Abstract Algebra Notes

Cruz Godar

Math 481, 482, and 483/560
Professor Brussel
Cal Poly, Fall 2017–Spring 2018

I — Groups

Definition 1.1: A **group** is a set G equipped with a binary operation such that

1. $ab \in G$ for all $a, b \in G$.
2. $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. There is an $e \in G$ with $ae = ea = a$ for all $a \in G$.
4. For all $a \in G$, there is an $a^{-1} \in G$ with $aa^{-1} = a^{-1}a = e$.

Example: One important type of group is a *symmetry group*, formed by taking the collection S_X of symmetries of a set X — that is, structure-preserving bijections from X to itself. If $X = \mathbb{R}$, for instance, then S_X contains translational symmetries and stretching/shrinking ones.

Definition 1.2: Let $n \in \mathbb{N}$. The **integers modulo n** are the set $\mathbb{Z}_n = \{0, 1, ..., n-1\}$. $\mathbb{Z}_n$ is a group, with the operation given by addition mod n.

Definition 1.3: Let $n \in \mathbb{N}$. The group $\mathbf{U(n)}$ is defined as $U(n) = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$, with the operation given by multiplication mod n.

Definition 1.4: The **dihedral group** of degree n is the the group D_n of symmetries of a regular n-gon, given by $D_n = \{e, r, r^2, ..., r^{n-1}, s, rs, r^2s, ..., r^{n-1}s\}$, where r is a rotation counter-clockwise by $\frac{2\pi}{n}$, s is a reflection over the x-axis, and the operation is function composition. Note that $sr = r^{-1}s$.

Definition 1.5: The **symmetric group** of degree n is the group S_n of permutations on n elements, defined as $\{\sigma : \{1, ..., n\} \twoheadrightarrow \{1, ..., n\}\}$, where each σ is a bijection and the operation is given by function composition. We use **cycle notation** to denote elements of S_n: the element $(124) \in S_4$, for example, denotes the function σ with $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(4) = 1$, and $\sigma(3) = 3$.

Definition 1.6: The **general linear group** of degree n over k is $GL_n(k) = \{A \in M_n(k) \mid \det A \neq 0\}$, with the operation given by matrix multiplication. Typically, k is $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}$.

Definition 1.7: The **special linear group** of degree n over k is $SL_n(k) = \{A \in M_n(k) \mid \det A = 1\}$, with the operation again given by matrix multiplication.

Definition 1.8: The **orthogonal group** of degree n is $O_n = \{A \in M_n(\mathbb{R}) \mid AA^{\mathrm{T}} = I\}$, and the **special orthogonal group** of degree n is $SO_n = \{A \in O_n \mid \det A = 1\}$. The **unitary group**, U_n, and **special unitary group**, SU_n, are defined identically, except their matrices are taken from $M_n(\mathbb{C})$ and require that $A\overline{A}^{\mathrm{T}} = I$.

Definition 1.9: The **order** of a group G is $|G|$. A **finite group** is one that has finite order.

Definition 1.10: A group G is **Abelian** if $ab = ba$ for all $a, b \in G$.

Proposition 1.11: Let G be a group. Then $e \in G$ is unique.

Proof: Suppose there were $e, e' \in G$ such that $ae = ea = ae' = e'a = a$ for all $a \in G$. Then $ee' = e$ and $ee' = e'$, so $e = e'$.

Proposition 1.12: Let G be a group. If $ab = ac$ for $a, b, c \in G$, then $b = c$, and similarly, if $ab = cb$, then $a = c$.

Proposition 1.13: Let G be a group and $a \in G$. Then a^{-1} is unique.

Proof: If there were $a^{-1}, \left(a^{-1}\right)' \in G$ such that $aa^{-1} = a^{-1}a = a\left(a^{-1}\right)' = \left(a^{-1}\right)'a = e$, then $aa^{-1} = a\left(a^{-1}\right)'$, so $a^{-1}aa^{-1} = a^{-1}a\left(a^{-1}\right)'$, and so $a^{-1} = \left(a^{-1}\right)'$.

Definition 1.14: Let G be a group. A set $H \subseteq G$ is a **subgroup** of G, written $H \leq G$, if H is itself a group under G's operation.

Example: For all groups, $\{e\} \leq G$, called the *trivial subgroup*, and $G \leq G$.

Example: If X is a regular, nonoriented n-gon and X' is a regular, oriented n-gon (so reflections count as symmetries of X, but not of X'), then $S'_X \leq S_X$.

Definition 1.15: $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ is a group with its operation given by stretching and rotating the plane — $z = re^{i\theta}$ represents the symmetry of stretching by r and rotating by θ (or equivalently, moving 1 to z). $S^1 = \{e^{i\theta} \mid \theta \in [0, 2\pi)\} = \{z \in \mathbb{C}^* \mid |z| = 1\}$ is also a group under the same operation, so $S^1 \leq C^*$.

Definition 1.16: The **quaternions** are the set

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}, i^2 = j^2 = k^2 = -1, ijk = -1\}.$$

$\mathbb{H}$ forms a group under addition, and $\mathbb{H}^*$ a group under multiplication. Similarly to S^1, we define the **unit 3-sphere** as $S^3 = \{z \in \mathbb{H}^* \mid |z| = 1\} \leq \mathbb{H}^*$.

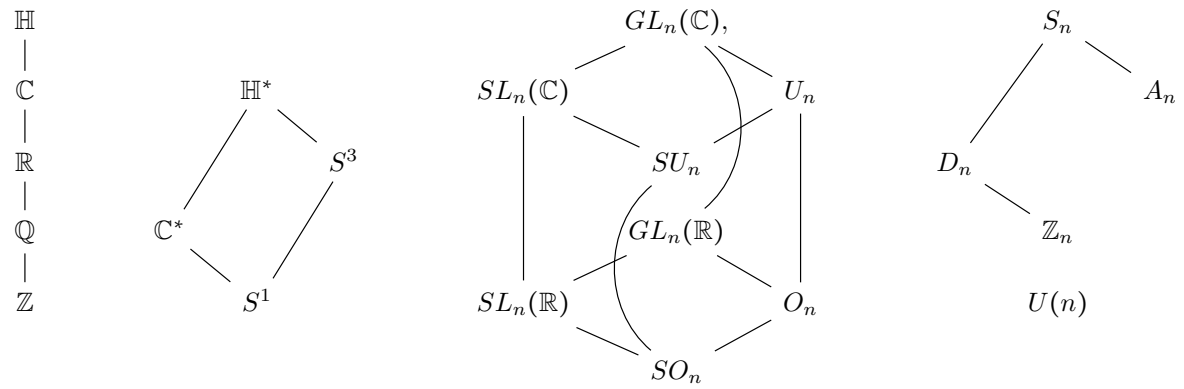
Proposition 1.17: Let G be a group. Then $H \subseteq G$ is a subgroup of G if and only if

1. $H \neq \varnothing$.
2. $ab \in H$ for all $a, b \in H$.
3. For all $a \in H$, $a^{-1} \in H$.

Proof: ($\Rightarrow$) If $H \leq G$, then the only statement to prove is that the identity of H is the same as that of G, so that we can be sure that $a^{-1} \in H$ is the same as a^{-1} in G. If the two identities are e_G and e_H, then $e_H e_G = e_H$ in G and $e_H e_H = e_H$ in H, so $e_H e_G = e_H e_H$ in G, and therefore $e_G = e_H$. Thus the inverses are the same, and so all three conditions are met.

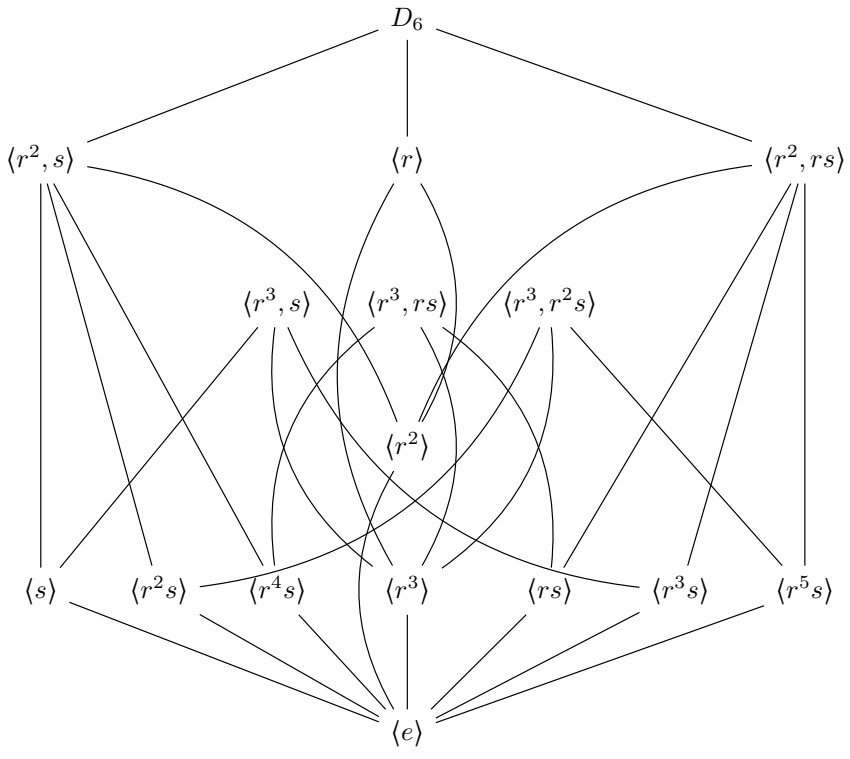
($\Leftarrow$) Let $a, b, c \in H$ (which is valid, since H is nonempty). Then $a, b, c \in G$, so $(ab)c = a(bc)$. Also, since $a^{-1} \in H$ (and this is the inverse from G), $aa^{-1} = e_G \in H$. We already know H is closed under G's operation, so $H \leq G$.

Example: The major groups:



Definition 1.18: Let G be a group and $a \in G$. The **group generated by** $\boldsymbol{a}$ is $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Example: The subgroup lattice of D_6:



Example: In D_n, $\langle r \rangle = \{e, r, r^2, ..., r^{n-1}\}$ and $\langle s \rangle = \{e, s\}$.

Definition 1.19: Let G be a group. The **order** of $a \in G$ is $|a| = |\langle a \rangle|$, or equivalently, the smallest $n \in \mathbb{N}$ such that $a^n = e$ if it exists, or ∞ if it does not.

Definition 1.20: The orders of the elements in $U(9) = \{1, 2, 4, 5, 7, 8\}$ are

$$|1| = 1, \qquad |2| = 6, \qquad |4| = 3, \qquad |5| = 6, \qquad |7| = 3, \qquad |8| = 2.$$

Proposition 1.21: Let G be a group and $a \in G$. Then $|a| = \left|a^{-1}\right|$.

Proof: Since $a^k = e$ if and only if $\left(a^k\right)^{-1} = e$, if and only if $\left(a^{-1}\right)^k = e$, the smallest $n \in \mathbb{N}$ such that $a^n = e$ will also be the smallest $m \in \mathbb{N}$ such that $\left(a^{-1}\right)^m = e$. Thus $|a| = \left|a^{-1}\right|$.

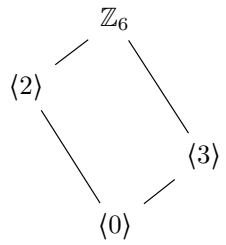
Definition 1.22: A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$, called a **generator** of G.

Theorem 1.23: A subgroup of a cyclic group is cyclic.

Proof: Let $G = \langle a \rangle$ and $H \leq G$. Then for all $h \in H$, $h = a^m$ for some $m \in \mathbb{Z}$. Let $S = \{m \in \mathbb{N} \mid a^m \in H\}$, let m_0 be the minimum element of S, and let $h = a^m \in H$ be arbitrary. Then $m = m_0 q + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < m_0$, so $a^m = a^{m_0 q + r}$, or equivalently, $a^r = a^{m - m_0 q}$. Since $a^m = h \in H$ and $a^{m_0 q} = (a^{m_0})^q \in H$, $a^{m - m_0 q} = a^r \in H$. Thus if $r \neq 0$, $r \in S$ by definition, but $r < m_0$, the smallest element in S. ↯ Thus $r = 0$, and so $h = (a^{m_0})^q$ for some $q \in \mathbb{Z}$. Since h was arbitrary, $H = \langle a^{m_0} \rangle$.

Example: Since $\mathbb{Z}$ is cyclic, every subgroup of $\mathbb{Z}$ is of the form $\langle a \rangle$ for $a \in \mathbb{Z}$.

Example: The subgroups of $\mathbb{Z}_6$ are $\langle 0 \rangle$, $\langle 3 \rangle$, $\langle 2 \rangle$, and $\langle 1 \rangle = \mathbb{Z}_6$.



Theorem 1.24: Let $G = \langle a \rangle$ be cyclic with $|G| = n$. Then for any $k \in \mathbb{N}$, $\left|a^k\right| = \frac{n}{\gcd(n,k)}$.

Proof: Let $d = \gcd(n,k)$. We claim $\langle a^k \rangle = \langle a^d \rangle$.

($\subseteq$) Since $d|k$, $k = dq$ for some $q \in \mathbb{Z}$. Then $a^k = \left(a^d\right)^q \in \langle a^d \rangle$, so $\langle a^k \rangle \subseteq \langle a^d \rangle$.

($\supseteq$) By Bezout's identity, $d = ks + nt$ for some $s,t \in \mathbb{Z}$, so $a^d = a^{ks+nt} = \left(a^k\right)^s (a^n)^t = \left(a^k\right)^s (e)^t = \left(a^k\right)^s \in \langle a^k \rangle$. Thus $\langle a^d \rangle \subseteq \langle a^k \rangle$.

Now $\langle a^k \rangle = \langle a^d \rangle$, so in particular, $\left|a^k\right| = \left|a^d\right|$. We know $\left|a^d\right| = \frac{n}{d}$, since otherwise, if $\left|a^d\right| = m < \frac{n}{d}$, $a^{dm} = e$ amd $dm < n$, so $|G| = |a| < n$. ↯ Thus $\left|a^k\right| = \left|a^d\right| = \frac{n}{d}$.

Corollary 1.24.1: Let $G = \langle a \rangle$ with $|G| = n$. Then the generators of G are a^k with $\gcd(k,n) = 1$.

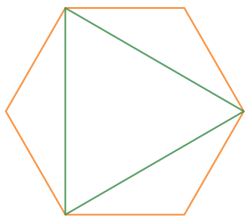
Proposition 1.25: Let G be a cyclic group and $a \in G$ such that $G \neq \langle a \rangle$. Then no element of $\langle a \rangle$ is a generator for G.

Proof: Suppose $|G| = n$. Since $\langle a \rangle \neq G$, $|a| < |G|$. Now every element of $\langle a \rangle$ is of the form a^k for some $k \in \mathbb{Z}$, and $\left|a^k\right| = \frac{|a|}{\gcd(k,|a|)} \leq |a| < |G|$, so no element of $\langle a \rangle$ is a generator for G.

Definition 1.26: Two groups G and H are **isomorphic** if there is a bijection $\varphi : G \longrightarrow H$ such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a,b \in G$. φ is called an **isomorphism**, and we write $G \simeq H$.

Example: $\mathbb{Z}_4 \simeq \langle i \rangle \leq \mathbb{C}^*$, since the map $\varphi : \mathbb{Z}_4 \longrightarrow \measuredangle i \rangle$ given by $\varphi(a) = i^a$ is an isomorphism.

Example: Let $H = \{x \in D_6 \mid x \text{ preserves an inscribed triangle}\} \leq D_6$. Then $H \simeq D_3$.



Proposition 1.27: Isomorphisms preserve identities, inverses, subgroups, and order (both of elements and groups).

II — The Symmetric Group

Definition 2.1: A ***k*-cycle** is an element of S_n of the form $(a_1 \cdots a_k)$.

Definition 2.2: A **transposition** is a 2-cycle.

Proposition 2.3: Every element of S_n can be expressed as a product of disjoint cycles.

Example: To remove duplicate numbers, start with 1 and pass it through the permutation, then pass the result through, and so on. Since every permutation is a bijection by definition, every number will be sent to a unique other. Once the permutation results in 1 again, close the cycle and continue with the next lowest unused number. For instance, if $\sigma = (124)(314)$, $\sigma(1) = 1$, so we start again with 2: $\sigma(2) = 4$. Then $\sigma(4) = 3$, and $\sigma(3) = 2$, so the permutation is (243).

Proposition 2.4: Disjoint cycles commute.

Proposition 2.5: Every element of S_n can be expressed as a product of transpositions.

Proof: For an arbitrary $\sigma \in S_n$, express σ as a product of disjoint cycles. Then for an individual cycle $(a_1 \cdots a_k)$, $(a_1 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_3)(a_1 a_2)$.

Definition 2.6: Let $\pi \in S_n$. The **permutation matrix** for π is P_π, defined by $(P_\pi)_{ij} = 1$ if $\pi(j) = i$ and 0 if not.

Example: For $\pi = (243) \in S_4$,

$$P_\pi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Proposition 2.7: All permutation matrices are orthogonal (that is, the columns form an orthonormal basis for $\mathbb{R}^n$, so $\det P_\pi = \pm 1$).

Definition 2.8: A permutation $\pi \in S_n$ is **even** if $\det P_\pi = 1$, and **odd** if $\det P_\pi = -1$.

Definition 2.9: The **alternating group** of degree n is $A_n = \{\pi \in S_n \mid \pi \text{ is even}\} \leq S_n$.

Proposition 2.10: For $n \geq 2$, $|A_n| = \frac{n!}{2}$.

Proof: Define $f : A_n \longrightarrow S_n \setminus A_n$ by $f(\pi) = (12)\pi$. Then $f^{-1}(\pi) = (12)\pi$, so f is invertible. Thus $|A_n| = |S_n \setminus A_n|$, so $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Theorem 2.11: Let $\pi \in S_n$. Then $\pi \in A_n$ if and only if π can be expressed as the product of evenly many transpositions. Moreover, when π is expressed in such a way, there are always the same number of transpositions (mod 2).

Proof: Suppose $\pi = \tau_1 \cdots \tau_k$, where each τ_i is a transposition. Then $P_\pi = P_{\tau_1} \cdots P_{\tau_k}$. Since P_{τ_i} has exactly 2 columns permuted from I_n, $\det P_{\tau_i} = -1$, so $\det P_\pi = (-1)^k$. Thus π is even if and only if k is even, proving both claims.

Theorem 2.12: Let $n \geq 3$. Then A_n is generated by 3-cycles.

Proof: Let $\pi \in A_n$. Then π is the product of evenly many transpositions. Group them in pairs, and consider an arbitrary pair, say $(ab)(cd)$.

If (ab) and (cd) have no common entries, then $(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$ (which is valid, since $b \neq c$ by assumption).

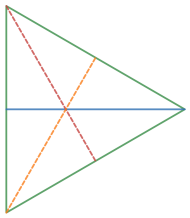
If (ab) and (cd) have one entry in common, then without loss of generality, $(cd) = (bd)$. Then $(ab)(cd) = (ab)(bd) = (abd)$.

Finally, if (ab) and (cd) share two entries, they are identical, so $(ab)(cd) = e$. Thus each pair is expressible as either one or two 3-cycles or the identity, and since we can omit the identities, π is the product of 3-cycles.

III — Cosets and Lagrange's Theorem

Definition 3.1: Let G be a group, $H \leq G$, and $a \in G$. The **left coset** of H in G with representative a is the set $aH = \{ah \mid h \in H\}$, and right cosets are defined similarly.

Example: Let $H = \langle r \rangle \leq D_3$. Then $eH = rH = r^2H = \{e, r, r^2\}$ and $sH = rsH = r^2sH = \{s, rs, r^2s\}$. If $K = \langle s \rangle$, then $eK = sK = \{e, s\}$, $rK = rsK = \{r, rs\}$, and $r^2sK = \{r^2, r^2s\}$.



Here, K fixes the solid blue line, rK moves it to the red dashed line, and r^2K to the yellow dashed line. The red and yellow lines are called **conjugate substructures** to the blue line. Conjugate substructures can be found by applying every element of a group — or just those that generate distinct cosets — to the original substructure.

Example: The cosets of $S^1 \leq \mathbb{C}^*$ are all the concentric circles around the origin.

Comment: In general, left cosets are more important than right ones, since function composition operates right-to-left.

Proposition 3.2: Let G be a group and $H \leq G$. Then the following are equivalent:

1. $aH = bH$.
2. $b \in aH$.
3. $b^{-}1a \in H$.

Definition 3.3: Let G be a group and $H \leq G$. The **index** of H in G is $[G : H] = |\{aH \mid a \in G\}|$.

Theorem 3.4: (Lagrange) Let G be a group and $H \leq G$. Then the set of left cosets $\{aH \mid a \in G\}$ partitions G into subsets of equal cardinality.

Proof: For all $b \in G$, $b \in bH$, so $G \subseteq \bigcup aH$. And clearly $\bigcup aH \subseteq G$, so $G = \bigcup aH$. Now we claim $aH \cap bH$ is either aH or $\varnothing$ for all $a, b \in G$. Suppose $aH \cap bH \neq \varnothing$. Then there is a $c \in aH \cap bH$, so by the previous result, $cH = aH$ and $cH = bH$, and therefore $aH = bH$. Thus G is the disjoint union of the cosets of H, so they are a partition.

To show that all cosets have the same cardinality, define a function $f : aH \longrightarrow H$ by $f(ah) = h$. Then f is a bijection, so $|aH| = |H|$.

Corollary 3.4.1: Let G be a group and $H \leq G$. Then $|G| = [G : H]|H|$.

Proof: Since $G = \bigsqcup aH$, $|G| = \sum |aH| = \sum |H| = \sum_{k=1}^{[G:H]} |H| = [G : H]|H|$.

Corollary 3.4.2: Let G be a finite group and let $H \leq G$. Then $|H| \mid |G|$.

Corollary 3.4.3: Let G be a finite group and let $a \in G$. Then $|a| \mid |G|$.

Corollary 3.4.4: Let G be a finite group and let $a \in G$. Then $a^{|G|} = e$.

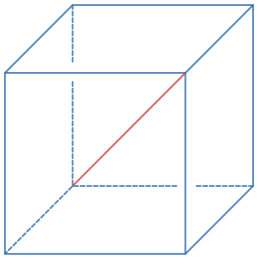
Corollary 3.4.5: Let $a, n \in \mathbb{N}$ with $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof: With $G = U(n)$, $|G| = |\{a \in \mathbb{N} \mid a < n, \gcd(a, n) = 1\}| = \varphi(n)$, so $a^{|G|} = a^{\varphi(n)} = 1$.

Corollary 3.4.6: Let $a \in \mathbb{N}$ and p prime. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Example: Find the order of the group of orientation-preserving symmetries of a regular cube.

Let G be this group and let $H \leq G$ be the subgroup fixing the red line.



There are six elements of G that fix the red line (pick one of the two vertices on the line to face up — then there are three symmetries that permute the three vertices adjacent to it, making six in total).

And there are four conjugate substructures of the line, so there are four distinct cosets of H. Thus $[G : H] = 4$, and therefore $|G| = [G : H]|H| = 24$.

Theorem 3.5: There is only one cyclic group of each finite order, and only one of any infinite order, up to isomorphism.

Proof: Let G be cyclic with $|G| = n$. Then $G = \langle a \rangle$ for some $a \in G$, so the map $\varphi : G \longrightarrow \mathbb{Z}_n$ given by $a^k \longmapsto k \cdot 1$ is an isomorphism.

If G is infinite, then G must be countable, since it can be written as $\{e, a, a^2, ...\}$. Then there is an isomorphism given by $a^k \longmapsto k \cdot 1$. Not that it is *not* sufficient to claim that $G \simeq \mathbb{Z}$ since G is countable — that definition requires only a bijection, which need not be multiplicative.

Proposition 3.6: Let $\varphi : G \longrightarrow G'$ be an isomorphism. Then

1. $|G| = |G'|$.
2. $\varphi(e_G) = e_{G'}$.
3. $\varphi(a^{-1}) = \varphi(a)^{-1}$.
4. $|\varphi(a)| = |a|$.
5. If $H \leq G$, then $\varphi(H) \leq \varphi(G) = G'$.
6. If G is Abelian, then so is G'.

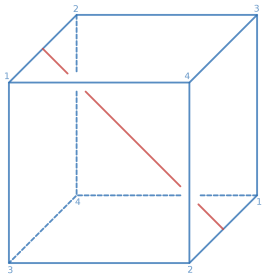
Theorem 3.7: (Cayley) Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.

Proof: Let $a \in G$ and define $\lambda_a : G \longrightarrow G$ by $\lambda_a(b) = ab$. Then if we number the elements of G from 1 to n, $\lambda_a \in S_n$. Let $G' = \{\lambda_a \in S_n \mid a \in G\}$. We claim $G \simeq G'$, where the isomorphism is given by $\lambda(a) = \lambda_a$.

Clearly, λ is onto, since $G' = \lambda(G)$ by definition. To show that λ is injective, suppose $\lambda(a) = \lambda(b)$. Then $\lambda_a = \lambda_b$, so in particular, $\lambda_a(e) = \lambda_b(e)$. Thus $a = b$. Finally, λ is multiplicative, since $\lambda(ab) = \lambda_{ab} = \lambda_a\lambda_b = \lambda(a)\lambda(b)$. Thus λ is an isomorphism, so $G \simeq G' \leq S_n$.

Example: Determine the rotation group of the cube.

Let the group be G. By our previous work, we know $|G| = 24$, and by Cayley's Theorem, we know $G \leq S_6$. But $|S_6| = 720$, and there are far too many order-24 subgroups of S_6 to determine the correct one (or even easily make a complete list). Instead, fix the four diagonals from the previous example and number the vertices 1–4 by which line they are contained in. Then each element of G must fix one of the four diagonals by the previous example, so $G \leq S_4$.



Now each rotation about one of the four diagonal axes fixes one number and permutes the other three, so it is a 3-cycle. Since we have all 8 possible 3-cycles from this method, G contains A_4. Draw a new line that connects the midpoints of the edges with endpoints 1 and 2 (shown in the above figure). A rotation about this axis fixes 3 and 4 and permutes 1 and 2, so $(12) \in G$. Thus $|G| \geq |A_4| + 1 = 13$, since $(12) \notin A_4$, and since $|G| \mid |S_4| = 24$, $|G| = 24$. Thus $G = S_4$.

Since we can form a regular octahedron by replacing each face of the cube with a vertex and each vertex with a face (that is, the cube and octahedron are *dual*), the rotation group of the octahedron is also S_4.

Definition 3.8: Let G be a group. An **automorphism** of G is an isomorphism from G to itself. Notice that every automorphism is completely determined by where it sends the generators of G, since $\varphi(a_1^{k_1} \cdots a_n^{k_n}) = \varphi(a_1)^{k_1} \cdots \varphi(a_n)^{k_n}$.

Definition 3.9: Let G be a group. The **automorphism group** of G is the group of automorphisms of G, denoted Aut G.

Example: Aut $\mathbb{Z} = \{e, \varphi\}$, where $e : 1 \longmapsto 1$ and $\varphi : 1 \longmapsto -1$. Thus Aut $\mathbb{Z} \simeq \mathbb{Z}_2$.

Proposition 3.10: For any group G, and $a \in G$, $\gamma_a : G \longrightarrow G$ defined by $\gamma_a(b) = aba^{-1}$ is an automorphism.

Definition 3.11: Let G be group. The **inner automorphism group** of G is Inn $G = \{\gamma_a \mid a \in G\}$.

Definition 3.12: Let G and G' be groups. The **direct product** of G and G' is $G \times G' = \{(a, a') \mid a \in G, a' \in G'\}$, where $(a, a')(b, b') = (ab, a'b')$.

Proposition 3.13: Let G and G' be groups. Then $G \times G'$ is a group, and $|G \times G'| = |G||G'|$.

Proposition 3.14: Let G and G' be groups and let $(a, a') \in G \times G'$. Then $|(a, a')| = \text{lcm}(|a|, |a'|)$.

Corollary 3.14.1: $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.

Definition 3.15: A group G is an **internal direct product** if there are two subgroups $H, K \leq G$ such that $HK = \{hk \mid h \in H, k \in K\} = G$, $H \cap K = \{e\}$, and $hk = kh$ for all $h \in H$ and $k \in K$. If this is the case, $G \simeq H \times K$.

Example: $D_6 = \langle r^2, s \rangle \langle r^3 \rangle$.

Proposition 3.16: Isomorphism is an equivalence relation.

Proposition 3.17: Let G and G' be groups. Then $G \times G' \simeq G' \times G$.

Proposition 3.18: If $H \simeq H'$ and $K \simeq K'$, then $H \times K \simeq H' \times K'$.

Definition 3.19: Let G be a group. Two elements $b, c \in G$ are **conjugate** if $b = aca^{-1}$ for some $a \in G$.

Definition 3.20: Let G be a group. Two subgroups $H, K \leq G$ are **conjugate** if $H = aKa^{-1}$ for some $a \in G$.

Proposition 3.21: Conjugacy is an equivalence relation.

Proof: Let G be a group. Then for all $b \in G$, $b = ebe^{-1}$, so conjugation is reflexive. If $c = aba^{-1}$, then $b = \left(a^{-1}\right) c \left(a^{-1}\right)^{-1}$, so it is symmetric, and if $c = aba^{-1}$ and $d = a'c\left(a'\right)^{-1}$, then $d = \left(a'a\right) b \left(a'a\right)^{-1}$, so it is transitive.

Proposition 3.22: Let G be a group, $a, b \in G$, and $H \leq G$. Then $|b| = \left|aba^{-1}\right|$ and $H \simeq aHa^{-1}$.

Theorem 3.23: (The Amazing Conjugation Trick) Let $\sigma, \tau \in S_n$ with $\tau = (\tau_1 \cdots \tau_k)$. Then $\sigma\tau\sigma^{-1} = (\sigma(\tau_1) \cdots \sigma(\tau_k))$.

Proof: Let $a \in \{1, ..., n\}$. If $a \in \{\sigma(\tau_1), ..., \sigma(\tau_k)\}$, then $a = \sigma(\tau_i)$ for some i, so $(\sigma(\tau_1)\cdots\sigma(\tau_k))a = \sigma(\tau_{i+1})$ (or $\sigma(\tau_1)$ if $i = k$). But $\sigma\tau\sigma^{-1}(a) = \sigma\tau(\tau_i) = \sigma(\tau_{i+1})$ (or, again, $\sigma(\tau_1)$ if $i = k$). If $a \notin \{\sigma(\tau_1), ..., \sigma(\tau_k)\}$, then $(\sigma(\tau_1)\cdots\sigma(\tau_k))a = a$. And $\sigma^{-1}(a) \notin \{\tau_1, ..., \tau_n\}$, so $\sigma\tau(\sigma^{-1}(a)) = \sigma(\sigma^{-1}(a)) = a$ too. Thus $\sigma\tau\sigma^{-1} = (\sigma(\tau_1)\cdots\sigma(\tau_k))$.