theory of groups.

Sylow’s notes for these lectures still exist in the Oslo University Library, and they have recently been edited and published [17]. They give a very legible account

* E-mail: bentb@math.uio.no.
of the central parts of Abel’s and Galois’s theory of algebraic equations. Since Sylow had just returned from a year of studies in Germany and France, they also presumably represent what was then the current view of the theory of equations. Their approach to the theory of algebraic equations is much more direct than the one presented in most modern university courses (except for Harold Edwards’ nice textbook [3]). For these reasons, I think they may be of some interest to students of algebra and to historians of mathematics.

The notes, written in the standard Norwegian of that time, today look very old-fashioned. To make them at least partially accessible to people not familiar with the Norwegian language, I give here a short summary in English and an even shorter introduction.¹

SYLOW’S THEOREMS

It is natural to ask whether these lectures contain any hint of the Sylow Theorems [20] about the existence of subgroups of given orders in a finite group. These were published in 1872, and Jesper Lützen has shown in [11] that Sylow knew them at least two years earlier. Apparently, though, Sylow did not have his famous theorems in 1862–1863. After his proof (in lecture 8) of Cauchy’s theorem that any (finite) group contains cyclic subgroups of any prime order dividing the order of the group, Sylow added the questions: “What if \( m \) is divisible by \( n \)? Can the proof above be extended?” But that is all. He had apparently posed the problem but not yet solved it.

Lützen notes, however, that Sylow’s proofs of his theorems rely heavily on the fact that any (finite) group is the Galois group of an equation (with coefficients from some extension of the rationals), citing the simple proof Sylow gave for this fact in 1868, in [19]. This same proof is found in the present lectures of 1862 at the end of chap. 8.

GALOIS THEORY

As is well known, Évariste Galois presented his ideas on the theory of solvability of algebraic equations to the French Academy of Sciences in three different papers between 1829 and 1831. The first two were lost; the third was returned with a request for clarifications. This rewriting was still unfinished at the time of the duel which ended Galois’ life in May of 1832, and Galois’s works were largely forgotten. It is true that his main results had been stated (without proof) in two short notes in the “Bulletin de Ferrusac” of 1830, but these notes were hard to read and made little impact. Only 14 years later, in 1846, did Joseph Liouville acquaint the mathematical world with Galois’s ideas by publishing a selection of his posthumous

¹ The entire text (78 pages) is available from the Institute of Mathematics, University of Oslo (P.O. Box 1053, Blindern, N-0316 Oslo, Norway). It was the historian Elin Strøm who in the spring of 1994 directed my attention to Sylow’s papers and kindly provided me with copies. I am grateful to her both for this and for useful discussions. I also thank Jesper Lützen for kind and helpful comments, and an anonymous referee for making me aware of Purkert’s paper [14].
papers in the *Journal des mathématiques pures et appliquées*. In preparation for this, he also gave a private seminar on Galois theory, probably in 1843–1844. One of the participants was Joseph Serret, then a student of Liouville.

Even after that, the ideas took some time to catch on. The successive editions of Serret’s influential *Cours d’algèbre supérieure* [16] provide an interesting illustration. In the first edition (1849), Galois theory is mentioned only in passing (p. 4, and in a footnote on p. 344); in the second (1854) Galois’s paper, “Sur la théorie des nombres” [5], is treated in detail (Leçon 25), but his other work is not. It was in the third edition (1866) of the *Cours* that Galois theory for the first time was presented in a major textbook. One reason for the delay was Liouville’s announcement that he was preparing a commentary on Galois’s work; this prevented others from entering the field. Regrettably, that commentary never appeared. A full account of Liouville’s role in the resurrection of Galois theory is found in Lützen’s biography of Liouville [10, 131 and chap. 14].

Lectures on Galois theory came more quickly than printed expositions. According to George A. Miller [13, 321], Serret lectured on Galois theory in Paris as early as 1848. It would be interesting to know the contents of these lectures. Miller claims that the first to give a course in Galois theory in Germany was Richard Dedekind, in Göttingen in 1858 [10, 323]. Walter Purkert’s paper [14] gives more information on these lectures. In Italy, Enrico Betti taught Galois Theory at the University of Pisa in 1859–1861 [10, 323]. Only after Camille Jordan’s great *Traité des substitutions* of 1870 [8] did Galois’s ideas come to occupy the central place in algebra which they deserve.

**LUDVIG SYLOW**

The son of an officer (who later became a member of the government), Ludvig Sylow (1832–1918) was interested in mathematics as early as his schooldays. He graduated from the University of Christiania in 1855, with excellent marks, and then became a schoolteacher, since no university position was available. But he kept up his mathematical studies, at first working on elliptic functions in the tradition of Abel and Jacobi, inspired by the professor in pure mathematics, Ole Jacob Broch. Finding Abel’s papers on the solvability of algebraic equations by radicals more interesting, Sylow was led from them (by the professor in applied mathematics, Carl Anton Bjerknes; see Kragemo [9, 78]) to Galois.

In 1860, at the eighth meeting of Scandinavian scientists in Copenhagen, Sylow presented his reconstruction [18] of the last, highly fragmentary, part of Abel’s unfinished paper [2] on algebraic solvability of equations. It appeared that in 1828 Abel had known considerably more about the possible forms of solutions of such equations than, for instance, Leopold Kronecker, the leading expert on algebraic equations around 1860, had thought. (See the interesting paper [7] by Gårding and Skau (esp. p. 95), as well as Kragemo [9].) This paper marked the beginning of Sylow’s lifelong and very thorough study of Abel’s work, which culminated in the new edition he brought out with Lie of Abel’s *Œuvres*, as well as in the excellent article [21] he wrote in 1902 for the 100th anniversary celebration of Abel’s birth.
In 1861–1862 Sylow had a travel grant for studies in Berlin and Paris. In his report to the ministry afterwards, he recounts that in Paris he heard lectures by Chasles on “higher geometry, in particular the theory of conics” [S], Liouville on rational mechanics, and Duhamel on “la méthode des limites” and its history. In addition, “made [myself] acquainted with newer works, particularly in the theory of equations” [S]. In Berlin he sat in on no courses, since Weierstrass was ill, and the other lectures were of little interest. He worked instead in the library, studying number theory and the theory of equations. He also got acquainted with Carl Borchardt, the editor of Crelle’s Journal, and had useful discussions with Kronecker. It is interesting to note that no lectures in algebra or the theory of equations are mentioned from his stay either in Paris or in Berlin.

The following year, 1862, Broch was elected to the Norwegian National Assembly (Stortinget), and Sylow acted as his substitute at the University. That was the occasion for the lectures discussed here, in which Sylow aimed to explain the main features of Abel’s and Galois’s approach to the theory of algebraic equations, without trying to survey all that was known. In particular, the connections to the division problems in the theory of elliptic functions, which were so important in Abel’s work, are barely mentioned.

Aside from this brief university sojourn, Sylow remained at the Gymnasium in Halden for close to 40 years but kept up his mathematical work. The theorems which are now named after him were published in 1872 [20]. Then he worked for eight years (having leave of absence for four of them) in collaboration with Sophus Lie, to prepare the definitive edition of Abel’s Œuvres, which appeared in 1881 [1]. Lie emphasized that the greater part of the work was done by Sylow. Sylow’s main interest was algebra (theory of groups), but he also wrote about elliptic functions. He was co-editor of the Acta Mathematica, and in 1894 he was made an honorary doctor at the University of Copenhagen. At last, in 1898, when he was 65 years old, an extraordinary professorship was created for him at the urging of Lie. He kept on lecturing with zeal and enthusiasm until the end of his long life. For further biographical information on Sylow, the article [9] by Kragemo probably is the best source.

THE MANUSCRIPT AND ITS TERMINOLOGY

The manuscript is written on 17 large sheets of paper, each folded once, to make four written pages. The sheets are numbered from 1 to 15, with two different sheets 12, and one extra sheet containing material to be inserted at the ends of sheets 5 and 7. In addition there are 11 sheets containing preliminary versions of parts of the lectures, computations for examples, and the like. They have not been reproduced in [17]. The handwriting is small and a bit cramped, but in general quite legible.

The lectures contain no references to the literature. Judging from the text of the lectures, and from Kragemo [9, 78], it seems clear that the main sources Sylow used were the second edition (1854) of Serret’s Cours [16], Galois’s papers [5; 6] in Liouville’s Journal (1846), and, of course, Abel’s collected works (in Holmboe’s edition of 1839). At one point in Lecture 8 the name Schönemann is mentioned;
that probably refers to the paper [15] of Theodor Schönemann. The elimination formulas in chapter 3 are credited to Newton and Waring, but no precise reference is given. Other results are credited to Abel, Galois, and Cauchy, but without precise references. The text on the first seven sheets is divided (by Sylow) into eight chapters, marked by numbers 1–8, but with no other headings. In the whole manuscript Sylow provides only one heading (at the top of sheet 14). I have provided some more, to make it easier to read.

In the summary below, I reproduce the main theorems given in the lectures, while omitting much of the intervening text (proofs, comments, examples). I have tried to use language which is not too different from Sylow's own expressions. Attributions of results to named persons are due to Sylow. Since mathematical language has changed since Sylow wrote these notes, a few remarks on terminology are in order.

The word “group” was introduced into algebra by Galois in 1830, but with a meaning which differed slightly from the modern one. It denoted a subgroup of the group of permutations of the roots of a given polynomial, but in the language of the 1860's, a permutation of the roots is just a list of the roots in a specified order, or, in other terms, an indexing of the set of roots by the integers \( \{0, 1, \ldots, (n - 1)\} \) (or by the residue classes of integers modulo \( n \)). A substitution (“Ombytning” is Sylow's word) is the transition from one permutation to another, or, in modern terms, a transformation of the index set \( \{0, 1, \ldots, (n - 1)\} \) (or of the corresponding equivalence classes modulo \( n \)) onto itself. Thus, substitutions can be composed, permutations cannot. A group, then, in the language of the 1860's, is “a set of permutations, such that any substitution that takes one member of the group to another, takes every member of the group to another member, without introducing alien permutations” [17, 21, my translation].

With this definition, many of the arguments will, of course, take place not in the group itself but in the associated set of substitutions. The construction of equivalence classes modulo a subgroup, however, takes place in the set of permutations. Sylow describes it as a partition of the given group (i.e., set of permutations) into subsets such that every two of these subsets “have the same set of substitutions, but no permutation in common” [17, 30]. The fact that this set of subsets can again be associated with a group in the modern sense of that word is used only indirectly. As is well known, the modern, abstract formulation of the group concept evolved very slowly; a beginning can be seen in work by Cayley in 1854, the completion in Heinrich Weber’s textbook of 1895–1896. (For a good account of this development, see Hans Wussing's book [23].)

The word “field” (“Körper” in German) was used by Dedekind in his lectures of 1858 (see [14, 3]), but it did not come in general use till the early 1890's, with Weber’s work [22]. The expression generally used until then was “rationally known quantities,” which means either the field of rational numbers or some finite extension of it, depending on the context. The process of extending the field of coefficients is referred to as “considering some additional quantity to be known.”

Throughout these lectures, Sylow works in the setting in which one algebraic
equation $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ is given. The problem considered is to clarify the relations between the coefficients $a_0, a_1, \ldots, a_{n-1}$ and the roots $x_0, x_1, \ldots, x_{n-1}$ of that equation, in particular, to find out when the equation is solvable by radicals. The roots are generally considered to be distinct. Sylow refers to this equation as “the equation” or “the given equation,” and to its roots simply as “the roots.”

Before turning to the lectures themselves, it is important to keep in mind the following minor points of terminology. “Equations” are polynomial equations, with “rationally known” coefficients. Polynomials are generally understood to be monic (leading coefficient equal to one). Sylow often speaks about equations where modern readers might find it more natural to speak about polynomials, and he talks about splitting or reduction of the equation where nowadays we would speak about factorisation of the polynomial. The words “function” and “expression” are used synonymously for a rational expression. An “entire function” is a polynomial.

**SUMMARY OF THE LECTURES**

**Chapter 1. Introduction**

- Definition of rational and irrational quantities, algebraic operations and quantities, algebraic equations and functions. Solvability of algebraic equations.
- Every algebraic equation has a root (in the complex numbers). *Proof by calculus.* Write $z = x + iy$, $f(z) = u(x, y) + iv(x, y)$, where $x, y, u, v$ are real, and note that $u^2 + v^2$ has a minimal value for some finite $(x_0, y_0)$. Then show by calculus that this minimal value must be zero. [The existence of a minimum is considered obvious.]
- Hence every polynomial of degree $n > 0$ can be factored (over the complex numbers) into a product of $n$ linear factors.

**Chapter 2. Reducible and Irreducible Equations**

- If an algebraic quantity $x_0$ can be defined by two different equations $F(x) = 0$ and $f(x) = 0$, then it can also be defined by $\phi(x) = 0$, where $\phi$ is the greatest common factor of $F$ and $f$. Hence there is one monic equation of lowest degree which defines $x_0$, and that equation is irreducible.
- When an irreducible equation has one root in common with some other equation with rational coefficients, then it has all its roots in common with that equation.
- Irreducibility of an equation depends on which quantities are considered to be known: the equation $x^2 - 4x + 2 = 0$ is irreducible if only rational numbers are known, but it becomes reducible if $\sqrt{2}$ is known.
- Equations with multiple roots are reducible (because $f(x) = 0$ and $df/dx(x) = 0$ then have a common factor).
- If $n$ is a prime number, then the equation $x^n - a = 0$ is reducible only if $\sqrt[n]{a}$ is rationally known. If $n$ is not a prime, it is reducible only if $\sqrt[n]{a}$ is rationally known for some factor $m$ of $n$.
- If $t_0 + t_1a^{1/n} + t_2a^{2/n} + \cdots + t_{n-1}a^{(n-1)/n} = 0$, where $n$ is prime and $a^{1/n}$ cannot
be expressed rationally by $a$ and $t_0, t_1, \ldots, t_{n-1}$, then all the $t_j$ are equal to zero. (Credited to Abel.)

Chapter 3. Symmetric Functions

- The coefficients in the equation $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ are symmetric functions of the roots. Hence every rational function of the coefficients is a symmetric function of the roots. The converse question is of the highest importance for the theory of equations.
- Newton’s equations relating the coefficients to the sums of powers of the roots are proved.
- Elimination in Newton’s equations gives the sums of powers of the roots as polynomials in the coefficients. The coefficients of these polynomials are integers.
- Elimination in Newton’s equations also gives the coefficients of the given equation as polynomials in the sums of powers of the roots. The coefficients of these polynomials are not necessarily integers.
- Every symmetric entire function of the roots can be expressed as an entire function of the coefficients of the equation; that expression is linear in the coefficients of the given function and involves no division. Two proofs of this are given. The first comes from the two previous statements; the second uses Waring’s more direct approach.

Chapter 4. Polynomial Functions of the Roots

- An entire nonsymmetric function [i.e., a polynomial] of the roots can take on at most $n!$ different values when the roots are permuted in every possible way. If the function depends on just one of the roots, it takes on at most $n$ values; if it involves two roots, it may take on at most $n(n-1)$ values.
- If $v_0$ is a given function of the roots and $v_1, v_2, \ldots, v_{m-1}$ are the different values it takes on when the roots are permuted, then every symmetric function of the $v_j$ is also a symmetric function of the roots.
- Every entire function $u_0$ of the roots is itself a root of an algebraic equation of degree $m \leq 2 \cdot 3 \cdots n$, the roots of which are the $m$ different values $u_0$ takes on when the roots are exchanged in all possible ways. The coefficients of this new equation are entire functions of the coefficients in the given equation and of those in $u_0$.
- If the coefficients in the given equation and those of $u_0$ are integers, then the coefficients in this new equation are integers, too.
- Every rational function of the roots of an equation $f(x) = 0$ can be written as an entire function of the roots, and in such a way that no root appears to a power greater than $(n-1)$. Two somewhat different algorithms for this reduction are given.

Chapter 5. Theorems about Irreducibility

- If an equation whose coefficients are integers has a rational root, then that root is an integer. More generally, if, in an equation whose coefficients are integers,
some entire function of the roots takes on a rational value, then that value is an integer. [Recall: all equations are monic.]

- When an equation whose coefficients are integers is reducible, then the coefficients of the equations into which it is reduced are integers.

- When all coefficients in an equation are multiples of some prime $m$ and some entire function of the roots has a rational value, then that value is divisible by $m$. It follows that if such an equation is reducible, the coefficients of the equations into which it can be reduced will be divisible by $m$. Hence if the coefficients of an equation are all divisible by $m$ and the last coefficient not divisible by $m^2$, then the equation is irreducible.

- These theorems hold also for equations with coefficients from other domains with unique factorization. Also, equations with rational coefficients can be transformed into equations with integer coefficients by the substitution $x = z/D$, where $D$ is the common denominator of the coefficients.

- Application to an equation connected to the theory of elliptic functions: for general $\alpha$, the equation $x^8 - 6\alpha x^4 + 4\alpha(1 + \alpha)x^2 - 3\alpha^2 = 0$ is irreducible.

---

**Chapter 6. The Group of an Equation**

- **Problem.** Can a non-symmetric function of the roots be expressed rationally by the coefficients?

- For “general” equations we have proved that the answer is no: when a rational expression in the roots is rationally expressible by the coefficients, it is symmetric.

- A rational expression $\phi(x_0)$ in only one of the roots of an irreducible equation is rationally known if and only if its numerical value is unchanged when $x_0$ is replaced by any of the other roots of the equation. **Proof of sufficiency.** If $\phi$ is invariant, then $\phi(x_0) = \phi(x_1) = \cdots = \phi(x_{n-1}) = (1/n)(\phi(x_0) + \phi(x_1) + \cdots + \phi(x_{n-1}))$ is symmetric, hence rational. **Proof of necessity.** If $x_0$ is a root in the irreducible equation $f(x) = 0$ and $\phi(x_0) = A$, then $f$ and the equation $\phi(x) - A = 0$ have a common root. The irreducibility of $f$ then implies that $\phi(x_j) - A = 0$, for all roots $x_j$ of $f$.

- The case of a rational expression $u_0$ involving two or more of the roots is reduced to this, by first constructing an algebraic quantity by which all the roots can be expressed rationally. To do this, we choose rational numbers $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ such that when the $x_j$ are exchanged in all the $n! = m$ possible ways, the quantity $v_0 = \alpha_0 x_0 + \alpha_1 x_1 + \cdots + \alpha_{n-1} x_{n-1}$ will take on $m$ different values. (The condition means that there are a finite number of equations which are not to be satisfied, and we have an infinite number of rationals $\alpha_j$ to choose from.) Using this $v_0$, we find that:

  (i) Every rational function $u_0$ of the roots can be expressed rationally by $v_0$ and the coefficients of the equation.

**Proof.** Let $v_0, v_1, v_2, \ldots, v_{m-1}$ be the $m = n!$ different values into which $v_0$ is
changed when \( x_j \) are permuted in all possible ways, and let \( u_0, u_1, u_2, \ldots, u_{m-1} \) be the corresponding values of \( u_0 \) (these are not necessarily different!). Then note that the sums \( \sum_{i=0}^{m-1} u_i v_j^k = c_k \), for \( k = 0, 1, \ldots, m - 1 \), are symmetric in the \( u_i \), hence in the \( x_j \), and therefore rational. These \( m \) equations are linear in the \( u_j \), and their determinant is nonzero, so we can solve them to get the \( u_j \) as rational expressions in the \( v_j \).

(ii) Since \( v_0 \) is a root in the equation \( (v - v_0)(v - v_1) \cdots (v - v_{m-1}) = 0 \), which has rational coefficients, \( v_0 \) is a root in some irreducible equation of degree \( \mu \leq m \). Let the other roots in that equation be \( v_1, v_2, \ldots, v_{\mu-1} \). Then every rational function \( u_0 \) in the \( x_j \) can be written as a rational expression in \( v_0 \). Therefore it is rational in the coefficients if and only if it is unchanged when \( v_0 \) is replaced by any of \( v_1, \ldots, v_{\mu-1} \).

- It follows that \( u_0 \) can be expressed rationally by the coefficients in the given equation if and only if it is unchanged under that subset of all permutations of the \( x_j \) which exchanges the first \( \mu \) of the \( v_j \) among themselves and the rest of them among themselves.

- **This subset of the set of all permutations of the roots is called the group of the given equation** [Sylow’s emphasis]. In other words, a rational function of the roots can be expressed rationally by the coefficients if and only if it is invariant under the substitutions which belong to the group of the equation.

- The reasoning in this chapter is valid also for equations with repeated roots, provided that each of them is considered as just one root [i.e., not counting multiplicity].

- The substitutions belonging to the group have the property that if any two of them are applied one after the other, the result is a third substitution which belongs to the group.

- For any given group of permutations of \( x_0, x_1, \ldots, x_{n-1} \) there exists a function of the roots which is unchanged by the substitutions in the group but not by any other substitution. The proof starts from a function \( v_0 \) which takes on \( n! \) different values when the roots are permuted. Let \( v_0, v_1, \ldots, v_{\mu-1} \) be the values corresponding to the given group. Then it is possible to find a rational \( \alpha \) such that the function \( F_0 = (\alpha - v_0)(\alpha - v_1) \cdots (\alpha - v_{\mu-1}) \) has the desired property.

- Finally, it is shown that for any group there exists an equation to which it belongs.

**Proof.** The general equation of degree \( n \) is used, with the quantity \( F_0 \) defined above considered as known. [Note. Thus the given group is the Galois group of an equation with coefficients from the extension \( Q(F_0) \) of the rationals. Whether there exists an equation with rational coefficients, and having the specified Galois group, is quite another matter! As far as I know that problem is unsolved even today. See [12], esp. p. 1.]
Chapter 7. Relations between the Equation and Its Group

- Rational relations [i.e., equations] between the roots of the given equation are conserved under the substitutions that belong to the group of the equation.
- If a rational expression in the roots takes on \( \nu \) different values under the substitutions of the group, it satisfies an equation of degree \( \nu \) with rationally known coefficients, and whose roots are these \( \nu \) values. The number \( \nu \) is a divisor of the number of permutations in the group of the given equation.
- The group of this new equation is transitive. (It will be shown in the next chapter that this implies that the equation is irreducible.)

**Example.** The theorems above are used to show how the equation \( x^4 + x^3 + x^2 + x + 1 = 0 \) can be solved by radicals.

- If \( u_0 \) and \( v_0 \) are two rational expressions in the roots of the given equation, and if all the substitutions in the group of the equation which leave \( v_0 \) invariant also leave \( u_0 \) unchanged, then \( u_0 \) can be expressed rationally by \( v_0 \).
- Finally, if a given function \( u_0 \) of the roots is considered as known, the group is reduced to those elements of the original group which leave \( u_0 \) unchanged.

Chapter 8. Substitutions

- A substitution may be written as a product of cyclic substitutions. The order of a substitution is defined. A cyclic substitution of \( n \) roots is of order \( n \). If \( n \) is prime, then any substitution of order \( n \) is cyclic.
- Different notations for substitutions and for composition of substitutions are discussed. Composition is not necessarily commutative. It is verified that the substitutions belonging to a group have the properties which are used to define groups in the modern sense of that word.
- The group of a general equation of degree \( n \) is of order \( n! \).
- An equation with no repeated roots is irreducible if and only if its group is transitive.
- If the given equation is irreducible, the order of its group is a multiple of its degree. In any equation of degree \( n \), the order of the group is a divisor of \( n! \).
- If the degree of the equation is prime and the group contains no cyclic substitution of all the roots, then the equation is reducible. Equivalently, any irreducible equation of prime degree contains in its group a cyclic substitution of all the roots. (Credited to Schönemann.)

**Generalization (Cauchy).** A group contains cyclic substitutions of every prime order which is a divisor of the number of substitutions in the group (i.e., the order of the group).

[Note, following the main text: “What if \( m \) is divisible by \( \nu^d \)? Can the above be extended?”]
The number of substitutions belonging to the group of an irreducible equation is at least equal to the degree of that equation. We will study the class of the irreducible equations whose group has this minimal number of substitutions.

In an irreducible equation whose group has only \( n \) substitutions, every root can be expressed rationally by any of the others. Conversely, if every root can be expressed rationally by one of them, then the group has only \( n \) permutations.

If, in addition, the degree of the equation is prime, then every substitution in its group must be of order \( n \). Then, if one root can be expressed rationally by one other, say \( x_1 = \theta(x_0) \), it follows that the remaining roots can be written \( x_2 = \theta^2(x_0), \ldots, x_{n-1} = \theta^{n-1}(x_0) \), with \( \theta^n(x_0) = x_0 \).

Conversely, if the degree of an irreducible equation is prime and one of the roots is a rational function of one other, \( x_1 = \theta(x_0) \), then the remaining roots are given by \( \theta^2(x_0), \theta^3(x_0), \ldots, \theta^{n-1}(x_0) \), where \( \theta^n(x_0) = x_0 \). Thus, the group contains just one cyclic substitution repeated \( n \) times.

Regardless of whether the degree \( n \) is prime or not, if the roots are given by \( \theta^2(x_0), \theta^3(x_0), \ldots, \theta^{n-1}(x_0) \), then the equation is solvable by radicals. The proof proceeds by noting that the group then must be cyclic and that the quantity

\[
v = \{x_0 + \omega x_1 + \omega^2 x_2 + \cdots + \omega^{n-1} x_{n-1}\}^n,
\]

where \( \omega \) is an \( n \)th root of unity, is invariant under cyclic permutations of the roots, and therefore rational. Using all the \( n \) different values of \( \omega \), we get \( n \) such quantities \( v \). Taking \( n \)th roots and solving the resulting system of linear equations, we find rational expressions for the \( x_i \) in terms of the \( n \)th roots of unity and of these \( n \) values of \( v \).

This expression for the roots is simple, but it has the drawback that it contains \( n - 1 \) root signs, and therefore gives \( n^{n-1} \) values, not just the \( n \) roots. A closer analysis shows how to get rid of that complication.

Regardless of whether the degree \( n \) is prime or not, it is true that if the group is cyclic, or, equivalently, if the roots may be written as \( x_0, \theta(x_0), \theta^2(x_0), \ldots, \theta^{n-1}(x_0) \), then the equation is solvable by radicals.

Such equations have been called abelian by Kronecker.

It follows that if the equation is irreducible and of prime degree, and if one of the roots may be expressed rationally by one of the others, then the equation is solvable by radicals.

Two examples are considered. First the general quadratic equation \( x^2 + ax + b = 0 \) is shown to be abelian, and its solution is deduced from the general theory.
Then the equation \( x^{n-1} + x^{n-2} + \cdots + x + 1 = 0 \), with \( n \) prime, is considered, and it is shown that the \( n \)th roots of unity can be expressed by radicals and the \( (n - 1) \)st roots of unity.

[Sheet 9] [Equations with Real Coefficients]

- If the roots are as above and the coefficients in the function \( \theta \) are real, then either all the roots are real or none of them are real.
- If, in addition, the coefficients of the given equation are real, then the quantities \( v \) from Sheet 8 can be expressed rationally by real quantities and an \( n \)th root \( \omega \) of unity. By separating real and imaginary parts in the expressions for the \( v \)'s and in the resulting expressions for the roots, it is then shown that to solve the equation requires one:
  1. to divide the periphery of the circle into \( n \) equal parts.
  2. to divide an angle, which can now be constructed, in \( n \) equal parts.
  3. to extract the square root of one quantity, which can now be computed.

- Example. \( (x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \cdots + x + 1 = 0 \). The \( n \)th roots of unity can be expressed by radicals and the \( (n - 1) \)st roots of unity (as was found by other means before).
- To divide the periphery of the circle into \( n \) equal parts when \( n \) is prime, it is sufficient
  1. to extract the square root of \( n \),
  2. to divide the periphery into \( (n - 1) \) equal parts,
  3. to divide a certain angle, which can now be constructed, into \( (n - 1) \) equal parts.
- In particular, the circle can be divided into \( n \) equal parts using only straightedge and compass when \( n \) is a prime of the form \( 2^p + 1 \).
- Example. The same conclusions about solvability by radicals and constructability with straightedge and compass are also deduced from the equation which expresses \( x = \cos \phi \) in terms of \( \cos(2n + 1)\phi \), although through somewhat heavier computations.

[Sheet 10]

- It has been shown (sheet 8) that the roots of an abelian equation can be written in the form
  \[
  x_0 = \frac{1}{n} \{-a_1 + \psi v_1 + q_2(\psi v_1)^2 + q_3(\psi v_1)^3 + \cdots + q_{n-1}(\psi v_1)^{n-1}\} = \phi(\psi v_1) \tag{1}
  \]
  where \( v_1 \) and all the coefficients are rational expressions in known quantities and one \( n \)th root \( \omega \) of unity.
- To obtain a converse statement, we consider \( \omega \) to be known, and suppose that
the equation \( x^n - v = 0 \) is irreducible. Then every quantity of the form (1) will be a root in some irreducible equation of degree \( n \), with rationally known coefficients, and the roots of this equation can be written as \( x_0, \theta(x_0), \theta^2(x_0), \ldots, \theta^{n-1}(x_0) \).

- If we do not consider \( \omega \) to be known, it is hard to find symmetric expressions in the roots to be used instead of the \( v \) in the preceding theory. The most important case is when only rational numbers are known; or rather that only such quantities are known that leave the equation \( (x^n - 1)/(x - 1) = 0 \) irreducible. The resulting equations are important in the theory of solvable equations with rational coefficients. There also are intermediate cases, where some quantity is known which renders the equation \( (x^n - 1)/(x - 1) = 0 \) reducible without giving rational expressions for the \( \omega \). [These problems are not discussed further in the present lectures.]

[Generalized Abelian Equations]

- Now consider a more general case, in which the degree of the given equation is no longer a prime, but where the group is still supposed to contain just \( n \) substitutions, and where, consequently, each root can be expressed rationally by any one of the others.

- In that situation, there is a factorization \( n = m \cdot m' \) such that the roots of the equation can be arranged in \( m' \) cycles, each consisting of \( m \) roots, in such a way that every substitution belonging to the group either exchanges permutations only within the individual cycles or exchanges whole cycles among themselves.

- Generally, when the roots of an equation of degree \( n = m \cdot m' \) can be placed in \( m' \) cycles, each of order \( m \), such that every substitution belonging to the group either exchanges permutations only within the individual cycles or exchanges whole cycles among themselves, then the given equation is split into \( m' \) equations of degree \( m \), the coefficients of each of which are rational expressions in the coefficients of the given equation and one root of an auxiliary equation of degree \( m' \) with rationally known coefficients.

- These \( m' \) equations are abelian, hence solvable by radicals.

[Sheet II]

- In general this auxiliary equation \( \phi(x) = 0 \) is not solvable by radicals, and its roots cannot be expressed as rational functions of each other. If they can, then a substitution in the group of the given equation which leaves one of the roots \( y_k \) of \( \phi(x) = 0 \) invariant must leave them all invariant. Necessary and sufficient for that is that every substitution which keeps one of the cycles in the group invariant keeps them all invariant.

- An equivalent condition is the following: If \( \theta \) and \( \phi \) are two substitutions from its group, \( x_0 \) a root, and \( k \) a positive integer, then there is a positive integer \( l \) such that \( \theta\phi^l(x_0) = \phi^l\theta(x_0) \).

- In that case, the auxiliary equation again splits into a number of abelian equations, the coefficients of which depend rationally on the roots of a new auxiliary equation (which may or may not be of the same kind).
There is one simple case where the given equation can be completely reduced to abelian equations: when every root of an irreducible equation can be rationally expressed by one of them, \(x_0\), and in such a way that if \(\theta\) and \(\theta_1\) are two of these functions, then \(\theta \theta_1(x_0) = \theta_1 \theta(x_0)\), then the given equation splits into only abelian equations, and hence is solvable by radicals.

This reasoning can be used to solve abelian equations of composite degree: an abelian equation of degree \(n = m \cdot m'\) splits into \(m'\) abelian equations of degree \(m\) with coefficients dependent on a root of an abelian equation of degree \(m'\). Since all roots can be expressed rationally by \(x_0\), it is sufficient to know one root of the first equation and one root of one of the \(m\)th degree equations.

If \(m\) or \(m'\) is composite, the reduction can be continued: if \(n = a^b b^c \cdots l^e\), where \(a, b, \ldots, l\) are different primes, then the solution of the given abelian equation can be reduced to solving \(\alpha\) equations of degree \(a\), \(\beta\) equations of degree \(b, \ldots, \lambda\) equations of degree \(l\).

If we apply this to the equation \((x^5 + 1)/(x - 1) = 0\), we find Gauss's theorem on the division of circles.

In view of an earlier result (sheet 8), these considerations imply the following theorem: let an irreducible equation be of degree \(n = a^b b^c \cdots l^e\), where \(a, b, c, \ldots, l\) are primes, and suppose that every root can be rationally expressed by one of them, \(x_0\), in such a way that if \(\theta\) and \(\theta_1\) are two of these functions, then \(\theta \theta_1(x_0) = \theta_1 \theta(x_0)\). Then the equation may be solved by solving \(\alpha\) equations of degree \(a\), \(\beta\) equations of degree \(b, \ldots, \lambda\) equations of degree \(l\), each of which is abelian and hence solvable by radicals.

Abelian equations whose degree is composite and contains different primes can be solved in yet another way. Write \(n = m_1 m_2 \cdots m_p = m_1 \mu_1 = m_2 \mu_2 = \cdots = m_p \mu_p\), and let \(x_0\) be one of the roots. We have seen that \(x_0\) is a root of one equation \(F_1(x, y_1) = 0\) of degree \(\mu_1\) with coefficients depending on the root \(y_1\) of an auxiliary equation \(\phi_1(y) = 0\) of degree \(m_1\); and it is also a root of an equation \(F_2(x, y_2) = 0\) of degree \(\mu_2\), with coefficients depending on the root \(y_2\) of an auxiliary equation \(\phi_2(y) = 0\) of degree \(m_2\), etc. If the \(m_1, m_2\), etc. are relatively prime, these equations \(F_1(x, y_1) = 0, F_2(x, y_2) = 0\), etc. have \(x_0\) as their only common root, and hence have the common factor \((x - x_0)\). The coefficient of this factor, i.e., \(x_0\), is a rational function of \(y_1, y_2, \ldots, y_p\), and the solution of the given equation is reduced to solving the equations \(\phi_{i}(y) = 0\).

Several examples are given with computations carried out in great detail as follows.

[At the end of sheet 11 and the beginning of sheet 12] The binomial equation \(x^n - 1 = 0\) is discussed. Primitive roots of unity are defined, and their number is shown to be equal to the number of integers \(p, 1 < p < n\), which are relatively prime to \(n\).

The equation \((x^7 - 1)/(x - 1) = x^6 + x^5 + \cdots + x + 1 = 0\) is solved by radicals in three different ways: by reduction to two cubic equations, to three...
quadratic equations, and by combining these two. [Not all of the computations have been transcribed in [17].]

- The equation \( z^3 + z^2 - 2z - 1 = 0 \) has the roots \( 2 \cos(2\pi/7), 2 \cos(6\pi/7), \) \( 2 \cos(4\pi/7) \). The preceding theory is used to obtain alternative expressions for them.

[Sheet 12a]

- Now suppose that the degree of the given equation is composite, but that one of the roots can be expressed rationally by one of the others, \( x_1 = \theta(x_0) \). Then there is a number \( m \) such that for \( 1 \leq j < m \), all \( \theta^j(x_0) \) are different roots, and \( \theta^m(x_0) = x_0 \). Then this \( m \) is a factor of \( n \), say \( n = m \cdot m' \), and the roots may be placed in \( m' \) disjoint cycles, each containing \( m \) roots, in such a way that every substitution in the group either exchanges the roots in each cycle among themselves or exchanges the whole cycles among themselves.

- The equation then can be split into \( m' \) equations of degree \( m \), whose roots are the roots of the given equation, and where the coefficients of each of them depend rationally on one of the roots of an auxiliary equation of degree \( m' \) (with rationally known coefficients). This root is a symmetric function of the roots in the corresponding cycle.

- Two examples are considered in much detail. The first is reciprocal equations: \( f(x) = 0 \) where the polynomial \( f \) satisfies the equation \( f(x) = x^nf(1/x) \). [Three explicit equations of this kind are treated; only one has been transcribed.] The second is a modular equation from the theory of elliptic functions. [The computations here are rather laborious, and have not been transcribed. Sylow gives no reference to the theory of elliptic functions or modular equations.]

[Adjunction of New Known Quantities]

- When the roots of some irreducible auxiliary equation are considered known, the equation will either remain irreducible or split into a number of equations all of the same degree. Each of these equations is obtained from one of them by substitutions belonging to the group of the given equation.

- The same reduction is obtained by adjoining a quantity which is a rational function of the roots in the given equation. It is also a symmetric function of the roots in one of the factors.

- If the given equation is of prime degree, it cannot be made reducible without being split into only linear equations.

- Definition. An equation is called primitive if whenever it is made reducible by the adjunction of some new known quantity, it splits into only linear equations.

[Sheet 13]

- An equation is primitive if and only if its roots can be arranged in \( \nu' \) cycles each having \( \nu \) roots and such that by any substitution belonging to the group of the equation, either the roots are exchanged only within each cycle or whole cycles are exchanged.
The general equation of degree 4 is primitive.

When the roots of some irreducible auxiliary equation are counted among the known quantities, the group of the given equation will either remain unchanged or split into several partial groups each having the same number of substitutions. Each of these partial groups is the group of the given equation when the new quantity has been adjoined. They all have the same substitutions, and the permutations in one of them are moved to the permutations in each of the others by use of one and the same substitution from the group.

Conversely, let the group of the given equation split into $n$ partial groups each having $n$ permutations and having the properties described. Then there is an auxiliary equation whose group has $n$ permutations, such that if the roots of that equation are adjoined to the known quantities, the group is reduced to one having just $n$ permutations.

[Sheets 14 and 15] On Equations Solvable by Radicals and of Prime Degree

To solve an irreducible equation by radicals means that one successively adjoins roots of irreducible equations $x^m - a = 0, x^{m_1} - a_1 = 0$, etc., to the known quantities. Here $m, m_1, \ldots$ are prime numbers, $a$ is rational, and each following $a_j$ is rational in terms of the previous adjunctions. This is repeated until the given irreducible equation becomes reducible. In this process, it can be assumed that the necessary roots of unity are known.

Let the given equation become reducible when a root of the equation $x^p - r = 0$ is adjoined. Then $p$ is equal to the degree $n$ of the given equation, and since that is a prime, the equation can be reduced only by splitting into $n$ factors of the first degree.

Before this last adjunction, the group of the given equation must have been reduced to a cyclic group of order $n$.

Working backwards from this, it is found that all the substitutions belonging to the original group must have been of the form $\phi(k) = ak + b \mod n$, where $a$ and $b$ are constants. Here, $b$ will take on all values $0, 1, \ldots, n - 1$, and $a$ takes values $1, e^\omega, e^{2\omega}, \ldots, e^{(n-1)\omega}$, where $e$ is a primitive root of unity and $\alpha \cdot \alpha' = n - 1$.

The proof of the converse, that if the group admits substitutions of this form only, then the equation is solvable by radicals, is rather long. It uses the quantity $s_1 = (x_0 + \omega x_1 + \omega^2 x_2 + \cdots + \omega^{n-1} x_{n-1})^n$, where $\omega$ is an $n$th root of unity. We have seen (in our work with abelian equations) that $s_1$ is invariant under substitutions of the form $\phi(k) = k + b$. Now we show that it takes on $\alpha'$ different values under the substitutions $\phi(k) = ak$. Then two pages of computation lead to formulas expressing the roots as linear combinations of the $n$th roots of $s_1$ with coefficients which are rational in $s_1$ and $\omega$.

For an irreducible equation of prime degree to be solvable by radicals, it is necessary and sufficient that its group contains only substitutions of the form $(k, ak + b)$ (that is, $x_k \rightarrow x_{\phi(k)}$, where $\phi(k) = ak + b \mod n)$).
This criterion can be expressed in another way: For an irreducible equation of prime degree to be solvable by radicals, it is necessary and sufficient that all its roots can be expressed rationally by two of them.

An irreducible equation of prime degree is solvable by radicals or not, according to whether its group contains \( n \) or more cyclic substitutions of all roots.

Application to general equations. The general cubic equation is solved by radicals. General equations of degree higher than the fifth are not solvable by radicals, because it has been proved earlier that the general quintic equation is not solvable.

REFERENCES

Unpublished Source
S. Sylow’s report to the Ministry of Education, National Archives of Norway. Papers of the Department for Church and Education.

Published Sources
5. Évariste Galois, Sur la théorie des nombres, Bulletin des sciences mathématiques 13 (1830), or [4, 15–23].
6. Évariste Galois, Mémoire sur les conditions de résolubilité des équations par des radicaux, Journal des mathématiques pures et appliquées 11 (1846), or [4, 33–50].
9. Helge Bergh Kragemo, Ludvig Sylow, Norsk Matematisk Tidsskrift 15 (1933), 73–99. [In German]
17. Ludvig Sylow, Forelesninger over algebraisk Lignings og Substitutions theorie, holdte ved Universitetet i Christiania som Prof. O. J. Brochs Vicar 1862, ed. Bent Birkeland, Oslo: Matematisk Institutt 1995. [In Norwegian]