Dummit & Foote Ch. 2.4: Subgroups Generated by Subsets of a Group

Scott Donaldson

Jul. - Aug. 2023

1. (7/13/23)

Prove that if H is a subgroup of G then $\langle H \rangle = H$.

Proof. Let $H \leq G$. To show that $\langle H \rangle = H$, we must show that each is contained in the other. By definition, $H \subseteq \langle H \rangle$, so it remains to be proven that $\langle H \rangle \subseteq H$.

Let $h \in \langle H \rangle$. Recall that:

$$\langle H \rangle = \bigcap_{\substack{H \subseteq K \\ K \leq G}} K,$$

that is, for all subset $K \leq G$ with $H \subseteq K$, we have $h \in K$. In particular, since H is a subgroup of G, we have $h \in H$, since $H \leq G$ and $H \subseteq H$. Therefore $\langle H \rangle \subseteq H$, and it follows that $\langle H \rangle = H$. □

2. (7/17/23)

Prove that if A is a subset of B then $\langle A \rangle \leq \langle B \rangle$. Give an example where $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle$.

Proof. Let G be a group and let $A \subseteq B \subseteq G$. Recall that one definition of $\langle A \rangle$ is the set of all finite words of elements and inverses of elements of A, that is, every element of $\langle A \rangle$ can be written $a_1^{\varepsilon_1} a_2^{\varepsilon_2} ... a_n^{\varepsilon_n}$, where $n \in \mathbb{Z}, n \geq 0$ and $a_i \in A, \varepsilon_i = \pm 1$ for each i. Since A is a subset of B, $a_i \in A \Rightarrow a_i \in B$, and so each element $a_1^{\varepsilon_1} a_2^{\varepsilon_2} ... a_n^{\varepsilon_n} \in \langle A \rangle$ is also in $\langle B \rangle$. Therefore $\langle A \rangle \leq \langle B \rangle$.

Now let $G = \mathbb{Z}/3\mathbb{Z}$, $A = \{1\}$, and $B = \{0, 1\}$. Then we have $A \subseteq B$ with $A \neq B$ but $\langle A \rangle = \langle B \rangle = G$. □

3. (7/17/23)

Prove that if H is an abelian subgroup of G then $\langle H, Z(G) \rangle$ is abelian. Give an explicit example of an abelian subgroup H of a group G such that $\langle H, C_G(H) \rangle$ is not abelian.

Proof. Let G be a group and let H be an abelian subgroup of G. Recall that $Z(G) = \{g \in G \mid xg = gx \text{ for all } x \in G\}$, that is, the set of elements of G that commute with every element of G. We will show that $\langle H, Z(G)\rangle$ is an abelian subgroup of G.

First, we will show that the product of any two elements commutes with both elements. Let $a, b \in G$ be commuting elements. Then:

$$(ab)a = aba = aab = a(ab), \text{ and } (ab)b = abb = bab = b(ab),$$

as desired.

Now the generated subgroup $\langle H, Z(G)\rangle$ is constructed from finite words of elements and inverses of elements from H and $Z(G)$. Since H is an abelian subgroup and elements of $Z(G)$ (and therefore their inverses) commute with every element of G (and therefore H), it follows that every element in $\langle H, Z(G)\rangle$ is a product of commuting elements. Every such element therefore commutes with every other element in H and $Z(G)$, as well as any other product of elements of H and $Z(G)$. Thus $\langle H, Z(G)\rangle$ is an abelian subgroup of G.

However, it does not follow that $\langle H, C_G(H)\rangle$ is an abelian subgroup of G. Let $G = D_8$ and $H = \{1, r^2\}$. The centralizer of H in G is all of G, since every element of H commutes with every other element of G (that is, $H = Z(G)$). Then the generated subgroup $\langle H, C_G(H)\rangle = \langle H, G\rangle = G$, which is non-abelian. □

4. (7/17/23)

Prove that if H is a subgroup of G then H is generated by the set $H - \{1\}$.

Proof. Let $H \leq G$ and consider $\langle H - \{1\}\rangle$. If $H = \{1\}$, then $H - \{1\} = \emptyset$, and so by definition $\langle H - \{1\}\rangle = \{1\} = H$.

Suppose $H \neq \{1\}$. Then there exists some $h \in H$ with $h \neq 1$. Since H is a subgroup, it is closed under inverses, so $h^{-1} \in H$. We generate $\langle H - \{1\}\rangle$ by taking finite products of elements of H, and so $hh^{-1} = 1 \in \langle H - \{1\}\rangle$. Further, we cannot construct any element outside of H by taking products of elements of H, so we must therefore have $\langle H - \{1\}\rangle = (H - \{1\}) \cup \{1\} = H$. □

5. (7/20/23)

Prove that the subgroup generated by any two distinct elements of order 2 in S_3 is all of S_3.

Proof. The elements of order 2 in S_3 are $(1,2), (1,3)$, and $(2,3)$. Since any two of these elements permute one of $\{1,2,3\}$ to the other two, without loss of generality we can consider the subgroup generated by a single pair of them. We will consider the subgroup generated by $(1,2)$ and $(1,3)$.

The subgroup contains the identity element, since $(1,2)(1,2) = (1)$. It also contains both elements of order 3, since $(1,2)(1,3) = (1,3,2)$ and $(1,3)(1,2) =$

$(1,2,3)$. Finally, the subgroup contains the third element of order 2, since $(1,2)(1,2,3) = (2,3)$. Together these are all the elements of S_3.

Therefore the subgroup generated by any two elements of S_3 is all of S_3. □

6. (7/20/23)

Prove that the subgroup of S_4 generated by $(1,2)$ and $(1,2)(3,4)$ is a noncyclic group of order 4.

Proof. Let us construct the subgroup of S_4 generated by $(1,2)$ and $(1,2)(3,4)$. Both elements have order 2, so we will not consider any higher powers of each. Their product is $(3,4)$, which also has order 2. At this point the subgroup consists of $\{(1), (1,2), (1,2)(3,4), (3,4)\}$. Taking the product of $(3,4)$ with either of $(1,2)$ or $(1,2)(3,4)$ results in the other element, respectively. Therefore there is no way to obtain new elements not already in this subgroup.

Thus the subgroup of S_4 generated by $(1,2)$ and $(1,2)(3,4)$ has order 4. Further, it is noncyclic, since it contains no elements of order 4 (in fact, it is isomorphic to the Klein 4-group V_4). □

7. (7/22/23)

Prove that the subgroup of S_4 generated by $(1,2)$ and $(1,3)(2,4)$ is isomorphic to the dihedral group of order 8.

Proof. Let $A \leq S_4 = \langle (1,2), (1,3)(2,4) \rangle$. Now A naturally contains the product $(1,2) \cdot (1,3)(2,4) = (1,3,2,4)$. So let us consider a map $\varphi : D_8 \to A$ defined by $\varphi(s) = (1,2)$ and $\varphi(r) = (1,3,2,4)$. In order to show that φ is an isomorphism, we must show that the generators and relations in D_8 hold under φ in A.

In S_4, $(1,2)$ has order 2 and $(1,3,2,4)$ has order 4 (like s and r respectively in D_8). It remains to be shown that the relation $sr = r^{-1}s$ holds under φ. Now $\varphi(s)\varphi(r) = (1,2) \cdot (1,3,2,4) = (1,3)(2,4)$. Also, $\varphi(r)^{-1}\varphi(s) = (1,3,2,4)^{-1} \cdot (1,2) = (1,4,2,3) \cdot (1,2) = (1,3)(2,4)$, and so the relation holds as well under φ.

So far, this shows that φ is a homomorphism into A; it remains to be shown that is is both one-to-one and onto. The below table demonstrates exhaustively that φ is injectiv, because no two elements in D_8 have the same image under φ in A:

$x \in D_8$	$\varphi(x) \in A$
1	(1)
r	$(1,3,2,4)$
r^2	$(1,2)(3,4)$
r^3	$(1,4,2,3)$
s	$(1,2)$
sr	$(1,3)(2,4)$
sr^2	$(3,4)$
sr^3	$(1,4)(2,3)$

This shows that A contains at least 8 elements, but not that it contains exactly 8 elements. The multiplication table below shows that A is closed among the 8 elements we know to be included. It is not possible to generate any other element of S_4 outside of A, and thus φ is an isomorphism, and so $A = \langle (1,2), (1,3)(2,4) \rangle$ is isomorphic to D_8.

(1)	$(1,3,2,4)$	$(1,2)(3,4)$	$(1,4,2,3)$	$(1,2)$	$(1,3)(2,4)$	$(3,4)$	$(1,4)(2,3)$
$(1,3,2,4)$	$(1,2)(3,4)$	$(1,4,2,3)$	(1)	$(1,3)(2,4)$	$(3,4)$	$(1,4)(2,3)$	$(1,2)(3,4)$
$(1,2)(3,4)$	$(1,4,2,3)$	(1)	$(1,3,2,4)$	$(3,4)$	$(1,4)(2,3)$	$(1,2)$	$(1,3)(2,4)$
$(1,4,2,3)$	(1)	$(1,3,2,4)$	$(1,3,2,4)$	$(1,4)(2,3)$	$(1,2)(3,4)$	$(1,3)(2,4)$	$(3,4)$
$(1,2)$	$(1,4)(2,3)$	$(3,4)$	$(1,3)(2,4)$	(1)	$(1,4,2,3)$	$(1,2)(3,4)$	$(1,3,2,4)$
$(1,3)(2,4)$	$(1,2)(3,4)$	$(1,4)(2,3)$	$(3,4)$	$(1,3,2,4)$	(1)	$(1,4,2,3)$	$(1,2)(3,4)$
$(3,4)$	$(1,3)(2,4)$	$(1,2)$	$(1,4)(2,3)$	$(1,2)(3,4)$	$(1,3,2,4)$	(1)	$(1,4,2,3)$
$(1,4)(2,3)$	$(3,4)$	$(1,3)(2,4)$	$(1,2)(3,4)$	$(1,4,2,3)$	$(1,2)(3,4)$	$(1,3,2,4)$	(1)

□

8. (7/24/23)

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

Proof. By Lagrange's theorem, the order of a subgroup must divide the order of its parent group. Therefore it suffices to show that, if the subgroup of S_4 generated by $(1,2,3,4)$ and $(1,2,4,3)$ contains more than half of the elements of S_4, then it must be all of S_4.

Beginning with the two elements $(1,2,3,4)$ and $(1,2,4,3)$, we obtain the cyclic subgroups generated by each. For $(1,2,3,4)$, this is $(1), (1,3)(2,4)$, and $(1,4,3,2)$. For $(1,2,4,3)$, we also obtain $(1,4)(2,3)$ and $(1,3,4,2)$. We now have 7 elements.

We can obtain as products of the generating elements the 3-cycles $(1,3,2) = (1,2,3,4)(1,2,4,3)$ and $(1,4,2) = (1,2,4,3)(1,2,3,4)$ [9 elements]. Then, we can obtain a pair of 2-cycles, namely $(2,4) = (1,3,2)(1,2,4,3)$ and $(2,3) = (1,4,2)(1,2,3,4)$ [11 elements]. Next, we can obtain two more 3-cycles $(2,3,4) = (2,4)(2,3)$ and $(2,4,3) = (2,3)(2,4)$ [13 elements].

At this point, noting that the order of S_4 is $4! = 24$, we can stop, because we have generated more than half of its elements. Since the subgroup generated by $(1,2,3,4)$ and $(1,2,4,3)$ contains more than half of the elements of S_4, it must in fact be S_4. □

9. (7/24/23)

Prove that $SL_2(\mathbb{F}_3)$ is the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$.

Proof. We first construct $SL_2(\mathbb{F}_3)$ by considering all those 2x2 matrices with entries from $\{0, 1, 2\}$ whose determinant is 1 (under modular arithmetic). These, and only these, are:

$$\begin{pmatrix}0 & 1\\ 2 & 0\end{pmatrix} \quad \begin{pmatrix}0 & 1\\ 2 & 1\end{pmatrix} \quad \begin{pmatrix}0 & 1\\ 2 & 2\end{pmatrix} \quad \begin{pmatrix}0 & 2\\ 1 & 0\end{pmatrix} \quad \begin{pmatrix}0 & 2\\ 1 & 1\end{pmatrix} \quad \begin{pmatrix}0 & 2\\ 1 & 2\end{pmatrix}$$
$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix} \quad \begin{pmatrix}1 & 1\\ 2 & 0\end{pmatrix}$$
$$\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix} \quad \begin{pmatrix}1 & 2\\ 1 & 0\end{pmatrix} \quad \begin{pmatrix}1 & 2\\ 2 & 2\end{pmatrix}$$
$$\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix} \quad \begin{pmatrix}2 & 0\\ 1 & 2\end{pmatrix} \quad \begin{pmatrix}2 & 0\\ 2 & 2\end{pmatrix} \quad \begin{pmatrix}2 & 1\\ 0 & 2\end{pmatrix} \quad \begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix} \quad \begin{pmatrix}2 & 1\\ 2 & 0\end{pmatrix}$$
$$\begin{pmatrix}2 & 2\\ 0 & 2\end{pmatrix} \quad \begin{pmatrix}2 & 2\\ 1 & 0\end{pmatrix} \quad \begin{pmatrix}2 & 2\\ 2 & 1\end{pmatrix}$$

Next, we will consider the subgroup of $GL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ (A) and $\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$ (B). However, we will find it expedient to generate elements not with these two matrices, but with the products:

$$ABA = \begin{pmatrix}2 & 0\\ 1 & 2\end{pmatrix} \text{ (C), and}$$
$$BAB = \begin{pmatrix}2 & 1\\ 0 & 2\end{pmatrix} \text{ (D).}$$

The reason that the matrices C and D are more helpful to work with is that they each have order 6, and so we can generate more elements by considering their powers than we do with the given matrices. In fact, we have $C^2 = B$ and $D^2 = A$, respectively.

Through exploration, we can rewrite the above table of the 24 matrices of $SL_2(\mathbb{F}_3)$ using only products of C and D:

C^2DC^2	$(C^5D)^5$	DC^2	D^2CD^2	DC^5	$(C^2D)^2$
$I = C^6D^6$	C^2	C^4	D^2	$(DC)^3$	$(DC^5)^5$
D^4	C^5D	CD			
C^3	C	C^5	D	$(CD)^3$	C^2D
D^5	$(DC^2)^2$	DC			

The process toward completing this table encompassed a rather brute force approach. We took arbitrary powers and products of C and D, which quickly yielded many new elements but soon tapered off and resulted in already existing elements. For the final matrix left outstanding, we determined computationally which entries would have been possible in a pair of matrices to be multiplied together to obtain it, and then found those in the table of existing elements (the matrix in question was $\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} = (C^2)(DC^2)$).

While this process is a bit unsatisfying methodologically and aesthetically, it does prove that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ generate the subgroup $SL_2(\mathbb{F}_3)$ of $GL_2(\mathbb{F}_3)$. □

10. (7/30/23)

Prove that the subgroup of $SL_2(\mathbb{F}_3)$ generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is isomorphic to the quaternion group of order 8.

Proof. In our notation, we will write the generating matrices as $\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$, and let A be the subgroup generated by them. Recall that Q_8 is generated by $\langle i, j \mid i^2 = j^2, i^4 = j^4 = 1, ji = i^{-1}j \rangle$.

Now let $\varphi : Q_8 \to A$ be defined by $\varphi(i) = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$ and $\varphi(j) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. For φ to be a homomorphism, the generators and relations of Q_8 must hold under φ in A.

We have

$$\varphi(i)^2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \text{ and } \varphi(j)^2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix},$$

so $\varphi(i)^2 = \varphi(j)^2$. And $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $\varphi(i)^4 = \varphi(j)^4 = I$.

Finally, note that $\varphi(i)^{-1} = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}$. It follows that

$$\varphi(i)^{-1}\varphi(j) = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} \text{ and}$$
$$\varphi(j)\varphi(i) = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

so all of the generators and relations of Q_8 hold under φ in A. Therefore φ is a homomorphism. Further, φ is surjective, since every element of A can be written as the image of some element of Q_8 under φ. Then $|A| \leq |Q_8| = 8$.

However, since we have shown that there exist at least 5 unique elements of A (the generating matrices, their product, the inverse of $\varphi(i)$, and the identity), by Lagrange's theorem A must contain 8 elements, and φ must then also be one-to-one, that is, an isomorphism. Thus A is isomorphic to Q_8. $\square$

11. (7/30/23)

Show that $SL_2(\mathbb{F}_3)$ and S_4 are two nonisomorphic groups of order 24.

Proof. From Exercise 9., $SL_2(\mathbb{F}_3)$ contains 24 elements, as does S_4. However, in $SL_2(\mathbb{F}_3)$, the element $\begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}$ has order 6, while no element in S_4 has order greater than 4. Therefore for any map $\varphi : SL_2(\mathbb{F}_3) \to S_4$, there is no element in S_4 such that $\varphi(\begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}^6) = \varphi(\begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix})^6$. Then no such φ is an isomorphism, and so the groups are not isomorphic to each other. $\square$

12. (8/3/23)

Prove that the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8.

Proof. Let A be the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ and let $\varphi : D_8 \to A$ be defined on generators by

$$\varphi(s) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } \varphi(r) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

We will show that φ is an isomorphism.

The orders of the generators in D_8 hold under φ in A:

$$\varphi(s)^2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$\varphi(r)^4 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^4 = \left(\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^2 \right)^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We also note that $\varphi^{-1}(r) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, and that

$$\varphi(s)\varphi(r) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \varphi^{-1}(r)\varphi(s).$$

Then φ is a surjective homomorphism. Since the order of A is 8 (the upper-middle, upper-right, and middle-right entries may each be 0 or 1, so there are $2^3 = 8$ possible upper triangular matrices), φ is also injective, and is thus an isomorphism. Thus the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to D_8. □

13. (8/3/23)

Prove that the multiplicative group of positive rational numbers is generated by the set $\{\frac{1}{p} \mid p \text{ is a prime}\}$.

Proof. Consider the subgroup $\langle\{\frac{1}{p} \mid p \text{ is a prime }\}\rangle$ of the positive rational numbers under multiplication. Since this generated group is closed under inverses, it contains every prime p. It is also closed under multiplication, and so contains 1, the identity, and every integer greater than 1, which can be expressed as a product of primes.

It follows that for any positive rational number $\frac{n}{m} = nm^{-1}$, but n and m are contained in the generated subgroup, and by the subgroup criterion, so is nm^{-1}. Therefore the group of positive rational numbers under multiplication is equal to $\langle\{\frac{1}{p} \mid p \text{ is a prime }\}\rangle$. □

14. (8/3/23)

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. Let A be a finite group. From Exercise 4., the finite subset $A - \{1\}$ generates A. □

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

Proof. From Chapter 1.2, Exercise 14., the subset $\langle 1, -1\rangle$ generates $\mathbb{Z}$ (in fact, $\langle 1\rangle$ is sufficient). □

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic.

Proof. Let $H = \langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, ..., \frac{a_n}{b_n} \rangle$. Let $k = b_1 \cdot b_2 \cdot ... \cdot b_n$ and consider the subgroup generated by $\frac{1}{k}$. Now b_1 divides k, so if $b_1 c = k$, then $\underbrace{\frac{1}{k} + ... + \frac{1}{k}}_{c \text{ times}} = \frac{1}{b_1}$. Further, $\underbrace{\frac{1}{b_1} + ... + \frac{1}{b_1}}_{a_1 \text{ times}} = \frac{a_1}{b_1}$, so the first generator of H is contained in $\langle \frac{1}{k} \rangle$. Similarly, every generator of H is contained in $\langle \frac{1}{k} \rangle$. Therefore every finitely generated group of $\mathbb{Q}$ is a cyclic group generated by the inverse of the product of the denominators of the generators. □

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

Proof. If $\mathbb{Q}$ were finitely generated, then we would have

$$\mathbb{Q} = \langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, ..., \frac{a_n}{b_n} \rangle = \langle \frac{1}{k} \mid k = b_1 \cdot b_2 \cdot ... \cdot b_n \rangle.$$

However, $\frac{1}{2k} \in \mathbb{Q}$ but $\frac{1}{2k} \notin \langle \frac{1}{k} \rangle$ (since we can only obtain multiples of $\frac{1}{k}$). Therefore $\mathbb{Q}$ is not finitely generated. □

15. (8/3/23)

Exhibit a proper subgroup of $\mathbb{Q}$ which is not cyclic.

Proof. Let A be the subgroup of $\mathbb{Q}$ generated by the set $\{\frac{1}{2^n} \mid n \in \mathbb{Z}^+\}$. If we assume that A is cyclic, then there exists a $k > 0$ such that $A = \langle \frac{1}{k} \rangle$. However, we can always choose an n such that $\frac{1}{2^n} < \frac{1}{k}$, and so A contains an element that is not generated by $\frac{1}{k}$, a contradiction. Therefore A is not cyclic.

To show that A is not equal to all of $\mathbb{Q}$, we note that only elements whose denominator is a power of 2 may be generated from $\{\frac{1}{2^n} \mid n \in \mathbb{Z}^+\}$. That is, A contains $\frac{5}{16} = \frac{1}{4} + \frac{1}{16}$ but not $\frac{5}{13}$. Thus A is a proper subgroup of $\mathbb{Q}$ which is not cyclic. □

16. (8/4/23)

A subgroup M of G is called a *maximal subgroup* if $M \neq G$ and the only subgroups of G which contain M are M and G.

(a) Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.

Proof. Let H be a proper subgroup of the finite group G. Suppose that there is no proper subgroup $M \leq G$ such that $H \leq M \leq G$. Then H itself is maximal, because the only subgroups of G which contain H are H and G. However, if there is an M with $H \leq M \leq G$, then we follow a similar proof that either M is maximal or is contained in another proper subgroup. Since G is finite, we can continue this process until we reach some K that is maximal. □

(b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.

Proof. Let $R = \{1, r, r^2, ..., r^{n-1}\} \in D_{2n}$. Clearly R is a proper subgroup because $s \notin R$. Any larger subgroup of D_{2n} must contain an element of the form sr^k. Then that subgroup also contains s, because $s = sr^k sr^{n-k}$ (the product of sr^k with an element in the subgroup of rotations), and so it contains every element of D_{2n} (generated by s and r). Therefore the only subgroups containing R are R and D_{2n}, and so R is a maximal subgroup. □

(c) Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only if $H = \langle x^p \rangle$ for some prime p dividing n.

Proof. Let $G = \langle x \rangle$, $|G| \geq 1$.

First, let H be a subgroup of G with $H = \langle x^p \rangle$, where p is a prime number dividing n (to show that H is a maximal subgroup). Suppose there exists some subgroup M such that $H \leq M \leq G$ and $H \neq M$. Then M contains some element x^k. Because H consists of powers of x whose exponents are multiples of p, p must not divide k. Since p is prime, it follows that p and k are relatively prime. By Bézout's identity, there exist $a, b \in \mathbb{Z}$ such that $ap + bk = 1$, which implies that $x = x^{ap+bk} = x^{ap}x^{bk}$. Now M contains H, so it contains x^{ap}, and since it contains x^k, it contains powers of x whose exponents are multiples of k, namely x^{bk}. It therefore contains their product, $x^{ap}x^{bk} = x$. However, since M contains x, it also contains every power of x, and is thus equal to G. Then the only subgroups of G containing H are H and G, and so H is maximal.

Next, let H be a maximal subgroup of G (to show that $H = \langle x^p \rangle$, with p a prime dividing n). Since H is cyclic, by the well-ordering theorem, choose the smallest $p \in \mathbb{Z}^+$ (not necessarily a prime) such that $x^p \in H$. Then $H = \langle x^p \rangle$. Suppose that p is composite, with $p = ab$ and $a, b > 1$. Now $H = \langle x^p \rangle = \{1, x^p, x^{2p}, ...\}$ but $\langle x^a \rangle = \{1, x^a, x^{2a}, ..., x^{ab} = x^p, ...\}$ is a proper subgroup of G containing H, which contradicts H being a maximal subgroup of G. Therefore p is a prime, and must divide n (if not, then because p is relatively prime to n, we have $H = G$, and so H is not a proper subgroup). □

17. (8/8/23)

Let G be a finitely generated group, say $G = \langle g_1, g_2, ..., g_n \rangle$, and let $\mathcal{S}$ be the set of all proper subgroups of G. Then $\mathcal{S}$ is partially ordered by inclusion. Let $\mathcal{C}$ be a chain in $\mathcal{S}$.

(a) Prove that the union, H, of all the subgroups of $\mathcal{C}$ is a subgroup of G.

Proof. First, let $x, y \in H = \bigcup \mathcal{C}$. Let H_1, H_2 be subgroups in the chain $\mathcal{C}$, and without loss of generality let $x \in H_1, y \in H_2$, and $H_1 \leq H_2$. Since $x \in H_1$ and $H_1 \leq H_2$, we also have $x \in H_2$. Also, H_2 is closed under inverses, so $y^{-1} \in H_2$. Then because H_2 is also closed under the binary operation on G, we have $xy^{-1} \in H_2$.

Then for any two elements in H, the union of $\mathcal{C}$, the product of one with the inverse of the other is in H, which fulfills the subgroup criterion. □

(b) Prove that H is a *proper* subgroup.

Proof. Toward contradiction, suppose that H is not a proper subgroup, that is, that $H = G$. Then for each of the generators g_i of G we have $g_i \in H$. Let $H_1 \leq H_2 \leq ... \leq H_n$ be subgroups in the chain $\mathcal{C}$. Without loss of generality, suppose $g_1 \in H_1, g_2 \in H_2$, and so on. We end at $g_n \in H_n$, and since the subgroups are ordered, we have all generators $g_i \in H_n$. However, since H_n is closed, this implies that all elements of G are contained in the proper subgroup H_n, a contradiction. Therefore H is a proper subgroup of G. □

(c) Use Zorn's Lemma to show that $\mathcal{S}$ has a maximal element (which is, by definition, a maximal subgroup).

Proof. Recall that Zorn's Lemma states that if A is a nonempty partially ordered set in which every chain has an upper bound then A has a maximal element.

Now from the two preceding proofs, we know that there exists an upper bound for any chain $\mathcal{C}$, namely the union of subgroups in the chain, H. We have $H \in \mathcal{S}$ (it is a proper subgroup) and $H_i \leq H$ for all H_i in the chain $\mathcal{C}$. Since $\mathcal{S}$ is a nonempty partially ordered set (G is finitely generated and is not the trivial group, so $\mathcal{S}$ at least contains the trivial subgroup), by Zorn's Lemma it contains a maximal element, which is by definition a maximal subgroup. □

18. (8/10/23)

Let p be a prime and let $Z = \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+\}$ (so Z is the multiplicative group of all p-power roots of unity in $\mathbb{C}$). For each $k \in \mathbb{Z}^+$ let $H_k = \{z \in Z \mid z^{p^k} = 1\}$ (the group of p^k-th roots of unity). Prove the following:

(a) $H_k \leq H_m$ if and only if $k \leq m$

Proof. First, let $k \leq m$ (to show that $H_k \leq H_m$). Let $h \in H_k$, so $h^{p^k} = 1$. Notice that $h^{p^m} = h^{p^k p^{m-k}} = (h^{p^k})^{p^{m-k}} = 1^{p^{m-k}} = 1$. This implies that $h \in H_m$, and so $H_k \leq H_m$.

Next, let $H_k \leq H_m$ (to show that $k \leq m$). Now if we choose $h = e^{\frac{2\pi i}{p^k}}$, then $h^{p^k} = (e^{\frac{2\pi i}{p^k}})^{p^k} = e^{2\pi i} = 1$. Also, p^k is the smallest positive integer for which $h^{p^k} = 1$. Now $h \in H_k$, and by inclusion we also have $h \in H_m$, which implies that $h^m = 1$. Therefore m must be no less than k, that is, $k \leq m$. □

(b) H_k is cyclic for all k (assume that for any $n \in \mathbb{Z}^+$, $\{e^{2\pi i/n} \mid t = 0, 1, ..., n-1\}$ is the set of all n-th roots of 1 in $\mathbb{C}$)

Proof. We will show that $H_k = \langle e^{\frac{2\pi i}{p^k}} \rangle$. It follows immediately that, for any element that is a p^k-th root of unity, it can be written in the form $e^{\frac{2\pi i t}{p^k}} = (e^{\frac{2\pi i}{p^k}})^t$, $t \in \{0, ..., n-1\}$. Thus all of H_k is generated by $e^{\frac{2\pi i}{p^k}}$. □

(c) every proper subgroup of Z equals H_k for some $k \in \mathbb{Z}^+$ (in particular, every subgroup of Z is finite and cyclic)

Proof. Suppose H is a subgroup of Z and let $g, h \in H$. For some $n_1, n_2 \in \mathbb{Z}^+$, we have $g^{p^{n_1}} = h^{p^{n_2}} = 1$ (suppose also that $n_2 \geq n_1$). Since $g^{p^{n_1}} = 1$ and $n_2 \geq n_1$, we also have $g^{p^{n_2}} = 1$. This implies that both g and h are in the subgroup H_{n_2}, and so $H \leq H_{n_2}$, which is a proper subgroup of Z, and from above, is cyclic. Every subgroup of a cyclic subgroup is also cyclic, and therefore every proper subgroup of Z is finite and cyclic. □

(d) Z is not finitely generated.

Proof. Suppose toward contradiction that Z is finitely generated by $\langle z_1, z_2, ..., z_m \rangle$ with $z_1^{p^{n_1}} = ... = z_m^{p^{n_m}} = 1$. Let $k = p^{n_1} p^{n_2} ... p^{n_m}$. Because Z is closed under multiplication, for any $z \in Z$, we must have $z^k = 1$. However, the element $e^{\frac{2\pi i}{2k}} \in Z$ cannot be generated by the given set of generators (which can only generate elements of the form $e^{\frac{2\pi i t}{k}}$). Thus Z is not finitely generated. □

19. (8/10/23)

A nontrivial abelian group A (written multiplicatively) is called *divisible* if for each element $a \in A$ and each nonzero integer k there is an element $x \in A$ such that $x^k = a$, i.e., each element has a k-th root in A (in additive notation, each element is the k-th multiple of some element of A).

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

Proof. Let $\frac{n}{m} \in \mathbb{Q}$ and let $k \neq 0$. Then $(\frac{n}{mk})k = \frac{n}{m}$, so $\frac{n}{m}$ is the k-th multiple of an element of $\mathbb{Q}$. Therefore $\mathbb{Q}$ is divisible. □

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

Proof. Let $|A| = n < \infty$. The order of every element of A divides n, so we have $a^n = 1$ for all $a \in A$. Thus there are no $a, b \in A$ such that $b^n = a$. Therefore A is not divisible. □

20. (8/10/23)

Prove that if A and B are both nontrivial abelian groups, then $A \times B$ is divisible if and only if both A and B are divisible groups.

Proof. First, let A and B both be divisible. For each $a \in A, b \in B, k \neq 0$, there exist $x \in A, y \in B$ such that $x^k = a$ and $y^k = b$. Then for the element $(a, b) \in A \times B$, we have $(a, b) = (x^k, y^k) = (x, y)^k$, so $A \times B$ is divisible.

Next, let $A \times B$ be divisible. For each $(a, b) \in A \times B, k \neq 0$, there exists $(x, y) \in A \times B$ such that $(x, y)^k = (a, b)$. This implies that $(x^k, y^k) = (a, b)$, and so $x^k = a, y^k = b$ (that is, x is the k-th root of a and y is the k-th root of b). Then A and B are both divisible.

Thus $A \times B$ is divisible if and only if A and B are both divisible groups. □