Book Review

Rings and Fields

Graham Ellis

Oxford University Press 1992, 169pp.

ISBN 0-19-853455-8

Reviewed by Des MacHale

When I was an undergraduate, there was very little choice of texts in algebra. Archbold's *Algebra* and Herstein's *Topics in Algebra* were our standard texts and for consultation we used Birkhoff and Mac Lane, van der Waerden and sometimes Jacobson. That was more or less it. Modern students are almost spoiled for choice and in recent times there has been a great variety of excellent texts in algebra, beautifully produced and with a wealth of exercises and examples. Among these we might mention books by Allenby, Dubkin, Fraleigh, McCoy, Lidl/Pilz, and Gallian.

Now a new algebra text comes to join the ranks, *Rings and Fields* by Graham Ellis, reflecting many of the changes in emphasis in algebra that have happened over the last twenty years. All of the traditional core topics are still there of course –Euclidean domains, primitive and cyclotomic polynomials, finite fields, ruler and compass constructions, solvability by radicals, Wedderburn's theorem, Galois groups, and an introduction to groups as far as solubility, but now modern students are exposed to topics of more recent interest and indeed to the exciting prospect of actually **applying** abstract algebra, a concept unheard of when I was an undergraduate. Thus Graham Ellis's book has sections and indeed sometimes whole chapters on such areas as diophantine equations, projective planes, error correcting codes, cryptography, elliptic curves and factorization of large integers.

For those who teach courses including such topics, *Rings and Fields* will be very valuable indeed. The pace is leisurely, the exposition clear and there are many geometric diagrams to illustrate what is going on. I found the chapter on error correcting codes particularly good and (shame on me!) felt I understood for the first time what was going on and I have no doubt that the undergraduates I teach would understand it as well.

The book has a strong geometric flavour and the section linking the theorems of Pappus and Desargues via Wedderburn's theorem is particularly valuable–this is material that every mathematician should be familiar with. The chapter on cryptography (unfortunately called 'cryptography' in the Contents), elliptic curves and factorization is exciting and should stimulate students to explore the foothills of the recent proof of Fermat's Last Theorem.

Any reservations? Well, no book is perfect (unless written by the reviewer!), so I feel that it is important to list ways in which the current book could be improved for the future editions that it definitely deserves to have. Any mathematical undergraduate that I have spoken with over the past thirty years felt that every course and every text could do with more examples and solved problems and *Rings and Fields* could certainly benefit from more of these – its modest length of 169 pages could tolerate some extension. More exercises too would be welcome and by more, I mean hundreds more! These could range from the very easy to the very difficult and preferably starred à la Herstein.

As a group theorist I suppose that I was a bit saddened to see groups relegated to Chapter 8 as an afterthought to Galois groups, but then this is a text on rings and fields; but just six exercises on groups is a bit mean–I give my students over 500, though most of these are just for the record.

Overall though, *Rings and Fields* is a fine text, very clear and very well written, a very welcome addition to the literature of algebra, which should be on the shelf of every mathematician and in the possession of very mathematical undergraduate worthy of the name. It is beautifully produced and virtually free from misprints and is undoubtedly user friendly for students. Maybe future editions will be even better.

Des MacHale,
Department of Mathematics,
University College, Cork.