MATH 113: Abstract Algebra

Jack Lipson

September 19, 2023

Contents

Chapter 0

A Few Preliminaries

0.1 Sets and Equivalence Relations

Note. $\mathbb{R}^*$ and $\mathbb{C}^*$ represent the set of all nonzero real and complex numbers. Zero is excluded from $\mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$.

Note. When a set contains an element b that's algebraically or arithmetically equivalent to another element(s), our set can be partitioned into subsets $\overline{b}$ which denote all entitites equivalent to b. e.g. $\frac{2}{3} = \frac{4}{6}$.

Definition 1 (Parititon)**.** A *partition* of a set is a decomposition of the set into subsests s.t. every element is in exactly one subset, or *cell*.

Definition 2 (Equivalence Relation)**.** For a nonempty set S, $\sim$ is an equivalence relation between elements of S if for all $a, b, c \in S$, $(S, \sim)$ satisfies:

1. (Reflexive) $a \sim a$.
2. (Symmetric) $a \sim b \Rightarrow b \sim a$.
3. (Transitive) $a \sim b \wedge b \sim c \Rightarrow a \sim c$.

Non-equivalence relations usually use $\mathscr{R}$.

Note. All relations $\mathscr{R}$ are defined as $\{(a, b) \text{ for a } \in A, b \in B \mid a \mathscr{R} b\} \subseteq A \times B$. For equivalence relations, $\sim \subseteq S \times S$.

Remark (Natural Parition)**.** $\sim$ yields a natural partition of S: $\overline{a} = \{x \in S \mid x \sim a\}$ for all $a \in S$.

Explanation. For any $a \in S$, $a \in \overline{a}$. So each element of S is in at least one cell. To show that a is in exactly one cell, let $a \in \overline{b}$ as well. We must show

$\overline{a} = \overline{b}$. $\Rightarrow$: If $x \in \overline{a}$ then $x \sim a$. From our assumption $a \sim b$ so by (3), $x \sim b$ so $x \in \overline{b}$ thus, $\overline{a} \subseteq \overline{b}$. $\Leftarrow$: If $x \in \overline{b}$, $x \sim b$. From our assumption, $a \sim b$ so, by (2), $b \sim a$ meaning $x \sim a$ via (3) implying $x \in \overline{a}$ s.t. $\overline{b} \subseteq \overline{a}$. This completes the proof.

Definition 3 (Equivalence Class)**.** Each cell $\overline{a}$ in a natural partition given by an equivalence relation is called an equivalence class.

Definition 4 (Congruence Modulo n)**.** Let h, k be distinct integers and $n \in \mathbb{Z}^+$. We say h *congruent* to k modulo n, written $h \equiv k \pmod{n}$ if $n \mid h - k$ s.t. $h - k = ns$ for some $s \in \mathbb{Z}$.

Definition 5 (Residue Classes Modulo)**.** Equiva;ence calsses for congruence modulo n are *residue classes modulo* n.

Remark. Each residue class modulo $n \in \mathbb{Z}^+$ contains an infinite number of elements.

Definition 6 (Irreducible)**.** An irreducible polynomial $h(x)$ is one that cannot be factored into polynomials in $\mathcal{P}(\mathbb{R})$ all of lower degree than $h(x)$.

Chapter 1

Introduction to Groups

1.1 Binary Operations

Definition 7 (Binary Operation)**.** A *binary operation* $*$ on a set S is a rule that assigns to each ordered pair (a, b) of elements of S another element of S generally denoted $a * b$ or formally $*(a, b)$. To be *well-defined*, $*$ must assign a value to every possible $a * b$.

Definition 8 (Closure under $*$)**.** A set S is *closed under* $*$ if for all $a, b \in S$, $a * b \in S$. If a subset H of S is also closed under $*$, this is referred to as the *induced operation* $*$ on H.

Definition 9 (Commutative Operation)**.** A binary operation $*$ on a set S is *commutative* iff $a * b = b * a$ for all $a, b \in S$.

Definition 10 (Associative operation)**.** A binary operation $*$ on a set S is *associative* iff $(a * b) * c = a * (b * c)$ for all $a, b, c \in S$.

Note. Associativty of function compostion follows.

Remark. A binary operation on a set, typically finite, can be represented as follows:

$*$	a	b	c
a	b	b	b
b	a	c	b
c	c	b	a

1.2 Groups

Definition 11 (Group). A group $\langle G, * \rangle$ is a set G combined with a binary operation $*$ on G which satisfies the following axioms:

($\mathscr{G}_1$) $*$ is associative.

($\mathscr{G}_2$) There exists a **unique** *identity* element e on G s.t. $e * x = x * e$ for all $x \in G$.

($\mathscr{G}_3$) For each $a \in G$, there exists an $a' \in G$ s.t. $a' * a = a * a' = e$. This a' is called the *inverse* of a with respect to the operation $*$.

($\mathscr{G}_4$) *(optional if part of binary operation definition)* G is closed under $*$.

Theorem 1 (Left/Right Cancellation). If G is a group with binary operation $*$, then the *left and right* cancellation laws hold s.t. $a * b = a * c \Rightarrow b = c$ and $b * a = c * a \Rightarrow b = c$ for all $a, b, c \in G$.

Proof. The right cancellation proof is identical to that below.

$$\begin{aligned} a * b &= a * c && \because \text{ by supposition} \\ a' * (a * b) &= a' * (a * c) && \because \text{ inverse axiom.} \\ (a' * a) * b &= (a' * a) * c && \because \text{ associativity axiom} \\ e * b &= e * c && \because \text{ inverse axiom} \\ b &= c && \square \text{ identity axiom} \end{aligned}$$

$\square$

Theorem 2. Trivially, in a group G, $(ab)' = b'a'$ for all $a, b \in G$.

Remark. Note that the solutions x, y to $a * x = b$ and $y * a = b$ have unique solutions in G for any $a, b \in G$. Similarly, e is unique.

Note (Idempotent for $*$). An element x of S is *idempotent for* $*$ if $x * x = x$. This is always in the identity element.

Definition 12 (Abelian Group). A group G is *abelian* if its binary operation is commutative.

Definition 13 (Roots of Unity). Call the elements of the set $U_n := \{z \in \mathbb{C} \mid z^n = 1\}$ the n^{th} roots of unity, usually listed as $1 = \zeta^0, \zeta^1, \zeta^2, \ldots, \zeta^{n-1}$.

Remark. Let the unit circle $U := \{z \in \mathbb{C} \mid |z| = 1\}$. Clearly, for any $z_1, z_2 \in U$, $|z_1 z_2| = |z_1||z_2| = 1$ such that $z_1 z_2 \in U$ implying U is closed under $\cdot$. Note then that $\langle U, \cdot \rangle \simeq \langle R_{2\pi}, +_{2\pi} \rangle$. Similarly, $\langle U_n, \cdot \rangle \simeq \langle \mathbb{Z}_n, +_n \rangle$ for $n \in \mathbb{Z}^+$.

Definition 14 (Addition Modulo n). We respecitvely write $\mathbb{Z}_n$ and $\mathbb{R}_c$ to denote $[0, 1, \ldots, n-1]$ and $[0, c]$. Addition modulo n/c is written $+_n$ or $+_c$.

1.3 Isomorphic Binary Structures

Definition 15 (Binary Algebraic Structures). For two *binary algebraic structures* $\langle S, *\rangle$ and $\langle S', *'\rangle$ to be structurally alike, we would need a one-to-one correspondence between the elements $x \in S$ and $x' \in S'$ s.t. if $x \leftrightarrow x'$ and $y \leftrightarrow y'$ then $x * y \leftrightarrow x' *' y'$.

Remark (Homomorphism Property). This last condition is called the *homorphism property*. If the function ϕ is NOT one-to-one, it is a homormorphism only.

Definition 16 (Isomorphism). An *isomorphism* of S with S' is a one-to-one function ϕ mapping S onto S' such that $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in S$.

If such a map exists, S and S' are called *isomorphic binary structures* denoted $S \simeq S'$.

Note (Show Binary Algebraic Structures are Isomorphic).

(Step 1) Define the function ϕ which defines $\phi(s)$ for all $s \in S$ and gives the isomorphism from $S \to S'$.

(Step 2) Show ϕ is one-to-one.

(Step 3) Show ϕ is onto.

(Step 4) Show $\phi(x * y) = \phi(x) *' \phi(y)$ for all $x, y \in S$.

Example. Take the isomorphism $\phi \colon \mathbb{R} \to \mathbb{R}^+ \colon x \longmapsto e^x$ from $\langle \mathbb{R}, +\rangle$ to $\langle \mathbb{R}^+, \cdot\rangle$. Clearly, $\forall x \in \mathbb{R}, \phi(x) \in \mathbb{R}^+$ and ϕ is bijective. Last, for $x, y \in \mathbb{R}$, $\phi(x + y) = e^{x*y} = e^x e^y = \phi(x) \cdot \phi(y)$.

Definition 17 (Structural Property). A structural property is any property of a binary structure that is invariant to any isomorphic structure. These, like cardinality, are used to show no such isomorphism exists between structures.

Example. Although $\langle \mathbb{Q}, +\rangle$ and $\langle \mathbb{Z}, +\rangle$ both have cardinality $\aleph_0$ and have many one-to-one functions between them, the equation $x + x = c$ has a solution $x \in Q$ for all $c \in \mathbb{Q}$, but this is not true for $\mathbb{Z}$ if, say, $c = 3$. This structural propery distinguishes these binary structures and thus they are not isomorphic under the usual addition.

Theorem 3. Suppose $\langle S, * \rangle$ has an identity element e for $*$. If $\phi\colon S \to S'$ is an isomorphism to $\langle S', *' \rangle$ then $\phi(e)$ is an identity element for $*'$ on S'.

Proof. Because an isomorphism exists from $S \to S'$, for any element $s' \in S'$, there exists exactly one element $s \in S$ s.t. $\phi(s) = s'$. By the definition of an isomorphism $s' = \phi(s) = \phi(s * e) = \phi(s) *' \phi(e) = s' *' \phi(e)$ for an arbitary element s' of S. This implies $\phi(e)$ is the identity element for S'. □

1.4 More on Groups and Subgroups

Definition 18 (Semigroup)**.** A semigroup is an algebraic structure combining a set with an associative binary oxperation.

Definition 19 (Monoid)**.** A monoid is a semigroup that has an identity element corresponding to its binary operation.

Definition 20 (Subgroup)**.** If a subset H of a group G is closed under the binary operation of G and is itself a group, H is a *subgroup* of G. This is denoted $H \leq G$. $H < G \Rightarrow H \neq G$.

Example. $\langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$, but $\langle \mathbb{Q}, \cdot \rangle$ is *not* a subgroup of $\langle \mathbb{R}, - \rangle$.

Definition 21 (Proper and trivial subgroups)**.** If G is a group, the subgroup consisting of G itself is the *improper subgroup* of G. All other subgroups are *proper subgroups*. The subgroup $\{e\}$ is the *trivial subgroup* of G and all other subgroups are nontrivial.

Theorem 4. A subset H of a group G is a subgroup of G if and only if:

1. H is closed under the binary operation of G.
2. the identity e of G is in H.
3. for all $a \in H$, $a^{-1} \in H$ also.

Proof. $\Rightarrow$: Let H be a subgroup of G. By definition, H is closed under G's binary operation (1). H must have an identity element because it is a group. Because $a * x = a$ and $y * a = a$ have unique solutions, H's identity element must be the same in H group as G group (2). (3) is trivial because H is a group.

$\Leftarrow$: Let (1), (2), (3) be true. Then H has a unique identity element on its binary operation ($\mathscr{G}_2$), each element of H has a unique inverse in H ($\mathscr{G}_3$), and H is closed under the binary operation of G (*optional* $\mathscr{G}_4$). To satisfy ($\mathscr{G}_1$), the binary operation on H must be associative s.t., for all $a, b, c \in H$, $(ab)c = a(bc)$. But this is clearly holds in G so ($\mathscr{G}_1$) is satisfied and H is a subgroup of G. □

1.5 Cyclic Groups

Theorem 5. Let G be a group and $a \in G$. Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G and the *smallest* subgroup of G that contains a.

Proof. Let's first check H is indeed a subgroup of G. (1) For any $r, s \in \mathbb{Z}$, $a^r * a^s = \overbrace{(a * \cdots * a)}^{a\ r\ \text{times}} * \overbrace{(a * \cdots * a)}^{a\ s\ \text{times}} = a^{r+s} \in H$ so we have closure. (2) Let $e := a^0 \in H$ so for all $r \in \mathbb{Z}$, $a^r * a^0 = a^r$. (3) For all $r \in \mathbb{Z}$, $a^r \in H$ so $\exists a^{-r} \in H$ such that $a^r * a^{-r} = a^0 = e$. Thus, $H \leq G$.

Next, to show it's the smallest possible subgroup, just take the set $\{a\}$. To have closure, we must add a^n $\forall n \in Z^+$. To have inverses, we must have a^{-n} so our set becomes $\{a^n \mid n \in Z \setminus \{0\}\}$. To have an identity, we must have a^0 and this completes the proof. □

Definition 22 (Cyclic Subgroup of G)**.** For any $a \in G$, define $\langle a \rangle$ to be the set $\{a^n \mid n \in \mathbb{Z}\}$. This is called the *cyclic subgroup of G generated by a*. An element a of a group G *generates* G and is a *generator for* G if $\langle a \rangle = G$.

Definition 23 (Cyclic Group)**.** A group is *cyclic* if there is some element a in G that generates G.

Example. $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$ so Z_4 is cyclic and both 1 and 3 are generators.

Example. The group $\langle \mathbb{Z}, + \rangle$ is a cyclic group generated ONLY by 1 and -1.

Remark (Subgroup Diagrams)**.** Lattice, or *subgroup diagrams*, can be drawn such that lines run down from a group G to a group H if $H < G$.

Example. Take two group structures of order 4: $\mathbb{Z}_4$ and the Klein 4-group *Vierergruppe* defined as follows:

$\mathbb{Z}_4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

V :

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

We can map these as:

$$\begin{tikzcd} Z_4 \arrow[d, dash] \\ \{0,2\} \arrow[d, dash] \\ \{0\} \end{tikzcd}$$

and

$$\begin{tikzcd} & V \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \{e,a\} \arrow[dr, dash] & \{e,b\} \arrow[d, dash] & \{e,c\} \arrow[dl, dash] \\ & \{e\} & \end{tikzcd}$$

.

Definition 24 (Order)**.** If the cyclic subgroup $\langle a \rangle$ of G is finite, we say the *order* of a is the order $|\langle a \rangle|$. Otherwise, a is of *infinite order*.

Theorem 6. Every cyclic group is abelian.

Theorem 7 (Division Algortihm for $\mathbb{Z}$)**.** If $m \in \mathbb{Z}^+$ and $n \in \mathbb{Z}$, then there exist unique integers q, r such that

$$n = mq + r \quad \text{and} \quad 0 \leq r < m.$$

Proof. From the archimedean property, there is a unique q such that $qm \leq n < (q+1)m$. Then, $0 \leq r = n - mq < m$ is unique. We regard q and r as the quotient and nonnegative remainder respectively when n is divided by m. □

Theorem 8. A subgroup of a cyclic group is cyclic.

Proof. Take a cyclic group G with subgroup H. If $H = \langle e \rangle$, then H is cyclic and the proof is complete.

Otherwise, $H \neq \langle e \rangle$ so there exists $b \in H, b \neq e$. Because G is cyclic, there must exist $a \in G$ such that a generates G, i.e. for all $n \in \mathbb{Z}^+$, a^n spans every value of G including every element of H. Let $c := a^m$ where m is the least positive integer such that $c \in H$. Now, for all $b \in H$, take n such that $b = a^n$. From division algorithm, there exist integers q, r such that $n = mq + r$ so $a^n = a^{mq+r} = (a^m)^q a^r$ which implies, because $a^m \in H$ and H is a group so $a^{-m} \in H$, $a^n(a^m)^{-q} = a^r$. H is a group so this implies $a^r \in H$. Because $0 \leq r < m$ and m is the least positive integer such that $a^m \in H$, $r = 0$ such that $n = mq$ for all $b = a^n = (a^m)^q \in H$. $\langle c \rangle = H$ so H is cyclic. □

Definition 25 (Greatest Common Divsior). The positive generator d of the cyclic group $H = \{nr + ms \mid n, m \in \mathbb{Z}\}$ under addition is called the *greatest common divisor* of r and s, written $d = \gcd(r, s)$.

Definition 26. Two integers are *relatively prime* if their gcd is 1.

Theorem 9. Let G be a cyclic group with generator a. If the order of G is infinite, then G is isomorphic to $\langle \mathbb{Z}, + \rangle$. If G has finite order n, then G is instead isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$.

Proof. Take the following two cases. **Case 1:** For all positive integers m, $a^m \neq e$. Suppose $a^h = a^k$ and $h > k$. Thus, $a^h a^{-k} = a^{h-k} = e$ which contradicts our assumption. Therfore, each element of G can be uniquely expressed as a^m for a unique $m \in \mathbb{Z}$. The map $\phi : G \to \mathbb{Z}$ defined as $\phi(a^i) = i$ is then well-defined and bijective on $\mathbb{Z}$. Last, $\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j)$ so the homomorphism property is satisfied and ϕ is an isomorphism to $\langle \mathbb{Z}, + \rangle$.

Case 2: $a^m = e$ for some $m \in \mathbb{Z}^+$. Let n be the smallest positive integer so $a^n = e$. If $s \in \mathbb{Z}$ and $s = q + r$ for $0 \leq r < n$, then $a^s = a^{nq+r} = (a^n)^q a^r = a^r$. Like in case 1, if $0 < k < h < n$ and $a^h = a^k$, then $a^{h-k} = e$ and $0 < h - k < n$ contradicting our assumption that n is the smallest positive integer possible. Hence, $a^0, a^1, a^2, \ldots, a^{n-1}$ are all distinct and comprise all elements of G. We can then make the map $\psi : G \to \mathbb{Z}_n$ defined by $\psi(a^i) = i$ for $i = 0, 1, \ldots, n-1$ is well-defined and bijective on Z_n. Also, because $a^n = e$, $a^i a^j = a^k$ whenever $k = i +_n j$. Therefore, $psi(a^i a^j) = i +_n j = \psi(a^i) +_n \psi(a^j)$ satisfying the homomorphism property so ϕ is an isomorphism to $\langle \mathbb{Z}_n, +_n \rangle$. $\square$

Theorem 10. Let G be a cyclic group generated by a with n elements. Let $b \in G$ and $b = a^s$. Then, b generates a cyclic subgroup H of G containing n/d elements where d is the greatest common divisor of n and s. Also, $\langle a^s \rangle = \langle a^n \rangle \Leftrightarrow \gcd(s, n) = \gcd(t, n)$.

Proof. We already know b generates a cyclic subgroup H of G. And that because it is finite, it has only as many elements as the smallest power m of b so $b^m = e$. This and $b = a^s$ implies $(a^s)^m = e$ if and only if n divides ms because $a^n = e$ because G is of finite order n. Let $d = \gcd(n, s)$ such that we want to find the smallest m so $\frac{ms}{n} = \frac{m(s/d)}{(n/d)}$ is an integer. This implies (n/d) divides m so the smallest m we can pick *is* n/d. Thus, H has order n/d.

We know G is isomorphic to $\langle \mathbb{Z}_n, +_n \rangle$ so taking cyclic subgroup $\langle d \rangle$ of $\mathbb{Z}_n$ where d divides n implies $\langle d \rangle$ has n/d elements and contains all positive integers m less than n such that $\gcd(m, n) = d$. Thus, there is only one subgroup of $\mathbb{Z}_n$ of order n/d. It immediately follows that $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$. $\square$

Corollary. If a is a generator of a finite cyclic group G of order n, then the other generators of G are the elements of the form a^r, where r is relatively prime to n.

Example. For instance, we can derive the subgroup diagram for Z_{18} as:

$$\begin{tikzcd}
& \langle 1\rangle = Z_{18} \arrow[dl, dash] \arrow[dr, dash] & & \\
\langle 2\rangle \arrow[dr, dash] & & \langle 3\rangle \arrow[dl, dash] \arrow[dr, dash] & \\
& \langle 6\rangle \arrow[dr, dash] & & \langle 9\rangle \arrow[dl, dash] \\
& & \langle 0\rangle &
\end{tikzcd}$$

1.6 Generating Sets and Cayley Digraphs

Example. The Klein 4-group $V = \{e, a, b, c\}$ is generated by $\{a, b\}$ since $ab = c$. It is similarly generated by $\{a, c\}, \{b, c, \}$, and $\{a, b, c\}$.

Theorem 11. The intersection of some subgroups H_i of a group G for $i \in I$ is again a subgroup of G where I is the set of indices.

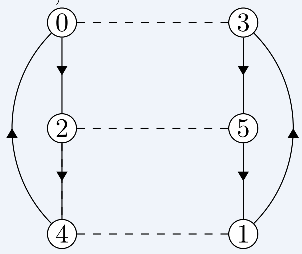
Proof. First, closure. For any $a, b \in \bigcap_{i\in I} H_i$, because each H_i has closure, $a, b \in H_i \Rightarrow ab \in H_i$ so $ab \in \bigcap_{i\in I} H_i$. Similarly, because the identity element of G is in H_i for all $i \in I$, $e \in \bigcap_{i\in I} H_i$. Last, for all $a \in H_i$, because H_i is a group, $a^{-1} \in H_i$. Thus, for any $a \in \bigcap_{i\in I} H_i$, $a \in H_i$ for all i so $a^{-1} \in H_i$ for all i so $a^{-1} \in \bigcap_{i\in I} H_i$. □

Definition 27 (Subgroup generated by $\{a_i \mid i \in I\}$)**.** Let G be a group and $a_i \in G$ for $i \in I$. The smallest subgroup of G containing $\{a_i \mid i \in I\}$ is the *subgroup generated by* $\{a_i \mid i \in I\}$. If this subgroup is all of G then the set *generates* G and the a_i are the *generators of* G. If there is a finite set that generates G, we say G is *finitely generated*.

Definition 28 (Digraph)**.** A directed graph, abbreviated as *digraph*, consists of a fininite number of points, or *vertices* and some *arcs* denoted by an arrowhead joining them together.

Definition 29 (Cayley Digraphs)**.** Cayley digraphs draw arcs of different types between each element of G demonstrating what each element is generated by. Of course, if $x \to y$ means $xa = y$ then $ya^{-1} = x$. Traveling opposite to arrow direction implies this second equality.

Example. For instance, we can create the digraph for Z_6 with generator set $S = \{2, 3\}$ as:



with solid (2) and dashed (3) lines. Dashed lines have no arrowhead because 3 is its own inverse.

Chapter 2

Permutations, Cosets, and Direct Products

2.1 Groups of Permutations

Definition 30 (Permutation of a set)**.** A *permutation of a set* A is a function $\phi\colon A \to A$ that is both one to one and onto.

Remark (Permutation Multiplication)**.** Function composition $\circ$ is a binary operation on the collection of all permutations of a set A. We call this operation *permutation multiplication.*

Remark. Let σ, τ be permutations of a set A so σ, τ are both one-to-one function mapping A onto A. then, $\sigma \circ \tau$, or simply $\sigma\tau$ is a permutation as long as it is one-to-one.

For any $a_1, a_2 \in A$, if $(\sigma\tau)(a_1) = (\sigma\tau)(a_2)$ gives $(\sigma(\tau(a_1))) = (\sigma()\tau(a_1))$. Because σ is injective, $\tau(a_1) = \tau(a_2)$. Because τ is injective, $a_1 = a_2$ so $\sigma\tau$ is injective.

For any $a \in A$, there exists some $binA$ so $\sigma(b) = a$ because σ is onto A. Because τ is onto A, there exists some $c \in A$ so $\tau(c) = b$. Thus, $a = (\sigma\tau)(c)$ so $\sigma\tau$ is onto A.

Example. Given a set $A = \{1, 2, 3, 4, 5\}$, we can write a permutation σ as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}.$$

so $\sigma(1) = 4$, etc.

Theorem 12. Let A be a nonempty set, and S_A be the collection of all permutations of A. Then, S_A is a group under permutation multiplication.

Proof. Because the composition of two permutations of A results in a permutation, we have closure under $\circ$. For any functions f, g, h, $((f \circ g) \circ h)(x) = (f(g)) \circ (h)(x) = f(g(h))(x) = f(g \circ h)(x)$ so $\mathscr{G}_1$ is easily satisfied. The permutation $\imath$ defined as $\imath(a) = a$ for all $a \in A$ is the identity ($\mathscr{G}_2$). Last, for any permutation σ, σ^{-1} reverse the direction of the mapping σ such that $\sigma^{-1}(a)$ is the element a' of A so $\sigma(a') = a$. This exists because σ is bijective. For any $a \in A$, $\imath(a) = a = \sigma(a') = \sigma(\sigma^{-1}(a')) = (\sigma\sigma^{-1})(a)$ and $\imath(a') = a' = \sigma^{-1}(a) = \sigma^{-1}(\sigma(a')) = (\sigma^{-1}\sigma)(a')$ satisfying $\mathscr{G}_3$. □

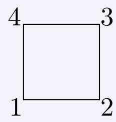
Remark. To define an isomorphism $\phi\colon S_A \to S_B$, we let $f\colon A \to B$ have one-to-one function mapping A onto B so A and B have the same cardinality so for $\sigma \in S_A$, let $\phi(\sigma) = \bar{\sigma} \in S_B$ so that for all $a \in A$, $\bar{\sigma}(f(a)) = f(\sigma(a))$.

Definition 31 (Symmetric Group on n Letters)**.** Let A be the finite set $\{1, 2, \ldots, n\}$. The group of all permutations of A is the *symmetric group on n letters* S_n. Note that S_n has $n!$ elements.

Remark. S_3 is also the 3rd dihedral group D_3 of *symmetries of an equilateral triangle* where ρ_i is rotations and μ_i is mirror images in bisectors of angles such that D_3 is made up of:

$$\left\{\begin{matrix} \rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & \mu_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, & \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{matrix}\right\}$$

Definition 32 (nth Dihedral Group D_n)**.** The *nth dihedral group D_n* is the group of symmetries of the regular n-gon.

Example (Octic Group D_4). Given a square: 

, D_4 is the set of:

$$\left\{\begin{array}{ll} \rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, & \mu_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, & \mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, & \delta_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \\ \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, & \delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}. \end{array}\right\}$$

where ρ_i, μ_i, δ_i represent rotations, mirror images in perpendicular bisectors of sides, and diagonal flips respectively.

Definition 33 (Image of H under f). Let $f\colon A \to B$ be a function and H be a subset of A. The *image of H under f* is the set $\{f(h) \mid h \in H\}$ and is denoted $f[H]$.

Lemma 1. Let G, G' be groups and $\phi\colon G \to G'$ be a one-to-one function such that for all $x, y \in G$, $\phi(xy) = \phi(x)\phi(y)$. Thus $\phi[G]$ is a subgroup of G' and ϕ provides an isomorphism of G with $\phi[G]$.

Proof. We simply prove the subgroup requirements. For any $x', y' \in \phi[G]$, there exist $x, y \in G$ so $\phi(x) = x'$ and $\phi(y) = y'$. By hypothesis, $\phi(xy) = \phi(x)\phi(y)$ so $x'y' \in \phi[G]$ so $\phi[G]$ is closed under the operation of G'. Next, say e' is the identity of G'. Then, $e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e)$. Cancellation in G' shows $e' = \phi(e)$ so $e' \in \phi[G]$. Last, for any $x' \in \phi[G]$, $e' = \phi(e) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = x'\phi(x^{-1})$ implying $x'^{-1} = \phi(x^{-1}) \in \phi[G]$. Thus $\phi[G]$ is a subgroup of G'. We already showed ϕ is onto and therefore an isomorphism of G with $\phi[G]$. $\square$

Theorem 13 (Cayley's Theorem). Every group is isomorphic to a group of permutations.

Proof. Let G be a group. We want to show G is isomorphic to a subgroup of S_G. By the previous lemma, we need only define a universal one-to-one function $\phi\colon G \to S_G$ with the homomorphism property. For any $x, g \in G$, let's define left multiplication by x via $\lambda_x\colon G \to G$ as $\lambda_x(g) = xg$. For all $c \in G$, $\lambda_x(x^{-}1c) = x(x^{-}1c) = c$ so clearly λ_x maps G onto G. Also, for any $a, b \in G$, $\lambda_x(a) = \lambda_x(b) \Rightarrow xa = xb \Rightarrow a = b$ through left cancellation. Thus, λ_x is one-to-one, onto, and a permutation of G. Now, we define $\phi\colon G \to S_G$ as $\phi(x) = \lambda_x$ for all $x \in G$.

To satisfy our lemma, we now only show ϕ is one-to-one and has the homomorphism property. Let e be the identity on G so that $\phi(x) = \phi(y)$ implies $\lambda_x = \lambda_y$ so $\lambda_x(e) = \lambda_y(e) \Rightarrow xe = ye \Rightarrow x = y$. Last, for any $x, y, g \in G$, $\lambda_{xy}(g) = (xy)g = x(yg) = \lambda_x(\lambda_y(g)) = \lambda_x\lambda_y(g)$ so $\phi(xy) = \phi(x)\phi(y)$ satisfying the homomorphism property. □

Definition 34 (Left/Right Regular Representation)**.** The map $\phi\colon G \to S_G$ defined as above is the *left regular represention* of G and the map $\mu\colon G \to S_G$ defined by $\mu(x) = \rho_{x^{-1}}$ where $\rho_x(g) = gx$ for all $x, g \in G$ is the *right regular representation* of G.

2.2 Orbits, Cycles, and the Alternating Groups

Definition 35 (Orbit of a under $\sigma \in S_A$)**.** Let A be a set and $\sigma \in S_A$. For a fixed $a \in A$, the set $\mathcal{O}_{a.\sigma} = \{\sigma^n(a) \mid n \in \mathbb{Z}\}$ is the *orbit of a under σ*.

Remark. Let σ be a permutation of a set A. The equivalence classes in A are determined by the following equivalence class:

$$\text{For } a, b \in A, \text{ let } a \sim b \text{ if and only if } b = \sigma^n(a) \text{ for some } n \in \mathbb{Z}.$$

These are called the *orbits of σ*.

Explanation. $\sim$ is an equivalence relation because it is:

1. **reflexive:** $a \sim a$ clearly because $a = \imath(a) = \sigma^0(a)$.
2. **symmetric:** If $a \sim b$, then $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$ so $a = \sigma^{-n}(b)$ and $-n \in \mathbb{Z}$ so $b \sim a$.
3. **transitive:** If $a \sim b, b \sim c$, then $b = \sigma^n(a)$ and $c = \sigma^m(b)$ for some $n, m \in \mathbb{Z}$. This implies $c = \sigma^m(\sigma^n(a)) = \sigma^{n+m}(a)$ so $a \sim c$.

Example. The orbits of $\imath$ are the singleton subsets of A.

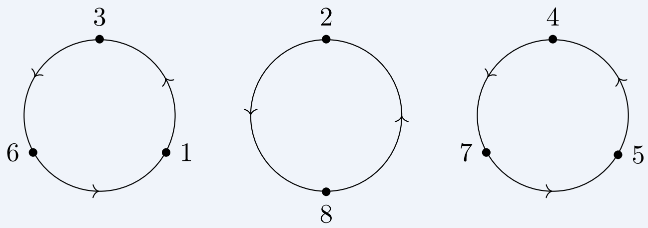
Example. Given the permutation σ of a finite set A defined as:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix},$$

the complete list of orbits of σ are

$$\{1, 3, 6\}, \ \{2, 8\}, \text{ and } \{4, 5, 7\},$$

which we can map in the following way:



Definition 36. A permutation $\sigma \in S_n$ is a *cycle* if it has at most one orbit containing more than one element. The *length* of a cycle is the number of elements in its largest orbit.

Remark. We can use *cyclic notation* to simply denote $\mu = (1, 3, 6)$.

Remark. Cycles are *disjoint*. That is, no interger appears in the notations of 2 different cycles. Note that multiplication of disjoint cycles *is* commutative.

Theorem 14. Every permutation σ of a finte set is a product of disjoint cycles.

Proof. Let $B_1, B_2, \ldots, B_r$ be the orbits of σ and define the cycle μ_i as:

$$\mu_i(x) = \begin{cases} \sigma(x) & x \in B_i \\ x & \text{otherwise.} \end{cases}$$

Clearly, $\sigma = \mu_1\mu_2\cdots\mu_r$. Because the orbits $B_1, B_2, \ldots, B_r$ are disjoint equivalence-classes, the cycles $\mu_1, \mu_2, \ldots, \mu_r$ are disjoint also. $\square$

Example. Take the disjoint cycles $\sigma = (1, 3, 5, 2)$ and $\tau = (2, 5, 6)$. To find $\sigma\tau$ (τ first), begin with 1 so $\sigma\tau = (1, \ldots)$. τ doesn't map 1 but σ maps it to 3 so we get $(1, 3, \ldots)$. Following this cycle, 3 isn't mapped anywhere by τ but is mapped to 5 so $(1, 3, 5, \ldots)$. 5 is mapped to 6 but 6 isn't mapped anywhere so it stays fixed as $(1, 3, 5, 6, \ldots)$. Beginning a new cycle, 2 is mapped to 5 then back to 2 so it becomes (1,3,5,6)(2). Finally, 4 isn't mapped anywhere by either so it stays as 4. Thus, $(1, 3, 5, 2)(2, 5, 6) = (1, 3, 5, 6)(2)(4) = (1, 3, 5, 6)$.

Definition 37 (Transposition)**.** A cycle of length 2 is a *transposition.*

Corollary. Any permutation of a finite set of at least 2 elements is a product of transpositions. The identity, for S_n with $n \geq 2$ is $(1, 2)(1, 2)$.

Theorem 15. No permutation in S_n can be expressed both as a product of an even and odd number of transpositions.

Proof. (Linear Algebra) Recall $S_A \sim S_B$ if A, B have the same cardinality. Permutations work with n rows of the $n \times n$ I_n which has determinant 1. Interchanging any two rows changes the sign of the determinant. If C is a matrix obtained by some permutation σ of I_n and C could be obtained by an even and odd number of transpositions of rows, then its determinant would be both 1 and -1. $\square$

Proof. (Orbits) Let $\sigma \in S_n$ and $\tau = (i, j)$ be a transposition in S_n.

Case I: Suppose the orbits of σ and $\tau\sigma$ differ by 1. Suppose i, j are in different orbits of σ. Writing σ as a product of disjoint cycles with the first containing j and the second containing i, e.g. $(b, j, \times, \times, \times)(a, i, \times, \times)$ implies that $\tau\sigma = (i, j)\sigma = (i, j)(b, j, \times, \times, \times)(a, i, \times, \times)$ after calculating is $(a, j, \times, \times, \times, b, i, \times, \times)$. This is because a feeds into i now j feeds into $\times, \times, \times$ and b feeds into j now i into $\times, \times$. This is now a single orbit.

Case II: Suppose instead that i, j are in the same orbit of σ so σ can be written as the product of disjoint cycles so the first cycle is of form $(a, i, \times, \times, \times, b, j, \times, \times)$. $\tau\sigma = (i, j)\sigma$ gives $(a, j, \times, \times)(b, i, \times, \times, \times)$. This single orbit has been split into two.

These cases show the number of orbits of $\tau\sigma$ differs from the number of orbits of σ by 1. The identity permutation $\imath$ has exactly n orbits becasue each element is the only member of its orbit. So the orbits of a permutation $\sigma \in S_n$ must differ from n by an even or odd number. Each new transposition multiplied with the identity trying to create σ must then change that product's orbits by 1. So, there cannot be 2 sequences of different size because that would imply σ has different numbers of orbits. $\square$

Definition 38. Even/Odd Permutation A permutation of a finite set is known as *even or odd* depending on whether it can be written the product of an even or odd number of transpositions.

Example. The identity permutation $\imath \in S_n$ is even because it is $(1, 2)(1, 2)$.

Theorem 16. If $n \geq 2$, the collection of even permutations of $\{1, 2, 3, \ldots, n\}$ forms a subgroup of order $n!/2$ of the symmetric group S_n. Note the set of odd permutations is of the same size.

Proof. Take the set of even and odd (A_n and B_n) permutations in S_n Let τ be any fixed transposition in S_n. Because $n \geq 2$, we might as well suppose $\tau = (1, 2)$. Take the function $\lambda_\tau \colon A_n \to B_n$ defined as $\lambda_\tau(\sigma) = \tau\sigma$ for $\sigma \in A_n$. σ is even so $(1, 2)\sigma$ can be expressed as an odd number of transpositions so $\tau\sigma \in B_n$. Because S_n is a group, for any $\sigma, \mu \in A_n$, $\lambda_\tau(\sigma) = \lambda_\tau(\mu)$ implies $\sigma = \mu$ so λ_τ is injective. Note also that $\tau = \tau^{-1}$ so if $\rho \in B_n$, then $\tau^{-1}\rho \in A_n$ and $\lambda_\tau(\tau^{-1(\rho)}) = \tau(\tau^{-1}(\rho)) = \rho$ implying λ_τ is onto B_n. So B_n and A_n are of the same size because they are finite. The fact the set of even permutations is a subgroup is trivial. □

Definition 39 (Alternating Group A_n on n Letters)**.** The subgroup S_n consisting of the even permutations of n letters if the *altering group* A_n *on* n *letters*.

2.3 Cosets and the Theorem of Lagrange

Theorem 17. Let H be a subgroup of G. Let the relation $\sim_L$ be defined on G by

$$a \sim_L b \quad \text{if and only if} \quad a^{-1}b \in H.$$

Let $\sim_R$ be defined on G by

$$a \sim_R b \quad \text{if and only if} \quad ab^{-1} \in H.$$

Then $\sim_L, \sim_R$ are both equivalence relations on G.

Proof. (Just $\sim_L$) For any $a \in G$, $a^{-1}(a) = e \in H$ so $\sim_L$ is reflexive. For any $a, b \in G$, suppose $a^{-1}b \in H$. Because this is a subgroup, $(a^{-1}b)^-1 \in H$ so that $b^{-1}a \in H$ and thus $b \sim_L a$ so $\sim_L$ is symmetric. Lastly, if $a \sim_L b, b \sim_L c$ for some $a, b, c \in G$, then $a^{-1}b, b^{-1}c \in H$. By closure $a^{-1}bb^{-1}c = a^{-1}c \in H$ so $a \sim_L c$ implying $\sim_L$ is transitive. Thus, $\sim_L$ is an equivalence relation. □

Definition 40 (Left/Right Cosets)**.** Let H be a subgroup of group G. The subset $aH = \{ah \mid h \in H\}$ of G is the *left coset* of H containing a while the subset $Ha = \{ha \mid h \in H\}$ is the *right coset* of H containing a.

Example. Take the subgroup $3\mathbb{Z}$ of $\mathbb{Z}$. Using additive notation, the left coset of $3\mathbb{Z}$ containing m is $m + 3\mathbb{Z}$. When $m = 0$, $3\mathbb{Z} = \{\cdots, -3, 0, 3, \cdots\}$ so $3\mathbb{Z}$ is itself such a left coset. Similarly, $1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$ are left cosets. Together, these partition $\mathbb{Z}$. Because $\mathbb{Z}$ is abelian, left coset $m + 3\mathbb{Z}$ is the same as right coset $3\mathbb{Z} + m$.

Lemma 2. Take the one-one map $\phi\colon H \to gH$ so $\phi(h) = gh$ for each $h \in H$. This is onto gH by definition. Next, suppose $\phi(h_1) = \phi(h_2)$ for some $h_1, h_2 \in H$. Thus, $gh_1 = gh_2$ so by cancellation in G, $h_1 = h_2$ implying ϕ is bijective. If H is of finite order, then ϕ and a similar function for right cosets have equal numbers of elements to H.

Theorem 18 (Theorem of Lagrange)**.** Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Proof. Let n be the order of G and H have order m. Every coset (left or right) of a subgroup H of a group G has the same number of elements as H, namely m. Let G be partitioned into r left cosets of H so $n = rm$ implying m is a divisor of n. □

Corollary. Every group of prime order is cyclic.

Proof. Let G be of prime order P and $a \in G, a \neq e$. Thus, $\langle a \rangle$ of G has at least 2 elements. But by Lagrange's Theorem, the order $m \geq 2$ of a must divide the prime p implying $m = p$ so $\langle a \rangle = G$ so G is cyclic. □

Definition 41. Let H be a subgroup of a group G. The number of left cosets of H in G is the *index* $(G : H)$ *of* H *in* G. The index may be infinite or finite.

Theorem 19. Suppose H and K are subgroups of a group G so $K \leq H \leq G$ and suppose $(H : K)$ and $(G : H)$ are both finite. Then $(G : K) = (G : H)(H : K)$ is finite.