Heisenberg: Solution

(I). We show ab^{-1} and $b^{-1}a$ commute:

$$\begin{aligned}
& (ab^{-1})(b^{-1}a) &=& (b^{-1}a)(ab^{-1}) \\
\iff & ab^{-2}a &=& b^{-1}a^2b^{-1} \\
\iff & aba &=& b^{-1}a^{-1}b^{-1} \\
\iff & aba &=& (bab)^{-1} \\
\iff & (aba)(bab) &=& e \\
\iff & (ab)(ab)(ab) &=& e \\
\iff & (ab)^3 &=& e
\end{aligned}$$

(II). And a commutes with $aba^{-1}b^{-1}$ because (much harder):

$$\begin{aligned}
& a(aba^{-1}b^{-1}) &=& (aba^{-1}b^{-1})a && (1) \\
\iff & a(aba^{-1}b^{-1})a^{-1}(aba^{-1}b^{-1})^{-1} &=& e && (2) \\
\iff & a(aba^{-1}b^{-1})a^{-1}(bab^{-1}a^{-1}) &=& e && (3) \\
\iff & a^{-1}ba^{-1}b^{-1}a^{-1}bab^{-1}a^{-1} &=& e && (4) \\
\iff & a^{-1}b(bab)bab^{-1}a^{-1} &=& e && (5) \\
\iff & a^{-1}b^{-1}ab^{-1}ab^{-1}a^{-1} &=& e && (6) \\
\iff & a^{-1}b^{-1}ab^{-1}ab^{-1} &=& a && (7) \\
\iff & ab^{-1}ab^{-1}ab^{-1} &=& e && (8) \\
\iff & (ab^{-1})^3 &=& e && (9)
\end{aligned}$$

(1) $\Rightarrow$ (2) rewrites $xy = yx$ as $xyx^{-1}y^{-1} = e$, where $x = a$ and $y = aba^{-1}b^{-1}$; (2) $\Rightarrow$ (3) uses the socks-and-shoes rule; (3) $\Rightarrow$ (4) rewrites a^2 as a^{-1} in the front; (4) $\Rightarrow$ (5) rewrites $a^{-1}b^{-1}a^{-1} = (aba)^{-1}$ as bab (compare with the middle of the last derivation); (5) $\Rightarrow$ (6) rewrites b^2 as b^{-1}; (6) $\Rightarrow$ (7) $\Rightarrow$ (8) right-multiplies by a and left-multiplies by a^{-1} (replacing a^{-2} with a).

Suppose G is freely generated by a and b, or in other words all group elements are products of powers of a and b, and it is not possible to express a or b in terms of each other (in particular e, a, a^2, b, b^2 are all distinct).

In the first derivation **(I)**, the observation $(ab)^3 = e$ is equivalent to aba and bab being inverses is prescient. Another consequence, to be used momentarily:

$$\begin{array}{rrcccc} & aba & = & (ab^{-1})(b^{-1}a) & = & pq \\ \iff & bab & = & (pq)^{-1} & = & q^{-1}p^{-1}, \end{array}$$

denoting $p = ab^{-1}$ and $q = b^{-1}a$ for convenience.

Interpret the equation $(ab^{-1})b = a = b(b^{-1}a)$ as a **sliding rule**: a recipe for how to slide one group element past another (with compromises along the way). In particular, the rule $pb = bq$ says we can slide p past b from left to right as long as we turn the p into q, or conversely we can slide q past b from right to left as long as we turn the q into a p. But then how do we slide p and q past b the other directions? Using $b^{-1} = b^2$ we can determine

$$\begin{array}{rcl} qb &=& (b^{-1}a)b \\ &=& b(bab) \\ &=& bq^{-1}p^{-1} \end{array} \qquad \text{and} \qquad \begin{array}{rcl} bp &=& b(ab^{-1}) \\ &=& (bab)b \\ &=& q^{-1}p^{-1}b \end{array}$$

In conclusion, if we have an expression which is a bunch of ps and qs on one side of b, these sliding rules let us convert it into an expression with a (probably different) bunch of ps and qs on the other side of b. Since p and q also commute, we can conclude all group elements can be put into a "standard form" like $b^u p^v q^w$ with $-1 \le u, v, w \le 1$ (or $0 \le u, v, w \le 2$, same difference); in particular, this means the order (cardinality) is $|G| = 3^3 = 27$.

In **(II)** we work with the **commutator** $[a, b] := aba^{-1}b^{-1}$ of two elements a and b, so-called because it "measures" the extent to which a and b fail to commute. (This intuition extends further to describe the structure of a group; see *central series* and *nilpotence class*.) In particular, two elements commute ($xy = yx$) if and only if the commutator is trivial ($[x, y] = e$).

Our derivation in **(II)** only showed a commutes with $[a,b]$, or in other words $[a,[a,b]] = e$, but it is possible to show this implies $[b,[a,b]] = e$ too.

Note $xy = xy$ implies $y^{-1}x = xy^{-1}$ and $yx^{-1} = x^{-1}y$ (multiply on the left or right by x^{-1} or y^{-1} appropriately); also, it implies e.g. $x^2y = xxy = xyx = yxx = yx^2$; similar reasoning shows any power of x commutes with any power of y (positive or negative). Socks-and-shoes implies $[x,y]^{-1} = [y,x]$. By symmetry, we could have done the derivation in **(II)** with the letters a and b swapped, which gives $[b,[b,a]] = e$, which thus implies $[b,[a,b]] = e$.

Since $c := [a,b]$ commutes with G's generators a and b, it is **central**: it commutes with all group elements. We can interpret $ab = cba$ or $ba = abc^{-1}$ as another sliding rule for how to move a and b past each other, from which we may conclude all group elements are expressible in a standard form like $a^u b^v c^w$ with $-1 \le u, v, w \le 1$ (or $0 \le u, v, w \le 2$, if so inclined).

We can also express these ideas in the esoteric language of group theory.

For **(I)**, consider the subgroup $H = \langle ab^{-1}, b^{-1}a \rangle$ of G. To show it's normal, it suffices to check conjugating H's generators by G's generators doesn't leave H: both $a(b^{-1}a)a^{-1}$ and $b(b^{-1}a)b^{-1}$ simplify to ab^{-1}, and both $a(ab^{-1})a^{-1}$ and $b(ab^{-1})b^{-1}$ simplify to bab, which we found earlier is $(b^{-1}a)^{-1}(ab^{-1})^{-1}$.

We can say "$a \equiv b \bmod H$" because $b^{-1}a$ and ab^{-1} are in H. Thus in the quotient group G/H, all bs turn into as and so all elements can be represented by a power a^u with $0 \le u \le 2$. Moreover, ab^{-1} and $b^{-1}a$ commute and have order 3 in H, so H is elementary abelian of order $3^2 = 9$. From this we can conclude the order of G is $|G| = [G:H]|H| = 3 \cdot 3^2 = 27$.

Or for **(II)**, consider the subgroup $K = \langle [a,b] \rangle$. It is cyclic of order 3. As $[a,b]$ is central, so is K, so in particular it is normal. We can say "$ab \equiv ba \bmod K$" because $(ab)(ba)^{-1}$ is in K. Thus in the quotient group G/K all elements are expressible as $a^u b^v$ with $0 \le u, v \le 2$, or in other words G/K is elementary abelian of order 3^2. Once again, $|G| = [G:K]|K| = 3^2 \cdot 3 = 27$.

Our group G has an explicit matrix representation, by writing

$$a = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad c = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

In this matrix group, numbers are interpreted mod 3, meaning all matrix entries are in $\mathbb{F}_3 = \{0, 1, 2\}$ where addition and multiplication "wrap around" (for comparison, clock arithmetic is mod 12), which means e.g. $-1 \equiv 2$ represent the same scalar. Here, $c = aba^{-1}b^{-1}$, and the group of matrices generated by a and b using matrix multiplication are the unitriangular ones:

$$G = \left\{ \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; x, y, z \text{ in } \mathbb{F}_3 \right\}.$$

This is the **Heisenberg group** $H_3(\mathbb{F}_3)$. The continuous version $H_3(\mathbb{R})$ (which uses real numbers instead of integers mod 3) has infinitesimal generators analogous to a and b which represent position and momentum operators in quantum mechanics (also present in the Heisenberg uncertainty principle).

The **Burnside group** $B(k, n)$ is the "free"-est group of exponent n generated by k generators. That means all group elements are products of powers of generators $a_1, \cdots, a_k$ and the only relations that exist between the generators are those that can be derived from the assumption that $g^n = e$ for all group elements g. Our group is $H_3(\mathbb{F}_3) = B(2, 3)$. In general, if $n = 3$ the Burnside group has order $|B(k, 3)| = 3^{\binom{k}{1}+\binom{k}{2}+\binom{k}{3}}$. While it is known whether or not $B(k, n)$ is finite for many small values of (k, n), no general rule is known.

The complexity of the derivation for **(II)** is not at all an outlier in computational group theory. The **word problem** for groups asks if there is an algorithm that, when given a group (presented by a set of generators and relations between them) can decide when two "words" represent the same element. It turns out to be **undecidable**: there is no such algorithm.