6 Theory of Group Actions

11/14: You should think about and try to solve the starred questions, but several of them are quite messy and some are difficult, so only submit the ones without stars.

1. Exercises 4.1.7-4.1.8 of Dummit and Foote (2004).

7. Let G be a transitive permutation group on the finite set A. A **block** is a nonempty subset B of A such that for all $\sigma \in G$, either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$ (here $\sigma(B)$ is the set $\{\sigma(b) \mid b \in B\}$).

(a) Prove that if B is a block containing the element $a \in A$, then the set G_B defined by $G_B = \{\sigma \in G \mid \sigma(B) = B\}$ is a subgroup of G containing G_a.

Proof. To prove that G_B is a subgroup, it will suffice to show that G_B is nonempty, closed under multiplication, and closed under inverses. Since we naturally have $e(B) = B$, G_B is nonempty. Suppose $\sigma, \tau \in G_B$. Then $\sigma(B) = B$ and $\tau(B) = B$. It follows that $[\sigma \cdot \tau](B) = \sigma(\tau(B)) = \sigma(B) = B$, so $\sigma \cdot \tau \in G_B$ as well. Thus, G_B is closed under multiplication. Now suppose $\sigma \in G_B$. Then $\sigma(B) = B$. It follows since σ is bijective that $\sigma^{-1}(B) = B$ as well. Thus, $\sigma^{-1} \in G_B$, and hence G_B is closed under inverses.
We know that $G_a = \{\sigma \in G \mid \sigma(a) = a\}$. To prove that $G_a \subset G_B$, it will suffice to show that every $\sigma \in G_a$ is an element of G_B. Let $\sigma \in G_a$ be arbitrary. Since B is a block, either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$. Suppose for the sake of contradiction that $\sigma(B) \cap B = \emptyset$. Since $\sigma(a) = a$, we have that $\sigma(a) \in B$ and $\sigma(a) \in \sigma(B)$. Consequently, $\sigma(a) \in \sigma(B) \cap B$, a contradiction. Therefore, $\sigma(B) = B$, and $\sigma \in G_B$, as desired. □

(b) Show that if B is a block and $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ are all the distinct images of B under the elements of G, then these form a partition of A.

Proof. To prove that the $\sigma_i(B)$ form a partition of A, it will suffice to show that they are pairwise disjoint and that all $a \in A$ lie in some $\sigma_i(B)$.
Suppose for the sake of contradiction that there exist $1 \leq i \neq j \leq n$ such that $\sigma_i(B) \cap \sigma_j(B) \neq \emptyset$. Then there exists an $a \in A$ such that $a = \sigma_i b = \sigma_j b'$ for some $b, b' \in B$. Since $\sigma_i b = \sigma_j b'$, $b = \sigma_i^{-1}\sigma_j b'$. It follows that $b \in \sigma_i^{-1}\sigma_j(B)$ and $b \in B$, so $b \in \sigma_i^{-1}\sigma_j(B) \cap B$, a contradiction.
Let $a \in A$ be arbitrary, and pick some $b \in B$. Since the action is transitive, there exists $\sigma \in G$ such that $\sigma(b) = a$. Thus, $a \in \sigma(B)$. But since $\sigma_1(B), \sigma_2(B), \ldots, \sigma_n(B)$ encapsulates *all* distinct images of B under the elements of G, $\sigma(B) = \sigma_i(B)$ for some $1 \leq i \leq n$, as desired. □

(c) A (transitive) group G on a set A is said to be **primitive** if the only blocks in A are the trivial ones: The sets of size 1 and A itself. Show that S_4 is primitive on $A = \{1, 2, 3, 4\}$. Show that D_8 is not primitive as a permutation group on the four vertices of a square.

Proof. To prove that S_4 is primitive on A, it will suffice to show that if $B \subset A$ contains 2 or 3 elements, then there exists $\sigma \in S_4$ such that $\emptyset \neq \sigma(B) \cap B \neq B$. Let $B \subset A$ contain 2 or 3 elements. Pick $a \in A \setminus B$ and $b \in B$. Then $\sigma = (a, b) \in S_4$ guarantees that at least one element of B is left in $\sigma(B)$ and one element is taken out, meaning that $\emptyset \neq \sigma(B) \cap B \neq B$, as desired.
To prove that D_8 is not primitive on A (where $1, 2, 3, 4$ denote the four vertices of a square going clockwise), it will suffice to find a block $B \subset A$ with cardinality not equal to 1 or 4. Choose $B = \{1, 3\}$. Then if r is a clockwise rotation by $90°$ and s is a reflection along the diagonal from vertex 1 to 3, $e, r^2, s, sr^2 : B \mapsto B$ and $r, r^3, sr, sr^3 : B \mapsto A \setminus B$. □

(d) Prove that the transitive group G is primitive on A if and only if for each $a \in A$, the only subgroups of G containing G_a are G_a and G (i.e., G_a is a **maximal** subgroup of G). *Hint.* See Exercise 2.4.16. Use part (a).

Proof. Suppose first that G acts transitively and is primitive on A. Let $a \in A$ be arbitrary, and let $H \leq G$ contain G_a. Define $B = \{h(a) \mid h \in H\}$. We now seek to prove that B is a block.
To prove that B is a block, it will suffice to show that for all $\sigma \in G$, either $\sigma(B) = B$ or $\sigma(B) \cap B = \emptyset$. Let $\sigma \in G$ be arbitrary. We divide into two cases ($\sigma \in H$ and $\sigma \notin H$).

If $\sigma \in H$, then every $\sigma h(a) \in \sigma(B)$ is an element of B since $\sigma, h \in H$ implies $\sigma h \in H$ implies $\sigma h(a) \in B$. Thus, $\sigma(B) = B$ in this case. If $\sigma \notin H$, then suppose for the sake of contradiction that $\sigma(B) \cap B \neq \emptyset$. Let $b \in \sigma(B) \cap B$. Then $b = \sigma(h(a))$ for some $h(a) \in B$ and $b = h'(a)$ for some $h'(a) \in B$. It follows that $\sigma h(a) = h'(a)$. Consequently, ${h'}^{-1}\sigma h \cdot a = a$, so ${h'}^{-1}\sigma h \in G_a \subset H$. But if ${h'}^{-1}\sigma h \in H$, then $\sigma \in h'Hh^{-1} = H$, a contradiction. Therefore, B is a block.
Having proven that B is a block, we complete the proof in this direction. Since G is primitive, $B = G$ or $|B| = 1$. If $B = G$, then $H = G$. If $|B| = 1$, then since $e \in H$ implies $e(a) = a \in B$, the definition of B implies that every $h \in H$ makes $h(a) = a$. But this means that $H \leq G_a$; this combined with the hypothesis that $G_a \leq H$ means that $H = G_a$.

Now suppose that for each $a \in A$, the G_a is a maximal subgroup of G. To prove that (the transitive group) G is primitive on A, it will suffice to show that the only blocks in A are the trivial ones. Let B be an arbitrary block in A. Pick an $a \in B$. By part (a), $G_a \leq G_B \leq G$. It follows by the hypothesis that G_a is maximal that $G_B = G_a$ or $G_B = G$. We now divide into two cases. If $G_B = G_a$, suppose for the sake of contradiction that there exists $b \neq a$ in B. Since $G \curvearrowright A$ is transitive, there exists $\sigma \in G$ such that $\sigma(a) = b$. It follows since B is a block that $\sigma(B) = B$, hence $\sigma \in G_B = G_a$. But this implies that $\sigma(a) = a$, a contradiction. Therefore, $B = \{a\}$. On the other hand, if $G_B = G$, then let $a \in A$ be arbitrary. By transitivity, there once again exists $\sigma \in G$ such that $\sigma \cdot b = a$ for some $b \in B$. But since $G = G_B$, $\sigma(B) = B$, so $a \in B$. Therefore, $A \subset B$, so $B = A$, as desired. □

8. A transitive permutation group G on a set A is called **doubly transitive** if for any (hence all) $a \in A$, the subgroup G_a is transitive on the set $A \setminus \{a\}$.

(a) Prove that S_n is doubly transitive on $\{1, 2, \ldots, n\}$ for all $n \geq 2$.

Proof. Let $\Sigma = \{1, 2, \ldots, n\}$. It follows from the definition of S_n that $S_n \curvearrowright \Sigma$ is transitive. Now let $k \in \Sigma$ be arbitrary, and let $G = S_n$ (for ease of writing G_a instead of S_{n_a} or something). Then G_a is the set of all permutations of Σ that fix k, which is naturally transitive on $\Sigma \setminus \{a\}$ for $n \geq 2$. (The $n \geq 2$ condition helps us avoid the case where $\Sigma = \emptyset$.) Therefore, S_n is doubly transitive on Σ, as desired. □

(b) Prove that a doubly transitive group is primitive. Deduce that D_8 is not doubly transitive in its action on the four vertices of a square.

Proof. Let G a transitive permutation group on A be doubly transitive. To prove that G is primitive, it will suffice to show that the only blocks in A are the trivial ones. Let $B \subset A$ be an arbitrary block. We divide into two cases ($B = A$ and $B \neq A$). If $B = A$, then we are done. If $B \neq A$, then we can pick $c \in A \setminus B$. Additionally, since B (as a block) is nonempty, we may pick an $a \in B$. Now suppose for the sake of contradiction that there exists $b \in B$ such that $b \neq a$. Then since G_a is transitive on $A \setminus \{a\}$, there exists $\sigma \in G_a$ such that $\sigma(b) = c$. This implies that $\sigma(B) \supsetneq B$. However, since $G_a \leq G_B$ by Exercise 7a, $\sigma(B) = B$, a contradiction. Therefore, $B = \{a\}$, as desired.
Since D_8 acting on the four vertices of a square is not primitive by Exercise 7c, we have by the above argument that it cannot be doubly transitive in action on this set either, as desired. □

2. Exercise 4.2.9 of Dummit and Foote (2004).

9. Prove that if p is a prime and G is a group of order p^α for some $\alpha \in \mathbb{Z}^+$, then every subgroup of index p is normal in G. Deduce that every group of order p^2 has a normal subgroup of order p.

3. Suppose that G acts transitively and faithfully on a finite set X, and that G is abelian. Prove that $|G| = |X|$. Show that the equality need not hold if G is not abelian.

Proof. We approach this proof from the perspective of the Orbit-Stabilizer Theorem. According to it,

$$|G| = |\operatorname{Orb}(x)| \cdot |\operatorname{Stab}(x)|$$

for all $x \in X$. Since $G \curvearrowright X$ is transitive, $\mathrm{Orb}(x) = X$, and we can further refine the above to

$$|G| = |X| \cdot |\operatorname{Stab}(x)|$$

Thus, to prove that $|G| = |X|$, it will suffice to show that $|\operatorname{Stab}(x)| = 1$ for all $x \in X$. To do so, we will show that $\operatorname{Stab}(x) = \operatorname{Stab}(y)$ for all $x, y \in X$, from which it will follow that $\operatorname{Stab}(x) = \bigcap_{y \in X} \operatorname{Stab}(y) = \{e\}$ for all $x \in X$, as desired. Let $x, y \in X$ be arbitrary. Since G is transitive, there exists $g \in G$ such that $g \cdot x = y$. Now suppose $h \in \operatorname{Stab}(y)$. Then since G is abelian,

$$\begin{aligned} g \cdot x &= y \\ &= h \cdot y \\ &= h \cdot (g \cdot x) \\ &= hg \cdot x \\ &= gh \cdot x \\ &= g \cdot (h \cdot x) \end{aligned}$$

It follows by the cancellation lemma that $h \cdot x = x$, i.e., $h \in \operatorname{Stab}(x)$. Having shown that an arbitrary element of one stabilizer is necessarily in another, we know that all stabilizers are equal, and thus have the desired result.

Let $G = D_6$ and X be the a set of three points in the plane that D_6 can shuffle around. There are elements of D_6 that move every point to every other point, so the action is transitive, and the only element that fixes every point is the identity, so the action is faithful. Additionally, D_6 is not abelian: recall our special rule for commuting in D_6 as $rs = sr^{-1}$. And lastly, note that $|G| = 6 \neq 3 = |X|$, as desired. □

4. Let G be a finite group and let H be any subgroup.

   (a) Prove that the left action of G on the coset space G/H has kernel $N = \bigcap_{g \in G} gHg^{-1}$.

   Proof. Let $gH \in G/H$ be arbitrary. We seek to show that $\operatorname{Stab}(gH) = gHg^{-1}$. Suppose $\sigma \in \operatorname{Stab}(gH)$ is such that $\sigma \cdot gH = gH$. Then $\sigma gH = gH$, i.e., for every $h \in H$, there exists $h' \in H$ such that $\sigma gh = gh'$. It follows that $\sigma = gh'h^{-1}g^{-1} \in gHg^{-1}$.
   Therefore, we have that

   $$\ker = \bigcap_{gH \in G/H} \operatorname{Stab}(gH) = \bigcap_{g \in G} \operatorname{Stab}(gH) = \bigcap_{g \in G} gHg^{-1}$$

   as desired. □

   (b) Prove that $N = \bigcap_{g \in G} gHg^{-1}$ is the largest normal subgroup of G contained in H.

   Proof. Suppose for the sake of contradiction that there exists $M \triangleleft G$ such that $M \subset H$ and $M \supsetneq N$. □

5. **The Quaternions.** Let $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ be a 4-dimensional vector space over $\mathbb{R}$. Define a non-commutative associative multiplication structure on $\mathbb{H}$ by the formulae

   $$ij = -ji = k \qquad jk = -kj = i \qquad ki = -ik = j \qquad i^2 = j^2 = k^2 = -1$$

   (a) ($\star$) Show that there is a map $\phi : \mathbb{H} \to M_2(\mathbb{C})$, where $M_2(\mathbb{C})$ is the vector space of 2×2 matrices over $\mathbb{C}$, defined by sending

   $$i \mapsto \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \qquad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad k \mapsto \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

   for which

i. ϕ is injective as a map of vector spaces over $\mathbb{R}$.

ii. ϕ respects multiplication; if q_1, q_2 are two quaternions, then $\phi(q_1 q_2) = \phi(q_1)\phi(q_2)$. This should reduce easily enough to the case where q_i, q_j are elements of the set $\phi(1), \phi(i), \phi(j), \phi(k)$. The map ϕ is not a group homomorphism since 0 is not an invertible quaternion, but we shall see below in part (c) that non-zero quaternions form a group, so ϕ restricted to $\mathbb{H}^\times$ is actually a homomorphism from $\mathbb{H}^\times$ to $\mathrm{GL}_2(\mathbb{C})$.

(b) Define the conjugate of a quaternion $q = a + bi + cj + dk$ by $\bar{q} := a - bi - cj - dk$. Prove that $N(q) := q\bar{q} = a^2 + b^2 + c^2 + d^2$.

Proof. We have that

$$\begin{aligned} N(q) &= q\bar{q} \\ &= (a + bi + cj + dk)(a - bi - cj - dk) \\ &= a^2 - abi - acj - adk + abi - b^2i^2 - bcij - bdik + acj - bcji - c^2j^2 - cdjk + adk - bdki - cdkj - d^2k^2 \\ &= a^2 - b^2i^2 - bcij - bdik - bcji - c^2j^2 - cdjk - bdki - cdkj - d^2k^2 \\ &= a^2 - b^2i^2 - bcij - bdik + bcij - c^2j^2 - cdjk + bdik + cdjk - d^2k^2 \\ &= a^2 - b^2i^2 - c^2j^2 - d^2k^2 \\ &= a^2 + b^2 + c^2 + d^2 \end{aligned}$$

as desired. □

(c) Prove that non-zero quaternions $\mathbb{H}^\times$ form a group under multiplication.

Proof. To prove that $(\mathbb{H}^\times, \cdot)$ is a group, it will suffice to show that there exists an identity element e, there exist inverses for every element, and associativity holds. Pick 1 to be the identity element; we clearly have that

$$1 \cdot (a + bi + cj + dk) = (a + bi + cj + dk) \cdot 1 = a + bi + cj + dk$$

where $a + bi + cj + dk \in \mathbb{H}^\times$ is arbitrary. For every $q \in \mathbb{H}^\times$, pick $\bar{q}/N(q)$ to be its inverse; by part (a), we have that

$$q \cdot \frac{\bar{q}}{N(q)} = \frac{N(q)}{N(q)} = 1 = \frac{N(q)}{N(q)} = \frac{\bar{q}}{N(q)} \cdot q$$

Associativity holds by hypothesis. Therefore, $\mathbb{H}^\times$ is a group, as desired. □

(d) Let $Q = \langle i, j \rangle$ be the subgroup of $\mathbb{H}^\times$ generated by i, j. Prove that Q is a group of order 8. (Q is known as the "quaternion group.")

Proof. The elements of Q are

$$Q = \{1 = i^4, -1 = i^2, i, j, -i = i^3, -j = j^3, k = ij, -k = ji\}$$

We can confirm by manual computation that the product of any two of these elements is in Q. The rest of the group axioms are satisfied since any set defined in terms of group generators is a group. □

(e) Prove that every subgroup of Q is normal.

Proof. Let $H \leq Q$, and let $h \in H$. We want to show that $qhq^{-1} \in H$ for all $q \in Q$. We divide into two cases ($q = 1, -1$, and $q \neq 1, -1$). If $q = 1, -1$, then both q, q^{-1} commute with h, so $qhq^{-1} = qq^{-1}h = h \in H$. If $q \neq 1, -1$, then □

(f) Let $N = \pm 1 \subset Q$. Prove that $Q/N \cong (\mathbb{Z}/2\mathbb{Z})^2$ and that Q/N is not isomorphic to a subgroup of Q.

(g) ($\star$) Let Γ be the subgroup of $\mathbb{H}^\times$ generated by the elements of Q together with $\frac{1}{2}(1+i+j+k)$. Prove that Γ is a group of order 24.

(h) Prove that Γ is *not* isomorphic to S_4, and Q is *not* isomorphic to D_8. In fact, $\Gamma = \mathrm{SL}_2(\mathbb{F}_3)$.

(i) ($\star$) Construct a surjective homomorphism from Γ to A_4.

(j) Prove that the subgroup $\mathbb{H}^1$ of quaternions q with $N(q) = 1$ is a subgroup of $\mathbb{H}^\times$. Deduce that the 3-sphere $S^3 \subset \mathbb{R}^4$ defined by $a^2 + b^2 + c^2 + d^2 = 1$ has a natural structure of a group. Note that S^1 also has a natural group structure given by rotations in $\mathrm{SO}(2)$. It turns out that S^n has a natural (i.e., continuous) group structure only for $n = 1$ and $n = 3$.

(k) ($\star$) Say that a quaternion is **pure** if it is of the form $bi+cj+dk$, i.e., $a = 0$. We may identify pure quaternions with $\mathbb{R}^3$. Show that if u is a pure quaternion, then quq^{-1} is still a pure quaternion for any $q \in \mathbb{H}^\times$.

(l) ($\star$) Prove that the action of q on $\mathbb{R}^3$ by $q \cdot u = quq^{-1}$ is via elements of $\mathrm{SO}(3)$, and deduce that there is a homomorphism $\mathbb{H}^\times \to \mathrm{SO}(3)$.

(m) ($\star$) Prove that the restriction of this homomorphism to $\mathbb{H}^1 \to \mathrm{SO}(3)$ is surjective and has kernel of order 2.