Notes on Finite Groups and Subgroups[1]

These notes assume an elementary understanding of sets, functions, binary relations, binary operations, and categories.

The symmetry revealing actions that result in distinct states of a regular polygon (rotations only or rotations and reflections) create an interesting pattern. We can model this set of actions and their combinations as actions in succession with a binary operation that is associative, has identity, and has inverses. We call these structures groups. We might wonder if all binary operations with these characteristics imitate symmetry revealing actions. We notice how closely related symmetry is to beauty, and we might wonder how much complexity there might be hidden behind the elegant interplay of symmetries.

When observing the group formed on a two-dimensional regular polygon represented by a non-rectangular rhombus, we notice a few things. First, it has four elements. We call the size of a group its order. Next, it is commutative. We call commutative groups abelian groups after the pioneer of group theory, Niels Henrik Abel. Finally, all the elements of the group are their own inverses. We might wonder what other groups have these properties. Though we won't make sense of it now, we call this family of groups on regular n-gons D_{2n}. Though the "D" stands for dihedral, for now you might think of it as the rotations and reflections across a "diagonal."

We can record all the interactions of elements in the group on a Cayley table. The commutativity is represented by a symmetry across the diagonal. The self-inverse property is represented by a diagonal made up of only identity elements. Studying the Cayley table of the group acting on the rhombus, we find that it satisfies the sudoku rules. This motives our first theorem:

(The Sudoku Rule) Linear equations over finite groups have solutions and those solutions are unique. *Proof.* Let $ax = b$ and $ya = b$ be equations over a group $\mathcal{G}$ with variables x and y and a' be the inverse of a. We can construct the solutions $x = a'b$ and $y = ba'$. Then, assume that the equation $ax = b$ has two solutions, x_1 and x_2. If $ax_1 = b$ and $ax_2 = b$, $x_1 = a'b = x_2$. Thus, the solution of $ax = b$ is unique. A similar argument demonstrates that the left-hand solution y is also unique.

καὶ ἐγένετο φῶς

This is a big step beyond knowing that the identity is unique and inverse pairs are distinct. We might wonder how many groups can exist of a given order, and this information goes a long way toward exploring that question for small groups. For exploration, we might try to find all the possible group structures for orders four, five, and six.

When observing the actions on an equilateral triangle, D_6, we find a similar group structure. In this case, it has order six; it is not commutative; and two elements have distinct inverses. For exploration, we might create a Cayley table for this group or the similar group of actions on a square.

[1] Elliott Best, Proofs and Modern Mathematics, *Jackson Hole Classical Academy*, Spring 26.

After we have defined a mathematical pattern, one of the first things we wonder about are sub-patterns or subobjects, in this case, subgroups. We write $H < G$ to say that H is a subgroup of G, and we often talk about non-trivial subgroups to exclude $\{e\}$ or proper subgroups to exclude the group itself.

We can find, for example, that D_4 three subgroups of order two, and the group on the triangle has one subgroup of order three and three subgroups of order two. We can display these subgroups and their partial ordering with a directed graph called a subgroup diagram or a subgroup lattice. To explore, we might create a subgroup diagram for the subgroups of the actions on a square. After some practice, I recommend creating a template for these diagrams in LaTeX.

Note that because a subgroup is a part of a larger group structure, to prove a set is a subgroup we can assume associativity as inherited, and we only need to demonstrate closure, identity, and inverses.

Further observing D_6, we notice that there is some notion of isomorphism between it and the set of permutations on three elements under composition. The reflections can correspond to the transpositions and generate the rest the relation. In this way all the characteristics of the group we have observed are represented equally in both structures.

(The Permutation Group on n-Elements) The permutations on n elements are a group under composition. Sometimes we call this family of groups P_n. *Proof.* The composition of bijections is a bijection, the identity permutation has the properties of an identity element, and a function is a bijection if and only if it has an inverse.

φῶς ἐκ φωτός

We might wonder if all groups are isomorphic to a permutation group. Toward that end we observe that there is the same notion of isomorphism between the actions on the rhombus and the permutation elements (), (12), (34), and (12)(34). So, rather, we might wonder if all groups are isomorphic to a subgroup of a permutation group. For exploration, we might create a Cayley table and subgroup diagram for the permutation group on four elements.

After finding subgroups, we want to characterize them, understand what types of subgroups can exist, and understand the role subgroups play in the larger structure of the group.

(Center Subgroup) The set of all elements that commute with every element in the group is a subgroup called the center. *Proof.* Let $\mathcal{G}$ be a group. If a and b commute with every $g \in \mathcal{G}$, $(ab)g = agb = g(ab)$ and ab also commutes with every element in $\mathcal{G}$. The identity is included in the center by definition. If a commutes with every $g \in \mathcal{G}$ and its inverse is a', $a'g = (a'g)aa' = a'aga' = ga'$ and its inverse is also included in the center.

τὸ φῶς τῶν ἀνθρώπων

(Centralizer Subgroups) The set of all elements that commute with a single element a the group is a subgroup called the centralizer of a. By definition, the intersection of all the centralizers in a group is the center. *Proof.* As a weaker theorem, the proof is identical to that of the center subgroup. Let $\mathcal{G}$ be a group. If a and b commute with $g \in \mathcal{G}$, then $(ab)g = agb = g(ab)$. Of course, e commutes with every g. And if a commutes with g, then $a'g = a'gaa' = a'aga' = ga'$.

τὸ φῶς ἐν τῇ σκοτίᾳ φαίνει

The center and centralizers of an abelian group are the whole group. Therefore, this subgroup is only interesting in non-abelian groups. In that case when elements of a group don't commute, there exists a unique element that connects their distinct products. We call this a commutator.

(Commutator Subgroup) The set generated by all the commutators in a group is a subgroup called the commutator subgroup or the derived subgroup. *Proof.* By construction, closure is assumed. The identity is the commutator of itself. For all $a, b \in \mathcal{G}$, if $(ab)x = ba$, then $(ba)x' = ab$ where x' is the inverse of x. So, the inverse of a commutator is also a commutator.

ὡς τέκνα φωτὸς περιπατεῖτε

For exploration, we might find the center and commutator subgroup of the symmetry groups on a regular n-gon and the permutation groups on n elements for $2 \leq n \leq 4$. We can add this information to our subgroup diagrams.

As we explore these relationships, the behavior of the commutator subgroup in P_3 appears interesting. There is gravity in the imbalance of its closure and the fact that its elements are the products of all the transpositions. We might wonder if this is how all commutator subgroups behave. We might also wonder if the center is always a subgroup of the commutator subgroup or under what conditions it is.

(Intersection of Subgroups) The intersection of two subgroups is a subgroup. *Proof.* Let H and K be subgroups of $\mathcal{G}$ with shared elements a and b whose respective inverses are a' and b'. For all $a, b \in H \cap K$, by definition $a, b \in H$ and $a, b \in K$. Because H and K are subgroups themselves, $e, a', b', ab \in H$, $e, a', b', ab \in K$, and thus $e, a', b', ab \in H \cap K$.

ἐπιφαύσει σοι ὁ χριστός

We might wonder if the union of two subgroups is also a subgroup, but there is no way of ensuring that the union is closed. Instead, similar to the definition of the commutator subgroup, we can relax closure and wonder what two subgroups generate.

(Subgroup Product) Any two subgroups generate a new subgroup called the subgroup product. *Proof.* Let H and K be subgroups of $\mathcal{G}$. By definition, we assume that the product HK is closed. The identity is certainly included. Then, if $ab \in HK$ and a' and b' are the inverses of a and b respectively, $b'a' \in HK$ and $(ab)(b'a') =$ with shared elements a and b whose respective inverses are a' and b'. For all $a, b \in H \cap K$, by definition $a, b \in H$ and $a, b \in K$. Because H and K are subgroups themselves, $e, a', b', ab \in H$, $e, a', b', ab \in K$, and thus $e, a', b', ab \in H \cap K$.

ἐκ σκότους φῶς λάμψει

(Element Generated Cycles) The set of elements generated by a single element forms a subgroup. We call this a cyclic group or subgroup depending on the context. We sometimes notate the cyclic group of order n as C_n. Based on this theorem we can begin notating the inverse of a as a^{-1}. We talk about the order of an element in reference to the order of the subgroup it generates. *Proof.* Let $\mathcal{G}$ be a group with $a \in \mathcal{G}$. For $m, n \in \mathbb{N}$, $a^m a^n = a^{m+n}$ by the axioms of counting. Now, consider the elements generated by a each represented by a^k for some $k \in \mathbb{N}$. As a consequence of the uniqueness of the identity, until $a^k = e$, each element generated by a is unique. However, at some point this set of distinct elements will exceed the size of the group, and so a^k must equal e for some value of k by the sudoku theorem. This suggests we can expand the exponent notation to integers in a well-defined way. By additivity of exponents, if $(a^k)(a^1) = a$, then $a^k = a^0 = e$, and if $(a)(a^m) = a^k = a^0 = e$ for some m, then a^{-1} is the inverse of a.

ὃς ἔλαμψεν ἐν ταῖς καρδίαις

Based on the theorem above, we can create another representation of groups called a cycle diagram. We call a subgroup maximal if there is no other subgroup that contains it besides the group itself. Cycle diagrams are graphs that represent all the maximal cycles and their generators.

(Cyclic Groups and the Integers Modulo n) Every cyclic group order n is isomorphic to the integers modulo n under addition. Because of this we often notate cyclic groups as $\mathbb{Z}_n$ instead. *Proof.* Let $\mathcal{G}$ be a cyclic group generated by a. For all $k \in \mathbb{Z}$, consider the correspondence of a^k to $k \mod n$. Without a formal definition of isomorphism, it is clear that both groups exhibit the same structure based on the additive law of exponents and the modular congruence of cycles.

φωτισμὸν τῆς γνώσεως

(Abelian Order Subgroups) In an abelian group $\mathcal{G}$, the sets $H_n = \{x \in \mathcal{G} : x^n = e \text{ for some } n \in \mathbb{N}\}$ are subgroups. *Proof.* If $a, b \in H_n$, then $a^n = e$ and $b^n = e$. Similarly, by commutativity $(ab)^n = a^n b^n = e$. For all $n \in N$, $e^n = e$. If $x^n = e$, then $(x^{-1})^n = (x^m)^n = (x^n)^m = (x^n)^m = e^m = e$ for some $m \in \mathbb{N}$.

τῆς δόξης τοῦ ϑεοῦ

At this point, we are running low on groups to study. After we look inside of groups for the same structure, we turn ourselves inside out and consider how we might combine groups to create larger groups. The simplest way to do this is by defining a component-wise operation on the cartesian product. It turns out, this is the categorical product of groups.

(Direct Product Groups) If G and H are groups under the operations $\star_G$ and $\star_H$ respectively, then the cartesian product $G \times H$ is a group under the operation $(g_1, h_1) \star (g_2, h_2) = (g_1 \star_G g_2, h_1 \star_H h_2)$. By construction, this structure inherits all the group products trivially from its component groups. The identity is (e_G, e_H) and the inverse of (a, b) is (a^{-1}, b^{-1}).

For exploration, we might create cycle diagrams for $\mathbb{Z}_2 \times \mathbb{Z}_2$ (Is this a new group of order 4?), $\mathbb{Z}_2 \times \mathbb{Z}_4$ (Does this appear to be isomorphic to the actions on a square?), and $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_2$ (Does this suggest an infinite family of finite groups?). For a challenge, we might investigate $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times P_3$. Based on the cartesian product we know it is order 12. We might wonder about the character of an abelian group times a non-abelian group. The answer is clear from the definition of the direct product.