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 reader 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