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

Scott Donaldson

Jul. 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:

$$\begin{array}{cccccc}
\begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix} & \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix} & & & \\
\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} & \begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix} & \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} & \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} & \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} & \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix} \\
\begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix} & \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix} & & &
\end{array}$$

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:

$$\begin{array}{cccccc}
C^2DC^2 & (C^5D)^5 & DC^2 & D^2CD^2 & DC^5 & (C^2D)^2 \\
I = C^6D^6 & C^2 & C^4 & D^2 & (DC)^3 & (DC^5)^5 \\
D^4 & C^5D & CD & & & \\
C^3 & C & C^5 & D & (CD)^3 & C^2D \\
D^5 & (DC^2)^2 & DC & & &
\end{array}$$

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

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

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. $\square$