MATH 150A Winter 2020 - **Problem Set 7 solutions**

due February 28

1. Find a presentation in terms of generators and relations for the following groups.

   (a) $\mathbb{Z} \times \mathbb{Z}$

   $$\mathbb{Z} \times \mathbb{Z} = \langle x, y \mid xyx^{-1}y^{-1} \rangle.$$

   Here x and y are the generators for each copy of $\mathbb{Z}$. The only relation needed is that they commute with each other, $xy = yx$.

   (b) $C_3 \times C_3$

   $$C_3 \times C_3 = \langle x, y \mid x^3, y^3, xyx^{-1}y^{-1} \rangle.$$

   As above we have generators x and y for each copy of C_3 and the relation that they commute. Additionally $x^3 = 1$ and $y^3 = 1$.

   (c) S_3

   Since $S_3 \cong D_3$, we have the presentation

   $$D_3 = \langle r, s \mid r^3, s^2, rsrs \rangle.$$

   The symmetries of the triangle permute the 3 vertices, so r is a 3 cycle, $r = (1\ 2\ 3)$, and s is a swap, $s = (1\ 2)$.

   (d) A_4

   Similar to the previous example, S_4 can be viewed as the symmetries of a tetrahedron by permuting the 4 vertices. Then A_4 consists of the orientation-preserving symmetries, which are the rotations.

   Let x be one of the rotations that fixes one of the vertices. This is a 3-cycle, such as $x = (1\ 2\ 3)$, which fixes vertex 4. Let y be one that fixes another vertex, such as $y = (2\ 3\ 4)$, which fixes vertex 1. Conjugating x by y or y^{-1}, we can get the rotations the fix either of the other two vertices,

   $$yxy^{-1} = (1\ 3\ 4),$$

   $$y^{-1}xy = (1\ 4\ 2).$$

   so we can generate all eight 3-cycles. Additionally, we have the product

   $$xy = (1\ 2\ 3)(2\ 3\ 4) = (1\ 2)(3\ 4),$$

   and conjugating by y and y^{-1} gives the remaining two elements

   $$yx = (1\ 3)(2\ 4),$$

$$y^{-1}xy^2 = (1\ 4)(2\ 3).$$

Therefore $\{x, y\}$ generates A_4. Now we need the relations. Two easy ones are $x^3 = 1$ and $y^3 = 1$. Since xy is an elements with order 2, we have $xyxy = 1$. These are sufficient to present the group:

$$A_4 = \langle x, y \mid x^3, y^3, xyxy \rangle.$$

A brute-force method of showing that these relations are sufficient is to list out all the elements of A_4 in terms of the generators:

$$A_4 = \{1, x, x^2, y, xy, x^2y, y^2, xy^2, x^2y^2, y^2x, xy^2x, x^2y^2x\}$$

and then show that the product of each of these elements with either x or y can be put into the form of one of the other elements on the list using the relations. I don't know of a more efficient way to show this is true.

The above is just one of multiple presentations of A_4. The textbook gives another with 3 generators as the "tetrahedral group".

2. The group $G = \langle x, y \mid xyx^{-1}y^{-1} \rangle$ is called a *free abelian group*. Prove a mapping property of this group: If u and v are elements of an abelian group A, there is a unique homomorphism $\varphi : G \to A$ such that $\varphi(x) = u$ and $\varphi(y) = v$.

   Since φ is a homomorphism, it sends each word in x, y to the word with x replaced by u and y replaced by v. Therefore the map is uniquely determined by the facts that $\varphi(x) = u$ and $\varphi(y) = v$, and that it is a homomorphism. To show that this definition of φ is well-defined, we need to check that $\varphi(r) = 1$ for each relation r in the presentation of G, since $r = 1$ in G and $\varphi(1) = 1$.

   $$\varphi(xyx^{-1}y^{-1}) = uvu^{-1}v^{-1}.$$

   Since A is abelian, u and v commute, so $uvu^{-1}v^{-1} = 1$ as desired.

3. Let F be the free group on $\{x, y\}$. Prove that the elements $u = x^2$, $v = y^2$, and $z = xy$ generate a subgroup isomorphic to the free group on $\{u, v, z\}$.

   Let G be the free group on $\{u, v, z\}$ and $\varphi : G \to F$ be the homomorphism with $\varphi(u) = x^2$, $\varphi(v) = y^2$, $\varphi(z) = xy$. We want to show that φ is injective, in which case it is an isomporphism onto its image, the subgroup $\langle x^2, y^2, xy \rangle$ of F.

   We proceed by induction on $n \geq 1$ to prove that any reduced word $r \in G$ of length n satisfies:

   - if r ends in u then the reduced word of $\varphi(r)$ ends in x,
   - if r ends in u^{-1} then the reduced word of $\varphi(r)$ ends in $x^{-1}x^{-1}$,
   - if r ends in v then the reduced word of $\varphi(r)$ ends in yy,
   - if r ends in v^{-1} then the reduced word of $\varphi(r)$ ends in y^{-1},
   - if r ends in z then the reduced word of $\varphi(r)$ ends in xy or $x^{-1}y$,
   - if r ends in z^{-1} then the reduced word of $\varphi(r)$ ends in yx^{-1} or $y^{-1}x^{-1}$.

The base case is $n = 1$, where the reduced words with length 1 are $u, v, z, u^{-1}, v^{-1}, z^{-1}$, which satisfy the property.

For $n > 1$ let $r = r_1 \cdots r_n$ be a reduced word. Assume the property holds for all reduced words of length $n-1$. Let $r' = r_1 \cdots r_{n-1}$ which satisfies the property by the induction hypothesis. Since r is reduced, $r_n \neq r_{n-1}^{-1}$. We check that the property holds for each possible value of r_n:

- For $r_n = u$, there is only cancelation with $\varphi(r')$ if $r_{n-1} = z^{-1}$, in which case $\varphi(r)$ ends in yx or $y^{-1}x$. Otherwise $\varphi(r)$ ends in xx.
- For $r_n = u^{-1}$, there is never cancelation with $\varphi(r')$ so $\varphi(r)$ ends in $x^{-1}x^{-1}$.
- For $r_n = v$, there is never cancelation with $\varphi(r')$ so $\varphi(r)$ ends in yy.
- For $r_n = v^{-1}$, there is only cancelation with $\varphi(r')$ if $r_{n-1} = z$, in which case $\varphi(r)$ ends in xy^{-1} or $x^{-1}y^{-1}$. Otherwise $\varphi(r)$ ends in $y^{-1}y^{-1}$.
- For $r_n = z$, there is only cancelation with $\varphi(r')$ if $r_{n-1} = u^{-1}$, in which case $\varphi(r)$ ends in $x^{-1}y$. Otherwise $\varphi(r)$ ends in xy.
- For $r_n = z^{-1}$, there is only cancelation with $\varphi(r')$ if $r_{n-1} = v$, in which case $\varphi(r)$ ends in yx^{-1}. Otherwise $\varphi(r)$ ends in $y^{-1}x^{-1}$.

Therefore $\varphi(r) \neq 1$ for any $r \in G$ with reduced word of positive length. So $\ker \varphi$ is trivial and φ is injective.

4. Let F be the free group on a nonempty set S with $|S| = k$. How many elements with reduced word of length n does F have?

   Let $S = \{a_1, \ldots, a_k\}$. The elements of F are the words in alphabet

   $$S \cup S^{-1} = \{a_1, \ldots, a_k, a_1^{-1}, \ldots, a_k^{-1}\}.$$

   The only requirement for such a word to be reduced is that a letter is never followed by its inverse. To make a reduced word $x_1 x_2 \cdots x_n$ of length n, we will choose the letters one at a time. For the first letter we can choose any $x_1 \in S \cup S^{-1}$, so there are $2k$ choices. The second letter can be any element $x_2 \in S \cup S^{-1}$ except for x_1^{-1}, so there are $2k - 1$ choices. Similarly, we have $2k - 1$ choices for each letter after that, up to x_n. Therefore the total number of possible reduced words of length n is

   $$2k(2k-1)^{n-1}.$$

5. (a) Prove that the additive group of $\mathbb{Q}$ is not finitely generated.

   Let S be a finite set of rational numbers,

   $$S = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_k}{b_k} \right\}$$

   where $a_i, b_i \in \mathbb{Z}$ and $b_i > 0$ for each $i = 1, \ldots, k$. Let d be the least common multiple of $b_1, \ldots, b_k$. Then each element of S can be rewritten as a fraction with denominator d, by $a_i/b_i = a_i'/d$ where a_i' is the integer $a_i d/b_i$.

The subgroup generated by S consists of all sums and differences of its elements, so $g \in \langle S \rangle$ has the form

$$g = n_1 \frac{a_1'}{d} + \cdots + n_k \frac{a_k'}{d} = \frac{n_1 a_1' + \cdots + n_k a_k'}{d}$$

for some integers $n_1, \ldots, n_k$. Since all elements of $\langle S \rangle$ can be written with denominator d, it has no positive elements less than $1/d$. In particular the rational number $1/(d+1)$ is not in $\langle S \rangle$. Therefore S does not generate $\mathbb{Q}$.

(b) Prove that the multiplicative group $\mathbb{Q}^\times$ is not finitely generated.

Again let S be a finite set of rational numbers,

$$S = \left\{ \frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_k}{b_k} \right\}.$$

Every element g of the subgroup generated by S has the form

$$g = \left(\frac{a_1}{b_1} \right)^{n_1} \cdots \left(\frac{a_k}{b_k} \right)^{n_k} = a_1^{n_1} b_1^{-n_1} \cdots a_k^{n_k} b_k^{-n_k}$$

for some integers $n_1, \ldots, n_k$. Suppose $g \in \langle S \rangle$ is an integer prime number. Then by Euclid's Lemma, g must divide at least one of $a_1, \ldots, a_k, b_1, \ldots, b_k$. There are only a finite number of primes that satisfy this property. Therefore there exists a prime p that divides none of them, and so p is not in $\langle S \rangle$. Therefore S does not generate $\mathbb{Q}^\times$.