Permutation Groups and the Semidirect Product

Dylan C. Beck

Groups of Permutations of a Set

Given a nonempty set X, we may consider the set $\mathfrak{S}_X$ (Fraktur "S") of bijections from X to itself. Certainly, the identity map $\iota : X \to X$ defined by $\iota(x) = x$ for every element x of X is a bijection, hence $\mathfrak{S}_X$ is nonempty. Given any two bijections $\sigma, \tau : X \to X$, it follows that $\sigma \circ \tau$ is a bijection from X to itself so that $\mathfrak{S}_X$ is closed under composition. Composition of functions is associative. Last, for any bijection $\sigma : X \to X$, there exists a function $\sigma^{-1} : X \to X$ such that $\sigma^{-1} \circ \sigma = \iota = \sigma \circ \sigma^{-1}$: indeed, for every x in X, there exists a unique y in X such that $\sigma(y) = x$, so we may define $\sigma^{-1}(x) = y$. We conclude therefore that $(\mathfrak{S}_X, \circ)$ is a (not necessarily abelian) group. We refer to $\mathfrak{S}_X$ as the **symmetric group on the set** X. Considering that a bijection of a set is by definition a permutation, we may sometimes call $\mathfrak{S}_X$ the *group of permutations of the set* X.

Given that $|X| < \infty$, there exists a bijection between X and the set $\{1, 2, \dots, |X|\}$ that maps an element from X uniquely to some element of $\{1, 2, \dots, |X|\}$. Consequently, in order to study the group of permutations of a finite set, we may focus our attention on the permutation groups of the finite sets $[n] = \{1, 2, \dots, n\}$ for all positive integers n. We refer to the group $\mathfrak{S}_{[n]}$ as the **symmetric group on n letters**, and we adopt the shorthand $\mathfrak{S}_n$ to denote this group.

Proposition 1. We have that $|\mathfrak{S}_n| = n! = n(n-1)(n-2) \cdots 2 \cdot 1$.

Proof. By definition, the elements of $[n]$ are bijections from $[n]$ to itself. Each bijection $\sigma : [n] \to [n]$ is uniquely determined by the values of $\sigma(1), \sigma(2), \dots, \sigma(n)$. Consequently, we may construct a bijections from $[n]$ to itself by specifying the values $\sigma(i)$ for each integer $1 \leq i \leq n$ in turn. Certainly, there are n distinct choices for the value of $\sigma(1)$. Once this value has been specified, there are $n-1$ distinct choices for the value of $\sigma(2)$ that differ from $\sigma(1)$. Once both $\sigma(1)$ and $\sigma(2)$ have been specified, there are $n-2$ distinct choices for the value of $\sigma(3)$ that differ from both $\sigma(1)$ and $\sigma(2)$. Continuing in this manner, there are $n-i+1$ distinct choices for the value of $\sigma(i)$ that differ from $\sigma(1), \sigma(2), \dots, \sigma(i-1)$ for each integer $1 \leq i \leq n$. By the Fundamental Counting Principle, there are $\prod_{i=1}^n (n-i+1) = n(n-1)(n-2) \cdots 2 \cdot 1 = n!$ distinct bijections from $[n]$ to itself. $\square$

Permutations and the Symmetric Group on n Letters

Considering that every element σ of $\mathfrak{S}_n$ is uniquely determined by the values $\sigma(1), \sigma(2), \dots, \sigma(n)$, we may visualize σ as the following $2 \times n$ array by listing $\sigma(i)$ beneath each integer $1 \leq i \leq n$.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Using the fact that $\sigma(\sigma(i)) = \sigma^2(i)$ for each integer $1 \leq i \leq n$, we may build upon this array to list the image $\sigma^2(i)$ of $\sigma(i)$ under σ beneath $\sigma(i)$ for each integer $1 \leq i \leq n$.

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma^2(1) & \sigma^2(2) & \cdots & \sigma^2(n) \end{pmatrix}$$

Continue in this manner until each of the integers $1 \leq i \leq n$ appears in the same column twice. Observe that the columns of this array give rise to **cycles** $(i, \sigma(i), \sigma^2(i), \dots, \sigma^{r_i - 1}(i))$ whose entries are distinct. We say that two cycles $(a_1, a_2, \dots, a_k)$ and $(b_1, b_2, \dots, b_\ell)$ are **disjoint** whenever the entries a_i and b_j are distinct for all pairs of integers $1 \leq i \leq k$ and $1 \leq j \leq \ell$.

Example 1. Compute the disjoint cycles of the following permutation.

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

Solution. Computing the disjoint cycles amounts to building the array until each of the integers $1 \leq i \leq n$ appears in the same column twice. Explicitly, we have the following array.

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

Consequently, the disjoint cycles of σ are $(1, 2, 5)$, $(3, 8)$, (4), and $(6, 7)$. ◇

Given a cycle $(i, \sigma(i), \sigma^2(i), \dots, \sigma^{r_i - 1}(i))$, we refer to the non-negative integer r_i as its **length**. Cycles of length k are called **k-cycles**. Cycles of length 2 are known as **transpositions**. Observe that if σ in $\mathfrak{S}_n$ has k disjoint cycles of lengths $r_1, \dots, r_k$, then $r_1 + \cdots + r_k = n$. Even more, every permutation σ in $\mathfrak{S}_n$ is uniquely determined by its disjoint cycles. Consequently, we may write σ as a product of its disjoint cycles $\sigma = (i_1, \sigma(i_1), \dots, \sigma^{r_1 - 1}(i_1))(i_2, \sigma(i_2), \dots, \sigma^{r_2 - 1}(i_2)) \cdots (i_k, \sigma(i_k), \dots, \sigma^{r_k - 1}(i_k))$ for some integers $1 \leq i_1, i_2, \dots, i_k \leq n$; we call this the **cycle decomposition** of σ. Conversely, given a permutation σ with cycle decomposition $\sigma_1 \sigma_2 \cdots \sigma_k$, we can reconstruct σ as follows.

1.) Build a $2 \times n$ array with the integers $1, 2, \dots, n$ listed in order in the first row.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ & & & \end{pmatrix}$$

2.) In order to fill the space below the integer 1, first locate the integer 1 in some cycle σ_{j_1}.

3.) Given that 1 is immediately followed by a right parenthesis, then $\sigma(1)$ is the integer that begins the cycle σ_{j_1}; otherwise, $\sigma(1)$ is the integer that immediately follows 1 in the cycle σ_{j_1}.

4.) Repeat the above two steps until the integers $\sigma(1), \sigma(2), \dots, \sigma(n)$ are all found.

Based on the commentary at the beginning of the page above, we have the following propositions.

Proposition 2. Given a cycle σ of length r, we have that $\operatorname{ord}(\sigma) = r$.

Proof. Observe that if $\sigma = (a_1, a_2, \dots, a_r)$ is a cycle, then $\sigma^i(a_j) = a_{j+i \,(\mathrm{mod}\, r)}$. Consequently, we have that $\sigma^i(a_j) = a_j$ if and only if $j + i \equiv j \pmod{r}$ if and only if $i \equiv 0 \pmod{r}$, from which it follows that $\operatorname{ord}(\sigma) = \min\{i \geq 1 \mid \sigma^i(a_j) = a_j \text{ for all integers } 1 \leq j \leq r\} = r$. $\square$

Our next proposition states that the cycle decomposition is unique up to rearrangement.

Proposition 3. Given disjoint cycles σ_1 and σ_2, we have $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Proof. By definition, the cycle σ_1 maps some set $\{m_1, \dots, m_i\} \subseteq [n]$ one-to-one and onto itself, and likewise, the cycle σ_2 maps some set $\{n_1, \dots, n_j\} \subseteq [n]$ one-to-one and onto itself.

Given that σ_1 and σ_2 are disjoint, we have that $\{m_1, \dots, m_i\} \cap \{n_1, \dots, n_j\} = \emptyset$, hence by the algorithm outlined above Example 2, the permutation obtained by $\sigma_1\sigma_2$ is the same as the permutation obtained by taking $\sigma_2\sigma_1$. Explicitly, if the integer i is in neither σ_1 nor σ_2, then we must have that $\sigma(i) = i$; otherwise, the integer i appears in either σ_1 or σ_2 but not both. $\square$

Proposition 4. Given a permutation σ with cycle decomposition $\sigma_1\sigma_2 \cdots \sigma_k$ such that r_i is the length of the cycle σ_i, we have that $\operatorname{ord}(\sigma) = \operatorname{lcm}(r_1, r_2, \dots, r_k)$.

Proof. By Proposition 3, disjoint cycles commute, hence we have that

$$\operatorname{ord}(\sigma) = \operatorname{ord}(\sigma_1 \cdots \sigma_k) = \min\{i \geq 1 \mid (\sigma_1 \cdots \sigma_k)^i = \iota\} = \min\{i \geq 1 \mid \sigma_1^i \cdots \sigma_k^i = \iota\}.$$

We claim that $\sigma_1^i \cdots \sigma_k^i = \iota$ if and only if $\sigma_j^i = \iota$ for each integer $1 \leq j \leq k$. Certainly, if $\sigma_j^i = \iota$ for each integer $1 \leq j \leq k$, then $\sigma_1^i \cdots \sigma_k^i = \iota$. Conversely, if $\sigma_j^i \neq \iota$ for some integer $1 \leq j \leq k$, then $\sigma_1^i \cdots \sigma_k^i \neq \iota$ because the cycles $\sigma_1, \dots, \sigma_k$ are all disjoint. Consequently, we conclude that

$$\begin{aligned} \operatorname{ord}(\sigma) &= \min\{i \geq 1 \mid \sigma_j^i = \iota \text{ for each integer } 1 \leq j \leq k\} \\ &= \min\{i \geq 1 \mid \operatorname{ord}(\sigma_j) = r_j \text{ divides } i \text{ for each integer } 1 \leq j \leq k\} = \operatorname{lcm}(r_1, \dots, r_k). \end{aligned}$$ $\square$

We refer to a permutation σ of order 2 as an **involution**. By Proposition 4, if the cycle decomposition of a permutation σ is the product of disjoint transpositions, then σ is an involution.

Example 2. Give the cycle decomposition of the permutation from Example 1; then, use Proposition 4 to find its order.

Solution. Considering that the disjoint cycles of σ are $(1, 2, 5)$, $(3, 8)$, (4), and $(6, 7)$, it follows that the unique (up to arrangement) cycle decomposition of σ is $\sigma = (1, 2, 5)(3, 8)(4)(6, 7)$. By Proposition 4, we have that $\operatorname{ord}(\sigma) = \operatorname{lcm}(3, 2, 1, 2) = \operatorname{lcm}(6, 1, 2) = \operatorname{lcm}(6, 2) = 6$. $\diamond$

Considering that $(\mathfrak{S}_n, \circ)$ is a group, it follows the product $\sigma = \sigma_1 \cdots \sigma_k$ of (not necessarily disjoint) cycles $\sigma_1, \dots, \sigma_k$ is again a permutation. Given that this is the case, we can reconstruct σ as follows.

1.) Build a $2 \times n$ array with the integers $1, 2, \dots, n$ listed in order in the first row.

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ & & & \end{pmatrix}$$

2.) In order to fill the space below the integer 1, first locate the integer 1 in the cycle σ_{j_1} that is farthest to the right among the cycles in the product $\sigma_1 \cdots \sigma_k$.

3.) Given that 1 is immediately followed by a right parenthesis, then 1 maps to the integer b_{j_1} that begins σ_{j_1}; otherwise, 1 maps to the integer n_{j_1} that immediately follows 1 in σ_{j_1}.

4.) Locate the integer b_{j_1} or n_{j_1} in the cycle that is farthest to the right among the cycles in the product $\sigma_1 \cdots \sigma_{j_1 - 1}$; then repeat the third step.

5.) Repeat the third and fourth steps until it is not possible; the last integer found is $\sigma(1)$.

6.) Repeat the the above four steps until the integers $\sigma(1), \sigma(2), \ldots, \sigma(n)$ are found.

One useful way to think about and to understand the mechanics of this algorithm is that function composition is read from right to left. Considering that each cycle is itself a permutation, in order to find the image of i under the map $\sigma_1 \cdots \sigma_k$, we follow the image of i under the successive composite maps σ_k, $\sigma_{k-1}\sigma_k$, etc., all the way up to $\sigma_1 \cdots \sigma_k$. Further, if the integer $\sigma_j(i)$ does not appear in σ_{j-1}, then $\sigma_{j-1}\sigma_j(i) = \sigma_j(i)$, hence we must only consider the cycle farthest to the right that *contains* the integer under consideration: all cycles that do not contain $\sigma_j(i)$ will fix $\sigma_j(i)$.

Example 3. Find the permutation $\sigma = (1,3,4)(4,5)(1,4)(2,3)$ of $\mathfrak{S}_5$ in two-line notation.

Solution. Using the algorithm above, we find that 1 maps to 4; then, 4 maps to 5; and finally, 5 does not appear in any cycle to the left of $(4,5)$, so it follows that $\sigma(1) = 5$. We find next that 2 maps to 3; then, 3 maps to 4; and there are no permutations to the left of $(1,3,4)$, so it follows that $\sigma(2) = 4$. We find next that 3 maps to 2 in the last cycle, and 2 does not appear in any cycle to the left of $(2,3)$, so it follows that $\sigma(3) = 2$. We find next that 4 maps to 1; then, 1 maps to 3; and there are no permutations to the left of $(1,3,4)$, so it follows that $\sigma(4) = 3$. Last, we find that 5 maps to 4; then, 4 maps to 1; and there are no permutations to the left of $(1,3,4)$, so it follows that $\sigma(5) = 1$. We conclude therefore that σ can be written in two-line notation as follows.

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

Often, it is advantageous to omit the cycles of length 1 (or 1-cycles) when describing a permutation via its cycle decomposition. For instance, the permutation $\sigma = (1,2,3)$ can be viewed as the 3-cycle

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

in $\mathfrak{S}_3$ or as the permutation τ in $\mathfrak{S}_n$ for any integer $n \geq 3$ that acts as σ on the subset $\{1,2,3\}$ and acts as the identity on the subset $\{4, \ldots, n\}$. Consequently, a permutation is uniquely determined by its cycle decomposition (excluding 1-cycles) *regardless of the symmetric group to which it belongs.*

Proposition 5. For every integer $n \geq 3$, the symmetric group $\mathfrak{S}_n$ is not abelian.

Proof. Consider the cycles $\sigma = (1,2)$ and $\tau = (1,3)$ in $\mathfrak{S}_3$. By the paragraph above, we may view σ and τ as elements of $\mathfrak{S}_n$ for every integer $n \geq 3$. Considering that $\sigma\tau = (1,2)(1,3) = (1,3,2)$ is not equal to $\tau\sigma = (1,3)(1,2) = (1,2,3)$, we conclude that $\mathfrak{S}_n$ is not abelian for any integer $n \geq 3$. $\square$

Q1, January 2010. Give an explicit isomorphism between $\mathfrak{S}_3$ and $\mathrm{GL}_2(\mathbb{F}_2)$, i.e., the group of all invertible 2×2 matrices with entries in the field of two elements $\mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$.

Proposition 6. For every integer $n \geq 3$, the center $Z(\mathfrak{S}_n)$ of the symmetric group $\mathfrak{S}_n$ is $\{\iota\}$.

Proof. On the contrary, we will assume that there exists a nontrivial permutation σ of $Z(\mathfrak{S}_n)$. Consequently, there exist distinct integers i and j such that $\sigma(i) = j$. By hypothesis that $n \geq 3$, there exists another integer k distinct from i and j. Consider the transposition $\tau = (i, k)$. We have that $\sigma\tau(i) = \sigma(k) \neq j = \tau(j) = \tau\sigma(i)$. For if it were the case that $\sigma(k) = j$, then we would have that $\sigma(k) = \sigma(i)$ so that $k = i$ by hypothesis that σ is a bijection — a contradiction. But then, σ does not commute with τ, contradicting our assumption that σ is in $Z(\mathfrak{S}_n)$. $\square$

Q1c, August 2015. Given a group G, denote the center of G by

$$Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}.$$

Observe that $Z(G)$ is a normal subgroup of G. Construct subgroups $Z_i(G)$ inductively as follows.

1.) Begin with $Z_0(G) = \{e_G\}$.

2.) For each integer $i \geq 0$, let $Z_{i+1}(G)$ be the subgroup of G that is the pre-image of the center of the group $G/Z_i(G)$ so that $Z_{i+1}(G)/Z_i(G)$ is the center of $G/Z_i(G)$.

We note that G is nilpotent if $Z_n(G) = G$ for some integer $n \geq 1$. Give an example of a group G with a normal subgroup H such that both H and G/H are nilpotent but G is not nilpotent.

Given a permutation σ in $\mathfrak{S}_n$ with cycle decomposition $\sigma_1 \cdots \sigma_k$ such that σ_i has length r_i, we may rearrange (if necessary) the σ_i so that $r_1 \leq \cdots \leq r_k$. We refer to the ordered k-tuple $(r_1, \dots, r_k)$ as the **cycle type** of σ. Considering that an ordered k-tuple $(r_1, \dots, r_k)$ with $r_1 \leq \cdots \leq r_k$ and $r_1 + \cdots + r_k = n$ is an integer partition of n with k parts by definition, we have the following.

Proposition 7. Given a positive integer n, the number of distinct cycle types of permutations in $\mathfrak{S}_n$ is equal to the number of distinct integer partitions of n.

Our next proposition states that cycle type is unique up to conjugation.

Proposition 8. Given two permutations ρ and σ in $\mathfrak{S}_n$, there exists a permutation τ in $\mathfrak{S}_n$ such that $\tau\rho\tau^{-1} = \sigma$ (i.e., ρ and σ are conjugate in $\mathfrak{S}_n$) if and only if ρ and σ have the same cycle type.

Before we prove the proposition, we need the following lemma (that appeared on a past qual).

Q1a, August 2017. Consider the k-cycle $\sigma = (a_1, \dots, a_k)$. Prove that for any permutation τ in $\mathfrak{S}_n$ with $n \geq k$, we have that $\tau\sigma\tau^{-1} = (\tau(a_1), \dots, \tau(a_k))$.

Proof. Given any integer $1 \leq i \leq n$, we will assume that $\sigma(i) = j$. By hypothesis that τ is a permutation, it follows that τ^{-1} exists and satisfies $\tau^{-1}(\tau(i)) = i$ so that $\sigma\tau^{-1}(\tau(i)) = \sigma(i) = j$. Consequently, we have that $\tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$ so that $\tau\sigma\tau^{-1}$ sends $\tau(i)$ to $\tau(j)$.

Given that σ is the k-cycle $\sigma = (a_1, \dots, a_k)$, it follows that σ fixes all integers in $[n] - \{a_1, \dots, a_k\}$, hence $\tau\sigma\tau^{-1}$ fixes all integers in $[n] - \{\tau(a_1), \dots, \tau(a_k)\}$. Likewise, we have that $\sigma(a_i) = a_{i+1}$ for all integers $1 \leq i \leq k-1$ and $\sigma(a_k) = a_1$, hence $\tau\sigma\tau^{-1}$ maps $\tau(a_i)$ to $\tau(a_{i+1})$ for all integers $1 \leq i \leq k-1$ and $\tau\sigma\tau^{-1}$ maps $\tau(a_k)$ to $\tau(a_1)$. Put another way, we have that $\tau\sigma\tau^{-1} = (\tau(a_1), \dots, \tau(a_k))$. $\square$

Proof. (Proposition 8) Given that ρ and σ are conjugate in $\mathfrak{S}_n$, there exists a permutation τ in $\mathfrak{S}_n$ such that $\tau\rho\tau^{-1} = \sigma$. We may assume that $\rho = \rho_1 \cdots \rho_k$ is the cycle decomposition of ρ so that

$$\sigma = \tau\rho\tau^{-1} = (\tau\rho_1\tau^{-1}) \cdots (\tau\rho_k\tau^{-1})$$

is the cycle decomposition of σ. By the above lemma, it follows that $\tau\rho_i\tau^{-1}$ are cycles of the same length as ρ_i, hence we must have that ρ and σ have the same cycle type.

Conversely, we will assume that ρ and σ have the same cycle type $(r_1, \dots, r_k)$. Consequently, we have that $\rho = \rho_1 \cdots \rho_k$ and $\sigma = \sigma_1 \cdots \sigma_k$ for some disjoint cycles ρ_i and some disjoint cycles σ_i with $\text{length}(\rho_i) = r_i = \text{length}(\sigma_i)$. Considering that $[n]$ is a finite set, we may construct a bijection $\tau : [n] \to [n]$ that maps the cycle ρ_i to the cycle σ_i. Even more, we may construct τ in such a way that for any cycle $\rho_i = (a_{i,1}, \dots, a_{i,r_i})$ and the corresponding cycle $\sigma_i = (b_{i,1}, \dots, b_{i,r_i})$, we have that $\tau(a_{i,j}) = b_{i,j}$. We claim that $\tau\rho\tau^{-1} = \sigma$. By the above lemma, we have that

$$\tau\rho\tau^{-1}(\tau(a_{i,j})) = \tau\rho(a_{i,j}) = \tau(a_{i+1,j}) = b_{i+1,j} = \sigma(b_{i,j}) = \sigma(\tau(a_{i,j})).$$

By construction, we have that τ is a bijection from $[n]$ to itself, hence every element of $[n]$ can be written as $\tau(a_{i,j})$ for some integer $1 \leq a_{i,j} \leq n$. We conclude therefore that $\tau\rho\tau^{-1} = \sigma$. $\square$

Example 4. Give an explicit bijection $\tau : [3] \to [3]$ that conjugates $\rho = (1, 2, 3)$ and $\sigma = (1, 3, 2)$.

Solution. By the proof of Proposition 8, we must have that $\tau(1) = 1$, $\tau(2) = 3$, and $\tau(3) = 2$ so that $\tau = (1)(2, 3)$. Let us verify that $\tau\rho\tau^{-1} = \sigma$. Considering that $\tau\tau = (1)(2, 3)(1)(2, 3) = (1)(2)(3) = \iota$, it follows that $\tau = \tau^{-1}$ so that $\tau\rho\tau^{-1} = (1)(2, 3)(1, 2, 3)(1)(2, 3) = (1, 3, 2) = \sigma$, as desired. $\diamond$

Example 5. Give an explicit bijection $\tau : [8] \to [8]$ that conjugates $\rho = (1, 3, 5)(2, 7)(4, 8)(6)$ and $\sigma = (1)(2, 5, 8)(3, 4)(6, 7)$.

Solution. Certainly, we could proceed in the manner outlined in the proof of Proposition 8; however, this answer from Arturo Magidin gives a beautiful way to construct τ more easily. First, we write down the cycle type of ρ and σ; then, we arrange the cycles of ρ and σ in some (not necessarily unique) manner so that the cycles have non-decreasing length; and last, we construct a 2×8 array with ρ in the first line and σ in the second line. Observe that the cycle type of ρ and σ is $(1, 2, 2, 3)$, hence we may arrange $\rho = (6)(2, 7)(4, 8)(1, 3, 5)$ and $\sigma = (1)(3, 4)(6, 7)(2, 5, 8)$ to obtain τ.

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

By reading off the array, we find that $\tau = (1, 2, 3, 5, 8, 7, 4, 6)$. Observe that $\tau\rho\tau^{-1} = \sigma$ if and only if $\tau\rho = \sigma\tau$. We leave it to the reader to verify that $\tau\rho = \sigma\tau$, as desired. $\diamond$

Computing the inverse of a permutation can be quite tedious; however, if we have a permutation σ written as its cycle decomposition $\sigma = \sigma_1 \cdots \sigma_k$, then Proposition 2 above gives a way to write down the inverse of σ. Explicitly, if σ_i has length r_i, then $\sigma_i\sigma_i^{r_i - 1} = \sigma_i^{r_i} = \iota = \sigma_i^{r_i - 1}\sigma_i$. Consequently, we have that $\sigma_i^{-1} = \sigma_i^{r_i - 1}$. Considering that disjoint cycles commute, we have the following.

Proposition 9. Given a permutation σ with cycle decomposition $\sigma = \sigma_1 \cdots \sigma_k$ and cycle type $(r_1, \dots, r_k)$, we have that $\sigma^{-1} = \sigma_1^{r_1 - 1} \cdots \sigma_k^{r_k - 1}$.

Ultimately, Proposition 9 reduces the matter of finding inverses of permutations written in cycle decomposition bearable, as finding the inverse of a cycle is quite easy: observe that for the k-cycle $(a_1, \dots, a_k)$, by the proof of Proposition 2, we have that $(a_1, \dots, a_k)^{k-1} = (a_1, a_k, a_{k-1}, \dots, a_3, a_2)$.

We turn our attention now to the matter of the combinatorics (or mathematics of counting) in the symmetric group. Our first result follows immediately from Propositions 7 and 8.

Proposition 10. Given a positive integer n, the number of distinct conjugacy classes of $\mathfrak{S}_n$ is equal to the number of distinct integer partitions of n.

Proof. By Proposition 8 above, there exists a bijection

$$\{\text{distinct conjugacy classes of } \mathfrak{S}_n\} \leftrightarrow \{\text{distinct cycle types of permutations in } \mathfrak{S}_n\}$$

that sends the conjugacy class of some permutation ρ with cycle type $(r_1, \dots, r_k)$ to the cycle type $(r_1, \dots, r_k)$. Explicitly, the permutations ρ and σ are conjugate (and hence in the same conjugacy class) if and only if they have the same cycle type, hence this map is injective. Further, this map is surjective because for any cycle type $(r_1, \dots, r_k)$, we can construct a permutation ρ with cycle type $(r_1, \dots, r_k)$, and by Proposition 8, conjugation preserves cycle type. Consequently, we have that

$$\#\{\text{distinct conjugacy classes of } \mathfrak{S}_n\} = \#\{\text{distinct cycle types of permutations in } \mathfrak{S}_n\}.$$

By Proposition 7 above, the latter is equal to the number of distinct integer partitions of n. $\square$

Q1b, August 2017. Compute the number of distinct conjugacy classes in $\mathfrak{S}_5$.

Often, the best way to count something is to establish a bijection between what we want to count and something for which we already know the cardinality; however, counting can sometimes be successfully accomplished by naïvely underestimating and multiplying by the number of times each element in the set was undercounted. We illustrate this principle in the following proposition.

Proposition 11. Given a positive integer n, the number of distinct k-cycles in $\mathfrak{S}_n$ is $\frac{n!}{k(n-k)!}$.

Proof. Every k-cycle in $\mathfrak{S}_n$ is constructed in the following manner.

1.) Choose k elements from among the n elements of $[n]$. We can do this in $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ ways.

2.) Order the k elements in some way. Bear in mind that there is no "first" term in the ordering because $(a_1, \dots, a_k)$ is the same as $(a_k, a_1, \dots, a_{k-1})$, etc. Consequently, the order only matters for $k - 1$ of the elements, hence there are $(k-1)!$ ways to order the k elements.

By the Fundamental Counting Principle, there are $\frac{n!}{k!(n-k)!} \cdot (k-1)! = \frac{n!}{k(n-k)!}$ k-cycles in $\mathfrak{S}_n$. $\square$

The Alternating Group on n Letters

Until now, we have only briefly mentioned the notion of a transposition, i.e., a cycle of length 2. By Proposition 2, the order of any transposition τ is 2; by Proposition 4, the order of any product of disjoint transpositions is also 2, hence a product of disjoint transpositions is an involution. Our next proposition gives some motivation to further understand transpositions.

Proposition 12. Every permutation can be written as the product of a unique number of (not necessarily disjoint) transpositions.

Proof. Considering that every permutation can be written as the product of disjoint cycles, it suffices to show that any cycle $(a_1, \dots, a_k)$ can be written as a product of (not necessarily disjoint) transpositions. But this is quite simple: we have that $(a_1, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2)$. By Proposition 8, we have that cycle type is unique up to conjugation, hence the number of transpositions is uniquely determined by the cycle type of a permutation. $\square$

Considering that every permutation σ in $\mathfrak{S}_n$ can be written as the product of a unique number of (not necessarily disjoint) transpositions, we can define the **parity** of a permutation to be the parity (even or odd) of the number $t(\sigma)$ of transpositions in the transposition decomposition of σ. Further, we refer to the number $\operatorname{sgn}(\sigma) = (-1)^{t(\sigma)}$ as the **sign** of the permutation σ. Observe that σ is even if and only if $\operatorname{sgn}(\sigma) = 1$, and likewise, σ is odd if and only if $\operatorname{sgn}(\sigma) = -1$.

Proposition 13. Consider the map $\operatorname{sgn} : \mathfrak{S}_n \to \{-1, 1\}$ defined by $\operatorname{sgn}(\sigma) = (-1)^{t(\sigma)}$. We have that $\ker(\operatorname{sgn})$ is a normal subgroup of $\mathfrak{S}_n$ of index 2. Consequently, we have that $|\ker(\operatorname{sgn})| = n!/2$.

Proof. Observe that $\{-1, 1\}$ is a multiplicative group with identity 1. Consequently, we have that

$$\operatorname{sgn}(\rho\sigma) = (-1)^{t(\rho\sigma)} = (-1)^{t(\rho)+t(\sigma)} = (-1)^{t(\rho)}(-1)^{t(\sigma)} = \operatorname{sgn}(\rho)\operatorname{sgn}(\sigma)$$

so that sgn is a group homomorphism. We leave it as an exercise for the reader to prove the more general fact that the kernel of any group homomorphism from G is a normal subgroup of G (and conversely, a normal subgroup N of G is precisely the kernel of the group homomorphism $\pi : G \to G/N$), from which it follows that $\ker(\operatorname{sgn})$ is a normal subgroup of $\mathfrak{S}_n$. By Lagrange's Theorem, we have that $[G : \ker(\operatorname{sgn})] = |G|/|\ker(\operatorname{sgn})| = |G/\ker(\operatorname{sgn})|$. Using the First Isomorphism Theorem, we conclude that $G/\ker(\operatorname{sgn}) \cong \{-1, 1\}$ so that $|G/\ker(\operatorname{sgn})| = |\{-1, 1\}| = 2$. Considering that the last sentence of the claim is a restatement of the second sentence, our proof is complete. $\square$

We define the **alternating group** A_n **on n letters** to be the normal subgroup $\ker(\operatorname{sgn})$ of $\mathfrak{S}_n$ from Proposition 10. Observe that σ is in $\ker(\operatorname{sgn})$ if and only if $\operatorname{sgn}(\sigma) = 1$ if and only if σ is even, hence the alternating group on n letters is precisely the subgroup of $\mathfrak{S}_n$ consisting of even permutations. Of course, this matches with our intuition: the identity map $\iota : [n] \to [n]$ is the identity element of $\mathfrak{S}_n$; it can be represented as a the product of 1-cycles $\iota = (1)(2) \cdots (n)$ with 0 transpositions, hence we have that $\operatorname{sgn}(\iota) = (-1)^{t(\iota)} = (-1)^0 = 1$ so that ι is even. Given any two even permutations ρ and σ, we have that $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$ because σ^{-1} has the same cycle type as σ and hence the same number of transpositions. By the one-step subgroup test, we conclude that $\operatorname{sgn}(\rho\sigma^{-1}) = (-1)^{t(\rho\sigma^{-1})} = (-1)^{t(\rho)+t(\sigma^{-1})} = (-1)^{t(\rho)+t(\sigma)} = (-1)^{2r+2s} = 1$ so that $\rho\sigma^{-1}$ is even.

Proposition 14. Every permutation of odd order is even; however, the converse is not true — namely, there exist even permutations with even order.

Proof. Given that σ is a permutation of odd order, it follows that $\operatorname{lcm}(r_1, \dots, r_k)$ is odd, where $(r_1, \dots, r_k)$ is the cycle type of σ. Consequently, we must have that r_i is odd for each integer $1 \leq i \leq k$. By the proof of Proposition 12, an r_i-cycle is the product of $r_i - 1$ transpositions, hence σ is the product of $(r_1 - 1) + \cdots + (r_k - 1)$ transpositions. Each of the integers $r_i - 1$ is even, so this sum is even, and σ is a product of an even number of transpositions, i.e., σ is even.

Conversely, if σ is the product of an even number of disjoint transpositions, then σ is even by definition, and the order of σ is 2 by Proposition 4 (or the discussion at the start of the section). $\square$

Other interesting tidbits for you to consider (and possibly prove for yourself) are as follows.

(a.) A_n is generated by all 3-cycles. (Try to prove this one by yourself first. Check the proof here.)

(b.) A_n is simple for $n = 3$ and $n \geq 5$. (This is more involved. Check the proof here.)

(c.) A_5 is the smallest non-abelian simple group; it is also the smallest non-solvable group.

(d.) A_4 has the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$ as a proper normal subgroup via the injective group homomorphism $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to A_4$ defined by $(0, 0) \mapsto \iota$, $(1, 0) \mapsto (1, 2)(3, 4)$, $(0, 1) \mapsto (1, 3)(2, 4)$, and $(1, 1) \mapsto (1, 4)(2, 3)$. (Check the details for yourself.) Consequently, A_4 is not simple: $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \varphi(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is a nontrivial normal subgroup of A_4. Further, the sequence of groups

$$0 \to \mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{\varphi} A_4 \xrightarrow{\pi} \frac{A_4}{\varphi(\mathbb{Z}_2 \times \mathbb{Z}_2)} \to 0$$

is exact. Later, this will make more sense, but for now, suffice it to say that this implies that quartic polynomials can be solved by radicals (i.e., there exists a quartic formula). We will eventually see that the non-solvability of A_5 implies that there is no quintic formula, and even more, polynomials of degree ≥ 5 are not solvable by radicals (hence the name "solvable").

Cayley's Theorem

Cayley's Theorem is an example of a simple observation with larger implications.

Theorem 1. (Cayley's Theorem) Every group is isomorphic to a group of permutations.

Proof. Given a group G and any element g of G, consider the map $\varphi_g : G \to G$ defined by $\varphi_g(x) = gx$. By hypothesis that g is a group, it follows that g^{-1} is an element of G so that

$$\varphi_g \circ \varphi_{g^{-1}}(x) = \varphi_g(g^{-1}x) = gg^{-1}x = x = g^{-1}gx = \varphi_{g^{-1}}(gx) = \varphi_{g^{-1}} \circ \varphi_g(x)$$

for every element x of G. Consequently, it follows that $\varphi_{g^{-1}}$ is the inverse function of φ_g so that φ_g is a bijection from G to itself. By definition, therefore, φ_g is a permutation of G and hence an element of the symmetric group $\mathfrak{S}_G$ on the set G. We claim that the map $\sigma : G \to \mathfrak{S}_G$ defined by $\sigma(g) = \varphi_g$ is a group homomorphism. Observe that for any element k of G, we have that

$$\sigma(gh)(k) = \varphi_{gh}(k) = ghk = \varphi_g(hk) = \varphi_g \circ \varphi_h(k).$$

Considering that k is arbitrary, it follows that $\sigma(gh) = \varphi_g \circ \varphi_h = \sigma(g)\sigma(h)$ as functions, where concatenation is meant as function composition on $\mathfrak{S}_G$. Consequently, σ is a group homomorphism. Further, we have that g is in $\ker \sigma$ if and only if $\varphi_g = \mathrm{id}_{\mathfrak{S}_G}$ if and only if $\varphi_g(x) = \mathrm{id}_{\mathfrak{S}_G}(x)$ for all elements x of G if and only if $gx = x$ for all elements x of G if and only if $g = e_G$ by cancellation in G. We conclude that σ is injective, hence $G \cong \sigma(G) \leq \mathfrak{S}_G$ by the First Isomorhpism Theorem. □

Corollary 1. Every finite group of order n is isomorphic to a subgroup of $\mathfrak{S}_n$.

Proof. By Cayley's Theorem, every finite group G of order n is isomorphic to a subgroup of $\mathfrak{S}_G$. But as we suggested in the first section above, we have that $\mathfrak{S}_G \cong \mathfrak{S}_n$. Indeed, there exists a bijection $f : G \to [n]$ because they are finite sets of the same cardinality. We can extend f to a group isomorphism $\varphi : \mathfrak{S}_G \to \mathfrak{S}_n$ by declaring that for any permutation σ in $\mathfrak{S}_G$, we have that $\varphi(\sigma)$ is the permutation in $\mathfrak{S}_n$ that maps $f(g)$ to $f(h)$ whenever $\sigma(g) = h$. By taking inspiration from the proof of Proposition 7, we define $\varphi : \mathfrak{S}_G \to \mathfrak{S}_n$ by $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$, and we check that

(i.) $\varphi(\sigma)$ is a permutation of $[n]$ because it is a bijection from $[n]$ to itself (follow the arrows);

(ii.) φ is a group homomorphism because $\varphi(\sigma \circ \tau) = f \circ (\sigma \circ \tau) \circ f^{-1} = (f \circ \sigma \circ f^{-1}) \circ (f \circ \tau \circ f^{-1})$ shows that $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$ by the associativity of function composition; and

(iii.) φ is a bijection with function inverse $\psi : \mathfrak{S}_n \to \mathfrak{S}_G$ defined by $\psi(\rho) = f^{-1} \circ \rho \circ f$. Indeed, observe that $\psi \circ \varphi(\sigma) = \psi(f \circ \sigma \circ f^{-1}) = f^{-1} \circ (f \circ \sigma \circ f^{-1}) \circ f = \sigma$ and conversely. □

Certainly, we can use the same idea to prove that $\mathfrak{S}_X \cong \mathfrak{S}_Y$ for any sets X and Y with $|X| = |Y|$.

Q2, January 2014 (Revisited). Consider a group G with a subgroup H such that $[G : H] = n$. Prove that there exists a normal subgroup K of G such that $K \subseteq H$ and $[G : K] \leq n!$.

The Automorphism Group

Given a group G, we say that a group isomorphism from G to itself is an **automorphism** of G. We denote by $\mathrm{Aut}(G)$ the set of automorphisms of G, i.e., we have that

$$\mathrm{Aut}(G) = \{\varphi : G \to G \,|\, \varphi \text{ is a group isomorphism}\}.$$

Proposition 15. Given a group G, we have that $(\mathrm{Aut}(G), \circ)$ is a group under function composition.

Proof. Observe that the identity map $\iota : G \to G$ defined by $\iota(g) = g$ is an automorphism of G. Consequently, $\mathrm{Aut}(G)$ is nonempty: ι is the identity element of $\mathrm{Aut}(G)$. Composition of functions is associative, and compositions of bijective homomorphisms are bijective homomorphisms. Last, every bijective group homomorphism has an inverse that is a bijective group homomorphism. □

Given any element $g \in G$, observe that the map $\varphi_g : G \to G$ defined by $\varphi_g(x) = gx$ is always a bijection by the proof of Cayley's Theorem; however, it is not typically a group homomorphism because it is not true that $gxy = \varphi_g(xy) \neq \varphi_g(x)\varphi_g(y) = gxgy$ for all elements $x, y \in G$. But with a slight modification, we obtain an automorphism of G: $gxyg^{-1} = (gxg^{-1})(gyg^{-1})$ for all elements $x, y \in G$, hence the map $\chi_g(x) = gxg^{-1}$ is a group homomorphism. Cancellation in G shows that χ is also a bijection (e.g., its inverse is $\chi_{g^{-1}}$), hence χ is an automorphism of G for every element g of G. We refer to the set $\mathrm{Inn}(G) = \{\chi_g : G \to G \,|\, g \in G\}$ as the **inner automorphisms** of G.

Proposition 16. Given a group G, we have that $(\mathrm{Inn}(G), \circ)$ is a group under function composition.

Proof. Observe that the identity map $\iota : G \to G$ defined by $\iota(g) = g$ for every element g in G is an inner automorphism of G. Consequently, $\mathrm{Inn}(G)$ is a nonempty subset of $\mathrm{Aut}(G)$. By the one-step subgroup test, it suffices to show that if φ and ψ are in $\mathrm{Inn}(G)$, then $\varphi \circ \psi^{-1}$ is in $\mathrm{Inn}(G)$. □

Proposition 17. Given a group G with center $Z(G)$, we have that $G/Z(G) \cong \mathrm{Inn}(G)$.

Proof. Use the First Isomorphism Theorem. We leave the details to the reader. □

Proposition 18. Given a group G, prove that $\mathrm{Inn}(G)$ is cyclic if and only if $\mathrm{Inn}(G) = \{\iota\}$.

Proof. Of course, if $\mathrm{Inn}(G) = \{\iota\}$, then $\mathrm{Inn}(G)$ is (trivially) cyclic. Conversely, we will assume that $\mathrm{Inn}(G)$ is cyclic, i.e., there exists an element $g \in G$ such that $\mathrm{Inn}(G) = \langle \chi_g \rangle$. It is not difficult to see that $\chi_g^n = \chi_{g^n}$ for every integer n. Given any element h of G, therefore, there exists an integer n such that $\chi_h = \chi_g^n$, i.e., $hxh^{-1} = \chi_h(x) = \chi_g^n(x) = \chi_{g^n}(x) = g^n x g^{-n}$. Particularly, when $x = g$, we have that $hgh^{-1} = g^n g g^{-n} = g^{n+1} g^{-n} = g$ so that $hg = gh$. But the same argument can be made for all elements h of G, hence all elements of G commute with G. Ultimately, we conclude that $gxg^{-1} = xgg^{-1} = x$ for all elements x of G so that $\chi_g = \iota$ and $\mathrm{Inn}(G) = \{\iota\}$. □

Corollary 2. Given a group G with center $Z(G)$, if $G/Z(G)$ is cyclic, then G is abelian.

Proof. Given that $G/Z(G)$ is cyclic, it follows that $\mathrm{Inn}(G)$ is cyclic so that $\mathrm{Inn}(G) = \{\iota\}$. Consequently, χ_g is the identity map for every $g \in G$. We leave it to the reader to finish the proof. □

Recall that the unique (up to isomorphism) cyclic group of order n is given by $\mathbb{Z}_n = (\mathbb{Z}/n\mathbb{Z}, +)$. Using a similar idea as in the proof of Corollary 1, if $\varphi : G \to H$ is an isomorphism of groups, then $\psi : \mathrm{Aut}(G) \to \mathrm{Aut}(H)$ defined by $\psi(\gamma) = \varphi \circ \gamma \circ \varphi^{-1}$ is an isomorphism. Consequently, in order to study the automorphism group of a cyclic group of order n, it suffices to study the automorphism group $\mathrm{Aut}(\mathbb{Z}_n)$. For this, we need to recall some elementary number theory. By Bézout's Identity, we have that $k + n\mathbb{Z}$ is a unit in $\mathbb{Z}_n$ if and only if $\gcd(k, n) = 1$. Further, every group homomorphism $\psi : \mathbb{Z}_n \to \mathbb{Z}_n$ is uniquely determined by $\psi(1 + n\mathbb{Z})$ because we must have that

$$\begin{aligned}
\psi(m + n\mathbb{Z}) &= \psi(\underbrace{(1 + n\mathbb{Z}) + \cdots + (1 + n\mathbb{Z})}_{m \text{ summands}}) \\
&= \underbrace{\psi(1 + n\mathbb{Z}) + \cdots + \psi(1 + n\mathbb{Z})}_{m \text{ summands}} + n\mathbb{Z} \\
&= m\psi(1 + n\mathbb{Z}) + n\mathbb{Z}.
\end{aligned}$$

Combined, these observations imply that $\psi : \mathbb{Z}_n \to \mathbb{Z}_n$ is an automorphism if and only if $\psi(1 + n\mathbb{Z})$ is a unit. Consequently, we have that $|\mathrm{Aut}(\mathbb{Z}_n)| = \phi(n)$, where $\phi(n)$ is Euler's totient function.

Corollary 3. Given a positive integer n, we have that $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$, where $\mathbb{Z}_n^\times$ denotes the multiplicative group of units modulo n.

Corollary 4. (Euler's Theorem) Given an integer a with $\gcd(a, n) = 1$, we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

Corollary 5. (Fermat's Little Theorem) Given an integer a and a prime integer p with $\gcd(a, p) = 1$, we have that $a^p \equiv a \pmod{p}$.

Semidirect Products

Earlier in the semester, we studied the direct product $H \times K$ of two groups H and K. We found that $H \times K$ is a group whose operation is given by $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$. Given that H and K are both normal subgroups of a larger group G such that $H \cap K = \{e_G\}$ and $G = HK$, we found that $G \cong H \times K$. Unfortunately, if only one of H or K were normal, we could only say that HK is a subgroup of G (cf. Q1, August 2013). Even worse, if neither H nor K is normal in G, then we could not say anything at all. But this brings to mind a natural question: does there exist a group G' such that $H \trianglelefteq G'$, $K \leq G'$ (but K is not necessarily normal in G'), and $H \cap K = \{e_{G'}\}$?

Before we answer this question in the affirmative, let us thoroughly examine what we already know. Given a group G such that $H \trianglelefteq G$ and $K \leq G$, we have that HK is a subgroup of G, hence for any two elements $h_1 k_1, h_2 k_2 \in HK$, we have that $(h_1 k_1)(h_2 k_2)$ is in HK. We may write the element $h_1 k_1 h_2 k_2$ in the form $h_3 k_3$ for some elements $h_3 \in H$ and $k_3 \in K$ by observing that

$$h_1 k_1 h_2 k_2 = h_1 k_1 h_2 k_1^{-1} k_1 k_2 = h_1 (k_1 h_2 k_1^{-1})(k_1 k_2)$$

and using the fact that H is normal in G, hence ghg^{-1} is in H for all $h \in H$ and $g \in G$. Particularly, we have that $k_1 h_2 k_1^{-1}$ is in H so that $h_3 = h_1(k_1 h_2 k_1^{-1})$ and $k_3 = k_1 k_2$.

Using this observation as our motivation, we set out to define the group G' hinted at in the beginning of this section. By the previous section, the map $\chi_{k_1} : H \to H$ defined by $\chi_{k_1}(h) = k_1 h k_1^{-1}$ gives a map from K to $\mathrm{Aut}(H)$, so we may write the above displayed equation as

$$(h_1 k_1)(h_2 k_2) = (h_1 \chi_{k_1}(h_2))(k_1 k_2).$$

Observe that this defines a multiplication in HK intrinsically in terms of H and K.

Proposition 19. Given any groups H and K with a group homomorphism $\varphi : K \to \mathrm{Aut}(H)$, we define the **semidirect product** of H and K to be the set of ordered pairs in $H \times K$ endowed with the multiplication outlined in the above displayed equation. Put another way, we define the semidirect product of H and K to be the following set endowed with the prescribed multiplication.

$$H \rtimes_\varphi K \stackrel{\text{def}}{=} \{(h, k) \mid h \in H,\, k \in K, \text{ and } (h_1, k_1)(h_2, k_2) \stackrel{\text{def}}{=} (h_1 \varphi(k_1)(h_2), k_1 k_2)\}$$

(i.) We have that $H \rtimes_\varphi K$ is a group of order $|H||K|$.

(ii.) We have that $H_\varphi = \{(h, e_K) \mid h \in H\}$ and $K_\varphi = \{(e_H, k) \mid k \in K\}$ are both subgroups of $H \rtimes_\varphi K$ such that $H \cong H_\varphi$ and $K \cong K_\varphi$.

(iii.) We have that H_φ is a normal subgroup of $H \rtimes_\varphi K$ such that $H_\varphi \cap K_\varphi = \{e_{H \rtimes_\varphi K}\}$.

(iv.) For all ordered pairs $((h, e_K), (e_H, k)) \in H_\varphi \times K_\varphi$, we have that $\kappa(k)\eta(h)\kappa(k)^{-1} = \eta(\varphi(k)(h))$.

Proof. (i.) Clearly, we have that $|H \rtimes_\varphi K| = |H \times K| = |H||K|$. Considering that $\varphi(K)$ is a subgroup of the automorphism group of H, it follows that $\varphi(k)(h)$ is an element of H for all elements k of K. Consequently, we have that $h_1 \varphi(k_1)(h_2)$ is an element of H by hypothesis that H is a group. Likewise, we have that $k_1 k_2$ is an element of K by hypothesis that K is a group. We conclude therefore that $H \rtimes_\varphi K$ is closed under the multiplication defined above. Observe that the identity element of $H \rtimes_\varphi K$ is given by the ordered pair (e_H, e_K): indeed, we have that

$$(e_H, e_K)(h, k) = (e_H \varphi(e_K)(h), e_K k) = (h, k) \text{ and}$$

$$(h, k)(e_H, e_K) = (h\varphi(k)(e_H), ke_K) = (he_H, k) = (h, k)$$

because any automorphism of H must send e_H to itself. Given any element (h, k) of $H \rtimes_\varphi K$, its two-sided inverse is given by $(\varphi(k)^{-1}(h^{-1}), k^{-1})$. Explicitly, we have that

$$(h, k)(\varphi(k)^{-1}(h^{-1}), k^{-1}) = (h\varphi(k) \circ \varphi(k)^{-1}(h^{-1})), kk^{-1}) = (hh^{-1}, e_K) = (e_H, e_K) \text{ and}$$

$$\begin{aligned}(\varphi(k)^{-1}(h^{-1}), k^{-1})(h, k) &= (\varphi(k)^{-1}(h^{-1})\varphi(k^{-1})(h), k^{-1}k) \\ &= (\varphi(k)^{-1}(h^{-1})\varphi(k)^{-1}(h), e_K) \\ &= (\varphi(k)^{-1}(h^{-1}h), e_K) = (\varphi(k)^{-1}(e_H), e_K) = (e_H, e_K)\end{aligned}$$

because φ is a group homomorphism, hence $\varphi(k^{-1}) = \varphi(k)^{-1}$ for all elements k of K. Proving that this multiplication is associative is just a (tedious) matter of out the details.

(ii.) Considering that H_φ and K_φ both contain the identity (e_H, e_K) of $H \rtimes_\varphi K$, they are nonempty. Given any two elements (h_1, e_K) and (h_2, e_K) of H_φ, observe that

$$(h_1, e_K)(h_2, e_K)^{-1} = (h_1, e_K)(\varphi(e_K)^{-1}(h_2^{-1}), e_K^{-1}) = (h_1, e_K)(h_2^{-1}, e_K),$$

hence $(h_1, e_K)(h_2, e_K)^{-1}$ is in H_φ, as its second component is e_K. By the one-step subgroup test, H_φ is a subgroup of $H \rtimes_\varphi K$. Given any two elements (e_H, k_1) and (e_H, k_2) of K_φ, we have that

$$(e_H, k_1)(e_H, k_2)^{-1} = (e_H, k_1)(\varphi(k_1)^{-1}(e_H^{-1}), k_2^{-1}) = (e_H, k_1)(e_H, k_2^{-1}),$$

hence $(e_H, k_1)(e_H, k_2)^{-1}$ is in K_φ, as its first component is e_H. Once again appealing to the one-step subgroup test, we conclude that K_φ is a subgroup of $H \rtimes_\varphi K$. Consider the surjective map $\eta : H \to H_\varphi$ defined by $\eta(h) = (h, e_K)$. Given any elements h_1, h_2 of H, we have that

$$\eta(h_1 h_2) = (h_1 h_2, e_K) = (h_1 \varphi(e_K)(h_2), e_K e_K) = (h_1, e_K)(h_2, e_K) = \eta(h_1)\eta(h_2),$$

hence η is a group homomorphism. Considering that $\ker \eta = \{e_H\}$, it follows that η is injective. By the First Isomorphism Theorem, we conclude that $H \cong H_\varphi$. By an analogous argument applied to the surjective map $\kappa : K \to K_\varphi$ defined by $\kappa(k) = (e_H, k)$, we conclude that $K \cong K_\varphi$.

(iii.) Given any element (h_1, k_1) of $H \rtimes_\varphi K$ and any element (h, e_K) of H_φ, we have that

$$\begin{aligned}(h_1, k_1)(h, e_K)(h_1, k_1)^{-1} &= (h_1\varphi(k_1)(h), k_1 e_K)(\varphi(k_1)^{-1}(h_1^{-1}), k_1^{-1}) \\ &= (h_1\varphi(k_1)(h)\varphi(k_1 e_K)(\varphi(k_1)^{-1}(h_1^{-1})), k_1 e_K k_1^{-1}) \\ &= (h_1\varphi(k_1)(h)\varphi(k_1)(\varphi(k_1^{-1})(h_1^{-1})), e_K)\end{aligned}$$

is an element of H_φ, from which it follows that $H_\varphi \trianglelefteq H \rtimes_\varphi K$. Observe that (h,k) is in $H_\varphi \cap K_\varphi$ if and only if $h = e_H$ and $k = e_K$, hence we conclude that $H_\varphi \cap K_\varphi = \{(e_H, e_K)\} = \{e_{H \rtimes_\varphi K}\}$.

(iv.) Given any ordered pair $(h,k) \in H \times K$, we have that

$$(e_H, k)(h, e_K)(e_H, k)^{-1} = (e_H \varphi(k)(h), ke_K)(\varphi(k)^{-1}(e_H^{-1}), k^{-1})$$

$$= (e_H \varphi(k)(h)\varphi(k)(\varphi(k^{-1})(e_H^{-1})), e_K) = (\varphi(k)(h), e_K),$$

from which it follows that $\kappa(k)\eta(h)\kappa(k)^{-1} = \eta(\varphi(k)(h))$, as desired. $\square$

Our next proposition illustrates to what extent a semidirect product is not a direct product.

Proposition 20. Given any groups H and K with a group homomorphism $\varphi : K \to \operatorname{Aut}(H)$, the following properties are equivalent.

(a.) The set-theoretic identity map $\iota : H \rtimes_\varphi K \to H \times K$ is a group isomorphism.

(b.) The group homomorphism $\varphi : K \to \operatorname{Aut}(H)$ is trivial, i.e., we have that $\varphi(k)(h) = h$ for all elements k in K and h in H, i.e., $\varphi(k)$ is the identity automorphism for all elements k in K.

(c.) K_φ is normal in $H \rtimes_\varphi K$.

Proof. Given that $\iota : H \rtimes_\varphi K \to H \times K$ defined by $\iota(h,k) = (h,k)$ is a group isomorphism, it follows that for all ordered pairs (h_1, k_1) and (h_2, k_2) of $H \times K$, we have that

$$\underbrace{(h_1h_2, k_1k_2) = (h_1,k_1)(h_2,k_2)}_{\text{group structure of } H \times K} = \underbrace{\iota((h_1,k_1)(h_2,k_2)) = \iota(h_1\varphi(k_1)(h_2), k_1k_2)}_{\text{group structure of } H \rtimes_\varphi K} = (h_1\varphi(k_1)(h_2), k_1k_2).$$

Comparing the left- and right-hands sides and using the cancellative property of H, we find that $h_2 = \varphi(k_1)(h_2)$ for all elements h_2 of H and all elements k_1 of K, as desired.

Given that φ is trivial, for any elements (h_1, k_1) of $H \rtimes_\varphi K$ and (e_H, k) of K_φ, we have that

$$(h_1,k_1)(e_H,k)(h_1,k_1)^{-1} = (h_1\varphi(k_1)(e_H), k_1k)(\varphi(k_1)^{-1}(h_1^{-1}), k_1^{-1})$$

$$= (h_1, k_1k)(h_1^{-1}, k_1^{-1})$$

$$= (h_1\varphi(k_1k)(h_1^{-1}), k_1kk_1^{-1}) = (h_1h_1^{-1}, k_1kk_1^{-1}) = (e_H, k_1kk_1^{-1}).$$

Considering that $k_1kk_1^{-1}$ is in K, it follows that K_φ is a normal subgroup of $H \rtimes_\varphi K$.

Given that K_φ is normal in $H \rtimes_\varphi K$, it follows that for all elements h_1 in H and for any k and k_1 in K, there exists an element k_2 in K such that $(h_1,k_1)(e_H,k)(h_1,k_1)^{-1} = (e_H,k_2)$. Consequently, we have that $(h_1,k_1)(e_H,k) = (e_H,k_2)(h_1,k_1)$ as elements of $H \rtimes_\varphi K$ so that

$$(h_1, kk_1) = (h_1\varphi(k_1)(e_H), kk_1) = (h_1,k_1)(e_H,k) = (e_H,k_2)(h_1,k_1) = (\varphi(k_2)(h_1), k_2k_1).$$

Considering these as elements of the group $H \times K$, we have that $\varphi(k_2)(h_1) = h_1$ and $k = k_2$ by the cancellative property of K. Considering that h_1 and k are arbitrary, it follows that $\varphi(k)$ is the identity automorphism on for all elements k in K. But this implies that

$$\iota((h_1,k_1)(h_2,k_2)) = \iota(h_1\varphi(k_1)(h_2), k_1k_2) = \iota(h_1h_2, k_1k_2) = (h_1h_2, k_1k_2) = (h_1,k_1)(h_2,k_2)$$

for any ordered pairs $(h_1,k_1), (h_2,k_2) \in H \times K$, hence ι is a group isomorphism. $\square$

Example 6. Consider the semidirect product of $H = \mathbb{Z}_3$ and $K = \mathbb{Z}_4$ with respect to the group homomorphism $\varphi : \mathbb{Z}_4 \to \operatorname{Aut}(\mathbb{Z}_3)$ defined by $\varphi(n + 4\mathbb{Z}) = \nu_n$, where $\nu_n : \mathbb{Z}_3 \to \mathbb{Z}_3$ is the **inversion** automorphism defined by $\nu(k + 3\mathbb{Z}) = (-1)^n k + 3\mathbb{Z}$. Prove that $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ has a cyclic Sylow 2-subgroup; then, deduce that $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ is not isomorphic to the alternating group A_4 on four letters or the dihedral group D_{12} (i.e., the group of symmetries of the hexagon).

Solution. By Proposition 19, we have that $|\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4| = |\mathbb{Z}_3||\mathbb{Z}_4| = 3 \cdot 4 = 2^2 \cdot 3$, and $(\mathbb{Z}_4)_\varphi \cong \mathbb{Z}_4$ is a cyclic subgroup of order 4, i.e., a cyclic Sylow 2-subgroup of order 4. Considering that A_4 does not have any elements of order 4, it follows that A_4 does not have a cyclic subgroup of order 4 so that $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ is not isomorphic to A_4. On the other hand, we claim that D_{12} has at least three elements of order 2 and that $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ has only one element of order 2.

Observe that the elements of D_{12} are of the form $r^i s^j$ for some integers $0 \leq i \leq 5$ and $0 \leq j \leq 1$ with $srs = r^{-1}$. Evidently, we have that s, r^3, and rs are all elements of order 2. Each element of $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ is of the form $(a + 3\mathbb{Z}, b + 4\mathbb{Z})$ and satisfies $(a+3\mathbb{Z}, b+4\mathbb{Z})(a+3\mathbb{Z}, b+4\mathbb{Z}) = (a + (-1)^b a + 3\mathbb{Z}, 2b + 4\mathbb{Z})$, hence an element of $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ has order 2 if and only if $3 \,|\, (a + (-1)^b a)$ and $4 \,|\, 2b$. Considering that $4 \,|\, 2b$ if and only if $2 \,|\, b$, it follows that $b + 4\mathbb{Z} = 0 + 4\mathbb{Z}$ or $b + 4\mathbb{Z} = 2 + 4\mathbb{Z}$. Either way, we have that $a + (-1)^b a = 2a$, from which it follows that $3 \,|\, 2a$ if and only if $3 \,|\, a$ if and only if $a + 3\mathbb{Z} = 0 + 3\mathbb{Z}$. Consequently, the only element of order 2 in $\mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ is $(0 + 3\mathbb{Z}, 2 + 4\mathbb{Z})$. $\diamond$

Example 7. Given a group H, we define the **holomorph** of H to be the semidirect product of $H \rtimes_\iota \operatorname{Aut}(H)$ with respect to the identity homomorphism $\iota : \operatorname{Aut}(H) \to \operatorname{Aut}(H)$, i.e., we have that $\operatorname{Hol}(H) = H \rtimes_\iota \operatorname{Aut}(H)$. Given that $H = \mathbb{Z}_2 \times \mathbb{Z}_2$, prove that $\operatorname{Aut}(H) \cong \mathfrak{S}_3$ and $\operatorname{Hol}(H) \cong \mathfrak{S}_4$.

Proposition 21. Consider the semidirect product of H and K with respect to the group homomorphism $\varphi : K \to \operatorname{Aut}(H)$. We have the set-theoretic fact that

$$[Z(H) \cap \operatorname{Fix}(\varphi(K))] \times [Z(K) \cap \ker \varphi] \subseteq Z(H \rtimes_\varphi K),$$

where $\operatorname{Fix}(\varphi(K))$ is the set of elements in H that are fixed by all automorphisms of $\varphi(K)$.

Proof. Given any elements h in $Z(H) \cap \operatorname{Fix}(\varphi(K))$ and k in $Z(K) \cap \ker \varphi$, we have that

$$(h, k)(h_1, k_1) = (h\varphi(k)(h_1), kk_1) = (hh_1, kk_1) = (h_1 h, k_1 k) = (h_1 \varphi(k_1)(h), k_1 k) = (h_1, k_1)(h, k)$$

for any (h_1, k_1) in $H \rtimes_\varphi K$. Explicitly, we have that $\varphi(k)(h_1) = h_1$ because k is in $\ker \varphi$, i.e., $\varphi(k)$ is the identity automorphism on H; $hh_1 = h_1 h$ and $kk_1 = k_1 k$ because h and k are in the center of H and K; and $h = \varphi(k_1)(h)$ because h is in $\operatorname{Fix}(\varphi(K))$, i.e., h is fixed by all automorphisms. $\square$

Q1c., January 2017. Consider a prime integer p. Give an example of a non-abelian group of order p^n whose center contains more than one normal subgroup of order p.