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. □

(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. □

(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. □