Introduction to Groups

Arjun Vardhan

January 2022

1 Integers mod n

- The congruence class or residue class of a mod n, denoted $\overline{a}$, is the set of all integers congruent to a modulo n. That is, $\overline{a} = \{n \in \mathbb{N} : n \equiv a \bmod n\}$.
- There are precisely n distinct congruence classes mod n, namely, $\overline{1}, \overline{2}, ..., \overline{n-1}$.
- The set of these congruence classes is called the integers mod n, denoted $\mathbb{Z}/n\mathbb{Z}$.
- Addition and multiplication for the elements of $\mathbb{Z}/n\mathbb{Z}$ is defined as $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} * \overline{b} = \overline{a * b}$.
- The collection of residue classes in $\mathbb{Z}/n\mathbb{Z}$ that have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$, denoted $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \exists\, \overline{c} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \overline{a} * \overline{c} = 1\}$ is a notable subset of $\mathbb{Z}/n\mathbb{Z}$.
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$**. That is,** $\overline{a}$ **has a multiplicative inverse in** $\mathbb{Z}/n\mathbb{Z}$ **if and only if gcd**$(a, n) = 1$**.** *Proof:* Let $X = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$. Suppose $\overline{a} \in X$. Then, there exist $x, y \in \mathbb{N}$ such that $ax + ny = 1$, and thus $ax \equiv 1 \bmod n$. So $\overline{a} * \overline{x} = 1$ and $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. The converse is shown to be true with a similar argument. ■

2 Basic Axioms

- A binary operation on a set G is a function $* : G \times G \to G$.
- $(G, *)$ is a group if:
  1. $a * b \in G$ for all $a, b \in G$.
  2. $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
  3. There exists $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.
  4. For all $a \in G$, there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

  $(G, *)$ is an abelian group if $a * b = b * a$ for all $a, b \in G$.
- $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under $+$; the identity is $\overline{0}$ and the inverse of $\overline{a}$ is $\overline{-a}$.
- $(\mathbb{Z}/n\mathbb{Z})^\times$ is an abelian group under $*$; the identity is $\overline{1}$.
- If $(A, \bigstar)$ and $(B, \Diamond)$ are groups, then the direct product of A and B, $A \times B = \{(a, b) : a \in A, b \in B\}$ where $(a_1, b_1) * (a_2, b_2) = (a_1 \bigstar a_2, b_1 \Diamond b_2)$ with $a_1, a_2 \in A$ and $b_1, b_2 \in B$.
- $A \times B$ is a group.
- **If** $(G, *)$ **is a group, then:**
  1. **The identity of G is unique.** *Proof:* Suppose f and g are both identities of G. Then, $f * g = g * f = f = g$. ■
  2. **For each** $a \in G$**,** a^{-1} **is unique.** *Proof:* Suppose b and c are both inverses of a. Then, $a * b = e$ and $c * a = e$. Thus, $c = c * e = c * (a * b) = (c * a) * b = e * b = b$. ■
  3. $(a^{-1})^{-1} = a$ **for all** $a \in G$**.** *Proof:* Since $a^{-1} * a = a * a^{-1}$, $(a^{-1})^{-1} = a$, by the definition of an inverse. ■

4. $(a*b)^{-1} = b^{-1}*a^{-1}$**, for all** $a,b \in G$**.** *Proof:* Let $c = (a*b)^{-1}$. So $c*a*b = e \Rightarrow a*(b*c) = e \Rightarrow b*c = a^{-1}*e \Rightarrow b*c = a^{-1} \Rightarrow c = b^{-1}*a^{-1}$ ■.

- **Left and Right Cancellation Laws:**
  1. **If** $au = av$**, then** $u = v$**.** *Proof:* $au = av \Rightarrow a = avu^{-1} \Rightarrow vu^{-1} = e \Rightarrow v = u$. ■
  2. **If** $ua = va$**, then** $u = v$**.** *Proof:* $ua = va \Rightarrow a = u^{-1}va \Rightarrow e = u^{-1}v \Rightarrow u = v$. ■
- Let $x \in G$. The order of x, denoted $|x|$, is the smallest postive integer n such that $x^n = e$. If no such n exists, then x is said to have infinite order.
- Let $x \in G$ and $a, b \in \mathbb{Z}^+$. Then, $x^a x^b = x^{a+b}$, $(x^a)^b = x^{ab}$ and $(x^a)^{-1} = x^{-a}$.
- Let $H \subset G$, $H \neq \phi$. If $e \in H$, and for all $h, k \in H$, $hk, h^{-1} \in H$, then H is a subgroup of G.
- If $x \in G$, then $\{x^n : n \in \mathbb{N}\}$ is the cyclic subgroup generated by x.
- If $|x| = n$, then $e, x, x^2, ..., x^{n-1}$ are all distinct. If $|x| = \infty$, then all powers of x are distinct.

3 Dihedral Groups

- For all $n \in \mathbb{N}$, $n \geq 3$, D_{2n}, the dihedral group of order $2n$, is the set of all symmetries of a regular n-sided polygon.
- Consider a regular n-gon fixed at the origin. The vertices are numbered from 1 to n. Since for each vertex i there is a permutation that sends 1 to i, vertex 2 will end up at either $i-1$ or $i+1$. So there are $2n$ possible permutations or symmetries, that is, n rotations by $\frac{2\pi}{n}$ radians and n reflections about the n lines of symmetry.
- Let r be a clockwise rotation about the origin by $\frac{2\pi}{n}$ radians. Let s be the reflection about the line passing through vertex 1 and the origin. Then,
  1. $e, r, r^2, ..., r^{n-1}$ are all distinct, and $|r| = n$.
  2. $|s| = 2$.
  3. $s \neq r^i$ for all $i \in \mathbb{N}$.
  4. $sr^i \neq sr^j$ for all $0 \leq i, j \leq n-1$ if $i \neq j$. Thus, $D_{2n} = \left\{e, r, r^2, ..., r^{n-1}, s, sr, sr^2, ..., sr^{n-1}\right\}$.
  5. $rs = sr^{-1}$. This shows that s and r don't commute and thus D_{2n} is non-abelian.
  6. $r^i s = sr^{-i}$, for all $0 \leq i \leq n-1$.

4 Symmetric Groups

- Let $\Omega \neq \phi$, and let S_Ω be the set of all bijections from Ω to itself. Then, S_Ω is a group under function composition. Its identity is the identity permutation. S_Ω is called the symmetric group on Ω.
- When $\Omega = \{1, 2, 3, ..., n\}$, then it is denoted S_n, the symmetric group of order n.
- $|S_n| = n!$.
- The cycle $(a_1 a_2 ... a_m)$ is the permutation which sends a_i to a_{i+1}, $1 \leq i \leq m-1$, and sends a_m to a_1.
- If $\sigma = (123)(45)(76)$, then $\sigma^{-1} = (321)(54)(67)$.
- S_n is non-abelian for $n \geq 3$.
- Two cycles are disjoint if they have no numbers in common.
- Disjoint cycles commute.
- The cycle decomposition of a permutation expresses it as a product of disjoint cycles.
- The order of a permutation is the least common multiple of the lengths of the cycles in its cycle decomposition.

5 Quaternion Group

- The Quaternion Group, denoted Q_8, is defined as: $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, where 1 is the identity, $|-1| = 2$, $-1 * a = a * (-1) = -a$ for all $a \in Q_8$, $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$, $jk = i$, $kj = -i$, $ki = j$ and $ik = -j$.
- Q_8 is a non-abelian group of order 8.

6 Homomorphisms and Isomorphisms

- Let $(G, \bigstar)$ and $(H, \Diamond)$ be groups. A homomorphism is a map $f : G \to H$ such that $f(g_1 \bigstar g_2) = f(g_1) \Diamond f(g_2)$, for all $g_1, g_2 \in G$.
- The map $f : G \to H$ is called an isomorphism if f is a homomorphism and f is bijective. If such an f exists, G and H are said to be isomorphic, denoted $G \cong H$.
- **If $G \cong H$, then:**
  1. $|G| = |H|$.
  2. G **is abelian if and only if** H **is abelian.** *Proof:* Suppose G is abelian. Then $x * y = y * x$ for all $x, y \in G$. Let $c, d \in H$. Since f is surjective, $c = f(a)$ and $d = f(b)$ for some $a, b \in G$. Thus, $c * d = f(a) * f(b) = f(a * b) = f(b * a) = f(b) * f(a) = d * c$. Conversely, suppose H is abelian. Let $a, b \in G$. Since f is surjective, there exist $c, d \in H$ such that $f(a) = c$ and $f(b) = d$. Thus, $f(a * b) = f(a) * f(b) = f(b) * f(a) = f(b * a)$. Since f is injective, this means that $a * b = b * a$. ■
  3. G **is cyclic if and only if** H **is cyclic.** *Proof:* Suppose G is cyclic. Then $a \in G \Rightarrow a = x^m$, $m \in \mathbb{Z}$ for some $x \in G$. Let $b \in H$. Since f is surjective, $b = f(c)$ for some $c \in G$. Let $c = x^k$. Then $b = f(x^k) = f(x)^k$. Thus H is a cyclic group generated by $f(x)$. Conversely, suppose H is cylic, generated by x. Let $b \in H$, $b = x^k$. Since f is surjective, $b = f(c)$ and $x = f(d)$ for some $c, d \in G$. Thus, $f(c) = f(d)^k = f(d^k)$. Since f is injective, $c = d^k$ and thus G is cyclic, generated by d. ■
- $|f(x)| = |x|$**, if** f **is an isomorphism.** *Proof:* First we must show that an homomorphism maps identity elements of two groups to each other. Let e_G be the identity element for G and e_H for H. Then, $e_G * g = g$ for all $g \in G$. Let $f(g) = h$. Then $f(e_G * g) = f(e_G) * f(g) = f(e_G) * h$. But $f(e_G * g) = f(g) = h$. So $f(e_G) * h = h$ and thus $f(e_G) = e_H$. Now let $x \in G$, $f(x) = y$ and $|x| = n$. So $x^n = e_G$ and thus $f(x^n) = f(x)^n = y^n = e_H$. Thus $|y| \leq n$. Suppose $|y| = k < n$. Then $f(x^k) = f(x)^k = y^k = e_H$. But since f is injective, $x^k = e_G$ which is a contradiction. So $|y| = n$. ■
- **Corollary: Two isomorphic groups have the same number of elements of order** n**, for all** $n \in \mathbb{N}$**.**
- If $f : G \to H$ is a homomorphism, the kernel of f, denoted $\mathrm{Ker}(f)$, is $\{g \in G : f(g) = e_H\}$.
- **Ker**(f) **is a subgroup of G.** *Proof:* Let $h, k \in \mathrm{Ker}(f)$. Then $f(h) = f(k) = e_H$. $f(h * k) = f(h) * f(k) = e_H$ so H is closed under $*$. We already showed that a homomorphism maps identity elements to each other so $e_G \in \mathrm{Ker}(f)$. $f(h * h^{-1}) = f(h) * f(h^{-1}) = e_H * f(h^{-1})$. But $f(h * h^{-1}) = f(e_G) = e_H$, so $f(h^{-1}) = e_H$. Thus $h^{-1} \in \mathrm{Ker}(f)$. ■
- f **is injective if and only if Ker**$(f) = \{e\}$**.** *Proof:* First, we need to show that a homomorphisms sends inverses to inverses. Let $g \in G$, $f(g) = h$. Then, $f(g * g^{-1}) = f(g) * f(g^{-1}) = h * f(g^{-1}) = e$. So $f(g^{-1}) = h^{-1}$. Now suppose f is injective. Then e_G will be the only element mapped to e_H, so $\mathrm{Ker}(f) = \{e\}$. Conversely, suppose $\mathrm{Ker}(f) = \{e\}$. Let $g_1, g_2 \in G$. Suppose $f(g_1) = f(g_2)$. Then, $f(g_1 * {g_2}^{-1}) = f(g_1) * f({g_2}^{-1}) = f(g_1) * f(g_2)^{-1} = f(g_1) * f(g_1)^{-1} = e$. Since $\mathrm{Ker}(f) = \{e\}$, $g_1 * {g_2}^{-1} = e$ and thus $g_1 = g_2$. So f is injective. ■
- $\mathrm{Aut}(G)$ is the set of all isomorphisms from G onto G.

- **The automorphism group of G, that is, $\mathbf{Aut}(G)$, is a group under function composition.** *Proof:* The identity homomorphism is bijective so it belongs to $\mathrm{Aut}(G)$. Let $f, h \in \mathrm{Aut}(G)$. Since f, h are bijective, so are $f \circ h$ and f^{-1}. Since f, h are from G onto G, so are $f \circ h$ and f^{-1}. Let $g_1, g_2 \in G$. Then, $f \circ h(g_1 * g_2) = f(h(g_1) * h(g_2)) = f \circ h(g_1) * f \circ h(g_2)$. Let $f(g_1) = g_3$ and $f(g_2) = g_4$. Then, $f^{-1}(g_3 * g_4) = g_1 * g_2 = f^{-1}(g_3) * f^{-1}(g_4)$. Thus we see that if f, h are homomorphisms, then so are $f \circ h$ and f^{-1}. ■

7 Group Actions

- A group action on a set A is a map from $G \times A$ to A, denoted $g \cdot a$, such that:
  1. $g_1 \cdot (g_2 \cdot a) = (g_1 * g_2) \cdot a$.
  2. $e \cdot a = a$ for all $a \in A$.
- For each fixed $g \in G$, we have $\sigma_g : A \to A$, $\sigma_g(a) = g \cdot a$. For all $g \in G$, σ_g is a permutation of A.
- **The map from G to the symmetric group over A defined by $g \to \sigma_g$ is a homomorphism.** *Proof:* Let $f : G \to S_A$, $f(g) = \sigma_g$. Let $g_1, g_2 \in G$. Then, $f(g_1 * g_2) = \sigma_{g_1 * g_2}$. Now, $\sigma_{g_1 * g_2} : A \to A$, $\sigma_{g_1 * g_2}(a) = (g_1 * g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1} \circ \sigma_{g_2}(a)$. So $f(g_1 * g_2) = f(g_1) \circ f(g_2)$. ■
- The above map is called the permutation representation of the group action.
- Let $g \cdot a = a$ for all $g \in G$, $a \in A$. This is the trivial action and is said to act trivially on A.
- If distinct elements of G induce distinct permutations of A, then the action is said to be faithful. The permutation representation of a faithful action is injective.
- The kernel of the action of G on A is defined as $\{g \in G : g \cdot a = a, \forall a \in A\}$. For the trivial action, the kernel is all of G.
- The stabilizer of a in G is defined as $\{g \in G : g \cdot a = a\}$.
- Let G act on itself with $g_1 \cdot g_2 = g_1 * g_2$. This is called the left regular action of G on itself and is faithful.
- **The kernel of an action of G on A is the same as the kernel of the permutation representation of the action.** *Proof:* Let the kernel of the action be H and the kernel of the permutation representation be K. Let (1) represent the identity permutation in S_A. Then, $H = \{g \in G : g \cdot a = a, \forall a \in A\}$ and $K = \{g \in G : \sigma_g = (1)\}$. Let $g_1 \in H$. Then $g_1 \cdot a = a$ for all $a \in A$. Therefore $\sigma_{g_1} = a$ for all $a \in A$, and thus $\sigma_{g_1} = (1)$. Let $g_2 \in K$. Then $\sigma_{g_2} = (1)$ and so $g_2 \cdot a = a$ for all $a \in A$. Thus $g_2 \in H$. ■