[15] A. Schrijver, Theory of Linear and Integer Programming. Wiley-Interscience: Chichester, 1986.

[16] T. A. Springer, Invariant Theory. Lecture Notes in Mathematics 585. Springer-Verlag: Berlin-Heidelberg-New York, 1977.

[17] Hermann Weyl, *David Hilbert and his mathematical work*, Bull. Amer. Math. Soc. **50** (1944), 612-654.

[18] Hermann Weyl, The Classical Groups, Their Invariants and Representations. Princeton University Press: New Jersey, 1939.

[19] Hermann Weyl, The Theory of Groups and Quantum Mechanics, (English translation). Methuen: London, 1931.

Acknowledgement I am indebted to Rod Gow for reading the first version of this article and supplying me with some additional historical information and references.

D. W. Lewis,
Department of Mathematics,
University College,
Belfield,
Dublin 4.

SYLOW'S PROOF OF SYLOW'S THEOREM

Rod Gow

1. Introduction

While looking through some early volumes of *Mathematische Annalen*, we came across a paper with the following title:

Théorèmes sur les groupes de substitutions.

Par M. L. Sylow à Frederikshald en Norvege.

This was, of course, the paper containing Ludwig Sylow's fundamental contribution to group theory, [9]. We thought it might be interesting to see how Sylow actually proved his theorem and then to comment briefly on some later proofs and earlier work. It is likely that there have been prior discussions of the history of Sylow's theorem in the literature and we apologize for failing to acknowledge any relevant publications. (Our excuse is that the UCD library is badly stocked with periodicals on the history of science.)

Sylow's starting point is as follows: *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.* (The notation of Sylow is a little wayward to modern tastes. His prime is denoted by n, rather than the traditional p. Later in the paper, the expression $np + 1$ appears as the number of Sylow subgroups, but p denotes merely some non-negative integer. In virtually all later literature relating to the proof of Sylow's theorem and earlier literature on Cauchy's theorem that we have seen, the prime is represented by p. We shall follow standard practice and denote our prime by p in this exposition, except when enunciating Sylow's theorems in his own words.) We recognize the statement above as Cauchy's theorem, which we would normally state as: *if a prime p divides the order of a finite group, then the group contains an element of order p.* The stipulation that we should have a group of permutations is irrelevant, although in Cauchy's day, abstract finite groups would not have been under consideration. Indeed in the fourth edition of Serret's book, there is some discussion of permutation groups and of groups of linear fractional transformations, but no discussion of abstract groups or of Cauchy's theorem. There is, however, a discussion of a construction, due to Cauchy, of a Sylow p-subgroup of the symmetric group S_n in [8, p.302]. Cauchy's theorem underlies Sylow's proof. It is not proved. Later proofs sought to remove this reliance on Cauchy's theorem, whose original demonstration was quite complicated, although it contained germs of ideas vital to modern group theory. In particular, Frobenius was able to give a proof of the existence of Sylow subgroups which avoided Cauchy's theorem and became the standard proof of Sylow's theorem until the advent of Wielandt's proof in 1959, [11].

Sylow proves the existence of a Sylow p-subgroup P in a finite group G, at the same time showing that if N is the normalizer of P in G, then $|G : N| \equiv 1 \bmod p$. Afterwards, he shows that any other Sylow p-subgroup Q is conjugate to P in G. A basic idea used by Sylow, the spirit of which really occurs in all proofs, is that of letting P and Q permute the cosets of N by multiplication. Simple congruences modulo p force out the desired conclusion. Needless to say, Sylow does not talk in terms of permuting cosets, but this is the way to interpret his procedures nowadays.

2. Sylow's proof

We now consider the details of Sylow's proof. We try to follow the spirit, as we see it, of Sylow's ideas but use more modern concepts to try to explain what is happening. We will make a few comments about Sylow's precise method later. Let G be a non-trivial finite group and let p^α be the p-part of $|G|$, where p is a prime and $\alpha \geq 1$. Let P be a p-subgroup of G of maximal order and let N be its normalizer in G. Sylow first proves that $|N : P|$ is not divisible by p. From our point of view, this is clear. If p divides $|N : P|$, Cauchy's theorem guarantees the existence of a subgroup of M/P of order p in the quotient group N/P. M is then a p-subgroup of order larger than $|P|$, which is impossible. Sylow next proves that P contains all elements of p-power order in N. His proof is essentially the same as any modern one. Suppose ϕ is an element of N not in P. The elements $\vartheta\phi^i$, where ϑ runs over P and i over the integers, form a subgroup of N properly containing P. The order of this subgroup is $|P|m$, where m is the smallest positive integer j such that $\phi^j \in P$. But m clearly divides the order of ϕ. Since P is a p-subgroup of maximal order, ϕ cannot have order a power of p, as required.

The crucial part of the proof is to show that $|G : N|$ is not divisible by p. Once this is known, we see that $|P| = p^a$, and the existence of Sylow p-subgroups is established. In fact, Sylow shows that $|G : N| \equiv 1 \bmod p$, which is another part of his basic theorem. The following would seem to be a modern version of his argument. P permutes the left cosets of N in G by left multiplication. It fixes N, because it is contained in N. It fixes no other left coset. For if P fixes the coset ψN, we have $\psi^{-1}P\psi \leq N$. But the argument above shows that the p-subgroup $\psi^{-1}P\psi$ now contained in N equals P, as it has the same order as P. Hence $\psi \in N$ and $\psi N = N$, as required. The left cosets of N different from N fall into P-orbits of size greater than 1, and the size of each orbit is a power of p, as it divides the order of P, by the orbit-stabilizer theorem. This proves what Sylow gives as his first theorem, where we return to Sylow's original notation:

Si n^α 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^α; si de plus $n^\alpha\nu$ 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 $n^\alpha\nu(np+1)$.

Sylow's second theorem is the following:

Tout étant posé comme au théorème précédent, le groupe G contient précisement $np+1$ groupes distincts d'ordre n^α; on les obtient tous en transformant l'un quelconque d'entre eux par les *substitutions de G, tout groupe étant donné par $n^\alpha \nu$ transformantes distinctes.*

His proof is the following (returning to our notation). Let Q be a subgroup of order $|P|$. Q permutes the left cosets of N in G into orbits, the size of each Q-orbit being a power of p. As the number of orbits is congruent to 1 modulo p, it fixes a coset. Thus $\psi^{-1}Q\psi \leq N$ for some ψ. But the argument of the previous paragraph shows that $\psi^{-1}Q\psi = P$, as P contains all p-elements in N. Sylow notes that the same argument proves that any p-subgroup of G is contained in a conjugate of P. Thus the standard results comprising Sylow's theorem are obtained.

Having proved his main theorems, Sylow continues his paper by considering the conjugating action of the p-group P on itself. P acts on P according to the rule

$$\vartheta \to \phi^{-1}\vartheta\phi.$$

This is a permutation action, since

$$\vartheta_2^{-1}\vartheta_1^{-1}\phi\vartheta_1\vartheta_2 = (\vartheta_1\vartheta_2)^{-1}\phi(\vartheta_1\vartheta_2).$$

The orbits of P acting in this way are its conjugacy classes (not so-called by Sylow) and their sizes are powers of p. Since the identity of P forms a single orbit, we have an equation of the form

$$p^\alpha = 1 + p^a + p^b + \cdots$$

This implies that at least $p - 1$ of the indices a, b, ..., are 0. Thus, in modern terminology, the centre of P is non-trivial (the argument is unchanged to this day).

An element ϑ_0 of order p may then be found in the centre. If Θ_0 denotes the subgroup of P generated by ϑ_0, Sylow essentially forms the quotient group P/Θ_0 of order $p^{\alpha-1}$. This group has a non-trivial centre. Let ϑ_1 project onto an element of order p in the centre of P/Θ_0. Then $\vartheta_1^p = \vartheta_0^a$. Furthermore

$$\vartheta^{-1}\vartheta_1\vartheta = \vartheta_0^b\vartheta_1$$

for all ϑ in P (here b depends on ϑ). The elements of the form $\vartheta_0^i\vartheta_1^k$ form a (normal) subgroup of P of order p^2. Continuing in this way, we then obtain ϑ_2 so that

$$\begin{aligned}\vartheta_2^p &= \vartheta_0^c\vartheta_1^d\\ \vartheta^{-1}\vartheta_2\vartheta &= \vartheta_0^e\vartheta_1^t\vartheta_2\end{aligned}$$

for all $\vartheta \in P$ (the exponents again depending on ϑ). This leads to Sylow's third theorem:

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

$$\vartheta = \vartheta_0^i\vartheta_1^k\vartheta_2^l\ldots\vartheta_{\alpha-1}^r$$

où

$$\begin{aligned}\vartheta_0^n &= 1\\ \vartheta_1^n &= \vartheta_0^a\\ \vartheta_2^n &= \vartheta_0^b\vartheta_1^c\\ \vartheta_3^n &= \vartheta_0^d\vartheta_1^e\vartheta_2^f\\ &\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

et où l'on a

$$\begin{aligned}\vartheta^{-1}\vartheta_0\vartheta &= \vartheta_0\\ \vartheta^{-1}\vartheta_1\vartheta &= \vartheta_0^\beta\vartheta_1\\ \vartheta^{-1}\vartheta_2\vartheta &= \vartheta_0^\gamma\vartheta_1^\delta\vartheta_2\\ \vartheta^{-1}\vartheta_3\vartheta &= \vartheta_0^\varepsilon\vartheta_1^\zeta\vartheta_2^\eta\vartheta_3\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

Thus, Sylow obtains the beginnings of the structure theory for p-groups, showing in particular that such groups are solvable.

As we explained earlier, we have tried to render Sylow's proof into a modern formulation. To give some of the flavour of Sylow's version, we describe his proof of the fact that p does not divide $\nu = |N : P|$. P is a permutation group of degree r, say, and so may be thought to act on certain variables $x_1, \ldots, x_r$. Let y_0 be a rational function of the x_i which is invariant under P but fixed by no other permutation. This function takes ν different values under the action of N, each of which is fixed by P. A homomorphic image N' of N acts faithfully and transitively on these functions (following the custom of the time, Sylow uses the word isomorphic rather than homomorphic). (N' is just the quotient group N/P.) If p divides ν, then N' contains a permutation of order p by Cauchy's theorem and Sylow obtains a contradiction to this using the same line of reasoning that proved that P contains all elements of p-power order in N.

3. Cauchy's theorem

We turn now to a brief look at Cauchy's theorem, which was vital to Sylow's proof. The paper, [2], in which Cauchy's proof appears is well worth studying. It is 102 pages long and its general spirit is quite close to modern algebra, unlike that of many ostensibly algebraic papers of the 19th century, which are often hopelessly vague. Much of the elementary theory of permutations may be found there. For example, the size of a conjugacy class of S_n containing an element of a given cycle type is determined. Among other things, Cauchy gives an explicit construction of a Sylow p-subgroup of S_n ([2, pp.195-196]). This is interesting in itself, as it requires the idea of a wreath product. Wreath products play a vital role in the study of permutation and linear groups.

The concept of a double coset decomposition of a group relative to two subgroups is implicit in §12 of [2]. To paraphrase Cauchy's argument, the following is proved. Let G be a finite group containing subgroups A and B. Suppose that no non-identity element of A is conjugate to an element of B. Then the size of a double coset AgB is $|A||B|$. Moreover, G is the disjoint union of all the different double cosets. Consequently, with the hypothesis as above, $|A||B|$ divides $|G|$. Cauchy applies this when $G = S_n$, A is a Sylow p-subgroup of S_n (which he has already constructed) and B is a subgroup whose order is divisible by the prime p. Since $|A||B|$ cannot divide $n!$, a non-trivial element of A is conjugate to an element of B and thus Cauchy's theorem is proved. With a little more care and determination, the existence part of Sylow's theorem might easily have been obtained by Cauchy 30 or more years before Sylow's proof. Cauchy's proof of his theorem is reproduced in Jordan's famous treatise, [6, pp.26-29]. Cauchy's theorem applies to a subgroup of S_n, but Cayley's embedding theorem, that a finite group G is isomorphic to a subgroup of $S_{|G|}$, shows that it applies to any abstract finite group.

4. Later proofs of Sylow's theorem

Fairly soon after the publication of Sylow's theorem in 1872, attempts were made to avoid the use of Cauchy's theorem in its proof. In 1877, Eugen Netto gave a proof in [7] which used only part of the proof of Cauchy's theorem. In Netto's situation, as in Sylow's, we have a subgroup G of S_n of order k, where k is divisible by the prime p. (Note that Netto uses what has become standard notation in respect of n and p). He assumes Cauchy's constructive result that S_n contains a Sylow p-subgroup, H, say, of order p^f, and then proves that G contains a Sylow p-subgroup. We found Netto's proof difficult to follow, but it seems clear that he is using a decomposition of S_n into (G, H)-double cosets. He obtains the equation

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

where s is an integer, and $p^\alpha \geq p^\beta$, and so on. Multiplying each side above by $kp^f/n!$, we obtain the usual equation expressing the order of S_n as the sum of the sizes of the different (G, H)-double cosets. The powers of p that appear in the denominators are the orders of the intersections of G with various conjugates of H. Netto's proof, in double coset form, has become a standard one. An alternative is to embed a finite group into a finite general linear group $\mathrm{GL}(n, p)$, where p is a prime, and use the fact that the linear group contains an explicit Sylow subgroup, consisting of lower triangular matrices with all diagonal entries equal to 1. See, for example, the exercises on p.36 of [5].

The proof that was to become the standard proof of the existence of Sylow subgroups until 1959 is that of Frobenius, [3]. Although it appeared in 1887, it is dated Zürich, March 1884. Perhaps this is evidence that the publication backlogs of journals are not a new phenomenon. Frobenius aims to remove all reference to Cauchy's work and keep the discussion as elementary as possible. The proof is by induction, the main tool to be used being the conjugacy class equation in a finite group. The concept of a quotient group is also required. Frobenius works with an abstract finite group H, noting that it may be considered as a group of permutations. He also notes that his abstract finite group is defined by three axioms, which he states. He then considers the centre, G, of H and supposes that p divides its order. He shows (without using Cauchy's theorem) that the centre contains an element P of order p. He declares that two elements of H are to be considered (relatively) equal if they differ only by a power of P. The relatively different elements form a group, whose order is $|H|/p$ (this is the quotient group of H modulo the cyclic group generated by P). By induction, this group has a Sylow subgroup which lifts back to give a Sylow subgroup of H.

Finally, he supposes that p does not divide $|G|$. The conjugacy class equation shows that there must be an element not in the centre, the size of whose conjugacy class is relatively prime to p. But then the p-part of the order of the centralizer of this element equals the p-part of $|H|$, and since the order of this centralizer is less than that of H, by induction, the centralizer contains a Sylow p-subgroup of H, as required. This proof may be found in such early textbooks as those of Burnside, [1], and Hilton, [4].

6. Life and work of Sylow

We close by making a few remarks about the life and career of Sylow. Sylow (1832-1918) taught from 1858 to 1898 at a school in Halden (Frederikshald) in Norway. A town of this name is located south of Oslo, near the Swedish border. A chair was created for him in 1898 at Christiana (Oslo) University. His other main paper is [10], devoted to complex multiplication of elliptic functions and associated singular moduli. He seems to have been drawn to this subject while editing a new edition of the collected work of Abel, his famous compatriot, who contributed important early work on elliptic functions. Sylow's 1872 paper showed that he had considerable talent in abstract algebra and it is a pity that he did not

get more opportunity to put his talent into effect.

References

[1] W. Burnside, Theory of Groups of Finite Order. Cambridge Univ. Press: Cambridge, 1897.

[2] A. L. Cauchy, *Mémoire sur les arrangements que l'on peut former avec des lettres données*, Exercices d'analyse et de physique mathématique, tome III. Bachelier: Paris, 1844.

[3] F. G. Frobenius, *Neuer Beweis des Sylowschen Satzes*, J. für die reine und angewandte Math. **100** (1887), 179-181.

[4] H. Hilton, An Introduction to the Theory of Finite Groups. Clarendon Press: Oxford, 1908.

[5] B. Huppert, Endliche Gruppen I. Springer-Verlag: Berlin-Heidelberg-New York, 1967.

[6] C. Jordan, Traité des substitutions et des équations algébriques. Gauthier-Villars: Paris, 1870.

[7] E. Netto, *Neuer Beweis eines Fundamentaltheorems aus der Theorie der Substitutionslehre*, Math. Ann. **13** (1878), 249-250.

[8] J.-A. Serret, Cours d'algèbre supérieure, tome II (quatrième édition). Gauthier-Villars: Paris, 1879.

[9] L. Sylow, *Théorèmes sur les groupes de substitutions*, Math. Ann. **5** (1872), 584-594.

[10] L. Sylow, *Sur la multiplication complexe des fonctions elliptiques*, Journal de mathématiques pures et appliquées (quatrième série) **3** (1887), 109-254.

[11] H. Wielandt, *Ein Beweis für die Existenz der Sylowgruppen*, Arch. Math. **10** (1959), 401-402.

Rod Gow,
Department of Mathematics,
University College,
Belfield,
Dublin 4.