Math 500: HW 1 due Friday, January 31, 2025.

Credit: Solutions by Charles Rezk, slightly modified by Nathan.

1. Let G be a group. Suppose $a, b \in G$ are such that $|a| = m$, $|b| = n$, and $ab = ba$. Show that if $\gcd(m, n) = 1$, then $c := ab$ has order mn. (Here $|a|$ is the order of a.)

   Solution. Because $ab = ba$, we have the formula $c^k = (ab)^k = a^k b^k$ for all $k \in \mathbb{Z}$. (You can assume this. It can be proved for $k > 0$ by induction on k, then extended to all integers k.)

   From the hypotheses $|a| = m$ and $|b| = n$, we have that $c^{mn} = a^{mn} b^{mn} = (a^m)^n (b^n)^m = e$. Thus, we already know that $|c|$ must divide mn.

   Suppose $k \in \mathbb{Z}$ is such that $c^k = e$. I will show that $mn \mid k$, which together with $|c| \mid mn$ proves $|c| = mn$.

   Since $e = c^k = a^k b^k$, we have $a^k = b^{-k}$. In general, $|x^k|$ divides $|x|$, since $\langle x^k \rangle \leq \langle x \rangle$. Thus $|a^k| \mid m$ and $|b^{-k}| \mid n$, and since $\gcd(m, n) = 1$, we must have that $|a^k| = 1 = |b^{-k}|$, i.e., that $a^k = e = b^k$. This in turn implies $m \mid k$ and $n \mid k$, and therefore $mn \mid k$ since $\gcd(m, n) = 1$.

2. Show that if an element a in a group G has finite order m, then for any positive integer k such that $\gcd(k, m) = 1$, there exists an element $x \in G$ such that $x^k = a$.

   Solution. Write $|a| = m$. Since k and m are relatively prime, there exist integers u, v such that $1 = uk + vm$. Thus

   $$a = a^{uk+vm} = (a^u)^k (a^m)^v = (a^u)^k,$$

   since $a^m = e$. Thus we can set $x = a^u$, so $x^k = a$.

3. Prove that if G is a group such that $a^2 = e$ for all $a \in G$, then G is abelian.

   This implies that $a = a^{-1}$, as an immediate consequence of the identity $aa = e$. Given $a, b \in G$, the hypothesis also gives $(ab)^2 = e$, i.e., $abab = e$. From this we get

   $$ab = aeb = a(abab)b = (aa)ba(bb) = ebae = ba.$$

4. Consider $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ in $G = \mathrm{GL}_2\mathbb{R}$. Compute the orders of elements A, B, AB, BA. Fun fact: The subgroup $\langle A, B \rangle$ of G turns out to be

   $$\mathrm{SL}_2\mathbb{Z} := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \;\middle|\; a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}.$$

   Solution. We have $|A| = 4$ and $|B| = 3$. (Note that $A^2 = -I$ and $B^3 = I$.) Furthermore, $AB = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $BA = \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$. Inductively, we check see that $(AB)^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ and hence $|AB| = \infty$. Similarly, $(BA)^n = \left(\begin{smallmatrix} 1 & 0 \\ -n & 1 \end{smallmatrix}\right)$ and hence $|BA| = \infty$.

5. Give an example of subgroups $K \leq H \leq G$ such that K is normal in H, H is normal in G, but K is not normal in G. (Hence "is normal subgroup" is not a transitive relation.)

   Solution. It is handy to use the fact that every subgroup of index 2 is normal. Thus, an example is given by

   $$D_8 = \langle r, s\rangle \supsetneq \langle r^2, s\rangle \supsetneq \langle s\rangle,$$

   since $\langle s\rangle$ is not a normal subgroup of D_8.

   Another example is $G = S_4$, $H = \{e, (12)(34), (13)(24), (14)(23)\}$ which is isomorphic to $C_2 \times C_2$, and $K = \{e, (12)(34)\}$. Here, $H \leq G$ is normal because conjugation preserves the cycle type of a permutation and H is the identity plus all elements of cycle type $(ab)(cd)$. Also, $K \leq H$ is normal because H is abelian.

6. Show $G = SL_2(\mathbb{Z}/3)$ has $|G| = 24$ and give examples of subgroups of G of orders 3, 8, and 6. Hint: see [DF] §2.4 #9-10.

   Solution. First I claim that $|GL_2(\mathbb{Z}/3)| = 48$. An invertible matrix has the form $[v_1 \;\; v_2]$, where v_1, v_2 is a basis of the vector space $V = (\mathbb{Z}/3)^2$. There are $8 = 9 - 1$ ways to pick $v_1 \neq 0$, and then $6 = 9 - 3$ to pick v_2 which is not a mulitple of v_1. Thus $|GL_2(\mathbb{Z}/3)| = 8 \cdot 6 = 48$.

   The determinant homomorphism $\det: GL_2(\mathbb{Z}/3) \to (\mathbb{Z}/3)^\times = \{\pm 1\}$ is surjective (e.g., $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ has determinant -1). Thus $SL_2(\mathbb{Z}/3)$ is a subgroup of index 2, so $|G| = 24$.

   Here are some elements of G:

   $$-I = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad P = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}.$$

   Clearly $|-I| = 2$ and $|P| = 3$, and $|-P| = 6$, so we get cyclic subgroups $\langle P\rangle$ and $\langle -P\rangle$ of orders 3 and 6.

   Now consider

   $$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad B = PAP^{-1} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad C = PBP^{-1} = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}.$$

   Note that we must have $PCP^{-1} = A$, since $P^3 = I$. It is immediate to check that $A^2 = -I$ and $AB = C$, which in turn implies $B^2 = -I = C^2$ and $BC = A$ and $CA = B$ (by conjugating the original formulas by P and P^2). Therefore, the subset

   $$Q := \{\pm I, \; \pm A, \; \pm B, \; \pm C\}$$

   is closed under multiplication, and so is a subgroup of order 8.

   (In fact, Q is the only subgroup of order 8, and contains all elements in G which have order 2^k for some k.)

7. Show that every non-identity element of a free group has infinite order. (Hint: need to use the description of elements of free group in terms of reduced words.)

   Solution. Let $x \in F(S)$ with $x \neq e$. I can write this as a reduced word in S, so $x = a_1 \cdots a_n$ with $n \geq 1$, $a_n \in S \cup S^{-1}$ and $a_i \neq a_{i+1}^{-1}$. In any group G, if $g, h \in G$ then $|g| = |hgh^{-1}|$ since

$(hgh^{-1})^n = hg^nh^{-1}$ is e if and only if $g^n = h^{-1}eh = e$. If $a_1 = a_n^{-1}$, we will instead compute the order of $a_n x a_n^{-1}$ which is $a_2 a_3 \cdots a_{n-1}$ as a reduced word. Repeating as necessary, we can reduce to the case of $x \in F(S)$ where $a_1 \neq a_n^{-1}$ (the process has to stop as the word gets strictly shorter). Then the concatenation of x with itself k times is a reduced word and hence $x^k \neq e$ for all k. So x has infinite order, as needed.

Here's an alternate solution that works directly on initially given x: I claim there exists an integer k with $1 \leq k+1 \leq n/2$ such that $a_{k+1} \neq a_{n-k}^{-1}$. There are two cases:

- If n is even, and if there is no such k, then

$$x = a_1 \cdots a_{n/2}\, a_{n/2}^{-1} \cdots a_1^{-1},$$

  but this is clearly not a reduced word.

- If n is odd, and if there is no such k, then

$$x = a_1 \cdots a_{(n-1)/2}\, a_{(n+1)/2}\, a_{(n-1)/2}^{-1} \cdots a_1^{-1}, \qquad a_{(n+1)/2} = a_{(n+1)/2}^{-1}.$$

  But by construction of the free group, no element from S can be its own inverse, so this is impossible.

So now let k be the *smallest* integer $k \geq 0$ such that $a_{k+1} \neq a_{n-k}^{-1}$. Therefore we can write

$$x = uvu^{-1}, \qquad u = a_1 \cdots a_k, \quad v = a_{k+1} \cdots a_{n-k}, \quad u^{-1} = a_{n-k+1} \cdots a_n = a_k^{-1} \cdots a_1^{-1}.$$

Note that if $k = 0$ then this just says $x = v$. It follows that $x^d = (uvu^{-1})^d = uv^d u^{-1}$ for $d > 0$. Since $a_{k+1} \neq a_{n-k+1}^{-1}$, the expression

$$x^d = uv^d u^{-1} = (a_1 \cdots a_k)(a_{k+1} \cdots a_{n-k}) \cdots (a_{k+1} \cdots a_{n-k})(a_k^{-1} \cdots a_1^{-1})$$

presents this element as a reduced word, of length $2k + d(n-2k) > 0$, so it is not the identity element. Therefore x has infinite order.

8. Give a presentation of S_4 with 2 generators, and prove that your presentation is correct.

Solution. Choose $a, b, c \in S_4$ so that a is a 2-cycle, b is a 3-cycle, and $c = ab$ is a 4-cycle. (For instance, $a = (1\ 2)$, $b = (2\ 3\ 4)$, $c = (1\ 2\ 3\ 4)$.) Then the following are all presentations of S_4:

$$S_4 \approx \langle a, b \mid a^2, b^3, (ab)^4 \rangle \approx \langle a, c \mid a^2, c^4, (ac)^3 \rangle \approx \langle b, c \mid b^3, c^4, (cb^{-1})^2 \rangle.$$

I'll discuss the first one. Let $G := \langle a, b \mid a^2, b^3, (ab)^4 \rangle$. From what I have said we have an obvious homomorphism $\alpha\colon G \to S_4$, sending $a \mapsto (1\ 2)$ and $b \mapsto (2\ 3\ 4)$. We know another presentation of S_4:

$$S_4 = \langle s_1, s_2, s_3 \mid s_1^2, s_2^2, s_3^2, (s_1 s_3)^2, (s_1 s_2)^3, (s_2 s_3)^3 \rangle, \qquad s_1 = (1\ 2), s_2 = (2\ 3), s_3 = (3\ 4).$$

We can use this to construct a homomorphism $\beta\colon S_4 \to G$, so that

$$\beta(s_1) = a, \quad \beta(s_2) = abab^{-1}a, \quad \beta(s_3) = abab^{-1}ab.$$

To show this exist, we need to check that the six relations go to the identity in G. Before I begin, note that

$$abab = b^{-1}ab^{-1}a$$

since $(ab)^4 = e$. Then we have

$$\begin{aligned}
\beta(s_1^2) &= a^2 = e,\\
\beta(s_2^2) &= (abab^{-1}a)^2 = abab^{-1}a \cdot abab^{-1}a = e,\\
\beta(s_3^2) &= (abab^{-1}ab)^2\\
&= abab^{-1}\underline{ab \cdot ab}ab^{-1}ab\\
&= abab^{-1}\underline{b^{-1}ab^{-1}a}ab^{-1}ab = abababab = e,\\
\beta(s_1s_3s_1s_3) &= a \cdot abab^{-1}ab \cdot a \cdot b^{-1}abab^{-1}a\\
&= bab^{-1}abab^{-1}\underline{abab}ba\\
&= bab^{-1}abab^{-1}\underline{b^{-1}ab^{-1}a}ba\\
&= bab^{-1}\underline{abab}ab^{-1}aba\\
&= bab^{-1}\underline{b^{-1}ab^{-1}a}ab^{-1}aba\\
&= babababa = e,
\end{aligned}$$

$$\begin{aligned}
\beta((s_1s_2)^3) &= a \cdot abab^{-1}a \cdot a \cdot abab^{-1}a \cdot a \cdot abab^{-1}a\\
&= bab^{-1}abab^{-1}ababba\\
&= bab^{-1}abab^{-1}\underline{b^{-1}ab^{-1}a}ba\\
&= bab^{-1}\underline{abab}ab^{-1}aba\\
&= bab^{-1}\underline{b^{-1}ab^{-1}a}ab^{-1}aba\\
&= babababa = e,\\
\beta((s_2s_3)^3) &= (abab^{-1}a \cdot abab^{-1}ab)^3 = b^3 = e.
\end{aligned}$$

Now compute that $\beta \circ \alpha$ and $\alpha \circ \beta$ are identity maps.

$$\beta(\alpha(a)) = \beta(s_1) = a, \qquad \beta(\alpha(b)) = \beta(s_2s_3) = b,$$

$$\begin{aligned}
\alpha(\beta(s_1))\alpha(a) &= a,\\
\alpha(\beta(s_2)) &= \alpha(abab^{-1}a)\\
&= s_1 \cdot s_2\underline{s_3 \cdot s_1} \cdot s_3s_2 \cdot s_1\\
&= s_1s_2s_1s_3s_3s_2s_1 = s_1s_2s_1s_2s_1 = s_2,\\
\alpha(\beta(s_3)) &= \alpha(\beta(s_2)b) = s_2(s_2s_3) = s_3.
\end{aligned}$$

9. Prove that $\langle a, b \mid a^2b^{-2}, aba^{-1}b\rangle$ is a presentation of the quaternion group of order 8.

Solution. Write $G = \langle a, b \mid a^2b^{-2}, aba^{-1}b\rangle$. We have a surjective homomorphism

$$\phi\colon G \to Q, \qquad \phi(a) = i, \quad \phi(b) = j.$$

I'll show $|G| \leq 8$.

The second relation says $aba^{-1} = b^{-1}$, while the first relation says $a^2 = b^2$. Thus

$$a^2 = aa^2a^{-1} = ab^2a^{-1} = aba^{-1} \cdot aba^{-1} = b^{-2} = a^{-2}.$$

This implies $a^4 = e$, and also $b^4 = a^4 = e$. Also, $a^2 = b^2$ commutes with both a and b, and so is in the center of the group. Note also that $ba = ba^{-1}a^2 = a^2ba^{-1} = aba^{-2} = a^2ab$.

Since $a^4 = b^4 = e$, any word in G can be reduced to one which is an alternating product of a^is and b^js, where $i, j \in \{1, 2, 3\}$. But since $a^2 = b^2$ is in the center, these can be "pulled out" to the left, everything has form either x or a^2x, where

$$x \in \{e, a, b, ab, ba, aba, bab, abab, baba, \dots\}.$$

But we also have the identity $ba = a^2ab$, so we can reduce everything to one of

$$e, a, b, ab, a^2, a^2a, a^2b, a^2ab.$$

Thus $|G| = 8$.

10. Show that $\langle a, b \mid aba^{-1}b^{-2},\ bab^{-1}a^{-2} \rangle \cong \{e\}$.

Solution. The relations imply $ab = b^2a$ and $ba = a^2b$. Thus

$$e = \underline{ab}b^{-1}a^{-1} = b^2ab^{-1}a^{-1} = b\underline{ba}b^{-1}a^{-1}ba^2bb^{-1}a^{-1} = ba,$$

and so $b = a^{-1}$. But then the first relation reduces to $e = aba^{-1}b^{-2} = aa^{-1}a^{-1}a^2 = a$, so $a = b = e$.