A NONCOMMUTATOR IN SL_2

KEITH CONRAD

In a group G, the *commutator* of two elements g and h is $[g,h] := ghg^{-1}h^{-1}$. Since $gh = [g,h]hg$, we see g and h commute if and only if $[g,h] = e$. Thus the commutator of g and h "measures" how far they are from commuting, and G is abelian if and only if all commutators are trivial.

The set of commutators in G is closed under inversion and conjugation:

$$[g,h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h,g],$$

$$k[g,h]k^{-1} = kghg^{-1}h^{-1}k^{-1} = (kgk^{-1})(khk^{-1})(kg^{-1}k^{-1})(kh^{-1}k^{-1}) = [kgk^{-1}, khk^{-1}]. \tag{1}$$

However, the set of commutators is not always closed under multiplication.

An example of a group containing a product of commutators that is not a commutator is $\mathrm{SL}_2(\mathbf{R})$: in this group $-I_2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is a product of 4 commutators but is not a commutator.[1] The following theorem is a generalization of this property of $-I_2$.

Theorem 1. *Let F be a field with more than 3 elements and $2 \neq 0$ in F. In $\mathrm{SL}_2(F)$, $-I_2$ is a product of 4 commutators, and $-I_2$ is a commutator if and only if $-1 = x^2 + y^2$ for some x and y in F.*

This includes $F = \mathbf{R}$ since -1 is not a sum of two (or any number of) squares in $\mathbf{R}$. Saying $2 \neq 0$ in F is reasonable, since if $2 = 0$ then $-I_2 = I_2$, which is uninteresting.

Proof. In $\mathrm{SL}_2(F)$, $I_2 = ((\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})(\begin{smallmatrix} 1 & 0 \\ -2 & 1 \end{smallmatrix}))^2$. The matrices $(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$ and $(\begin{smallmatrix} 1 & 0 \\ -2 & 1 \end{smallmatrix})$ are each commutators: since F has more than three elements it contains a nonzero a such that $a^2 \neq 1$, and $[(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}), (\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix})] = (\begin{smallmatrix} 1 & b(a^2-1) \\ 0 & 1 \end{smallmatrix})$ and $[(\begin{smallmatrix} 1/a & 0 \\ 0 & a \end{smallmatrix}), (\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix})] = (\begin{smallmatrix} 1 & 0 \\ c(a^2-1) & 1 \end{smallmatrix})$ for all b and c in F, so by letting $b = 1/(a^2-1)$ and $c = -2/(a^2-1)$ we realize $(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$ and $(\begin{smallmatrix} 1 & 0 \\ -2 & 1 \end{smallmatrix})$ as commutators. (When $F = \mathbf{R}$ we can use $a = 2$, $b = 1/3$, and $c = -2/3$.)

To show $-I_2$ is a commutator in $\mathrm{SL}_2(F)$ if and only if $-1 = x^2 + y^2$ for some x and y in F, suppose first that $-I_2 = [A,B] = ABA^{-1}B^{-1}$ for some A and B in $\mathrm{SL}_2(F)$. We may assume we're in the case that -1 is not a square in F, since if it is then it is also a sum of two squares where one square is 0.

<u>Step 1</u>: A and B have trace 0.

Solving the equation $-I_2 = ABA^{-1}B^{-1}$ for A,

$$A = -BAB^{-1} \Longrightarrow \mathrm{Tr}(A) = \mathrm{Tr}(-BAB^{-1}) = -\mathrm{Tr}(A) \Longrightarrow 2\,\mathrm{Tr}(A) = 0 \Longrightarrow \mathrm{Tr}(A) = 0,$$

where the last step depends on $2 \neq 0$ in F. That $\mathrm{Tr}(B) = 0$ is similar.

<u>Step 2</u>: $A^{-1} = -A$, $B^{-1} = -B$, $[A,B] = (AB)^2$, and $\mathrm{Tr}(AB) = 0$.

A 2×2 matrix M of trace 0 has the form $(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix})$, and when it has determinant 1 we have $M^{-1} = (\begin{smallmatrix} -a & -b \\ -c & a \end{smallmatrix}) = -M$. Therefore if A and B are in $\mathrm{SL}_2(F)$ with trace 0, their commutator is $[A,B] = ABA^{-1}B^{-1} = AB(-A)(-B) = (AB)^2$.

[1] In the group $\mathrm{GL}_2(\mathbf{R})$, $-I_2$ is a commutator: $-I_2 = [(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}), (\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix})]$, where $\det(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}) = \det(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}) = -1$.

Rewriting $-I_2 = ABA^{-1}B^{-1}$ as $AB = -BA$, we have $\mathrm{Tr}(AB) = -\mathrm{Tr}(BA) = -\mathrm{Tr}(AB)$, so $2\,\mathrm{Tr}(AB) = 0$ and thus $\mathrm{Tr}(AB) = 0$.

Step 3: $-1 = x^2 + y^2$ for some x and y in F. We'll do this in two ways.

Method 1: Since $\mathrm{Tr}(A) = 0$, we can write $\boxed{A = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)}$. Since $\det A = 1$, $-a^2 - bc = 1$. Then being in the case that -1 is not a square in F implies $c \neq 0$.

Conjugating a commutator conjugates the elements being "commutated" by (1), so $-I_2 = [CAC^{-1}, CBC^{-1}]$ for all C in $\mathrm{SL}_2(F)$. Use $C = \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$, so $CAC^{-1} = \left(\begin{smallmatrix} a+ct & * \\ c & -(a+ct) \end{smallmatrix}\right)$. Since $c \neq 0$, for a suitable t we have $a + ct = 0$. Put this t in C and rename CAC^{-1} and CBC^{-1} as A and B, so $-I_2 = [A, B]$ where A has diagonal entries 0: $A = \left(\begin{smallmatrix} 0 & -1/c \\ c & 0 \end{smallmatrix}\right)$. (The upper right entry is $-1/c$ since $\det A = 1$.) Running through Steps 1 and 2 with this new A and B, $\mathrm{Tr}(B) = 0$ and $[A, B] = (AB)^2$. Set $B = \left(\begin{smallmatrix} x & y \\ z & -x \end{smallmatrix}\right)$. Then

$$-I_2 = [A, B] = (AB)^2 = \begin{pmatrix} x^2 + z^2/c^2 & xy - xz/c^2 \\ -xz + xyc^2 & x^2 + y^2c^2 \end{pmatrix}.$$

From either diagonal entry, -1 is a sum of two squares in F.

Method 2: By Step 2, $A^{-1} = -A$, so $A^2 = -I_2$. Thus eigenvalues of A are square roots of -1, which are not in F by the case we're in, so A has no eigenvector in F^2. Hence for nonzero $\mathbf{v} \in F^2$, $A\mathbf{v} \notin F\mathbf{v}$, which implies $\mathcal{B} := \{\mathbf{v}, A\mathbf{v}\}$ is a basis of F^2. Since $A^2 = -I_2$, the matrix for A relative to $\mathcal{B}$ is $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, so $UAU^{-1} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ for an invertible matrix U in $\mathrm{M}_2(F)$, and $\det(UAU^{-1}) = \det A = 1$. Similarly, $\det(UBU^{-1}) = 1$. Rename UAU^{-1} as A and UBU^{-1} as B, so $-I_2 = [A, B]$ where $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. By Step 1, $\mathrm{Tr}(B) = 0$, so we can write $B = \left(\begin{smallmatrix} x & y \\ z & -x \end{smallmatrix}\right)$. Then $AB = \left(\begin{smallmatrix} -z & x \\ x & y \end{smallmatrix}\right)$. Since $\mathrm{Tr}(AB) = 0$ by Step 2, $-z + y = 0$, so $z = y$. Thus $B = \left(\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right)$, so $1 = \det B = -x^2 - y^2$, which implies $-1 = x^2 + y^2$.[2]

Conversely, assume $-1 = x^2 + y^2$ with x and y in F. For $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} x & y \\ y & -x \end{smallmatrix}\right)$ in $\mathrm{SL}_2(F)$, $[A, B] = (AB)^2 = \left(\begin{smallmatrix} -y & x \\ x & y \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} x^2+y^2 & 0 \\ 0 & x^2+y^2 \end{smallmatrix}\right) = -I_2$. □

Example 2. In $\mathbf{C}$, $-1 = i^2 + 0^2$, so $-I_2 = [A, B]$ for $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbf{C})$.

For odd primes p, -1 is a sum of two squares in $\mathbf{Z}/p\mathbf{Z}$, so $-I_2$ is a commutator in $\mathrm{SL}_2(\mathbf{Z}/p\mathbf{Z})$. This is also true in $\mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$ since $-I_2 \equiv I_2 \bmod 2$. Each finite field contains some $\mathbf{Z}/p\mathbf{Z}$, so $-I_2$ is a commutator in $\mathrm{SL}_2(F)$ when F is finite. Thus Theorem 1 doesn't give us a *finite* group in which some product of commutators is not a commutator. The smallest such finite groups have order 96 and there are two of them up to isomorphism: see https://math.stackexchange.com/questions/7811 and [1]. This is due to R. Guralnick in his Ph.D. thesis. In both of these groups, there are 29 commutators and the subgroup they generate has order 32. One such group is $G = (Q_8 \times (\mathbf{Z}/(2))^2) \rtimes \mathbf{Z}/(3)$ where a generator of $\mathbf{Z}/(3)$ acts on Q_8 by the order 3 automorphism having the effect $i \mapsto j \mapsto k \mapsto i$ and it acts on $(\mathbf{Z}/(2))^2$ through the order 3 automorphism $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbf{Z}/(2))$.[3]

References

[1] L-C. Kappe and R. F. Morse, "On commutators in groups", pp. 531-558 in *Groups St. Andrews 2005, Vol. 2*, Cambridge Univ. Press (2007).

[2] This second approach to Step 3, when $F = \mathbf{R}$, is one answer to the question about commutators on the MO page https://mathoverflow.net/questions/44269.

[3] This group G can also be described as $Q_8 \rtimes A_4$ where A_4 acts nontrivially on Q_8 through its cyclic quotient $A_4/V \cong \mathbf{Z}/(3)$ where V is the unique 2-Sylow subgroup of A_4.