

UCC Library and UCC researchers have made this item openly available.
Please [let us know](#) how this has helped you. Thanks!

Title	When is a finite ring a field?
Author(s)	MacHale, Desmond
Publication date	1996-12
Original citation	MacHale, D. (1996) 'When is a Finite Ring a Field?', Bulletin of the Irish Mathematical Society, 37, pp. 35-38.
Type of publication	Article (peer-reviewed)
Link to publisher's version	http://www.irishmathsoc.org/bull37/index.php Access to the full text of the published version may require a subscription.
Rights	© 1996 Irish Mathematical Society
Item downloaded from	http://hdl.handle.net/10468/9608

Downloaded on 2022-05-22T19:32:57Z



UCC

University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

$k = l = m = 0$. Therefore C has order 8, in which case $C = R$. Therefore the commutator subset of a ring of order 8 is an ideal. We conclude that 16 is the smallest order of a ring in which the commutator subset is not an ideal.

Acknowledgement The author is grateful to P. D. MacHale for several discussions on the topic of this note.

References

- [1] B. Fine, *Classification of finite rings of order p^2* , Mathematics Magazine 66 (1993), 248-252.
- [2] C. R. Fletcher, *Rings of small order*, Mathematical Gazette 64 (1980), 9-22.

T. Creedon,
Department of Mathematics,
University College,
Cork.

WHEN IS A FINITE RING A FIELD?

Des MacHale

When I was an undergraduate, there were two theorems in algebra that took my fancy. The first was

Theorem 1. *A finite integral domain is a field.*

The second was the beautiful theorem of Wedderburn (1905).

Theorem 2. *A finite division ring is a field.*

I often wondered why the standard proof of Theorem 1 was relatively easy and why all of the proofs of Theorem 2 are relatively difficult. I wondered too if it might be possible to prove a single theorem that would include both Theorem 1 and Theorem 2 as special cases. The following is an attempt in that direction.

Theorem 3. *Let $\{R, +, \cdot\}$ be a finite non-zero ring with the property that if a and b in R satisfy $ab = 0$, then either $a = 0$ or $b = 0$. Then $\{R, +, \cdot\}$ is a field.*

Recall that $\{R, +, \cdot\}$ is an integral domain if $\{R, +, \cdot\}$ is a commutative ring with unity $1 \neq 0$ with the property that $ab = 0$ implies either $a = 0$ or $b = 0$. Clearly, a finite integral domain satisfies the hypothesis of Theorem 3.

Recall too that a division ring $\{R, +, \cdot\}$ is a ring in which the non-zero elements of R form a multiplicative group with unity 1. A finite division ring $\{R, +, \cdot\}$ also satisfies the hypothesis of Theorem 3. To see this, suppose that for elements a and b of R , we have $ab = 0$. If $a = 0$, we are finished, so suppose that $a \neq 0$. Then a^{-1} exists in R . Hence $b = 1b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$, as required. Note finally that in the hypothesis of Theorem 3,

we are assuming neither commutativity of multiplication, nor the existence of inverses. These have all to be established.

Proof of Theorem 3: Since $R \neq \{0\}$, we can choose a fixed non-zero element a of R . Let

$$R = \{r_1, r_2, \dots, r_n\}.$$

Define a function $\alpha : R \rightarrow R$ by

$$(r_i)\alpha = r_i a$$

for all i . Now if $(r_i)\alpha = (r_j)\alpha$, then $r_i a = r_j a$ and hence $(r_i - r_j)a = 0$. Since $a \neq 0$, this forces $r_i = r_j$, so α is one-to-one, and since R is finite, α is onto. Thus there exist elements t and t^* in R such that

$$ta = a \text{ and } t^*a = t.$$

Now define a function $\beta : R \rightarrow R$ by

$$(r_i)\beta = ar_i$$

for all i . Again, if $(r_i)\beta = (r_j)\beta$, then $ar_i - ar_j = 0 = a(r_i - r_j)$, so $r_i = r_j$. Thus β is one-to-one, hence onto, and there exist elements s and s^* in R such that

$$as = a \text{ and } as^* = s.$$

Now let x be any element of R . Since α and β are onto, there exist elements b and c in R such that

$$x = ba = ac.$$

We now have

$$tx = t(ac) = (ta)c = ac = x,$$

so t is a left unity for $\{R, +, \cdot\}$. Similarly,

$$xs = (ba)s = b(as) = ba = x,$$

so s is a right unity for $\{R, +, \cdot\}$. Thus $t = ts = s = 1$ is a unity for R .

Now as $as^* = s = 1 = t = t^*a$, it follows that a has a right inverse s^* and a left inverse t^* . Thus

$$s^* = 1s^* = (t^*a)s^* = t^*(as^*) = t^*1 = t^*,$$

so $s^* = t^* = a^{-1}$ and we see that each non-zero element a in R is invertible in R . Thus R is a finite division ring and hence by Wedderburn's theorem, R is a field. This completes the proof. ■

Of course, the theory now proceeds to show that $|R| = p^n$ for some prime p and positive integer n and if $R_1 = |R_2| = p^n$, then R_1 and R_2 are both isomorphic to the unique Galois field $\text{GF}(p^n)$, a rather remarkable result given the innocent looking hypothesis of Theorem 3.

Finally, we mention three other directions in which Wedderburn's theorem can be strengthened.

Theorem 4. [1] Let $\{R, +, \cdot\}$ be a finite ring with unity $1 \neq 0$ such that more than $|R| - \sqrt{|R|}$ elements of R are invertible. Then $\{R, +, \cdot\}$ is a field.

The example $\{\mathbb{Z}_{p^2}, \oplus, \odot\}$ for a prime p shows that this result is best possible.

Theorem 5. [2] Let $\{R, +, \cdot\}$ be a finite ring with unity $1 \neq 0$ in which every non-zero ring commutator $xy - yx$ is invertible. Then $\{R, +, \cdot\}$ is commutative.

Of course, $\{R, +, \cdot\}$ need not be a field, as $\{\mathbb{Z}_4, \oplus, \odot\}$ shows.

Theorem 6. [3] Let $\{R, +, \cdot\}$ be a finite non-zero ring and suppose that for each $a \neq 0$ there exists a unique b with $aba = a$. Then $\{R, +, \cdot\}$ is a field.

References

- [1] D. MacHale, *Wedderburn's theorem revisited*, Bull. IMS 17 (1986), 44-46.
- [2] D. MacHale, *Wedderburn's theorem revisited (again)*, Bull. IMS 20 (1988), 49-50.

- [3] N. H. McCoy, *The Theory of Rings*. Macmillan: New York, 1964.

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

A RE-ANALYSIS OF BESSEL'S ERROR DATA

A. Kinsella

Introduction

The Gaussian (Normal) probability model

$$f(x; \mu, \sigma) = \frac{\exp(-(x - \mu)^2 / 2\sigma^2)}{\sigma(2\pi)^{1/2}}$$

is, arguably, the most widely used probability model because of

1. the fact that it is found as a limiting form of other common probability models;
2. the operation of the Central Limit Theorem which gives rise to the Gaussian form;
3. the intuitive appeal of the model as a description of measurement errors in that it postulates that, in the long run, measurements will zone in on the "true but unknown" quantity of interest, μ , and will be close to this value, lying between $(\mu - \sigma)$ and $(\mu + \sigma)$ some 68% of the time;
4. the mathematical tractability of linear and quadratic functions of Gaussian random variables which are used in Student's t and F ratio tests;
5. the ability of the model to readily change location and shape because of the independence of μ , the location parameter, and σ , the shape parameter.

A simple transformation of the random variable, namely,

$$y = |x|$$