2 Groups

2.2 Basic Properties and Order

Problem 2.38. *For each element g of the listed groups below, find the order of g, $|g|$.*

(a) $[3] \in (\mathbb{Z}_{15}, +)$.

(b) $[3] \in (U_{10}, \cdot)$.

(e) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} \in S_5$.

(f) $R_2 \in D_3$

(g) $\begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix} \in GL(2, \mathbb{Z}_2)$

For part (a), $|[3]| = 5$ as $3+3+3+3+3 \equiv 0 \pmod{15}$. For part (b), $|[3]| = 4$ as $3^4 = 81 \equiv 1 \pmod{10}$. For part (e), the order of the given $\sigma \in S_5$ is 2 as $\sigma^2 = e$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \text{[*]} = \text{Id}.$$

For part (f), $|R_2| = 3$ as a 240° rotation of a triangle must be repeated three times in order for the triangle to reach its original orientation, e. For part (g):

$$\begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix} \begin{pmatrix} [1] & [1] \\ [0] & [1] \end{pmatrix} = \begin{pmatrix} [1]+[0] & [1]+[1] \\ [0]+[0] & [0]+[1] \end{pmatrix} = \begin{pmatrix} [1] & [0] \\ [0] & [1] \end{pmatrix};$$

therefore the order of the matrix is 2.

Problem 2.39. *In each infinite group below, find all elements of finite order:*

(a) $(\mathbb{R}, +)$,

(b) $(\mathbb{R}^\times, \cdot)$,

(c) $(\mathbb{C}^\times, \cdot)$,

(d) $D(n, \mathbb{R}) = \{diag(c_1, \ldots, c_n) \,|\, c_i \in \mathbb{R}^\times, 1 \leq i \leq n\}$.

For part (a), the set of finite-order elements of $(\mathbb{R}, +)$ is $\{0\}$. For part (b), the set of finite-order elements of $(\mathbb{R}^\times, \cdot)$ is $\{1, -1\}$ as $(-1)^2 = 1$. For part (c), the set of finite-order elements contains all n-th roots of unity. For part (d), the set of finite-order elements of the group of diagonals composed of $\mathbb{R}$ is the trivial set composed of 1s along the diagonal of the $n \times n$ matrix.[†]

Problem 2.40. *Let G be a group and let $g \in G$.*

(a) *Show* $|g^{-1}| = |g|$.

[*] This may be incorrect notation but it gets the idea across.

[†] In research, I found that finite-order elements are called *torsion elements* and that groups can be classified as a *torsion group* if it only contains torsion elements. Reportedly this term comes from algebraic topology, but the connection is so complex that I can't understand how they're related—something about twisting a space?

(b) For $h \in G$, show $|hgh^{-1}| = |g|$.

(c) If $|g| < \infty$, show $g^{-1} = g^{|g|-1}$.

The following proofs will address each part respectively:

Proof. We know that by Theorem 2.11 part (2) that $g^{n_1} = g^{n_2}$ if and only if $n_1 \equiv n_2 \pmod{|g|}$. By the definition of an element's order, $g^n = e$ for some minimal positive exponent n. We can then say $g^n = e \Rightarrow (g^n)^{-1} = e^{-1} \Rightarrow g^{-n} = e$ which can only be true if n and $-n$ are equivalent $\pmod{n}$. Therefore, because $-n \equiv n \equiv 0 \pmod{n}$, $|g^{-1}| = |g|$. □

Proof. We can start by rewriting $|hgh^{-1}| = |g|$ as $(hgh^{-1})^n$ which can be simplified:

$$hg(h^{-1}h)g(h^{-1}h)gh^{-1} \cdots = hg^n h^{-1}.$$

We can also say that $hg^n h^{-1} = e$ is true only when $g^n = e$ as it allows

$$hg^n h^{-1} = heh^{-1} = hh^{-1} = e.$$

To demonstrate they are both the minimal exponent, consider $(hgh^{-1})^m = e$. We can simplify it to e as $h^{-1}(hgh^{-1})^m h = g^m = e$, thus $m = n$ and $|hgh^{-1}| = |g|$. □

Proof. By definition, $g^{|g|} = e$. Multiplying both sides by g^{-1}, we get $g^{|g|}g^{-1} = eg^{-1} \Rightarrow g^{|g|-1} = g^{-1}$ by Theorem 2.9 part (1). □

Problem 2.45 ($g^2 = e \implies$ Abelian)**.** *Suppose G is a group so that $g^2 = e$ for every $g \in G$. Show that G is abelian. Hint: Show $g \in G$ implies $g^{-1} = g$ and then apply this fact to the product of two elements.*

Proof. Suppose G is a group such that $g^2 = e$ $\forall g \in G$. Thus $g^2 g^{-1} = eg^{-1} \Rightarrow g = g^{-1}$ by Theorem 2.9 part (1). Next, using another element h and Theorem 2.9 part (2), we can say:

$$(gh)^{-1} = h^{-1}g^{-1} = hg \text{ and } (gh)^{-1} = (gh)$$

as every element is its own inverse in this given G. Therefore G must be abelian. □

2.3 Subgroups and Direct Products

2.3.1 Subgroups

Problem 2.53. *Show the following subsets are groups:*

(b) $\{5^a \mid a \in \mathbb{Q}\} \subseteq \mathbb{R}^\times$.

(c) $k\mathbb{Z}_n = \{k[m] \mid [m] \in \mathbb{Z}_n\} \subseteq \mathbb{Z}_n$ where $k \in \mathbb{Z}$ and $n \in \mathbb{N}$.

(g) $SL(n, \mathbb{R}) \subseteq GL(n, \mathbb{R})$.

(h) $\{T \in GL(n, \mathbb{R}) \mid Tv_0 = \lambda v_0, \lambda \in \mathbb{R}^+\} \subseteq GL(n, \mathbb{R})$ for some fixed $v_0 \in \mathbb{R}^n$.

In order to demonstrate the given subsets are groups, we need to show that their operation is closed, that all elements are associative, that there exists an identity, and that each element has an inverse.

(b) The subset from part (b) is a group as it:

- (i) is closed, as $(5^a) \cdot (5^n) = 5^{a+n}$, $a + n \in \mathbb{Q}\ \forall n \in \mathbb{Q}$;
- (ii) is associative, as $(5^a 5^b)5^c = 5^{a+b+c} = 5^a(5^b 5^c)\ \forall b, c \in \mathbb{Q}$;
- (iii) contains an identity, 5^0, as $5^a 5^0 = 5^{a+0} = 5^a$, and;
- (iv) has an inverse for every element, as $5^a 5^{-a} = 5^{a-a} = 5^0$.

(c) The subset from part (c) is a group as it:

- (i) is closed, as $k[i] + k[j] = k[i + j] \in k\mathbb{Z}_n$;
- (ii) is associative, as $k[i] + (k[j] + k[l]) = (k[i] + k[j]) + k[l] = k[i + j + l]$;
- (iii) contains an identity, as $k[0] \equiv 0 \pmod{n}$, and;
- (iv) has an inverse for every element, as $k[i] + k[-i] = k[0] \equiv 0 \pmod{n}$.

(g) The subset from part (g) is a group as it:

- (i) is closed, as two $n \times n$ invertible matrices with $\det = 1$ will produce an invertible matrix with $\det = 1$;
- (ii) is associative, as all matrices in the general linear group are associative;
- (iii) contains an identity, the identity matrix with $\det(I_n) = 1$, and;
- (iv) has an inverse for every element, as $\det(A) = 1 \Rightarrow \det(A^{-1}) = \frac{1}{\det(A)} = 1^{-1} = 1$.

(h) The subset from part (h) is a group as it:

- (i) is closed, as $(ST)v_0 = S(Tv_0) = S(\lambda v_0) = \lambda S v_0 = \lambda\mu v_0$;
- (ii) is associative, as all elements in the general linear group are associative;
- (iii) contains an identity, the identity matrix: $I_n v_0 = 1v_0$, and;
- (iv) has an inverse for every element, as $v_0 = T^{-1}Tv_0 = T^{-1}\lambda v_0 = \lambda T^{-1}v_0 \Rightarrow T^{-1}v_0 = \lambda^{-1}v_0$.

Problem 2.54. *Show the following are not subgroups:*

(a) $\{5^a \mid a \in \mathbb{Q}^+\} \subseteq \mathbb{R}^\times$.

(e) For $v_0 \in \mathbb{R}^n$, $\{T \in GL(n, \mathbb{R}) \mid Tv_0 = 2v_0\} \subseteq GL(n, \mathbb{R})$.

The subsets are not groups if they fail to uphold one of the four axioms discussed above. The subset from part (a) fails to be a group as the exclusion of $-a$ from Q^+ removes all possible non-trivial inverses from the set. The subset from part (e) fails to be a group as it excludes the identity matrix, which never maps to an eigenvalue of 2.

Problem 2.55. *Calculate the centralizers of the following subsets:*

(b) $\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\} \subseteq GL(2, \mathbb{R})$.

Let

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

We wish to compute the centralizer of A in $GL(2,\mathbb{R})$, namely

$$C_{GL(2,\mathbb{R})}(A) = \{X \in GL(2,\mathbb{R}) \mid XA = AX\}.$$

Take an arbitrary $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{R})$. Then

$$XA = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix},$$

and

$$AX = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}.$$

For $XA = AX$, we equate the corresponding entries:

(i) From the $(1,1)$-entry: $a = a + c$ implies $c = 0$.

(ii) From the $(1,2)$-entry: $a + b = b + d$ implies $a = d$.

(iii) The $(2,1)$-entry yields $c = c$, which is automatically satisfied.

(iv) The $(2,2)$-entry gives $c + d = d$; with $c = 0$ this holds automatically.

Thus, every matrix X commuting with A must be of the form

$$X = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix},$$

where $a \in$
$mathbbR^{\times}$ (to ensure that X is invertible) and $b \in \mathbb{R}$.

Hence, the centralizer of A in $GL(2,\mathbb{R})$ is

$$C_{GL(2,\mathbb{R})}(A) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \in \mathbb{R}^{\times},\ b \in \mathbb{R} \right\}.$$

Problem 2.56. *Show the following:*

(a) $\langle [2] \rangle = U_5$.

(b) $\langle 3, 11 \rangle = \mathbb{Z}$.

Answer here...

Problem 2.63 (Subgroups of $\mathbb{Z}$ and $\mathbb{Z}_n$)**.** *Complete the following:*

(a) If $H \neq \{0\}$ is a subgroup of $\mathbb{Z}$, let k be the minimal element of $\mathbb{N} \cap H$. Show k exists and that $H = \langle k \rangle$. Hint: If $m \in H$, use the ~~Euclidean~~ Division Algorithm to write $m = kq + r$ with $0 \leq r < k$ and show $kq \in H$ so that $r \in H$.

(b) *Conclude that the set of subgroups of* $\mathbb{Z}$ *is* $\{\langle k \rangle = k\mathbb{Z} \mid k \in \mathbb{Z}_{\geq 0}\}$.

(c) *For* $n \in \mathbb{N}$, *show that every* ~~*subset*~~ *subgroup of* $\mathbb{Z}_n$ *is of the form* $\langle k \rangle$ *for* $0 \leq k < n$.

(d) *Show* $\langle [k] \rangle = \langle [(k,n)] \rangle$. *Hint: For* $\subseteq$, *use* $(k,n) \,|\, k$. *For* $\supseteq$, *write* $(k,n) = kx + ny$.

(e) *Conclude that the set of subgroups of* $\mathbb{Z}_n$ *is* $\{\langle [k] \rangle \mid k \in \mathbb{N}$ *and* $k \mid n\}$.

(f) *Find all subgroups of* $\mathbb{Z}_{15}$.

Answer here..

2.3.2 Direct Products

Problem 2.57. *Evaluate the following:*

(a) $([3]_7, [5]_6) \cdot ([2]_7, [5]_6) \in U_7 \times U_6$.

(b) $([2]_4, [3]_5, [6]_7) + ([3]_4, [2]_5, [1]_7) \in \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$.

Answer here...