COMMUTATORS IN RINGS

T. Creedon

Abstract We exhibit with proof a ring of minimal order in which the commutator subset is not a subring.

Introduction

It is well known that the product of two commutators in a group need not be a commutator. However the smallest order of a group in which this occurs is 96. We produce an example of a ring of order 16 in which the subset of all commutators is not a subring. We prove that this example is minimal by showing that in all rings of order less than 16 the subset of all commutators is an ideal and therefore also a subring. Throughout this paper $\mathbf{Z}_2$ denotes the field of integers modulo 2, C_p denotes the cyclic group of order p and $\langle a \rangle$ denotes the additive group generated by an element a. The commutator of two elements a and b in a ring is denoted $[a,b] = ab - ba$. A presentation for a finite ring R consists of a set of generators $g_1, \ldots, g_k$ of the additive group of R together with relations which specify the additive order of the generators and the multiplication with which R is endowed. For example $\langle a : 2a = 0, a^2 = a \rangle$ is a presentation for Z_2 and we write $\mathbf{Z}_2 = \langle a : 2a = 0, a^2 = a \rangle$.

Example

Consider the ring R of order 16 consisting of all 2×2 matrices with entries in $\mathbf{Z}_2$,

$$R = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

where a, b, c and d run over the elements of $\mathbf{Z}_2$. By direct calculation, we find that the commutator subset C of R consists of the

following eight matrices

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

We remark that C is an additive subgroup of R. However, since

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \notin C,$$

we see that C is not closed under multiplication and so C is not a subring of R and hence not an ideal of R.

We now prove that for all rings of order less than 16, the commutator subset is an ideal. We do this by examining the structure of these rings. Note that any commutative ring has commutator subset $\{0\}$, which is an ideal. Since all abelian groups of orders 1, 2, 3, 5, 6, 7, 10, 11, 13, 14 and 15 are cyclic, the rings of these orders must be commutative and therefore in all these rings the commutator subset is an ideal. The rings of order p^2, where p is a prime number, have been classified (see [1], [2]). There are only two non-commutative rings of order p^2. These are rings with additive group $C_p \oplus C_p = \langle a \rangle \oplus \langle b \rangle$, where $pa = pb = 0$. When $p = 2$, the two rings are given by

$$R_1 = \langle a, b : 2a = 2b = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$$

and

$$R_2 = \langle a, b : 2a = 2b = 0, a^2 = a, b^2 = b, ab = b, ba = a \rangle.$$

The commutator subset of R_1 is $\{0, a+b\}$ and this is an ideal of R_1. The commutator subset of R_2 is also $\{0, a+b\}$ and this is an ideal of R_2. When $p = 3$, the two rings are given by

$$R_3 = \langle a, b : 3a = 3b = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$$

and

$$R_4 = \langle a, b : 3a = 3b = 0, a^2 = a, b^2 = b, ab = b, ba = a \rangle.$$

The commutator subset of R_3 is $\{0, a + 2b, 2a + b\}$ and this is an ideal of R_3. The commutator subset of R_4 is also $\{0, a+2b, 2a+b\}$ and this is an ideal of R_4. Therefore in all rings of orders 4 and 9, the commutator subset is an ideal.

It is well known that any ring can be decomposed into a direct sum of rings of prime power order. Therefore the only non-commutative rings of order 12 are of the form $R_1 \oplus R_2$, where S_1 is a non-commutative ring of order 4 and S_2 is of order 3. Clearly S_2 is commutative and as we mentioned above there are only two non-commutative rings of order 4 and the commutator subset of each of these rings is an ideal. Hence the commutator subset of a ring of order 12 is an ideal.

The only remaining case to be considered is where the ring R has order 8. In this case R must have additive group C_8 (in which case R is commutative), $C_4 \oplus C_2$ or $C_2 \oplus C_2 \oplus C_2$.

Suppose first that R has additive group $C_4 \oplus C_2 = \langle a \rangle \oplus \langle b \rangle$, where $4a = 2b = 0$. Since $2b = 0$, we see that $2[a, b] = 0$ and the commutator subset of R is $C = \{0, [a, b]\}$. Therefore C is an additive subgroup of R. Every element of R is of the form $ma + nb$, where $m = 0$, 1, 2, or 3 and $n = 0$ or 1. It follows from the identities

$$a[a, b] = [a, ab], \; [a, b]a = [a, ba], \; b[a, b] = [ba, b], \; [a, b]b = [ab, b]$$

that C is an ideal of R.

Finally, suppose that R has additive group

$$C_2 \oplus C_2 \oplus C_2 = \langle a \rangle \oplus \langle b \rangle \oplus \langle c \rangle,$$

where $2a = 2b = 2c = 0$. It is easily seen that the commutator subset C of R is an additive group. By considering different cases we shall show that C must be an ideal of R.

Case1 Suppose that $[a, b] = 0$. Then the commutator subset is $\{0, [a, c], [b, c], [a + b, c]\}$. Any element of R is of the form $ka + lb + mc$, where each of k,l and m is either 0 or 1. We have

$$\begin{aligned}(ka + lb + mc)[a, c] &= kaac - kaca + lbac - lbca + mcac - mcca \\ &= k[a, ca] + l[a, bc] + m[ca, c] \in C.\end{aligned}$$

Also, since $[a, b] = 0$, we have

$$\begin{aligned}[a, c](ka + lb + mc) &= kaca - kcaa + lacb - lcab + macc - mcac \\ &= k[a, ca] + lacb - lcba + macc - mcac \\ &= k[a, ca] + l[a, cb] + m[ac, c] \in C.\end{aligned}$$

Similarly $(ka + lb + mc)[b, c] \in C$ and $[b, c](ka + lb + mc) \in C$. So C is an ideal. Similarly if $[b, c] = 0$ or $[a, c] = 0$, then C is an ideal. So we can suppose $[a, b], [b, c]$ and $[a, c]$ are all non-zero.

Case 2 Suppose that $[a, b] + [b, c] = 0$. Now $[a + c, b] = 0$ and

$$C = \{0, [a, c], [a, b], [a, b + c]\}.$$

We have

$$\begin{aligned}(ka + lb + mc)[a, c] &= k(aac - aca) + l(bac - bca) + m(cac - cca) \\ &= k[a, ac] + l(b(a + c)c - bc(a + c)) + m[ca, c] \\ &= k[a, ac] + l((a + cbc - bc(a + c)) + m[ca, c] \\ &= k[a, ac] + l[(a + c), bc] + m[ca, c] \in C.\end{aligned}$$

Similarly

$$\begin{aligned}&[a, c](ka + lb + mc) \in C, \\ &(ka + lb + mc)[a, b] \in C\end{aligned}$$

and

$$[a, b](ka + lb + mc) \in C,$$

also. Therefore C is an ideal.

Case 3 Suppose that $[a, b] + [b, c] + [a, c] = 0$. Then $[b, c] = [a, b + c]$ and

$$C = \{0, [a, b], [a, c], [a, b + c]\}.$$

As above we can easily show that C must be an ideal.

We can finally suppose that all of the cases above do not occur. Thus it follows that if $k[a, b] + l[b, c] + m[a, c] = 0$, then

$k = l = m = 0$. 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,