justifies . . . those things which, up till now, have merely been 'Adhockeries for mathematical convenience'."

The two volumes do not have a bibliography because this had been provided in (0). Since Koopman's work (1957) on probability in quantum mechanics is cited in (I, p. 15) and (II, p. 303), I mention that it was not a book, but a chapter in the Proceedings of a Symposium. Also Ramsey's initials were not FDR though he might have made a good philosopher king. On a point of terminology, "Bayesian estimation interval" would be better than "Bayesian confidence interval" (II, p. 244), which sounds too much like a square circle. When "Bayesian" is dropped, the confusion is apt to be further increased.

On p. 225 of (I) de Finetti discusses decimals with missing digits, or with digits having the "wrong" frequencies, and he seeks a bibliographical reference. One such is *Proc. Cambridge Philos. Soc.* **37** (1941), p. 200, where the reviewer conjectured a relationship between entropy and the Hausdorff-Besicovitch dimensionality of such sets, a relationship that was proved by Eggleston in 1949. Hausdorff-Besicovitch dimensionality could be used to enrich de Finetti's theoretical discussion of "levels" of zero probability (I, §3.11).

In summary, these volumes make important writings of this pioneer available to the English-reading world, and will encourage some probabilists, statisticians, and philosophers of science to learn Italian.

I. J. Good

BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 83, Number 1, January 1977

Presentation of groups, by D. L. Johnson, London Mathematical Society Lecture Note Series, no. 22, Cambridge Univ. Press, New York and London, 1976, v + 204 pp., $11.95.

Given a set X there exists a free group F having X as a basis; the elements of F are all *words* in X, that is, all formal products $x_1^{e_1} \cdot \ldots \cdot x_n^{e_n}$, where $x_i \in X$ and $e_i = \pm 1$. The set X is called a basis of F because it behaves very much as a basis of a vector space does: given any function φ: $X \to G$, where G is an arbitrary group, there is a unique homomorphism $\tilde{\varphi}$: $F \to G$ extending φ. An immediate consequence of the existence of free groups is the theorem that every group G is a quotient group of a free group. If X is the underlying set of G and φ: $X \to G$ is the identity, then $\tilde{\varphi}$ is a homomorphism of F onto G, where F is free with basis X; if R is the kernel of $\tilde{\varphi}$, then $F/R \cong G$. One knows that every subgroup of a free group is itself free, so that R is free on some basis Y' comprised of certain words in X, and, obviously, Y' generates R. Since R is a normal subgroup of F, however, one may describe R by a smaller set of words than Y', namely, a set Y that generates R as a normal subgroup of F (in building R from Y, one may not only form words in Y, he may also form words in conjugates fyf^{-1} for $f \in F$). These two sets of words X and Y describe F and R completely, hence describe $G = F/R$. $\langle X | Y \rangle$ is called a *presentation* of G (note that G has many presentations!), the set X is called a set of *generators*, and the set Y is called a set of *relations*.

We now reverse the procedure. Rather than starting with a known group G and finding presentations of it, let us now begin with a presentation $\langle X | Y \rangle$ and ask what information we can extract about the corresponding group. This question is the subject of what is now called "Combinatorial Group Theory". We note at once that this question is not merely "of intrinsic interest". In practice, a group is often given by a presentation, and this is how one must deal with it. For example, this may be the most convenient description of the fundamental group of a polyhedron (knot groups are such groups).

The first question one might pose is whether every word in $G = \langle X | Y \rangle$ has a canonical form; can we determine when two words in X describe the same element of G? This is clearly equivalent to asking if we can determine whether an arbitrary word in X is the identity element in G. This last question is called the "word problem" for G. Even in the most favorable instance when both X and Y are finite (G is then called *finitely presented*), this question is undecidable in the precise sense of the logicians (Boone and Novikov, independently, proved this in the late 1950s). Even worse, the crude question–what is the order of G?–is also impossible; it is undecideable whether an arbitrary finite presentation describes the trivial group of order 1. As the author says in his introduction, every successful description of a group G from some presentation of G "is a triumph over nature".

Faced with the negative results above, one is forced to retreat to less ambitious questions. Are there "nice" presentations that are manageable? What properties of G can be determined from some presentation of it? An important such theorem is due to Magnus: if G has a presentation with one relator (the set Y of relations is a singleton), then G has a solvable word problem. Fundamental groups of compact surfaces are of this type. Another important, related result about one-relator groups is the "Freiheitsatz"; if the relator y involves $x_1, \ldots, x_n$ ($x_i \in X$) (and y is "cyclically reduced"–a simple but technical adjective we will not define), then every subgroup of G generated by a proper subset of $\{x_1, \ldots, x_n\}$ is free with that subset as basis. A third beautiful theorem is due to G. Higman: What are the subgroups of finitely presented groups? Answer: A group G that is finitely generated is a subgroup if and only if it has a presentation whose set of relations can be given by an algorithm. Less spectacular results are of the form: here is a presentation of, say, the generalized quaternions; we may tinker with it to actually prove it defines a group of order 2^n (the negative theorems say such results are impossible for arbitrary presentations; man may triumph over particular presentations). If one cannot determine the order of G from a presentation, can one determine whether it is finite? Indeed, it is this question that the book under review really cares about. Now there are two major results along these lines, one treated, the other not. The untreated theorem is the very difficult solution of *Burnside's problem*: Is every finitely generated group G in which $x^n = 1$ for all $x \in G$ (where n is a fixed positive integer) necessarily finite? The problem originated when Burnside proved that G is finite if, in addition, one assumes it has a faithful complex representation, that is, G is a subgroup of $m \times m$ nonsingular complex matrices for some m.

Adjan and Novikov proved in 1970 that if n is odd and sufficiently large, then G may be infinite. There are still some interesting open questions here; for example, if one assumes that G is finitely presented, not merely finitely generated, must G be finite? The second major result solves a variant of Burnside's problem. Suppose one replaces the hypothesis "$x^n = 1$ for all $x \in G$" by the hypothesis "every element in G has finite order". (Of course, infinite such groups exist, for we have relaxed the Burnside hypothesis–we do not demand a uniform bound on the orders of elements.) In 1964, antedating Adjan and Novikov, it was shown by Golod and Šafarevič that there exist infinite finitely generated p-groups for any prime p. Their results simultaneously solved the "Classfield Tower" problem of number theory as well as an open problem of Kuroš in ring theory! Although the original proof of Golod and Šafarevič uses homological algebra, there now exist nonhomological proofs. The author chooses to follow a homological approach due to Roquette, and develops from scratch all necessary machinery. The basic idea is to find a "minimal" presentation of a finite p-group G, and interpret the number of generators and number of relations as dimensions of certain cohomology groups. The Burnside basis theorem asserts that any two minimal generating sets of G have the same size, say, $d(G)$. If we let k denote the field of integers modulo p, one observes that the cohomology groups $H^i(G, k)$ are finite-dimensional vector spaces over k and that $d(G) = \dim H^1(G, k)$. Next, if we define $r(G) = \dim H^2(G, k)$, then one proves that any presentation of G needs at least $r(G)$ relators. The Golod-Šafarevič Theorem says: If G is a nontrivial finite p-group, then

$$4r(G) > d(G)^2.$$

The tale ends by exhibiting a finitely generated p-group G having a presentation violating the above inequality (where now $r(G)$ and $d(G)$ are just dimensions of suitable cohomology groups); such a group G must be infinite. Johnson does prove the Golod-Šafarevič inequality; unfortunately, he does not give the example that violates it (an example may be found in Herstein's book, *Noncommutative rings*, Carus Monograph 15).

There are, of course, other weapons available to a combinatorial group theorist: Cayley diagrams, coset enumeration (Todd and Coxeter), Reidemeister rewriting process, free differential calculus (Fox), Tietze transformations, Tartakovskiĭ method, small cancellation theory, geometric interpretations of this theory (Lyndon and Schupp), and more.

This book is a lively introduction to Combinatorial Group Theory; it is clearly written and it has many examples and exercises. The author has succeeded in whetting the appetites of young graduate students by feeding them an excellent meal (Golod-Šafarevič) that includes several pleasant side dishes (groups with equal numbers of generators and relations, wreath products, and cyclically presented groups). In order to continue the feast and experience a more varied menu, the students are advised to consult the delicious books listed in its bibliography.

JOSEPH ROTMAN