

Dummit & Foote Ch. 2.1: Subgroups, Definition and Examples

Scott Donaldson

May 2023

Let G be a group.

1. (5/22/23)

In each of (a) - (e) prove that the specified subset H is a subgroup of the given group G :

- (a) H = the set of complex numbers of the form $a + bi$, $a \in \mathbb{R}$, $G = \mathbb{C}$ (under addition)

Proof. Let $a + bi, b + bi \in H$. $(b + bi) + (-b - bi) = 0$, so the inverse of $b + bi$ is $-b - bi$.

Then $a + bi - b + bi = (a - b) + (a - b)i \in H$. By the subgroup criterion, H is a subgroup of G . \square

- (b) H = the set of complex numbers of absolute value 1, i.e., the unit circle in the complex plane, $G = \mathbb{C}$ (under multiplication)

Proof. Let $a + bi, c + di \in H$. Since $|a + bi| = 1$, $\sqrt{a^2 + b^2} = 1$. The multiplicative inverse of a is $\frac{a-bi}{\sqrt{a^2+b^2}} = a - bi$. And the absolute value of $a - bi$ is $\sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2} = 1$. Thus H is closed under inverses.

Further, the product $(a + bi)(c + di) = ac - bd + (ad + bc)i$ has absolute value $\sqrt{(ac - bd)^2 + (ad + bc)^2}$. This simplifies to:

$$\begin{aligned}\sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2} &= \\ \sqrt{a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2} &= \sqrt{a^2(c^2 + d^2) + b^2(c^2 + d^2)} = \\ \sqrt{(a^2 + b^2)(c^2 + d^2)} &= \sqrt{a^2 + b^2} \sqrt{c^2 + d^2} = 1,\end{aligned}$$

and so H is closed under multiplication. Thus it is a subgroup of G . \square

- (c) $H =$ for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators divide n , $G = \mathbb{Q}$ (under addition)

Proof. Formally, $H = \{p/q \in \mathbb{Q} \mid q \text{ divides } n\}$. Let $p_1/q_1, p_2/q_2 \in H$. Since q_1, q_2 divide n , let $aq_1 = bq_2 = n$. Then $p_1/q_1 = ap_1/aq_1 = ap_1/n$ and $p_2/q_2 = bp_2/bq_2 = bp_2/n$. The additive inverse of $p_2/q_2 = bp_2/n$ is $-bp_2/n$. The sum $ap_1/n + (-bp_2/n) = (ap_1 - bp_2)/n$ has a denominator that divides n (or else simplifies to a denominator that divides n), and so it is an element of H . By the subgroup criterion, H is a subgroup of G . \square

- (d) $H =$ for fixed $n \in \mathbb{Z}^+$ the set of rational numbers whose denominators are relatively prime to n , $G = \mathbb{Q}$ (under addition)

Proof. As immediately above, let $p_1/q_1, p_2/q_2 \in H$. Let a be the greatest common divisor of q_1 and q_2 , and let $q_1 = ar_1, q_2 = ar_2$. Since q_1, q_2 are relatively prime to n , so too are the corresponding divisors a, r_1 , and r_2 . Now the sum of the first element with the inverse of the second element is:

$$p_1/q_1 - p_2/q_2 = p_1/ar_1 - p_2/ar_2 = \frac{p_1r_2 - p_2r_1}{ar_1r_2},$$

and since the factors in the divisor are all relatively prime to n , so is their product, and so the result is an element of H . Thus by the subgroup criterion, H is a subgroup of G . \square

- (e) $H =$ the set of nonzero real numbers whose square is a rational number, $G = \mathbb{R}$ (under multiplication)

Proof. Let $x_1, x_2 \in H$, with $x_1^2 = p_1/q_1 \in \mathbb{Q}, x_2^2 = p_2/q_2 \in \mathbb{Q}$.

The multiplicative inverse of x_2 is $1/x_2$. Consider x_1/x_2 . Now $(x_1/x_2)^2 = \frac{p_1/q_1}{p_2/q_2} = \frac{p_1}{q_1} \cdot \frac{q_2}{p_2} = \frac{p_1q_2}{p_2q_1} \in \mathbb{Q}$. Thus by the subgroup criterion, H is a subgroup of G . \square

2. (5/22/23)

In each of (a) - (e) prove that the specified subset H is *not* a subgroup of the given group G :

- (a) $H =$ the set of 2-cycles, $G = D_{2n}$ for $n \geq 3$

Proof. H is not closed. Let $\sigma_1 = (1, 2), \sigma_2 = (2, 3)$, then $\sigma_1\sigma_2 = (1, 3, 2)$, a 3-cycle and therefore not in H . \square

- (b) $H =$ the set of reflections, $G = D_{2n}$ for $n \geq 3$

Proof. Formally, $H = \{sr^k \in D_{2n} \mid 0 \leq k < n\}$. H is not closed. For example, $sr, sr^2 \in H$ but $sr^2sr = sr^2r^{-1}s = srs = ssr^{-1} = r^{-1} \notin H$. \square

- (c) $H = \{x \in G \mid |x| = n\} \cup \{1\}$, G a group containing an element of order n where n is a composite integer greater than 1

Proof. By counterexample, let $G = \mathbb{Z}/8\mathbb{Z}$ under modular addition. Let $n = 8$. The elements 1 and 3 have order 8, so both are in H . However, their sum, 4, has order 2, and so is not an element of H . \square

- (d) $H =$ the set of (positive and negative) odd integers together with 0, $G = \mathbb{Z}$

Proof. Let $k_1, k_2 \in H$. Since both are odd, there exist $n_1, n_2 \in \mathbb{Z}$ such that $k_1 = 2n_1 + 1$ and $k_2 = 2n_2 + 1$. Their sum, then, is $2n_1 + 1 + 2n_2 + 1 = 2n_1 + 2n_2 + 2 = 2(n_1 + n_2 + 1)$, which is an even integer, and so is not an element of H . \square

- (e) $H =$ the set of real numbers whose square is a rational number, $G = \mathbb{R}$ (under addition)

Proof. By counterexample, consider $\sqrt{2}, \sqrt{3} \in H$. Their sum, $\sqrt{2} + \sqrt{3}$, when squared, is equal to $(\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6} \notin \mathbb{Q}$. Therefore H is not closed, and is not a subset of G . \square

3. (5/22/23)

Show that the following subsets of the dihedral group D_8 are actually subgroups:

- (a) $\{1, r^2, s, sr^2\}$

Proof. For these 4 elements, we will exhaustively show that the subset fulfills the criteria for a subgroup of D_8 .

Each element is its own inverse in D_8 , so the set is closed under inverses.

It is also closed under the product of two elements. Considering only the non-trivial products, starting with r^2 : $r^2s = sr^{-2} = sr^2$ and $r^2sr^2 = sr^{-2}r^2 = s$. For s : $ssr^2 = r^2$. Finally for sr^2 : $sr^2r^2 = s$; $sr^2s = ssr^{-2} = r^2$. Since the subset is closed under inverses and the binary operation, it is a subgroup. \square

- (b) $\{1, r^2, sr, sr^3\}$

Proof. Similar to above, each element is its own inverse. To show it is closed, then, starting with r^2 : $r^2sr = sr^{-2}r = sr^{-1} = sr^3$; $r^2sr^3 = sr^{-2}r^3 = sr$. For sr : $sr r^2 = sr^3$; $sr sr^3 = ssr^{-1}r^3 = r^2$. Finally for sr^3 : $sr^3r^2 = sr^{-1}r^2 = sr$; $sr^3sr = ssr^{-3}r = r^{-2} = r^2$. Thus it is a subgroup of D_8 . \square

4. (5/22/23)

Give an explicit example of a group G and an infinite subset H of G that is closed under the group operation but is not a subgroup of G .

Proof. Let $G = \mathbb{Z}$, $H = \mathbb{Z}^+$. For any two $n, m \in H$, we have $n > 0$ and $m > 0$. Their sum, $n + m$, is also greater than zero, and so is an element of H . However, H does not contain the identity element 0 (as well as containing no additive inverses of any elements), and so is not a subgroup of G . \square

5. (5/22/23)

Prove that G cannot have a subgroup H with $|H| = n - 1$, where $n = |G| > 2$.

Proof. Let G be a finite group of order $n > 2$ and suppose (toward contradiction) that H is a subgroup of G with order $n - 1$. Since H is a subgroup, $1 \in H$. There is exactly one element of G that is not an element of H , and it is not the identity. Call that element g . Then g^{-1} must be an element of H . However, g^{-1} has no inverse in H , since by definition g is not in H . Therefore H cannot be a subgroup, contradicting the initial assumption that H is a subgroup of G with order $n - 1$. \square

6. (5/23/23)

Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G (called the *torsion subgroup* of G). Give an explicit example where this set is not a subgroup when G is non-abelian.

Proof. We will show that the given set is closed and closed under inverses, and is thus a subgroup of G .

First, let $g_1, g_2 \in G$ with $|g_1| = n$ and $|g_2| = m$. Let k be the least common multiple of n and m . Then $g_1^k = g_2^k = 1$. And, given that G is abelian, we have $g_1^k g_2^k = (g_1 g_2)^k = 1$. Thus the order of $g_1 g_2$ is finite, so the set is closed.

Next, it suffices to demonstrate that, for all $g \in G$ with $|g| = n$, we have $|g^{-1}| = n$, so the set is also closed under inverses and is thus a subgroup of G .

In the non-abelian group $G = GL_2(\mathbb{R})$, however, consider the two elements $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$. Each has order 2. However, their product is $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. Multiplied by itself, this results in $\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$, and in general, it can be proven through induction that $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$; that is, it has infinite order. Thus the set of elements with finite order is not closed in $GL_2(\mathbb{R})$ and so it is not a subgroup. \square

7. (5/23/23)

Fix some $n \in \mathbb{Z}$ with $n > 1$. Find the torsion subgroup of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. Show that the set of elements infinite order together with the identity is *not* a subgroup of this direct product.

Proof. The torsion subgroup of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ is $\{(k, m) \mid |(k, m)| < \infty, k \in \mathbb{Z}, 0 \leq m < n\}$. Considering $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ under addition, suppose that (k, m) has order p , so $p(k, m) = (0, 0)$. Then $pk = 0$ (in \mathbb{Z}) and $mk = 0$ (in $\mathbb{Z}/n\mathbb{Z}$). The only value of k that satisfies this is 0. Because $\mathbb{Z}/n\mathbb{Z}$ is finite, all values of m have finite order (that is, there exists a p for all $m \in \mathbb{Z}/n\mathbb{Z}$ such that $pm = 0$).

It follows that the torsion subgroup of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$ is $\{(0, m) \mid 0 \leq m < n\}$.

Now let A = the set of elements of infinite order together with identity, that is, $A = \{(k, m) \mid |(k, m)| = \infty\} \cup \{(0, 0)\}$. $(1, 1)$ and $(-1, 1)$ are both in A . However, their sum, $(0, 1)$, has finite order (it is in the torsion subgroup, above), and so A is not closed, and is therefore not a subgroup of $\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$. \square

8. (5/27/23)

Let H and K be subgroups of G . Prove that $H \cup K$ is a subgroup if and only if either $H \subseteq K$ or $K \subseteq H$.

Proof. First, to show that $H \cup K$ a subgroup implies that $H \subseteq K$, let $h \in H$ and $k \in K$. Because $H \cup K$ is a subgroup, it is closed, and since $h, k \in H \cup K$, it follows that $hk \in H \cup K$. Then either $hk \in H$ or $hk \in K$.

If $hk \in H$, then, since H is closed under inverses, $h^{-1} \in H$, we have $h^{-1}hk \in H \Rightarrow k \in H$. This implies that $K \subseteq H$. Or, if $hk \in K$, then similarly $hkk^{-1} = h \in K \Rightarrow H \subseteq K$.

Next, to show that one subgroup being contained in the other implies that their union is a subgroup, without loss of generality let $H \subseteq K$. In this case $H \subseteq K \Rightarrow H \cup K = K$, which by definition is a subgroup of G .

Thus $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$. \square

9. (5/27/23)

Let $G = GL_n(F)$, where F is any field. Define

$$SL_n(F) = \{A \in GL_n(F) \mid \det A = 1\}$$

(called the *special linear group*). Prove that $SL_n(F) \leq GL_n(F)$.

Proof. Clearly $SL_n(F)$ is a subset of $GL_n(F)$, since by definition $A \in SL_n(F)$ implies $A \in GL_n(F)$. It remains to be proven that $SL_n(F)$ is a subgroup, which we will show by the subgroup criterion.

Let $B \in SL_n(F)$. From elementary linear algebra, the determinant of the product of two matrices is equal to the product of the two determinants of each matrix. So $1 = \det I_n = \det B^{-1}B = \det B^{-1} \det B = \det B^{-1}$. Then the determinant of B 's inverse is also 1, so $SL_n(F)$ is closed under inverses.

Next, let $A \in SL_n(F)$ and consider the product AB^{-1} . From above, the determinant of this matrix is equal to $\det A \det B^{-1} = 1 \cdot 1 = 1$. Thus $SL_n(F)$ is also closed under matrix multiplication, and so is a subgroup of $GL_n(F)$. \square

10. (5/27/23)

- (a) Prove that if H and K are subgroups of G then so is their intersection $H \cap K$.

Proof. Let $g_1, g_2 \in H \cap K$. Then $g_1 \in H, g_2 \in H, g_1 \in K$, and $g_2 \in K$. It follows that the product g_1g_2 is an element of both H and K , since both subgroups are closed. Thus $g_1g_2 \in H \cap K$, and so $H \cap K$ is closed.

Similarly,

$$g \in H \cap K \Rightarrow g \in H, g \in K \Rightarrow g^{-1} \in H, g^{-1} \in K \Rightarrow g^{-1} \in H \cap K,$$

which shows that $H \cap K$ is also closed under inverses and is therefore a subgroup of G . \square

- (b) Prove that the intersection of an arbitrary nonempty collection of subgroups of G is again a subgroup of G (do not assume the collection is countable).

Proof. Let \mathcal{H} be a collection of nonempty subgroups of G . Consider $\bigcap_{H \in \mathcal{H}} H = \{h \in G \mid h \in H \text{ for all } H \in \mathcal{H}\}$. Let h_1, h_2 be in this subset. Then for all $H \in \mathcal{H}$, $h_1 \in H$ and $h_2 \in H$, so $h_1h_2 \in H$. So this intersection is closed under the binary operation of G . Similarly, for all $H \in \mathcal{H}$, $h \in H \Rightarrow h^{-1} \in H$, and so it is also closed under inverses.

Thus an arbitrary nonempty collection of subgroups is a subgroup. \square

11. (5/27/23)

Let A and B be groups. Prove that the following sets are subgroups of the direct product $A \times B$:

- (a) $\{(a, 1) \mid a \in A\}$

Proof. Let $(a_1, 1), (a_2, 1)$ in the set. Then $(a_1, 1)(a_2, 1) = (a_1a_2, 1)$. Now $a_1a_2 \in A$, so this is closed. Also, given $(a, 1)$, $a \in A \Rightarrow a^{-1} \in A$, so $(a, 1)^{-1} = (a^{-1}, 1)$ is in the set. Since it is closed and closed under inverses, it is a subgroup. \square

- (b) $\{(1, b) \mid b \in B\}$

Proof. The proof is identical to the one above but using $b_1, b_2 \in B$ in place of $a_1, a_2 \in A$. \square

- (c) $\{(a, a) \mid a \in A\}$, where here we assume $B = A$ (called the *diagonal subgroup*).

Proof. Let $(a_1, a_1), (a_2, a_2)$ in the set. Then $(a_1, a_1)(a_2, a_2) = (a_1a_2, a_1a_2)$. Since $a_1a_2 \in A$, it is closed. Also, $(a, a)^{-1} = (a^{-1}, a^{-1})$, so it is closed under inverses and is therefore a subgroup. \square

12. (5/27/23)

Let A be an abelian group and fix some $n \in \mathbb{Z}$. Prove that the following sets are subgroups of A :

- (a) $B = \{a^n \mid a \in A\}$

Proof. Let $a, b \in A$. Then $a^n, b^n \in B$. From Ch. 1, Ex. 24, since A is abelian, $a^n b^n = (ab)^n$. Thus the product ab is an element of B , so it is closed.

Also, the inverse of a^n is a^{-n} , which is equal to $(a^{-1})^n$, so B is closed under inverses and is thus a subgroup of A . \square

- (b) $B = \{a \in A \mid a^n = 1\}$.

Proof. Let $a, b \in B$. Then $a^n = b^n = 1$. Since A is abelian, we also have $1 = a^n b^n = (ab)^n$. Thus B is closed.

Also, $a^n = 1$ implies that its inverse, $a^{-n} = (a^{-1})^n = 1$, so B is closed under inverses and is a subgroup of A . \square

13. (5/27/23)

Let H be a subgroup of the additive group of rational numbers with the property that $1/x \in H$ for every nonzero element x of H . Prove that $H = \{0\}$ or \mathbb{Q} .

Proof. If $H = \{0\}$, then the definition trivially holds. Suppose that H contains at least one other element, $\frac{m}{n}$. Since H is closed under addition,

$m \in H$. Then, by definition of H , $\frac{1}{m} \in H$. It follows that $\underbrace{\frac{1}{m} + \dots + \frac{1}{m}}_{m \text{ times}} = 1 \in H$.

Now let $\frac{p}{q}$ be any rational number. We can show that it is contained in H by: $\underbrace{1 + \dots + 1}_{q \text{ times}} = q \Rightarrow \frac{1}{q} \in H$. Then $\underbrace{\frac{1}{q} + \dots + \frac{1}{q}}_{pq \text{ times}} = \frac{p}{q} \in H$. Thus, from its definition, if H contains any other rational number other than zero, it is itself the group of rational numbers under addition. \square