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 $a + ai, a \in \mathbb{R}$, $G = \mathbb{C}$ (under addition)

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

Then $a + ai - b + bi = (a - b) + (a - b)i \in H$. 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:

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

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. □

(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. □

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

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. □

(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 of 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: $srr^2 = sr^3$; $srsr^3 = ssr^{-1}r^3 = r^2$. 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 elememts), 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 $n - 1$. $\square$