1. (DF2.2.4) For each of S_3, D_8, and Q_8, compute the centralizers of each element and find the center of each group. Does Lagrange's Theorem simplify your work?

   Recall that the centralizer of an element in a group G and the center of a group G are both subgroups of G. This means that by Lagrange's theorem, the order of these subgroups divides the order of the group.

   So because $|S_3| = 6 = 2 \cdot 3$, $|D_8| = 8 = 2^3$, and $Q_8 = 8 = 2^3$, our work is simplified because we only need to find subgroups whose order divides these orders (of course, a group may not have a subgroup whose order is a particular divisor of the group's order).

   Then for each group,

$$\begin{aligned} S_3 &= \{1, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\} \\ D_8 &= \left\{1, r, r^2, r^3, s, sr, sr^2, sr^3\right\} \\ Q_8 &= \{1, -1, i, -i, j, -j, k, -k\}, \end{aligned}$$

   we compute the centralizers of each element. So for every element $g \in G$, we compute $C_G(g)$ by inspection (trying out elements in the group which commute until we reach a suitable number of elements). In these groups,

$$\begin{aligned} C_{S_3}(1) &= S_3 \\ C_{S_3}((1\,2)) &= \{1, (1\,2)\} \\ C_{S_3}((1\,3)) &= \{1, (1\,3)\} \\ C_{S_3}((2\,3)) &= \{1, (2\,3)\} \\ C_{S_3}((1\,2\,3)) &= \{1, (1\,3\,2)\} \\ C_{S_3}((1\,3\,2)) &= \{1, (1\,2\,3)\} \end{aligned}
\qquad
\begin{aligned} C_{D_8}(1) &= D_8 \\ C_{D_8}(r) &= \left\{1, r, r^2, r^3\right\} \\ C_{D_8}(r^2) &= D_8 \\ C_{D_8}(r^3) &= \left\{1, r, r^2, r^3\right\} \\ C_{D_8}(s) &= \left\{1, r^2, s, sr^2\right\} \\ C_{D_8}(sr) &= \left\{1, r^2, sr, sr^3\right\} \\ C_{D_8}(sr^2) &= \left\{1, r^2, sr^2, s\right\} \\ C_{D_8}(sr^3) &= \left\{1, r^2, sr^3, sr\right\} \end{aligned}
\qquad
\begin{aligned} C_{Q_8}(1) &= Q_8 \\ C_{Q_8}(-1) &= Q_8 \\ C_{Q_8}(i) &= \{1, -1, i, -i\} \\ C_{Q_8}(-i) &= \{1, -1, i, -i\} \\ C_{Q_8}(j) &= \{1, -1, j, -j\} \\ C_{Q_8}(-j) &= \{1, -1, j, -j\} \\ C_{Q_8}(k) &= \{1, -1, k, -k\} \\ C_{Q_8}(-k) &= \{1, -1, k, -k\} \end{aligned}$$

   It is clear from enumerating all of these centralizers that $Z(S_3) = \{1\}$, $Z(D_8) = \left\{1, r^2\right\}$, and $Z(Q_8) = \{1, -1\}$.

2. (DF2.3.26) Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a \colon Z_n \to Z_n \quad \text{by} \quad \sigma_a(x) = x^a \text{ for all } x \in Z_n.$$

   (a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime.

   Proof. Let Z_n be a cyclic group of order n and $\sigma_a \colon Z_n \to Z_n$ be as given and suppose that a is coprime to n. Then there exist $s, t \in \mathbb{Z}$ such that $1 = as + nt$.
   We show σ_a is surjective. For any $y \in Z_n$, we have $y = y^1 = y^{as+nt} = (y^s)^a \cdot (y^n)^t = (y^s)^a \cdot 1^t = (y^s)^a$, where the fact that $|y| \mid n$ was used in the fourth equality. Then for any $y \in Z_n$, we have that $y^s \in Z_n$ and so $\sigma_a(y^s) = y$.

We show σ_a is injective by showing its kernel is the trivial subgroup of Z_n. Suppose there exists $x \in Z_n$ where $x \neq 1$, such that $\sigma_a(x) = x^a = 1$. Observe that because $\gcd(a, n) = 1$, there exist integers s, t such that $1 = as + nt$, so that $x = x^1 = x^{as+nt} = (x^a)^s = 1^s = 1$. But $x \neq 1$, which is a contradiction. Hence $\ker \sigma_a = \{1\}$, and σ_a is injective.

This map preserves the group operation as well. For $x, y \in Z_n$, because cyclic groups are abelian, $\sigma_a(xy) = (xy)^a = x^a y^a = \sigma_a(x)\sigma_a(y)$.

Conversely, suppose σ_a is an automorphism. When $n = 1$, the cyclic group $Z_n = \{1\}$, and so for every integer a, $\gcd(a, 1) = 1$. So without loss of generality, consider cyclic groups Z_n where $n > 1$. Then by contradiction, suppose that $\gcd(a, n) > 1$. Then the map σ_a cannot be injective as assumed, because $s = \frac{n}{\gcd(a,n)} \in \mathbb{Z}$ and $t = \frac{a}{\gcd(a,n)} \in \mathbb{Z}$. Since Z_n is a cyclic group, it is generated by some element $z \neq 1$ (since $n > 1$), so that $Z_n = \langle z \rangle$, and $|z| = n$. But $s < n$, since $\gcd(a, n) > 1$. Hence $z^s \neq 1$, and so

$$\sigma_a(z^s) = (z^s)^a = \left(z^{\frac{n}{\gcd a,n}}\right)^{t \cdot \gcd(a,n)} = z^{tn} = (z^n)^t = 1^t = 1.$$

So $\ker \sigma_a$ is not a trivial subgroup (contains a nontrivial element) of Z_n, and so σ_a cannot be injective, which is in contradiction with the assumption that σ_a is an automorphism. Hence $\gcd(a, n) = 1$.

Therefore σ_a is an automorphism of Z_n if and only if a and n are relatively prime. □

(b) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.

Proof. Let σ_a be as given. Suppose $a \equiv b \pmod{n}$, so that there exists $k \in \mathbb{Z}$ such that $b = a + kn$. Then for any element $x \in Z_n$, $\sigma_b(x) = x^b = x^{a+kn} = x^a(x^n)^k = x^a \cdot 1^k = x^a = \sigma_a(x)$. Since x was arbitrary, the action of σ_a and σ_b agree on Z_n and so the maps are equivalent as mappings from Z_n to Z_n.

Conversely, suppose $\sigma_a = \sigma_b$, so that for any $x \in Z_n$, $\sigma_a(x) = x^a = x^b = \sigma_b(x)$. Then $1 = x^b x^{-a} = x^{b-a}$, which implies that $n \mid b - a$, which by definition is equivalent to $b \equiv a \pmod{n}$, since there exists an integer k such that $b - a = nk \iff b = a + nk$. □

(c) Prove that *every* automorphism of Z_n is equal to σ_a for some integer a.

Proof. Let σ be an arbitrary automorphism of Z_n. Let $Z_n = \langle z \rangle$, so that $|z| = n$ and since z generates Z_n, we may write any element in Z_n as a power of z. Because σ is a bijection from Z_n to Z_n, there exists an $a \in \mathbb{Z}$ such that $\sigma(z) = z^a$. Then for any element $x \in Z_n$, there exists an integer k such that $x = z^k$. Then by properties of automorphisms,

$$\sigma(x) = \sigma(z^k) = (\sigma(z))^k = (z^a)^k = (z^k)^a = x^a.$$

Hence $\sigma = \sigma_a$, since x was any element in Z_n. Since σ was arbitrary, it follows that any automorphism of Z_n is equivalent to σ_a for some integer a. □

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\overline{a} \mapsto \sigma_a$ is an isomorphism of $(\mathbb{Z}/n\mathbb{Z})^\times$ onto the automorphism group of Z_n (so $\mathrm{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$).

Proof. Let σ_i be an automorphism of Z_n as given. Then for any element $x \in Z_n$,

$$(\sigma_a \circ \sigma_b)(x) = \sigma_a(\sigma(b)(x)) = \sigma_a(x^b) = (x^b)^a = x^{ab} = \sigma_{ab}(x).$$

Note that σ_{ab} is an automorphism if and only if ab is coprime to n, which can be guaranteed if both a and b were already coprime to n. When a and b are coprime to n, σ_a, σ_b, and σ_{ab} are automorphisms of Z_n. Hence $\sigma_a \circ \sigma_b = \sigma_{ab}$. This is enough to see that the map $\overline{a} \mapsto \sigma_a$ preserves the group operation; for $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\overline{a} \cdot \overline{b} = \overline{ab} \mapsto \sigma_{ab} = \sigma_a \circ \sigma_b.$$

Observe that the mapping is injective because in (b) we showed that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod n$, which by definition of $(\mathbb{Z}/n\mathbb{Z})^\times$ is also equivalent to $\overline{a} = \overline{b}$.

Furthermore, the mapping is surjective because every automorphism σ of Z_n is equal to σ_a for some integer a, so we can combine this with $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod n$, where b can be chosen to be the remainder of dividing a by n. Since $\overline{b}$ is a residue class of $(\mathbb{Z}/n\mathbb{Z})^\times$, we have that the preimage of σ under this mapping is $\overline{b}$, so all automorphisms of Z_n have a preimage in $(\mathbb{Z}/n\mathbb{Z})^\times$ under this mapping.

Hence the mapping $\overline{a} \mapsto \sigma_a$ is an isomorphism from $(\mathbb{Z}/n\mathbb{Z})^\times$ onto $\mathrm{Aut}(Z_n)$, so the order of these groups are equal ($|(\mathbb{Z}/n\mathbb{Z})^\times| = |\mathrm{Aut}(Z_n)| = \varphi(n)$), and both groups are cyclic. Hence $\mathrm{Aut}(Z_n)$ is an abelian group of order $\varphi(n)$. □

3. (DF2.4.14) A group H is called *finitely generated* if there is a finite set A such that $H = \langle A \rangle$.

(a) Prove that every finite group is finitely generated.

Proof. Suppose G is a group of finite order. Then it is clear that $G = \langle G \rangle$, since G has finitely many elements and any finite product of elements and their inverses in G is also in G, because G is a group ($\langle G \rangle \subseteq G$). Furthermore, every element of G can be seen as the product of one element, itself, of G ($G \subseteq \langle G \rangle$). Hence $G = \langle G \rangle$ is finitely generated. □

(b) Prove that $\mathbb{Z}$ is finitely generated.

Proof. Observe that the additive group $\mathbb{Z}$ is generated by $\langle 1 \rangle$ (or $\langle -1 \rangle$), since any integer multiple of 1 (or -1) is also an integer ($\langle \pm 1 \rangle \subseteq \mathbb{Z}$), and we may express every integer n as $n \cdot 1$ (or $(-n) \cdot (-1)$) ($\mathbb{Z} \subseteq \langle \pm 1 \rangle$). Hence $\mathbb{Z} = \langle \pm 1 \rangle$ is finitely generated. □

(c) Prove that every finitely generated subgroup of the additive group $\mathbb{Q}$ is cyclic. [If H is a finitely generated subgroup of $\mathbb{Q}$, show that $H \leq \langle 1/k \rangle$, where k is the product of all the denominators which appear in a set of generators for H.]

Proof. Let H be any finitely generated subgroup of the additive group $\mathbb{Q}$. Let H be generated by the set of rational numbers $\left\{\frac{a_1}{k_1}, \frac{a_2}{k_2}, \dots, \frac{a_n}{k_n}\right\}$, where n is some positive integer (H may be generated by the empty set, and in this case $H = \{1\}$ would already be cyclic).

Then let $k = \prod_{i=1}^{n} k_i$, so that we may consider the cyclic subgroup $\langle 1/k \rangle = \left\{ \dots, \frac{-2}{k}, \frac{-1}{k}, 1, \frac{1}{k}, \frac{2}{k}, \dots \right\}$ of $\mathbb{Q}$. We can show that $H \leq \langle 1/k \rangle$.

Clearly H contains the same identity as $\langle 1/k \rangle$ (by taking the empty product of the generators). Every element in H is of the form $\sum$ so H is a nonempty subset of $\langle 1/k \rangle$. Then because H is abelian (since addition commutes we can collect like terms), we may write every element in H as $\sum_{i=1}^{n} c_i \frac{a_i}{k_i}$, for some integers $c_i \in \mathbb{Z}$. Then rewrite the sum where all terms have a common denominator k, say the sum is written in the form $\frac{C}{k}$, where $C = \sum_{i=1}^{n} a_i c_i \left(\prod_{j \neq i} k_j \right)$. Since $C \in \mathbb{Z}$, any element in H is an element in $\langle 1/k \rangle$, so that H is a nonempty subset of $\langle 1/k \rangle$.

The group H is closed under addition and taking inverses (subtraction). For any two elements $x = \sum_{i=1}^{n} c_i \frac{a_i}{k_i}, y = \sum_{i=1}^{n} d_i \frac{a_i}{k_i}$ of H, where c_i, d_i are some integers, $x + y = \sum_{i=1}^{n} (c_i + d_i) \frac{a_i}{k_i}$ and $-x = \sum_{i=1}^{n} -c_i \frac{a_i}{k_i}$. Both are clearly elements of H.

Hence $H \leq \langle 1/k \rangle$, and we know that subgroups of cyclic groups are cyclic, so H is cyclic. Since H was any finitely generated subgroup of $\mathbb{Q}$, it follows that any finitely generated subgroup of $\mathbb{Q}$ is cyclic. □

(d) Prove that $\mathbb{Q}$ is not finitely generated.

Proof. Suppose via contradiction that $\mathbb{Q}$ is finitely generated, say by the set of rational numbers $\left\{ \frac{a_1}{k_1}, \frac{a_2}{k_2}, \dots, \frac{a_n}{k_n} \right\}$, where n is a positive integer (clearly n is not 0). Then let $k = \prod_{i=1}^{n} k_i$. Observe that there is no way to form with a finite sum of these rational numbers the rational number $\frac{C}{k+1}$, since $k_i \nmid k + 1$ (since $k \nmid k + 1$) for $1 \leq i \leq n$. This is in contradiction with the assumption that $\mathbb{Q}$ is finitely generated (we should be able to generate every rational number with a finite sum of rational numbers). Hence $\mathbb{Q}$ is not finitely generated. □

4. (DF2.4.16) A subgroup M of a group G is called a *maximal subgroup* if $M \neq G$ and the only subgroups of G which contain M are M and G.

(a) Prove that if H is a proper subgroup of the finite group G then there is a maximal subgroup of G containing H.

Proof. Let H be a proper subgroup of G as given. Then we may extend this subgroup into a larger subgroup of G by generating the subgroup $H_1 = \langle H, \{m\} \rangle$, for some $m \in G$ not in H. This new subgroup H_1 is either G itself or it is a subgroup of G containing H. If $H_1 = G$, then H is a maximal subgroup of G containing H. Otherwise, we will have to extend H_1 into a larger subgroup of G and see if this next subgroup is equal to G or not.

So we can form a recursive algorithm for generating even larger and larger subgroups of G which contain H. Let $H_{i+1} = \langle H_i, \{m_i\} \rangle$, for $0 \leq i$, where m_i is an element of G not in H_i. Let $H_0 = H$. This algorithm terminates at the j-th step when there are no more elements m_j not in H_j such that the next subgroup containing H, H_{j+1} is not equal to G; that is to say, if we extended H_j any more we would form G. It follows that H_j a maximal subgroup of G containing H.

This algorithm will terminate because G is finite; furthermore G is finitely generated. For instance, we could always take m_i from a finite set that generates G, and so this algorithm is guaranteed to end in a number of steps less than or equal to the cardinality of this set.

So in however many finite steps it takes to keep extending H into larger and larger subgroups of G (but not so large that the resulting subgroup is equal to G), we will reach a point where the resulting subgroup is indeed a maximal subgroup of G containing H. □

(b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.

Proof. The subgroup of all rotations in a dihedral group D_{2n} has order n. By Lagrange's theorem, the order of subgroups of D_{2n} must divide $2n$.

Observe that there are no factors of $2n$ strictly larger than n aside from $2n$. Furthermore, any other group of order n in D_{2n} distinct from the subgroup of all rotations will not contain all n rotations, so these other subgroups of order n will not contain the subgroup of all rotations.

Hence the subgroup of all rotations in a dihedral group is a maximal subgroup. □

(c) Show that if $G = \langle x \rangle$ is a cyclic group of order $n \geq 1$ then a subgroup H is maximal if and only if $H = \langle x^p \rangle$ for some prime p dividing n.

Proof. Let $G = \langle x \rangle$ be a cyclic group of order $n \geq 1$ as given. Then suppose that $H = \langle x^p \rangle$ for some prime p dividing n. Then suppose by way of contradiction that there is a proper subgroup H' of G containing H, so that H is a proper subgroup of H'. Then it follows that there is an element $y = x^m$ in H' *not* in H, where m is coprime to p. If m was not coprime to p, then it follows that m is a multiple of p and so this element would really an element of H.

Because m and p are coprime, there exist integers s, t such that $sm + pt = 1$. Since H' is a group (which contains $H = \langle x^p \rangle$), we may take the product $(x^m)^s(x^p)^t = x^{ms+pt} = x$. Then we may take any power of x and so it follows that $H' = G$, which is in contradiction to the assumption that H' was a proper subgroup of G.

Hence $H = \langle x^p \rangle$ is a maximal subgroup of G.

Conversely, suppose H is a maximal subgroup of G. Because all subgroups of cyclic groups are cyclic, $H = \langle x^m \rangle$ for some integer m. Without loss of generality, let m be a positive integer strictly greater than 1 (as $m = 1$ makes $H = G$). Then by way of contradiction, suppose m is composite, so that there exist integers a, b such that $m = ab$. Then it follows that $H = \langle x^m \rangle = \langle x^{ab} \rangle \leq \langle x^b \rangle$, since all elements of H are in the form $x^{nab} = (x^b)^{na}$, which are elements of $\langle x^b \rangle$. Hence H is not a maximal subgroup of G as assumed, so k is not composite as assumed.

Hence k is a prime number p. Furthermore, p divides n because otherwise $\gcd p, n = 1$ (this happens when primes are either larger than n or if p is not a divisor of n). If $\gcd(p, n) = 1$, then the order of $H = \langle x^p \rangle$ is $n/\gcd(p, n) = n/1 = n$, which makes $H = G$, but H is a maximal subgroup of G, so H cannot equal G.

Hence $H = \langle x^p \rangle$ for some prime p which divides n.

Therefore, H is a maximal subgroup of G if and only if $H = \langle x^p \rangle$ for some prime p dividing n. $\square$