Homework 3 Solutions

Based on the third edition of *Abstract Algebra* by Dummit and Foote.

2.2 Centralizers and Normalizers

Section 2.2, Exercise 2

Prove that $C_G(Z(G)) = G$ and deduce that $N_G(Z(G)) = G$.

Solution. Every $z \in Z(G)$ commutes with every $g \in G$. Thus every $g \in G$ centralizes every element of $Z(G)$, so $G \subseteq C_G(Z(G))$. The reverse inclusion is automatic, hence

$$C_G(Z(G)) = G.$$

For any subset $A \subseteq G$, one has $C_G(A) \leq N_G(A)$: if g commutes with every element of A, then $gAg^{-1} = A$. Therefore

$$G = C_G(Z(G)) \leq N_G(Z(G)) \leq G,$$

and consequently $N_G(Z(G)) = G$. □

Section 2.2, Exercise 3

Prove that if A and B are subsets of G with $A \subseteq B$ then $C_G(B)$ is a subgroup of $C_G(A)$.

Solution. Take $g \in C_G(B)$. By definition, $gb = bg$ for every $b \in B$. Since every $a \in A$ also lies in B, we have $ga = ag$ for every $a \in A$. Hence $g \in C_G(A)$, proving $C_G(B) \subseteq C_G(A)$. Both centralizers are subgroups of G, so this containment gives $C_G(B) \leq C_G(A)$. □

Section 2.2, Exercise 9

For any subgroup H of G and any nonempty subset A of G define $N_H(A)$ to be the set

$$\{h \in H \mid hAh^{-1} = A\}.$$

Show that $N_H(A) = N_G(A) \cap H$ and deduce that $N_H(A)$ is a subgroup of H (note that A need not be a subset of H).

Solution. By definition,

$$\begin{aligned} N_H(A) &= \{h \in H : hAh^{-1} = A\} \\ &= H \cap \{g \in G : gAg^{-1} = A\} = H \cap N_G(A). \end{aligned}$$

The normalizer $N_G(A)$ is a subgroup of G. The intersection of two subgroups of G is again a subgroup; therefore $N_H(A) = H \cap N_G(A) \leq H$. □

Section 2.2, Exercise 10

Let H be a subgroup of order 2 in G. Show that $N_G(H) = C_G(H)$. Deduce that if $N_G(H) = G$ then $H \leq Z(G)$.

Solution. Write $H = \{1, h\}$, where $h \neq 1$ and $h^2 = 1$. Certainly $C_G(H) \leq N_G(H)$. Conversely, if $g \in N_G(H)$, then $ghg^{-1} \in H$. Since $h \neq 1$, we have $ghg^{-1} = h$. Thus $gh = hg$, and g centralizes both elements of H. Hence $N_G(H) \leq C_G(H)$ and

$$N_G(H) = C_G(H).$$

If $N_G(H) = G$, then $C_G(H) = G$, so every element of G commutes with h. Thus $h \in Z(G)$, and of course $1 \in Z(G)$; hence $H \leq Z(G)$. □

2.3 Cyclic Groups and Cyclic Subgroups

Section 2.3, Exercise 16

Assume $|x| = n$ and $|y| = m$. Suppose that x and y commute: $xy = yx$. Prove that $|xy|$ divides the least common multiple of m and n. Need this be true if x and y do not commute? Give an example of commuting elements x, y such that the order of xy is not equal to the least common multiple of $|x|$ and $|y|$.

Solution. Let $L = \text{lcm}(m, n)$. Since x and y commute,

$$(xy)^L = x^L y^L = 1 \cdot 1 = 1.$$

The order of an element divides every positive exponent that gives the identity, so $|xy| \mid L$.

Commutativity is essential. In S_3, take $x = (12)$ and $y = (23)$. Both have order 2, whereas $xy = (123)$ has order 3; thus $|xy|$ does not divide $\text{lcm}(2, 2) = 2$.

Even when x and y commute, equality need not hold. If g generates a cyclic group of order $n \geq 2$, take $x = g$ and $y = g^{-1}$. Then $|x| = |y| = n$, but $xy = 1$, so

$$|xy| = 1 < n = \text{lcm}(|x|, |y|).$$

□

Section 2.3, Exercise 24

Let G be a finite group and let $x \in G$.

(a) Prove that if $g \in N_G(\langle x \rangle)$ then $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Prove conversely that if $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$ then $g \in N_G(\langle x \rangle)$. [Show first that $gx^k g^{-1} = (gxg^{-1})^k = x^{ak}$ for any integer k, so that $g\langle x \rangle g^{-1} \leq \langle x \rangle$. If x has order n, show the elements $gx^i g^{-1}$, $i = 0, 1, \ldots, n-1$ are distinct, so that $|g\langle x \rangle g^{-1}| = |\langle x \rangle| = n$ and conclude that $g\langle x \rangle g^{-1} = \langle x \rangle$.]

Note that this cuts down some of the work in computing normalizers of cyclic subgroups since one does not have to check $ghg^{-1} \in \langle x \rangle$ for every $h \in \langle x \rangle$.

Solution.

(a) If $g \in N_G(\langle x \rangle)$, then $g \langle x \rangle g^{-1} = \langle x \rangle$. In particular,

$$gxg^{-1} \in \langle x \rangle,$$

so $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(b) Conversely, suppose $gxg^{-1} = x^a$. For every $k \geq 1$, we have

$$gx^k g^{-1} = \underbrace{(gxg^{-1}) \cdot \cdots \cdot (gxg^{-1})}_{k \text{ terms}} = (gxg^{-1})^k = x^{ak} \in \langle x \rangle .$$

It follows that $g \langle x \rangle g^{-1} \subseteq \langle x \rangle$. Conjugation by g is a bijection, so the finite sets $g \langle x \rangle g^{-1}$ and $\langle x \rangle$ have the same cardinality. The displayed inclusion is therefore equality. Hence $g \in N_G(\langle x \rangle)$.

□

Section 2.3, Exercise 26

Let Z_n be a cyclic group of order n and for each integer a let

$$\sigma_a : Z_n \longrightarrow Z_n \qquad \text{by} \qquad \sigma_a(x) = x^a \quad \text{for all } x \in Z_n.$$

(a) Prove that σ_a is an automorphism of Z_n if and only if a and n are relatively prime (automorphisms were introduced in Exercise 20, Section 1.6).

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

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

(d) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$. Deduce that the map $\bar{a} \mapsto \sigma_a$ 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 $\varphi(n)$).

Solution. Fix a generator c of Z_n.

(a) For every integer a, the rule $\sigma_a(x) = x^a$ is a homomorphism because Z_n is abelian. Its image is $\langle c^a \rangle$. Now

$$|c^a| = \frac{n}{\gcd(a, n)},$$

so c^a generates Z_n exactly when $\gcd(a, n) = 1$. Since Z_n is finite, surjectivity is equivalent to bijectivity. Thus σ_a is an automorphism if and only if $\gcd(a, n) = 1$.

(b) Two homomorphisms out of a cyclic group are equal exactly when they agree on a generator. Hence

$$\sigma_a = \sigma_b \iff c^a = c^b \iff c^{a-b} = 1 \iff n \mid (a - b) \iff a \equiv b \pmod{n}.$$

(c) If $\alpha \in \mathrm{Aut}(Z_n)$, then $\alpha(c)$ is again a generator of Z_n. Thus $\alpha(c) = c^a$ for some a relatively prime to n. Since a homomorphism from a cyclic group is determined by the image of its generator, $\alpha = \sigma_a$.

(d) For every $x \in Z_n$,

$$(\sigma_a \circ \sigma_b)(x) = \sigma_a(x^b) = x^{ab},$$

so $\sigma_a \circ \sigma_b = \sigma_{ab}$. Consequently

$$\Psi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathrm{Aut}(Z_n), \qquad \overline{a} \longmapsto \sigma_a,$$

is well-defined by part (b), is a homomorphism by the composition formula, is injective by part (b), and is surjective by part (c). Therefore

$$\mathrm{Aut}(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

In particular, $\mathrm{Aut}(Z_n)$ is abelian and has order $\varphi(n)$.

□

2.4 Subgroups Generated by Subsets

Section 2.4, Exercise 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.

(b) Prove that $\mathbb{Z}$ 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.]

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

Solution.

(a) Every finite group G is generated by the finite set G itself (or by $G \setminus \{1\}$ when G is nontrivial). Hence every finite group is finitely generated.

(b) The additive group $\mathbb{Z}$ is generated by 1: every integer is an integral multiple of 1. Thus $\mathbb{Z} = \langle 1 \rangle$.

(c) Let $H \leq \mathbb{Q}$ be generated by

$$q_i = \frac{a_i}{b_i} \qquad (1 \leq i \leq r),$$

where $b_i > 0$. Put $D = b_1 b_2 \cdots b_r$. Each q_i lies in $\langle \frac{1}{D} \rangle$, so $H \leq \langle \frac{1}{D} \rangle$. Since subgroups of cyclic groups are cyclic, it follows that every finitely generated subgroup of $\mathbb{Q}$ is cyclic.

(d) If $\mathbb{Q}$ were finitely generated, part (c) would make it cyclic, say $\mathbb{Q} = \langle q \rangle$. If $q = 0$, this subgroup is trivial. If $q \neq 0$, then $q/2 \in \mathbb{Q}$ is not an integral multiple of q, so $q/2 \notin \langle q \rangle$, again a contradiction. Therefore $\mathbb{Q}$ is not finitely generated.

□

Section 2.4, Exercise 18

Let p be a prime and let $Z = \{z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \in \mathbb{Z}^+\}$ (so Z is the multiplicative group of all p-power roots of unity in $\mathbb{C}$). For each $k \in \mathbb{Z}^+$ let $H_k = \{z \in Z \mid z^{p^k} = 1\}$ (the group of p^kth roots of unity). Prove the following:

(a) $H_k \leq H_m$ if and only if $k \leq m$

(b) H_k is cyclic for all k (assume that for any $n \in \mathbb{Z}^+$, $\{e^{2\pi i t/n} \mid t = 0, 1, \ldots, n-1\}$ is the set of all nth roots of 1 in $\mathbb{C}$)

(c) every proper subgroup of Z equals H_k for some $k \in \mathbb{Z}^+$ (in particular, every proper subgroup of Z is finite and cyclic)

(d) Z is not finitely generated.

Solution. As printed, part (c) omits the trivial subgroup: if $\mathbb{Z}^+ = \{1, 2, \ldots\}$, then no listed H_k is trivial. To state the classification without an exception, set $H_0 = \{1\}$.

(a) If $k \leq m$ and $z \in H_k$, then

$$z^{p^m} = \left(z^{p^k}\right)^{p^{m-k}} = 1,$$

so $H_k \leq H_m$. Conversely, if $k > m$, the primitive p^kth root $\zeta_k = e^{2\pi i/p^k}$ lies in H_k but not in H_m. Therefore

$$H_k \leq H_m \quad \Longleftrightarrow \quad k \leq m.$$

(b) The p^kth roots of unity are exactly

$$1, \zeta_k, \zeta_k^2, \ldots, \zeta_k^{p^k-1}.$$

Hence $H_k = \langle \zeta_k \rangle$ is cyclic of order p^k.

(c) Let $K < Z$. We know K is nontrivial. If the orders of elements of K were unbounded, then for every r there would be $u \in K$ of order p^s with $s \geq r$. By part (b), such u generates H_s, so $H_r \leq H_s \leq K$. Since

$$Z = \bigcup_{r \geq 0} H_r,$$

this would give $K = Z$, contrary to properness. Thus the orders of elements of K are bounded. Choose the largest k for which K contains an element u of order p^k. Then $\langle u \rangle = H_k \leq K$. Every $v \in K$ has order at most p^k, hence belongs to H_k; therefore $K = H_k$.

Thus every nontrivial proper subgroup is H_k for a unique $k \geq 1$. In particular, every proper subgroup is finite cyclic.

(d) If Z were generated by finitely many elements $z_1, \ldots, z_r$, choose k_i with $z_i \in H_{k_i}$ and put $k = \max_i k_i$. Since H_k is a subgroup containing every generator,

$$\langle z_1, \ldots, z_r \rangle \leq H_k < Z,$$

a contradiction. Hence Z is not finitely generated.

□