Homework Assignment 5

Due Friday, February 28

In class we classified all subgroups of the finite cyclic group Z_n, putting putting them in bijection with the divisors of n. Let's begin by taking care of the infinite case.

1. Let $H = \langle x \rangle$ be an infinite cyclic group. Let a, b be integers. Show $\langle x^a \rangle = \langle x^b \rangle$ if and only if $b = \pm a$. Conclude that the subgroups of H are indexed by the natural numbers. Identifying H with $\mathbb{Z}$, describe all the subgroups of $\mathbb{Z}$ (you may use words).

   Proof. If $b = a$ then certainly $\langle x^a \rangle = \langle x^b \rangle$. Suppose instead $b = -a$. Then $x^b = (x^a)^{-1} \subseteq \langle x^a \rangle$ so that $\langle x^b \rangle \leq \langle x^a \rangle$. An identical argument shows $\langle x^a \rangle \leq \langle x^b \rangle$ so that they are equal.

   Conversely, suppose $\langle x^a \rangle = \langle x^b \rangle$. Then $x^a = (x^b)^l = x^{bl}$, and $x^b = (x^a)^k = x^{ak}$. Therefore $x^b = x^{ak} = x^{blk}$. As x has infinite order, all of its powers are distinct, so that $b = blk$. Thus $lk = 1$. Since $l, k \in \mathbb{Z}$ this implies the are both 1 or -1. In each case $a = \pm b$ and we are done.

   In particular, we have shown that the subgroups of H are precisely the sets $\langle x^a \rangle$, for each $a \in \mathbb{N}$. If $H = \mathbb{Z}$, then the subgroup forresponding to the natural number a is $a\mathbb{Z} = \{0, \pm a, \pm 2a, \cdot\}$ the multiples of a. $\square$

2. A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.

   (a) Prove that every finite group is finitely generated.

   Proof. It is always true that all the elements of a group generate a group: $H = \langle H \rangle$. So we can take $A = H$ which is a finite set whenever H is a finite group.

   Note: the generating set we specified here will often have redundancies, for instance it will list $Z_3 = \langle 1, x, x^2 \rangle$ when it could just be $\langle x \rangle$. But since we are just looking to exhibit a finite generating set this is no problem. $\square$

   (b) Prove that $\mathbb{Z}$ is finitely generated.

   Proof. Since $\mathbb{Z} = \langle 1 \rangle$ is cyclic we can take $A = \{1\}$. Note that we have now showed every cyclic group is finitely generated. $\square$

   (c) Prove that every finitely generated subgroup of the additive group $H \leq \mathbb{Q}$ is cyclic. (Hint, show that H is a subgroup of a cyclic subgroup of $\mathbb{Q}$).

   Proof. Let A be the finite generating set and, and write it as

   $$A = \left\{ \frac{a_1}{b_1}, \cdots, \frac{a_n}{b_n} \right\}.$$

   Let $b = b_1 \cdot b_2 \cdots b_n$. In particular, for all i we have $b = c_i b_i$ for some c_i. Then for every i we have:

   $$\frac{a_i}{b_i} = \frac{c_i a_i}{c_i b_i} = \frac{c_i a_i}{b} = c_i a_i \left(\frac{1}{b} \right) \in \left\langle \frac{1}{b} \right\rangle.$$

   Since every element of A is in $\langle 1/b \rangle$, the subgroup generated by A is too. That is $\langle A \rangle \leq \langle 1/b \rangle$. But $\langle 1/b \rangle$ is cyclic, and every subgroup of a cyclic group is cyclic, so that $\langle A \rangle$ is cyclic as well. $\square$

(d) Conclude that $\mathbb{Q}$ is not finitely generated.

Proof. By part (c), if $\mathbb{Q}$ is finitely generated, it is cyclic. Thus we would have $\mathbb{Q} = \langle \frac{a}{b} \rangle$ for some $a, b \in \mathbb{Z}$. In particular, there would be some $n \in \mathbb{Z}$ such that $n\frac{a}{b} = \frac{1}{2b}$. Solving for n gives

$$n = \frac{1}{2a},$$

a contradiction as n has to be an integer. Thus $\mathbb{Q}$ is not cyclic, and therefore not finitely generated. □

3. We now classify all groups of order 4. In particular, up to isomorphism there are only 2, Z_4 and V_4.

(a) Let G be a group and suppose that the order of every element of G is ≤ 2. Show that G is abelian.

Proof. Let $x, y \in G$. In any group there is some c such that $xy = cyx$. Indeed, solving for c gives

$$c = xyx^{-1}y^{-1}.$$

We hope to compute that $c = 1$. As x and y both have order ≤ 2, we have $x^{-1} = x$ and $y^{-1} = y$. Thus:

$$c = xyx^{-1}y^{-1} = xyxy = (xy)(xy) = 1,$$

as $|xy| \leq 2$ as well.
Note: in general c is called the *commutator* of x and y and is often denoted $[x, y]$. It measures how well x and y commute. It will be studied in more detail in homework 6. □

(b) Show that if $|G| = 4$ then G is abelian. (Hint: by the takehome, for every $x \in G$, $|x|$ divides $|G|$).

Proof. If G has an element x of order 4 then $G = \langle x \rangle \cong Z_4$ is cyclic, and therefore abelian. Otherwise, every element of G has order < 4, but the order of every element must at least divide 4 so every element of G has order ≤ 2. Thus by part (a) G must be abelian. □

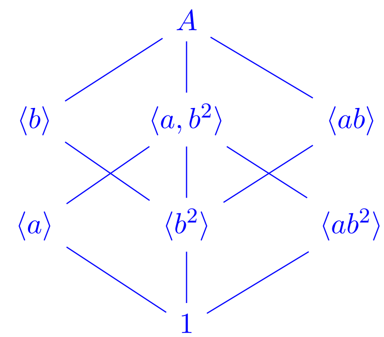
(c) Deduce if $|G| = 4$ then $G \cong Z_4$ or $G \cong V_4$. (Hint, if G is not Z_4 then start filling out a multiplication table and your hand will be forced).

Proof. If G is not Z_4 then $G = \{1, a, b, c\}$ with $|a| = |b| = |c| = 2$. Let's compute ab. If $ab = a$ then $b = 1$, so this cannot happen. Similarly, $ab \neq b$, and as $a^{-1} = a \neq b$, we also have $ab \neq 1$. Thus $ab = c$. As G is abelian by part (b) we have $ba = c$ as well. And from here we derive that $ac = b$ and $bc = a$ using that every element is its own inverse. This is precisely the multplication rule for V_4. □

4. It would be nice if a group was classified by it's subgroup lattice. Unfortunately, this is not the case. In this exercise we will draw the latices of two nonisomorphic groups of order 16 with the same lattice of subgroups. We follow Dummit and Foote Chapter 2.5 Exercises 12-14.

(a) Consider the group $A = Z_2 \times Z_4 = \langle a, b | a^2 = b^4 = 1, ab = ba \rangle$. It has order 8, and has 3 subgroups of order 4. $\langle a, b^2 \rangle \cong V_4$, $\langle b \rangle \cong Z_4$ and $\langle ab \rangle \cong Z_4$. Every proper subgroup is contained in one of these 3. Draw the lattice of A.

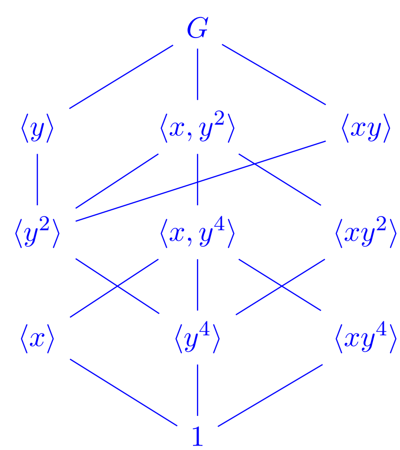
Proof. Notice that $\langle a, b^2 \rangle$ has 3 subgroups of order 2, given by $\langle a \rangle, \langle b^2 \rangle$ and $\langle ab^2 \rangle$. The other 2 only have one subgroup of order 2. In the first case it is $\langle b^2 \rangle$, and in the second it is $\langle (ab)^2 \rangle$. But we notice that since A is abelian, $(ab)^2 = a^2 b^2 = b^2$. Thus the lattice looks as follows:



□

(b) Consider the group $G = Z_2 \times Z_8 = \langle x, y | x^2 = y^8 = 1, xy = yx \rangle$. It has order 16 and has 3 subgroups of order 8. $\langle x, y^2 \rangle \cong Z_2 \times Z_4$, $\langle y \rangle \cong Z_8$, and $\langle xy \rangle \cong Z_8$. Every proper subgroup of G is contained in one of these 3. Draw a lattice of all subgroups of G, giving each subgroup in terms of at most two generators. (Note, you know the subgroups of the cyclic groups of order 8, and computed those of $Z_2 \times Z_4$ in part (a), now you just must see where they overlap).

Proof. The lattice below $\langle x, y^2 \rangle$ should have exactly the same shape as the lattice for A in part (a), but with a replaced by x and b by y^2. The lattice below $\langle y \rangle$ is a chain of subgroups generated by y^2, y^4 and 1. Similarly, the subgroups below $\langle xy \rangle$ are those generated by $(xy)^2 = y^2$, and $(xy^4) = y^4$. Thus the lattice looks as follows.



□

(c) Consider the group $M = \langle u, v | u^2 = v^8 = 1, vu = uv^5 \rangle$. This is often called the *modular group* of order 16. It has three subgroups of order 8, $\langle u, v^2 \rangle \cong Z_2 \times Z_4$, $\langle v \rangle \cong Z_8$, and $\langle uv \rangle \cong Z_8$. Show that the latice of subgroups of M is the same as the one for G. Notice also that $M \not\cong G$ since M is not abelian.

Proof. Above we used that $(xy)^2 = x^2y^2 = y^2$ to show that the subgroup of order 4 in $\langle xy \rangle$ was $\langle y^2 \rangle$, and we used that $(xy^2)^2 = x^2y^4 = y^4$ to show that the subgroup of order 2 in $\langle xy^2 \rangle$ was $\langle y^4 \rangle$. Here we must be a bit more careful.

We first compute the subgroup of order 4 in $\langle uv \rangle$, by noticing that

$$(uv)^2 = (uv)(uv) = u(vu)v = u(uv^5)v = u^2v^6 = v^6.$$

Note that this is in $\langle v \rangle$ which is cyclic of order 8, so that $\langle v^6 \rangle = \langle v^{\gcd(6,8)} \rangle = \langle v^2 \rangle$. This lines up with the abelian case. Next let's compute the subgroup of order 2 in $\langle uv^2 \rangle$.

$$(uv^2)^2 = (uv^2)(uv^2) = uv(vu)v^2 = uv(uv^5)v^2 = u(vu)(v^7) = u(uv^5)v^7 = u^2v^{12} = v^4.$$

Thus the subgroup of order 2 is $\langle v^4 \rangle$ again lining up with the abelian case. Since these were the only times we had to commute variables in part (b), the rest goes through identically, so that we have the following lattice.