Fields and Galois Theory (part 3): Groups (by Evan Dummit, 2020, v. 2.00)

Contents

3 Groups

The set of symmetries of a geometric or algebraic object carries a natural structure under composition. This composition operation is associative (since function composition is associative), there is always an identity element (namely, the identity symmetry that leaves the object unchanged), and every element has an inverse (namely, the "inverse" symmetry that reverses everything). To study the collection of symmetries, therefore, is essentially the same as studying algebraic structures with a single operation that satisfy these three properties: namely, groups. Our goal in this chapter is to give an overview of groups and basic group theory, with the ultimate goal of describing (in the next chapter) how to use groups to study the structure of fields and field extensions; as such, we will focus on understanding elementary properties of finite groups and only survey a portion of some of the deeper results.

3.1 Examples and Basic Properties of Groups

- We have already discussed rings, which yield a large class of examples of groups. Here is the formal definition of a group:
- Definition: A group is any set G having a (closed) binary operation $\star$ that satisfies the three axioms [G1]-[G3]:

  [G1] The operation $\star$ is associative: $g \star (h \cdot k) = (g \star h) \star k$ for any elements g, h, k in G.

  [G2] There is a (two-sided) identity element e: $e \star g = g = g \star e$ for any element g in G.

  [G3] Every element has a (two-sided) inverse: for any g in G, there exists g^{-1} in G with $g \star g^{-1} = e = g^{-1} \star g$.

- Like with rings, certain groups will also possess additional properties. However, due to the comparatively minimal structure imposed by the axioms for a group, there is only one term that we will introduce now:
- Definition: If a group satisfies axiom [G4], we say it is an abelian group[1].

  [G4] The operation $\star$ is commutative: $g \star h = h \star g$ for any elements g, h in G.

- There are a number of common conventions regarding group notation.
  - We will frequently omit the symbol for the group operation $\star$ and simply write gh for $g \star h$. We will also often write the operation as $\cdot$ or $+$ when it represents multiplication or addition in a ring, and write 1 or 0 for the corresponding identity elements respectively.
  - Because the group operation is associative, we do not need to specify the order in which the multiplications are performed when we have more than 2 terms, and can simply write expressions like ghk without needing to use parentheses to distinguish between $(gh)k$ and $g(hk)$.[2]
  - If $g \in G$, for any positive integer n we define $g^n = \underbrace{g \star g \star \cdots \star g}_{n \text{ terms}}$, $g^{-n} = \underbrace{g^{-1} \star g^{-1} \star \cdots \star g^{-1}}_{n \text{ terms}}$, and $g^0 = e$.
  - In an abelian group, we often write the group operation "additively" using the addition symbol $(+)$, denote the identity element as 0, and denote additive inverses with minus signs $(-)$.
  - Thus (for example) in an additive abelian group we would define $ng = \underbrace{g + g + \cdots + g}_{n \text{ terms}}$ for $n > 0$.
- Definition: If G is a group, the order of G, denoted as $|G|$ or $\#G$, is the cardinality of G as a set.
- Like with rings, we can deduce a few properties of group arithmetic immediately from the axioms:
- Proposition (Basic Arithmetic): Let G be a group. The following properties hold in G:
  1. The identity element e is unique, and $e^{-1} = e$.
     - Proof: For (1), if there were two identity elements e and e', then $e' = e \cdot e' = e$ by the left-identity property of e and the right-identity property of e'. The second statement follows immediately by observing that $ee = e$.
  2. G has left and right cancellation: for any g, h, k in G, either of $gh = gk$ or $hg = kg$ implies $h = k$.
     - Proof: If $gh = gk$ then $h = eh = (g^{-1}g)h = g^{-1}(gh) = g^{-1}(gk) = (g^{-1}g)k = ek = k$. The other statement follows similarly.
  3. Inverses are unique. Also, a one-sided inverse of g is automatically a two-sided inverse of g.
     - Proof: If h and k are both inverses of g, then $gh = e = gk$, so by cancellation we see $h = k$.
     - The second statement follows by observing that $gh = e$ implies $h = eh = (g^{-1}g)h = g^{-1}(gh) = g^{-1}e = g^{-1}$, and likewise $hg = e$ also implies $h = g^{-1}$.

[1] Less commonly, abelian groups are also called commutative groups. A group that is not abelian is called non-abelian. The term "abelian" is named after Neils Henrik Abel, who was a foundational figure in the study of groups; it is stylized in lowercase (rather than in uppercase as "Abelian") in honor of the depth of his contribution.

[2] Technically, this statement requires a proof; it is straightforward though tedious to use induction on the number of terms in the product to establish that all such products are equal to the one where the order is composed left-to-right, as in $((gh)k)l$.

4. For any $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$, and $(g^{-1})^{-1} = g$.
   - Proof: We have $(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e$ and likewise for the product in the other order.
   - For the second statement observe that $(g^{-1})^{-1}g^{-1} = e = gg^{-1}$, and then cancelling g^{-1} yields $(g^{-1})^{-1} = g$.
5. For any $g \in G$ and any integers m, n, we have $g^{m+n} = g^m g^n$, $g^{mn} = (g^m)^n$, and $(g^n)^{-1} = g^{-n}$.
   - Proof: If m and n are both nonnegative then $g^{m+n} = \underbrace{g \cdot g \cdot \dots \cdot g}_{m+n \text{ terms}} = (\underbrace{g \cdot g \cdot \dots \cdot g}_{m \text{ terms}}) \cdot (\underbrace{g \cdot g \cdot \dots \cdot g}_{n \text{ terms}}) = g^m g^n$ and $g^{mn} = \underbrace{g \cdot g \cdot \dots \cdot g}_{mn \text{ terms}} = \underbrace{g^m \cdot g^m \cdot \dots \cdot g^m}_{n \text{ terms}} = (g^m)^n$. The other cases (e.g., m nonnegative, n negative) follow in the same way.
   - The last statement follows by observing that $(\underbrace{g \cdot g \cdot \dots \cdot g}_{n \text{ terms}}) \cdot (\underbrace{g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}}_{n \text{ terms}}) = e$ by repeatedly cancelling in the middle.

3.1.1 Basic Examples of Groups

- Here are some basic examples (and non-examples) of groups:
- Example (Additive Groups): Any ring R forms an abelian group under its addition operation $+$, as follows immediately from the ring axioms.
  - Thus for example, $(\mathbb{Z}, +)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, $(F[x], +)$, and $(M_{n\times n}(F), +)$ are all groups. The identity element is 0, and inverses are simply additive inverses.
- Example (Vector Spaces): If F is a field and V is an F-vector space, then $(V, +)$ is an abelian group, as follows immediately from the vector space axioms.
- Example (Multiplicative Groups): If R is any ring with 1, then the collection of units in R, denoted $R^\times$, forms a group under multiplication $\cdot$.
  - Explicitly, this follows because multiplication is associative, the multiplicative identity 1 is a unit, and the product and multiplicative inverse of units are units. If R is commutative, then $(R^\times, \cdot)$ is an abelian group.
  - Thus for example, $(\mathbb{Z}/m\mathbb{Z})^\times$, the collection of residue classes in $\mathbb{Z}/m\mathbb{Z}$ relatively prime to m, forms an abelian group under multiplication.
- Example (Matrix Groups): The set $GL_n(F)$ of invertible $n \times n$ matrices with entries in the field F, forms a group under multiplication.
  - This is a special case of the previous example, since $GL_n(F)$ is the collection of units in the ring $M_{n\times n}(F)$ of $n \times n$ matrices with entries in F. When $n \geq 2$ this group is non-abelian.
  - If $F = \mathbb{F}_q$ is a finite field, we can compute the order of this group by observing that an $n \times n$ matrix is invertible precisely when its rows are linearly independent.
  - There are $q^n - 1$ possible choices for the first row (any nonzero vector). Once we have chosen the first k rows, the $(k+1)$st row must be linearly independent from the subspace spanned by the first k rows, which by assumption has dimension k: thus, there are $q^n - q^k$ possible choices for the $(k+1)$st row. This holds for each row, so we see that the total number of elements in $GL_n(F)$ is $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$.
- Example: The set $G = \{e\}$, with operation $e \cdot e = e$, is a group called the trivial group.
- Non-Example: The integers do not form a group under multiplication, because 0 has no multiplicative inverse.
  - More generally, no ring (except the trivial ring) will form a group under multiplication, since 0 cannot have a multiplicative inverse in any ring where $1 \neq 0$.

- Example (Klein 4-Group): The set $V_4 = \{e, a, b, c\}$ with identity e, and other multiplications given by $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $ac = ca = b$, and $bc = cb = a$, forms a group. This group is called the Klein 4-group (in German, "Viergruppe"), and is an abelian group of order 4.
  - It is straightforward (although tedious) to verify that multiplication is associative. In this group, every element is its own inverse.
- Example (Group of nth Roots of Unity): For any positive integer n, if $\zeta_n = e^{2\pi i/n}$, then the set $G = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}$ forms a group under multiplication.
  - Explicitly: associativity is inherited from $\mathbb{C}$, the identity element is 1, and $(\zeta_n^k)^{-1} = \zeta_n^{n-k}$ for any $0 \le k \le n-1$.
  - This group consists of the solutions to the equation $x^n - 1 = 0$ in $\mathbb{C}$, which are called the nth roots of unity.
  - For example, when $n = 4$, we obtain the multiplicative group $G = \{1, i, -1, -i\}$.
- Example (Quaternion Group): The set $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ forms a group under the multiplication relations $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $ki = -ik = j$, and $jk = -kj = i$. This group is called the quaternion group, and is a non-abelian group of order 8.
  - It is straightforward (although tedious) to verify that the multiplication is associative, and clearly 1 is an identity element.
  - Furthermore, 1 and -1 are their own multiplicative inverses, while the inverses of i, j, k are $-i, -j, -k$ respectively.
- We can also construct new groups using Cartesian products.
  - Recall that if S and T are sets, the Cartesian product $S \times T$ is the set of ordered pairs (s, t) where $s \in S$ and $t \in T$.
- Proposition (Cartesian Products of Groups): If $(G, \star)$ and $(H, \circ)$ are groups, then the Cartesian product $G \times H$ is also a group, with operation performed componentwise: $(g_1, h_1) \triangle (g_2, h_2) = (g_1 \star g_2, h_1 \circ h_2)$. The identity element is $e_{G \times H} = (e_G, e_H)$ and inverses are given by $(g, h)^{-1} = (g^{-1}, h^{-1})$. The group $G \times H$ has order $|G| \cdot |H|$, and is abelian if and only if both G and H are abelian.
  - Proof: Each of the group axioms for $G \times H$ follows immediately from the corresponding axioms in G and H, and the statement about the order follows from the definition of Cartesian product for sets.
  - For the abelian condition, clearly $(g_1, h_1) \triangle (g_2, h_2) = (g_1 \star g_2, h_1 \circ h_2)$ is equal to $(g_2, h_2) \triangle (g_1, h_1) = (g_2 \star g_1, h_2 \circ h_1)$ for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$ if and only if $g_1 \star g_2 = g_2 \star g_1$ and $h_1 \circ h_2 = h_2 \circ h_1$ for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$.
- Example: The Cartesian product $Q_8 \times (\mathbb{Z}/5\mathbb{Z})$ is a non-abelian group of order $8 \cdot 5 = 40$.

3.1.2 Dihedral Groups

- As we briefly outlined, groups arise naturally from studying symmetries of objects. Among the simplest objects in geometry are regular n-gons, whose associated symmetry group is called the dihedral group, and denoted[3] $D_{2 \cdot n}$.
  - Geometrically, these symmetries are the possible ways to move an n-gon around in space (rotating or reflecting it) and then placing it back on top of itself so that all of the vertices and edges line up.
  - For example, for $n = 4$ (corresponding to the symmetries of a square), one possibility is to rotate the square $\pi/2$ radians counterclockwise in the plane around its center. Another possibility is to reflect the square about one of its diagonals (in fact there are two such maps).

[3] Many authors denote the symmetry group of the n-gon as D_n (emphasizing the geometric flavor of the group), but in group theory literature the notation D_{2n} (emphasizing the elements of the group) is more common. We adopt the notation $D_{2 \cdot n}$ as a sort of compromise between these two.

- If we label the vertices of the n-gon $1, 2, \dots, n$, then we can identify all of these symmetries by their corresponding permutations of the vertices.
  - For example, if we label the vertices of the square as $1, 2, 3, 4$ counterclockwise, then a counterclockwise rotation of $\pi/2$ radians would correspond to the permutation σ with $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 4$, and $\sigma(4) = 1$.
  - The collection of symmetries $D_{2 \cdot n}$ of the regular n-gon can then be made into a group as follows: if g and h are both elements of $D_{2 \cdot n}$, we define the composition $g \cdot h$ to be the symmetry obtained by first applying h, and then g (i.e., by function composition).
  - This operation is associative since function composition is associative, the identity element is the identity transformation (i.e., the symmetry leaving all vertices fixed), and the inverse of a symmetry g is the symmetry g^{-1} that reverses all of the rigid motions of g.
- Proposition (Order of $D_{2 \cdot n}$): For any integer $n \geq 3$, the dihedral group $D_{2 \cdot n}$ has order $2n$.
  - Proof: Under a symmetry, the vertex labeled 1 can be moved to any of the n vertices, and then the vertex labeled 2 must go to one of the 2 vertices adjacent to it. But once we have fixed the locations of vertices 1 and 2, then all of the other vertices' locations are determined uniquely (since vertex 3 must go to the unique vertex adjacent to the new position of vertex 2 that is not already occupied by vertex 1, and so forth).
  - Thus there are at most $2n$ possible symmetries of a regular n-gon, so $|D_{2 \cdot n}| \leq 2n$.
  - On the other hand, we can explicitly list $2n$ distinct symmetries: there are the n possible rotations counterclockwise about the center by $2\pi k/n$ radians for $0 \leq k \leq n-1$, and there are also n possible reflections about a line through the center of the n-gon.
  - Explicitly: if n is odd, these are the n lines passing through one vertex and the center, while if n is even there are $n/2$ lines passing through a pair of opposite vertices and $n/2$ others that bisect a pair of opposite sides.
  - Each of these symmetries is different, so $D_{2 \cdot n}$ has order $2n$ as claimed.
- We can give a more concrete description of the elements in $D_{2 \cdot n}$ in terms of particular rotations and reflections.
  - Explicitly, let r represent the counterclockwise rotation of the n-gon by $2\pi/n$ radians: as a permutation, we have $r(1) = 2$, $r(2) = 3$, ... , $r(n-1) = n$, and $r(n) = 1$. Then r^k represents a counterclockwise rotation by $2\pi k/n$ radians, so the elements $\{e, r, r^2, \dots, r^{n-1}\}$ are distinct, and $r^n = e$.
  - Also, let s represent the reflection of the n-gon across the line through vertex 1 and the center of the n-gon. As a permutation, we have $s(1) = 1$, $s(2) = n$, $s(3) = n-1$, ... , and $s(n) = 2$. It is then easy to see that s^2 is the identity element, and that $s \neq r^i$ for any i, since the only power of r that fixes vertex 1 is the identity element.
  - From this we can conclude that all of the elements $\{s, sr, sr^2, \dots, sr^{n-1}\}$ are distinct, since $sr^i = sr^j$ would imply $r^{i-j} = e$ by cancellation, and they are also all distinct from the elements $\{e, r, r^2, \dots, r^{n-1}\}$ since $sr^i = r^j$ would imply $s = r^{j-i}$ by cancellation.
  - Hence we see that $D_{2 \cdot n} = \{e, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$.
  - To describe the multiplication of any two elements in this list, we first observe that $rs = sr^{-1}$ (so in particular, $D_{2 \cdot n}$ is always non-abelian). This relation can be visualized geometrically, since rotating and then reflecting is equivalent to reflecting and then rotating in the opposite direction.
  - Alternatively, we can compute $rs(1) = r(1) = 2$ and $rs(2) = r(n) = 1$, and also $sr^{-1}(1) = s(n) = 2$ and $sr^{-1}(2) = s(1) = 2$. Then since rs and sr^{-1} agree on vertices 1 and 2, they agree on all vertices, so they are equal.
  - Then by an easy induction, we see that $r^i s = sr^{-i}$ for all i.
- To summarize the discussion, $D_{2 \cdot n} = \{e, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$, where r and s are elements satisfying the relations $r^n = s^2 = e$ and $rs = sr^{-1}$.
  - Using these relations (and the ancillary fact that $r^i s = sr^{-i}$ for any i) we can compute the product of any two elements in $D_{2 \cdot n}$.
  - For example, in $D_{2 \cdot 7}$, we have $(sr^5)(r^4) = sr^9 = sr^2$, $(r^4)(sr^5) = sr^{-4}(r^5) = sr$, and $(sr^2)(sr) = s(r^2 s)r = s(sr^{-5})r = s^2 r^{-4} = r^3$.

3.1.3 Symmetric Groups and Cycle Decompositions

- Another natural class of groups arises from "symmetries" of sets.
  - To illustrate the idea, observe that the set S_3 of permutations of the set $A = \{1, 2, 3\}$ (formally, the set of bijections of S with itself) forms a group under composition.
  - Note that there are a total of $3! = 6$ such bijections. A somewhat-convenient way to represent these maps is to write a list of the elements of the domain and range vertically: thus the map f with $f(1) = 2$, $f(2) = 3$, and $f(3) = 1$ would be written as $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.
  - In this notation, the 6 elements of S_3 are $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.
  - To compute the product of two elements in S_3, we can simply trace the behavior of each element of $\{1, 2, 3\}$ under the corresponding composition of functions.
  - Thus, for example, if $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, to compute the product gh we observe that (i) h sends 1 to 3, and g sends 3 to 3, so gh sends 1 to 3, (ii) h sends 2 to 1, and g sends 1 to 2, so gh sends 2 to 2, and (iii) h sends 3 to 2, and g sends 2 to 1, so gh sends 3 to 1.
  - Thus, $gh = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. In a similar way we can compute $hg = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, so we see in particular that S_3 is non-abelian.
  - It is very tedious to verify that these operations actually form a group using this explicit description (checking associativity, for example, requires 6^3 individual calculations), and the notation is also quite cumbersome.
- We can clarify matters by generalizing this idea to arbitrary sets.
- Proposition (Symmetric Groups): If A is any set, the set of bijections from A to itself forms a group under function composition. This group is the symmetric group on the set A and is denoted S_A.
  - Proof: The group operation is well-defined because the composition of two bijections is also a bijection. Property [G1] follows because function composition is associative, property [G2] follows because the identity map is a bijection, and property [G3] follows because the inverse of a bijection is also a bijection.
  - If A is a finite set of cardinality n, then $|S_A| = n!$, since bijections on a finite set are the same as injections, and there are clearly $n!$ injections from A to itself (the first element has n possible destinations, the second then has $n - 1$, and so forth). If A is infinite, then clearly $|S_A| = \infty$.
- We will primarily be interested in the case where $A = \{1, 2, \dots, n\}$, in which case we will write the group as S_n, the symmetric group on n objects.
  - First, we would like a more convenient way to describe the elements in S_n. We can achieve this by writing permutations in terms of cycles $(a_1\, a_2\, \dots\, a_k)$.
  - Explicitly, the cycle $(a_1\, a_2\, \dots\, a_k)$ is the permutation σ with $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, ... , $\sigma(a_{k-1}) = a_k$, and $\sigma(a_k) = a_1$, where all other elements are mapped to themselves. This permutation "cycles" the elements $a_1, a_2, \dots, a_k$ one step forward (whence the name).
  - Thus, for example, inside S_4 the cycle $(2\,1\,4)$ is the permutation with $\sigma(2) = 1$, $\sigma(1) = 4$, $\sigma(4) = 2$, and $\sigma(3) = 3$.
  - Not every permutation can be written as a single cycle, but it is not hard to see that every permutation can be written as a product of disjoint cycles (i.e., cycles having no elements in common) such as $(1\,3)\,(2\,4)$, which represents the permutation with $\sigma(1) = 3$, $\sigma(3) = 1$, $\sigma(2) = 4$, and $\sigma(4) = 2$. Such a representation is called the cycle decomposition of σ.

- Explicitly, to determine all of the cycles in the cycle decomposition of a permutation σ, we start with the smallest number x not contained in one of the cycles we have identified, and repeatedly apply σ until we obtain a repeated element. In other words, we evaluate $a_1 = x$, $a_2 = \sigma(a_1)$, $a_3 = \sigma(a_2)$, $a_4 = \sigma(a_3)$, ... until the list repeats.
- It is easy to see that the first repeated value will always be x (since $a_i = a_j$ implies $\sigma(a_{i-1}) = \sigma(a_{j-1})$ so that $a_{i-1} = a_{j-1}$ since σ is a bijection), and so we obtain a cycle $(x\, a_2\, \dots\, a_k)$ containing x. We repeat this process until we have identified the cycles containing every element in $\{1, 2, \dots, n\}$.

- Example: Find the cycle decomposition of the permutation $\sigma \in S_6$ with $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 4$, $\sigma(4) = 1$, $\sigma(5) = 2$, and $\sigma(6) = 6$.
  - We start with $n = 1$: we compute $\sigma(1) = 3$, $\sigma(3) = 4$, and $\sigma(4) = 1$. This gives the cycle $(1\,3\,4)$.
  - The smallest number not yet used is $n = 2$: then $\sigma(2) = 5$ and $\sigma(5) = 2$, so we obtain the cycle $(2\,5)$.
  - The smallest number not yet used is $n = 6$: since $\sigma(6) = 6$ we obtain the cycle (6).
  - Since we have used all 6 elements in cycles, we see that the cycle decomposition of σ is $\boxed{(1\,3\,4)(2\,5)(6)}$.

- Definition: The length of a cycle is the number of elements it contains. A cycle of length k is called a k-cycle, and 2-cycles are often called transpositions.

- The notation for cycle decompositions is not unique. For example, the cycle $(1\,3\,4)$ corresponds to the same permutation as the cycle $(3\,4\,1)$, and the cycle decomposition $(1\,3\,4)(2\,5)(6)$ is the same as $(2\,5)(6)(1\,3\,4)$.
  - We typically will adopt the convention of writing the cycles with the smallest element first, and ordering the cycles in increasing order of their first element. Under this convention, it follows by a straightforward induction argument that the cycle decomposition is unique, and that the algorithm we described above will compute it.
  - We will also usually omit 1-cycles when we write cycle decompositions, with the convention always being that any unlisted elements are fixed (i.e., mapped to themselves). Thus, we would simply write $(1\,3\,4)(2\,5) \in S_6$ and omit the 1-cycle (6). This convention is useful when describing permutations that fix most of the elements in the set.

- We can also compute products using cycle decompositions, with the important remark that the products of cycles are read right-to-left, since they are representing compositions of functions.
  - We can compute the cycle decomposition of the product by tracing what happens to each element $1, 2, \dots, n$ under each of the cycles from right-to-left, and then using the cycle decomposition algorithm.

- Example: If $g = (1\,3\,4)(2\,5)$ and $h = (1\,2)(3\,5)$ inside S_5, compute the cycle decomposition of gh.
  - Since h sends 1 to 2, and g sends 2 to 5, the composition gh sends 1 to 5.
  - To compute the next element in the cycle containing 1 we need to determine where gh sends 5. Since h sends 5 to 3, and g sends 3 to 4, we see that gh sends 5 to 4.
  - Continuing, we see $gh(4) = g(4) = 1$, which completes a cycle $(1\,5\,4)$.
  - Also, since $gh(2) = g(1) = 3$ and $gh(3) = g(5) = 2$, we get the other cycle $(2\,3)$. Thus the cycle decomposition of gh is $\boxed{(1\,5\,4)(2\,3)}$.

- Example: The six elements in S_3 have respective cycle decompositions 1, $(1\,2)$, $(1\,3)$, $(2\,3)$, $(1\,2\,3)$, $(1\,3\,2)$.
  - We can compute, for example, $(1\,2)(1\,3) = (1\,3\,2)$, by tracing what happens to each element from right to left in each of the cycles. (Explicitly, these tracings would look something like $1 \to 3 \to 3$, $3 \to 1 \to 2$, and $2 \to 2 \to 1$.)
  - Similarly, $(1\,3)(1\,2) = (1\,2\,3)$, $(1\,3\,2)(1\,2) = (2\,3)$, and $(1\,2)(1\,3\,2)(1\,3) = (2\,3)$ as well.

- As a final remark we observe that any two disjoint cycles commute, and so (by a trivial induction) two permutations with disjoint cycle decompositions will also commute.

3.1.4 Orders of Elements

- If g is an element of G, the powers of g, namely $\{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$ play an important role in understanding the behavior of multiplication by g.
- Definition: If g is an element of the group G, the order of g, written $|g|$, is the smallest positive integer n such that $g^n = e$, if such an n exists. If $g^n \neq e$ for any positive integer n, we say $|g| = \infty$.
  - If G is a finite group, then every element of G has finite order, since the set of powers $\{e, g, g^2, \dots\}$ must be finite, and if $g^a = g^b$ with $a < b$ then cancelling g^a yields $g^{b-a} = e$.
  - Example: The order of the identity element in any group is always 1.
  - Example: Inside $G = \{1, i, -1, -i\}$, the element -1 has order 2 since $(-1)^2 = 1$ but $-1 \neq 1$. Similarly, both i and $-i$ have order 4.
  - Example: Inside $(\mathbb{Z}, +)$, the order of every nonidentity element is ∞, whereas inside $(\mathbb{Z}/7\mathbb{Z}, +)$, the order of every nonidentity element is 7.
  - Example: Inside $(\mathbb{C}^\times, \cdot)$, the order of $\zeta_6 = e^{2\pi i/6}$ is 6, while the order of 2 is ∞.
  - Example: Inside $(\mathbb{Z}/11\mathbb{Z})^\times$, the powers of $\overline{2}$ are $\{1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$. We see that $\overline{2}^{10} = 1$ but no lower power is equal to 1, so the order of $\overline{2}$ is 10 inside $\mathbb{Z}/11\mathbb{Z}$.
  - Example: Inside $GL_2(\mathbb{Q})$, the order of $A = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ is 3, since A^3 is the identity matrix, but neither A nor A^2 is.
  - Example: Every nonidentity element in the group $(\mathbb{Z}/p\mathbb{Z})^n$, the Cartesian product of n copies of $\mathbb{Z}/p\mathbb{Z}$, has order p.
- Proposition (Properties of Order): Suppose g, h are elements of the group G. Then the following hold:
  1. If $g^n = e$ for some $n > 0$, then g has finite order and the order of g divides n.
     - Proof: Clearly, if $g^n = e$ for some $n > 0$, then $g^k = e$ for some minimal positive integer k by the well-ordering axiom of $\mathbb{Z}$.
     - Now let k be the order of u and apply the division algorithm to write $n = qk + r$ with $0 \le r < k$: then we have $g^r = g^n (g^k)^{-q} = e \cdot e^{-q} = e$.
     - If r were not zero, then we would have $g^r = e$ with $0 < r < k$, which contradicts the definition of order. Thus $r = 0$, meaning that k divides n.
  2. If g has order k, then $g^a = g^b$ if and only if k divides $b - a$. If g has infinite order, then $g^a \neq g^b$ for $a \neq b$.
     - Proof: If $b - a = dk$ then $g^{b-a} = (g^k)^d = e^d = e$, and then multiplying by g^a yields $g^b = g^a$.
     - Conversely, if $g^a = g^b$ then $g^{b-a} = e$, and so by (1) we conclude k divides $b - a$.
     - For the second statement, if $g^a = g^b$ with $a \neq b$, then $g^{b-a} = e = g^{a-b}$ so $g^n = e$ for $n = |b - a|$; then by (1), g would have finite order.
  3. If g has order k, then g^n has order $k/\gcd(n, k)$. In particular, if n and k are relatively prime, then g^n also has order k.
     - Proof: Let $d = \gcd(n, k)$: then $(g^n)^{k/d} = (g^k)^{n/d} = e^{n/d} = e$, so the order of g^n cannot be larger than k/d.
     - Furthermore, if $e = (g^n)^a = g^{na}$, the result above implies that k divides na, so that k/d divides $(n/d)a$.
     - But since k/d and n/d are relatively prime, this implies k/d divides a, and so $a \geq k/d$.
     - Thus, the order of g^n is equal to k/d as claimed. The second statement is simply the case $d = 1$.
  4. If $g^n = e$ and $g^{n/p} \neq e$ for any prime divisor p of n, then g has order n.
     - Proof: Suppose g has order k: then by (1), k must divide n. If $k < n$, then there must be some prime p in the prime factorization of n that appears to a strictly lower power in the factorization of k: then k divides n/p.
     - But then $g^{n/p}$ would be an integral power of $g^k = e$, so that $g^{n/p} = e$, which is a contradiction. Thus, $k = n$.

5. If $gh = hg$, g has order n, h has order m, and m and n are relatively prime, then gh has order mn.
   - Proof: If $gh = hg$ then by a trivial induction every power of g commutes with every power of h.
   - Then we can observe that $(gh)^{mn} = (g^n)^m (h^m)^m = e^m e^n = e$, so gh has some finite order $d \le mn$.
   - Since $(gh)^d = e$, we see that $e = e^n = (gh)^{dn} = (g^n)^d w^{dn} = w^{dn}$, so by (1), m divides dn.
   - Then since m and n are relatively prime, this implies m divides d. By a symmetric argument, n divides d.
   - Since m and n are relatively prime, this means mn divides d, and so the only possibility is $d = mn$.
   - Warning: This result fails (essentially completely) in non-abelian groups. For example, in the matrix group $GL_2(\mathbb{R})$, the matrices $g = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$ and $h = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ both have order 2, but the product matrix $gh = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ has infinite order.

- We will be able to say more about orders of elements in particular groups later, once we discuss cosets. For now we record a few basic observations about element orders in dihedral and symmetric groups:
   - In the dihedral group $D_{2\cdot n}$, since $r^n = e$ but $r^k \neq e$ for $0 < k < n$, we see that $|r| = n$. Then by our results above on orders, the order of r^k is $n/\gcd(k,n)$.
   - Also, since $(sr^k)^2 = s(r^k s)r^k = s(sr^{-k})r^k = s^2 = e$, we see that $\left|sr^k\right| = 2$ for any k.
   - In the symmetric group S_n, the order of any n-cycle $\sigma = (a_1\, a_2\, \ldots\, a_n)$ is n, since $\sigma^n = 1$, but $\sigma^k(a_1) = a_k$ (so $\sigma^k \neq 1$) for $1 \le k \le n-1$.
   - In particular, we can see that every nonidentity element in S_3 has order 2 or 3.
   - Furthermore, in S_n, if a lies in a k-cycle for the permutation τ, then $\tau^n(a) = a$ only when k divides n by the argument given above. Thus, the order of τ is the least common multiple of the lengths of the cycles in its cycle decomposition.
   - For example, the powers of $\tau = (1\,3\,5)(2\,6) \in S_6$ are $\tau^2 = (1\,5\,3)$, $\tau^3 = (2\,6)$, $\tau^4 = (1\,3\,5)$, $\tau^5 = (1\,5\,3)(2\,6)$, and $\tau^6 = 1$, so τ indeed has order 6.

- As we have seen (in the examples of S_3 and $(\mathbb{Z}/p\mathbb{Z})^n$), even when the order of G is composite it is possible that all its nonidentity elements have prime order. We can therefore only expect a general existence result for elements of prime order:

- Theorem (Cauchy's Theorem): Suppose G is a group and p is a prime dividing $|G|$. Then there exists an element of G of order p.
   - Proof: Consider the set S of ordered p-tuples of elements $(g_1, g_2, \ldots, g_p)$ in G such that $g_1 g_2 \cdots g_p = e$. Since $g_p = (g_{p-1} \cdots g_2 g_1)^{-1}$ there are exactly $|G|^{p-1}$ such p-tuples, so the cardinality of S is divisible by p.
   - Also observe that if $(g_1, g_2, \ldots, g_p) \in S$ then any cyclic permutation, such as $(g_2, \ldots, g_p, g_1)$, is also in S. If not all the elements in the tuple are equal, then there are p distinct cyclic permutations of this tuple in S, while if all elements are equal there is only 1, namely $(g, g, \ldots, g)$.
   - Thus, since $\#S$ is divisible by p, and the number of tuples of the first type is divisible by p, the number of tuples of the second type must be divisible by p. In particular, there must be at least one tuple $(g, g, \ldots, g)$ with $g \neq e$: then $g^p = e$ so g is an element of order p.

3.1.5 Subgroups

- Like with subrings, subfields, and vector subspaces, we have a natural notion of subgroup:

- Definition: If G is a group, we say a subset S of G is a subgroup if it also possesses the structure of a group, under the same operations as G.
   - Observe that if S is a subset of a group, in order for the operation $\star$ to be well-defined inside S, we must have $g \star h \in S$ for any $g, h \in S$.

- Then axiom [G1] automatically holds, since it holds in G. In order for [G2] to hold, there must be an identity element e_S in S with the property that $ge_S = g$ for every $g \in S$. However, by the cancellation law in G, since $ge_S = g = ge_G$, we see that $e_S = e_G$: in other words, S must contain the identity element of G.
- Finally, in order for [G3] to hold, we require that for every $g \in S$, it must have an inverse g_S^{-1}. Since $gg_S^{-1} = e_S = e_G = gg_G^{-1}$ by cancellation in G we must have $g_S^{-1} = g_G^{-1}$, which is to say, the inverse of g must be in S.

- Example: For any group G, the sets $\{e\}$ and G are always subgroups of G. The subgroup $\{e\}$ is called the trivial subgroup.
- Proposition (Subgroup Criterion): A subset S of G is a subgroup if and only if S contains the identity of G and is closed under the group operation of G and inverses. Equivalently, S is a subgroup if and only if $e_G \in S$ and for any $g, h \in S$, the element $gh^{-1} \in S$.
  - Proof: If S is a subgroup, then as noted above S must contain the identity of G and be closed under the group operation and inverses. Conversely, if S contains the identity of G and is closed under the group operation and inverses, then it is also a group.
  - For the second statement, if S is a subgroup then $e_G \in S$ and for any $g, h \in S$ we must have $h^{-1} \in S$ and then $gh^{-1} \in S$.
  - Conversely, if $e_G \in S$ and $gh^{-1} \in S$ for any $g, h \in S$, setting $g = e_G$ implies that $h^{-1} \in S$ so S is closed under inverses.
  - Then for any $k \in S$, setting $h = k^{-1}$ and using the fact that $(k^{-1})^{-1} = k$ implies that $gh^{-1} = gk \in S$ so S is closed under the group operation, hence is a subgroup.
- Corollary (Intersection of Subgroups): The intersection of an arbitrary collection of subgroups of G is also a subgroup of G.
  - Proof: Let $S = \bigcap_{i \in I} G_i$ where the G_i are subgroups of G. Then by the subgroup criterion, $e_G \in G_i$ for all $i \in I$, so S contains e_G.
  - Furthermore, for any $g, h \in S$ we have $g, h \in G_i$ for all i. Thus, $gh^{-1} \in G_i$ for all i by the subgroup criterion, so $gh^{-1} \in S$ so S is a subgroup.
- Using the subgroup criterion, we can construct additional examples of groups.
- Example: The set $(\mathbb{Q}^+, \cdot)$ of positive rational numbers under multiplication is a subgroup of $(\mathbb{C}, \cdot)$ since it satisfies the subgroup criterion.
- Non-Example: The set $(\mathbb{Z}_{\geq 0}, +)$ of nonnegative integers under addition is not a subgroup of $(\mathbb{Z}, +)$ since it is not closed under additive inverses.
- Non-Example: The set of odd integers together with 0, under addition, is not a subgroup of $(\mathbb{Z}, +)$ since it is not closed under the group operation of addition.
- Example: The set $(SL_n(F), \cdot)$ of matrices with coefficients in F having determinant 1 is a subgroup of $(GL_n(F), \cdot)$.
  - Explicitly, $\det(I_n) = 1$, and if $\det(A) = \det(B) = 1$, then $\det(AB) = \det(A)\det(B) = 1$ and $\det(A^{-1}) = \det(A)^{-1} = 1$ by basic properties of determinants.
- Example (Centers): If G is a group, the center $Z(G)$ is the subgroup consisting of all of elements G that commute with every other element of G. Explicitly, $Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$.
  - To see that $Z(G)$ is a subgroup, observe that it contains the identity, and if $a, b \in Z(G)$ and $g \in G$, then $(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$ so that $ab \in Z(G)$, and also $ga^{-1} = a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1} = a^{-1}g$ so that $a^{-1} \in Z(G)$.
  - Example: The group G is abelian if and only if $Z(G) = G$.

- Example: The center of the dihedral group $D_{2\cdot 4}$ is $\{e, r^2\}$ since both of these elements commute with all the other elements of the group (powers of r all commute with one another, and also $(r^2)(sr^k) = (r^2 s)r^k = (sr^2)r^k = (sr^k)(r^2)$), but no other elements do (since $sr^k = r^k s$ implies $sr^k = sr^{-k}$ so that $r^{2k} = e$, and also $r(sr^k) = sr^{k-1}$ while $(sr^k)r = sr^{k+1}$).
- Example: The center of the symmetric group S_3 is $\{1\}$, since one may verify that none of the 2-cycles commutes with any of the 3-cycles.

- Example (Alternating Groups): For a positive integer n, we define the subgroup A_n of S_n to be all the elements in S_n that can be written as the product of an even number of transpositions (not necessarily disjoint transpositions). This subgroup is called the alternating group.
  - We can see that A_n is a subgroup: the identity is the product $(1\,2)(1\,2)$ (or, perhaps better, the empty product of 0 transpositions), it is closed under multiplication (since the product of two even numbers of transpositions is clearly also of that form), and it is closed under inverses since the inverse of a transposition is itself (so the inverse of a product of an even number of transpositions is also the product of an even number of transpositions).
  - It is not hard to see that every permutation in S_n is a product of some number of transpositions, since for any n-cycle we can write $(a_1\, a_2\, \dots\, a_n) = (a_1\, a_n)(a_1\, a_{n-1}) \cdots (a_1\, a_2)$ as a product of $n-1$ transpositions.
  - Thus, A_n contains every cycle of odd length, along with the product of any two cycles of even length. Thus, by taking products of such elements, we see that A_n contains every permutation whose cycle decomposition contains an even number of cycles of even length.
  - In fact, we will prove later that these are all of the permutations in A_n, and that there are precisely $n!/2$ such elements.
  - For example, we have $A_3 = \{1, (1\,2\,3), (1\,3\,2)\}$, and also $A_4 = \{1, \{1\,2\,3), (1\,2\,4), (1\,3\,2), (1\,3\,4), (1\,4\,2), (1\,4\,3), (2\,3\,4), (2\,4\,3), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

3.1.6 Generation and Presentations

- If S is a subset of a group, it need not necessarily be a subgroup. We can, however, formulate a notion of "smallest subgroup" containing S.
- Definition: If G is a group and S is a subset of G, the set $\langle S \rangle$, the subgroup generated by S, is the intersection of all subgroups of G containing S.
  - Although this definition is clearly well-posed, we have not really described what the elements in this subgroup $\langle S \rangle$ actually are.
  - If $g_1, g_2, \dots, g_n \in S$, then since S is closed under multiplication and inverses, we see that any "word" in the g_i and their inverses (namely, any product whose terms are all among the g_i and their inverses, like $g_1 g_3^{-1} g_1 g_4$ or $g_8 g_2^{-1} g_4 g_4 g_4$) is contained in S.
  - Conversely, the collection of such finite words does in fact form a subgroup, since the identity element is a finite word, the product of any two finite words is also a finite word, and the inverse of a finite word is also a finite word via the formula $(h_1 h_2 \cdots h_d)^{-1} = h_d^{-1} \cdots h_2^{-1} h_1^{-1}$.
  - We will remark that if S is the empty set, then $\langle S \rangle = \{e\}$. (This agrees with the explicit description of $\langle S \rangle$ as the collection of all possible words if we adopt the usual convention that an empty product represents the identity element.)
- Definition: If G is a group and S is a subset of G with $G = \langle S \rangle$, we say G is generated by S. If G is generated by a finite set, we say G is finitely generated.
  - Example: The group $(\mathbb{Z}, +)$ is generated by $\{1\}$, since the subgroup $\langle 1 \rangle$ contains all positive and negative multiples of 1, and zero, hence is the entire group.
  - Example: From our explicit description of the dihedral group $D_{2\cdot n} = \{e, r, r^2, \dots, s, sr, sr^2, \dots\}$, we can see that $D_{2\cdot n}$ is generated by $\{r, s\}$.

- Example: The group $(\mathbb{Q}, +)$ is generated by the infinite set $\{1, 1/2, 1/3, 1/4, \dots\}$ since any rational number $p/q \in \mathbb{Q}$ is equal to $p(1/q)$. In fact $(\mathbb{Q}, +)$ is not finitely generated: if S is any finite set of generators, and p is any prime not dividing any of the generators' denominators, then $1/p$ is not in the subgroup $\langle S \rangle$.

- We would like (whenever possible) to find a small set of generators for G, since we can then describe all of the elements of G in terms of this small set of generators.
  - Of course, simply knowing a list of generators of G does not say very much about the actual structure of G, because there may be numerous relations between these generators. For example, in $D_{2 \cdot n}$, the generators r and s satisfy the relations $r^n = e$, $s^2 = e$, and $rs = sr^{-1}$.
  - In fact, inside $D_{2 \cdot n}$ these three relations imply all other possible relations between r and s (e.g., $r^{2n} = e$ and $srs^3 = r^{-1}$).
  - To see this consider any group generated by elements r and s such that $r^n = e$, $s^2 = e$, and $rs = sr^{-1}$. Any element in this group is a finite product of terms r, s, r^{-1}, s^{-1}, and by using $r^{-1} = r^{n-1}$ and $s^{-1} = s$ each product can be rewritten to use only r and s. By using the third relation to move all s terms to the left of all r terms, we see any element is in fact of the form $s^a r^b$, and then we may reduce the exponents so that $a \in \{0, 1\}$ and $b \in \{0, 1, \dots, n-1\}$ using the first two relations. Thus, we see that any such group must have at most $2n$ elements, but since $D_{2 \cdot n}$ already has $2n$ elements, there cannot be any further "collapsing". This means that these three relations are enough to fully describe all of the behavior of $D_{2 \cdot n}$.
  - We will be interested in searching for generators and relations that describe the structure of other groups.

- Definition: If G is a group generated by S, and there is some collection of relations $R_1, R_2, \dots, R_n, \dots$ among the elements of S (and their inverses, and the identity e) that imply any other such relation, we call this collection of generators and relations a presentation of G, and write $G = \langle S \,|\, R_1, R_2, \dots, R_n, \dots \rangle$.
  - Explicitly, a "relation" is an equation in the elements of S, the inverses of the elements in S, and the identity e. We can always write any relation in the form [word] $= e$, for some word (i.e., finite product of elements) in $S \cup S^{-1}$.
  - Example: From our analysis above, a presentation of $D_{2 \cdot n}$ is $D_{2 \cdot n} = \left\langle r, s \,|\, r^n = s^2 = e,\ rs = sr^{-1} \right\rangle$.
  - Example: A presentation of $(\mathbb{Z}/m\mathbb{Z}, +)$ is $\mathbb{Z}/m\mathbb{Z} = \langle a \,|\, a^m = e \rangle$. Note that we have written the presentation multiplicatively (the generator a corresponds to the element $\overline{1} \in \mathbb{Z}/m\mathbb{Z}$, with $e = \overline{0}$).
  - It is possible, for infinite groups, that there may be infinitely many independent relations among its elements (even if the group itself is finitely generated). In general, if G has a presentation with a finite number of generators and relations, we say it is finitely presented. Finite groups are always finitely presented: we could simply take the generators to be the full list of elements in G, and the relations to be the entire multiplication table for G.

- Example: A presentation of the quaternion group Q_8 is $Q_8 = \left\langle i, j \,|\, i^4 = e,\ i^2 = j^2,\ ij = ji^{-1} \right\rangle$.
  - It is not hard to see that the elements i and j generate Q_8 and satisfy the three indicated relations.
  - Conversely, the relations $i^2 = j^2$ and $i^4 = e$ imply $j^4 = e$, and by similar logic as in the dihedral groups we can write every element in the form $i^a j^b$. By replacing i^2 with j^2 if necessary, and using $i^4 = j^4 = e$, we can always take $a \in \{0, 1\}$ and $b \in \{0, 1, 2, 3\}$.
  - Thus, this presentation describes a group of order at most 8. Thus, it is a presentation of Q_8, as claimed.

- Presentations give a convenient way to describe the elements of a group, but it is often very difficult to tell whether two given elements (written in terms of the generators) of the group are necessarily equal[4].
  - In fact, it is quite difficult even to determine whether a given presentation contains any elements other than the identity (i.e., whether the presentation describes anything other than the trivial group).

[4]This problem of deciding whether two words are equal in an arbitrary presentation is known as the word problem for groups. It has been proven that there exists a finitely presented group G such that the word problem is undecidable in G, meaning that it is not possible to construct an algorithm that always answers the question correctly in a finite amount of time.

- For example, the presentation $\langle r, s \,|\, r^4 = s^2 = e,\ rs = sr^{-1} \rangle$ describes[5] $D_{2\cdot 4}$, a group of order 8.
- On the other hand, the very similar presentation $\langle r, s \,|\, r^4 = s^2 = e,\ rs = sr^2 \rangle$ turns out to describe a group of order 2, since in this group one has $r = rs^2 = (rs)s = sr^2s = (sr)rs = (sr)sr^2 = s(rs)r^2 = s(sr^2)r^2 = s^2r^4 = e$.

3.1.7 Cyclic Groups

- The simplest nontrivial case of (sub)group generation is the case where S consists of a single element g: in this case, $\langle S \rangle = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$ consists of the powers of g.
- Definition: A group G is cyclic if it is generated by a single element: in other words, if there exists some $g \in G$ such that $G = \langle g \rangle = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$.
  - Example: $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}$, under addition, are both cyclic groups generated by 1.
  - Example: The group $\{1, \zeta_n, \dots, \zeta_n^{n-1}\}$ of nth roots of unity is cyclic, generated by ζ_n.
  - Example: The subgroups $\{1, r, r^2, \dots, r^{n-1}\}$ and $\{e, sr^k\}$ for any k are cyclic subgroups of $D_{2\cdot n}$.
  - It is easy to see that every cyclic group is abelian, since powers of g all commute with one another. Hence in particular, $D_{2\cdot n}$ and S_n are not cyclic groups.
  - If G is cyclic with generator g of infinite order, then $g^a \neq g^b$ for any $a \neq b$ as we have previously noted, and so $G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$ has infinitely many elements.
  - On the other hand, if H is cyclic with generator g having finite order n, then $g^a = g^b$ if and only if $a \equiv b \pmod{n}$. Thus in fact $G = \{e, g, g^2, \dots, g^{n-1}\}$ so that G contains n elements.
  - In both cases, we see that the order of G is equal to the order of its generator g: thus, the two uses of "order", one referring to elements and the other referring to groups, are related in a very natural way.
  - Also from our results on order, if g has order n then the order of g^k in H is then $n/\gcd(k, n)$, and so H is generated by any element of the form g^d for d relatively prime to n.
- The subgroups of cyclic groups have a particularly nice structure, in that they are all cyclic also:
- Proposition (Subgroups of Cyclic Groups): If $G = \langle g \rangle$ is a cyclic group, then every subgroup of G is cyclic. More specifically, if $|g| = \infty$, then every subgroup of G can be uniquely written as $\langle g^d \rangle$ for some nonnegative integer d (and all of these subgroups are distinct), and if $|g| = n$, then every subgroup of G can be uniquely written as $\langle g^d \rangle$ for some nonnegative integer d dividing n, and this subgroup has order n/d (and all of these subgroups are also distinct). Subgroups of the listed forms have $\langle g^a \rangle \subseteq \langle g^b \rangle$ if and only if a divides b.
  - Proof: Suppose $G = \langle g \rangle$ is cyclic and H is a subgroup of G.
  - If $h = g^k$ is any element of H, then $g^{|k|}$ is also in H, since it is either equal to h or to h^{-1} (and H is a subgroup). Since $g^0 = e$ is always in H, we see that H is completely characterized by the set of positive integers $S = \{n \in \mathbb{N} : g^n \in H\}$.
  - If S is empty, then $H = \{e\}$ and all of the results follow (in the case where $|g| = n$ note that $H = \langle g^n \rangle$).
  - Otherwise, S is nonempty, so by the well-ordering axiom we see that S has a minimal element d. Then H contains g^d hence $\langle g^d \rangle$. If $h = g^a$ is any other element of H, if we write $a = qd + r$ by the division algorithm, we would have $g^r = g^a(g^d)^{-q} \in H$, so by minimality of d we must have $r = 0$. This means $h = g^a = (g^d)^q$ and so h is in $\langle g^d \rangle$. Thus, $H \subseteq \langle g^d \rangle$ hence $H = \langle g^d \rangle$.
  - For the remaining statements, if $|g| = \infty$ then since all the powers of g are distinct, the subgroups $\langle g^a \rangle$ and $\langle g^b \rangle$ are distinct because the set of multiples of a is distinct from the set of multiples of b for any positive $a \neq b$.

[5] Technically, we have not described exactly what an arbitrary presentation of this form actually means. Briefly: first define the collection of all finite words on S to be the set of all finite strings of elements in $S \cup S^{-1} \cup \{e\}$. Then define an equivalence relation on the set of finite words by defining a "direct equivalence" to be replacement of gg^{-1} or $g^{-1}g$ with e or the reverse, or by applying one of the relations once. We then define two words to be equivalent if there is some sequence of direct equivalences that turns one word into the other. The set of elements in the presentation is then the collection of equivalence classes under this equivalence relation, and the group operation is concatenation of strings. One must, of course, verify that this operation respects the equivalence relation to ensure it is well defined, and then show that it is associative (both of these verifications are fairly technical, but not conceptually difficult: the idea is to work with "reduced words"). The identity element is e, and the inverse of a word $g_1g_2\dots g_n$ is $g_n^{-1}\dots g_2^{-1}g_1^{-1}$.

- If $|g| = n$, suppose $H = \langle g^d \rangle$ where d is minimal and positive. If we write $n = q'd + r'$ by the division algorithm, then $g^{r'} = g^n (g^d)^{-q'} \in H$, so by minimality of d we must have $r = 0$, meaning that d divides n. Then the order of $\langle g^d \rangle$ is the same as the order of g^d, which is $n/\gcd(d,n) = n/d$. All of these subgroups are then clearly distinct because their orders are distinct.
- The final statement, about the containments of subgroups, is immediate.

- Example: The subgroups of $\mathbb{Z}/18\mathbb{Z}$ are $\langle 1 \rangle$ (order 18), $\langle 2 \rangle$ (order 9), $\langle 3 \rangle$ (order 6), $\langle 6 \rangle$ (order 3), $\langle 9 \rangle$ (order 2), and $\langle 0 \rangle$ (order 1).
- Cyclic groups also arise naturally from the multiplicative groups of fields:
- Theorem (Cyclic Groups and Fields): If F is a finite field, then the group of units $F^\times$ is cyclic. More generally, if G is any finite subgroup of the group of units in any field (finite or not), then G is cyclic.
  - Our proof is nonconstructive: we will establish the existence of an element in G having order $|G|$ without explicitly finding one. (Such an element is called a primitive root in the context of $\mathbb{Z}/m\mathbb{Z}$ or finite fields.)
  - Proof: First we will show that if M is the maximal order among all elements in G, then the order of every element in G divides M. Then we will show that $M = |G|$, which will establish that G is cyclic.
  - For the first claim, suppose g has order M, and let h be any other element of order k. If k does not divide M, then there is some prime q which occurs to a higher power q^f in the factorization of k than the corresponding power q^e dividing M.
  - By properties of orders, the element g^{q^f} has order M/q^f, and the element h^{k/q^e} has order q^e. Since these two orders are relatively prime and $gh = hg$ (since these are elements in a field), we see that the element $g^{q^f} \cdot h^{k/q^e}$ has order $M \cdot q^{f-e}$. This is a contradiction because this element's order is larger than M. Thus, k divides M as claimed.
  - For the second claim, any element of order M generates a subgroup of G having M elements, so $M \le |G|$.
  - Furthermore, by the above, we know that all elements in G have order dividing M, so the polynomial $p(x) = x^M - 1$ has $|G|$ roots in $F[x]$. But by unique factorization in $F[x]$, this is impossible unless $M \ge |G|$, since a polynomial of degree M can only have at most M roots in $F[x]$.
  - Hence we conclude $M = |G|$, meaning that some element has order $|G|$. This element is then a generator of G and G is cyclic.
- Example: The group $(\mathbb{Z}/7\mathbb{Z})^\times$ is cyclic of order 6. Indeed, 3 is a generator, since its powers are $\{1, 3, 2, 6, 4, 5\}$.
- Example: The unit group G of $\mathbb{F}_3[x]/(x^2 + x + 2)$ is cyclic of order 8.
  - With some calculation, we can see that x is a generator of G.
  - Explicitly, we can compute $x^2 \equiv 2x + 1$ so that $x^4 \equiv 2$, and thus $x^8 \equiv 1$.
  - By our results on orders, this implies that x has order 8 inside G, so it is a generator.

3.1.8 Group Isomorphisms and Homomorphisms

- We now formalize the notion of when two groups have identical structures, which captures the same idea as with rings:
- Definition: Let $(G, \star)$ and $(H, \circ)$ be groups. A group isomorphism φ from G to H is a bijective function $\varphi : G \to H$ such that $\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2)$ for all g_1 and g_2 in G. If there is an isomorphism $\varphi : G \to H$, we say G and H are isomorphic, and write $G \cong H$.
  - We will often suppress the notation for the group operations and write the condition simply as $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$.
  - If R and S are rings, then it is easy to see any ring isomorphism $\varphi : R \to S$ yields a group isomorphism of the groups $(R, +)$ and $(S, +)$, and also (when restricted to the respective unit groups) yields a group isomorphism of $(R^\times, \cdot)$ with $(S^\times, \cdot)$.

- Example: For $G = \mathbb{Z}/6\mathbb{Z}$ and $H = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, the map $\varphi : G \to H$ defined via $\varphi(n \bmod 6) = (n \bmod 2,\, n \bmod 3)$ is an isomorphism of groups, since we have previously shown it is a ring isomorphism.
- Example: For $G = D_{2\cdot 3}$ and $H = S_3$, the map $\varphi : G \to H$ defined by associating a symmetry of the equilateral triangle with its associated permutation on the labeled vertices of the triangle is a group isomorphism. The geometric description implies that it respects the group operations, and it is a bijection because it is injective and both groups have order 6. (Alternatively, of course, one could write down all the operations explicitly and just check.)
- Example: For $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}^+, \cdot)$, the map $\varphi : G \to H$ defined via $\varphi(x) = e^x$ is an isomorphism from G to H. The map respects the group operation since $e^{x+y} = e^x e^y$, and it is a bijection since it has an inverse map $\varphi^{-1}(x) = \ln(x)$.

- As with rings we can establish a number of basic properties of isomorphisms, including the fact that being isomorphic is an equivalence relation:
- Proposition (Properties of Isomorphisms): If G, H, K are any groups, the following hold:
  1. The identity map $I : G \to G$ defined by $I(g) = g$ for all $g \in G$ is an isomorphism from G to G.
     - Proof: I is clearly a bijection and respects the group operation.
  2. If $\varphi : G \to H$ is an isomorphism, then the inverse map $\varphi^{-1} : H \to G$ is also an isomorphism.
     - Proof: Essentially by definition, φ^{-1} is also a bijection.
     - Now suppose $\varphi^{-1}(h_1) = g_1$ and $\varphi^{-1}(h_2) = g_2$, so that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$.
     - Then $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = h_1 h_2$, meaning that $\varphi^{-1}(h_1 h_2) = g_1 g_2 = \varphi^{-1}(h_1)\varphi^{-1}(h_2)$, so φ^{-1} is also an isomorphism.
  3. If $\varphi : G \to H$ and $\psi : H \to K$ are isomorphisms, then the composition $\psi\varphi : G \to K$ is also an isomorphism.
     - Proof: The composition of two bijections is a bijection, and also $(\psi\varphi)(g_1 g_2) = \psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1)\varphi(g_2)) = \psi\varphi(g_1)\psi\varphi(g_2)$, so $\psi\varphi$ is an isomorphism.
  4. If $\varphi : G \to H$ is an isomorphism and $g \in G$, then $\varphi(e_G) = e_H$ and $\varphi(g^n) = \varphi(g)^n$ for any $n \in \mathbb{Z}$. In particular, $|g| = |\varphi(g)|$.
     - Proof: First, we have $\varphi(e_G)\varphi(g) = \varphi(e_G g) = \varphi(g) = e_H \varphi(g)$, so cancelling $\varphi(g)$ yields $e_H = \varphi(e_G)$.
     - For $n \geq 0$ the statement $\varphi(g^n) = \varphi(g)^n$ follows by a trivial induction using $\varphi(g^n) = \varphi(g^{n-1}g) = \varphi(g^{n-1})\varphi(g) = \varphi(g)^n$.
     - If $n < 0$ it follows again by induction, starting with the base case $\varphi(g^{-1}) = \varphi(g)^{-1}$, which follows from $\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H$.
     - For the last statement, combine the first two to see that $g^n = e_G$ if and only if $\varphi(g)^n = e_H$, so g and $\varphi(g)$ must have the same order.
  5. If $\varphi : G \to H$ is an isomorphism, then $gh = hg$ if and only if $\varphi(g)\varphi(h) = \varphi(h)\varphi(g)$. In particular, G is abelian if and only if H is abelian.
     - Proof: If $gh = hg$ then $\varphi(g)\varphi(h) = \varphi(gh) = \varphi(hg) = \varphi(h)\varphi(g)$, and the reverse implication follows the same way because φ^{-1} is also an isomorphism. The second statement follows immediately.
  6. If $\varphi : G \to H$ is an isomorphism and K is any subset of G, then K is a subgroup of G if and only if the set $\varphi(K) = \{\varphi(k) : k \in K\}$ is a subgroup of H.
     - Proof: If K is a subgroup of G, then for any $h_1, h_2 \in \varphi(K)$ there exist $k_1, k_2 \in K$ such that $\varphi(k_1) = h_1$ and $\varphi(k_2) = h_2$.
     - Then $e_H = \varphi(e_G) \in \varphi(K)$ and $h_1 h_2^{-1} = \varphi(k_1)\varphi(k_2)^{-1} = \varphi(k_1 k_2^{-1}) \in \varphi(K)$, so $\varphi(K)$ satisfies the subgroup criterion. The reverse implication follows in the same way because φ^{-1} is also an isomorphism.

- In order to show that two given groups are isomorphic, we essentially need to construct an isomorphism between them, which can often be difficult to do[6]. Even if we are handed an isomorphism, actually verifying that it is an isomorphism can be very time-consuming.

[6] More specifically, it has been shown that the isomorphism problem for groups (given two groups, decide whether or not they are isomorphic) is undecidable.

- On the other hand, it is often easier to show that two given groups cannot be isomorphic to one another, if one of the properties of isomorphisms above fails.
- For example, the group $D_{2\cdot 4}$ is not isomorphic to S_3, because the former has order 8 and the latter has order 6, and so there cannot even exist a bijection between their underlying sets of elements.
- In a similar way we can see that $D_{2\cdot 4}$ is not isomorphic to $\mathbb{Z}/8\mathbb{Z}$, because the latter is abelian and the former is not; likewise, S_3 is not isomorphic to $\mathbb{Z}/6\mathbb{Z}$.
- Also, $D_{2\cdot 4}$ is not isomorphic to Q_8, because there are 5 elements of order 2 in $D_{2\cdot 4}$ (namely, r^2 and sr^k for $0 \le k \le 3$) but only 1 element of order 2 in Q_8 (namely, -1).

- A fundamental goal of group theory is to classify (up to isomorphism) all of the groups of a given order.
  - By extending arguments like the ones given above, one can show, for example, that the five groups $D_{2\cdot 4}$, Q_8, $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ are nonisomorphic groups of order 8.
  - It turns out that any group of order 8 must be isomorphic to one of these five, but to prove this fact only from the results we have developed so far would be very difficult.
- A first step towards such a classification is to classify cyclic groups:
- Proposition (Isomorphism and Cyclic Groups): Any two cyclic groups of the same order are isomorphic. More explicitly, any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and any infinite cyclic group is isomorphic to $\mathbb{Z}$.
  - Proof: We show the second statement, which implies the first one because isomorphism is an equivalence relation.
  - First suppose $G = \langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}$ is cyclic of order n, and consider the map $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ defined via $\varphi(\overline{a}) = g^a$.
  - This map is well-defined because $g^n = e$ implies that $g^a = g^b$ whenever $a \equiv b \pmod{n}$, it is clearly surjective and hence a bijection (since both sets have the same size), and $\varphi(\overline{a} + \overline{b}) = g^{a+b} = g^a g^b = \varphi(\overline{a})\varphi(\overline{b})$. Thus, it is an isomorphism.
  - In the case where $G = \langle g \rangle = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$ is an infinite cyclic group, consider the map $\varphi : \mathbb{Z} \to G$ defined via $\varphi(a) = g^a$. This map is injective (since $g^a \neq e$ for any $a \neq 0$), surjective (by definition of $\langle g \rangle$), and $\varphi(a + b) = g^{a+b} = g^a g^b = \varphi(a)\varphi(b)$, so it is an isomorphism.
- We now study maps that respect the structure of group operations without the requirement that they be bijections.
- Definition: Let $(G, \star)$ and $(H, \circ)$ be groups. A group homomorphism φ from G to H is a function $\varphi : G \to H$ such that $\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2)$ for all g_1 and g_2 in G.
  - As with rings, every isomorphism is a homomorphism, but the reverse is not generally true.
  - Example: If R and S are any rings, then a ring homomorphism $\varphi : R \to S$ is automatically a group homomorphism on the additive and multiplicative groups of R and S.
  - Example: As particular special cases of the above, the projection maps $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ and $\varphi : F[x] \to F[x]/p$, defined in each case by $\varphi(a) = \overline{a}$, are group homomorphisms.
  - Example: The map $\varphi : (\mathbb{Z}/n\mathbb{Z}) \to D_{2\cdot n}$ given by $\varphi(\overline{a}) = r^a$ is a group homomorphism: it is well-defined because $a \equiv b \pmod{n}$ implies $r^a = r^b$ because $r^n = e$, and also $\varphi(\overline{a} + \overline{b}) = r^{a+b} = r^a r^b = \varphi(\overline{a})\varphi(\overline{b})$. This map is injective but not surjective.
  - Example: If G is the additive abelian group of all smooth real-valued functions, the derivative map $D : G \to G$ given by $D(f) = f'$ is a group homomorphism, since $D(f+g) = (f+g)' = f' + g' = D(f) + D(g)$.
  - Example: Let G and H be any groups. The zero map $z : G \to H$ given by $z(g) = e_H$ for every $g \in G$ is a group homomorphism.
  - Example: If H is a subgroup of G, the inclusion map $\iota : H \to G$ given by $\iota(h) = h$ is a group homomorphism.
- Many of the properties we established for isomorphisms also hold for homomorphisms (using the same proofs).

- Specifically, property (3) and most of (4) carry over: the composition of homomorphisms is a homomorphism, and homomorphisms respect the identity element, powers, and multiplicative inverses.

- If we do not have any structural information about the nature of the map φ, it can be difficult to verify the homomorphism condition, since it would seem that we would need to verify the condition separately for every pair of elements in G.
  - However, if we have a set of generators for G, we can express all of the other elements in terms of the generators, and so it is reasonable to think that we can reduce the calculation to one involving only the generators.
  - Explicitly, suppose that G is generated by the set S. If $g_1 g_2 \cdots g_n = e_G$ is any relation with the $g_i \in S \cup S^{-1}$, then applying φ to both sides yields $\varphi(g_1)\varphi(g_2)\cdots\varphi(g_n) = e_H$: this means that the images of the generators must satisfy the same relation in H.
  - Conversely, suppose that G is generated by $S = \{s_i\}$, and $\varphi(s_i) = r_i$: then every element in G can be written as a product of the elements in $S \cup S^{-1}$ so the values of $\varphi(s_i)$ determine the value of $\varphi(g)$ for every $g \in G$. Furthermore, if the elements r_i satisfy all of the same relations as the elements s_i, then (one may verify) φ will be well-defined, and it is immediate that φ is then a group homomorphism.
  - This means that if G is generated by $S = \{s_i\}$ satisfying a collection of relations, and elements $r_i \in H$ have the property that the r_i satisfy the same relations, then there exists a (unique) homomorphism $\varphi : G \to H$ such that $\varphi(s_i) = r_i$ for each i.

- To summarize: if we have a presentation of G, then to verify that $\varphi : G \to H$ is a homomorphism, all we need to do is check that φ respects all of the relations in the presentation.

- Example: Show that there is a group homomorphism $\varphi : D_{2\cdot 3} \to S_3$ with $\varphi(r) = (1\,2\,3)$ and $\varphi(s) = (1\,2)$.
  - Since $D_{2\cdot 3} = \langle r, s \,|\, r^3 = s^2 = e,\ rs = sr^{-1} \rangle$, by the discussion above we need only verify the relations.
  - We see $\varphi(r)^3 = (1\,2\,3)^3 = 1$, $\varphi(s)^2 = (1\,2)^2 = 1$, and also that $\varphi(r)\varphi(s) = (1\,2\,3)(1\,2) = (1\,3) = (1\,2)(1\,3\,2) = (1\,2)(1\,2\,3)^{-1} = \varphi(s)\varphi(r)^{-1}$.
  - Since $\varphi(r)$ and $\varphi(s)$ satisfy the required relations, we conclude that there is such a homomorphism.
  - In fact, since S_3 is generated by $\varphi(r)$ and $\varphi(s)$, φ is surjective, hence a bijection and thus an isomorphism.

- Associated to a group homomorphism are two fundamental objects: the kernel and image.

- Definition: If $\varphi : G \to H$ is a group homomorphism, the kernel of φ, denoted $\ker\varphi$, is the set of elements in G mapped to e_H by φ. In other words, $\ker\varphi = \{g \in G : \varphi(g) = e_H\}$.
  - Intuitively, the kernel measures how close φ is to being the zero map: if the kernel is large, then φ sends many elements to the identity, while if the kernel is small, φ sends few elements to the identity.
  - Example: The kernel of the reduction homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ with $\varphi(a) = \overline{a}$ is the subgroup $m\mathbb{Z}$.
  - Example: The kernel of the derivative map D is the collection of constant functions.

- Definition: If $\varphi : G \to H$ is a group homomorphism, the image of φ, denoted $\operatorname{im}\varphi$, is the set of elements in H of the form $\varphi(g)$ for some $g \in G$.
  - In the context of general functions, the image is often called the range of φ.
  - Intuitively, the image measures how close φ is to being surjective: indeed (by definition) φ is surjective if and only if $\operatorname{im}\varphi = H$.

- The kernel and image of a homomorphism are subgroups of G and H respectively:

- Proposition (Kernel and Image): Let $\varphi : G \to H$ be a group homomorphism. Then

  1. The image $\operatorname{im}\varphi$ is a subgroup of H.
     - Proof: Since $\varphi(e_G) = e_H$, the image contains e_H. Furthermore, if $h_1, h_2 \in \operatorname{im}\varphi$ so that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$ for some $g_1, g_2 \in R$, then $h_1 h_2^{-1} = \varphi(g_1 g_2^{-1})$ is also in $\operatorname{im}\varphi$. Thus $\operatorname{im}\varphi$ is a subgroup.

2. The kernel $\ker \varphi$ is a subgroup of G. Also, if $g \in \ker \varphi$, then aga^{-1} is in $\ker \varphi$ for any $a \in G$.
   - Proof: Since $\varphi(e_G) = e_H$, the kernel contains e_G. Furthermore, if $g_1, g_2 \in \ker \varphi$ then $\varphi(g_1 g_2^{-1}) = e_H e_H^{-1} = e_H$, so $g_1 g_2^{-1} \in \ker \varphi$. Thus $\ker \varphi$ is a subgroup.
   - Moreover, we see $\varphi(aga^{-1}) = \varphi(a) e_H \varphi(a^{-1}) = \varphi(a)\varphi(a)^{-1} = e_H$ so that $aga^{-1} \in \ker \varphi$.
3. The kernel is zero (i.e., $\ker \varphi = \{e_G\}$) if and only if φ is injective. In particular, φ is an isomorphism if and only if $\ker \varphi = \{e_G\}$ and $\operatorname{im} \varphi = H$.
   - Proof: If $\varphi(g_1) = \varphi(g_2)$, then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H$, so $g_1 g_2^{-1} \in \ker \varphi$. Thus, if the only element in $\ker \varphi$ is e_G, then we must have $g_1 g_2^{-1} = e_G$ so that $g_1 = g_2$.
   - Conversely, if $g \in \ker \varphi$ and φ is injective, then $\varphi(g) = e_H = \varphi(e_G)$ implies $g = e_G$, so $\ker \varphi = \{e_G\}$.
   - The second statement is then immediate since $\ker \varphi = \{e_G\}$ is equivalent to φ being injective and $\operatorname{im} \varphi = H$ is equivalent to φ being surjective.

3.2 Cosets and Quotient Groups

- We would now like to generalize the idea of modular arithmetic and quotients into the context of groups.
  - We can give a similar sort of motivation to the development we gave with ideals of rings. However, some of the details will be a little bit more difficult because of the non-commutativity of the group operation.
  - So suppose G is a group and N is a subset of G (whose properties we intend to characterize in a moment), and let us say that two elements $a, b \in G$ are "congruent modulo N" if $a^{-1}b \in N$. (Note that this is just the multiplicative version of the statement $b - a \in I$ we used for ideals, but written in the order $(-a) + b$ instead.)
  - We would like "congruence modulo N" to be an equivalence relation: this requires $a \equiv a \pmod{N}$, $a \equiv b \pmod{I}$ implies $b \equiv a \pmod{N}$, and $a \equiv b \pmod{N}$ and $b \equiv c \pmod{N}$ implies $a \equiv c \pmod{N}$.
  - The first condition requires $a^{-1}a = e_G \in N$.
  - The second condition says: if $a^{-1}b \in N$ then $b^{-1}a \in N$. Since $b^{-1}a = (a^{-1}b)^{-1}$, this is the same as saying that N is closed under inverses.
  - The third condition says: if $a^{-1}b \in N$ and $b^{-1}c \in N$, then $a^{-1}c \in N$. Since $a^{-1}c = (a^{-1}b)(b^{-1}c)$, this is the same as saying that N is closed under multiplication.
  - Thus, all of these conditions together are equivalent to saying that N is a subgroup of G, which seems quite reasonable.
- We would also like congruences to respect the group operation, which to say, if $a \equiv c \pmod{N}$ and $b \equiv d \pmod{N}$ then $ab \equiv cd \pmod{N}$.
  - The hypotheses are equivalent to saying that there exist $n_1, n_2 \in N$ such that $a^{-1}c = n_1$ and $b^{-1}d = n_2$, which is to say, $c = an_1$ and $d = bn_2$.
  - Then the desired condition is that $(ab)^{-1}(cd) = b^{-1}a^{-1}an_1bn_2 = b^{-1}n_1bn_2$ is in N, for any $a, b \in G$ and $n_1, n_2 \in N$.
  - This condition is a bit unwieldy, but if we set $n_2 = e_G$ and $b^{-1} = c$, then it reduces to the statement that $cn_1c^{-1} \in N$ for any $c \in G$ and any $n_1 \in N$.
  - On the other hand, if $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$, then if we write $b^{-1}n_1b = n_3 \in N$ (by hypothesis) then the element $b^{-1}n_1bn_2 = n_3n_2$ is then also in N, since N is a subgroup.
  - Thus, to summarize, the hypothesis that $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$ is equivalent to saying that congruences respect the group operation.
  - With this extra condition in hand, we can then define residue classes: the residue class $\overline{a}$ is the collection of all b such that $a \equiv b \pmod{N}$: explicitly, $\overline{a} = \{b \in G : a^{-1}b \in N\} = \{an : n \in N\}$.
  - Finally, we can define the group operation on residue classes via $\overline{a} \cdot \overline{b} = \overline{ab}$, and observe that this operation is well defined because congruence respects the group operation: if $\overline{a} = \overline{c}$ and $\overline{b} = \overline{d}$, then $\overline{ab} = \overline{cd}$, because $a \equiv c \pmod{N}$ and $b \equiv d \pmod{N}$ imply that $ab \equiv cd \pmod{N}$ per the above discussion.

- From this discussion, we can see that the desired conditions on N are that N be a subgroup with the additional property that $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$.
  - With these assumptions, the collection of residue classes $\overline{a} = aN = \{an : n \in N\}$ will then have a well-defined group operation given by $\overline{a} \cdot \overline{b} = \overline{ab}$.
  - We will also note that the statement that $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$ is equivalent to the statement that for every $c \in G$, the set $cNc^{-1} = \{cnc^{-1} : n \in N\}$ is equal to N itself.
  - One direction is clear, since if $cNc^{-1} = N$ for every $c \in G$, then certainly $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$.
  - On the other hand, if $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$, then $cNc^{-1} \subseteq N$ for all c. In particular, plugging in c^{-1} for c yields $c^{-1}Nc \subseteq N$, which is equivalent to $N \subseteq cNc^{-1}$: thus we must have $cNc^{-1} = N$ for all $c \in G$.
- We will now examine more closely the properties of the sets aH for $a \in G$ and H a subgroup of G (these sets are called left cosets of H), and also the properties of normal subgroups, the subgroups for which $cNc^{-1} = N$ for all $c \in G$.

3.2.1 Cosets of Subgroups, Lagrange's Theorem

- Definition: If H is a subgroup of G and $a \in G$, the set $aH = \{ah : h \in H\}$ is called a left coset of H. We also define the index of H in G, denoted $[G : H]$, to be the number of distinct left cosets of H in G.
  - We also have a symmetric notion of $Ha = \{ha : h \in H\}$, which is called a right coset of H. If G is abelian, then left and right cosets are the same, but when G is non-abelian, this need not be the case. We will see in a moment that the definition of the index is independent of whether we use left or right cosets.
  - If G is an additive abelian group, we will write (left) cosets as $a + H$; note that this notation is consistent with our prior use of $r + I$ in rings.
  - Example: If $H = \{e, r^2\}$ in $G = D_{2\cdot 4}$, then there are four left cosets of H in G, namely $eH = r^2H = \{e, r^2\}$, $rH = r^3H = \{r, r^3\}$, $sH = sr^2H = \{s, sr^2\}$, and $srH = sr^3H = \{sr, sr^3\}$.
  - Example: If $H = \{1, (1\,2\,3), (1\,3\,2)\}$ in $G = S_3$, then there are two left cosets of H in G, so $[G : H] = 2$. Explicitly, these cosets are $1H = (1\,2\,3)H = (1\,3\,2)H = \{1, (1\,2\,3), (1\,3\,2)\}$ and $(1\,2)H = (1\,3)H = (2\,3)H = \{(1\,2), (1\,3), (2\,3)\}$.
  - Example: If $H = \{1, (1\,3)\}$ in $G = S_3$, then there are three left cosets of H in G, so $[G : H] = 3$. Explicitly, these cosets are $1H = (1\,3)H = \{1, (1\,3)\}$, $(1\,2)H = (1\,3\,2)H = \{(1\,2), (1\,3\,2)\}$, and $(2\,3)H = (1\,2\,3)H = \{(2\,3), (1\,2\,3)\}$.
  - Example: If $H = 2\mathbb{Z} = \{\dots, -2, 0, 2, 4, \dots\}$ in $G = \mathbb{Z}$, then there are two (left) cosets of H in G, so $[G : H] = 2$. These cosets are $0 + H = \{\dots, -2, 0, 2, 4, \dots\}$ and $1 + H = \{\dots, -3, 1, 3, 5, \dots\}$.
- In each of the examples above, all of the left cosets have the same size (which is then the same size as $eH = H$), and the left cosets form a disjoint partition of G. This is true in general:
- Proposition (Properties of Cosets): Let H be a subgroup of G. Then the following hold:
  1. For any $a \in G$, the map $f : H \to aH$ defined by $f(h) = ah$ is a bijection between H and gH.
     - Proof: By definition of aH, the map f is surjective. On the other hand, $f(h_1) = f(h_2)$ is equivalent to $ah_1 = ah_2$, which by cancellation implies $h_1 = h_2$: thus, f is also injective, hence it is a bijection.
  2. For any $a \in G$, the only left coset of H containing a is aH.
     - Proof: Clearly aH is a left coset of H containing a since $e \in H$, so we need to show it is the only one.
     - If $a \in bH$ then by definition $a = bh$ for some $h \in H$.
     - Then for any $h' \in H$, since $hh' \in H$ because H is a subgroup, we see that $ah' = b(hh') \in bH$. Thus bH contains aH.

    - On the other hand, for any $bh'' \in bH$, since $b = ah^{-1}$ we can write $bh'' = a(h^{-1}h'') \in aH$ because $h^{-1}h'' \in H$ again because H is a subgroup. Thus, aH contains bH, so they are equal.

3. Any two left cosets of H in G are either disjoint or identical. Thus, the left cosets of H in G partition G.
    - Proof: Suppose aH and bH are left cosets of H. If they are disjoint we are done, so suppose they have some common element g.
    - But then by (2), this means $aH = gH = bH$, so $aH = bH$. The other statement is immediate since any $g \in G$ is contained in the left coset gH.

4. For any $a, b \in G$, we have $aH = bH$ if and only if $a^{-1}b \in H$.
    - Proof: If $aH = bH$ then since $b \in aH$ this means $b = ah$ for some $h \in H$: then $a^{-1}b = a^{-1}ah = h \in H$.
    - Conversely, if $a^{-1}b \in H$, then $b = ah$ for some $h \in H$, and so $b \in aH$. Then by (2), this means $bH = aH$.

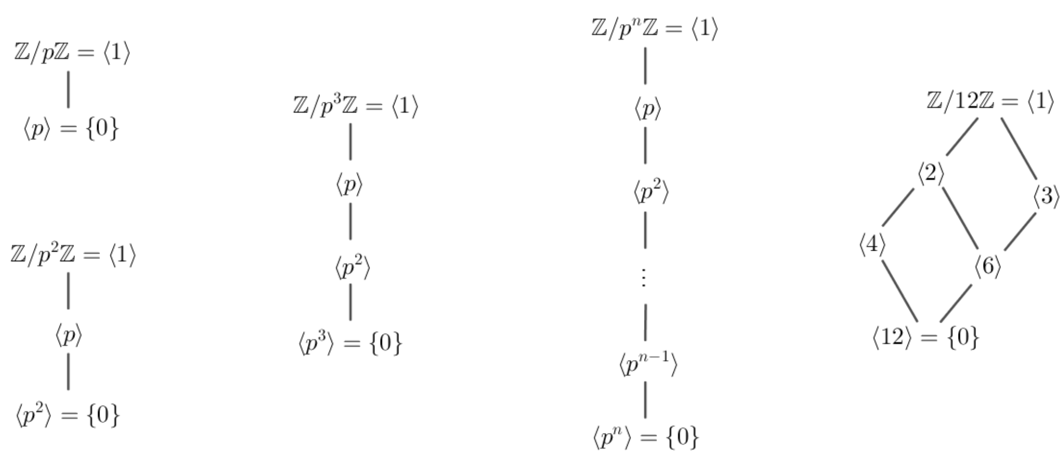
- Remark: All of these properties also hold if we replace "left coset" with "right coset" everywhere, and modify the statements accordingly.

- These properties seem rather simple, but we can deduce a very important consequence from them:
- Theorem (Lagrange's Theorem): If H is a subgroup of G, then $\#G = \#H \cdot [G : H]$, where if one side is infinite then both are. In particular, if G is a finite group, then the order of any subgroup H divides the order of G.
    - Proof: By our properties of cosets, each left coset of H has a bijection with H, and so all of the left cosets have the same cardinality.
    - Since the left cosets form a partition of G, we may partition the $\#G$ elements into a total of $[G : H]$ left cosets each of which has size $\#H$.
    - Thus, $\#G = \#H \cdot [G : H]$. The second statement follows immediately from this relation, since $[G : H]$ is an integer.
    - Remark: If we work with right cosets instead of left cosets, we obtain the same formula: thus, the number of left cosets is equal to the number of right cosets.
- Corollary (Orders of Elements): If G is a finite group of order n, then for every $g \in G$ the order of g divides n, and $g^n = e$.
    - Proof: Let $H = \langle g \rangle$ be the cyclic subgroup generated by g. As we have shown, the order of H is equal to the order of g, and by Lagrange's theorem we see that it divides n. The second statement follows immediately.
- Although its proof is seemingly easy, Lagrange's theorem is an extremely important tool in unraveling the structure of groups (particularly, finite groups) since it substantially narrows the possible orders for elements and subgroups of G. For example, we can completely classify the groups of order at most 7:
- Proposition (Groups of Small Order): Suppose G is a group. Then the following hold:
    1. If G has prime order p, then G is cyclic and isomorphic to $\mathbb{Z}/p\mathbb{Z}$. In particular, any group of order 2, 3, 5, or 7 is cyclic.
        - Proof: If G is a group of order p, consider any nonidentity element g. The order of g must divide p, and it cannot be 1 because g is not the identity. Thus, g has order p, and then $G = \langle g \rangle$ is cyclic.
    2. If G has order 4, then G is abelian and isomorphic either to $\mathbb{Z}/4\mathbb{Z}$ or to $V_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
        - Proof: If G is a group of order 4, then the order of any nonidentity element must be 2 or 4. If G has an element of order 4 then it is cyclic and thus isomorphic to $\mathbb{Z}/4\mathbb{Z}$.
        - Otherwise, assume that every nonidentity element has order 2. Choose any two nonidentity elements a and b, and consider ab.
        - We cannot have $ab = e$ since this would imply $a = ae = a(ab) = a^2b = b$. Likewise, we cannot have $ab = a$ or $ab = b$ since cancellation would yield $b = e$ or $a = e$. Thus, ab is distinct from e, a, and b, so $G = \{e, a, b, ab\}$.

- Then ba cannot equal e, a, or b in the same way as above, so we must have $ab = ba$, so G is abelian.
- It is then not hard to see that the map $\varphi : (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \to G$ given by $\varphi(x, y) = a^x b^y$ is an isomorphism.

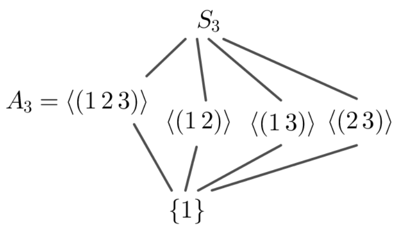
3. If G has order 6, then G is isomorphic either to $\mathbb{Z}/6\mathbb{Z}$ or to $S_3 \cong D_{2\cdot 3}$.
   - Proof: If G is a group of order 6, then the order of any nonidentity element must be 2, 3, or 6. If G has an element of order 6 then it is cyclic and thus isomorphic to $\mathbb{Z}/6\mathbb{Z}$.
   - Otherwise, assume that every nonidentity element has order 2 or 3. If every nonidentity element has order 2, then by the same argument given above for groups of order 4, if we choose two of them then they must commute and would generate a subgroup of order 4. But since 4 does not divide 6, this cannot occur.
   - Thus, G contains some element a of order 3, and so we obtain a subgroup $H = \{e, a, a^2\}$. Since $[G : H] = 2$ there is exactly one other left coset of H, say $bH = \{b, ba, ba^2\}$; these cosets are disjoint, so $b \notin H$.
   - Since there is also exactly one other right coset of H, which must contain b since $b \notin H$, it is $Hb = \{b, ab, a^2b\}$. Since left or right cosets partition G, this means $bH = Hb$.
   - Then b^2H is also a left coset of H, and it cannot equal bH since (by cancellation) this would imply $bH = H$, which is false.
   - Therefore, $b^2H = H$, and so b^2 is one of e, a, a^2. If b^2 were equal to a then b would have to have order 3, but then we could write $b = b^4 = a^2$, which is impossible. Likewise, b^2 cannot equal a^2, so we must have $b^2 = e$ so that b has order 2.
   - Also, since $bH = Hb$, we deduce $ab \in Hb = \{b, ab, a^2b\}$, so since $ab \neq b$, we must have either $ab = ba$ or $ab = ba^2$. But if $ab = ba$, then since a has order 3 and b has order 2, ab would have order 6, contradicting our hypothesis.
   - Thus, $ab = ba^2$, or equivalently, $ab = ba^{-1}$. Since $G = \langle a, b\rangle$ this means $G = \left\langle a, b : a^3 = b^2 = e,\ ab = ba^{-1}\right\rangle$ which is the same as the presentation for the dihedral group $D_{2\cdot 3}$. By our results on presentations, since G and $D_{2\cdot 3}$ both have order 6, we conclude that $G \cong D_{2\cdot 3} \cong S_3$ as claimed.

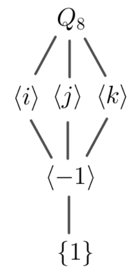
- We can also use Lagrange's theorem to simplify calculations involving subgroups, toward an ultimate goal of writing down all the possible subgroups of a given group.
- A convenient way to organize this information is by drawing the subgroup lattice of G (more formally called the Hasse diagram of G): we arrange all of the subgroups of G starting with the smallest subgroups at the bottom, and then draw paths to indicate immediate containments.
  - For $\mathbb{Z}/n\mathbb{Z}$, as we have shown, the subgroups are in bijection with the divisors of n, and $\langle a\rangle$ is contained in $\langle b\rangle$ precisely when a divides b. Here are a few examples of the resulting subgroup lattices:

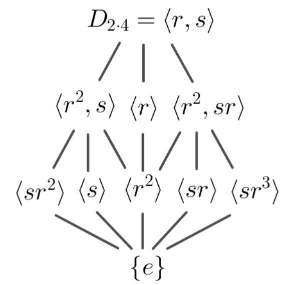


  - To compute an arbitrary subgroup lattice for a finite group, we may work as follows: first write down all of the cyclic subgroups (i.e., subgroups generated by a single element). Next, write down all possible "joins" of two cyclic subgroups (i.e., the smallest subgroup containing both), which yield all of the subgroups generated by two elements. Now repeat the process by computing all possible joins of three cyclic subgroups (equivalently, joins of a 2-generator subgroup with a cyclic subgroup), and so on, until all subgroups have been obtained.

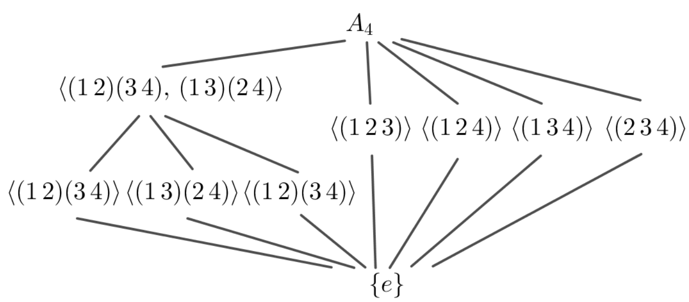
- Here is the result of following this procedure for some of the other small groups we have described:







- If G is a finite group, then the only possible orders of a subgroup are divisors of n. However, for any given divisor of n, there need not actually be a subgroup having that order.
  - For example, in the group A_4 of order 12, we claim that there is no subgroup of order 6. To see this we can simply construct the full subgroup lattice of A_4 using the algorithm described above:



  - Explicitly, one can show that any two 3-cycles that are not in the same subgroup of order 3 will generate all of A_4, as will any of the elements of order 2 together with any element of order 3.

- We will discuss a partial converse to Lagrange's theorem (namely, Sylow's theorems) in a later section.

3.2.2 Normal Subgroups and Quotient Groups

- We now continue with our discussion of quotient groups. As we have already explained, in order to have well-defined operations on the collection of left cosets of H, we must impose an additional condition on H:

- Definition: If K is a subgroup of G and $g \in G$, we define the conjugate of K by g, written gKg^{-1}, as $gKg^{-1} = \{gkg^{-1} : k \in K\}$. We say $g \in G$ normalizes K if $gKg^{-1} = K$, and we N is a normal subgroup of G, written $N \trianglelefteq G$, if every $g \in G$ normalizes N.
  - Example: Every subgroup of an abelian group is normal. In particular, if R is a ring and I is an ideal, then I is a normal subgroup of $(R, +)$.
  - When G is non-abelian, it is tedious to try to verify that $gKg^{-1} = K$ for every $g \in G$.
  - We can reduce the amount of calculation by observing that if $g, h \in G$ both normalize K, then $(gh)K(gh)^{-1} = g(hKh^{-1})g = gKg^{-1} = K$ so that gh also normalizes K, and also by multiplying by g^{-1} on the left and g on the right, $gKg^{-1} = K$ implies $K = g^{-1}Kg$ so that g^{-1} normalizes K.
  - Thus, since the identity clearly normalizes K, we see that the collection of elements normalizing K is a subgroup of G. This subgroup is called the normalizer of K in G, and is denoted $N_G(K)$.
  - Hence, to show K is normal, we need only verify that it is normalized by a set of generators for G.

- Example: If $H = \{e, r^2\}$ in $G = D_{2\cdot 4}$, then H is normal in G because $rHr^{-1} = \{e, r^2\} = H$ and $sHs^{-1} = \{e, sr^2s\} = \{e, r^2\} = H$.
- Non-Example: If $H = \{e, s\}$ in $G = D_{2\cdot 4}$, then H is not normal in G because $rHr^{-1} = \{e, rsr^{-1}\} = \{e, sr^2\} \neq H$.
- Example: If $H = \{1, (1\,2\,3), (1\,3\,2)\}$ in $G = S_3$, then H is normal in G because $(1\,2\,3)H(1\,2\,3)^{-1} = H$ since H contains $(1\,2\,3)$, and also $(1\,2)H(1\,2)^{-1} = \{1, (1\,3\,2), (1\,2\,3)\} = H$.
- Non-Example: If $H = \{1, (1\,3)\}$ in $G = S_3$, then H is not normal in G because $(1\,2)H(1\,2)^{-1} = \{1, (2\,3)\} \neq H$.

- Now we can construct quotient groups. When $N \trianglelefteq G$, we will also write the left coset aN as $\overline{a}$.
- Theorem (Quotient Groups): Let N be a normal subgroup of G. Then the collection of left cosets of N in G forms a group (the quotient group of G by N, denoted G/N) under the operation $(aN) \cdot (bN) = (ab)N$, or, in residue class notation, $\overline{a} \cdot \overline{b} = \overline{ab}$. In particular, the identity element is $\overline{e} = eN$ and inverses are given by $(gN)^{-1} = g^{-1}N$. Furthermore, we have $\#(G/N) = [G : N]$, and also if G is abelian then so is G/N.
  - If G is an additive abelian group we instead write $(a+N)+(b+N) = (a+b)+N$. As noted earlier, any ideal of a ring under addition is a normal subgroup, so our notation here is completely consistent with the notation we used for quotient rings.
  - Proof: First we must show that the operation is well-defined: that is, if we choose different elements $c \in aN$ and $d \in bN$, then the coset of cd is the same as that of ab.
  - To see this, if $c \in aN$ then $c = an_1$ for some $n_1 \in N$, and similarly $d = bn_2$ for some $n_2 \in N$.
  - Because $xN = yN$ if and only if $x^{-1}y \in N$, we see that $(ab)N = (cd)N$ is equivalent to $(ab)^{-1}(an_1bn_2) \in N$.
  - We see that $(ab)^{-1}(an_1bn_2) = b^{-1}a^{-1}an_1bn_2 = (b^{-1}n_1b)n_2$, and then since $b^{-1}n_1b \in N$ because b^{-1} normalizes N, we conclude that $(ab)^{-1}(an_1bn_2) \in N$.
  - Therefore, $(ab)N = (cd)N$, and so the operation is well-defined.
  - The three group axioms [G1]-[G3] then follow from the corresponding properties in G.
  - For example, for [G1] we have $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$.
  - For [G2], the multiplicative identity is $\overline{e}$, since $\overline{a} \cdot \overline{e} = \overline{ae} = \overline{a} = \overline{ea} = \overline{e} \cdot \overline{a}$, and for [G3] we have $\overline{a} \cdot \overline{a^{-1}} = \overline{aa^{-1}} = \overline{e} = \overline{a^{-1}a} = \overline{a^{-1}} \cdot \overline{a}$, so $\overline{a}^{-1} = \overline{a^{-1}}$.
  - For the last statements, by definition $\#(G/N)$ is the number of left cosets of N in G, which is $[G : N]$. Finally, if G is abelian then $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$ so G/N is also abelian.

- For convenience we can collect a number of equivalent properties for normality (some of which are more useful in particular contexts):
- Proposition (Normality Conditions): If N is a subgroup of G, the following are equivalent:
  1. N is a normal subgroup of G (i.e., $gNg^{-1} = N$ for every $g \in G$).
  2. The collection of left cosets of G forms a group under the operation $(aN)(bN) = abN$.
  3. $gNg^{-1} \subseteq N$ for every $g \in G$.
  4. $gN = Ng$ for every $g \in G$.
  5. Every left coset of G is also a right coset of G, and vice versa.
     - Condition (3) is usually the easiest to check, and to show (3) it is only necessary to verify that $g_in_jg_i^{-1} \in N$ for a set of generators g_i of G and a set of generators n_j of N.
     - Proof: In our motivation for the definition of normality, we showed that (2) implies (1) and that (3) implies (1). Our theorem constructing quotient groups shows that (1) implies (2), and also (1) clearly implies (3). Thus, (1), (2), and (3) are all equivalent.
     - For (4), $gN = Ng$ implies for any $n \in N$ there exists $n' \in N$ with $gn = n'g$. Thus $gng^{-1} = n' \in N$ for every $g \in G$ and $n \in N$, which is (3). Conversely, if $gNg^{-1} = N$, then multiplying every element in both sets on the right by g shows that $gN = Ng$, so (1) implies (4).

- For (5), clearly $gN = Ng$ for every $g \in G$ implies that every left coset is a right coset, so (4) implies (5). Conversely, if every left coset is a right coset, then since gN is the unique left coset containing g and Ng is the unique right coset containing g, we must have $gN = Ng$ for every g: thus, (5) implies (4).

- Here are some examples of quotient groups:
- Example: For $G = S_3$ and $N = \langle (1\,2\,3) \rangle$, identify the elements of G/N and determine the structure of G/N.
  - Since $[G : N] = |G| / |N| = 2$ there are 2 left cosets of G, so G/N is a group of order 2. Thus G/N will be isomorphic to $\mathbb{Z}/2\mathbb{Z}$.
  - We can compute the elements of G/N explicitly as $1N = \{1, (1\,2\,3), (1\,3\,2)\}$ and $(1\,2)N = \{(1\,2), (2\,3), (1\,3)\}$.
  - By the definition of the quotient group structure, we can then compute $[1N][1N] = 1$, $[1N][(1\,2)N] = (1\,2)N = [(1\,2)N][1N]$, and $[(1\,2)N][(1\,2)N] = (1\,2)^2 N = 1N$.
  - Indeed, the structure of G/N is precisely that of $\mathbb{Z}/2\mathbb{Z}$.
- Example: For $G = Q_8$ and $N = \langle -1 \rangle$, identify the elements of G/N and determine the structure of G/N.
  - Since $[G : N] = |G| / |N| = 4$ there are 4 left cosets of G, so G/N is a group of order 4.
  - The elements of G/N are $1N = \{1, -1\}$, $iN = \{i, -i\}$, $jN = \{j, -j\}$, and $kN = \{k, -k\}$. The identity element is $1N$.
  - By the definition of the quotient group structure, we can then compute, for example, $(iN)(jN) = ijN = kN$, and $(jN)(iN) = jiN = -kN = kN$.
  - Also, we have $(iN)^2 = i^2 N = -1N = 1N$, and likewise $(jN)^2 = 1N$ and $(kN)^2 = 1N$, so each nonidentity element of the group has order 2.
  - From our characterization of the groups of order 4, this tells us that G/N is isomorphic to the Klein 4-group V_4.
- Example: For $G = \mathbb{Z}/12\mathbb{Z}$ and $N = \langle 6 \rangle$, identify the elements of G/N and determine the structure of G/N.
  - Since $[G : N] = |G| / |N| = 6$ there are 6 left cosets of G, so G/N is a group of order 6.
  - The elements of G/N are $0+N = \{0, 6\}$, $1+N = \{1, 7\}$, $2+N = \{2, 8\}$, $3+N = \{3, 9\}$, $4+N = \{4, 10\}$, and $5+N = \{5, 11\}$.
  - We can see that $k(1+N) = k+N$ for any integer k, and so G/N is a cyclic group (of order 6) generated by $1+N$.
  - Remark: More generally, if $G = \langle g \rangle$ is cyclic and generated by the element g, it is not hard to see that G/N is cyclic and generated by $\overline{g} = gN$.
- Example: For $G = D_{2\cdot 6}$ and $N = \langle r^3 \rangle$, identify the elements of G/N and determine the structure of G/N.
  - Since $[G : N] = |G| / |N| = 6$ there are 6 left cosets of G, so G/N is a group of order 6.
  - The elements of G/N are $eN = \{e, r^3\}$, $rN = \{r, r^4\}$, $r^2N = \{r^2, r^5\}$, $sN = \{s, sr^3\}$, $srN = \{sr, sr^4\}$, and $sr^2N = \{sr, sr^2\}$.
  - Note that $(rN)^3 = r^3N = eN$ and $(r^2N)^3 = r^6N = eN$ so both rN and r^2N have order 3. In a similar way we can see that sN, srN, and sr^2N each have order 2.
  - From our characterization of the groups of order 6, this tells us that G/N is isomorphic to $D_{2\cdot 3} \cong S_3$. (In fact, an explicit isomorphism with $D_{2\cdot 3}$ can be obtained simply by reading off the corresponding label from the cosets, as we listed them above!)
- One of the primary reasons that quotient groups are of interest is that it is often possible to "piece together" information about N and G/N to yield information about G.
  - For example, using an argument of this type, we will prove later that if p is prime, then every group of order p^2 is abelian and isomorphic to one of $\mathbb{Z}/p^2\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

- We will remark that even if the isomorphism types of N and G/N are known, then this information does not uniquely determine the structure of G. For example, we have seen that both Q_8 and $D_{2\cdot 4}$ have normal subgroups N of order 2 (isomorphic to $\mathbb{Z}/2\mathbb{Z}$), such that the quotient group by N is isomorphic to the Klein 4-group.
- In general, the problem of describing all groups G having a normal subgroup N isomorphic to a specific group A and with G/N isomorphic to another specific group B is called the extension problem for groups.

* Of course, when G is large it can be quite difficult to understand the structure of G/N in a useful way. Nonetheless, such quotient groups can often have interesting properties.
  - For example, every element of the quotient group $\mathbb{Q}/\mathbb{Z}$ has finite order, although element orders in this group can be arbitrarily large. Explicitly, if p/q is in lowest terms then the coset $\overline{p/q}$ has order q, since $q \cdot \overline{p/q} = \overline{p} = \overline{0}$ but no smaller multiple of p/q will yield an integer.
  - As another example, if p is a prime and G represents the group of p-power roots of unity in $\mathbb{C}$ (i.e., the union of the p^nth roots of unity for all $n \geq 1$) and N represents the group of pth roots of unity, then G/N is isomorphic to G itself. Explicitly, one may verify that the map given by $\varphi(\zeta N) = \zeta^p$ is well-defined and yields an isomorphism of G/N with G.
* A common proof technique for establishing structural results about finite groups is to use induction on $|G|$, and piece information together from normal subgroups and quotient groups. A major obstruction to this type of argument occurs if G possesses no nontrivial proper normal subgroups:
* Definition: A group G is simple if $|G| > 1$ and the only normal subgroups of G are $\{e\}$ and G.
  - The cyclic groups $\mathbb{Z}/p\mathbb{Z}$ for p prime are simple, and in fact it is not hard to see that they are the only abelian simple groups.
  - Another family of simple groups is given by the alternating groups A_n for $n \geq 5$. (It is not as easy to see that these groups are simple!)
  - A major goal of finite group theory is to classify the finite simple groups, since they provide a partial analogue to the prime numbers in that they are the "building blocks" for the construction of groups from smaller groups.
  - This classification was completed (up to some minor components) in the 1980s, and established that there are 18 infinite families of finite simple groups, along with 26 "sporadic" simple groups not belonging to any of these families, such that every finite simple group is isomorphic to one of these listed groups. In total, the classification is estimated to run over 10000 pages, spanning several hundred papers by dozens of individual authors.

3.2.3 Quotients and Homomorphisms

* Like with rings, we also have various natural connections between normal subgroups and group homomorphisms.
  - To begin, observe that if $\varphi : G \to H$ is a group homomorphism, then $\ker \varphi$ is a normal subgroup of G.
  - In fact, we proved this fact earlier when we introduced the kernel, but let us remark again: if $g \in \ker \varphi$, then for any $a \in G$, then $\varphi(aga^{-1}) = \varphi(a)\varphi(g)\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = e$. Thus, $aga^{-1} \in \ker \varphi$ as well, and so by our equivalent properties of normality, this means $\ker \varphi$ is a normal subgroup.
  - Thus, we can use homomorphisms to construct new normal subgroups.
  - Equally importantly, we can also do the reverse: we can use normal subgroups to construct homomorphisms.
  - The key observation in this direction is that the map $\varphi : G \to G/N$ associating a group element to its residue class / left coset (i.e., with $\varphi(a) = \overline{a}$) is a ring homomorphism.
  - Indeed, the homomorphism property is precisely what we arranged for the left cosets of N to satisfy: $\varphi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \varphi(a) \cdot \varphi(b)$.

- Furthermore, the kernel of this map φ is, by definition, the set of elements in G with $\varphi(g) = e$, which is to say, the set of elements $g \in N$.
- Thus, we see that kernels of homomorphisms and normal subgroups are precisely the same things.

- Let us summarize these observations:

- Proposition (Projection Homomorphisms): If N is a normal subgroup of G, then the map $\varphi : G \to G/N$ defined by $\varphi(a) = \overline{a} = aN$ is a surjective group homomorphism called the projection homomorphism from G to G/N.
  - Proof: We have $\varphi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \varphi(a) \cdot \varphi(b)$, so φ is a homomorphism. Also, φ is surjective, essentially by definition: any residue class in G/N is of the form gN for some $g \in G$, and then $\varphi(g) = gN$.

- We also get the analogous statement of the first isomorphism theorem:

- Theorem (First Isomorphism Theorem): If $\varphi : G \to H$ is a group homomorphism, then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi$ is isomorphic to $\operatorname{im}\varphi$.
  - Intuitively, φ is a surjective homomorphism $\varphi : G \to \operatorname{im}\varphi$. To turn it into an isomorphism, we must "collapse" its kernel to a single element: this is precisely what the quotient group $G/\ker\varphi$ represents.
  - Proof: Let $N = \ker\varphi$. We have already shown that N is a normal subgroup of G, so now we will construct a homomorphism $\psi : G/N \to \operatorname{im}\varphi$, and then show that it is injective and surjective.
  - The map is defined as follows: for any residue class $gN \in G/N$, we define $\psi(gN) = \varphi(g)$.
  - To see ψ is well-defined, suppose that $g' \in gN$ is some other representative of the coset gN. Then $g' = gn$ for some $n \in N$, so $\psi(g'N) = \varphi(g') = \varphi(gn) = \varphi(g)\varphi(n) = \varphi(g) = \psi(gN)$ since $n \in \ker\varphi$, so ψ is well-defined.
  - It is then easy to see ψ is a homomorphism, since $\psi(\overline{a} \cdot \overline{b}) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(\overline{a})\psi(\overline{b})$.
  - Next, we see that $\psi(\overline{g}) = e$ precisely when $\varphi(g) = e$, which is to say $g \in \ker(\varphi) = N$, so that $\overline{g} = \overline{e}$. Thus, the only element in $\ker\psi$ is $\overline{e}$, so ψ is injective.
  - Finally, if h is any element of $\operatorname{im}\varphi$, then by definition there is some $g \in G$ with $\varphi(g) = h$: then $\psi(\overline{g}) = h$, meaning that ψ is surjective.
  - Since ψ is a homomorphism that is both injective and surjective, it is an isomorphism.

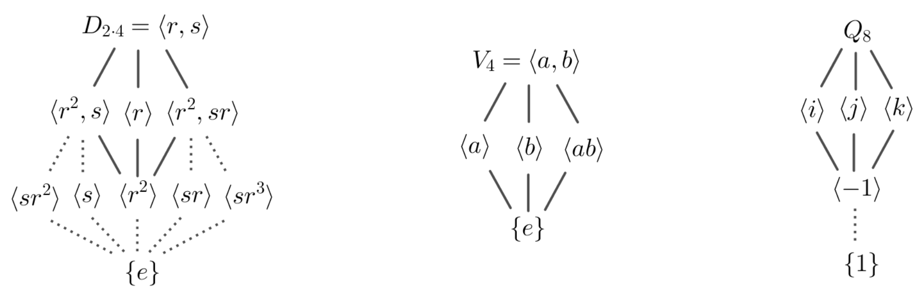
- By using the first isomorphism theorem, we can construct isomorphisms of groups.
  - In order to show that G/N is isomorphic to a group H, we search for a surjective homomorphism $\varphi : G \to H$ whose kernel is N.

- Example: Show that $\mathbb{Z}/12\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ as a group.
  - We seek a surjective homomorphism $\varphi : \mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ whose kernel is $12\mathbb{Z}$.
  - Once this idea is suggested, it is not hard to come up with a candidate, namely, $\varphi(a) = (a \bmod 3,\ a \bmod 4)$.
  - It is easy to verify that map is a homomorphism (since the individual maps of reduction mod 3 and reduction mod 4 are homomorphisms) and it is likewise fairly easy to see that the map is surjective by checking that the images of 0, 1, ... , 11 represent all of the elements in $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.
  - Finally, the kernel of the map consists of all integers a with $\varphi(a) = (0, 0)$, which is equivalent to saying $a \equiv 0 \pmod 3$ and $a \equiv 0 \pmod 4$, so that $3|a$ and $4|a$: thus, the kernel is precisely $12\mathbb{Z}$.
  - Therefore, by the first isomorphism theorem applied to φ, we conclude that $\mathbb{Z}/12\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.

- By using the first isomorphism theorem, we can establish the group analogues of the other isomorphism theorems:

- Theorem (Second Isomorphism Theorem): If A is a normal subgroup of G and B is any subgroup of G, then $AB = \{ab : a \in A, b \in B\}$ is a subgroup of G, $A \cap B$ is a normal subgroup of B, and $(AB)/B$ is isomorphic to $A/(A \cap B)$.

- Theorem (Third Isomorphism Theorem): If H and K are normal subgroups of G with $H \leq K$, then H is normal in K, K/H is normal in G/H, and $(G/H)/(K/H)$ is isomorphic to G/K.
- Theorem (Fourth Isomorphism Theorem): If N is a normal subgroup of G, then there is an inclusion-preserving bijection between the subgroups A of G containing N and the subgroups $\overline{A} = A/N$ of G/N. This bijection preserves the subgroup lattice structure, in the sense that it respects indexes, joins, intersections, and normality.
  - We will not give the full details of the proofs of the isomorphism theorems, although many of the details (such as checking various subgroups are normal, etc.) are relatively straightforward. Constructing the necessary isomorphisms for the second and third isomorphism theorems can be done via the first isomorphism theorem.
  - For example, to show that $(AB)/B$ is isomorphic to $A/(A \cap B)$, we verify that the map $\varphi : A \to (AB)/B$ given by $\varphi(a) = aB$ is a surjective homomorphism and then check that its kernel is $A \cap B$. Then the first isomorphism theorem yields an isomorphism of $A/(A \cap B)$ with $(AB)/B$.
  - Likewise, to show that $(G/H)/(K/H)$ is isomorphic to G/K, we verify that the map $\varphi : G/H \to G/K$ given by $\varphi(gH) = gK$ is a well-defined, surjective homomorphism with kernel K/H.
- We can give a few illustrations of the lattice isomorphism theorem:
  - For a first example, recall that we have shown that the subgroup $N = \langle r^2 \rangle$ of $G = D_{2\cdot 4}$ is normal, and that the quotient G/N is isomorphic to the Klein 4-group.
  - By dotting the lines to emphasize only the subgroups containing $\langle r^2 \rangle$, we can see explicitly a copy of the subgroup lattice for the Klein 4-group inside the subgroup lattice of $D_{2\cdot 4}$:



  - In the same way we can also identify the structure of the Klein 4-group's lattice inside Q_8, since the quotient of Q_8 by the subgroup $N = \langle -1 \rangle$ is also isomorphic to the Klein 4-group.

3.3 Group Actions

- We initially motivated the idea of a group as arising (in a natural way) from collections of symmetries of geometric or algebraic objects.
- We can make this interaction more precise using group actions, which formalize the notion of a group "acting on" a set in a way that is compatible with the structure of the group.
  - If we think of a group as a collection of symmetries of an object (and we think of the object as a set), each element of the group will behave as a function from the set to itself, and function composition will agree with the group operation.
  - Furthermore, the identity element of the group will act as the identity function, and inverses in the group will act as the corresponding inverse function.
  - These requirements lead naturally to the definition of a group action.

3.3.1 Definition and Basic Properties

- Definition: If G is a group and A is a set, a (left[7]) group action of G on A is a function from $G \times A$ to A, written as $g \cdot a$, such that

  [A1] The action is compatible with the group operation: $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for any $g_1, g_2 \in G$ and $a \in A$.

  [A2] The identity acts as the identity map: $e \cdot a = a$ for all $a \in A$.

- Here are a few basic examples of group actions:
- Example (S_n): If $A = \{1, 2, \dots, n\}$, then S_n acts on A via permutation. Explicitly, the action is $\sigma \cdot a = \sigma(a)$.
  - For example, if $n = 5$ we have $(1\,2\,3\,4) \cdot 1 = 2$, $(1\,2\,3)(4\,5) \cdot 4 = 5$, and $(2\,5\,1)(3\,4) \cdot 5 = 1$.
  - For [A1] we have $\sigma \cdot (\tau \cdot a) = \sigma \cdot (\tau(a)) = \sigma(\tau(a)) = (\sigma\tau)(a) = (\sigma\tau) \cdot a$ by the definition of the group action in S_n as function composition.
  - For [A2] we have $1 \cdot a = a$ for all $a \in A$ by the definition of the identity permutation.
- Example ($D_{2 \cdot n}$): If $A = \{V_1, V_2, \dots, V_n\}$ is the set of vertices of a regular n-gon (labeled counterclockwise), then $D_{2 \cdot n}$ acts on A by the geometric interpretation we used to define $D_{2 \cdot n}$.
  - For example, we have $r \cdot V_1 = V_2$, $r \cdot V_2 = V_3$, ... , $r \cdot V_{n-1} = V_n$, and $r \cdot V_n = V_1$, and $s \cdot V_1 = V_1$, $s \cdot V_2 = V_n$, $s \cdot V_3 = V_{n-1}$, ... , and $s \cdot V_n = V_2$.
  - The verification that this actually is a group action follows from the analysis we did in originally describing $D_{2 \cdot n}$ from its geometric definition.
- Example (Vector Space Multiplication): If $A = V$ is an F-vector space, then we have a group action $G = F^{\times}$ on V via scalar multiplication.
  - Explicitly, using $\star$ for the group action, we have $\alpha \star v = \alpha v$ for every $v \in A$ and $\alpha \in G$.
  - Axioms [A1] and [A2] follow in this case by the corresponding axioms for vector spaces.
- Example (Trivial Action): If G is any group and A is any set, then the trivial group action with $g \cdot a = a$ for all $g \in G$ and $a \in A$ is a group action of G on A.
  - It is easy to see that the trivial action satisfies both [A1] and [A2].
- Example (Left-Multiplication Action): If G is any group, then the left-multiplication action of G on itself is defined via $g \cdot a = ga$ for any $g \in G$ and $a \in G$. (The underlying set in this case is $A = G$.)
  - For [A1], we have $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a) = g_1(g_2 a) = (g_1 g_2)a = (g_1 g_2) \cdot a$ by associativity in G.
  - For [A2], we have $e \cdot a = ea = a$ by the identity property in G.
- Example (Conjugation Action): If G is any group, then G acts on the set $A = G$ by conjugation, via $g \cdot a = gag^{-1}$ for any $g \in G$ and $a \in A$.
  - For [A1], we have $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1 g_2 (a g_2^{-1}) g_1^{-1} = (g_1 g_2) a (g_1 g_2)^{-1} = (g_1 g_2) \cdot a$.
  - For [A2], we have $e \cdot a = eae^{-1} = a$.
- Example (Matrices on F^n): If F is a field, the general linear group $GL_n(F)$ acts on F^n via left multiplication $M \cdot \mathbf{v} = M\mathbf{v}$ for all $M \in GL_n(F)$ and $\mathbf{v} \in F^n$.
  - Axioms [A1] and [A2] follow in this case by the corresponding properties of matrix multiplication.
- Notice that we did not include as part of the definition of group action that inverses in the group act as the corresponding inverse function; this is because it actually follows from [A1] and [A2].

[7] There is also a notion of a right group action, which is a function from $A \times G$ to A whose [A1] statement reads as $(a \cdot g_2) \cdot g_1 = a \cdot (g_2 g_1)$ and whose [A2] statement reads as $a \cdot e = a$. Left and right group actions can be interchanged by observing that if $g \cdot a$ yields a left action, then $a \cdot g^{-1}$ yields a right action. In certain contexts, right actions can be more natural.

  - Explicitly, by [A1] and [A2], for any $g \in G$ we have $g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = e \cdot a = a$ and also $g \cdot (g^{-1} \cdot a) = (gg^{-1}) \cdot a = e \cdot a = a$: thus, g^{-1} acts as the inverse function of g.
  - For each $g \in G$, we obtain a map $\sigma_g : A \to A$ given by $\sigma_g(a) = g \cdot a$; the calculation above shows that σ_g is a bijection with inverse $\sigma_{g^{-1}}$.
  - Thus, under the group action, each element $g \in G$ is associated with a bijection σ_g from A to itself, which is an element of the permutation group S_A.
  - In fact, axiom [A1] tells us that this association is a group homomorphism from G to S_A: for any $a \in A$, we have $\sigma_{g_1 g_2}(a) = (g_1 g_2) \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_{g_2}(a))$, and thus $\sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2}$ as functions.
  - Conversely, any group homomorphism from G to S_A yields a group action of G on A: [A1] follows by the same calculation performed above, while [A2] follows by the observation that any homomorphism from G to S_A must map the identity of G to the identity of S_A.

- Together, our observations show that a group action of G on A is the same as a group homomorphism from G to S_A: in other words, every element of G acts by permuting the elements of A in a way that is consistent with the group operation in G.
  - Since any group action corresponds to a group homomorphism from G to S_A, it is then natural to consider the kernel of this homomorphism.
  - Group actions whose kernel is trivial (i.e., consists of only the identity element) are particularly noteworthy:

- Definition: The kernel of the group action of G on A is the kernel of the associated homomorphism from G to S_A, namely, the set of $g \in G$ with $g \cdot a = a$ for all $a \in A$. The group action is faithful if its kernel consists of only the identity element.
  - Example: The action of $D_{2 \cdot n}$ on the vertices of an n-gon is faithful, as is the action of S_n on $\{1, 2, \dots, n\}$ and the action of $F^\times$ on an F-vector space V.
  - Example: The kernel of the trivial action of G on A is all of G, and is thus not faithful if G is not the trivial group.
  - Example: The kernel of the left-multiplication action of G on itself is $\{e\}$ (by cancellation), and is therefore faithful.
  - Example: The kernel of the conjugation action of G on itself is its center $Z(G)$. If $Z(G) = \{e\}$ then the action is faithful, and otherwise it is not faithful.

- If a group action is faithful then the associated homomorphism from G to S_A is injective, and then by the first isomorphism theorem we see that G is isomorphic to its image in S_A. Applying this observation in particular to the left-multiplication action of G on itself yields the following theorem:

- Theorem (Cayley's Theorem): Every group is isomorphic to a subgroup of a symmetric group. Furthermore, if $|G| = n$, then G is isomorphic to a subgroup of S_n.
  - Proof: As we noted above, the left-multiplication action of G on itself is faithful, so we obtain an injective homomorphism $\varphi : G \to S_G$; thus by the first isomorphism theorem, G is isomorphic to $\operatorname{im} \varphi$, which is a subgroup of a symmetric group. The second statement is immediate.
  - Remark: Historically, groups were initially conceived as being permutation groups (i.e., subsets of symmetric groups), and it was only later that the axiomatic definition we used was adopted. Cayley's theorem, then, indicates that the historical and modern conceptions of a group are equivalent. Although the historical definition is more concrete, the axiomatic approach has the advantage of not requiring us to specify a particular symmetric group of which G is a subgroup, and makes many other tasks (e.g., involving homomorphisms and isomorphisms) much easier to handle.
  - As an example, if $G = Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ and we label the elements in that order, then i corresponds to the permutation $(1\,3\,2\,4)(5\,7\,6\,8)$ and j corresponds to the permutation $(1\,5\,2\,6)(3\,8\,4\,7)$. Thus, since Q_8 is generated by i and j, we see that the subgroup of S_8 generated by $(1\,3\,2\,4)(5\,7\,6\,8)$ and $(1\,5\,2\,6)(3\,8\,4\,7)$ is isomorphic to Q_8.

- If we have a (nontrivial) action of G on A, we can often obtain important structural information about G and about A by studying the group action.

- Definition: If G acts on A, then for any $a \in A$ the stabilizer of a is the set $G_a = \{g \in G : g \cdot a = a\}$ of elements of g fixing a.

  - The stabilizer is a subgroup of G: clearly $e \in G_a$ by [A2], and if $g, h \in G_a$ then $(gh)\cdot a = g\cdot(h\cdot a) = g\cdot a = a$ by [A1], and also $a = e \cdot a = (g^{-1}g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a$ so $g^{-1} \in G_a$.
  - Example: For the action of S_n on $\{1, 2, \dots, n\}$ by permutation, the stabilizer of n is the collection of all permutations that fix n. Since such permutations can permute $\{1, 2, \dots, n-1\}$ arbitrarily, this stabilizer is isomorphic to S_{n-1}.
  - Example: For the action of $D_{2\cdot n}$ on the vertices $\{V_1, \dots, V_n\}$ of a regular n-gon, the stabilizer of any vertex V_i consists of the identity map along with the reflection along the line passing through the center of the n-gon and V_i.
  - Example: For the left-multiplication action of G on itself, the stabilizer of any element $a \in G$ consists of only the identity (by cancellation).
  - Example: For the conjugation action of G on itself, the stabilizer of any element $a \in G$ consists of all elements $g \in G$ such that $gag^{-1} = a$, which is to say, all elements $g \in G$ with $ga = ag$ (i.e., all elements of G that commute with a).

- Definition: If G acts on A, then the orbits of G acting on A are the equivalence classes of the equivalence relation on A given by $a \sim b$ if there exists $g \in G$ with $b = g \cdot a$. If there is a single orbit (namely, A itself) then we say the action of G on A is transitive.

  - It is straightforward to verify that this relation $\sim$ is indeed an equivalence relation, so it makes sense to speak of its equivalence classes.
  - Explicitly, the orbits are the sets $G \cdot a = \mathcal{O}_a = \{g \cdot a : g \in G\}$ for the various elements $a \in A$. The set $G \cdot a$ is the orbit of a under G, and (per the definition) is the subset of A that can be obtained by starting at a and applying an element of G.
  - The term "orbit" is intended to connote the idea that the action of G sends a to various different places, and the orbit of a is the collection of all the places that a can go.
  - Example: For the action of S_n on $\{1, 2, \dots, n\}$ by permutation, for $\sigma = (1\,2\,3\,\dots\,n)$ we have $\sigma \cdot 1 = 2$, $\sigma \cdot 2 = 3$, ... , and $\sigma \cdot n = 1$, so there is a single orbit consisting of the entire set $\{1, 2, \dots, n\}$. This means the action is transitive.
  - Example: The left-multiplication action of G on itself is transitive, since for any $g, h \in G$ we have $(hg^{-1}) \cdot g = h$.
  - Example: For the conjugation action of $G = S_3$ on itself, there are three orbits: $\{e\}$, $\{(1\,2), (1\,3), (2\,3)\}$, and $\{(1\,2\,3), (1\,3\,2)\}$.

- We have an important combinatorial relation between orbits and stabilizers:

- Proposition (Orbit-Stabilizer Theorem): If G acts on the set A, then the number of elements in the orbit $\mathcal{O}_a$ is equal to $[G : G_a]$, the index of the stabilizer of a.

  - Proof: We will show that there is a bijection between elements $b \in \mathcal{O}_a$ and the left cosets bG_a of the stabilizer G_a.
  - Consider the map $f : G \to A$ with $f(g) = g \cdot a$. Then for any $g, h \in G$, we see that $f(g) = f(h)$ if and only if $g \cdot a = h \cdot a$ if and only if $a = g^{-1} \cdot (h \cdot a) = (g^{-1}h) \cdot a$ if and only if $g^{-1}h \in G_a$ if and only if $gG_a = hG_a$.
  - Therefore, for any $b \in \mathcal{O}_a$ with $b = g \cdot a$, we see that the fiber $f^{-1}(b)$ of the map f is precisely the left coset gG_a. This means that f yields a bijection between the left cosets of G_a with the elements of the orbit $\mathcal{O}_a$ of a.
  - The claimed result then follows immediately because the number of left cosets of G_a equals $[G : G_a]$, as we showed previously.

3.3.2 Polynomial Invariants and A_n

- Our primary interest in groups, and in group actions in particular, is to use them to study field extensions. An important action that will be relevant to our work is the action of S_n and its subgroups on polynomials.
- Example (S_n on Polynomials): If F is a field and $x_1, x_2, \dots, x_n$ are independent variables, then S_n acts on the polynomial ring $F[x_1, x_2, \dots, x_n]$ via "index permutation" of the variables. Explicitly, given a polynomial $p(x_1, x_2, \dots, x_n)$ and $\sigma \in S_n$, the action of σ is $\sigma \cdot p(x_1, x_2, \dots, x_n) = p(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$.
  - It is easy to see that this definition yields a group action, since $\sigma_1 \cdot (\sigma_2 \cdot p)) = \sigma_1 \cdot p(x_{\sigma_2(1)}, \dots, x_{\sigma_2(n)}) = p(x_{\sigma_1\sigma_2(1)}, \dots, x_{\sigma_1\sigma_2(n)}) = (\sigma_1\sigma_2) \cdot p$, and $1 \cdot p = p(x_1, \dots, x_n) = p$.
  - As an example, with $n = 4$ and $p(x_1, x_2, x_3, x_4) = (x_1 - 2x_2x_4)(4x_3^3 - x_4^2)$ then for $\sigma = (1\,2\,3\,4)$ we have $\sigma \cdot p = (x_2 - 2x_3x_1)(4x_4^3 - x_1^2)$.
- We can use the action of S_n on particular polynomials to extract information about certain subgroups of S_n. We will pursue additional examples when we study the roots of degree-3 and degree-4 polynomials, but we can describe how to use this action to study the alternating group A_n now:
  - For a fixed n, define the polynomial $D = \prod_{1 \le i < j \le n} (x_i - x_j)$. For example, when $n = 3$ we have $D = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.
  - Now consider the action of S_n on D via index permutation, so that for $\sigma \in S_n$ we have $\sigma(D) = \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)})$.
  - For example, with $n = 3$ and $\sigma = (1\,2\,3)$ we have $\sigma(D) = (x_2 - x_3)(x_2 - x_1)(x_3 - x_1) = -D$.
  - Now observe that since σ is a permutation, each term in the product for D will appear in $\sigma(D)$ except possibly with the variables in the other order. (With $\sigma = (1\,2\,3)$ above, the $x_2 - x_3$ term remains unchanged but the $x_1 - x_2$ term becomes $x_2 - x_1$.)
  - By collecting all the signs, we see that D and $\sigma(D)$ are the same except up to a product of some number of -1 terms, and therefore $\sigma(D) = \pm D$ for all $\sigma \in S_n$.
- Definition: For $\sigma \in S_n$ we define the sign $\text{sgn}(\sigma)$ of σ to be $+1$ if $\sigma(D) = D$ and -1 if $\sigma(D) = -D$. We call a permutation σ even if $\text{sgn}(\sigma) = 1$ and odd if $\text{sgn}(\sigma) = -1$.
- Proposition (Sign Map is a Homomorphism): The sign map is a group homomorphism $\text{sgn} : S_n \to \{\pm 1\}$. Equivalently, $\text{sgn}(\tau\sigma) = \text{sgn}(\tau)\text{sgn}(\sigma)$ for all $\sigma, \tau \in S_n$.
  - Proof: Let $\sigma, \tau \in S_n$: by definition we have $(\tau\sigma)(D) = \prod_{1 \le i < j \le n} (x_{\tau\sigma(i)} - x_{\tau\sigma(j)})$.
  - Suppose that $\sigma(\Delta)$ has k factors that are interchanged upon the application of σ. Consider what happens when we compute $\tau\sigma(\Delta)$ by applying σ first and then τ. When we do this, the action of σ will produce exactly k factors of the form $x_{\tau(j)} - x_{\tau(i)}$ with $i < j$; the rest will be $x_{\tau(i)} - x_{\tau(j)}$ with $i < j$.
  - Interchanging the "flipped" terms introduces a sign $(-1)^k = \text{sgn}(\sigma)$. After we "switch back" all of these terms, we will obtain $\tau(D)$. Symbolically,

$$\tau\sigma(D) = \tau(\sigma(D)) = (-1)^k \prod_{1 \le i < j \le n} (x_{\tau(i)} - x_{\tau(j)}) = \text{sgn}(\sigma) \cdot \tau(D) = \text{sgn}(\sigma)\text{sgn}(\tau) \cdot D$$

    where the last equality follows by the definition of $\text{sgn}(\tau)$.
  - Combining these results yields $\text{sgn}(\tau\sigma) \cdot D = \tau\sigma(D) = \text{sgn}(\sigma)\text{sgn}(\tau) \cdot D$, and therefore $\text{sgn}(\tau\sigma) = \text{sgn}(\tau)\text{sgn}(\sigma)$, as claimed.
- Using the sign map we can characterize the elements of the alternating group:
- Theorem (Alternating Group): The alternating group A_n is the kernel of the sign map (hence normal in S_n), consists of all even permutations, and has order $n!/2$.
  - Proof: First, the sign map is surjective because $\text{sgn}((1\,2)) = -1$ since the permutation $(1\,2)$ only flips the sign of the single term $x_1 - x_2$.

- Next, for any transposition $(i\,j)$, if we set $\sigma = (1\,i)(2\,j)$ then $\sigma(1\,2)\sigma = (i\,j)$, so since the sign map is a homomorphism we have $\text{sgn}((i\,j)) = \text{sgn}(\sigma(1\,2)\sigma) = \text{sgn}(\sigma) \cdot (-1) \cdot \text{sgn}(\sigma) = -1$. Thus, all transpositions are odd permutations.
- Since the sign map is a homomorphism, its kernel therefore consists of all permutations that can be written as a product of an even number of transpositions. But this is precisely how we defined A_n, so A_n is the kernel of the sign map and consists of all even permutations.
- Furthermore, since sgn is surjective, we see that $S_n/A_n \cong \text{im}(\text{sgn})$ has order 2, so $|A_n| = |S_n|/2 = n!/2$.
- Remark: This argument also shows that even permutations are those that are the product of an even number of transpositions, while odd permutations are those that are the product of an odd number of transpositions, and that no permutation is both even and odd (since the sign map is well-defined). As we noted earlier, a permutation is even if and only if it has an even number of even-length cycles in its cycle decomposition.

3.3.3 Groups Acting By Conjugation

- We now study in more detail the conjugation action of a group G on its set of elements.
  - As we noted earlier, if G is any group, then G acts on the set $A = G$ via $g \cdot a = gag^{-1}$ for any $g \in G$ and $a \in A$.
  - We may generalize this action by noting that G also acts elementwise on the collection of subsets of G, by defining $g \cdot S = \{gs : s \in S\}$ for an arbitrary subset S of G.
- First, we study the orbits of the conjugation action on elements:
- Definition: If G is a group and $a \in G$, we say that b is conjugate to a if there exists some $g \in G$ with $b = gag^{-1}$. The conjugacy class of a in G is the set of elements of G conjugate to a. Explicitly, the conjugacy class of a is the set $\{gag^{-1} : g \in G\}$, which is the orbit of a under conjugation by G.
  - Example: In an abelian group, each element is its own conjugacy class, since the condition is simply $b = gag^{-1} = gg^{-1}a = a$.
  - Example: More generally, a single element $\{a\}$ is its own conjugacy class precisely when $a \in Z(G)$, which is to say, when a commutes with every element of G.
  - Example: In $D_{2\cdot 4}$, the conjugacy classes are $\{1\}$, $\{r^2\}$, $\{r, r^3\}$, $\{s, sr^2\}$, and $\{sr, sr^3\}$. We can compute that $srs^{-1} = r^3$ and $rsr^{-1} = sr^2$ and $r(sr)r^{-1} = sr^3$, so the given collections are indeed conjugate, and it is not hard to verify that these sets are distinct conjugacy classes.
  - Example: In $GL_2(\mathbb{Q})$, the matrices $A = \begin{bmatrix} -3 & 5 \\ 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 \\ 0 & -4 \end{bmatrix}$ are conjugate via the matrix $M = \begin{bmatrix} 1 & -5 \\ 1 & 1 \end{bmatrix}$, since $MAM^{-1} = B$. We will remark that conjugacy of matrices is often studied in linear algebra (where it also has the same name), and it is a nontrivial problem to identify the possible conjugacy classes.
  - Example: In S_3, the conjugacy classes are $\{1\}$, $\{(1\,2), (1\,3), (2\,3)\}$, and $\{(1\,2\,3), (1\,3\,2)\}$. We can compute that $(1\,3) = g(1\,2)g^{-1}$, $(2\,3) = h(1\,2)h^{-1}$, and $(1\,2\,3) = g(1\,3\,2)g^{-1}$ for $g = (2\,3)$ and $h = (1\,3)$, so the given collections are conjugate to one another. It is not hard to verify that these sets are distinct conjugacy classes.
- We can in fact generalize the last example to compute the conjugacy classes in S_n:
- Proposition (Conjugacy Classes in S_n): If $\tau \in S_n$, then for any cycle $(a_1 \ldots a_n)$, we have $\tau(a_1 \ldots a_n)\tau^{-1} = (\tau(a_1) \ldots \tau(a_n))$. Thus, to conjugate a permutation σ by a permutation τ, we simply apply τ to all of the elements in the cycles of σ. In particular, two elements of S_n are conjugate if and only if they have the same cycle type.
  - Proof: The first statement is a direct calculation: for each i, we have $\tau(a_1 \ldots a_n)\tau^{-1}[\tau(a_i)] = \tau(a_1 \ldots a_n)(a_i) = \tau(a_{i+1})$, where we take $a_{n+1} = a_1$.

- Thus, by the cycle decomposition algorithm, there is a single cycle in $\tau(a_1\ \dots\ a_n)\tau^{-1}$, consisting of $(\tau(a_1)\ \dots\ \tau(a_n))$.
- The second statement follows from the first one by writing σ as a product of disjoint cycles $\sigma = \sigma_1 \cdots \sigma_d$ and observing that $\tau\sigma\tau^{-1} = (\tau\sigma_1\tau^{-1}) \cdots (\tau\sigma_d\tau^{-1})$.
- The last statement follows from the second one: any conjugate of σ has the same cycle type as σ by the calculation above.
- Conversely, if σ' has the same cycle type as σ, if we align cycles of corresponding lengths together from σ and σ', say so that the lists of all the elements in the cycles of σ are $a_1, \dots, a_n$ and σ' are $b_1, \dots, b_n$, then the permutation τ with $\tau(a_i) = b_i$ for each i will conjugate σ to σ'.

- Example: There are 5 conjugacy classes in S_4, since there are 5 possible cycle types: the identity, transpositions, 3-cycles, 4-cycles, and the 2,2-cycles.
  - Explicitly, the conjugacy classes are $\{1\}$, $\{(1\,2), (1\,3), (1\,4), (2,3), (2\,4), (3,4)\}$, $\{(1\,2\,3), (1\,2\,4), (1\,3\,2), (1\,3\,4), (1\,4\,2),$ ($\{(1\,2\,3\,4), (1\,2\,4\,3), (1\,3\,2\,4), (1\,3\,4\,2), (1\,4\,2\,3), (1\,4\,3\,2)\}$, and $\{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.
  - In general, the number of conjugacy classes in S_n will be the number of integer partitions of n.

- Example: For $\sigma = (1\,7\,4\,8\,6)$ and $\tau = (1\,5)(2\,4\,3)(6\,7)$ inside S_8, compute $\sigma\tau\sigma^{-1}$ and $\tau\sigma\tau^{-1}$.
  - From the procedure given in the proposition, we have $\sigma\tau\sigma^{-1} = (\sigma(1)\,\sigma(5))(\sigma(2)\,\sigma(4)\,\sigma(3))(\sigma(6)\,\sigma(7)) = \boxed{(7\,5)(2\,8\,3)(1\,4)}$.
  - Likewise, $\tau\sigma\tau^{-1} = (\tau(1)\,\tau(7)\,\tau(4)\,\tau(8)\,\tau(6)) = \boxed{(5\,6\,3\,8\,7)}$.

- Example: Show that $\sigma_1 = (1\,4\,3\,8)(2\,5\,6)$ and $\sigma_2 = (1\,2\,6)(3\,7\,4\,5)$ are conjugate inside S_8, and find an explicit permutation τ with $\sigma_2 = \tau\sigma_1\tau^{-1}$.
  - From the procedure given in the proposition, and making sure to include the 1-cycles, we can write the two permutations with cycles in corresponding order, as $\sigma_1 = (1\,4\,3\,8)(2\,5\,6)(7)$ and $\sigma_2 = (3\,7\,4\,5)(1\,2\,6)(8)$.
  - Then, for example, the permutation τ with $\tau(1) = 3$, $\tau(4) = 7$, $\tau(3) = 4$, $\tau(8) = 5$, $\tau(2) = 1$, $\tau(5) = 2$, $\tau(6) = 6$, and $\tau(7) = 8$ will have $\sigma_2 = \tau\sigma_1\tau^{-1}$. The cycle decomposition of this permutation τ is $\boxed{(1\,3\,4\,7\,8\,5\,2)}$.

- We record some useful general properties of the conjugation action:
- Proposition (Properties of Conjugation): Let G be a group acting on its set of elements by conjugation.

1. For any $g \in G$, the conjugation-by-g map $\varphi_g : G \to G$ is a group isomorphism, with inverse $\varphi_g^{-1} = \varphi_{g^{-1}}$. In particular, all elements in a given conjugacy class have the same order.
   - Proof: We have $\varphi_g(ab) = g(ab)g^{-1} = (gag^{-1})(gbg^{-1}) = \varphi_g(a)\varphi_g(b)$ so φ_g is a group homomorphism.
   - Furthermore, since $\varphi_{g^{-1}}(\varphi_g(a)) = g^{-1}[gag^{-1}](g^{-1})^{-1} = g^{-1}gag^{-1}g = a$ we see that $\varphi_{g^{-1}} \circ \varphi_g$ is the identity map; similarly $\varphi_{g^{-1}} \circ \varphi_g$ is also the identity, so φ_g is an isomorphism.
   - The second statement follows from the fact that group isomorphisms preserve orders of elements.
2. If S is any subset of G, then the stabilizer of S under the conjugation action of G is the normalizer $N_G(S) = \{g \in G : gSg^{-1} = S\}$. The number of conjugates of S in G is $[G : N_G(S)]$, the index of the normalizer.
   - We will remark that the normalizer $N_G(S)$ is also equal to the normalizer $N_G(\langle S \rangle)$ of the subgroup generated by S, the normalizer of any subgroup H contains H, and that a subgroup is normal in G if and only if its normalizer is all of G.
   - Proof: By definition, $g \in G$ stabilizes S under conjugation precisely when $gSg^{-1} = S$.
   - The second statement is an immediate consequence of the orbit-stabilizer theorem.
3. If a is any element of G, the stabilizer of S under the conjugation action of G is the centralizer $C_G(a) = \{g \in G : gag^{-1} = a\}$, the set of elements of G commuting with a. The number of conjugates of a in G is $[G : C_G(a)]$, the index of the centralizer.

- Proof: This is simply (2) applied to the set $S = \{a\}$.

4. (Class Equation) If G is a finite group and $g_1, \dots, g_d$ are representatives of the non-central conjugacy classes of G, then $\#G = \#Z(G) + \sum_{i=1}^{d} [G : C_G(g_i)]$.
   - Proof: As we noted above, the distinct conjugacy classes of G partition G, since they are equivalence classes of an equivalence relation.
   - As we also remarked above, each element of the center $Z(G)$ is its own conjugacy class.
   - The remaining conjugacy classes, by hypothesis, are represented by the elements $g_1, \dots, g_d$. By (3), the number of elements in the conjugacy class of g_i is equal to $[G : C_G(g_i)]$.
   - Thus, summing the sizes of all conjugacy classes yields $\#Z(G) + \sum_{i=1}^{d} [G : C_G(g_i)]$, which is also $\#G$.

- As a consequence of the class equation, we can deduce two important facts about p-groups:

- Proposition (Centers of p-Groups): If p is a prime and P is a finite p-group (i.e., a finite group whose order is a power of p), then $\#Z(P) > 1$.
  - Proof: By the class equation, if $g_1, \dots, g_d$ are representatives of the non-central conjugacy classes of P, then $\#P = \#Z(P) + \sum_{i=1}^{d} [P : C_P(g_i)]$.
  - Since the centralizer $C_P(g_i)$ is a subgroup of P, by Lagrange's theorem its order and index are both powers of p. Furthermore, since each g_i is by hypothesis non-central, this means $C_P(g_i)$ is a proper subgroup of P, and so its index is greater than 1.
  - Thus, each term in the sum $\sum_{i=1}^{d} [P : C_P(g_i)]$ is a multiple of p. Since $\#P$ is also a multiple of p, this means $\#Z(P) = \#P - \sum_{i=1}^{d} [P : C_P(g_i)]$ is also a multiple of p. Hence it cannot be equal to 1, so $\#Z(P) > 1$.

- Corollary (Groups of Order p^2): If p is a prime, then every group of order p^2 is abelian. Moreover, there are two such groups, up to isomorphism: $\mathbb{Z}/p^2\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.
  - Proof: Suppose G has order p^2. By Lagrange's theorem, every nonidentity element of G must have order p or p^2.
  - If there is an element of order p^2, then G is cyclic and isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$.
  - Now suppose every element has order p. By the proposition above, $Z(G)$ is not trivial, so suppose $g \in Z(G)$ has order p.
  - Then $N = \langle g \rangle$ is a normal subgroup of G, since $g \in Z(G)$. Observe that G/N has order $\#G/\#N = p$, and is therefore cyclic of order p. Suppose G/N is generated by $\overline{h}$: then every coset in G/N has the form $\overline{h}^a$ for some $a \in \{0, 1, \dots, p-1\}$ and so every element of G has the form $h^a g^b$ for some $a, b \in \{0, 1, \dots, p-1\}$.
  - Now consider the map $\varphi : (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \to G$ that maps $(a, b) \mapsto h^a g^b$. Furthermore, since $g \in Z(G)$, we have $gh = hg$, and since $g^p = h^p = e$ by the assumption that g and h have order p, this map is a well-defined group homomorphism since it is clearly multiplicative and g and h satisfy the same relations as the generators of $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ do.
  - But since there are p^2 elements of the form $h^a g^b$ and G has p^2 elements, φ is onto hence a bijection, hence an isomorphism.
  - In both cases, we see that G is abelian, and it is either isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ or to $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$, as claimed.

3.4 The Structure of Finite Groups

- In this section we will give a brief overview of some additional results that allow us to gain a better understanding of the structure of finite groups: the structure theorem for finitely-generated abelian groups, Sylow's theorems, and some remarks about direct and semidirect products.

3.4.1 Finitely-Generated Abelian Groups

- Our goal in this section is to establish a classification theorem for finitely generated abelian groups.
  - As a matter of fact, we will establish two different variations on the theorem, each of which has utility in different circumstances.
- Our classification, broadly stated, is as follows:
- Theorem (Finitely Generated Abelian Groups): If G is a finitely generated abelian group, then G is isomorphic to a direct product of cyclic groups.
  - As a pair of illustrations, we have $\mathbb{Z}/120\mathbb{Z} \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$ and $(\mathbb{Z}/64\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/16\mathbb{Z})$.
  - The main idea of the proof is to consider the various relations among the generators, and then use essentially the same procedure as the one used for row-reducing a matrix to convert the relations into an essentially diagonal form. We can then see immediately that the resulting diagonalized form corresponds to a direct product of cyclic groups, as claimed.
  - The approach we give is really a special case of the general classification of modules over principal ideal domains, and essentially the same method can be adapted to prove that more general classification.
- To prove this theorem, we first establish a lemma:
- Lemma: If G is a finitely generated abelian group, then G is finitely presented. In other words, G has a presentation with finitely many generators and finitely many relations.
  - The content here is that any collection of relations between the generators can always be reduced to a finite set.
  - Proof: We use induction on the number of generators n.
  - For the base case $n = 1$, we appeal to our characterization of cyclic groups, which can all be described using at most one relation.
  - For the inductive step, suppose any abelian group with n generators is finitely presented, and suppose G is abelian and has $n + 1$ generators $g_1, \dots, g_n, h$, where we write G as an additive group.
  - Since G is abelian, any such relation has the form $ah + b_1 g_1 + \cdots + b_n g_n = 0$ for some $a, b_i \in \mathbb{Z}$.
  - Consider the set of all possible tuples $(a, b_1, \dots, b_n) \in \mathbb{Z}^{n+1}$ for all possible relations between $h, g_1, \dots, g_n$. This set is a subgroup of $\mathbb{Z}^{n+1}$ since it contains the zero vector and is closed under subtraction, since the difference of two relations is also a relation.
  - Then the set of first coordinates of these tuples (i.e., the possible coefficients of h in all possible relations) is a subgroup of $\mathbb{Z}$.
  - If the subgroup is the trivial subgroup (0), then h does not appear in any relations: thus, all relations involve elements in the subgroup $\langle g_1, \dots, g_n \rangle$, and so by the inductive hypothesis we may reduce the collection to a finite set.
  - Otherwise, suppose the subgroup is $d\mathbb{Z}$ with $d > 0$. Then there exists a relation of the form $dh + e_1 g_1 + \cdots + e_n g_n = 0$, and the coefficient of h in every other relation is a multiple of d. We may then eliminate h from every other relation by subtracting an appropriate multiple of this relation.
  - Then, just as above, all of the remaining relations lie in the subgroup $\langle g_1, \dots, g_n \rangle$, so by the inductive hypothesis we may reduce the collection to a finite set. Adjoining the relation $dh + e_1 g_1 + \cdots + e_n g_n = 0$ then yields a finite set of relations that generate all relations, as claimed.
- We can now give the proof of one version of the theorem, using a similar idea as that used in the lemma:
- Theorem (Finitely Generated Abelian Groups, Invariant Factor Form): If G is a finitely generated abelian group, then there exists a nonnegative integer r (the rank of the group G) and a list of positive integers $a_1, \dots, a_k$ with $a_1 | a_2 | \cdots | a_k$ such that $G \cong \mathbb{Z}^r \times (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_k\mathbb{Z})$.
  - The terms in this decomposition of G are called the invariant factors of G. We will shortly establish that they are unique.

- $\circ$ Proof: Suppose G is a finitely generated abelian group, written additively.
- $\circ$ By the lemma, G has a presentation with finitely many generators and finitely many relations: suppose the generators are $g_1, \dots, g_n$ and the relations are $r_i : a_{1,i}g_1 + \cdots + a_{1,n}g_n = 0$ for each $1 \leq i \leq m$.
- $\circ$ Then we obtain a "relations matrix" $A = \{a_{i,j}\}_{1 \leq i \leq m, 1 \leq j \leq n}$.
- $\circ$ We may perform various elementary row and column operations on the relations matrix: specifically, we may interchange two rows or columns, we may negate a row of column, and we may add a scalar multiple of one row or column to another.
- $\circ$ The elementary row operations correspond to performing the corresponding operations on the relations, while the elementary column operations correspond to performing the corresponding relations on the generators (i.e., by making a change of generators). Note that none of the listed operations changes the isomorphism type of G.
- $\circ$ We can then perform the Euclidean algorithm on the upper left entry of A with the other entries in the first row, and then the first column, to obtain a matrix of the form $A' = \begin{pmatrix} c_1 & 0 & \cdots & 0 \\ 0 & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_{m,2} & \cdots & b_{m,n} \end{pmatrix}$.
- $\circ$ Now we repeat the procedure on the smaller matrix $\begin{pmatrix} b_{2,2} & \cdots & b_{2,n} \\ \vdots & \ddots & \vdots \\ b_{m,2} & \cdots & b_{m,n} \end{pmatrix}$, and continue until we are left with a "diagonal" matrix $D = \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_l \end{pmatrix}$, possibly with zero entries in the (i,i)-terms.
- $\circ$ We can then copy $c_2, \dots, c_l$ into the top row of the matrix and perform the Euclidean algorithm on them to place the resulting gcd a_1 in the upper-left entry, and then remove the rest of the entries in the top row. By construction, we see that a_1 divides all of the entries of the matrix.
- $\circ$ Repeating this procedure gives a relations matrix $D' = \begin{pmatrix} a_1 & & & & \\ & \ddots & & & \\ & & a_k & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$, where $a_1 | a_2 | \cdots | a_k$.
- $\circ$ Therefore, since each step does not change the isomorphism type of G, we see that G is isomorphic to the group with presentation $\langle h_1, \dots, h_n \,|\, h_1^{a_1} = e, \, \dots, h_k^{a_k} = e \rangle$, which is a presentation of $(\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_k\mathbb{Z}) \times \mathbb{Z}^{n-k}$.
- $\circ$ Thus, G is isomorphic to a direct product of cyclic groups of the claimed form.

- To illustrate the procedure, suppose $G = \langle x, y, z | -6x + 3y = 0, \, 10x + 5y = 0 \rangle$.
  - $\circ$ Then the relations matrix is $\begin{bmatrix} -6 & 3 & 0 \\ 10 & 5 & 0 \end{bmatrix}$. Now we use row and column operations:

$$\begin{bmatrix} -6 & 3 & 0 \\ 10 & 5 & 0 \end{bmatrix} \xrightarrow{C_1+2C_2} \begin{bmatrix} 0 & 3 & 0 \\ 20 & 5 & 0 \end{bmatrix} \xrightarrow[R_2-2R_1]{C_1 \leftrightarrow C_2} \begin{bmatrix} 3 & 0 & 0 \\ -1 & 20 & 0 \end{bmatrix} \xrightarrow{R_1+3R_2} \begin{bmatrix} 0 & 60 & 0 \\ -1 & 20 & 0 \end{bmatrix} \xrightarrow{R_1 \leftrightarrow -R_2} \begin{bmatrix} 1 & -20 & 0 \\ 0 & 60 & 0 \end{bmatrix} \xrightarrow{C_2+20C_1} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 60 & 0 \end{bmatrix}.$$

  - $\circ$ The relations matrix now has the desired form, so we can read off the presentation: it is $\langle p, q, r | p = 0, 60q = 0 \rangle$, which describes the group $\{e\} \times (\mathbb{Z}/60\mathbb{Z}) \times \mathbb{Z}$.

- We can also decompose the terms $\mathbb{Z}/n\mathbb{Z}$ into prime powers using the Chinese remainder theorem, as follows:
- Proposition (Chinese Remainder Theorem for $\mathbb{Z}$): If a and b are relatively prime integers, then $\mathbb{Z}/ab\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$. Thus, if n has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$, we have $\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})$.

- This result is a special case of the more general Chinese remainder theorem for rings, which states that if R is commutative with 1 and $I_1, I_2, \dots, I_n$ are pairwise comaximal ideals of R (i.e., with $I_i + I_j = R$ for all pairs $i \neq j$), then $R/(I_1 I_2 \cdots I_n) \cong (R/I_1) \times (R/I_2) \times \cdots \times (R/I_n)$ as rings.
- Proof: For the first part, consider the map $\varphi : \mathbb{Z} \to (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ given by $\varphi(n) = (n \bmod a,\ n \bmod b)$.
- This map is easily seen to be a ring homomorphism, and its kernel consists of the elements $n \in \mathbb{Z}$ divisible by both a and b. Since a and b are relatively prime, this means $\ker \varphi = ab\mathbb{Z}$.
- Thus, by the first isomorphism theorem, we obtain an injective ring homomorphism $\tilde{\varphi} : \mathbb{Z}/ab\mathbb{Z} \to (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$.
- But since $\mathbb{Z}/ab\mathbb{Z}$ and $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ both have cardinality ab, the map is also surjective, hence is an isomorphism.
- The second part follows by a trivial induction using the fact that the prime powers $p_i^{a_i}$ in the prime factorization of $n = p_1^{a_1} \cdots p_k^{a_k}$ are relatively prime.

- By decomposing each of the cyclic $\mathbb{Z}/n\mathbb{Z}$ factors from the invariant factor decomposition, we see that any finitely generated abelian group decomposes as a direct product of copies of $\mathbb{Z}$ with $\mathbb{Z}$ modulo prime powers:
- Theorem (Finitely Generated Abelian Groups, Elementary Divisor Form): If G is a finitely generated abelian group, then there exists a unique nonnegative integer r and a unique list of prime powers $p_i^{a_i}$ such that $G \cong \mathbb{Z}^r \times (\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})$.
  - Proof: The existence follows immediately from decomposing each of the $\mathbb{Z}/n\mathbb{Z}$ terms from the invariant factor decomposition into prime powers.
  - For the uniqueness, first regroup the terms in the direct product to collect identical factors together, as $G \cong \mathbb{Z}^r \times (\mathbb{Z}/p_1\mathbb{Z})^{b_{1,1}} \times (\mathbb{Z}/p_1^2\mathbb{Z})^{b_{1,2}} \times \cdots \times (\mathbb{Z}/p_1^{r_1})^{b_{1,r_1}} \times (\mathbb{Z}/p_2\mathbb{Z})^{b_{2,1}} \times \cdots \times (\mathbb{Z}/p_k^{r_k}\mathbb{Z})^{b_{k,r_k}}$ for some nonnegative integers $b_{i,j}$.
  - For any integer m, observe that the mth-power map φ_m on G is a group homomorphism from G to G since G is abelian. The kernel of φ_m consists of all elements of order dividing m in G.
  - More explicitly, for a prime power p^d, we can see that the elements in the kernel of φ_{p^d} are the identity in all components with primes $p_i \neq p$, and if the p-power component of G is $(\mathbb{Z}/p\mathbb{Z})^{b_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{b_2} \times \cdots \times (\mathbb{Z}/p^{r_1})^{b_r}$, then the elements in the kernel are $(\mathbb{Z}/p\mathbb{Z})^{b_1} \times (\mathbb{Z}/p^2\mathbb{Z})^{b_2} \times \cdots \times (\mathbb{Z}/p^d)^{b_d} \times (p\mathbb{Z}/p^{d+1}\mathbb{Z})^{b_{d+1}} \times (p^2\mathbb{Z}/p^{d+2}\mathbb{Z})^{b_{d+1}} \times \cdots \times (p^{r_1-d}\mathbb{Z}/p^{r_1}\mathbb{Z})^{b_r}$.
  - In other words, we obtain all of the elements in the copies of $\mathbb{Z}/p\mathbb{Z}$, ... , $\mathbb{Z}/p^{r_d}\mathbb{Z}$, but for higher powers of p we only get the elements of order dividing p^d in those copies.
  - Then the order of $\ker(\varphi_{p^d})$ is equal to the product of the orders of each of the terms given. It is not hard to see that the quotient $\ker(\varphi_{p^d})/\ker(\varphi_{p^{d+1}})$ is trivial in all components of the direct product except for the terms $\mathbb{Z}/p^k\mathbb{Z}$ with $k \geq d$, where it yields a copy of $\mathbb{Z}/p\mathbb{Z}$.
  - Therefore, by computing the order of each quotient $\ker(\varphi_{p^d})/\ker(\varphi_{p^{d+1}})$, we can determine the number of terms $\mathbb{Z}/p^k\mathbb{Z}$ in the direct product with $k \geq d$ for each positive integer d. This uniquely determines all of the $\mathbb{Z}/p^i\mathbb{Z}$ components in terms of the group structure of G.
  - Furthermore, if p is a prime not appearing in any of the prime-power components, we can see that G/pG is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$, so the rank r is also uniquely determined.
- The argument we gave establishes the uniqueness of the elementary divisors, and (with appropriate minor modification) also gives the uniqueness of the invariant factors.
  - Given the invariant factors, it is easy to find the elementary divisors, since we need only find the prime-power factorizations of the invariant factors and then break the terms apart using the Chinese remainder theorem as described above.
  - If we have a decomposition into elementary divisor form, we can reconstruct the invariant factor form recursively: the largest invariant factor is the product of the largest power of each prime, then the next largest invariant factor is the product of the largest remaining power of each prime, and so forth.
- Example: Find the elementary divisor form of $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/240\mathbb{Z})$.

- We simply break each term into prime powers. Since $6 = 2 \cdot 3$ and $240 = 2^4 \cdot 3 \cdot 5$ this yields $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$ and $\mathbb{Z}/240\mathbb{Z} \cong (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$.
- Thus, the elementary divisor form of $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/240\mathbb{Z})$ is $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$.

- Example: Find the invariant factor form of $(\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/16\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/125\mathbb{Z})$.
  - The prime powers are $2^4, 2^4$, 3, and $5^3, 5, 5$.
  - The largest factors are $2^4 \cdot 3 \cdot 5^3 = 6000$. Then the largest remaining factors are $2^4 \cdot 1 \cdot 5 = 80$, and the largest factors after those are $1 \cdot 1 \cdot 5 = 5$.
  - Since we have exhausted all factors, we have found all of the invariant factors, and the invariant factor form is $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/80\mathbb{Z}) \times (\mathbb{Z}/6000\mathbb{Z})$.

- Example: Classify the abelian groups of order 36 up to isomorphism, in both elementary divisor form and invariant factor form.
  - We first make a list of possible elementary divisors. Since $36 = 2^2 3^2$ we only need to work with the primes 2 and 3.
  - The possible cyclic factors for $p = 2$ are $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, while the possible cyclic factors for $p = 3$ are $\mathbb{Z}/9\mathbb{Z}$ and $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.
  - Thus, since all combinations are possible and distinct, we see that there are 4 abelian groups of order 36, and their elementary divisor forms are $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z})$, $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z})$, and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.
  - To convert these into invariant factor form, we follow the procedure described above to obtain the invariant factor forms $\mathbb{Z}/36\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/18\mathbb{Z})$, and $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$.

3.4.2 Sylow's Theorems

- We continue our analysis of the structure of finite groups: specifically, about the subgroups that a given group must possess.
  - If G has order n, then by Lagrange's theorem, the order of any subgroup of G must divide n.
  - From the classification of finitely generated abelian groups, it is not hard to see that if G is abelian, then G has a subgroup of order d for every divisor d of n.
  - However, if G is non-abelian, then it is not the case that there necessarily exists a subgroup of order d for every d dividing n: we saw explicitly that A_4, of order 12, has no subgroup of order 6. (A_4 does contain subgroups of orders 1, 2, 3, 4, and 12.)
  - Indeed, by Cauchy's theorem, if p is a prime dividing n, then G necessarily contains an element of order p, which will then generate a subgroup of G of order p.
  - What we will do now is extend this result by showing that if p^d is a prime power dividing the order of G, then in fact G must possess a subgroup of order p^d.

- First, some terminology:
- Definition: If p is a prime, a p-group is a group whose order is a power of p.
  - For example, $\mathbb{Z}/64\mathbb{Z}$, $D_{2 \cdot 4}$, and Q_8 are 2-groups, while $\mathbb{Z}/25\mathbb{Z}$ is a 5-group.

- Definition: If G is a group and p is a prime, a subgroup of G that is a p-group is called a p-subgroup of G. If p^d is the largest power of p dividing $\#G$, then a p-subgroup of G of order p^d is called a Sylow p-subgroup of G.
  - Remark: Some authors, at times, refer to Sylow p-subgroups as p-Sylow subgroups.
  - If p^d is the largest power of p dividing $\#G$, then p^d is the largest possible order of a p-subgroup of G, by Lagrange's theorem. A Sylow p-subgroup, therefore, is a p-subgroup of G of the maximum possible size.

- Example: S_4 contains a subgroup $H = \langle (1\,2\,3\,4),\, (2\,4) \rangle$ isomorphic to the dihedral group $D_{2\cdot 4}$ of order 8. Since $\#S_4 = 24 = 2^3 \cdot 3$, this subgroup H is a Sylow 2-subgroup of S_4.
- Example: The subgroup $\langle 4 \rangle$ of $\mathbb{Z}/36\mathbb{Z}$, which has order 9, is a Sylow 3-subgroup of $\mathbb{Z}/36\mathbb{Z}$. There is also a unique Sylow 2-subgroup of $\mathbb{Z}/36\mathbb{Z}$: the subgroup $\langle 9 \rangle$, which has order 4.

- Example: Identify all of the Sylow subgroups of A_5.
  - Note that A_5 has order $5!/2 = 60 = 2^2 \cdot 3 \cdot 5$. Therefore, the Sylow 2-subgroups have order 4, the Sylow 3-subgroups have order 3, and the Sylow 5-subgroups have order 5.
  - Observe that $\langle (1\,2)(3\,4),\, (1\,3)(2\,4) \rangle$ is a subgroup of order 4 inside A_5, isomorphic to the Klein 4-group, so it is a Sylow 2-subgroup. In fact, there are 5 of these subgroups inside A_5, obtained by fixing one point and taking the Klein 4-subgroup of the resulting subgroup isomorphic to A_4. Explicitly, they are $\langle (1\,2)(3\,5),\, (1\,3)(2\,5) \rangle$, $\langle (1\,2)(4\,5),\, (1\,4)(2\,5) \rangle$, $\langle (1\,3)(4\,5),\, (1\,4)(3\,5) \rangle$, and $\langle (2\,3)(4\,5),\, (2\,4)(3\,5) \rangle$. In fact, these are all of the Sylow 2-subgroups, because the only elements of A_5 with order dividing 4 are the 2,2-cycles, and it is not hard to see that these are the only 2-groups that can be formed from them.
  - Likewise, the Sylow 3-subgroups are generated by 3-cycles. Since there are $5 \cdot 4 \cdot 3/3 = 20$ 3-cycles, and each Sylow 3-subgroup contains 2 different ones, there are 10 Sylow 3-subgroups.
  - Finally, the Sylow 5-subgroups are generated by 5-cycles. Since there are $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1/5 = 24$ 5-cycles, and each Sylow 5-subgroup contains 4 different ones, there are 6 Sylow 5-subgroups.

- It is not obvious that Sylow p-subgroups exist. This fact, and substantially more, is the content of the following results of Sylow:

- Theorem (Sylow's Theorems): Suppose that G is a finite group, p is a prime, and p^d is the largest power of p dividing the order of G. Then the following hold:
  1. G contains a Sylow p-subgroup.
  2. If P is any Sylow p-subgroup of G and Q is any p-subgroup of G, then Q is contained in some conjugate of P (and thus, Q is contained in a Sylow p-subgroup of G). As a consequence, all Sylow p-subgroups of G are conjugate in G (so in particular, they are all isomorphic).
  3. If n_p denotes the number of Sylow p-subgroups, then $n_p \equiv 1 \pmod{p}$. Furthermore, $n_p = [G : N_G(P)]$ where P is any Sylow p-subgroup of G, and so as a consequence, n_p is a divisor of $\#G/p^d$.

- We will prove each piece separately. Each of our arguments will use our results on group actions in a fundamental way.
  - Proof (Sylow 1): We induct on the order n of G. The base case $n = 1$ is trivial.
  - For the inductive step, let p be a prime and suppose any group of order strictly less than n has a Sylow p-subgroup.
  - Recall that the class equation in G says that $\#G = \#Z(G) + \sum_{i=1}^{e} [G : C_G(g_i)]$, where the $g_1, \dots, g_e$ are representatives of the non-central conjugacy classes of G and $Z(G)$ is the center of G.
  - If p divides $\#Z(G)$, then by Cauchy's theorem, $Z(G)$ has an element of order p, which then generates a normal subgroup N of G of order p. (The subgroup is normal because it is contained in $Z(G)$.)
  - Then G/N is a group of order n/p, so by the inductive hypothesis it has a Sylow p-subgroup $\overline{P}$, which is necessarily of order p^{d-1}.
  - Then by the lattice isomorphism theorem, the subgroup P of G containing N with $P/N = \overline{P}$ (i.e., the preimage of $\overline{P}$ under the projection map from G to G/N) has order $\#\overline{P} \cdot \#N = p^{d-1} \cdot p = p^d$ in G. Thus, P is a Sylow p-subgroup of G.
  - Now suppose that p does not divide $\#Z(G)$. Then since p divides $\#G$, at least one of the terms $[G : C_G(g_i)]$ must not be divisible by p.
  - Let $H = C_G(g_i)$. Since $[G : H]$ is not divisible by p, the order of H is divisible by p^d, and also because g_i is not in the center of G, H is a proper subgroup of G.
  - Thus, by the induction hypothesis, H has a Sylow p-subgroup P of order p^d: then P is also a Sylow p-subgroup of G.

- In either case, we see that G has a Sylow p-subgroup, as claimed.

- For the next part of the proof, we first establish a lemma about actions of p-groups:

- Lemma (Fixed-Point Congruence for p-Group Actions): Let p be a prime and suppose P is a p-group acting on a finite set A. Then $\#A \equiv \#\text{Fix}_P(A) \bmod p$, where $\text{Fix}_P(A)$ denotes the number of fixed points of P on A (in other words, the number of $a \in A$ such that $g \cdot a = a$ for all $g \in P$).

  - Proof: By the orbit-stabilizer theorem, the size of the orbit of any $a \in A$ is equal to $[P : P_a]$, the index of the stabilizer P_a of a, which is a divisor of $\#P$ by Lagrange's theorem.
  - Therefore, any orbit either has size 1, or has size divisible by p since P is a p-group. Note that $a \in A$ has an orbit of size 1 if and only if its stabilizer P_a is all of P, which is equivalent to saying that a is a fixed point of P.
  - Since the orbits partition A, this means that $\#A$ is equal to the total number of fixed points (the orbits of size 1) plus a multiple of p (the other orbits), and so $\#A \equiv \#\text{Fix}_P(A) \bmod p$ as desired.
  - Remark: This argument we gave to prove Cauchy's theorem is an application of this lemma to the cyclic permutation action of $\mathbb{Z}/p\mathbb{Z}$ on ordered p-tuples $(g_1, \dots, g_p)$ with $g_1 \cdots g_p = 1$.

- We now continue with the proof of Sylow's theorems:

  - Proof (Sylow 2): Let P be any Sylow p-subgroup of G and Q be any p-subgroup of G.
  - Observe that Q acts on the left cosets of P by left multiplication: explicitly, the action is $g \cdot (hP) = (gh)P$ for any $g \in Q$ and left coset hP of P.
  - Therefore, since Q is a p-group, by the lemma above, we see that the number of fixed points of this action is congruent to the number of left cosets $[G : P]$ modulo p.
  - But since P is a Sylow p-subgroup of G, the index $[G : P]$ is relatively prime to p, so the number of fixed points is nonzero.
  - Suppose that hP is a fixed point: this means $g \cdot (hP) = hP$ for all $g \in Q$, which is to say, $ghP = hP$. Equivalently, $gh \in hP$ for all $g \in Q$, which is to say, $Q \subseteq hPh^{-1}$. Thus, Q is contained in a conjugate of P as claimed.
  - For the second part, if Q is now any other Sylow p-subgroup, we see $Q \subseteq hPh^{-1}$ as above, but since Q and hPh^{-1} have the same cardinality, they must be equal: thus, P and Q are conjugate.

- Finally, we establish the last part of Sylow's theorems:

  - Proof (Sylow 3): Let P be a Sylow p-subgroup of G and take A to be the set of all Sylow p-subgroups of G.
  - Observe that P acts on A by conjugation: explicitly, the action is $g \cdot Q = gQg^{-1}$ for any $g \in P$ and any Sylow p-subgroup Q of G.
  - Therefore, since P is a p-group, by the lemma above, we see that the number of fixed points of this action is congruent modulo p to the number of Sylow p-subgroups of G. We will show that this action has a single fixed point: namely, P.
  - So suppose that Q is a fixed point: then $gQg^{-1} = Q$ for all $g \in P$, meaning that $P \leq N(Q)$. Since Q is a subgroup, $Q \leq N(Q)$ as well.
  - Notice that P and Q are then both Sylow p-subgroups of $N(Q)$, and so (2) applied to $N(Q)$ shows that P and Q are conjugate inside $N(Q)$. However, by definition Q is a normal subgroup of $N(Q)$, since all elements of $N(Q)$ normalize Q, and so the only possibility is to have $P = Q$.
  - Thus, P is the only fixed point of the conjugation action on A, and so the number n_p of Sylow p-subgroups is congruent to 1 modulo p as claimed.
  - For the last statement, consider the conjugation action of G on the set of its Sylow p-subgroups. The stabilizer of P under this action is the set of $g \in G$ such that $gPg^{-1} = P$, which is the normalizer $N_G(P)$ of P in G.

- Therefore, since all Sylow p-subgroups are conjugate by (2), the size of the orbit of P is n_p, which by the orbit-stabilizer theorem is also equal to $[G : N_G(P)]$. This is a divisor of $\#G$ by Lagrange's theorem, and since it is relatively prime to p, it must in fact divide $\#G/p^d$.

- Sylow's theorems are very useful for obtaining additional structural information about groups of a given order.
  - The first step is to make a list of all of the possible Sylow numbers (i.e., candidates for the numbers n_p of Sylow p-subgroups for each prime p dividing the order of G).
  - We can then try to exploit this information to pin down more of the group structure.
  - In particular, if we can show that a particular Sylow number n_p must be equal to 1, then we know the resulting Sylow p-subgroup must be normal.
  - This follows from Sylow (3): if P is the Sylow p-subgroup, then $n_p = [G : N_G(P)]$, so $n_P = 1$ if and only if $N_G(P) = G$, which is to say, when P is a normal subgroup of G.
  - Even when n_p is not necessarily equal to 1, it is often still useful to consider $N_G(P)$, since it is another subgroup of G whose order we know if we know n_p.

- Example: If G is a group of order 45, find the possible Sylow numbers of G and identify the possible structures of the Sylow subgroups of G.
  - Since $45 = 3^2 \cdot 5$ we see that n_3 is a divisor of 5 that is congruent to 1 modulo 3. The only such divisor is 1, so $n_3 = 1$ and there is a unique Sylow 3-subgroup of G, which has order $3^2 = 9$.
  - From our characterization of groups of order p^2, the Sylow 3-subgroup is isomorphic either to $\mathbb{Z}/9\mathbb{Z}$ or to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$.
  - Likewise, n_5 is a divisor of 9 that is congruent to 1 modulo 5, but the only such divisor is 1. Thus, $n_5 = 1$ also. This means that there is a unique Sylow 5-subgroup, which has order 5 and is thus isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

- Example: If G is a group of order 60, find the possible Sylow numbers of G and identify the possible structures of the Sylow subgroups of G.
  - Since $60 = 2^2 \cdot 3 \cdot 5$ we see that n_2 is a divisor of 15 that is odd. Thus, we have $n_2 \in \{1, 3, 5, 15\}$, and since a Sylow 2-subgroup has order 4, it is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
  - Likewise, n_3 is a divisor of $2^2 \cdot 5 = 20$ that is congruent to 1 modulo 3. This means $n_3 \in \{1, 10\}$ and since a Sylow 3-subgroup has order 3, it is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.
  - Finally, n_5 is a divisor of $2^2 \cdot 3 = 10$ that is congruent to 1 modulo 5. This means $n_5 \in \{1, 6\}$ and since a Sylow 5-subgroup has order 5, it is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

- By identifying the possible Sylow numbers for a given group order, we can sometimes prove that a group of that order cannot be simple:

- Example: Show that a group G of order 1375 cannot be simple.
  - Notice that $1375 = 5^3 \cdot 11$. Then n_5 is a divisor of 11 congruent to 1 modulo 5, so $n_5 \in \{1, 11\}$.
  - Also, n_{11} is a divisor of 5^3 congruent to 1 modulo 11. But the only such divisor is 1, meaning $n_{11} = 1$.
  - But then because $n_{11} = 1$, by our results above this means that the unique Sylow 11-subgroup is normal, and thus G cannot be simple.

- Frequently, the congruence conditions do not immediately force the existence of a normal Sylow subgroup. But sometimes we can count elements in these various Sylow subgroups and show that having all of the Sylow numbers be large would force the group to have too many elements.

- Example: Show that a group G of order 105 cannot be simple.
  - Notice that $105 = 3 \cdot 5 \cdot 7$. Thus, $n_3 \equiv 1 \bmod 3$ and divides $5 \cdot 7$, so must be among $\{1, 5, 7, 35\}$. The only possibilities are $n_3 \in \{1, 7\}$.

- Likewise, $n_5 \equiv 1 \bmod 5$ and divides $3 \cdot 7$, so must be among $\{1, 3, 7, 21\}$. The only possibilities are $n_5 \in \{1, 21\}$.
- Finally, $n_7 \equiv 1 \bmod 7$ and divides $3 \cdot 5$, so must be among $\{1, 3, 5, 15\}$. The only possibilities are $n_7 \in \{1, 15\}$.
- If any of n_3, n_5, and n_7 equals 1, then the corresponding Sylow subgroup is normal and then G is not simple.
- A priori it may seem that we could have $n_3 = 7$, $n_5 = 21$, and $n_7 = 15$. However, this is not actually possible: each Sylow 3-subgroup is cyclic and thus has $3 - 1 = 2$ elements of order 3.
- Each of these elements of order 3 generates the group, so all $7 \cdot (3 - 1) = 14$ of these elements must be distinct from each other.
- Likewise, there would have to be $21 \cdot (5 - 1) = 84$ elements of order 5, and $15 \cdot (7 - 1) = 90$ elements of order 7. But in total, we have identified $14 + 84 + 90 = 189$ different elements of G, and G cannot actually have this many elements.
- Therefore, we cannot have $n_3 = 7$, $n_5 = 21$, and $n_7 = 15$, so one of them must equal 1: thus G is not simple.

- Example: Show that a group G of order 132 cannot be simple.
  - Notice that $132 = 2^2 \cdot 3 \cdot 11$. Then n_2 is odd and divides $3 \cdot 11$, so $n_2 \in \{1, 3, 11, 33\}$. Likewise, $n_3 \equiv 1 \pmod 3$ and divides $2^2 \cdot 11$, so $n_3 \in \{1, 4, 22\}$, and $n_{11} \equiv 1 \pmod{11}$ and divides $2^2 \cdot 3$, so $n_{11} \in \{1, 12\}$.
  - As above, if n_3 or n_{11} equals 1, then the corresponding Sylow subgroup is normal.
  - Otherwise, we would have $n_{11} = 12$ and $n_3 \geq 4$: in this case we would obtain $12 \cdot (11 - 1) = 120$ elements of order 11 along with an additional $4 \cdot (3 - 1) = 8$ elements of order 3.
  - There are only $132 - 120 - 8 = 4$ elements remaining in the group, so since there is a Sylow 2-subgroup and it has order 4, all of the remaining elements must lie in this Sylow 2-subgroup, and there can be only one of them.
  - Thus, n_2, n_3, or n_{11} must equal 1, and so G cannot be simple.

3.4.3 Products of Subgroups

- We proved earlier that every finitely generated abelian group decomposes as a direct product of cyclic groups.
  - This result tells us that finitely generated abelian groups can be built up from subgroups by taking products.
  - We can often piece other groups together from subgroups in a similar way.
  - If H and K are subgroups of G, then we can certainly consider the subgroup $\langle H, K \rangle$ generated by H and K.
  - However, the elements in this subgroup are hard to write down in general, since they are words of arbitrary length in the elements of H and K.
  - If elements from H and K commute with one another, then by rearranging the elements in the word and using the fact that H and K are closed under multiplication, we can reduce any word to a product of the form hk for $h \in H$ and $k \in K$.
  - We will now look at the same set of elements for arbitrary subgroups.
- Definition: If H and K are subgroups of G, then the product HK is the set $HK = \{hk : h \in H, k \in K\}$.
  - The product of two subgroups is not necessarily a subgroup of G.
  - For example, for $H = \{1, (1\,2)\}$, $K = \{1, (1\,3)\}$ in $G = S_3$, the product $HK = \{1, (1\,2), (1\,3), (1\,3\,2)\}$, which is not a subgroup of G.
  - However, in some cases HK will be a subgroup: for example, with $H = \{1, (1\,2)\}$ and $K = \{1, (3\,4)\}$ in $G = S_4$, then $HK = \{1, (1\,2), (3\,4), (1\,2)(3\,4)\}$ is indeed a subgroup of G.

* Here are some properties of products of subgroups:
* Proposition (Products of Subgroups): Let G be a group and H and K be subgroups of G.

1. If H and K are finite, then $\#(HK) = \dfrac{\#H \cdot \#K}{\#(H \cap K)}$.
   * We remark that if H or K is infinite, then trivially HK is also infinite. We also emphasize that HK is not assumed to be a subgroup here.
   * Proof: Observe that HK is a union of left cosets of K: specifically: $HK = \cup_{h \in H} hK$.
   * We therefore need only count how many distinct left cosets are obtained, since each left coset has cardinality $\#K$.
   * Consider the action of H by left multiplication on the left cosets of K in HK: by definition, there is a single orbit for this action.
   * Notice that the stabilizer of the left coset eK is the set of $h \in H$ with $h \cdot eK = eK$, which is equivalent to saying $h \in K$. Thus, the stabilizer is simply the set of $h \in H$ such that $h \in K$, which is to say, it is the intersection $H \cap K$.
   * Thus, by the orbit-stabilizer theorem, the size of the orbit is equal to the index $[H : H \cap K]$. This means $\#(HK) = \#K \cdot [H : H \cap K] = \dfrac{\#H \cdot \#K}{\#(H \cap K)}$, as claimed.
2. The product HK is a subgroup of G if and only if $HK = KH$.
   * Proof: First suppose $HK = KH$ and let $g = hk$ and $g' = h'k'$ be elements of HK, with $h, h' \in H$ and $k, k' \in K$.
   * Then since $HK = KH$, the element $kh' \in KH$ is of the form $h''k''$ for some $h'' \in H$ and $k'' \in K$.
   * Then $gg' = hkh'k' = h(kh')k' = h(h''k'')k' = (hh'')(k''k') \in HK$.
   * Likewise, $g^{-1} = k^{-1}h^{-1} \in KH = HK$. Since the identity $e = ee$ is clearly in HK, this means HK is a subgroup of G.
   * Conversely, suppose HK is a subgroup. Then since H and K are both in HK, we have $\langle H, K \rangle = HK$ and so $KH \subseteq \langle H, K \rangle = HK$.
   * For the other containment, suppose $k \in K$ and $h \in H$. Then we have $h^{-1}k^{-1} \in HK$, so since HK is closed under inverses, we see $(h^{-1}k^{-1})^{-1} = kh$ must be in HK for any k, h. Thus, $HK \subseteq KH$, and so in fact $HK = KH$.
3. If $H \le N_G(K)$ or $K \le N_G(H)$, then HK is a subgroup of G.
   * Proof: Suppose $H \le N_G(K)$, and let $h \in H$ and $k \in K$.
   * By hypothesis, $hkh^{-1} \in K$, and therefore we can write $hk = (hkh^{-1})h \in KH$.
   * Thus, $hk \in KH$, and so $HK \subseteq KH$.
   * Likewise, $kh = h(hkh^{-1}) \in HK$, and so $KH \subseteq HK$.
   * We therefore have $KH = HK$, and so HK is a subgroup of G by (2).
   * The other case is essentially identical.
4. If H or K is a normal subgroup of G, then HK is a subgroup of G.
   * Proof: If H is normal in G, then $N_G(H) = G$, in which case $K \le N_G(H)$, so by (3), HK is a subgroup of G.
   * Likewise, if K is normal in G, then $H \le G = N_G(K)$, so again by (3), HK is a subgroup of G.
5. If both H and K are normal subgroups of G, and $H \cap K = \{e\}$, then HK is isomorphic to the direct product $H \times K$.
   * Remark: Under these hypotheses, we call the subgroup HK the internal direct product of H and K, and call the group $H \times K$ the external direct product of H and K. The difference is irrelevant as a practical matter, but the distinction is that the internal direct product is defined inside a group that already contains H and K as subgroups, whereas the external direct product is an explicit construction of a new group using the Cartesian product.
   * Proof: Since H is a normal subgroup of G, by (4) that means HK is a subgroup of G.
   * We first show that the elements of H commute with the elements of K.

   - To see this, observe that if $h \in H$ and $k \in K$, then $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$ is an element of K, since $hkh^{-1} \in K$ since K is normal in G.
   - But $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1})$ is also an element of H, since $kh^{-1}k^{-1} \in H$ since H is normal in G.
   - This means $hkh^{-1}k^{-1} \in H \cap K$, and so $hkh^{-1}k^{-1} = e$, meaning that $hk = kh$: thus, h and k commute.
   - Next, we claim that every element of HK can be written uniquely in the form hk with $h \in H$ and $k \in K$.
   - To see this suppose $hk = h'k'$ for $h, h' \in H$ and $k, k' \in K$. Then $(h')^{-1}h = k'k^{-1}$. But the left-hand side is an element of H while the right-hand side is an element of K, so by the assumption $H \cap K = \{e\}$, this common element must be the identity e.
   - Thus $(h')^{-1}h = e = k'k^{-1}$ and so $h' = h$ and $k' = k$, meaning h and k are unique.
   - Therefore, we have a well-defined map $\varphi : HK \to H \times K$ mapping hk to the ordered pair (h, k). It is a group homomorphism because if $g = hk$ and $g' = h'k'$ then $\varphi(gg') = \varphi(hkh'k') = \varphi(hh'kk') = (hh', kk') = \varphi(hk)\varphi(h'k') = \varphi(g)\varphi(g')$, where we used the fact that h' and k commute.
   - Finally, φ is trivially injective (since $(h, k) = (e, e)$ implies $hk = e$) and surjective (by definition of HK) and so it is an isomorphism.

6. If $n_p = 1$ for every prime p dividing $\#G$, then G is the (internal) direct product of its Sylow subgroups. Such groups are called <u>nilpotent</u> groups.
   - <u>Proof</u>: Note that the intersection of two Sylow subgroups with different primes is trivial, by Lagrange's theorem, since the order of their intersection divides the order of each group.
   - Therefore, since they are all normal since $n_p = 1$ for every prime p dividing $\#G$, by applying (5) repeatedly we see that the product of any number of the Sylow subgroups is isomorphic to their direct product.
   - In particular, since the product of all the Sylow subgroups has the same order as G, it is equal to G, and so G is isomorphic to the direct product of its Sylow subgroups.
   - <u>Remark</u>: Since abelian groups are trivially nilpotent, we could have classified finite abelian groups by using this result to reduce to the situation of classifying abelian p-groups.

- One common technique for analyzing the structure of finite groups is to start with the various Sylow subgroups, and then take various products or normalizers to construct larger subgroups in terms of these.

- <u>Example</u>: Show that every group of order 7007 is abelian, and classify them up to isomorphism.
   - We start by finding the possible Sylow numbers.
   - For a group of order $7007 = 7^2 \cdot 11 \cdot 13$, the number n_7 is congruent to 1 modulo 7 and divides $11 \cdot 13$. The only such number is 1, so $n_7 = 1$.
   - Likewise, $n_{11} \equiv 1 \pmod{11}$ and divides $7^2 \cdot 13$, but the only such divisor is 1. Similarly, the only possible value for n_{13} is 1.
   - This means all of the Sylow subgroups of G are normal, and so G is nilpotent. This means it is the direct product of its Sylow subgroups. All of these Sylow subgroups are abelian since their orders are either a prime or a square of a prime, so G is abelian.
   - Furthermore, by our classification of abelian groups, we see there are two isomorphism types for G: either $G \cong (\mathbb{Z}/49\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z}) \cong \mathbb{Z}/7007\mathbb{Z}$ or $G \cong (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/1001\mathbb{Z})$.

- For certain classes of group orders with a small number of prime divisors, we can essentially classify groups of that order using Sylow's theorems. We can illustrate by classifying the groups of order pq, where p and q are distinct primes:

- <u>Example</u> (Groups of Order pq): If p and q are primes with $p < q$ such that p does not divide $q - 1$, show that any group of order $n = pq$ is abelian and cyclic.
   - By Sylow's theorems, the number n_p divides q and is congruent to 1 modulo p. Since p does not divide $q - 1$, the only possibility is $n_p = 1$.

- Likewise, n_q divides p and is congruent to 1 modulo q, so since $p < q$ we must have $n_q = 1$.
- Therefore, both the Sylow p-subgroup and the Sylow q-subgroup are normal in G, and so G is isomorphic to their direct product.
- Since both groups are cyclic, we see $G \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z}) \cong \mathbb{Z}/pq\mathbb{Z}$ by the Chinese remainder theorem. Thus, G is cyclic as claimed.

- In the above example, if $q \equiv 1 \bmod p$, then in addition to the case $n_p = n_q = 1$ (in which case G is cyclic by the above argument) there is also another possibility, namely, $n_p = q$.
  - In this case, there are q total Sylow p-subgroups, each of which has $p-1$ elements of order p for a total of $q(p-1) = pq - q$ elements. Together with the q elements in the Sylow q-subgroup, this accounts for all of the elements in the group.
  - We have not yet shown that there actually exists such a group. However, in this hypothetical group, let P be a Sylow p-subgroup, generated by g, and Q be the Sylow q-subgroup, generated by h. We can see here that $PQ = G$ in this case by order considerations, even though G is not isomorphic to the direct product $P \times Q$.
  - Observe that g acts on the set of elements of Q by conjugation, since Q is normal in G. Thus, $ghg^{-1} = h^d$ for some positive integer d. Moreover, since g has order p, we see $h = g^p h g^{-p} = h^{d^p}$, and so $d^p \equiv 1 \pmod{q}$. This means d must be an element of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$, since d cannot equal 1 by the assumption that g and h do not commute. Note that such an element exists in $(\mathbb{Z}/q\mathbb{Z})^\times$, since $(\mathbb{Z}/q\mathbb{Z})^\times$ is cyclic (as we proved) and p divides its order $q-1$.
  - This indicates that we could take a presentation of this group as $\langle g, h \,|\, g^p = h^q = e,\ ghg^{-1} = h^d \rangle$ where d is an element of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$.
  - It may seem that we would obtain several different groups, one for each of the $p-1$ elements of order p in $(\mathbb{Z}/q\mathbb{Z})^\times$, but in fact they are all isomorphic to one another, as can be seen by changing variables from g to g^a for an appropriate value of $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.
  - To show that the presentation $\langle g, h \,|\, g^p = h^q = e,\ ghg^{-1} = h^d \rangle$ actually does describe a group of order pq, observe that by using the given relations, each element of the group is of the form $g^a h^b$ for some $a \in \{0, 1, \ldots, p-1\}$ and $b \in \{0, 1, \ldots, q-1\}$, so the order of the group is at most pq.
  - To show equality, we can give a construction of such a group, motivated by the left-multiplication action of G on the elements of Q. This action is transitive and faithful, and if we label the elements $\{e, h, h^2, \ldots, h^{q-1}\}$ of Q as $\{1, 2, \ldots, q\}$, then the permutation associated to h is $(1\,2\,3\,\ldots\,q)$, while the permutation associated to g is the product of $(q-1)/p$ p-cycles that conjugates h to h^d.
  - For example, for $p = 2$ and $q = 5$, we take $h = (1\,2\,3\,4\,5)$ and note that 2 generates $(\mathbb{Z}/5\mathbb{Z})^\times$, so we require $ghg^{-1} = h^2 = (1\,5\,4\,3\,2)$: thus we can take $g = (2\,5)(3\,4)$.
  - As another example, for $p = 3$ and $p = 7$, we take $h = (1\,2\,3\,4\,5\,6\,7)$ and note that 2 has order 3 in $(\mathbb{Z}/7\mathbb{Z})^\times$, so we require $ghg^{-1} = h^2 = (1\,3\,5\,7\,2\,4\,6)$, and so we can take $g = (2\,3\,5)(4\,7\,6)$.
  - For a more direct construction, we can take the subgroup $H = \left\{ \begin{bmatrix} x & y \\ 0 & 1 \end{bmatrix} : x, y \in \mathbb{F}_q \text{ with } x^p = 1 \right\}$ of upper-triangular matrices in $GL_2(\mathbb{F}_q)$ whose diagonal entries are $\{x, 1\}$ where $x^p = 1$.
  - Since $\mathbb{F}_q^\times$ is cyclic of order $q-1$ as we showed, and p divides $q-1$, the kernel of the pth power map has order p, so there are p possible values of x. Since there are q possible values of y, we see $\#H = pq$. This group H is generated by the elements $\tilde{g} = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ where a is a primitive pth root of unity, and $\tilde{h} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. It is not hard to see that $\tilde{g}^p = \tilde{h}^q = I_2$ and $\tilde{g}\tilde{h}\tilde{g}^{-1} = \tilde{h}^a$, so H has the desired presentation and is the unique non-abelian group of order pq up to isomorphism.

- Using similar arguments we can classify groups of order $p^2 q$ for certain values of p and q:

- Example (Groups of Order $p^2 q$): If p and q are distinct primes, show that any group G of order $p^2 q$ must have a normal Sylow p-subgroup or a normal Sylow q-subgroup. Furthermore, if p does not divide $q-1$ and $(p, q) \neq (2, 3)$, show that G must be abelian and isomorphic to $\mathbb{Z}/p^2 q\mathbb{Z}$ or to $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/pq\mathbb{Z})$.

- If $p > q$ then $n_p \in \{1, q\}$ but it cannot equal q because $q \not\equiv 1 \pmod{p}$. Thus in this case, $n_p = 1$.
- Otherwise, suppose $p < q$. Then $n_p \in \{1, q\}$ and $n_q \in \{1, p^2\}$ since $n_q \neq p$ because $p < q$ and so p cannot be congruent to 1 modulo q.
- If $n_q = p^2$ then there would be $p^2(q-1)$ elements of order q in these Sylow q-subgroups, leaving only $n - p^2(q-1) = p^2$ elements left for the Sylow p-subgroup, and so n_p would equal 1.
- Therefore, G also must have a normal Sylow subgroup in this case.
- If p does not divide $q-1$ then we cannot have $n_p = q$ so $n_p = 1$.
- Furthermore, if we had $n_q = p^2$, then $p < q$ and q divides $p^2 - 1$. But since q is prime, either q divides $p-1$ (impossible since $p < q$) or q divides $p+1$. But since $p < q$, the only possibility is that $q = p+1$. Since the only even prime is 2, this forces $p = 2$ and $q = 3$, which we specifically excluded.
- Therefore, we have $n_p = n_q = 1$, and so, as above, G is isomorphic to the direct product of its Sylow p-subgroup and its Sylow q-subgroup. Since both of these are abelian since their orders are either a prime or a square of a prime, we see that G is abelian.
- Then by the classification of finitely generated abelian groups, G is a direct product of cyclic groups, and based on its prime factorization we get the two possibilities $\mathbb{Z}/p^2q\mathbb{Z}$ and $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/pq\mathbb{Z})$ given above.

3.4.4 Semidirect Products

- We can extend the kind of analysis we made for groups of order pq, in which only one of the Sylow subgroups was normal to more general situations. Specifically, suppose we have subgroups H and K such that $G = HK$ where $H \cap K = \{e\}$, but now we only assume H is normal, not necessarily K.
  - Then since $G = HK$ and $H \cap K = \{e\}$, every element of G must be uniquely written in the form hk for $h \in H$ and $k \in K$, since the number of such products is $\#H \cdot \#K = \#G$.
  - It is no longer true, however, that elements of H will commute with elements of K, so in order to describe the multiplication in this group, we need to be able to convert a product $(h_1k_1) \cdot (h_2k_2)$ into a product of an element of H with an element of K.
  - Since $HK = G$ is a subgroup of G, we know that $HK = KH$, so the element $k_1h_2 \in KH$ must be of the form $h_3k_3 \in HK$. Then we can write $(h_1k_1) \cdot (h_2k_2) = h_1(k_1h_2)k_2 = h_1(h_3k_3)k_2 = (h_1h_3)(k_3k_2) \in HK$.
  - It is not so clear what precisely we can do to simplify this procedure.
  - However, notice that because H is normal, the elements of K act on H by conjugation: for each $k \in K$, it is true that $kHk^{-1} = H$, so for each $k \in K$, we have an associated isomorphism $\varphi_k : H \to H$ with $\varphi_k(h) = khk^{-1}$.
  - Therefore, using the notation above, we can evaluate the product $(h_1k_1) \cdot (h_2k_2)$ by noting that $k_1h_2 = \varphi_{k_1}(h_2)k_1$, and therefore $(h_1k_1) \cdot (h_2k_2) = [h_1\varphi_{k_1}(h_2)] \cdot [k_1k_2]$.
  - What we see is that if we work with ordered pairs $(h, k) \in H \times K$, then the composition operation we have is $(h_1, k_1) \star (h_2, k_2) = (h_1\varphi_{k_1}(h_2), k_1k_2)$: it behaves as normal multiplication in the K-component, but it is "twisted" by the isomorphism φ_{k_1} in the H-component.
  - For example, in the dihedral group $G = D_{2\cdot 5}$, if we take $H = \langle r \rangle = \{e, r, r^2, r^3, r^4\}$ and $K = \langle s \rangle = \{e, s\}$, then H is normal in G but K is not. The isomorphism φ_e has $\varphi_e(h) = ehe^{-1} = h$, so it is just the identity. The isomorphism φ_s has $\varphi_s(h) = shs^{-1} = h^{-1}ss^{-1} = h^{-1}$ for each $h \in H$, and so φ_s is the map taking each element of H to its inverse.
  - Indeed, using the ordered pair notation, we can then compute, for example, that $(r, s) \star (r^2, e) = (r\varphi_s(r^2), se) = (r \cdot r^{-2}, se) = (r^4, s)$, which, in regular notation inside G, reads as the statement $(rs)(r^2) = r^4s$, which is indeed true.
  - As we have noted previously, the isomorphisms of H with itself are called <u>automorphisms</u>, and the automorphisms of H will form a group under function composition, denoted $\mathrm{Aut}(H)$.
  - Furthermore, we must have $\varphi_{kk'} = \varphi_k \circ \varphi_{k'}$ for any $k, k' \in K$, since $\varphi_{kk'}(h) = (kk')h(kk')^{-1} = \varphi_k(\varphi_{k'}(h))$ for all $h \in H$. This means that the association of k to the map φ_k is actually a group homomorphism of K into $\mathrm{Aut}(H)$.

- The idea now is that we can reverse this process.
  - Explicitly, if H and K are any groups, then given a homomorphism σ of K into $\mathrm{Aut}(H)$, so that for each $k \in K$ we obtain an automorphism σ_k of H, we can use the calculation above to *define* a group operation $\star$ on ordered pairs (h, k) by taking $(h_1, k_1) \star_\sigma (h_2, k_2) = (h_1\sigma_{k_1}(h_2),\, k_1k_2)$.
  - The resulting group is called the semidirect product of H and K:
- <u>Theorem</u> (Semidirect Products): Let H and K be any groups, let $\sigma : K \to \mathrm{Aut}(H)$ be a group homomorphism with σ_k being the automorphism $\sigma(k)$ on H, and let G be the set of ordered pairs (h, k) for $h \in H$ and $k \in K$. Then G is a group with order $\#H \cdot \#K$ under the operation $(h_1, k_1) \star_\sigma (h_2, k_2) = (h_1\sigma_{k_1}(h_2),\, k_1k_2)$. Furthermore, the subset $\{(h, e) : h \in H\}$ is isomorphic to H and is a normal subgroup of G, while the subset $\{(e, k) : k \in K\}$ is isomorphic to K. This group is called the <u>semidirect product</u> of H and K with respect to σ, and is denoted $H \rtimes_\sigma K$.
  - <u>Proof</u>: Each of the assertions is a direct calculation.
  - For [G1], we have $[(h_1, k_1)\star_\sigma(h_2, k_2)]\star_\sigma(h_3, k_3) = (h_1\sigma_{k_1}(h_2),\, k_1k_2)\star_\sigma(h_3, k_3) = (h_1\sigma_{k_1}(h_2)\sigma_{k_1k_2}(h_3),\, k_1k_2k_3)$, while $(h_1, k_1) \star_\sigma [(h_2, k_2) \star_\sigma (h_3, k_3)] = (h_1, k_1) \star_\sigma (h_2\sigma_{k_2}(h_3),\, k_2k_3) = (h_1\sigma_{k_1}(h_2\sigma_{k_2}(h_3)),\, k_1k_2k_3) = (h_1\sigma_{k_1}(h_2)\sigma_{k_1}(\sigma_{k_2}(h_3)),\, k_1k_2k_3)$, and these are the same because $\sigma_{k_1k_2}(h_3) = \sigma_{k_1}(\sigma_{k_2}(h_3))$.
  - For [G2], we observe that (e, e) is the identity of G, since $(e, e) \star_\sigma (h, k) = (e\sigma_e(h),\, ek) = (h, k)$ and likewise $(h, k) \star_\sigma (e, e) = (h, k)$.
  - For [G3], the inverse of (h, k) is $(\sigma_{k^{-1}}(h^{-1}), k^{-1})$, since $(h, k)\star_\sigma(\sigma_{k^{-1}}(h^{-1}), k^{-1}) = (h\sigma_k(\sigma_{k^{-1}}(h^{-1})), kk^{-1}) = (e, e)$ and likewise $(\sigma_{k^{-1}}(h^{-1}), k^{-1}) \star_\sigma (h, k) = (e, e)$.
  - It is likewise straightforward to check that $\{(h, e) : h \in H\}$ is a normal subgroup isomorphic to H and that $\{(e, k) : k \in K\}$ is a subgroup isomorphic to K.
- The idea here is that semidirect products are somewhat like direct products (whose underlying set is also ordered pairs of elements of H and K) but have a different group operation.
  - In fact, if we take σ to be the identity map, then the semidirect product with respect to σ is simply the direct product.
  - Furthermore, we can view H and K as being embedded inside of the semidirect product $H \rtimes_\sigma K$ as the subgroups $\{(h, e) : h \in H\}$ and $\{(e, k) : k \in K\}$ respectively.
  - When we make this identification, we see that $H \cap K = \{e\}$, $G = HK$, and H is a normal subgroup of G: this is precisely the setup we started with.
  - Thus, from our discussion above, whenever we can decompose G as a product HK for two subgroups H and K with H normal in G and $H \cap K = \{e\}$, this means G must be isomorphic to a semidirect product $H \rtimes_\sigma K$ for some $\sigma : K \to \mathrm{Aut}(H)$.
  - The notation $H \rtimes_\sigma K$ is intended to evoke the direct product but also to point out the asymmetry between H (which is normal) and K (which need not be): the side of the symbol $\rtimes$ with the vertical bar identifies the subgroup that is not normal. When the map σ is clear from context, it is often omitted.
- We can use semidirect products to construct new groups of various orders.
- <u>Example</u>: Let $H = \langle a \rangle$ be cyclic of order 5 and $K = \langle b \rangle$ be cyclic of order 4.
  - Let $\sigma : K \to \mathrm{Aut}(H)$ be the homomorphism such that $\sigma_b(a) = a^2$. Note that there is such a homomorphism, because the squaring map has order 4 inside $\mathrm{Aut}(H) \cong (\mathbb{Z}/5\mathbb{Z})^\times$, which is cyclic of order 4 and generated by the element 2.
  - The resulting semidirect product $H \rtimes_\sigma K$ is a group of order 20 generated by a and b, and a, b satisfy the relations $bab^{-1} = a^2$, so this group has a presentation $\langle a, b \,|\, a^5 = b^4 = e,\, bab^{-1} = a^2 \rangle$.
  - We can construct a different semidirect product if instead we use the homomorphism $\tau : K \to \mathrm{Aut}(H)$ such that $\sigma_b(a) = a^4$. Then $H \rtimes_\sigma K$ is a group of order 20 generated by a and b, but now a, b satisfy the relations $bab^{-1} = a^4 = a^{-1}$, so this group has a presentation $\langle a, b \,|\, a^5 = b^4 = e,\, bab^{-1} = a^{-1} \rangle$.

- Both of these groups are different from the other groups of order 20 we have encountered: it is not abelian like $\mathbb{Z}/20\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/10\mathbb{Z})$, nor are they isomorphic to the dihedral group $D_{2\cdot 10}$ since the dihedral group has no elements of order 4.

- Example: Let $H = \langle a \rangle$ be cyclic of order n and $K = \langle b \rangle$ be cyclic of order 2.
  - Also let $\sigma : K \to \text{Aut}(H)$ be the map sending the nonidentity element $b \in K$ to the inversion automorphism with $\sigma_b(a) = a^{-1}$. Then the resulting semidirect product is a group of order $2n$ generated by a and b, and a, b satisfy the relations $bab^{-1} = a^{-1}$.
  - Here, we can see that the semidirect product is isomorphic to the dihedral group $D_{2\cdot n}$, with a playing the role of r and b playing the role of s.

- Example: Let p be a prime and let $H = \langle a \rangle \times \langle b \rangle$ be the direct product of two cyclic groups of order p, and let $K = \langle c \rangle$ be cyclic of order p.
  - Then H has the structure of an $\mathbb{F}_p$-vector space, and its group automorphisms will also be vector space isomorphisms. This means that $\text{Aut}(H) \cong GL_2(\mathbb{F}_p)$, with the action of a matrix being componentwise on the elements a and b.
  - Because $GL_2(\mathbb{F}_p)$ has order $(p^2 - 1)(p^2 - p)$, it has a Sylow p-subgroup of order p. We can realize this subgroup explicitly as the matrices of the form $\begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix}$ for $d \in \mathbb{F}_p$.
  - Now let $\sigma : K \to \text{Aut}(H)$ be the map with $\sigma(c) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, which is well-defined since this matrix has order p in $GL_2(\mathbb{F}_p)$. As an explicit automorphism of H, it acts as $\sigma_c(a^x, b^y) = (a^{x+y}, b^y)$. Thus, $\sigma_c(a) = a$ and $\sigma_c(b) = ab$.
  - The resulting semidirect product $H \rtimes_\sigma K$ is a non-abelian group of order p^3, and it has a presentation $\langle a, b, c : a^p = b^p = c^p = e,\ ab = ba,\ cac^{-1} = a,\ cbc^{-1} = ab \rangle$.

- We can also use semidirect products to classify groups of a given order, if we can establish the existence of an appropriate normal subgroup and "complement" subgroup.
  - In many cases, we will obtain several different possible choices for maps $\sigma : K \to \text{Aut}(H)$.
  - It can be shown that if K is cyclic and the images $\sigma_1(K)$ and $\sigma_2(K)$ inside $\text{Aut}(H)$ are conjugate subgroups, then in fact the resulting semidirect products are isomorphic.
  - Specifically, if $K = \langle a \rangle$ and $g\sigma_1(K)g^{-1} = \sigma_2(K)$, so that $g\sigma_1(a)g^{-1} = \sigma_2(a)^d$ for an integer d, then the map $\psi : H \rtimes_{\sigma_1} K \to H \rtimes_{\sigma_2} K$ given by $\psi(h, k) = ([\sigma_2]_g(h), a^d)$ is an isomorphism.

- Example: Classify the groups of order 30.
  - Since $30 = 2 \cdot 3 \cdot 5$, we must have $n_2 \in \{1, 3, 5, 15\}$, $n_3 \in \{1, 10\}$, and $n_5 \in \{1, 6\}$.
  - However, we cannot have both $n_3 = 10$ and $n_5 = 6$, since then there would be 20 elements of order 3 and 24 elements of order 5, which is more than the number of elements in the group. Thus, $n_3 = 1$ or $n_5 = 1$.
  - Therefore, the product of the Sylow 3-subgroup and Sylow 5-subgroup is also a subgroup of G (by our properties of subgroup products, since one of them is normal), and so G has a subgroup H of order 15.
  - Since 3 does not divide $5 - 1$, from our classification of groups of order pq, H is cyclic.
  - In fact, H is a normal subgroup of G: G acts on the two left cosets of H by left multiplication, so we have a homomorphism $\varphi : G \to S_2$. The image of this homomorphism has size 2 (since the action is transitive on cosets) and so the kernel, which contains H, must have size 15. This forces $H = \ker\varphi$ and so H is normal.
  - Now, there exists a Sylow 2-subgroup K of G. We then see $H \cap K = \{e\}$ since their orders are relatively prime, and since $\#H \cdot \#K = 30$, we have $HK = G$. Therefore, since H is normal, by our results on semidirect products, G must be isomorphic to a semidirect product $H \rtimes_\sigma K$ for some $\sigma : K \to \text{Aut}(H)$.
  - Since $H \cong \mathbb{Z}/15\mathbb{Z}$, one may verify that $\text{Aut}(H) \cong (\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times$, which is a product of a cyclic group of order 2 with a cyclic group of order 4.

- The map σ must send the nonidentity element $k \in K$ to an element of $\mathrm{Aut}(H)$ of order dividing 2. If σ is the trivial map, then G is abelian and isomorphic to $\mathbb{Z}/30\mathbb{Z}$.
- If $\sigma(k) = (-1, 1)$, then the resulting automorphism maps $(a, b) \in (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ to (a^{-1}, b). Then $\mathbb{Z}/5\mathbb{Z}$ is in the center of G, and G is isomorphic to $(\mathbb{Z}/5\mathbb{Z}) \times S_3$.
- If $\sigma(k) = (1, -1)$, then the resulting automorphism maps $(a, b) \in (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$ to (a, b^{-1}). Then $\mathbb{Z}/3\mathbb{Z}$ is in the center of G, and G is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times D_{2\cdot 5}$.
- If $\sigma(k) = (-1, -1)$, then the resulting automorphism maps $g \in (\mathbb{Z}/15\mathbb{Z})$ to g^{-1}. It is not hard to see that G is then isomorphic to $D_{2\cdot 15}$.
- Since these are all of the possible automorphisms, we see that up to isomorphism, there are four non-isomorphic groups of order 30: $\mathbb{Z}/30\mathbb{Z}$, $(\mathbb{Z}/5\mathbb{Z}) \times S_3$, $(\mathbb{Z}/3\mathbb{Z}) \times D_{2\cdot 5}$, and $D_{2\cdot 15}$.

• Example: Classify the groups of order 12.

- Since $12 = 2^2 \cdot 3$, we must have $n_2 \in \{1, 3\}$ and $n_3 \in \{1, 4\}$.
- First suppose that $n_3 = 4$. Then there are 8 elements of order 3, leaving only $12 - 8 = 4$ remaining elements, which must therefore form a unique Sylow 2-subgroup.
- Therefore, $n_2 = 1$, so the Sylow 2-subgroup H is normal in G. If K is any Sylow 3-subgroup, then $H \cap K = \{e\}$ since their orders are relatively prime, and since $\#H \cdot \#K = 12$, we have $HK = G$. Also, H is normal in G while K is not (since $n_3 = 4$).
- Therefore, G is a semidirect product $H \rtimes_\sigma K$ for some nontrivial $\sigma : K \to \mathrm{Aut}(H)$.
- If $H = \langle a \rangle$ is cyclic of order 4, then $\mathrm{Aut}(H) \cong (\mathbb{Z}/4\mathbb{Z})^\times$ is cyclic of order 2. But then if $K = \langle c \rangle$, there is no nontrivial map $\sigma : K \to \mathrm{Aut}(H)$, since $\sigma_c(a)$ would have order dividing both 2 and 3.
- Otherwise, $H = \langle a \rangle \times \langle b \rangle$ where a and b both have order 2. Then $\mathrm{Aut}(H) \cong GL_2(\mathbb{F}_2)$, which has order $(2^2 - 1)(2^2 - 2) = 6$. Thus, if $\sigma : K \to \mathrm{Aut}(H)$ is nontrivial, the image is a Sylow 3-subgroup of $GL_2(\mathbb{F}_3)$. Since all of these Sylow 3-subgroups are conjugate, we obtain a unique semidirect product up to isomorphism.
- Explicitly, if we take $\sigma : K \to \mathrm{Aut}(H)$ to be the map with $\sigma(c) = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, which is well-defined since this matrix has order 3, then as an explicit automorphism we have $\sigma_c(a) = b$ and $\sigma_c(b) = ab$.
- The resulting semidirect product $H \rtimes_\sigma K$ is a non-abelian group of order 12, and it has a presentation $\langle a, b, c : a^2 = b^2 = c^3 = e,\ ab = ba,\ cac^{-1} = b,\ cbc^{-1} = ab \rangle$. In fact, this group is isomorphic to A_4, with an isomorphism given explicitly by mapping $a \mapsto (1\,2)(3\,4)$, $b \mapsto (1\,4)(2\,3)$, and $c \mapsto (1\,2\,3)$.
- Now suppose $n_3 = 1$. If $n_2 = 1$ as well, then G is the direct product of its Sylow 2-subgroup with its Sylow 3-subgroup, and is isomorphic either to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$ or to $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/12\mathbb{Z}$.
- Otherwise, $n_2 = 3$. Then, if $H = \langle a \rangle$ is the unique Sylow 3-subgroup and K is any Sylow 2-subgroup, we see that $H \cap K = \{e\}$, $HK = G$, and H is normal in G, so G is a semidirect product $H \rtimes_\sigma K$ for some nontrivial $\sigma : K \to \mathrm{Aut}(H)$.
- Note here that $\mathrm{Aut}(H) \cong (\mathbb{Z}/3\mathbb{Z})^\times$ is cyclic of order 2, and generated by the inversion map $a \mapsto a^{-1}$.
- If $K = \langle b \rangle$ is cyclic of order 4, then there is one nontrivial homomorphism $\sigma : K \to \mathrm{Aut}(H)$, which has $\sigma_b(a) = a^{-1}$. The resulting semidirect product is a non-abelian group of order 12, and it has a presentation $\langle a, b, c : a^3 = b^4 = e,\ bab^{-1} = a^{-1} \rangle$.
- If $K = \langle b \rangle \times \langle c \rangle$ is Klein-4, then there are three nontrivial homomorphisms $\sigma : K \to \mathrm{Aut}(H)$. However, since their images are all the same, the resulting semidirect products are isomorphic. If we take $\sigma_b(a) = a$ and $\sigma_c(a) = a^{-1}$, then we obtain a presentation $\langle a, b, c : a^3 = b^2 = c^2 = e,\ bc = cb,\ bab^{-1} = a,\ cac^{-1} = a^{-1} \rangle$. In fact, this group is generated by c and $d = ab$, with presentation $\langle c, d : c^2 = d^6 = e,\ cdc^{-1} = d^{-1} \rangle$, which shows that it is isomorphic to the dihedral group $D_{2\cdot 6}$.
- Therefore, since we have examined all of the possible cases, there are five non-isomorphic groups of order 12: A_4, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$, $\mathbb{Z}/12\mathbb{Z}$, the nontrivial semidirect product $(\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$, and $D_{2\cdot 6}$.

Well, you're at the end of my handout. Hope it was helpful.