Séminaire BOURBAKI Mars 2013
65$^{\text{e}}$ année, 2012-2013, n$^{\text{o}}$ 1069, p. 319 à 342

THE PROOF OF ORE'S CONJECTURE
[after Ellers-Gordeev and Liebeck-O'Brien-Shalev-Tiep]

by **Gunter MALLE**

INTRODUCTION

The *commutator* $[g,h] := g^{-1}h^{-1}gh$ of two elements g,h of a group G is introduced in every first course in group theory, as well as the *commutator subgroup*

$$[G,G] := \langle [g,h] \mid g,h \in G \rangle,$$

generated by all commutators in G, and usually it is stated that not all elements of $[G,G]$ need to be commutators. The first such example of finite order may have been given by Fite [Fi02]. The smallest example of a finite group G for which $[G,G]$ contains non-commutators has order 96; in fact there are two non-isomorphic groups of that order in which the set of commutators does not equal the commutator subgroup, see Guralnick [Gu80].

In a 1951 paper, Oystein Ore [Ore] shows that every even element in a symmetric group of degree at least 3 is a commutator and claims that the proof can be extended to show that every element in a simple alternating group $\mathfrak{A}_n$ is a commutator. He concludes by saying that *"It is possible that a similar theorem holds for any simple group of finite order, but it seems that at present we do not have the necessary methods to investigate the question."* This has become known as *Ore's conjecture*, the recent solution of which [LOST] is the topic of this lecture:

Theorem 0.1 (Liebeck-O'Brien-Shalev-Tiep). — *Let G be a finite non-abelian simple group. Then every element of G is a commutator.*

In fact, at almost the same time as Ore, Noboru Ito [Ito51] showed the same statement for the alternating groups $\mathfrak{A}_n$, but without speculating about other finite simple groups.

The proof of Ore's conjecture relies on the classification of the finite simple groups and, through Lusztig's parametrization of irreducible characters of finite reductive groups, on the Weil conjectures; the final step also required a considerable amount of computer calculation.

Note that obvious generalizations of Theorem 0.1 fail to hold. For example Guralnick [Gu10] gives a quite general construction of groups, including non-solvable ones, with the property that $[G, G]$ does not consist of commutators only: let $G = U \wr H$ be the regular wreath product of two finite groups U, H with U abelian. If $|U| > 2$ or $|[H, H]| > 2$ then some element of $[H, G]$ is not a commutator in G (see also Isaacs [Is77] for a weaker result). Thus, for U of order at least 3 and any non-abelian simple group H this gives a non-solvable example G with factor group H, and in fact one may also obtain a *perfect* one (that is, a group G with $G = [G, G]$). Computer calculations show that the smallest example of a perfect group not all of whose elements are commutators is an extension of an elementary abelian group of order 2^4 with the alternating group $\mathfrak{A}_5$. Even closer to the case of simple groups, H. I. Blau [Bl94] proved that there exist (finitely many) quasisimple groups that contain non-commutator central elements (see Theorem 6.1 below). Recall that a group G is called *quasisimple* if it is perfect and the quotient $G/Z(G)$ by its center $Z(G)$ is (non-abelian) simple. The smallest such example is the exceptional 6-fold covering group of the alternating group $\mathfrak{A}_6$ (that is, a non-split central extension of the cyclic group of order 6 by $\mathfrak{A}_6$), for which the central elements of order 6 can be seen not to be commutators. So the property required by Ore's conjecture seems to be closely tied to simple groups.

We want to mention another open problem closely related to Ore's conjecture, which is concerned with the square $C^2 := \{xy \mid x, y \in C\}$ of a conjugacy class C, and which in the introduction to the book [AH85] is attributed to J. G. Thompson:

Conjecture 0.2 (J. G. Thompson). — *Let G be a finite non-abelian simple group. Then there exists a conjugacy class $C \subseteq G$ such that $C^2 = G$.*

Clearly, if $C^2 = G$ then every element in the product C^2 is a commutator, so the Thompson conjecture implies the (now proven) Ore conjecture. Many papers on the Ore conjecture actually show that the stronger Thompson conjecture holds for particular families of groups, so in this survey we will consider both conjectures simultaneously.

In a broader context, the Ore conjecture can be thought of as a particular instance of the surjectivity of word maps. For any word w in a free group F_r on r generators, and any group G, one can ask whether the corresponding word map is surjective, the Ore conjecture being the special case of the commutator word. This gives (non-commutative) analogues of diophantine equations on groups. For example, the representability of a group element by a product of kth powers, or by the kth power of a given word, can be considered to be analogues of Waring's problem in number theory. This point of view has been propagated by Shalev (see *e.g.*, [Sh09, LS09, LST11]).

One attractive feature of these questions, which we will insist on throughout this survey, is the fact that they also make sense for simple algebraic groups, where more powerful methods are available and much more can be shown to hold.

Let us end this introduction with a short historical overview on the proof of Ore's conjecture. After Ore and Ito proved the conjecture for the simple alternating groups, R.C. Thompson [Th61, Th62, Th62a] established it for the finite projective special linear groups $\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q))$. The symplectic groups $\mathrm{Sp}_{2n}(q)$ with $q \equiv 1 \pmod 4$ were handled by Gow [Gow88], and Bonten [Bo93] dealt with exceptional groups of Lie type of low rank. The case of sporadic groups was settled by Neubüser, Pahlings and Cleuvers [NPC84].

In 1998, E.W. Ellers and N.L. Gordeev [EG98] verified Ore's conjecture (and in fact Thompson's conjecture) for all finite simple groups of Lie type over a finite field $\mathbb{F}_q$, whenever $q \geqslant 9$. This will be explained in Section 1. Building on this result, Shalev [Sh09] then used asymptotic methods to show that for finite simple groups G, the proportion of commutators tends to 1 as $|G|$ tends to infinity. In that same paper he also showed that for any word $w \neq 1$, there exists $N = N(w)$ such that for every finite simple group G of order $|G| > N(w)$ we have $w(G)^3 = G$. The exponent 3 was later improved to 2 by Larsen, Shalev and Tiep [LST11]. We will discuss these methods and results in Sections 4 and 5. The remaining (infinitely many) simple groups of Lie type over small fields were then treated in the paper of Liebeck, O'Brien, Shalev and Tiep [LOST]. We sketch their approach in Section 2.

1. THE APPROACH BY ELLERS AND GORDEEV

Ellers and Gordeev [EG98] succeeded in proving Ore's conjecture for the finite simple groups of Lie type defined over fields of order at least 9. Since there are infinitely many distinct classical groups over any given finite field, this still leaves infinitely many open cases. The approach of Ellers-Gordeev is by direct computation. To get some idea on the method, one should consider the following model case for algebraic groups. This was proved by Pasiencier-Wang [PW62] over the complex numbers (with a precursor result by Goto [Go49] for compact semisimple Lie groups), and then Ree [Ree64] noticed that their argument can be extended to arbitrary algebraically closed fields:

Theorem 1.1 (Pasiencier-Wang, Ree). — *Let G be a semisimple linear algebraic group over an algebraically closed field. Then each element of G is a commutator.*

Proof (Sketch). — We want to show that $g \in G$ is a commutator. First note that a conjugate of a commutator is again a commutator, so we may replace g by any of its conjugates. By a result of Borel, any element of G lies in some Borel subgroup B of G, so we may assume that $g \in B$. Let $U = R_u(B)$ be the unipotent radical of

B, and $T \leqslant B$ a maximal torus. One now needs the following auxiliary claim, whose proof relies on a result of Kostant on the action of the Weyl group on the character group of T, see [Ree64, (3.1)]:

$(*)$ For any $s \in T$ there exists a regular element $t \in T$ (that is, with $C_G(t) = T$) and $x \in N_G(T)$ such that $x^{-1}tx = ts$.

Now let $g = su$ be the Jordan decomposition of g, where we may assume that $s \in T$, since all maximal tori of B are conjugate. By $(*)$ there exists a regular element $t \in T$ and $x \in N_G(T)$ with $x^{-1}tx = ts$. By Lemma 1.2 below applied to the regular element $ts \in T$ there is $b \in B$ with $b^{-1}tsb = tsu$, so that finally

$$g = su = t^{-1}b^{-1}tsb = t^{-1}b^{-1}x^{-1}txb = [t, xb]$$

is a commutator. □

Lemma 1.2. — *Let $B = U \cdot T$ be a semidirect product of a nilpotent normal subgroup U with an abelian group T. Then for $t \in T$ with $C_B(t) = T$ the coset tU is a single B-conjugacy class.*

Proof. — By induction over a central series of U one easily shows that the map $U \to U$, $u \mapsto [t, u]$, is bijective, so any $tv \in tU$ has the form t^u for some $u \in U$. □

An attempt to adapt this approach to finite groups of Lie type faces several problems. First, it is no longer true that all elements lie in a Borel subgroup. So one has to consider a larger collection of subgroups. Secondly, regular semisimple elements exist in the Borel subgroup only if the underlying field is sufficiently large compared to the rank. This is the principal reason why the Ellers-Gordeev method cannot handle all simple groups of Lie type.

In a series of three papers Ellers-Gordeev show a particular form of Gauss decomposition for elements of finite reductive groups. Recall that any finite simple group of Lie type G can be obtained by the following construction. (This does not apply to the Tits simple group ${}^2F_4(2)'$, which for most purposes should rather be considered as a 27th sporadic simple group.) There exist a simple linear algebraic group $\mathbf{H}$ of simply connected type over the algebraic closure of a finite field, and a Steinberg endomorphism $F : \mathbf{H} \to \mathbf{H}$, that is, a bijective morphism with finite fixed point set $H := \mathbf{H}^F$, such that $G = H/Z(H)$. Elements of G will be called regular if their preimages in the algebraic group $\mathbf{H}$ are. If $\mathbf{T} \leqslant \mathbf{B} \leqslant \mathbf{H}$ is an F-stable maximal torus inside an F-stable Borel subgroup of $\mathbf{H}$, then the image in G of $\mathbf{T}^F$, respectively of $\mathbf{B}^F$, is called a maximally split torus, respectively a Borel subgroup of G. The group of F-fixed points of the unipotent radical $R_u(\mathbf{B})$ is then called the unipotent radical of $\mathbf{B}^F$. Ellers-Gordeev [EG94, EG95, EG96] obtain the following statement on Gauss decompositions of elements.

Theorem 1.3 (Ellers-Gordeev). — *Let G be a finite simple group of Lie type, $T \leqslant B \leqslant G$ a maximally split torus inside a Borel subgroup of G, U the unipotent radical of B and U^- the unipotent radical of the opposite Borel subgroup. Fix $t \in T$. Then for any $1 \neq g \in G$ there exists $x \in G$ such that*

$$xgx^{-1} = u_1 t u_2 \quad \textit{for suitable } u_1 \in U^-,\ u_2 \in U.$$

For the special linear groups this was first shown by Sourour [So86]. In fact, Ellers-Gordeev prove the statement for Chevalley groups over any field K. Their proof takes roughly 50 pages of explicit calculation in the various families of groups of Lie type.

Corollary 1.4. — *In the situation of Theorem 1.3, suppose that $t_1, t_2 \in T$ are regular elements, and write C_1, C_2 for their conjugacy classes. Then $C_1C_2 \cup \{1\} = G$.*

Proof. — Let $1 \neq g \in G$, then by Theorem 1.3 some conjugate xgx^{-1} of g has the form $u_1t_1t_2u_2$ with $u_1 \in U^-$, $u_2 \in U$. Now by Lemma 1.2 applied to the semidirect products $B = UT$ and U^-T we can write $u_1t_1 = v_1t_1v_1^{-1}$, and $t_2u_2 = v_2t_2v_2^{-1}$ for suitable $v_1 \in U^-, v_2 \in U$, whence

$$xgx^{-1} = u_1t_1t_2u_2 = v_1t_1v_1^{-1}\, v_2t_2v_2^{-1} \in C_1C_2,$$

as claimed. □

Corollary 1.5. — *In the situation of Theorem 1.3, assume that T contains a regular element. Then the Ore conjecture holds for G.*

Proof. — Let $t \in T$ be regular and let C_1, C_2 in the previous corollary be the class of t, t^{-1} respectively. Then any element of $G \setminus \{1\}$ is a commutator, and $1 \in G$ trivially is. □

Now note that, given $\mathbf{H}$, $F : \mathbf{H} \to \mathbf{H}$, and a maximally split maximal torus $\mathbf{T} \leqslant \mathbf{H}$ as above, any regular semisimple element $s \in \mathbf{T}$ is F^m-stable for m sufficiently large. Thus there exist regular semisimple elements in T over fields of sufficiently large order. But this field size might vary with the characteristic and with the type of G. So more elaborate arguments are needed to establish a uniform, explicit bound:

Theorem 1.6 (Ellers-Gordeev [EG98]). — *Let G be a finite simple group of Lie type over a field of order at least 9. Then Thompson's and Ore's conjectures hold for G.*

In fact, for most families of groups they obtain an even smaller bound on the field size; for example, they show that Ore's conjecture holds for symplectic groups over fields of order at least 4. Note that this still leaves infinitely many open cases, namely the classical groups of unbounded rank.

In their proof, Ellers-Gordeev use the following factorization result by Lev [Lev94], which is shown by direct computation (a similar, but weaker decomposition statement had been shown by Sourour [So86] in his proof of Thompson's conjecture for $\mathrm{SL}_n(K)$).