

# Group Theory Homework 1

John Doe

January 03, 2025

## Problem 1

(Dummit and Foote, exercise 1.1.9)

Let  $G = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Q}\}$ .

- Prove that  $G$  is a group under addition.
- Prove that the nonzero elements of  $G$  are a group under multiplication. [Rationalize the denominators to find multiplicative inverses.]

## Solution

- a) We begin by showing closure under the operation. Take  $g_1, g_2 \in G$  so that  $\exists a, b, c, d \in \mathbb{Q}$  such that  $g_1 = a + b\sqrt{2}$ ,  $g_2 = c + d\sqrt{2}$ . Then  $g_1 + g_2 = a + b\sqrt{2} + c + d\sqrt{2} = (a + c) + (b + d)\sqrt{2} \in G$ , which follows from associativity, commutativity, and the distribution law on the field  $\mathbb{R}$ , and the fact that  $\mathbb{Q}$  is closed under addition. In fact, the associativity of addition on  $G$  trivially follows from the fact that  $G \subset \mathbb{R}$  and addition is associative in  $\mathbb{R}$ . Further,  $0 = 0 + 0\sqrt{2} \in G$  is an additive identity, which follows from the fact that 0 is the additive identity in  $\mathbb{R}$  already.

Now to show every element has an inverse, notice given  $g \in G$  with  $g = a + b\sqrt{2}$  and  $a, b \in \mathbb{Q}$ , let  $g' = (-a) + (-b)\sqrt{2} \in G$ , so that

$$\begin{aligned} g + g' &= a + b\sqrt{2} + (-a) + (-b)\sqrt{2} \\ &= a + (-a) + b\sqrt{2} + (-b)\sqrt{2} \\ &= (a + (-a)) + (b + (-b))\sqrt{2} \\ &= 0 \\ &= (-a) + (-b\sqrt{2}) + a + b\sqrt{2} \\ &= g' + g \end{aligned}$$

which follows from addition being commutative and associative in  $\mathbb{R}$ .

Thus  $G$  is a group under addition.

- b) Again we show closure under the operation. Take  $g_1, g_2 \in G$  so that  $\exists a, b, c, d \in \mathbb{Q}$  such that  $g_1 = a + b\sqrt{2}$ ,  $g_2 = c + d\sqrt{2}$ . Then  $g_1 g_2 = (a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2} \in G$  where our manipulations are valid since  $\mathbb{R}$  is a field, and  $ac + 2bd, ad + bc \in \mathbb{Q}$  follows from the closure of addition and multiplication on  $\mathbb{Q}$ . The associativity of multiplication follows from  $G \subset \mathbb{R}$ , and since  $1 = 1 + 0\sqrt{2} \in G$  is the multiplicative identity in  $\mathbb{R}$ , it is the multiplicative identity here too.

Now let  $g \in G$  with  $g = a + b\sqrt{2}$  and  $a, b \in \mathbb{Q}$ , and let  $g' = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}$ . Notice since  $\mathbb{Q}$  is closed under multiplication and division by nonzero elements, we need only check that  $a^2 - 2b^2 \neq 0$ . But this is equivalent to  $a = \pm b\sqrt{2}$ . We need only check nonzero elements of  $G$ , so we can throw out the case that

$a = b = 0$ . But then our condition is equivalent to  $\frac{a}{b} = \pm\sqrt{2}$ , an impossibility since  $\frac{a}{b} \in \mathbb{Q}$  and  $\sqrt{2} \notin \mathbb{Q}$ . Thus we indeed have  $g' \in G$ , and

$$\begin{aligned} gg' &= (a + b\sqrt{2}) \left( \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2} \right) \\ &= \left( \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2} \sqrt{2} \right) (a + b\sqrt{2}) \\ &= g'g \\ &= \frac{a^2}{a^2 - 2b^2} + \frac{ab\sqrt{2}}{a^2 - 2b^2} - \frac{ba\sqrt{2}}{a^2 - 2b^2} - \frac{2b^2}{a^2 - 2b^2} \\ &= \frac{a^2 - 2b^2}{a^2 - 2b^2} \\ &= 1. \end{aligned}$$

Thus  $G \setminus \{0\}$  is a group under multiplication.

## Problem 2

(Dummit and Foote, exercise 1.1.25)

Let  $G$  be a group. Prove that if  $x^2 = 1 \forall x \in G$ , then  $G$  is abelian.

## Solution

Let  $a, b \in G$ . Then observe

$$\begin{aligned} ab &= 1 \cdot ab \cdot 1 \\ &= b^2(ab)a^2 \\ &= b(ba)(ba)a \\ &= b(ba)^2a \\ &= b \cdot 1 \cdot a \\ &= ba \end{aligned}$$

so  $G$  is abelian.

## Problem 3

(Dummit and Foote, exercise 1.1.32) If  $x$  is an element of finite order  $n$  in a group  $G$ , prove that the elements  $1, x, x^2, \dots, x^{n-1}$  are all distinct. Deduce that  $|x| \leq |G|$ .

## Solution

Suppose by contradiction that  $x^a = x^b$  for some  $a, b \in \{0, 1, \dots, n-1\}$  with  $a \neq b$ . Without loss of generality, suppose  $a < b$ . Then  $x^{-a}x^a = 1 = x^{-a}x^b = x^{b-a}$ . But since  $b-a \leq (n-1) - 0 < n$ , we must have that  $x$  cannot be order  $n$ , a contradiction. Therefore  $1, x, \dots, x^{n-1}$  are all distinct. Further, each belongs to  $G$ , so  $G$  includes at least these elements, and thus  $n = |x| \leq |G|$ .

**Problem 4**

(Dummit and Foote, exercise 1.2.5)

If  $n$  is odd and  $n \geq 3$ , show that the identity is the only element of  $D_{2n}$  which commutes with all the elements of  $D_{2n}$ .

**Solution**

Recall that  $D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, sr = r^{-1}s \rangle$ . Suppose  $x \in D_{2n}$  commutes with all elements of  $D_{2n}$ .

Recall that  $r$  and  $s$  are generators of  $D_{2n}$ , and in particular  $D_{2n} = \{1, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}$

First, consider the case that  $x = r^k s$  for some  $k \in \{0, \dots, n-1\}$ . Then since  $x$  commutes universally,

$$\begin{aligned}
 rx &= xr \\
 \implies r(r^k s) &= (r^k s)r \\
 \implies r^{k+1}s &= r^k(r^{-1}s) \\
 &= r^{k-1}s \\
 \implies (r^{-k})r^{k+1} &= (r^{-k})r^{k-1} \\
 \implies r &= r^{-1} \\
 \implies r^2 &= 1
 \end{aligned}$$

but by definition,  $r$  has order  $n \geq 3$ , so this is a contradiction. Therefore, we must have  $x = r^k$  for  $k \in \{0, \dots, n-1\}$ :

$$\begin{aligned}
 xs &= sx \\
 \implies r^k s &= sr^k \\
 &= (sr)r^{k-1} \\
 &= r^{-1}(sr)r^{k-2} \\
 &\vdots \\
 &= r^{-k}s \\
 \implies r^k &= r^{-k} \\
 \implies r^{2k} &= 1
 \end{aligned}$$

Now since  $r$  has order  $n$ , we must have that  $n \mid 2k$ . But since  $k \leq n-1$ , we must have either  $n = 2k$  or  $k = 0$ . But the former situation is impossible since  $n$  is odd, so it must be true that  $k = 0$  and  $x = r^0 = 1$ . Thus any element in  $D_{2n}$  that commutes with every other element must be the identity.