BOOK REVIEWS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 17, Number 1, July 1987

0273-0979/87 $1.00 + $.25 per page

Finite groups of Lie type. Conjugacy classes and complex characters, by Roger W. Carter. John Wiley and Sons, Chichester, New York, Brisbane, Toronto and Singapore, 1985, xii + 554 pp., $69.95. ISBN 0-471-90554-2

The finite groups of Lie type are the finite analogues of the reductive Lie groups. The importance of these finite groups for the general theory of finite groups is shown by the classification of finite simple groups, according to which any finite noncyclic simple group which is not an alternating group or one of 26 sporadic groups is a composition factor of some finite group of Lie type.

Among the finite groups of Lie type occur classical groups over a finite field $\mathbf{F}_q$, such as the general linear group $\mathrm{GL}_n(\mathbf{F}_q)$ of all nonsingular $n \times n$ matrices over $\mathbf{F}_q$, the special orthogonal groups, and the symplectic groups over $\mathbf{F}_q$. One encounters such groups in the very beginning of the theory of finite groups: Galois in 1832 knew already the general linear groups over the prime fields. Subsequently, C. Jordan (around 1870) studied classical groups over finite fields. His work was continued by L. E. Dickson (in the beginning of this century). In their work they discussed primarily group-theoretical questions like the description of normal subgroups and of simple composition factors. Their methods were those of linear algebra.

The more recent developments of the theory of finite groups of Lie type can all be viewed as being due to invasions of the theory by other branches of mathematics.

These started in 1955, when C. Chevalley introduced ideas from the theory of complex semisimple Lie algebras. He constructed, for each simple Lie algebra (by a reduction modulo p procedure), a matrix group over $\mathbf{F}_q$, which led to a corresponding finite simple group. These matrix groups have many features in common with semisimple Lie groups. Somewhat later, in the sixties, the insight came that the best way to deal with Chevalley's groups is to view them in the context of the theory of linear algebraic groups. This theory was initiated by A. Borel in 1956 and further developed soon after. One is then led naturally to the use of ideas and methods from algebraic geometry, over fields of characteristic $p > 0$. In that context the definition of a finite group of Lie type is as follows.

Let $\overline{\mathbf{F}}_q$ be an algebraic closure of $\mathbf{F}_q$. An algebraic group over $\mathbf{F}_q$ (briefly: an $\mathbf{F}_q$-group) is a subgroup of some $\mathrm{GL}_n(\overline{\mathbf{F}}_q)$ whose elements are precisely the solutions of a system of polynomial equations in the matrix coordinates, with coefficients in $\mathbf{F}_q$. (Example: an orthogonal group over $\mathbf{F}_q$.) Then G is stable under the Frobenius automorphism F of $\mathrm{GL}_n(\overline{\mathbf{F}}_q)$ with $F((x_{ij})) = (x_{ij}^q)$. The group G^F of fixed points of F in G is a finite group. If G is connected in the Zariski topology (i.e., has no nontrivial algebraic subgroups over $\overline{\mathbf{F}}_q$ of finite index) and reductive (i.e., has no nontrivial connected normal algebraic p-subgroups, where $p = \mathrm{char}(\overline{\mathbf{F}}_q)$), then G^F is a finite group of Lie type. The most general finite group of Lie type is obtained by a slight generalization of this construction.

A key result for the theory of the finite groups G^F is the theorem of Lang (1956) according to which in a connected $\mathbf{F}_q$-group G the map $x \mapsto x(Fx)^{-1}$ of G into itself is surjective. In its applications to group-theoretical questions about G^F the procedure is to work first in G and then descend to G^F by using Lang's theorem.

The notions of the theory of linear algebraic groups (Borel subgroups, maximal tori, Weyl groups, ...) can be used advantageously to gain insight into the structure of finite groups of Lie type. A key notion here is that of BN-pair, or Tits system, introduced by Tits (1961).

In Carter's book the finite groups of Lie type are dealt with from the point of view sketched above. Its first chapter gives a résumé (without proofs) of the relevant facts from the theory of algebraic groups. Chapter 2 deals with BN-pairs. Lang's theorem is crucial for the discussion of conjugacy classes and centralizers in the groups G^F. These matters come in the next three chapters of the book. In particular, Chapter 5 gives a quite thorough discussion of the existing results about the difficult unipotent conjugacy classes (of elements whose eigenvalues are all equal to one), in reductive groups over arbitrary algebraically closed fields. Also, Chapter 13 gives a great deal of explicit data and tables about these classes. Carter's comprehensive discussion of unipotent classes is a very welcome addition to the literature, which makes the results more accessible.

The central topic of the book is the complex character theory of finite groups of Lie type. The interest in characters of such groups dates from the beginnings of character theory. In Frobenius's first paper on group characters (1896) he already determines the irreducible characters of the finite groups $\mathrm{PSL}_2(\mathbf{F}_p)$ of fractional linear transformations of the prime fields $\mathbf{F}_p$. Somewhat later, I. Schur dealt with the groups $\mathrm{SL}_2(\mathbf{F}_q)$. A much later substantial result is J. A. Green's determination of the irreducible characters of the finite groups $\mathrm{GL}_n(\mathbf{F}_q)$ (1955).

Some special irreducible characters of a general group of Lie type were discovered, notably the Steinberg character (Steinberg, 1956). Later, Harish-Chandra (1970) noticed that ideas and notions which first appeared in connection with real Lie groups and their infinite-dimensional representations (cuspidal characters, parabolic induction) could be used to bring some order in the set of irreducible characters of a finite group of Lie type. The results and constructions alluded to in this paragraph are of an "elementary" nature. They are discussed in Chapters 6, 9, 10 of Carter's book.

The elementary methods were (and are still) not powerful enough to achieve a construction of all irreducible characters of a general finite group of Lie type. The decisive progress in character theory—which does lead to such a construction—was made by P. Deligne and G. Lusztig (1976), when they introduced the methods and results from algebraic topology of algebraic varieties over finite fields, namely from l-adic cohomology (created by Grothendieck in the sixties). Their idea is to construct suitable algebraic varieties X over $\mathbf{F}_q$ on which a finite group G^F operates. One then obtains linear representations of G^F in the cohomology groups of X (with coefficients in an appropriate algebraically closed field of characteristic 0). An example of such a variety, for $G^F = \mathrm{GL}_n(\mathbf{F}_q)$, is the set of $x = (x_1, \ldots, x_n) \in (\overline{\mathbf{F}}_q)^n$ with

$$\det\left(x_j^{q^{i-1}}\right)_{1 \leqslant i,j \leqslant n} = 1.$$

The constructions of Deligne and Lusztig give virtual characters of a finite group of Lie type G^F, with good properties. In particular, any irreducible character of G^F is a constituent of Deligne-Lusztig character. To establish these properties, all the resources of algebraic topology have to be exploited.

The construction of the Deligne-Lusztig characters and a discussion of their properties are contained in Chapters 7, 8, 9 of Carter's book. The basic properties of the l-adic cohomology groups with proper support are given as axioms in Chapter 7 and the basic properties of the Deligne-Lusztig characters are deduced from those axioms. This is a sensible procedure. (An appendix to the book gives a bit more information about l-adic cohomology.) The discussion of the Deligne-Lusztig characters is the core of the book and it is quite well presented.

In more recent work, Lusztig has succeeded in describing the decomposition of the Deligne-Lusztig characters into irreducibles. The later chapters of the book can be viewed as an introduction to this work, not aiming at completeness. For example, the discussion of the all-important unipotent characters in Chapter 12 is sketchy.

Lusztig's work, mentioned above, can be found in his book *Characters of finite groups of Lie type* (1984). It exploits yet another, more recent, resource in algebraic topology, namely intersection cohomology. He obtains there a parametrization of the irreducible characters of a finite group of Lie type G^F, assuming the center of G to be connected. In still more recent work he has obtained a full description of the character table of a finite group of Lie type (under some mild restrictions).

To a diehard algebraist it may seem disturbing that in order to solve a concrete problem like the determination of the character table of an orthogonal group over a finite field, one has to invoke arcane theories such as l-adic cohomology and intersection cohomology (this is the present situation). This reviewer believes that, whatever simplifications the future might bring, the insights brought by these theories are there to stay. (One of these insights is that subtle phenomena in representation theory are tied up with the geometry of Schubert varieties and similar varieties.)

Carter's book contains a very good introduction to the present state of affairs and can be warmly recommended to anyone who is interested in penetrating into the highly interesting domain of finite groups of Lie type. The book has an extensive bibliography.

T. A. SPRINGER

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 17, Number 1, July 1987

0273-0979/87 $1.00 + $.25 per page

The arithmetic of elliptic curves, by Joseph H. Silverman, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, Berlin, Heidelberg and Tokyo, 1986, xii + 400 pp., $48.00. ISBN 0-387-96203-4

The arithmetic (= diophantine theory) of curves of genus 0 is now very well understood. That of curves of genus > 1 is still in a rudimentary and unsatisfactory state. For curves of genus 1 there is a large body of established theory and an even larger body of interrelated conjecture: the whole being currently in a state of exciting development.

We work over a ground field k, which may be the rationals $\mathbf{Q}$, or e.g., a global or local field. An elliptic curve defined over k consists of a curve of genus 1 together with a point 0 (say) on it, both defined over k (we shall often say "rational" instead of "defined over k"). Here we encounter our first puzzle. There is no known algorithm for deciding (e.g., when $k = \mathbf{Q}$) whether there is a rational point on a given curve of genus 1 or not: in particular there is no Hasse principle (local-global principle). However, to every curve of genus 1 there is associated in a canonical way an elliptic curve over the same ground field (its jacobian, a generalization of the notion from algebraic geometry). The theory of curves of genus 1 thus largely reduces to that of elliptic curves.

The points of an elliptic curve have a natural structure as an abelian group, the given point 0 being the neutral element ("zero") of the group. In fact the elliptic curves over a field k are precisely the abelian varieties of dimension 1 over k. In particular the set of rational points has a natural abelian group structure. When $k = \mathbf{Q}$ a famous theorem of Mordell states that this group is finitely generated. This result was generalized by Weil and others and the group is usually called the Mordell-Weil group (for the given elliptic curve and ground field). There is, however, as yet no algorithm for determining the Mordell-Weil group, though this can usually be done in specified cases. The absence of an algorithm here is closely associated with the failure of the Hasse principle mentioned above. The "obstruction" to the Hasse principle is encapsulated in a group discovered independently by Tate and Shafarevich and called the Tate-Shafarevich group. It has many interesting properties, both proved and conjectural. Without doubt the reviewer's most lasting contribution to the theory is the introduction of the cyrillic letter Ш ("sha") to denote this group, a usage which has become universal.