The latter is applied to the study of "ordinary" invertibility as well as "algebraic" invertibility in Banach algebras, and "essential" invertibility in the context of compact operators and Fredholm theory.

This book contains a wealth of material. There is a comprehensive set of exercises, carefully chosen to illustrate points in the main text and a large bibliography. It should prove invaluable both to the beginning graduate student in functional analysis and to the more experienced researcher looking for a readable account of the more specialised topics mentioned above.

H. R. DOWSON

KAROUBI, M. and LERUSTE, C., *Algebraic topology via differential geometry* (London Mathematical Society Lecture Note Series 99, Cambridge University Press 1987) 363 pp. 0 521 31714 2, £15. (Originally published in French as *Méthodes de géométrie différentielle en topologie algébrique*, Paris 1982.)

There are a number of topics in algebraic topology one might present in a first course, homology and cohomology of simplicial/CW complexes and/or manifolds being a particularly attractive option. Usually the approach is via simplicial or singular homology: each has its advantages and problems. The volume under review takes a third path; it is a presentation of the de Rham cohomology (DRC) of smooth manifolds.

This path too has its own strengths and weaknesses. On the positive side the algebraic formalism required (tensor calculus, exterior algebra) is fairly minimal and of general geometric interest anyway, a good investment for the prospective student. The resulting cohomology group has a *natural* multiplicative structure furnished by the wedge product. Most importantly this setting allows a fruitful interplay between topological and differential-geometric ideas. This interplay has been valued and used by many of the great geometers, Poincaré, E. Cartan, de Rham, H. Cartan, Weil, Thom and Whitney amongst them. However, from the mid-fifties until more recent times, differential forms were set aside in favour of more topological methods. Now, work of Quillen and especially Sullivan in the seventies has led to a new interest in the use of differential forms in topology.

The DRC also has its disadvantages. To my mind differential forms are a good deal less intuitive than simplicial (or even singular) chains, and of course, torsion phenomena are undetected by these cohomology groups, although the authors note that the modern presentation of DRC following Sullivan and others yields this richer structure.

Now to the book itself. As an introduction to DRC it is quite excellent. The treatment is self-contained and gives full details, full proofs—one could happily use this as a reading course for first-year postgraduate students. Prerequisites are very few; the book develops all the exterior algebra from scratch in the first chapter (30 pages), discusses differential forms on open subsets of $\mathbb{R}^n$ next (40 pages), and then gives a nice introduction to differentiable manifolds, producing a large number of significant examples: the spheres, projective spaces, classical groups, Stiefel and Grassmann manifolds (50 pages). So we are a third of the way through the book before meeting DRC, but I find this all to the good; the knowledgeable can skip these sections but they will prove invaluable to a beginning postgraduate.

Chapter IV gives the formal definitions and basic properties of DRC and Chapter V shows how one can compute these groups (computability is the key advantage of homology/cohomology). Computation takes place via the Mayer–Vietoris sequence, a simple version of the Künneth theorem is given and the DRC of spheres and complex projective spaces is computed. Fairly standard applications follow—Brouwer's fixed-point theorem and invariance of domain, Hopf's theorem concerning H-spaces.

Chapter VI deals with Poincaré duality for oriented manifolds; duality here is set up by integrating the wedge product of forms of complementary dimension. Various applications are given (including a determination of the multiplicative structure of the cohomology of complex

https://doi.org/10.1017/S0013091500028790 Published online by Cambridge University Press

projective space). The Künneth formula is then dealt with in full generality and as a major final application the authors prove the Lefschetz fixed-point theorem. Along the way the rèader learns about tubular neighbourhoods, the Gysin homomorphism, the Thom isomorphism and useful homological algebra is introduced as it is needed. The final chapter finishes off with a section entitled "Complements and problems", which gives a tantalizing glimpse of characteristic classes and many other nice topics. The book concludes with two appendices, the first giving a proof of Stoke's theorem, while the second presents in a "modern" way the Chern character and Chern classes of bundles. Indeed characteristic classes are defined for projective modules of finite type over certain algebras. The results are due to Karoubi and Connes, and are less accessible than the rest of the text. The book is reproduced from a clear and well-prepared typescript; I found few typing errors, and the translation is excellent (though the author's use of "notorious" for well-known, rather than unfavourably known, while correct, seems strange).

A very nice introduction to an important topic—I recommend it.

J. W. BRUCE

WELSH, D., *Codes and cryptography* (Clarendon Press, Oxford 1988) xii+257 pp, cloth: 0 19 853288 1, £35, paper: 0 19 853287 3, £13.95.

The explosive growth of information technology over the last decade or so has produced a corresponding interest in theoretical problems spawned by this growth. Foremost amongst such problems of interest to mathematicians are coding problems: how to encode your given source data into a (usually binary) form suitable for storage or transmission. Techniques for doing this depend very much on what purpose the codes are required to serve. There are ciphers for secrecy, error-control codes to protect against message corruption, data-compression codes to squeeze as much information as possible into each bit, and so on. Each has its own largely separate body of theory.

Welsh's *Codes and Cryptography* gives us a solid basic introduction to all these kinds of codes. He also describes the related areas of information theory, natural language, and complexity of algorithms, and how they connect with various aspects of coding. This brings us to one of the great strengths of the book: the breadth of the foundation which he builds for the subject. He manages to do this without ever being superficial in any area, so that one is confident one has been told the essentials. While this is a substantial achievement, it is done at the same time in a clear and straightforward style, conveying the information (without secrecy, corruption or compression!) transparently from page to reader.

As a bonus, the author has little-known gems scattered throughout the book. Those of us who didn't know of Aeneas Tacticus' (360 BC) cryptosystem using the knucklebone of a sheep, or of E. V. Wright's 250 page novel *Gadsby* which contains no letter 'e', can take great delight in these. I leave you to find others while you read this excellent introduction to codes and cryptography.

C. J. SMYTH

https://doi.org/10.1017/S0013091500028790 Published online by Cambridge University Press