

## WEDDERBURN'S THEOREM REVISITED

*Des MacHale*

One of the most delightful results in ring theory is the following theorem of J.M. Wedderburn (1905).

**THEOREM** *A finite division ring is a field.*

Besides being important in algebra, Wedderburn's theorem also finds applications in geometry. For example, it provides the only known proof that in a finite geometry the configuration of Pappus is implied by that of Desargues. Herstein's TOPICS IN ALGEBRA can be recommended for its proofs and discussion of Wedderburn's theorem.

The purpose of this note is to prove the following result:

**THEOREM** *Let  $R$  be a finite ring with unity and let  $T$  be the set of invertible elements of  $R$ . If  $|T| > |R| - \sqrt{|R|}$ , then  $R$  is a field.*

Thus, where Wedderburn's hypothesis demands that  $|T|=|R|-1$  to force the conclusion that  $R$  is a field, we demand only that  $|T| > |R| - \sqrt{|R|}$  to force the same conclusion. In a sense, our result is the best possible. Consider the ring  $R$  of residue classes mod  $p^2$ , for any prime  $p$ . This ring has exactly  $\phi(p^2) = p^2 - p = |R| - \sqrt{|R|}$  invertible elements, but  $R$  is clearly not a field.

To prove our theorem we need a number of elementary lemmas. Some of these are well-known but we include proofs for convenience. We let  $R$  be a finite ring with unity  $1 \neq 0$ . A left zero divisor is an element  $x \in R$  such that  $xy = 0$  for some  $y \in R$ ,  $y \neq 0$ . A right zero divisor is an element  $x \in R$  such that  $yx = 0$  for some  $y \in R$ ,  $y \neq 0$ . In particular,  $0$  is a left zero divisor and a right zero divisor.

**LEMMA 1** *For  $b \in R$ , if  $b^n$  is a left (resp. right) zero divisor for some  $n \geq 1$ , then  $b$  is a left (resp. right) zero divisor.*

**PROOF** Choose  $n > 1$  minimal such that  $b^n$  is a left zero divisor and let  $t \neq 0$  satisfy  $b^n t = 0$ . Then  $b(b^{n-1}t) = 0$  implies that  $b$  is a left zero divisor, since  $b^{n-1}t \neq 0$ . A similar proof applies for right zero divisors.

**LEMMA 2** *If  $b \in R$ , then either  $b$  is invertible or  $b$  is both a left and right zero divisor.*

**PROOF** Since  $R$  is finite there exist  $i, j \in \mathbb{N}$  with  $b^{i+j} = b^i$ . Thus  $b^{i+j} - b^i = b^i(b^j - 1) = (b^j - 1)b^i = 0$ .

Thus, either  $b^j = 1$  or  $b^i$  is a left and right zero divisor. If  $b^j = 1$  then  $b$  is invertible, and the alternative possibility implies that  $b$  is both a left and right zero divisor by lemma 1.

The key lemma is originally due to the Ganesan [1]. We prove a slightly modified version suitable for our needs.

**LEMMA 3** *Suppose that  $R$  has  $n > 1$  left divisors of zero. Then  $|R| \leq n^2$ .*

**PROOF** By lemma 2,  $R$  has precisely  $n > 1$  right zero divisors also. For  $x \in R$ , let  $A(x) = \{r \in R \mid xr = 0\}$ . Since  $R$  has  $n$  right zero divisors and  $n > 1$ , there exists  $x \in R$ ,  $x \neq 0$  such that  $1 < |A(x)| \leq n$ . Let  $y \neq 0$  be an element of  $A(x)$ . Then  $|yR| \leq n$ , since  $yR \subseteq A(x)$  because  $x(yr) = (xy)r = 0$ .

Now consider the groups  $\{R, +\}$  and  $\{yR, +\}$ . Define a function  $f : R \rightarrow yR$  by  $f(r) = yr$ , for all  $r \in R$ . By the left distributive law,  $f$  is a homomorphism from  $R$  onto  $yR$ . The kernel of  $f$  is  $\{r \in R \mid yr = 0\} = A(y)$ , so  $R/A(y)$  and  $yR$  are isomorphic as Abelian groups. In particular,

$$|R| = |A(y)| |yR| \leq n \cdot n = n^2, \text{ as claimed.}$$

We can now prove the stated theorem. Let  $D$  be the set of (left and right) zero divisors of  $R$  and suppose that  $|T| > |R| - \sqrt{|R|}$ . Since no zero divisor is invertible, lemma 2 implies that  $|T| + |D| = |R|$ . If  $D = \{0\}$ , then  $|T| = |R| - 1$ , so  $R$  is a field by Wedderburn's theorem. Otherwise, let  $|D| > 1$ . The conditions of lemma 3 are satisfied, so  $|R| \leq |D|^2$  and  $\sqrt{|R|} \leq |D|$ . However, combining  $|T| > |R| - \sqrt{|R|}$  and  $|T| = |R| - |D|$ , we get  $\sqrt{|R|} > |D|$ , which is a contradiction. This establishes the theorem.

#### REFERENCE

1. GANESAN, N.  
"Properties of Rings with a Finite Number of Zero Divisors II", *Math. Annalen* 161 (1965) 241-246.

#### ACKNOWLEDGEMENT

I wish to thank Pat Fitzpatrick for his help in streamlining the presentation of this paper.

*Mathematics Department,  
University College,  
Cork.*

## CAREERS FOR GRADUATES IN MATHEMATICS

*Nicholas Leonard*

This article is based on a talk given earlier this year to staff of UCC's Mathematics Department. It gives an account of the careers open to graduates who have followed degree programmes in mathematical disciplines including information on the actual first destinations of Irish and UK graduates and looks at the broader career horizons open to numerate graduates with the ability to think logically and quantitatively.

### 1. CAREER OPTIONS - AN OVERVIEW

In recent years graduates in Mathematical disciplines have fared better than most graduates entering a difficult employment market. This is because the quality of numeracy is increasingly important in a wide range of careers and also because their specific skills in mathematics, statistics or computer science are in demand in industry and commerce - particularly in engineering, computing and finance.

This first section looks at the careers for which a Mathematics-based degree is either required or particularly appropriate.

#### Teaching and Lecturing

The cuts in post-primary education expenditure in early 1983 resulting in a deterioration in staff/student ratios had an immediate effect on job prospects for newly qualified teachers of all subjects. However the number of arts and science graduates entering teacher training is falling steadily so the determined graduate with the right personal qualities for