Math 561/661 **Fall 2023**
Homework 5 **Drew Armstrong**

---

1. First Isomorphism Theorem. Let $\varphi : (G, *, \varepsilon_G) \to (H, \bullet, \varepsilon_H)$ be a group homomorphism. Consider the kernel and image:

$$\ker\varphi = \{a \in G : \varphi(a) = \varepsilon_H\},$$
$$\operatorname{im}\varphi = \{\varphi(a) : a \in G\}.$$

(a) Prove that φ is injective if and only if $\ker\varphi = \{\varepsilon_G\}$. In this case, prove that $G \cong \operatorname{im}\varphi$.
(b) Prove that $\ker\varphi$ is a normal subgroup of G, so the set of cosets $G/\ker\varphi$ is a group. Prove that the function $\Phi : G/\ker\varphi \to \operatorname{im}\varphi$ defined by $\Phi([a]) := \varphi(a)$ is a well-defined group isomorphism.

2. Orbit-Stabilizer Theorem. Let $(G, *, \varepsilon)$ be a group and let X be a set. An *action of G on X* is a function $G \times X \to X$, which we can denote by $(g, x) \mapsto g(x)$, satisfying two rules:

- For all $x \in X$ we have $\varepsilon(x) = x$.
- For all $a, b \in G$ and $x \in X$ we have $(a * b)(x) = a(b(x))$.

(a) Consider the relation $\sim$ on X defined by

$$x \sim y \iff \exists g \in G, y = g(x).$$

Prove that this is an equivalence relation. The equivalence classes are called *orbits*:

$$\operatorname{Orb}(x) := \{y \in X : x \sim y\} \subseteq X.$$

(b) For any $x \in X$ we define the *stabilizer subgroup*:

$$\operatorname{Stab}(x) := \{g \in G : g(x) = x\} \subseteq G.$$

Prove that $\operatorname{Stab}(x)$ is indeed a subgroup of G. [It need not be a normal subgroup.]
(c) Consider any element $x \in X$. From part (b) we may consider the set of cosets $G/\operatorname{Stab}(x)$. Prove that the function $\Phi : G/\operatorname{Stab}(x) \to \operatorname{Orb}(x)$ defined by $\Phi([a]) = a(x)$ is a well-defined bijection.

3. Burnside's Lemma. Suppose that the group $(G, *, \varepsilon)$ acts on the set X. Consider the set of pairs $(g, x) \in G \times X$ satisfying $g(x) = x$:

$$S = \{(g, x) : g(x) = x\} \subseteq G \times X.$$

Suppose that G and X are finite so that S is finite.

(a) Explain why $\#S = \sum_{x \in X} \#\operatorname{Stab}(x)$.
(b) For any $g \in G$, let $\operatorname{Fix}(g) = \{x \in X : g(x) = x\} \subseteq X$ be the set of elements of X that are "fixed by g". Explain why $\#S = \sum_{g \in G} \#\operatorname{Fix}(g)$. It follows from (a) and (b) that

$$\sum_{x \in X} \#\operatorname{Stab}(x) = \sum_{g \in G} \#\operatorname{Fix}(g).$$

(c) From Problem 2 we know that X is a disjoint union of orbits. Let X/G denote the set of orbits. Use the Orbit-Stabilizer Theorem to prove that $\sum_{x \in X} \#\operatorname{Stab}(x) = \#G \cdot \#(X/G)$, and conclude that the number of orbits is equal to the average number of elements of X fixed by an element of G:

$$\#(X/G) = \frac{1}{\#G} \cdot \sum_{g \in G} \#\operatorname{Fix}(g).$$

[Hint: Let $k = \#(X/G)$ and let $X = \text{Orb}(x_1) \sqcup \cdots \sqcup \text{Orb}(x_k)$ be the decomposition into orbits. For any element $x \in \text{Orb}(x_i)$ show that $\#\text{Stab}(x) = \#G/\#\text{Orb}(x_i)$. Now add them up.]

4. Counting Necklaces. Fix some integers $n, k \geq 1$. Let X be the set of words $(x_1, \ldots, x_n)$ with $x_i \in \{1, 2, \ldots, k\}$ for all i, so that $\#X = k^n$. The symmetric group S_n acts on the set X by permuting entries. Let $c = (1, 2, \ldots, n) \in S_n$ be the standard n-cycle and consider the cyclic group $G = \langle c \rangle$ of size n. The orbits of G acting on X are called *necklaces*. We can think of a necklace as a cyclic configuration of n beads using k possible colors.

(a) Explain why $\#\text{Fix}(c^i) = k^{\gcd(i,n)}$. [Hint: You investigated the permutations c^i in Problem 3 of Homework 2.]

(b) Use Burnside's Lemma to show that

$$\#\{\text{necklaces}\} = \frac{1}{n} \cdot \sum_{i=0}^{n-1} k^{\gcd(i,n)}.$$

(c) Compute the number of necklaces with 12 beads of 2 possible colors.

5. Euler's Totient Function. For any integer $n \geq 1$ we define

$$\phi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{a \in \mathbb{Z} : 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}.$$

(a) Consider any integer $k \geq 1$ and prime $p \geq 2$. Explain why $\phi(p^k) = p^k - p^{k-1}$. [Hint: The only integers less than p^k that are not coprime to p^k are the multiples of p.]

(b) Let R and S be rings. The *direct product ring* $R \times S$ is defined analogously to groups. It is straightforward to check that the groups of units satisfy

$$(R \times S)^\times = R^\times \times S^\times.$$

Combine this with the Chinese Remainder Theorem to prove for all $m, n \in \mathbb{Z}$ that

$$\gcd(m, n) = 1 \quad \Longrightarrow \quad \phi(mn) = \phi(m)\phi(n).$$

(c) Combine parts (a) and (b) to prove for any integer $n \geq 1$ that

$$\phi(n) = n \cdot \prod_{p|n} \frac{p-1}{p},$$

where the product is over the distinct prime divisors of n. [Hint: Write the prime factorization of n as $n = p_1^{k_1} \cdots p_N^{k_N}$. From part (a) we have $\phi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i - 1} = p_i^{k_i}(p_i - 1)/p_i$. Now use part (b).]