Conjecture

Exercise 2.46

Proof. First, notice that associativity follows from the definition of multiplication for real numbers. Then we only need to verify (i) closure under the operation, (ii) existence of an identity element, (iii) and closure under inverses.

Let $G = \{3^m 6^n \mid m, n \in \mathbb{Z}\}$.

(i) Suppose we have two elements $3^m 6^n$ and $3^a 6^b$.

   Then $(3^m 6^n)(3^a 6^b) = (3^m 3^a)(6^n 6^b) = (3^{m+a})(6^{n+b})$.

   Thus G is closed under the operation.

(ii) Consider the element g such that $m = n = 0$.

   Then $g = 3^0 6^0 = 1$ and $ga = ag = a$ for all $a \in G$.

   Thus there exists an identity element in G, namely $e = 1$.

(iii) Consider the elements $g, h \in G$ such that $g = 3^m 6^n$ and $h = 3^{-m} 6^{-n}$.

   Notice that by commutativity of multiplication,

$$gh = 3^m 6^n 3^{-m} 6^{-n} = (3^m 3^{-m})(6^n 6^{-n}) = 3^0 6^0 = e \tag{1}$$

   and

$$hg = 3^{-m} 6^{-n} 3^m 6^n = (3^{-m} 3^m)(6^{-n} 6^n) = 3^0 6^0 = e. \tag{2}$$

   Thus $gh = hg = e$ and $h =^{-1} g$. Thus G is closed under inverses.

Therefore G is a group. $\qquad\square$

Exercise 2.48

Proof. Note that associativity and closure follow from the definition of multiplication. Thus we need only to verify (i) existence of an identity and (ii) closure under inverses.

Let $G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; a, b, c \in \mathbb{R} \right\}$.

(i) Consider the element g such that $a = b = c = 0$.

   Notice that $g = I_3$, the 3×3 identity matrix.

   Thus G has an identity element, namely $e = I_3$.

(ii) Consider the definition of multiplication:

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+a' & b'+ac'+b \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{bmatrix}$$

Notice that if we can find some values (in terms of a, b, and c) of a', b', c' that satisfy the system of equations

$$a + a' = 0, \tag{3}$$
$$b' + ac' + b = 0, \tag{4}$$
$$c + c' = 0, \tag{5}$$

the resulting matrix will be exactly I_3.

Trivially (??) and (??) tell us that $a' = -a$ and $c' = -c$.

Then, plugging these values into the second equation yields $b' - ac + b = 0 \implies b' = ac - b$.

Therefore given any element $g = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$, there exists an inverse $^{-1}g = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$.

Thus G is closed under inverses.

Thus G is a group. □

Exercise 2.52

Proof. Since associativity follows from matrix multiplication, we only need to verify (i) closure under the operation, (ii) existence of an identity, and (iii) closure under inverses.

Let $G = \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \,\middle|\, a \in \mathbb{R}, a \neq 0 \right\}$.

(i) Since $\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} b & b \\ b & b \end{bmatrix} = \begin{bmatrix} 2ab & 2ab \\ 2ab & 2ab \end{bmatrix}$ and $2ab \neq 0$, it follows that G is closed under the operation.

(ii) In the case above, notice that if we let $b = 0.5$, $\begin{bmatrix} a & a \\ a & a \end{bmatrix} \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix} = \begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix} \begin{bmatrix} a & a \\ a & a \end{bmatrix} = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$.

Thus the identity is $\begin{bmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{bmatrix}$.

(iii) Then, it follows that the inverse of $\begin{bmatrix} a & a \\ a & a \end{bmatrix}$ is $\begin{bmatrix} (4a)^{-1} & (4a)^{-1} \\ (4a)^{-1} & (4a)^{-1} \end{bmatrix}$.

Thus G is closed under inverses. The elements of G can have inverses without nonzero determinants because the identity of G is different than the identity of $GL(2, \mathbb{R})$, which is I_2.

Thus G is a group. □

Exercise 3.2

In $\mathbb{Q}$, $\langle \frac{1}{2} \rangle = \{ \frac{n}{2} \mid n \in \mathbb{Z} \} = \{\ldots, -\frac{5}{2}, -2, -\frac{3}{2}, -1, -\frac{1}{2}, 0, \frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, \ldots\}$.

In $\mathbb{Q}^*$, $\langle \frac{1}{2} \rangle = \{ \frac{1}{2^n} \mid n \in \mathbb{Z} \} = \{\ldots, \frac{1}{64}, \frac{1}{32}, \frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, 32, 64, \ldots\}$

Exercise 3.6

a) Let $a = 6$, $b = 2$. Then in $\mathbb{Z}_{12}$, $|a| = 2$, $|b| = 6$, and $|a + b| = 3$.

b) Let $a = 3$, $b = 8$. Then in $\mathbb{Z}_{12}$, $|a| = 4$, $|b| = 3$, and $|a + b| = 12$.

c) Let $a = 5$, $b = 4$. Then in $\mathbb{Z}_{12}$, $|a| = 12$, $|b| = 3$, and $|a + b| = 4$.

Exercise 3.8

Suppose $H \leq D_3$ such that $R_{4\pi/3}$, $F_\theta \in H$.

First, $R_0 \in H$ by definition of subgroup.

We know from lecture that $R_{4\pi/3} \circ R_{4\pi/3} = R_{2\pi/3}$, so $R_{2\pi/3} \in H$.

We also know from lecture that $R_{4\pi/3} \circ F_\theta = F_{4\pi/3+\theta/2}$, a reflection unique from F_θ.

Then $R_{2\pi/3} \circ F_\theta$ gives us a third unique reflection $F_{2\pi/3+\theta/2}$.

There are only 3 unique reflections in D_3, so H contains all reflections of D_3.

Thus $H = \{R_0, R_{2\pi/3}, R_{4\pi/3}, F_0, F_{2\pi/3}, F_{4\pi/3}\} = D_3$.

Now, suppose $K \leq D_3$ such that F_{θ_1}, $F_{\theta_2} \in K$.

First, $R_0 \in K$ by definition of subgroup.

From lecture, $F_{\theta_1} \circ F_{\theta_2} = R_{2\theta_1 - 2\theta_2} \neq R_0$.

Then from the first part of this problem, it follows that we can generate the rest of D_3 with these elements.

Thus $K = D_3$.

Exercise 3.20

Let G be a group. Suppose $x \in G$ such that $x^2 \neq e$ and $x^6 = e$.

We wish to show that $x^4 \neq e$ and $x^5 \neq e$.

Proof ($x^4 \neq e$). Suppose, for the sake of contradiction, that $x^4 = e$.

Then, $x^4 x^2 = x^6 = e$ and $x^4 x^2 = ex^2 = x^2 \neq e$.

This implies that $e \neq e$. Absurd.

Thus, our assumption that $x^4 = e$ must be incorrect.

Thus $x^4 \neq e$. □

Proof ($x^5 \neq e$). Suppose, for the sake of contradiction, that $x^5 = e$.

Then, $xx^5 = x^6 = e$ and $xx^5 = xe = x$.

So, $xx = x^2$ and $xx = ee = e$.

This implies that $x^2 = e$. Absurd.

Thus, our assumption that $x^5 = e$ must be incorrect.

Thus $x^5 \neq e$. □

Exercise 3.26

Proof. Let G be a group and let $a, b \in G$ such that $|a| = |b| = 2$ and $ab = ba$.

Then $|a| = 2 \implies a^2 = e \implies a =^{-1} a$ and similarly, $b =^{-1} b$.

Consider the subset $H = \{e,\ a,\ b,\ ab\}$.

Notice that $xy \in H$ for all $x, y \in H$. This is easy to see between e, a, and b.

For ab, notice that $a(ab) = a^2 b = b$ and $(ab)a = (ba)a = ba^2 = b$ and similarly, $b(ab) = (ab)b = a$. Also, notice that $(ab)(ab) = a(ba)b = a(ab)b = a^2 b^2 = ee = e$. The identity case is trivial.

Thus H is closed under the operation of G and is thus a subset of G by the finite subgroup test. $\qquad\square$

Exercise 3.27

In class, we showed that for every even integer n, $R_{180} = R^{n/2} \in D_n$.

From $R^{n/2} \circ R^{n/2} = R_0$, it follows that $\left|R^{n/2}\right| = 2$.

Recall the order of F is also 2 for any reflection $F \in D_n$.

We also showed in class that $R^{n/2} \in Z(D_n)$ for even n.

So, $R^{n/2}$ commutes with every element of D_n by definition of center.

Then D_n contains (at least) two elements of order two that commute.

Thus by exercise 3.26, D_n has a subgroup of order 4.

Exercise 3.32

By definition of subgroup, $e \in H$ and $e \in K$, so $H \cap K \neq \emptyset$.

Suppose we have $a, b \in H \cap K$.

Then, $a, b \in H$ and $a, b \in K$ by definition of intersection.

We know these are both subgroups, so $^{-1}b \in H$ and $^{-1}b \in K$ by closure under inverse.

By closure under operation, $a^{-1}b \in H$ and $a^{-1}b \in K$.

It follows that $a^{-1}b \in H \cap K$, so $H \cap K$ is a subgroup by the one step subgroup test.