Name: Adam Frank **September 17, 2020**

Math 437: Homework Section 1

1. (2.1.1(b))
   Prove that the set of complex numbers of absolute value 1 in the complex plane form a subgroup under multiplication.

   Proof. Any such number can be represented by $e^{i\theta}$ for some choice of θ. Hence for any two such numbers

   $$e^{i\theta_1}(e^{i\theta_2})^{-1} = e^{i(\theta_1-\theta_2)}$$

   which is again in the set. Therefore it is a subgroup. □

2. (2.1.9)
   Prove that $SL_n(F) \leq GL_n(F)$.

   Proof. If $M, N \in SL_n(F)$ then since $|N| \neq 0$ we have that N^{-1} exists. Also $|N^{-1}| = \frac{1}{|N|} = 1$. So

   $$|MN^1| = |M||N^{-1}| = 1 \cdot 1 = 1$$

   Hence $MN^{-1} \in SL_n(F)$. □

3. (2.2.3)
   Prove that if A and B are subsets of G and $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

   Proof. First we establish the subset relation. If $x \in C_G(B)$ then $\forall y \in B$ we have $xy = yx$. Since $A \subseteq B$ then in particular this also holds for all $y \in A$.

   Next we let $x, y \in C_G(B)$ and we let $b \in B$ then $(xy^{-1})b = xby^{-1} = bxy^{-1}$ so $xy^{-1} \in C_G(B)$.

   This depends on the fact that if y commutes with b then so does y^{-1}. We can see this from the fact that $xy = yx$ implies $y^{-1}x = xy^{-1}$. □

4. (2.2.6(b))
   Let $H \leq G$. Show that $H \leq C_G(H)$ if and only if H is abelian.

   Proof. If $H \leq C_G(H)$ then for all $a, b \in H$ we have that $a \in C_G(H)$ and hence $ab = ba$. □

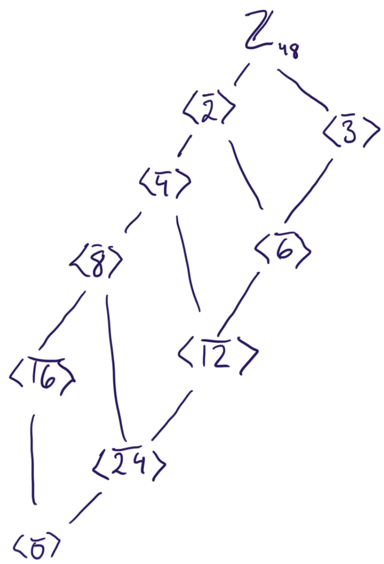
5. (2.2.9)
   For any subgroup H of G and non-empty subset $A \subseteq G$, define $N_H(A) = \{h \in H | hAh^{-1} = A\}$. Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H.

   Proof. If $x \in N_H(A)$ then $x \in G$ and $xAx^{-1} = A$ so $x \in N_G(A)$. Also directly we have $x \in H$. Hence $x \in N_G(A) \cap H$. Conversely, if $x \in N_G(A) \cap H$ then x immediately satisfies both conditions for $x \in N_H(A)$.

   Now because $N_G(A)$ is equal to the intersection of two subgroups it must be a subgroup. □

6. (2.3.6)
   In $\mathbb{Z}/48\mathbb{Z}$ write out all elements of $\langle \overline{a} \rangle$ for every $\overline{a}$. Find all inclusions between subgroups in $\mathbb{Z}/48\mathbb{Z}$.

Proof. The following lattice shows all of the subgroups of $\mathbb{Z}/48\mathbb{Z}$.



The following facts then entail all of the set memberships and subgroup relationships that exist in $\mathbb{Z}/48\mathbb{Z}$.

$$\begin{aligned}
\mathbb{Z}/48\mathbb{Z} &= \langle\overline{1}\rangle = \langle\overline{5}\rangle = \langle\overline{7}\rangle = \langle\overline{11}\rangle = \langle\overline{13}\rangle = \langle\overline{17}\rangle = \langle\overline{19}\rangle = \langle\overline{23}\rangle \\
&= \langle\overline{25}\rangle = \langle\overline{29}\rangle = \langle\overline{31}\rangle = \langle\overline{35}\rangle = \langle\overline{37}\rangle = \langle\overline{41}\rangle = \langle\overline{43}\rangle = \langle\overline{47}\rangle
\end{aligned}$$

$$\langle\overline{2}\rangle = \langle\overline{10}\rangle = \langle\overline{14}\rangle = \langle\overline{22}\rangle = \langle\overline{26}\rangle = \langle\overline{34}\rangle = \langle\overline{38}\rangle = \langle\overline{46}\rangle$$

$$\langle\overline{3}\rangle = \langle\overline{9}\rangle = \langle\overline{15}\rangle = \langle\overline{21}\rangle = \langle\overline{27}\rangle = \langle\overline{33}\rangle = \langle\overline{39}\rangle = \langle\overline{45}\rangle$$

$$\langle\overline{4}\rangle = \langle\overline{20}\rangle = \langle\overline{28}\rangle = \langle\overline{44}\rangle$$

$$\langle\overline{6}\rangle = \langle\overline{18}\rangle = \langle\overline{30}\rangle = \langle\overline{36}\rangle = \langle\overline{42}\rangle$$

$$\langle\overline{8}\rangle = \langle\overline{40}\rangle$$

$$\langle\overline{12}\rangle = \langle\overline{36}\rangle$$

□

7. (2.3.18)
Show that if H is any group and $h \in H$ with $h^n = 1$ then there is a unique homomorphism from $Z_n = \langle x\rangle$ to H such that $x \mapsto h$.

Proof. That there exists such a homomorphism: Define $\varphi(x^i) = h^i$. To see that this is a homomorphism let $x^i, x^j \in Z_n$. Then $\varphi(x^i x^j) = h^{i+j} = h^i h^j = \varphi(x^i)\varphi(x^j)$.

Now to see that this is unique, let ψ be any other homomorphism with $\psi(x) = h$. Then for any $x^i \in Z_n$ we must have $\psi(x^i) = \overbrace{\psi(x)\cdots\psi(x)}^{i \text{ times}} = \overbrace{\varphi(x)\cdots\varphi(x)}^{i \text{ times}} = \varphi(x^i)$. So in fact $\psi = \varphi$. □

8. (2.3.24(b))
   Let G be a finite group and $x \in G$. Prove that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x \rangle)$ [Show first that $gx^kg^{-1} = (gxg^{-1})^k = x^{ak}$ for any integer k so that $g\langle x\rangle g^{-1} \leq \langle x \rangle$. If x has order n show the elements $gx^ig^{-1}, i = 0, 1, \ldots, n-1$ are distinct, so that $|g\langle x\rangle g^{-1}| = |\langle x \rangle| = n$ and conclude equality.]

   Proof. We can easily see

$$gx^kg^{-1} = \overbrace{(gxg^{-1})\cdots(gxg^{-1})}^{k \text{ times}} = (gxg^{-1})^k = (x^a)^k = x^{ak}$$

   So we now have $g\langle x\rangle g^{-1} \subseteq \langle x \rangle$, and clearly this is closed under inverses and products, so $g\langle x\rangle g^{-1} \leq \langle x \rangle$.
   Now suppose $gx^ig^{-1} = gx^jg^{-1}$ for $i < j$ and $i, j \in \{0, 1, \ldots, n-1\}$. Then clearly $x^i = x^j$ and so $\mathbb{1} = x^{j-i}$. Since the order of x is n and $j - i < n$ then $j - i = 0$ hence $i = j$, a contradiction. $\lightning$
   This shows all the elements gx^ig^{-1} are distinct for $i = 0, 1, \ldots, n-1$. So $g\langle x\rangle g^{-1}$ has at least n elements. As a subset of $\langle x \rangle$ which has exactly n elements, these sets must be equal. Therefore $g \in N_G(\langle x \rangle)$ by definition. □

9. (2.4.8)
   Prove that $S_4 = \langle (1\ 2\ 3\ 4), (1\ 2\ 4\ 3) \rangle$.

   Proof. We prove that from these two we can generate any transposition. It then follows that we can generate any permutation.

$$\begin{aligned} (1\ 2\ 3\ 4)(1\ 2\ 4\ 3)^3(1\ 2\ 3\ 4) &= (1\ 2) \\ (1\ 2\ 4\ 3)^2(1\ 2\ 3\ 4) &= (1\ 3) \\ (1\ 2\ 3\ 4)^2(1\ 2\ 4\ 3) &= (1\ 4) \end{aligned}$$

   Now somewhat famously, because I have every transposition of the form $(1, i)$ for $i = 2, \ldots, n$ then I can generate any permutation I want. This is because

$$(i, j) = (1, i)(1, j)(1, i)$$

   And of course, now that we know this generates every transposition, then we can generate any cycle by writing it in a transposition decomposition.

$$(a_1\ a_2\ \ldots\ a_k) = (a_1\ a_k)\cdots(a_1\ a_3)(a_1\ a_2)$$

   Since this generates every cycle, and we know that every permutation has a cycle decomposition, then this generates every permutation. □

10. (2.4.13)
Prove that the multiplicative group of positive rationals is generated by $\{\frac{1}{p} | p \text{ is a prime }\}$.

Proof. Let G be the group generated by $\{\frac{1}{p} | p \text{ is a prime }\}$. As a first step let's see that $1 \in G$, but this is clear because $\frac{1}{2} \in G$ and $\left(\frac{1}{2}\right)^{-1} \in G$.
Let $r \in \mathbb{Q}^+$ and suppose $r = a/b$ where $a, b \in \mathbb{Z}^+$. Now let

$$a = x_1^{e_1} x_2^{e_2} \cdots x_m^{e_m}$$

$$b = y_1^{f_1} y_2^{f_2} \cdots y_n^{f_n}$$

be the prime decompositions of a and b. Now of course if either of these is 1, we have already shown it is in G. Otherwise, each $\frac{1}{y_i} \in G$ and so is $\frac{1}{y_i^{f_i}}$ and hence so is $1/b$.

Also each x_i is $\frac{1}{x_i}$ which is the multiplicative inverse of some element in the generating set. So $x_i \in G$ and so is $x_i^{e_i}$ and so is a.

In all cases we have seen $a, \frac{1}{b} \in G$ and so $a/b \in G$. $\square$

11. (2.4.19)
A non-trivial abelian group A is called *divisible* if for each element $a \in A$ and each non-zero integer k, there is an element $x \in A$ such that $x^k = a$, i.e. each element has a kth root.

(a) Prove that the additive group of rational numbers $\mathbb{Q}$, is divisible.

(b) Prove that no finite abelian group is divisible.

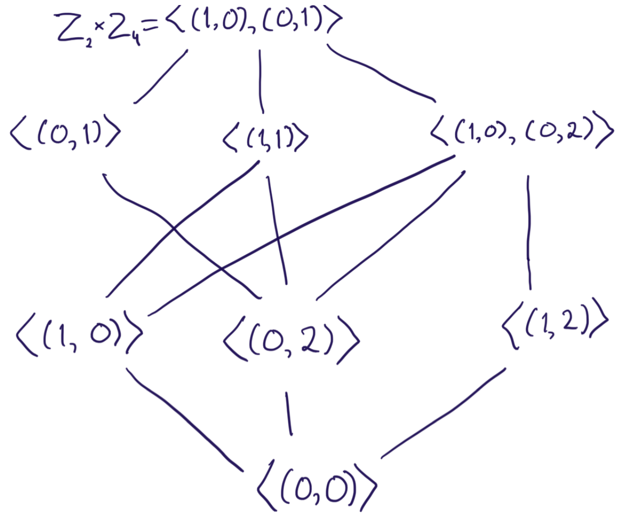
Proof. (a) For any $a/b \in \mathbb{Q}$ the number $\frac{a}{kb} \in \mathbb{Q}$ and since this is the additive group, that makes this the kth root.

(b) Say that G is a non-trivial abelian group with order $n = |G| > 1$. Let $x \in G$ be a non-identity element. If G is divisible then x has an nth root, call this y. Then $y^n = x$ but since n is the order of the group, $y^n = \mathbb{1} = x$. A contradiction. $\lightning$ $\square$

12. (2.5.7)
Find the center of D_{16}.

Proof. We have already seen that the only non-identity element of the dihedral group which commutes with everything, is the rotation by 180-degrees, when this is an element (homework 1). Hence $Z(D_{16}) = \{\mathbb{1}, r^4\}$. $\square$

13. (2.5.12)
The group $A = Z_2 \times Z_4 = \langle a, b | a^2 = b^4 = \mathbb{1},\ ab = ba \rangle$ has order 8 and three subgroups of order 4: $\langle a, b^2 \rangle \cong V_4$, $\langle b \rangle \cong Z_4$, and $\langle ab \rangle \cong Z_4$, and every proper subgroup is in one of these. Draw the lattice of all subgroups of A, giving each subgroup in terms of at most two generators.


$\mathbb{Z}_2 \times \mathbb{Z}_4 = \langle (1,0), (0,1) \rangle$
$\langle (0,1) \rangle$
$\langle (1,1) \rangle$
$\langle (1,0), (0,2) \rangle$
$\langle (1,0) \rangle$
$\langle (0,2) \rangle$
$\langle (1,2) \rangle$
$\langle (0,0) \rangle$