PRODUCTS OF GROUP COMMUTATORS

P. Hegarty and D. MacHale

Abstract We show that certain products of group commutators are commutators and derive a number of applications.

1. Introduction

If a and b are elements of a group G, we define the *commutator* of a and b, written as $[a, b]$, to be the group element $a^{-1}b^{-1}ab$. The following facts are immediate from the definition.

(i) The inverse of a commutator is a commutator

$$[a, b]^{-1} = [b, a]. \qquad (1)$$

(ii) Any conjugate of a commutator is a commutator

$$x^{-1}[a, b]x = [x^{-1}ax, x^{-1}bx]. \qquad (2)$$

(iii) By direct computation

$$[a, b] = [ba, a^{-1}] \qquad (3)$$
$$= [b^{-1}, ab] \qquad (4)$$
$$= [b^{-1}a, b] \qquad (5)$$
$$= [a, ab]. \qquad (6)$$

However, it is well known that the product of two commutators need not be a commutator. Guralnick, [5], shows that if the commutator subgroup G' satisfies either

(a) G' is abelian and $|G| < 128$ or $|G'| < 16$

or

(b) G' is non-abelian and $|G| < 96$ or $|G'| < 24$,

then the product of any two commutators is a commutator. He also gives examples to show that these two bounds are the best possible. Macdonald, [7], shows that if G has centre $Z(G)$ and satisfies

$$|G : Z(G)|^2 < |G'|,$$

then there is a product of commutators in G which is not a commutator in G, and produces infinitely many examples of this phenomenon.

In this note we investigate certain products of group commutators which can be written as single commutators. We also present analogous results for sums of ring commutators. We then apply the results for group commutators to give elementary proofs of two known group-theoretic results.

2. Products of group commutators

The following commutator identity appears, essentially without motivation, in [9, p.85]:

$$[xy, zt] = y^{-1}[x, t]y[y, t](yt)^{-1}[x, z](yt)t^{-1}[y, z]t. \qquad (7)$$

Putting $x = c$, $y = a^{-1}$, $z = d$, $t = b^{-1}$, we immediately obtain

$$[a, b][b, c][c, d][d, a] = (ba)^{-1}[ca^{-1}, db^{-1}](ba). \qquad (8)$$

Thus, the expression on the left-hand side of (8) is a single commutator. As special cases, we have

$$[a, b][b, c][c, a] = (ba)^{-1}[ca^{-1}, ab^{-1}](ba) = a^{-1}[b^{-1}ca^{-1}b, b^{-1}a]a \qquad (9)$$

by putting $d = a$ in (8), and

$$[a, b][b, c] = (ba)^{-1}[ca^{-1}, b^{-1}](ba) = [a^{-1}ba, a^{-1}c] \qquad (10)$$

by putting $d = 1$ in (8) and applying (3)-(6) several times.

Since (10) is fundamental to this paper, and actually appears in [8] and as an exercise in [1], we feel it is instructive to derive (7)-(10) in reverse order, starting from scratch. Firstly, we have

$$[a, b][b, c] = a^{-1}b^{-1}abb^{-1}c^{-1}bc = a^{-1}b^{-1}ac^{-1}bc$$
$$= (a^{-1}b^{-1}a)(c^{-1}a)(a^{-1}ba)(a^{-1}c) = [a^{-1}ba, a^{-1}c].$$

Secondly,

$$[a,b][b,c][c,a] = [a^{-1}ba, a^{-1}c][c,a] \text{ by (10)}$$
$$= [a^{-1}ba, a^{-1}c][a^{-1}c, a] \text{ by (5)}$$
$$= [a^{-1}b^{-1}ca^{-1}ba, a^{-1}b^{-1}a^2] \text{ by (10)}$$
$$= a^{-1}[b^{-1}ca^{-1}b, b^{-1}a]a \text{ by (2)},$$

which is just (9). Thirdly,

$$[a,b][b,c][c,d][d,a] = [a^{-1}ba, a^{-1}c][c^{-1}dc, c^{-1}a] \text{ by (10)}$$
$$= [a^{-1}ba, a^{-1}c][a^{-1}c, c^{-1}da] \text{ by (4)}$$
$$= [a^{-1}b^{-1}ca^{-1}ba, a^{-1}b^{-1}ac^{-1}da] \text{ by (10)}$$
$$= (ba)^{-1}[ca^{-1}, ac^{-1}db^{-1}](ba) \text{ by (2)}$$
$$= (ba)^{-1}[ca^{-1}, db^{-1}](ba) \text{ by (6)},$$

which is just (8). Equation (7) now follows easily on putting $a = y^{-1}$, $b = t^{-1}$, $c = x$ and $d = z$.

We now ask if either of

$$[a,b][b,c][c,d] \quad \text{or} \quad [a,b][b,c][c,d][d,e][e,a]$$

can always be written as a single commutator. We show that the answer is no. We need the following results from Liebeck, [6]. Let $G_4 = \langle a_1, a_2, a_3, a_4 \rangle$ be the free nilpotent group of class 2 on four generators. Put

$$c_{ij} = [a_i, a_j]$$

for $1 \le i < j \le 4$, so that $[c_{ij}, a_k] = 1$ for $1 \le i < j \le 4$ and all k. An arbitrary commutator in G may be written as

$$[a_1^{\alpha_1} a_2^{\alpha_2} a_3^{\alpha_3} a_4^{\alpha_4}, a_1^{\beta_1} a_2^{\beta_2} a_3^{\beta_3} a_4^{\beta_4}],$$

which simplifies to

$$\prod_{1 \le i < j \le 4} c_{ij}^{\delta_{ij}},$$

where $\delta_{ij} = \alpha_i \beta_j - \alpha_j \beta_i$.

The indices δ_{ij} satisfy the relation

$$\delta_{12}\delta_{34} - \delta_{13}\delta_{24} + \delta_{14}\delta_{23} = 0,$$

and this is a necessary and sufficient condition for

$$\prod_{i,j=1}^{4} c_{ij}^{\delta_{ij}}$$

to be a single commutator.

Consider $[a_1, a_2][a_2, a_3][a_3, a_4]$. Here,

$$\delta_{12}\delta_{34} - \delta_{13}\delta_{24} + \delta_{14}\delta_{23} = 1 \cdot 1 - 0 \cdot 0 + 0 \cdot 1 = 1 \ne 0,$$

so $[a_1, a_2][a_2, a_3][a_3, a_4]$ is not a commutator in G_4.

Suppose now that $[a,b][b,c][c,d][d,e][e,a]$ is always a commutator. Put $e = 1$ and we get that $[a,b][b,c][c,d]$ is always a commutator, contradicting the previous result. It is also clear that for any $n \ge 3$, neither $[x_1, x_2] \ldots [x_{n-1}, x_n]$ nor $[x_1, x_2] \ldots [x_n, x_{n+1}][x_{n+1}, x_1]$ can, in general, be written as a single commutator.

Finally, in this section, we mention some ring-theoretic analogues of the results we have presented for groups. If R is a ring and a and b are elements of R, then the ring commutator of a and b, written $[a,b]$, is defined to be the ring element $ab - ba$. It is well known that the sum of two ring commutators need not be a ring commutator and examples are very much easier to construct than the corresponding examples for groups.

The following identities for ring commutators are easily verified:

$$[a,b] + [b,c] = [a-c, b] \tag{11}$$
$$[a,b] + [c,a] = [a, b-c] \tag{12}$$
$$[a,b] + [b,c] + [c,a] = [a-c, b-c]$$
$$= [c-b, a-b]$$
$$= [b-a, c-a] \tag{13}$$
$$[a,b] + [b,c] + [c,d] + [d,a] = [a-c, b-d] \tag{14}$$
$$[x,t] + [y,t] + [x,z] + [y,z] = [x+y, z+t]. \tag{15}$$

Again, (11) and (14) cannot be extended to four and five variables, respectively. Examples are easy to construct in the ring of all 3×3 matrices of the form

$$
\begin{pmatrix}
a & f(x) & h(x,y) \\
0 & a & g(y) \\
0 & 0 & a
\end{pmatrix},
$$

where f, g and h are polynomials in the commuting indeterminates x and y over an arbitrary field F, and $a \in F$ (see [2]).

3. Applications

(A) Culler, [3], has shown that $[a,b]^n$ can be written as a product of $[\frac{n}{2}] + 1$ commutators, where $[k]$ denotes the greatest integer contained in k. Culler's methods are highly topological, however, and we now offer a simple proof based on (10).

Firstly, $[a,b][c,a]$ is a single commutator since, by (3) and (4),

$$
[a,b][c,a] = [ba, a^{-1}][a^{-1}, ca],
$$

which is a single commutator by (10). We use the following well-known identity (which, incidentally, can also be derived using (3)-(6) and (10)):

$$
[a,b]^2 = [b^{-1}, a][aba^{-1}b^{-1}a, b] \tag{16}
$$

For simplicity, we henceforth denote $aba^{-1}b^{-1}a$ by t. Equation (3) says that $[a,b] = [ba, a^{-1}]$. We may assume that a and b are generators of a free group G on two generators, since the commutator identities we are about to obtain for the free group may then be carried over homomorphically to any other group generated by two elements. Let α be the automorphism of G defined by setting $a\alpha = ba$, $b\alpha = a^{-1}$. Applying α to both sides of (16), we get

$$
[a,b]^2 = [a, ba][t\alpha, a^{-1}] = [a, ba][a, t\alpha a^{-1}], \tag{17}
$$

where we have used (4) to obtain the last part of the equation. Thus

$$
[a,b]^4 = [a, ba][a, t\alpha a^{-1}][b^{-1}, a][t, b], \tag{18}
$$

whence $[a,b]^4$ is a product of three commutators since, by the opening remark of this proof, the product of the middle two commutators in (18) is a single commutator. Now apply α to both sides of (18), and post-multiply both sides of the resulting equation by (16). By the same reasoning as above, we thus have $[a,b]^6$ equal to the product of four commutators. It is now a simple induction that $[a,b]^{2n}$ can always be expressed as the product of $n + 1$ commutators.

Finally, pre-multiply both sides of (16) by $[a,b]$ to get

$$
[a,b]^3 = [a,b][b^{-1}, a][t, b], \tag{19}
$$

whence $[a,b]^3$ is a product of two commutators, by the opening remark. By repeating the construction above of $[a,b]^{2n}$ as a product of $n+1$ commutators, we quickly see that $[a,b]^{2n+1}$ can always be expressed as a product of $n+1$ commutators also. This completes the proof of Culler's result.

(B) Edmunds, [4], showed that, in any group, any product of n commutators can always be expressed as the product of some $2n+1$ squares. We offer an elementary proof of this result, again based on (10).

Firstly, for any x_1 and x_2 in G,

$$
x_1^2 x_2^2 = [x_1^{-1}, x_2^{-1} x_1^{-1}](x_1 x_2)^2. \tag{20}
$$

It can now easily be shown by induction that for $k \geq 2$

$$
x_1^2 \ldots x_k^2 (x_1 \ldots x_k)^{-2} = \prod_{i=2}^{k} [z_{i-1}^{-1}, z_i^{-1}], \tag{21}
$$

where we have set

$$
z_r = x_1 \ldots x_r
$$

for $r \geq 1$. Put $k = 2n+1$ and use (10) on the right-hand side of (21) to obtain

$$
x_1^2 \ldots x_{2n+1}^2 (x_1 \ldots x_{2n+1})^{-2} = \prod_{i=1}^{n} [z_{2i-1} z_{2i}^{-1} z_{2i-1}^{-1}, z_{2i-1} z_{2i+1}^{-1}] \tag{22}
$$

which equates a product of n commutators and a product of $2n+2$ squares. We now show that every product

$$[a_1, a_2] \ldots [a_{2n-1}, a_{2n}]$$

of n commutators in G can be written in the form of the right-hand side of (22).

We simply equate corresponding terms, that is, for $i = 1, \ldots, n$, we put

$$a_{2i-1} = z_{2i-1} z_{2i}^{-1} z_{2i-1}^{-1} \tag{23}$$
$$a_{2i} = z_{2i-1} z_{2i+1}^{-1}, \tag{24}$$

where the z_r are as above. (23) is an equation for a_{2i-1} in terms of $x_1, \ldots, x_{2i}$ in which the variable x_{2i} appears only once and (24) is an equation for a_{2i} in terms of $x_1, \ldots, x_{2i+1}$ in which the variable x_{2i+1} appears only once.

What this means is that x_1 can be fixed arbitrarily and, having found $x_1, \ldots, x_l$, we have an equation for x_{l+1} in terms of $x_1, \ldots, x_l, a_l$, in which the variable x_{l+1} appears only once, so that the equation has a unique solution. It is easy to verify that the following recursion formula for the x_l is consistent with the $2n$ equations contained in (23) and (24).

$$x_1 = a_1$$
$$x_{2i} = z_{2i-1}^{-2} a_{2i-1}^{-1} z_{2i-1}, \quad 1 \le i \le n$$
$$x_{2i+1} = z_{2i}^{-1} a_{2i}^{-1} z_{2i-1}, \quad 1 \le i \le n$$

Hence, every product of n commutators can be written as a product of $2n + 2$ squares

$$[a_1, a_2] \ldots [a_{2n-1}, a_{2n}] = x_1^2 \ldots x_{2n+1}^2 (x_1 \ldots x_{2n+1})^{-2},$$

where the x_i are given by the recursion formulae above. However, from these formulae, we see that $x_2 = x_1^{-2} a_1^{-1} x_1 = a_1^{-2}$, which implies that $x_1^2 x_2^2 = a_1^2$ is a square. Thus, every product of n

commutators can in fact be written as a product of $2n + 1$ squares. as required.

References

[1] R. D. Carmichael, Introduction to the Theory of Groups of Finite Order. Dover: New York, 1956.

[2] P. J. Cassidy, *Products of commutators are not always commutators: an example.* Amer. Math. Monthly **86** (1972), 772.

[3] M. Culler, *Using surfaces to solve equations in free groups*, Topology **20** (1981), 133-145.

[4] C. C. Edmunds, *Products of commutators as products of squares*, Canad. J. Math. **27** (1975), 1329-1335.

[5] R. N. Guralnick, *Expressing group elements as commutators*, Rocky Mountain J. of Math. **10** (1980), 651-654.

[6] H. Liebeck, *A test for commutators*, Glasgow Math. J. **17** (1976), 31-36.

[7] I. D. Macdonald, *Commutators and their products*, Amer. Math. Monthly **93** (1986), 440-443.

[8] N. S. Mendelsohn, *Some examples of man-machine interaction*, in Computational Problems in Abstract Algebra, ed. by J. Leech. Pergamon Press: 1970.

[9] H. Neumann, Varieties of Groups. Springer Verlag: 1967.

P. Hegarty and D. MacHale,
Department of Mathematics,
University College,
Cork.