Essays on Algebra

James B. Wilson

April 3, 2003

Contents

Chapter I

Heuristics

I.1 Classics

I.1.1 Induction

I.1.2 Contrapositive vs. Contradiction

Both of these methods involve the negation of certain elements in an inference and so at times are confused. We reitterate their definitions to analyze the problem.

Proof by the **contrapositive**:

$$\begin{array}{lcl} \neg B & & \\ \neg B & \Rightarrow & \neg A \\ \hline A & \Rightarrow & B. \end{array}$$

Proof by **contradiction**:

$$\begin{array}{lcl} A & \Rightarrow & \neg B \\ & \Rightarrow\Leftarrow & \\ \hline A & \Rightarrow & B. \end{array}$$

Sometimes a proof reads something like this: Prove for every $a \in \mathbb{R}$, $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = ax$ is injective implies $a \neq 0$. **Proof:** Suppose $a \neq 0$ and that f is not injective. Whenever $f(x) = f(y)$ for some $x, y \in \mathbb{R}$. This requires $ax = ay$ and since $a \neq 0$ we know $1/a$ exists in $\mathbb{R}$ so we cancel to get $x = y$. Therefore f *is* injective contradicting our assumptions. Therefore by contradiction when $a \neq 0$, f is injective. $\square$

The concepts of the proof are correct but the

I.1.3 Equivalence

Do one step in a path, then it is true for the general path.

I.2 Needle-In-The-Haystack

Intent

Prove the existance of a unique solution or solution set. [1]

Motivation

When asked to prove existance, it is not uncommon to see a proof that majically proclaims some object into existance that some how verifies the properties required. This method is opaque in that a method to construct solutions is hidden from the reader. Often times the added condition that a result is unique helps seal a given solutions validity; certainly if there can be only one answer and we are lucky enough to have it, then chances are high that it is a correct answer. To illustrate this, consider the problem of finding the intersection of $f(x) = x^2 + 3x$ and $g(x) = -x - 4$.
Example:

- *Show a solution exists.* Given (2,-2) notice $f(2) = -2$ and $g(2) = -2$; therefore, $f(2) = g(2)$, so $(2, -2)$ is a point of intersection of the functions f and g.
- *Assume there are two solutions and show they are equivalent.* Now suppose f and g intersect at two pointes (x_1, y_1) and (x_2, y_2); $f(x_1) = g(x_1)$ and $f(x_2) = g(x_2)$ so that $f(x_1) - g(x_1) = 0 = f(x_2) - g(x_2)$.

$$\begin{aligned} f(x_1) - g(x_1) &= f(x_2) - g(x_2); \\ (x_1^2 + 3x_1) - (-x_1 - 4) &= (x_2^2 + 3x_2) - (-x_2 - 4) \\ x_1^2 + 4x_1 + 4 &= x_2^2 + 4x_2 + 4 \\ (x_1 + 2)^2 &= (x_2 + 2)^2 \\ |x_1 + 2| &= |x_2 + 2| \end{aligned}$$

  Now we know of one solution so we let $x_1 = 2$ which forces then $|x_2 + 2| = 4$ and so $x_2 = 2$. This proves (2,-2) is the unique solution.

□

Those readers that paid attention to the example will not be surprised to discover that it is incorrect. A graph of the two functions will immediately demonstrate (2,-2) is *not* a solution much less a unique one. We will get to the true solution in a moment. This illustrates a downside to this approach of existance and uniqueness proofs.

When we break down the proof into its logical components we can state the structure as follows:

- Let A and B be classes – in our examples these are solutions (x, y);
- S a sentence – here S is $f(x) = x^2 + 3x$ and $g(x) = -x - 4$;
- with T a sentential function of classes A and B – in the example T is $(x, f(x)) = (x, g(x))$;
- and finally we ask: does $S \Rightarrow \exists! A(T(A))$?;

and we prove it as follows:

$$\begin{array}{l} S \\ \exists A(T(A)) \\ \exists A, B(T(A) \wedge T(B)) \Rightarrow A = B \\ \hline \exists! A(T(A)). \end{array}$$

Now we look at an alternate structure for existance proofs.

[1] Thanks to Professor F.R. Beyl for this heuristic

Requirements

We consider any class A. The class may be a proper class, a set, or degeneratively an object or element. The heuristics works on existential sentential functions – sentences of the from:

$$\exists! A(S(A)),$$

where $S(A)$ is a sentential function of A. Refer to [Tar95] for details on the definitions of the logical constructions.

This means we require a sentence of the form: there exists a unique class A which validates (makes true) a statement S about A. For instance: there exists a unique x such that $x+2=5$ in $\mathbb{N}$.

Heuristic

$$\begin{aligned} \exists! A(S(A)) &\equiv \exists! B((B=A)\wedge S(A)) \\ &\equiv \exists! B((B=A)\wedge S(B)) \\ &\equiv \exists! B((\exists A(S(A))\Rightarrow B=A)\wedge S(B)). \end{aligned}$$

This means, given a sentence in the form: there exists a unique A such that a statement S verifies some property of A, we can make the same assertion by: (1) asserting there is an A which S validates; (2) there is a unique form B which A must assume; and (3) $S(B)$ is valid.

The title of *needle-in-the-haystack* heuristic illustrates the procedure. If we want the needle burried in the haystack we may approach the problem as in the first example and search till we find one, but we still have the task of searching the rest of the stack to prove this is the only one. If instead we first confirm there is only one needle, then when we have found one we may stop. In the general solution set case, if we first can confirm all needles are concentrated in a corner of the haystack, then we need only isolate this corner to find all the needles.

Usage

Consider the proof of the statement: $S \Rightarrow \exists! A(T(A))$, where S is a sentence and T a sentential function.

$$\begin{array}{l} S \\ \exists A(T(A)) \quad \Rightarrow \quad \exists! B(B=A) \\ T(B) \\ \hline \exists! A(T(A)). \end{array}$$

Now it appears that this method has more elements and thus requires more work. The advantage of this method is once step two is completed, step three is simplified because the target of possible classes is reduced to one. This one needs only to be verified.

A special point should be made about the process involved in this heuristic. Although the logic reveals the two class and then shows they are equal, the difference with the orignal approach is that we do no assume B exists or that it satisfies $T(B)$ to begin with. We must first construct what B should be, that is construct parameters for the A, only in our final step do we verify $T(B)$ is true – the existance part. In this regard it should not be confused with a proof in the form:

$$\begin{array}{l} S \\ \exists A, B(T(A), T(B)) \quad \Rightarrow \quad A=B \\ \exists A(T(A)) \\ \hline \exists! A(T(A)). \end{array}$$

which is nothing more than rearranging the order of the statements in the original existance proof technique.

Consequences

In some instance the class we must identify as existing uniquely is immediately evident. In such a case it can often be more efficient to identify this candidate first and pass the majority of the work to verifying uniqueness. For instance with algebra often times a candidate for identity is easily found, and the uniqueness follows almost instaneously. In such a case verifying first any identity is unique, may be redundent. *If you see the needle before you start looking, go ahead and pick it up.*

The needle-in-the-haystack heuristic may also interfear with certain proofing algorithms – such as those requied by compilers and optimization systems. The same implementation that searchs for a solution can be used to verify uniqueness, thus reducing complexity. However there is generally no direct approach to proving uniqueness of arbitrary statements; and, furthermore, given such an implementation the process still requires separate implementation to verify the conjectured unique class exists. *Although it would be nice to first know there is only one needle, the heuristic offers no method to reach this conclussion. Originally at least we knew the method of exhaustion (search the entire space) was a way to start.* [2]

Implementation

Using the same example we now use the naïve approach a high school math class would employ and observe it follows the needle-in-the-haystack heuristic.
Example:

$$\begin{aligned} x^2+3x &= -x-4; \\ x^2+4x+4 &= 0; \\ (x+2)^2 &= 0; \\ |x+2| &= 0; \\ x &= -2. \end{aligned}$$

So (-2,-2) is the solution, but we must check.

$$\begin{aligned} f(-2) &= (-2)^2+3(-2) = -2; \\ g(-2) &= -(-2)-4 = -2. \end{aligned}$$

□

First we locate the parameters of the unique solution, then we verify it is a solution.

I.3 Principle of Refinement

Consider Exercise-**??**. Two questions are asked in the exercise: first is the set $\{\sigma \in S_n \mid \sigma(n) = n\}$ a subgroup of S_n, and next is it isomorphic to S_{n-1}? Certain properties for subgroups will simplify the fisrt question and prove it is in fact a subgroup, however these properties do not resolve the question of wheter it is isomorphic to some other group. It is however to answer both questions simultaneously through the use of the *Principle of Refinement*. Consider the following theorem.

Theorem I.3.1 (Principle of Refinement) *Let A and B be groupoids (i.e.: sets with a binary operation). Given a mapping $f : A \to B$ such that $f(ab) = f(a)f(b)$ for all $a, b \in A$, define*

[2] Despite this lack of a clear starting point, the needle-in-the-haystack seems surprisingly congruent with human mathematical intuition.

$f(A) = \{x \in B \mid x = f(a)$ for some $a \in A\}$, it follows if $a_1, \ldots, a_m$ and $b_1, \ldots b_n$ are elements in A with the property that

$$a_1 \cdots a_m = b_1 \cdots b_n,$$

in the standard n-product, then the sequence of elements $f(a_1), \ldots, f(a_m)$ and $f(b_1), \ldots, f(b_n)$ are in $f(A)$ and have the property

$$f(a_1) \cdots f(a_m) = f(b_1) \cdots f(b_m),$$

again in the standard n-product.

Proof: Induction. □

While the definitions are seemingly trivial, and proved as such, the statement made by this theorem is fundamental: mappings with the homomorphism property preserve relations. The study of free groups makes it evident that each group is determined by its relations and thus homorphisms play a large role in understanding groups. Note we must be careful in how we percieve a relation to be preserved. It is completely possible for a homomorphism to preserve a relation by trivializing it; that is by making it equivalent to stating something obvious such as $x = x$. The relation remains true but may no longer be meaningful. The power of the principle lies in the following corollary.

Corollary I.3.2 *All the following are true:*

- *if G is a semigroup then $f(G)$ is also and furthermore f is a homomorphism;*
- *if G is a monoid then so is $f(G)$;*
- *if G is a group then $f(G)$ is a group.*
- *if G is an abelian group then $f(G)$ is abelian.*

Proof:

- If G is a semigroup then for all $a, b, c \in G$ we know $a(bc) = (ab)c$. By Theorem-I.3.1 it follows

  $$f(a)(f(b)f(c)) = f(a)f(bc) = f(a(bc)) = f((ab)c) = f(ab)f(c) = (f(a)f(b))f(c).$$

  So it is evident that the binary operation of A is associative with in the closed subset $f(G)$. Therefore $f(G)$ is a semigroup.

- Suppose G is a monoid, then there exists an element $e \in G$ which is the identity in G with the property $ae = a = ea$ for all $a \in G$. Applying Theorem-I.3.1 it must be that

  $$f(a)f(e) = f(a) = f(e)f(a).$$

  Therefore $f(e)$ is a two sided identity in $f(G)$ and so it is the identity for (the now termed) monoid $f(G)$.

- Consider G as a group. Every element $a \in G$ has an inverse a^{-1} and $a^{-1}a = e = aa^{-1}$ holds in G so by Theorem-I.3.1 the image has the relation:

  $$f(a^{-1})f(a) = f(e) = f(a)f(a^{-1}).$$

  Therefore $f(a^{-1})$ behaves as the inverse for $f(a)$ and so it is the inverse leaving $f(G)$ closed to inverses and so it is a group.

- Supposing G is abelian it follows given $a, b \in G$, $ab = ba$ and so once again by the Principle of Refinement $f(a)f(b) = f(b)f(a)$ in $f(G)$, so $f(G)$ is abelian.

□

Now returning the the exercise, consider constructing a map $f : S_{n-1} \to S_n$ that has the homomorphism property, and such that its image $f(S_{n-1})$ is simply the set $\{\sigma \in S_n \mid \sigma(n) = n\}$. Then by Corollary-I.3.2 it is automatic to state $f(S_{n-1})$ is a group, and thus a subgroup. And in addition we have a candidate for an isomorphism in hand. In this fashion we need not even know S_n is a group but only use that it has a well-defined binary operation.

It is important to emphasize that the properties apply to $f(G)$ and not to the entire codomain. Exercise-**??** illustrates a situation where a careless generalization will fail.

The morphism principle is in fact a general heuristic for categories.

Definition I.3.3 *A category $\mathscr{D}$ is a refinement of a concrete category $\mathscr{C}$ if given any object A in $\mathscr{D}$ and any morphism $f \in Hom_{\mathscr{C}}(A, -)$, then $f(A)$ is an object in $\mathscr{D}$.*

A refinement therefore introduces a restriction on the objects in a category in such a way as to be complatible with all morphisms. Theorem-I.3.1 can be stated as follows:

Definition I.3.4 *A mapping R from a category $\mathscr{C}$ to the set $\{True, False\}$ is rule whenever $R(\mathscr{C})$, defined as the set of all objects in $\mathscr{C}$ that evaluate to true, is a subcategory of $\mathscr{C}$.*

A relational rule is a rule on the category of groupoids defined as true whenever some relation $\prod_{i=1}^{m} a_i = \prod_{j=1}^{n} b_j$ is true for all elements in an object A.

Theorem I.3.5 *Every relational rule determines a refinement.*

Refinement can of course take place in other categories.

Example: The category of connected spaces is a refinement of the category of all topologies. This is evident because continuous functions on connnected spaces have connected images. [PENDING: reference]

However the category of complete spaces is not a refinement of the category of topologies. This can be seen because completeness is not a topological invariant. For example consider the continuous function e^x defined on the complete domain $\mathbb{R}$ and mapping surjectively onto $\mathbb{R}^+$. $\mathbb{R}^+$ has the cauchy sequence $(1/n)_{n\in\mathbb{Z}^+}$ which converges outside $\mathbb{R}^+$ to 0; thus $\mathbb{R}^+$ is not complete and so $e^{\mathbb{R}}$ is not in the subcategory, so the category is not a refinement. □

Chapter II

Subgroup Lattices

II.1 Lattices

A partially ordered set is a set that contains a pairwise relation that is reflexive, antisymmetric, and transitive. A partially ordered set is traditionally depicted as a simple oriented graph in which nodes represent elements in the set and edges connect elements virtically so that the lower element is less than the upper element in the ordering. Generally edges connect elements that preceed each other in the ordering and it is assumed any path from bottom to top relates to any additional orderings; vertical paths are valid relations since partially orderings are transitive,

A *lattice* is a partially ordered set, L, in which every pair of elements $a, b \in L$, there exists a unique *greatest lower bound* $a \Downarrow b$ and a *least upper bound* $a \Uparrow b$ in L. By definition $a \Downarrow b$ and $a \Uparrow b$ are associative, commutative and idempotent.

A lattice may not have the following relationship between any four distinct elements (that is any full subgraph which is a subdivision of the following graph):[1]

$$a \qquad b$$

$$c \qquad d,$$

and instead for any two elements a and b we insist the following be a full subgraph of the lattice:

$$a \Uparrow b$$

$$a \qquad\qquad b$$

$$a \Downarrow b.$$

A *bottom element* of a lattice L is an element $0 \in L$ such that given any $x \in L$, $0 \Downarrow x = 0$. Analogously a *top element* is an element $1 \in L$ such that $1 \Uparrow x = 1$. Naturally these elements are unique since $0 = 0 \Downarrow 0' = 0'$ and $1 = 1 \Uparrow 1' = 1'$.

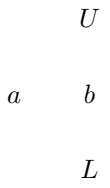
A partially ordered set P is *complete* if every nonempty subset, S, has both a greatest lower bound $\Downarrow S$ and a least upper bound $\Uparrow S$ in P; again both are unique given S. Every complete set is a lattice. If a lattice is complete then $\Downarrow S = \Downarrow_{a \in S} a$ and $\Uparrow S = \Uparrow_{a \in S} a$ by definition. If a lattice is finite then it is complete.

[1] This means a subgraph that contains all edges for which both nodes are included; furthermore, subdivision means nodes may be added on any edge as required to match the situation.

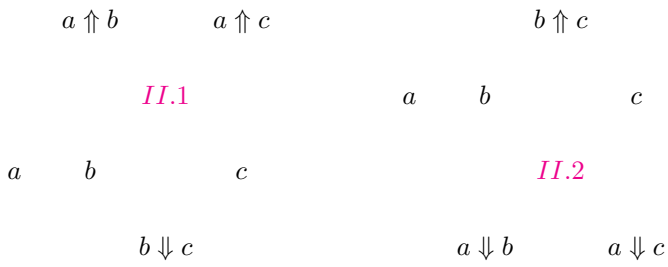
A lattice, L, is *distributive* if given $a, b, c \in L$, it follows:

$$a \Uparrow (b \Downarrow c) = (a \Uparrow b) \Downarrow (a \Uparrow c), \tag{II.1}$$
$$a \Downarrow (b \Uparrow c) = (a \Downarrow b) \Uparrow (a \Downarrow c). \tag{II.2}$$

A distributive lattice may not have a full subgraph which is a subdivision of the following (assume all nodes are distinct):



since $a \Uparrow (b \Downarrow c) = a \Uparrow U = a$ but $(a \Uparrow b) \Downarrow (a \Uparrow c) = U \Downarrow U = U$; II.2 also fails for a, b and c. In fact distributive lattices force the following structure on the lattice, (where the nodes need not be distinct):



To appreciate the complexity of distributive lattice study Figure-II.1 which illustrates in three dimensions what a typical distributive lattice must contain around each three nodes – note in some cases the nodes may not all be disjoint.

Suppose L is a lattice with top element 1 and bottom element 0. A lattice, L, is *complemented* if for every element $a \in L$, there exists an element $a^c \in L$ such that $a \Downarrow a^c = 0$ and $a \Uparrow a^c = 1$.
Example:

- The set of all subsets of a set is a complete, complemented, distributive lattice.
- The subgroups of a group form a complete lattice.
- The normal subgroups of a group form a complete modular lattice.
- The subgroup lattices of $\mathbb{Z}_p$, $\mathbb{Z}_{pq}$, $\mathbb{Z}_p \oplus \mathbb{Z}_p$, and S_3, are examples of complemented subgroup lattices; the groups $\mathbb{Z}_m$ $(m \neq pq)$, D_n and S_n with $n \geq 4$, are all non-complemented lattices.
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, and S_3 are groups which have non-distributive subgroup lattices.

□

An important observation with greatest lower bounds and least upper bounds is that they are completely determined by the ordering of the elements in the lattice. This means, although a definition is given for a least upper bound in some lattice, this definition is equivalent to any other definition that also matches the ordering. Therefore for instance the join of subgroups $\{H_i \mid i \in I\}$ can be defined equivalently as: the intersection of all subgroups which contains all H_i, the group generated by the union of each H_i, or the least subgroup which contains all H_i. Each definition should be verified as a compatible definition, but once known each from is interchangable.

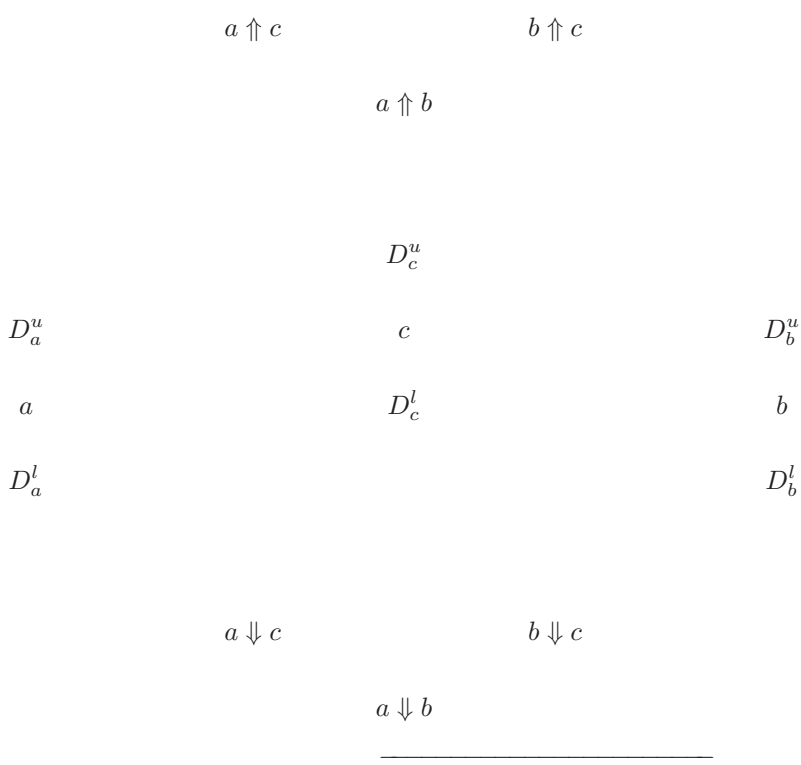
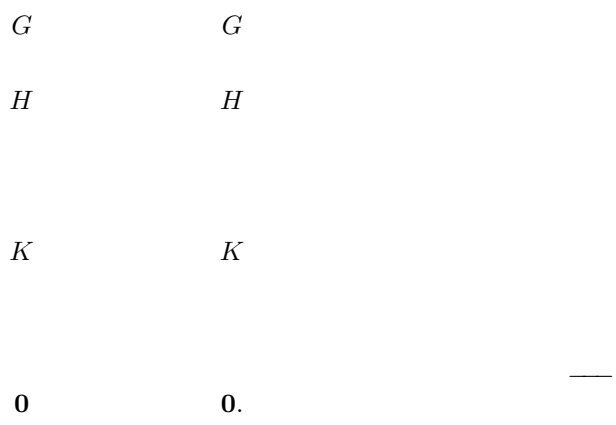


Figure II.1: 3-D Model of a Distributive fragment of a Lattice;
$D_x^u = x \Uparrow (y \Downarrow z)$ and $D_x^l = x \Downarrow (y \Uparrow z)$.

The subgroup lattice of a group always has a top and bottom element, namely **0** and G, where **0** is the set generated by the identity and G is the entire group. Despite having top and bottom elements, maximal and minimal subgroups of G are generally assumed to be proper subgroups.

Since normality is not transitive two distinct notations are adopted to illustrate normality in a subgroup lattice. In the case where $H \lhd K$, wher $H, K \leq G$, but H is not normal in G (the so called *local normal* case), the lattice is depicted as in the left diagram. However if H is also normal in all of G then the lattice is depicted as on the right.

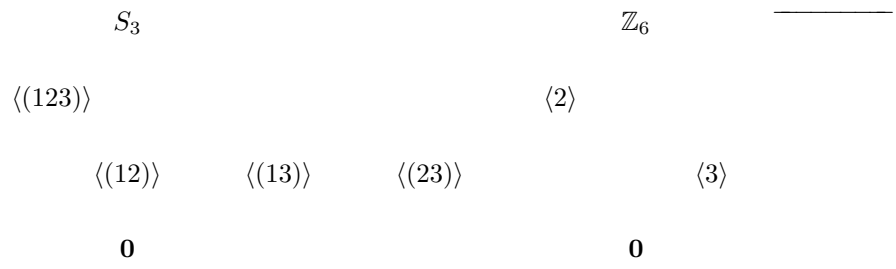


Therefore the normal subgroup lattice can be picked out from the full subgroup lattice by deleting any edges that are not highlighted with $\lhd\lhd$. Although **0** is always normal in every subgroup, the notation is generally omited unless context requires an explicit use of this added information.[2]

When given a specific example group, the length of the edges can be proportioned to illustrate the relative orders of the subgroups. Generally this is done by making the unit length equal to the greatest common divisor of all indices in the subgroup lattice. [3] Subsequent edges scale by the ratio of their index to that of this unit index. This is contrary to the typical edge length ideal for sets which seeks to make edge lengths match the relative cardinalities of the elements. When proportions are considered, the edges may be labeled with the index and if any two subgroups are on the same vertical level then they can be assumed as having the same order.[4]

Subgroup lattices may also occasionally include horizontal dashed line segments. These lines connect subgroups that are conjugate, and thus isomorphic. Some presentations may label these edges with a conjugating element, although this rarely includes all possible conjugating elements.

Example:



□

[2] It is common to add this when identifing a normal sequence, such as a central sequence.

[3] From the first Sylow Theorem we see unless the group is a p-group, then the unit length will thus be one, even though no edge in the graph will have length one.

[4] By the Theorem of Lagrange the order can be calculated by taking the product of all the indicies from the subgroup **0** to the subgroup in question.

II.2 Subgroup Lattices

Visualizing a lattice can offer insightful properties to a structure. In the context of groups, extensions, normality, centrality, decomposition (Krull-Schmidt) and many other properties can be determined from the lattice. The trouble with lattices is size; the lattices of groups of orders greater than 12 are generally too complex to be drawn in the plane. We investigate properties of subgroup lattices that can aid the visualization of these lattices of high order groups. We also discuss their construction in $\mathbb{R}^3$.

Definition II.2.1 (Class Ordering) *Given two conjugacy classes $\mathscr{A}$ and $\mathscr{B}$ of a group G, $\mathscr{A} \leq \mathscr{B}$ if for every subgroup $H \in \mathscr{A}$, there exist a subgroup $K \in \mathscr{B}$ such that $H \leq K$. The ordering is called the* class ordering *of G.*

Remark II.2.2 *It is equivalent to say every subgroup in $\mathscr{B}$ has a subgroup in $\mathscr{A}$.*

Lemma II.2.3 *Let G be a group with $g \in G$, and H and K subgroups.*

(a) $H \leq K$ if and only if $gHg^{-1} \leq gKg^{-1}$.

(b) $H \leq gKg^{-1}$ if and only if $g^{-1}Hg \leq K$.

(c) If $gHg^{-1} \leq H$ or $H \leq gHg^{-1}$ then $gHg^{-1} = H$.

Proof:

(a) When $H \leq K$ we see for every $h \in H$, $h \in K$; thus, $ghg^{-1} \in gKg^{-1}$ leaving $gHg^{-1} \leq gKg^{-1}$. If $gHg^{-1} \leq gKg^{-1}$ then for every $h \in H$, $ghg^{-1} = gkg^{-1}$ for some $k \in K$. Thus by cancellation it follows $h = k$ and so $H \leq K$.

(b) This is an immediate consequence of part (a) as seen by conjugating by g^{-1}.

(c) Suppose $gHg^{-1} \leq H$, then for all $h \in H$, $ghg^{-1} = k$ for some $k \in H$. Thus $g^{-1}kg = h$ so in fact $g^{-1}Hg \leq H$. Using part (b) we may conclude $H \leq gHg^{-1}$ and we borrow the antisymmetry of subgroups to conclude $H = gHg^{-1}$. In the second case when $H \leq gHg^{-1}$ by part (b) it follows $g^{-1}Hg \leq H$ and so $H = g^{-1}Hg$ so in fact $gHg^{-1} = H$.

□

Proposition II.2.4 *The class ordering of a group is a partial ordering.*

Proof: Given any conjugacy class $\mathscr{A}$ of G, we know there exists a subgorup $A \leq G$ such that $\mathscr{A} = \{gAg^{-1} \mid g \in G\} = {}^GA$. By Lemma-II.2.3 part (a) we know ${}^GH \leq {}^GK$ if $H \leq K$ If $H \in {}^GA$ and $K \in {}^GB$ where $H \leq K$, then ${}^GA = {}^GH \leq {}^GK = {}^GB$, so the class ordering is well-defined.

Every subgroup is a trivial subgroup of itself, so ${}^GH \leq {}^GH$ for all subgroups H.

Given ${}^GH \leq {}^GK$ and ${}^GK \leq {}^GH$ it follows there exist a subgroup $K' \in {}^GK$ and another $gHg^{-1} \in {}^GH$ where $H \leq K' \leq gHg^{-1}$; however, this implies $H = gHg^{-1}$ by Lemma-II.2.3 part (c). Therefore $H \leq K' \leq H$ so $H = K'$ and ${}^GH = {}^GK$.

Finally, if ${}^GH \leq {}^GK \leq {}^GL$ then for every $H' \in {}^GH$ there exists a $K' \in {}^GK$ and a $L' \in {}^GL$ where $H' \leq K' \leq L'$ and since subgroup ordering is transitive it follows $H' \leq L'$ and so ${}^GH \leq {}^GL$. So we may conclude that class ordering a partial ordering. □

Example: Consider S_5 which has the following subgroups:

$$S_3^{x,y} = \langle (a,b,c),(a,b) \rangle, \qquad \mathbb{Z}_6^{x,y} = \langle (a,b,c)(x,y) \rangle, \qquad \mathbb{Z}_3^{x,y} = \langle (a,b,c) \rangle, \qquad \mathbb{Z}_2^{x,y} = \langle (x,y) \rangle,$$

where we let a, b, c, x, y be distinct characters from $1, \ldots, 5$. For example, $S_3^{4,5} = \langle (123), (12) \rangle$ and $\mathbb{Z}_6^{4,5} = \langle (123)(45) \rangle$. As suggested by the notation, $S_3^{x,y} \cong S_3$,$\mathbb{Z}_6^{x,y} \cong \mathbb{Z}_6$, $\mathbb{Z}_3^{x,y} \cong \mathbb{Z}_3$ and $\mathbb{Z}_2^{x,y} \cong \mathbb{Z}_2$. Given any x, y, and x', y', we have the involution $(x, x')(y, y')$ in S_5 and we notice that $(x, x')(y, y') S_3^{x,y} (x, x')(y, y') = S_3^{x',y'}$ so that each $S_3^{x,y}$ is conjugate.[5] In the same way $(x, x')(y, y') \mathbb{Z}_6^{x,y} (x, x')(y, y') = \mathbb{Z}_6^{x',y'}$ making al the $\mathbb{Z}_6^{x,y}$ subgroups conjugate. Since the parent groups are conjugate, the subgroups are also conjugate so that $\mathbb{Z}_3^{x,y}$ are conjugate and $\mathbb{Z}_2^{x,y}$ are conjugate.

However notice that $\mathbb{Z}_3^{x,y} \leq S_3^{x,y}, \mathbb{Z}_3^{x,y}$ and also $\mathbb{Z}_2^{x,y} \leq S_3^{x,y}, \mathbb{Z}_3^{x,y}$, but $\mathbb{Z}_2^{x,y}$ and $\mathbb{Z}_3^{x',y'}$ are incomparable as are $S_3^{x,y}$ and $\mathbb{Z}_6^{x,y}$. So in the class ordering we have:

$$\left[S_3^{4,5}\right] \qquad \left[\mathbb{Z}_6^{4,5}\right]$$

$$\left[\mathbb{Z}_3^{4,5}\right] \qquad \left[\mathbb{Z}_2^{4,5}\right]$$

Which is not allowable in a lattice. Thus in general, the conjugacy class ordering is not a lattice. □

It should be noted that for several groups, the class ordering is a lattice, for instance S_4, A_5, D_4 and trivially any abelian group. We will explore when this occurs in a moment. The graph of the partial order does, however, posses some desired qualities: it is connected, it has a unique top and bottom element, and whenever it is a lattice it is complete and modular – a property akin to the structure of abelian subgroup lattices.

Example: In S_3, (12),(13), and (23) are all conjugate. Notice $\langle (12) \rangle \cap \langle (13) \rangle = \mathbf{0}$. This shows why ${}^{G}\bigcap_{i \in I} H_i$ is not always the greatest lower bound. In this case both groups are in the same conjugacy class so their greatest lower bound is ${}^{S_3}\langle (12) \rangle$ not ${}^{S_3}\mathbf{0}$.

Unfortunately we cannot rectify this by taking only representatives from distinct classes as we see in S_4. We pause to define some subgroups of S_4, let $f(1) = (1234)$, $f(2) = (1324)$, and $f(3) = (1243)$, and $x = 1, 2, 3$:

$$D_4^x = \langle f(x), f^2(x+1) \rangle, \qquad \mathbb{Z}_4^x = \langle f(x) \rangle, \qquad \mathbb{Z}_2^x = \langle f^2(x) \rangle.$$

Each of these produce three distinct pairwise conjugate subgroups of S_4. The greatest lower bound of $\{D_4^1, D_4^2, D_4^3\}$ and $\{\mathbb{Z}_4^1, \mathbb{Z}_4^2, \mathbb{Z}_4^3\}$ computed by intersection would require $D_4^1 \cap \mathbb{Z}_4^1$ and $D_4^1 \cap \mathbb{Z}_4^2$ be conjugate, to be well-defined. Unfortunately the left produces $\mathbb{Z}_4^1$ and the right $\mathbb{Z}_2^2$, two nonisomorphic subgroups, thus non-conjugate. □

The action of conjugation is inextricably connected with normality. If we partition the subgroup lattice into its conjugacy classes, then the resulting lattice is invariant to any further conjugation. This property immiates in a strong way the structure of the normal subgroup lattice of groups.

Corollary II.2.5 *The conjugacy lattice is modular.*

[5] We allow the degenerate case where $x = x'$ or $y = y'$ at which point the conjugating element becomes (y, y') or (x, x') or simply trivial.

Chapter III

Classic Groups

III.1 Dihedral Groups

Proposition III.1.1 *D_n is nilpotent if and only if $n = 2^i$ for some $i \geq 0$.*

Refer to Exercise-II.7.8.

Proposition III.1.2 *D_n is solvable for all $n \geq 1$.*

Proof: When $n = 1$, $D_n \cong \mathbb{Z}_2$ which is nilpotent and so also solvable. Now let $n > 1$.

Then $D_n/\langle a \rangle \cong \mathbb{Z}_2$ and $\langle a \rangle \cong \mathbb{Z}_n$. Both $\mathbb{Z}_n$ and $\mathbb{Z}_2$ are nilpotent and so they are both solvable. Applying Theorem-II.7.11, D_n is solvable for all $n > 1$. $\square$

III.2 General Quaternions

Definition III.2.1 *Given $n \geq 1$, define Q_{4n} as the group with the presentation*

$$\langle a, b \mid a^{2n} = e, a^n = b^2, ba = a^{-1}b \rangle$$

of order $4n$. The group is called the n^{th} quaternion group.

Note it is possible to define $Q_0 = \mathbf{0}$ when the context requieres; however, serveral of the following theorems would require special cases and thus this extension is not treated in detail.

Proposition III.2.2 *The group Q_{4n} exists and is unique for all $n \geq 1$. Moreover,*

$$Q_{4n} = \{e, a, \ldots, a^{2n-1}, b, ab, \ldots, a^{2n-1}b\}$$

and $|a| = 2n$, $|a^i b| = 4$, for all $i = 0, \ldots, 2n-1$.

Proof: The presentation given for Q_{4n} always determines a group. What is required is that Q_{4n} have order $4n$, and that it be the only group with this presentation of that order.

To show this first we construct a maximal set of elements of which Q_{4n} must be a subset. Given $ba = a^{-1}b$ we may assume a normal form for all elements: for all $x \in Q_{4n}$, $x = a^i b^j$ for some $i, j \geq 0$. Now define $c = a^n = b^2$ and notice:

$$c(a^i b^j) = a^{n+i} b^j = a^i c b^j = a^i b^{j+2} = (a^i b^j) c;$$

therefore, c is central in Q_{4n}. The order of a is at most $2n$, and thus the order of b divides 4. Using the property of c notice $a^ib^3 = a^icb = a^{n+i}b$; therefore, all elements are of the form a^ib^j with $j = 0, 1$. This produces the following maximal list of elements:

$$A = \{e, a, \ldots, a^{2n-1}, b, ab, \ldots, a^{2n-1}b\}.$$

Since A visibly has $4n$ elements, by the Pigeon-Hole-Principle in fact we see $A = Q_{4n}$. Therefore Q_{4n} exists and is unique.

Consequently $|a| = 2n$ to have sufficient elements. Now as a final corollary, $(a^ib)^2 = a^iba^ib = a^ia^{-i}b^2 = c$. Since $c^2 = a^{2n} = e$, it follows $|a^ib|$ divides 4. When $n > 1$, $c \neq e$ and so $|a^ib| = 4$, and when $n = 1$, $e \neq a = b^2$, so $Q_{4n} = \langle b\rangle$ and so $|a^ib| = 4$ always. □

In fact the only element of order 2 in Q_{4n} is $c = a^n = b^2$ forcing $\langle a^ib\rangle \cap \langle a^jb\rangle = \langle c\rangle$ for all $i, j \geq 0$.
Example: Notice, $Q_4 \cong \mathbb{Z}_4$, and when $n = 2$, Q_8 is simply the traditional quaternion group of order 8.

In fact Q_{4n} is not isomoprhic to D_{2n} for any $n \geq 1$. We see when $n = 1$, $Q_4 \cong \mathbb{Z}_4 \neq \mathbb{Z}_2 \times \mathbb{Z}_2 \cong D_2$, and when $n > 1$ we have a complete generating set $Q_{4n} = \langle a, b\rangle$ in which each generator has an order greater than 2; meanwhile, in D_{2n} one generator must always have order 2. □

The groups D_{2n} and Q_{4n} are similar in presentations:

$$\begin{aligned} D_{2n} &= \langle a, b \mid a^{2n} = e, b^2 = e, ba = a^{-1}b\rangle, \\ Q_{4n} &= \langle a, b \mid a^{2n} = e, b^2 = a^n, ba = a^{-1}b\rangle, \end{aligned}$$

and both have the same order, but as we saw in the example they are always distinct groups. However the group D_n is more important in describing the structure of Q_{4n}, than D_{2n} – as we see with the following result.

Lemma III.2.3 *Define $c = a^n = b^2$ and let $n > 1$. $C(Q_{4n}) = \langle c\rangle \cong \mathbb{Z}_2$.*

Proof: As shown in the proof of III.2.2, $c = a^n = b^2$ is central and of order 2. Suppose a^i is central for some i. Then $a^i(a^jb) = (a^jb)a^i$ which implies $a^{j+i}b = a^{j-i}b$ so that in fact $a^i = a^{-i}$ or simply when $a^{2i} = e$; thus, $i = n$ so $a^i = c$.

Now suppose a^ib is central for some i. It follows $(a^ib)a = a(a^ib)$ which requires $a^{i+1}b = a^{i-1}b$ so that $a = a^{-1}$. Since we also assume $n > 1$ it follows $|a| > 2$ so $a \neq a^{-1}$; thus by contradiction a^ib is never central.

Therefore the center of Q_{4n} is $\langle c\rangle$. □

Of course when $n = 1$, $C(Q_4) = Q_4$ since only then is it abelian.

Proposition III.2.4 *Q_{4n} is an extension of D_n by $\mathbb{Z}_2$. Moreover, when $n > 1$, $Q_{4n}/C(Q_{4n}) \cong D_n$ and $C(Q_{4n}) \cong \mathbb{Z}_2$.*

Proof: From Lemma-III.2.3 we know $C(Q_{4n}) = \langle c\rangle$, where $c = a^n = b^2$. The center is always normal, so quotient groups are defined.

Since the orders are finite we see $[\langle a\rangle : \langle c\rangle] = n$ and $[\langle b\rangle : \langle c\rangle] = 2$, which implies $a\langle c\rangle$ has order n and $b\langle c\rangle$ has order 2. Certainly $[Q_{4n} : \langle c\rangle] = 2n$ so all that remains is the following relation:

$$b\langle c\rangle a\langle c\rangle = ba\langle c\rangle = a^{-1}b\langle c\rangle = a^{-1}\langle c\rangle b\langle c\rangle.$$

Therefore $Q_{4n}/\langle c\rangle \cong D_n$ as it satisfys the relations and order of D_n. □

Corollary III.2.5 *Q_{4n} is nilpotent, of class $(i + 1)$, if and only if $n = 2^i$, $i \geq 0$.*

Proof: The center of Q_{4n} is $\langle c\rangle$ and Q_{4n} is an extension of D_n by $\langle c\rangle$. Thus the remainder of a central series of Q_{4n} is a central series in D_n. However D_n is nilpotent if and only if $n = 2^i$ for some $i \geq 0$ (see Proposition-III.1.1. Thus D_n – and consequently Q_{4n} – has a central series if and only if $n = 2^i$, for some $i \geq 0$. □

Moreover, $C_j(Q_{4n}) = \langle a^{2^{i-j}}\rangle$ for all $j = 1, \ldots, i-1$, so that

$$\mathbf{0} \lhd \langle a^{2^{i-1}}\rangle \lhd \cdots \lhd \langle a^2\rangle \lhd Q_{4\cdot 2^i}$$

is the ascending central series. When n is odd, $C_2(Q_{4n}) = C_1(Q_{4n}) \neq Q_{4n}$, and when $n = 2^i m$, with $(m, 2) = 1$, $C_i(Q_{4n}) = C_{i-1}(Q_{4n}) \neq Q_{4n}$.

Corollary III.2.6 *Q_{4n} is solvable, of class 2, for all $n \geq 1$.*

Proof: Since $Q_{4n}/C(Q_{4n}) \cong D_n$ and $C(Q_{4n}) \cong \mathbb{Z}_2$ and both D_n (Proposition-III.1.2) and $\mathbb{Z}_2$ are solvable; it follows by Theorem-II.7.11 that Q_{4n} is solvable. □

As with the case of D_n, producing a solvable series is found by traversing through the cyclic subgroup of index 2 – $\langle a\rangle$; however, the general derived series is ($n > 1$):

$$\mathbf{0} \lhd \langle a^2\rangle \lhd Q_{4n}.$$

Corollary III.2.7 *Every subgroup of Q_{4n} is a subgroup of $\langle a\rangle$ or isomorphic to Q_{4m} for some $m|2n$.*

Chapter IV

Classification

IV.1 The Structure of Classifications

The work of classifying finite groups presently falls to the complex field of simple groups. All finite simple groups are classified but most are sporadic and and exocitc and so remain out of reach. However the classic groups – those that have orders less than 16 for instance – demonstrate certain properties of classification that allow for a study. The following essay explores these properties naively. This is primarily research and little effort has been made to discover if these concepts are encapsulated in existing theories and have established notation conventions and names; therefore, the results should be taken for their semantics rather than their syntax.

Definition IV.1.1 *A classification in a category is a partition of the objects which respects isomorphism; that is, two isomorphic objects are in the same class.*

Definition IV.1.2 *An object, B, in a category is a* subobject *of A, if there exists a monomorphism* $B \rightarrowtail A$. *We write* $B \leq A$.

Since we deal with classifications, the use of specific objects may almost always be substituted by isomorphic copies of the objects. Especially when considering subobjects, it is sufficient to consider any object that can be embedded in another by a monomorphism. This does however create a problem – we would like subobjects to have the partial ordering properties. Both reflexive and transitive properties are easily proved; however, the antisymmetric case requires a general form of the Schroeder-Bernstein Theorem. Generally when in a concrete category, an object B is a subobject of A if $B \subseteq A$ and $x \mapsto x$ is a monomorphism. This definition will prove strong enough to avoid this problem.

Lemma IV.1.3 *The subobject relation is reflexive and transitive.*

Proof: The identity map from A to A is a monomorphism and clearly $A \subseteq A$ so that $A \leq A$.

Finally when $A \leq B$ and $B \leq C$ it follows $A \subseteq B$ and $B \subseteq C$ so that $A \subseteq C$. Also there exists maps $f : A \rightarrowtail B$ and $g : B \rightarrowtail C$ which are both monomorphisms. Therefore their composition is a monomorphism $gf : A \rightarrowtail C$, so in fact $A \leq C$. $\square$

Corollary IV.1.4 *In a concrete category, subobjects are partially ordered.*

Remark IV.1.5 *If a category posesses a version of the Schroeder- Bernstein Theorem, then subobjects are partially ordered. The general Schroeder-Bernstein Theorem can be stated as:* If there exists a monomorphism from an object A to another B and also a reciprical monomorphism from B to A, then there exists an isomorphism between A and B.

Proof: We already know subobjects are reflexive and transitive, so all that remains to show is that in this context they are also antisymmetric.

Given $A \leq B$ and $B \leq A$, we have $A \subseteq B$ and $B \subseteq A$; thus, set theoretically $A = B$. With the added assumption the morphism $f : B \rightarrowtail A$, defined by $f(x) = x$ and $g : B \rightarrowtail A$ also as $g(x) = x$, the composition $gf = id_A$ and $fg = id_B$. Therefore $A \cong B$. □

Definition IV.1.6 *Given a classification of a category, a particular class is of* null-type *(*type-0*) if for every object in the class, each subobject is also in the class; furthermore, the class is of* type-n *if for every object in the class each subobject is in the class or in a class of a lesser type.*

Any class of type-n is called typical*, and a classification of all typical classes is typical; otherwise, each is respectively* atypical*.*

It should be emphasized that types as defined above correspond to classes of classifications, not the underlying objects contained in a class. This essay is largely a study of classifications of groups. **Example:** In a classification of groups, **cyclic** is always a null-type class. This is because every subgroup of a cyclic group is cyclic. Moreover later we will see any typical classification with the cyclic class has as its unique bottom element this class. □

Example: The classification of groups into **abelian** and **non-abelian** is typical. Given every object is either abelian or non-abelian establishes that this is a partition of the objects (we also know both to be non-empty). Every subgroup of an abelian group remains abelian; therefore, abelian is a null-type class. However every non-abelian group contains at least one abelian subgroup – for instance the group generated by a single one of its generators. Thus non-abelian cannot be null-type and in fact this shows it is of type-1. Soon we will say abelian is subtypical to non-abelian and even that abelian is suborderinate to non-abelian. □

Example: The classification of groups into **simple** and **non-simple** is *not* typical. We can see this with some examples.

We can show A_5 is simple, yet it contains the subgroup

$$K_4 = \{\varepsilon, (12)(34), (13)(24), (14)(23)\}$$

in which the subgoup $\{\varepsilon, (12)(34)\}$ is normal. Thus not all subobjects are simple showing simple is not a null-type.

On the other hand, many non-simple groups, such as $\mathbb{Z}_6$, have simple subgroups – here $\mathbb{Z}_2 \cong \langle 3 \rangle$ and $\mathbb{Z}_3 \cong \langle 2 \rangle$. Thus non-simple cannot be of null-type either.

We will soon codify the reason this proves the classification is atypical, but for now it suffices to say there are only two possible classes, and neither is independent of the other; thus each is atypical so the entire class is atypical. □

Example: Both **dihedral** and the general **quaternions** are type-1 classes.

We can demonstrate dihedral groups have subgroups which are exclusively dihedral or cyclic. Thus the type for dihedral is only defined when cyclic is included; yet the whenever the type is defined, it is always type-1. The same can be shown for the general quaternions (see Corollary-III.2.7). □

Example: Groups of **nilpotency class** i have subgroups of nilpotency class k with $k \leq i$; thus for each $i \in \mathbb{Z}^+$, the nilpotency class i is a classification of type-i. Notice this generates an infinite collection of distinct types. □

Notice how classes can be typical without their classification being typical; however, the converse is never true. The intruging question is: is the type of a class immutable irrespective of the containing classification? To answer this we look into the ordering properties of types and classes.

Definition IV.1.7 *A typical class A is less than or equal to a typical class B if the type of A is less than or equal to the type of B. We denote the ordinal type of a class C by $T(C)$ and write $A \preceq B$.*

Proposition IV.1.8 *Typical ordering ($\preceq$) is a partial ordering.*

As hinted earlier, there is a further ordering of classifications. For instance, abelian is less than non-abelian.

Definition IV.1.9 *Let $\mathscr{C}$ be a classification, and let A and B be classes. $A \leq B$ if for every object x in B, some subobject of x is contained in A.*

This ordering we will call the *class subordering* of a classification. For convenience let $Subs(x)$ be the collection of all subobjects of an object x. Of course in order for $A \leq B$ and $A \neq B$, the objects in B must all have a *proper* subobject in A since classes are disjoint.

Proposition IV.1.10 *The class subordering is reflexive and transitive.*

Proof: Given any object $x \in A$, $x \in A$ and $x \in Subs(x)$; therefore, $x \in A \cap Subs(x)$ and so $A \cap Subs(x) \neq \varnothing$. Thus $A \leq A$.

Suppose $A \leq B$ and $B \leq C$. Therefore every object in C has a subobject in B, and subsequently every object in B has a subobject in A. Since a subobjects are partially ordered, it follows every object in C has a subobject in A; thus, $A \leq C$. $\square$

Theorem IV.1.11 *Let A and B be classes in a classification. If $A \leq B$ and $B \leq A$ and A contains an object x for which $Subs(x)$ is finite, then $A = B$.*

Proof: We work towards a contradiction and assume instead that $A \leq B$, $B \leq A$, and $A \neq B$, retain also the property that for some $x_0 \in A$, $Subs(x_0)$ is finite.

We build a chain of subgroups as follows: beginning with x_0, since $x_0 \in A$ and $A \leq B$ there exists a subobject $y_0 < x_0$ that is also in B. Next notice $B \leq A$ implies there exist an $x_1 < y_0$ that is in A. We already know that subobjects are transitive, therefore $x_1 < y_0 < x_0$ implies $x_1 < x_0$. Thus if we begin again in A to discover a y_1 in B. This iteration creates a chain of subobjects

$$\cdots y_n < x_n < \cdots < y_1 < x_1 < y_0 < x_0$$

with each $x_n \in A$ and $y_n \in B$. Now we use the assumption that $Subs(x_0)$ is finite to show that this chain of subobjects must terminate at some x_n or y_n.

Here we have reached a contradiction. If the chain ends with x_n, then x_n is an object in A which has no subobject in B, thus A is not less than or equal to B. The same problem arrises if the chain ends in y_n. Therefore the assumption is false, so in fact $A = B$. $\square$

Corollary IV.1.12 *In any classification, if an object in A has only finitely many subobjects, then the class subordering is a partial ordering.*

Proof: Combine Proposition-IV.1.10 with Theorem-IV.1.11. □

In some instances the condition for the antisymmetric property may be satisfied without finiteness assumptions. An added requirement of the chain

$$\cdots y_n < x_n < \cdots < y_1 < x_1 < y_0 < x_0$$

is that each x_i and y_j be non-isomorphic; otherwise, since A is closed to all isomorphic copies of x_i, it would also contain y_j, producing $y_j \in A \cap B$ so that by the rules of a partition, $A = B$. Moreover, each of these properties equally applies for B. It is difficult (maybe impossible) to engineer a chain which matches these conditions for every object in the respective classes A and B without forcing $A = B$. However to be certain, all that is required is to show some object in A or B has a finite subobject count.

Proposition IV.1.13 *Each typical class A has a subordinate chain to a null-type.*

Proof: Suppose A is a class with the smallest type to not have a subordinate chain to a null-type. Given an object $x \in A$, one of the following must be true: x has no subobjects other than x, every $y < x$ is in A, or for some $y < x$, y is in a class which is typically less than A. In both the first and second cases A would be a null-type and thus it would have a subordinate chain to a null-type trivially; therefore, the third case must be true.

Suppose y is in a class B which by our assumption is typically less than A. Thus by the assumptions on A, B must have a subordinate chain to a null-type. However this means the object x in A has all its subobjects in a chain of typical classes reaching a null-type. Take the maximum length subordinate chain which must exists since they are all bounded above by n. This chain is a subordinate chain to a null-type for A. □

Proposition IV.1.14 *Let A and B be classes in a typical classification. If $A \leq B$ then $A \preceq B$.*

Proof: Since $A \leq B$ each object in B has a subobject in A. Furthermore, since B is typical each subobject is in a class of equal or lesser type; thus, the subobjects from B found in A must be in a class of equal or lesser type. Thus the type of A is of equal or lesser type than that of B. □

Theorem IV.1.15 (Typical Anti-Symmetry) *Let A and B be classes in a typical classification. If $A \preceq B$ and $B \leq A$ then $A = B$.*

Proof: Given $B \leq A$ it follows $B \preceq A$. Therefore $A \preceq B$ and $B \preceq A$ therefore $T(A) = T(B)$.

Suppose $A \neq B$. Then since $B \leq A$, for each $x \in A$ there is a proper subobject, $y < x$, in B. Since A is typical each subobject is either in A or in a class of a lesser type; therefore, B is of a strictly lesser type than A. This is of course a contradiction since we just proved $T(A) = T(B)$. Therefore in fact A must equal B. □

Corollary IV.1.16 *All null-types in a typical classification are unique and furthermore serve as bottom elements in both the typical order and suborder.*

Proof: Suppose there exists a typical class A and a null-type class N. Since N is null-type it is defined to be a typical bottom element, so $N \preceq A$. Suppose $A \preceq N$, then clearly $T(A) = T(N)$ so typically N is unique.

Now consider the suborder. If $A \leq N$ then as above we know $N \preceq A$ so by Theorem-IV.1.15 we know $A = B$. Therefore N is unique and furthermore $N \leq A$ or N and A are not comparable. However each typical class has a chain to a null-type object, thus N must be comparable to A. Therefore N is the unique bottom element in the suborder. □

Combining the two orderings we now see the role of types in the structure of classes. Classes in a typical classification can be arranged as a partially ordered set in which every level corresponds to the type of the class.

Next when might this structure form a lattice?

A null-type must always be present in a typical ordering and it will be the unique bottom element thus we know given any two classes there is a lower bound. What we must construct is a unique greatest lower bound.

Suppose A and B are classes in a typical classification. Suppose C and D are also classes with the added property that $C, D \leq A$ and $C, D \leq B$ so that both are lower bounds.

Definition IV.1.17 *The typical intersection of to typicl classes A and B is the class C with the greatest type that is a lower bound of both.*

Proposition IV.1.18 *The typical intersection is well-defined.*

Proof: Clearly all lower bounds of A and B must have a type less than or equal the minimum type of A or B. However we must also show there is a unique class satisfying the typical intersect property. □

Chapter V

Presentations

Every group is isomorphic to a quotient group of a free group; thus, the opertunity arrises to describe all groups with their free presentations. Constructing a group from a presentation can be facilitated by upper bounds on order, normal forms, and reduced presentations arrived at through Tietze transformations. The following examples construct some parameters for common presentations; these parameters are tasks usually performed once and from then on implicitly inferred.

V.1 Maximum Order

V.2 Normal Forms

The idea of a normal form is to express all the elements in group in a canonical ordered fashion. So given the generators a, b and c, we may at times express all elements in the group in form $a^i b^j c^k$ for the appropriate i, j and k. In conjunction with any bounds on order, we may be able to list all the elements of the group. More formally, a normal form comes about when the group can be described as the complex of the cyclic subgroups of each generator, and so very commonly one such subgroup will be normal.

Theorem V.2.1 *Let G be a group generated by a and b and let $A = \langle a \rangle$ and $B = \langle b \rangle$. The following are equivalent.*

(i) *G has a normal form $a^i b^j$.*

(ii) *$G = AB = BA$.*

(iii) *$ba = a^i b$ for some i.???*

(iv) *$b^j a^i = a^k b^l$ for all i, j and for some k and l.*

(v) *A or B is normal in G. ???*

Proof: First notice when $n = 0$ that $a^0 b = eb = be = ba^0$. Next suppose for some $n \geq 0$ that $ba^n = a^{-n}b$. Then $ba^{n+1} = ba^n a = a^{-n}ba = a^{-(n+1)}b$. With respect to inverses notice, $a^{-1}b^{-1} = (ba)^{-1} = (a^{-1}b)^{-1} = b^{-1}a$; therefore, $ba^{-1} = ab$. Finally $ba^{-n} = b(a^{-1})^n$ so borrowoing from our previous induction starting with our new relation $ba^{-1} = ab$, we now see $ba^n = a^{-n}b$ for all n.

Let $m = 0$ and notice $b^0 a^n = ea^n = a^n b^0 = a^{(-1)^0 n} b^0$. Next given any $m \geq 0$ such that $b^m a^n = a^{(-1)^m n} b^m$ it follows

$$b^{m+1} a^n = bb^m a^{-n} = ba^{(-1)^m n} b^m = a^{-((-1)^m n)} b^{m+1} = a^{(-1)^{m+1} n} b^{m+1}.$$

Lastly when $m < 0$ we start with $b^{-m}a^{-n} = a^{(-1)^{-m}-n)}b^{-m}$ and multiply both sides by b^m to see $a^{-n}b^m = b^m a^{(-1)^{-m}-n)}$ so that in fact $b^m a^n = a^{(-1)^m n}b^m$ for all m, and so in fact for all m and n.

Given every elemente generted by a and b is of the form $x = x_1^{i_1} \cdots x_n^{i_n}$ where $x_j \in \{a, b\}$, it follows if for some j, $x_j = b$ and $x_{j+1} = a$ then

$$x = x_1^{i_1} \cdots x_j^{i_j} x_{j+1}^{i_{j+1}} \cdots x_n^{i_n} = x_1^{i_1} \cdots b^{i_j} a^{i_{j+1}} \cdots x_n^{i_n} = x_1^{i_1} \cdots a^{(-1)^{i_j} i_{j+1}} b^{i_j} \cdots x_n^{i_n}.$$

Therefore every element generated by a and b can be sorted into the form $a^i b^j$ for some suitible i and j. $\square$

V.3 Tietze Transforms

V.4 Table of Presentations

Class	Relations	Order	Normal Form	Sample Groups
$\left(\frac{a}{n}\right)$	$a^n = e$	n	a^i	$C_n, \mathbb{Z}_n$
$\left(\frac{a_1,\ldots,a_n}{i_1,\cdots,i_n}\right)$	$a^{i_1} = \cdots = a^{i_n} = e$	∞		$C_{i_1} * \cdots * C_{i_n}$
$\left(\frac{a_1,\ldots,a_n \mid a_j a_k}{i_1,\cdots,i_n, i_j i_k}\right)$	$a^{i_1} = \cdots = a^{i_n} = a_j a_k a_j^{i_j - 1} a_k^{i_k - 1} = e$	$i_1 \cdots i_n$	$a_1^{k_1} \cdots a_n^{k_n}$	$C_{i_1} \times \cdots \times C_{i_n}$
$\left(\frac{a,b \mid ab}{i,j,k}\right)$	$a^i = b^j = (ab)^k = e$	??	??	$D_n \cong \left(\frac{a,b \mid ab}{n,2,2}\right)$, $A_n \cong \left(\frac{a,b \mid ab}{odd(n),2,3}\right), n > 2$
$\left(\frac{a,b \mid abab^{-1}}{2n,4,1}\right)$	$a^{2n} = b^2 a^n = abab^{-1} = e$	$4n$	$a^i b$	Q_{4n}

Chapter VI

Number Theory

Proposition VI.0.1 *Let $a, b, c \in \mathbb{Z}^+$, with each distinct. Show that if*

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$$

then $a = 2$, $b = 3$ and $c = 6$.

Proof: Presume $a < b < c$. If neither a, nor b, nor c is 2, then $3 \leq a < b < c$ and so

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < \frac{1}{3} + \frac{1}{3} + \frac{1}{3} = 1;$$

hence, one must take the value 2, so $a = 2$ as it is the smallest.

Now we have only to determine when does

$$\frac{1}{b} + \frac{1}{c} = \frac{b+c}{bc} = \frac{1}{2}?$$

Equivalently we look for $2b + 2c = bc$. To this we simply solve for one variable:

$$2b + 2c = bc; \qquad 2c = bc - 2b; \qquad 2c = b(c-2); \qquad b = \frac{2c}{c-2}.$$

This equation has some visible bounds which we will exploit. Notice $c \geq 4$, and $b \geq 3$. Moreover,

$$4 \leq c; \qquad 0 \leq 2c - 8; \qquad 2c \leq 4c - 8 = 4(c-2); \qquad b = \frac{2c}{c-2} \leq 4.$$

So $3 \leq b \leq 4$. If $b = 4$, then $c = 4$ which cannot be; therefore, $b = 3$, and so $c = 6$. $\square$

Notice 6 is perfect – meaning the sum of all divisors less than the number itself equal the number. The next perfect number is 28, and it has the divisors 1,2,4,7,14, and 28. Notice:

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{7} + \frac{1}{14} + \frac{1}{28} = 1.$$

Is this the only solution for the generalized problem of length 5? We will see.

Proposition VI.0.2 *Let m be a perfect number. Then*

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = 1$$

where $a_i | m$ and $a_i \neq 1$.

Proof: A number m is perfect if and only if

$$\sum_{d|m} d = 2m.$$

Then simply:

$$2 = \sum_{d|m} \frac{d}{m} = \sum_{d|m} \frac{1}{m/d} = \sum_{d|m} \frac{1}{d}.$$

Since 1 is a divisor, one of these summands is 1; thus,

$$1 = \sum_{i=1}^{n} \frac{1}{a_i}.$$

□

We have skipped the case of length 4; we now return to it.
Example: Let $a, b, c, d \in \mathbb{Z}^+$ with each distinct. When does

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} = 1?$$

Take once again $a < b < c < d$. Notice we may borrow from our result for length 3 to find one solution:

$$1 = \frac{1}{2} + \frac{1}{2} = \frac{1}{2} + \frac{1}{2}\left(\frac{1}{2} + \frac{1}{3} + \frac{1}{6}\right) = \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \frac{1}{12}.$$

With the existance established, may we determine any from of uniqueness? Consider $2 < a < b < c < d$ once again. As before:

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} < \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = \frac{19}{20} < 1.$$

Once again we require that $a = 2$. Now we have a length 3 situation again:

$$\frac{1}{b} + \frac{1}{c} + \frac{1}{d} = \frac{1}{2}.$$

If we take $5 \leq b < c < d$ we may quickly check that

$$\frac{1}{5} + \frac{1}{6} + \frac{1}{7} \neq 1; \qquad \frac{1}{5} + \frac{1}{6} + \frac{1}{8} < 1;$$

thus, $b < 5$, so that indeed $b = 3, 4$. When $b = 3$ we need

$$\frac{1}{c} + \frac{1}{d} = \frac{1}{6}; \qquad 6c + 6d = cd; \qquad \frac{6c}{c-6} = d.$$

We may bound c knowing that $c < 12$ as $1/12+1/13 < 1/6$; thus, $c = 7, 8, 9, 10, 11$, $d = 42, 24, 18, 15$, and 11 fails to produce an integer. So the solutions here are:

$$(2, 3, 7, 42), (2, 3, 8, 24), (2, 3, 9, 18), (2, 3, 10, 15).$$

Now suppose $b = 4$, all that changes is $d = \frac{4c}{c-4}$ and $c > 4$. The upper bound on c is empirically found to be 8. Thus $c = 5, 6, 7$, but once again, 7 fails, so $d = 20, 12$. Now we may enumerate all solutions for the problem of length 4:

$$(2, 3, 7, 42), (2, 3, 8, 24), (2, 3, 9, 18), (2, 3, 10, 15), (2, 4, 5, 20), (2, 4, 6, 12).$$

□

Notice something peculiar about all but (2,3,10,15): in each, the last digit is precisely the least common multiple of the previous 3 digits. The same holds in the case of length 3.

Not much else can be said that generalizes. For the case of length 5, there are 72 solutions, for length 6, 2320. An estimated 15,000 solutions exist of length 7. In all cases greater than 4, there are solutions that begin with 3 instead of 2, and latter even 4, 5, etc. begin to work. The new solutions are somewhat behaved. All come out of the set of solutions derived from the previous solutions as follows:

Proposition VI.0.3 *Ever solution of length $k+1$ is of the form*

$$(a_1 + n_1, ..., a_j + n_j, x_j, x_{j+1}, \ldots, x_k)$$

where $(a_1, \ldots, a_k)$ is a solution of the length k problem (even though only the first j values may be used), and $n_i = 0, \ldots, 2^{i-1}$, and not all are 0. Note the x is completely determined by the previous values.

The only reason this is a proper superset is because occassionally the x_i value is not a unit fraction, and thus must be excluded.

Notice for example the case of length 4. The solutions of the form $(2, 3, -, -)$ are derived from the length 3 solution $(2, 3, 6)$ by simply adding 1 through 4 to the the thrid coordinate 6. With $(2, 4, -, -)$ we have added 1 to the second coordinate and the remaining values must be determined separately.

Notice there are solutions to length 9, 10, and possibly all others of a greater length which are all odd. This is the domain of the odd perfect numbers, should they exists. Notice however there are far far fewer and they do not grow exponentially as the even solutions do (so far).

For example:

(	3	5	7	9	11	15	21	135	10395	)
(	3	5	7	9	11	15	21	165	693	)
(	3	5	7	9	11	15	21	231	315	)
(	3	5	7	9	11	15	33	45	385	)
(	3	5	7	9	11	15	35	45	231	)

In closing, this is not as strongly related to perfect numbers as might be thought. It does explain that odd perfect numbers must have an even number of divisors, as is seen quickly:

$$\sum_{d|n, d\neq 1} \left(\frac{1}{d} \prod_{d|n} d \right) = \prod_{d|n} d = n^2.$$

So if the number of divisors is odd, then the sum of the non-unit divisors is a sum of an even number of elements, and thus even. As the sum is even, then 2 divides n^2, so 2 divides n. Thus if n is odd, it has an even number of divisors. Hence the odd perfect numbers will be found only as solutions of the odd length problem, and also with at least 10 divisors.[1] In particular since every odd perfect number takes the form $a^2 p^{2k+1}$ for some a and some k, it follows we may discuss some constraints on a.

Suppose $a = p_1^{k_1} \cdots p_n^{k_n}$; then

$$m = p_1^{2k_1}, \ldots, p_n^{2k_n} \cdot p^{2k+1}.$$

[1] It is in fact already known that this lower bound is far larger. 8 distinct primes must divide any odd perfect number, and such a number must have 300 digits or more.[Brent, Cohen, and te Riele.]

How many divisors does this have? Well only the exponents need be considered. Take a vector $(a_1, \ldots, a_{n+1})$ so that $0 \leq a_i \leq 2k_i$ and $0 \leq a_{n+1} \leq 2k+1$. Each vector then determines a unique factor:

$$p_1^{a_1} \cdots p_n^{a_n} \cdot p^{a_{n+1}}.$$

Moreover, any factor determines a unique such vector. Now we may count all such vectors with basic combinatorics as simply:

$$(2k_1 + 1) \cdots (2k_n + 1) \cdot (2k + 2).$$

Cearly this number is even, so no new information is given.

Chapter VII

Automorphisms

VII.1 Automorphisms

Theorem VII.1.1 *Let G be a group and G' it regular representation in S_G.*

- *The automorphisms of a group G are embedded in the group of inner automorphisms of S_G.*
- *When G is finite, if H and K are isomorphic subgroups of a group G', then there exists an automorphism σ carrying H to K, and furthermore, there corresponds and element $g \in S_G$ such that $H = gKg^{-1}$.*
- *$|G| = n$, then $G' \cap Aut\ G = \boldsymbol{0}$, $Aut\ G \leq S_{n-1}$.*

Chapter VIII

Conjugation

The merits of conjugation can be seen in numerous results about groups; however, conjugation is not always a controllable or predictable device. I explore here some of the more extreem examples of conjugation in a meger attempt to classify some of the exotic possiblities. As a general principle, any oddity of conjugation for which there is a nilpotent group example will be tolerated; if we cannot accept the conjugation of these groups we may as well ignore conjugation altogether and study only abelian groups.[1]

The study seeks to address the following questions:

- Besides isomorphism type, what are invariants of conjugation?
- To what degree are conjugacy classes separated entities of a group?
- How can problems in conjugation be avoided, and controlled?

To take up the first question we make an effort to find groups where conjugation connects all objects with the same isomorphism type. With the rare exception we find conjugation is typically insufficient to perform this task.

For the second question we look for groups whose conjugacy classes are connected necessarily from elements in the same class. While these groups occur more often, they can be classified into a still small and approachable family.

Finally for the last question we look at procedures of extending and embedding groups as to introduce new overriding conjugation that removes unwanted phenomena.

VIII.1 Ultra-conjugacy

Definition VIII.1.1 *Given a group G and a subgroup H, (G,H) is called a conjugacy pair if for all $h,k \in H$ where $|h| = |k|$ there exists a $g \in G$ such that $ghg^{-1} = k$. If (G,G) is a conjugacy pair then G is said to be ultra-conjugate. A conjugacy pair (G,H) is called a minimal if for all proper subgroups $H < K < G$ it follows (K,H) is not a conjugacy pair.*

Theorem VIII.1.2 *Given a conjugacy pair (G,H) there exists a minimal pair (K,H) with $H \leq K \leq G$.*

Proof: Suppose (G,H) is a conjugacy pair. Let $\{K_i \ : \ i \in I\}$ be the set of all subgroups $H \leq K_i \leq G$ for which (K_i,H) is a conjugacy pair. Given any chain $\{K_j \ : \ j \in J\}$ take

[1] It should be emphasized that as nilpotent groups have non-trivial centers their associated centralizers are forcibly larger than those of non-nilpotent groups. This means smaller conjugacy classes and over all less unexpected results.

$K = \bigcap_{j\in J} K_j$. Suppose for some $h, k \in H$ such that $|h| = |k|$ it follows for all $g \in K$ that $ghg^{-1} \neq k$, then for some $j \in J$ it follows for all $g \in K_j$ that $ghg^{-1} \neq k$, which is a contradiction. □

Proposition VIII.1.3 *$(S_G : G)$ is a conjugacy pair, where G is the regular representation of G in S_G.*

Proof: Since every element of a regular representation takes the form

$$\sigma = (a_1, \ldots, a_k)(b_1, \ldots, b_k) \cdots (z_1, \ldots, z_k)$$

where σ has order k, it follows any two elements of the same order are conjugate in S_n. □

Using the regular representation and our previous result we now see that minimal conjugacy pairs always exist. Next we may ask about uniqueness. However the following list of the first few minimal pairs proves the negative of this conjecture.
Example:

- (C_2, C_2);
- (S_3, C_3);
- (D_8, C_4), (Q_8, C_4);
- $(A_4, C_2 \times C_2)$;
- (D_{2n}, C_n);
- (D_{4n}, C_{2n}), (Q_{4n}, C_{2n}).
- (S_3, S_3).

□

Remark VIII.1.4 *It is a well known fact that order is an invariant of conjugation. This theorem gives a converse of sorts: equal orders imply conjugate, except possibly in a larger group. In a larger context, isomorphism type is invariant under conjugation and here too we can ask if this is all conjugation can preserve; that is, if two subgroups of a group G are isomorphic then are they conjugate under conjugate of G, or perhaps of some larger group containing G?*

The answer is a partial yes. This can be done, and indeed requires no more than embedding a group as its regular embedding in S_n. However there is a penalty to pay: conjugation on the group from outside may not leave the group invariant. We will see later that in some cases no choice will be sufficient to solve this problem. [2]

There is a special case when the group itself is enough to make a conjugacy pair; we explore this next.

* * *

Now we turn our attention to the particular case when a group is ultra-conjugate. For the remainder of this article we let G be an ultra-conjugate group.

[2] It should be noted that indeed every automorphism of a group is conjugation by S_n on the regular representation of of a group of order n.

Example: The groups $\mathbf{0}, C_2 = S_2$, and S_3 are ultra-conjugate. The only interesting case is S_3, and indeed the only abelian ultra-conjugate groups are $\mathbf{0}$ and C_2. □

Lemma VIII.1.5 *If G is finite of order n, then for all $p|n$ it follows $(p-1)|n$.*

Proof: If $p|n$ then there is an element of order p in G by Cauchy's Theorem. Now this element a generates a subgroup with $p-1$ order p elements which must all be conjugate. As all p order groups intersect trivially, if there are k many p order subgroups then there are $k(p-1)$ elements in G which must be conjugate. However the size of this conjugacy class equals $[G : C_G(a)]$, so its order must divide n; hence, $p-1|n$. □

This rules out all but 80 orders less than or equal to 1000. All but one of these orders has been searched.

Lemma VIII.1.6 *If $N \trianglelefteq G$ then G/N is ultra-conjugate.*

Proof: Take $hN, kN \in G/N$ where $|hN| = |kN|$. It follows $[\langle h\rangle : N] = [\langle k\rangle : N]$ so

$$|h| = |\langle h\rangle| = [\langle h\rangle : N]|N| = [\langle k\rangle : N]|N| = |k|.$$

So there exists a $g \in G$ such that $ghg^{-1} = k$. Now

$$(gN)(hN)(g^{-1}N) = ghg^{-1}N = kN.$$

Hence G/N is ultra-conjugate. □

Example: Subgroups of an ultra-conjugate group need not be ultra-conjugate. In S_3, A_3 on its own is the abelian group C_3 which is not ultra-conjugate as 1 is not conjugate to 2. □

Theorem VIII.1.7 *Every ultra-conjugate group has center trivial or isomorphic to C_2. Moreover, with the exception of $\mathbf{0}$ and C_2, no ultra-conjugate groups are nilpotent.*

Proof: If there are more than two non-trivial central elements of equal order then they cannot be conjugate. All central elements of order greater than 2 are thus not conjugate to their inverses. Moreover, a center with elements of order 2 can have only one. Thus the center is isomorphic to a subgroup of C_2. Furthermore, if $Z(G) \cong C_2$ then there is only one element of order 2 in G as the non-trivial element of the center has order 2 and is not conjugate to anything else.

Take G to be nilpotent and let

$$Z_0 = \mathbf{0} < Z_1 = Z(G) < \cdots < Z_n = G$$

to be the ascending central series. Certainly $Z_1 \cong C_2$, and as G/Z_1 is ultra-conjugate it follows $Z(G/Z_1) \cong \mathbf{0}$ or C_2. If $\mathbf{0}$, then $n = 2$ and $G = C_2$. Suppose C_2 then. Then G/Z_1 has a unique element of order 2 so G has a unique element of order 4 as all 2-subgroups contain Z_1 so the correspondance theorem applies. By induction G is a 2-group generated by a single element so it is C_{2^n} which clearly has center greater than C_2 whenever $n > 1$. Thus G is not ultra-conjugate. □

This theorem's principle result is to suggest we study ultra-conjugate groups with trivial centers. The next theorem tells us we should not allow the commutator to be too small either.

Theorem VIII.1.8 *The index of the commutator of G divides 2.*

Proof: From our lemma we know G/G' is ultra-conjugate. However from the definition we know G/G' is abelian. As the only abelian ultra-conjugate group is C_2, it follows $[G : G']|2$. $\square$

In particular it is helpful to notice how this is so. Consider $h \in G$. We need h to be conjugate to h^{-1}, say by an element $g \in G$. Then certainly

$$[g, h^{-1}]h^{-1} = gh^{-1}g^{-1} = h; \qquad [g, h^{-1}] = h^2.$$

Hence, if the order of h is odd then $h \in G'$. We will see in a moment the case for order 2^i elements. Before establishing this it is helpful to define the notation:

$$G_n = \{g \in G \ : \ |g| = n\}.$$

Clearly G is ultra-conjugate if and only if the conjugacy classes are precisely the G_n's (with the natural assumption that we ignore any emptysets G_n.)

Theorem VIII.1.9 *$N \trianglelefteq G$ if and only if for all $H \leq G$ such that $H \cong N$ it follows $H = N$. Moreover, if N contains an element of order j, then $G_j \subseteq N$.*

Proof: The final claim actually explains the first. Given any element h in N, it follows $ghg^{-1} \in N$ for all $g \in G$ as N is normal. However, h is conjugate to all elements of order $|h|$, so N contains $G_{|h|}$.

Now if H is also a subgroup of G which is isomorphic to N then clearly to every element in N there corresponds one of the same order in H; yet, N contains all such group elements so N contains H. By the pigeon-hole-principle $H = N$. $\square$

Given a element $h \in G$ of maximum (not maximal) order 2^m in G, it follows $h^2 \in G'$ so all $G_{2^i} \in G'$, where $i < m$, since G' is normal in G.

Remark VIII.1.10 *Many of these theorems mimic the observations of symmetric groups. It should be noted plainly that the only symmetric ultra-conjugate groups are S_n, $n \leq 3$. For instance, in S_n, $n > 3$ we have $(1\ 2)$ and $(1\ 2)(3\ 4)$, which are not conjugate. Worse than this we can have elements of the form:*

$$(1\ 2\ 3\ 4)(5\ 6\ 7\ 8), \qquad (1\ 2\ 3\ 4)(5\ 6)(7\ 8),$$

which even have the same length and still are not conjugate.

Remark VIII.1.11 *Using the results of these theorems and the GAP group library, all groups of order 1 to 1000, with the exception of those of order $768 = 2^8 \cdot 3$ have been checked for ultra-conjugate groups. Only S_n, $n \leq 3$, appear to be ultra-conjugate thus far.* [3] *Whether there no more ultra-conjugate groups is yet unknown, but it is probable that any which do exist will be exotic.*

Remark VIII.1.12 *Simple groups may provide a partial answer. It is already known that no Alternating group is ultra-conjugate. Moreover, the low order Lie type simple groups as well as the Mathieu groups yield no ultra-conjugates. Unfortunately each finite simple group has order ideal for ultra-conjugacy. However theoretical methods may be able to determine that the only ultra-conjugate simple group is C_2. If so, then the solvable ultra-conjugate groups will have to have compositions series composed of C_2's and C_p's where $p = 2^k + 1$.*

[3] The GAP 4 groups libraries were used. Beyond 1000 many other cases less than 2000 can be checked; however, the library has several holes in orders greater than 1000 so no conclussive results can be had. It should be noted that the search allowed for non-trivial

centers just incase such examples might be the only ones to appear.

At this point we return to explore the general conjugacy pairs to see if their methods may provide us with more information.

* * *

Consider the example of $D_8 = \langle a, b \mid a^4 = b^2 = 1, bab^{-1} = a^{-1} \rangle$. Here the elements a^2 and b determine isomorphic subgroups. However no automorphism of D_8 can send b to a^2 or visa-versa. **Example:** Suppose $f : D_8 \to D_8$ is an automorphism. Then $f(a) = a$ or a^{-1} as these are the only elements of order 4; hence, $f(a^2) = a^2$. If $f(b) = a^2$ then f is not injective so it is not an automorphism. □

What this illustrates is the potential for conjugacy pairs to be harmful to the structure of the conjugate subgroup. No matter what pair (G, D_8), is divised for D_8, the group G must act on D_8 as more than automorphisms. This leads the following natural definition.

Definition VIII.1.13 *A conjugacy pair (G, H) is normal if $H \trianglelefteq G$. We write (G/H) to specify a normal conjugacy pair.*

Proposition VIII.1.14 *A conjugacy pair (G/H) is normal then there exists a map $G \to Aut(H)$. This in part says G's action on H by conjugation is an automorphism.*

Proof: If $gHg^{-1} = H$ for all $g \in G$ then $f_g(h) = ghg^{-1}$ is an automorphism of H. Thus define $F : G \to Aut(H)$ by $F(g) = f_g$. □

Notice this states that D_8 can have no normal conjugacy pair, as no automorphism of D_8 can connect b with a^2.

VIII.2 Tanlged Groups

An intreguing question about conjugation might be posed now: Given a conjugacy class, is it possible that elements outside of the class will be sufficient to connect all the elements in the conjugacy class?[4] We may word the problem more pricesly:

Definition VIII.2.1 *A group acting on itself is called an automatic action. Furthermore, an automatic action is outer if each orbit is connected by some subset of the group that does not intersect the orbit; that is,*

$$Gx = (G \backslash Gx)x.$$

Remark VIII.2.2 *This should not be confused with the idea that all the elements in a conjugacy class are in the same centralizer. While this case certainly would be outer, many outer actions may have non-trivial action by elements in the same class; however, the goal is to treat these as redundant and consider only the action from outside the class itself.*

Non-outer auto-actions are easy to come by with the regular action of a group: in C_3, $C_3 + 1 = C_3$ which clearly is not the same as $\{0, 2\} + 1$. With conjugation the question is more involved. We will call a group *tangled* if some conjugacy class cannot be connected by the complement of the class. **Example:** The groups $SL_2(\mathbb{F}_q)$, (composition series is A_n over C_2) where $q \neq 2^k$, are tangled groups. Specifically they are tangled amongst the elements of order 4. Other tangled groups include $SU(3, 2)$, which is tangled amongst the elements of order 3, etc.

[4] In the trivial group we may say so vacuously.

The principle example of tangled groups are those with subgroups of the form $C_p \times C_p$ atop a central extension by C_p. These p^3 groups are conjugate internally but not extenerally. When a further external extension (meaning not from bellow) is applied, it is possible to conjugate these maximal p^2 groups together while the inside of each remains conjugate internally only by the elements inside. The version when $p = 3$ begins with the three tangled groups of order 216. The A_n over C_2 are simply the variety that works for $p = 2$. It is not clear yet whether this construction classifies all possible tangles; however, it does seem to cover all small order groups. □

VIII.2.1 Conjugacy Structure

Every conjugacy class can be seen as a labeled graph. Typically the graph is not simple as any centralizing elements appear as loops and there are often more than one element conjugating to the same element. However it is always possible to pick a spanning tree (indeed a spanning star). The labels of such a tree correspond exactly to a transversal of the cosets G/C_g where C_g is the centralizer of the root node g. As might be expected we may simply rotate around this spanning star around to rebuild the entire graph, so the choice of start point is unimportant. Now the choice of transversal is not always arbitrary and indeed the structure of possible transversals is illustrated by the nature of tangled groups.

Example: Consider the group S_3. Every non-trivial subgroup here is a centralizer for some element, and they give the following coset structures:

(1 3 2)	(2 3)
(1 2 3)	(1 3)
()	(1 2)

(1 2)	(2 3)	(1 3)
()	(1 2 3)	(1 3 2)

Notice the cosets of $S_3(1\ 2)$ line up so that each coset is conjugate to some the next only if it is conjugate in the centralizer. [PENDING: replace the trivial example with something explanitory.] □

Proposition VIII.2.3 *If* $[a] = \{g_1 a g_1^{-1}, \ldots, g_n a g_n^{-1}\}$ *is a conjugacy class in* G *for which* $\{g_1, \ldots, g_n\}$ *form a transversal of* G/C_a*, then for all* $b \in C_a$ *such that* $a \sim b$ *it follows* $g_i a \sim g_i b$.

Proof: The proof relies a simple trick: suppose that $a \sim b$ via g_i. Then at the $g_i C_a$ coset it follows

$$g_i b = g_i(g_i a g_i^{-1}) = g_i(g_i a) g_i^{-1}$$

so $g_i b \sim g_i a$. □

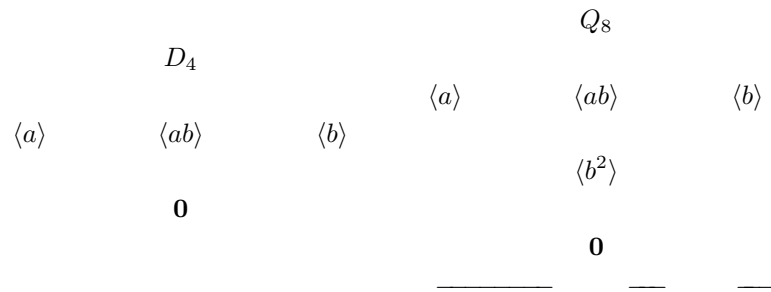
VIII.2.2 Cyclic Central Extensions

To illustrate the tangled groups we will need to adequitely construct them. One method relies on a simple version of the extension problem: central cyclic extensions. For example, the quaternion groups are all central cyclic extensions of dihedral groups. When drawing the lattice it is evident precisely how this extension functions.

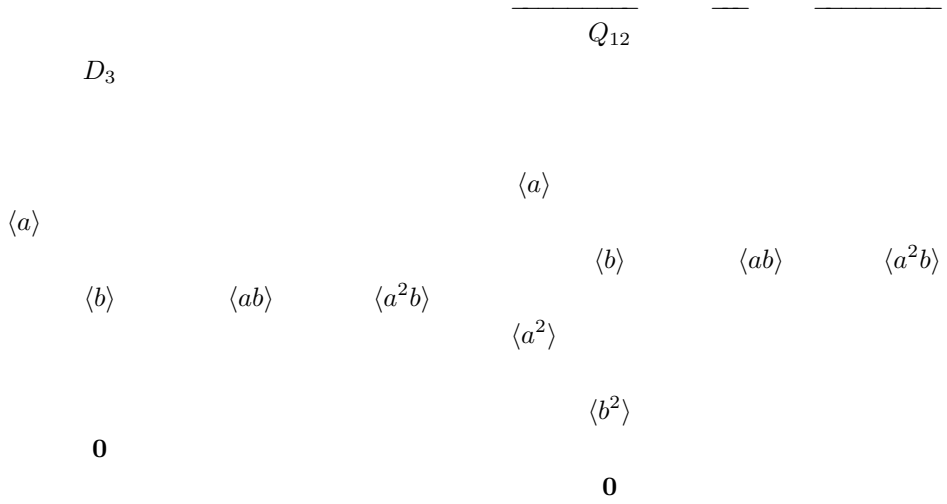
Example: The simplest example is $Q_4 \cong C_4$ and is a central cyclic extension of $D_2 \cong C_2$.

$$\begin{array}{ccc} & Q_4 & \\ D_2 & & \\ & \langle b^2 \rangle & \\ \mathbf{0} & & \\ & \mathbf{0} & \end{array}$$

Structurally the lattice has been "stood atop a pole." Indeed we see this again with the next example, $D_4 \cong C_2 \times C_2$ and its extension Q_8.



Once again we simply balance the given group on top of a pole which represents the C_2 by which we extend. However there is a subtle difference when we move to groups that are not 2-power groups. For instance with $D_3 \cong S_3$ and Q_{12}, we still begin by planting the group D_3 atop C_2, but now we are forced to drop in also a new subgroup C_3 to complete the lattice for the now existant C_6 subgroup.



□

With dihedral groups this type of extension is no problem as we already have a presentation for each dihedral group and the modification to add the extension is somewhat striaght forward. How might we do this for groups for which a presentation is not know, or for which no obvious generalization exists? Well we resort to the pictures for clues. Figuratively we would like to take any group Q and a prime order cyclic group C_p and stack the lattice of Q atop that of C_p. As C_p's lattice is always a "pole" this should correspond to the process illustrated by the quaternion groups. So we must consider the process used here and generalize. Here are the important facts:

- Every element g, of order k, must become an element g' of order pk.
- If an element g has order k such that $k \neq p^i$, then we must also include an element g'' of order k such that $g'^p = g''$, and $g'^k = b$.
- Elements of order p^i must become elements of order p^{i+1} so that $g'^p = b$.
- The "pole" subgroup must be central, and thus normal.

Thus we create the following generic "pole-product."

Definition VIII.2.4 *Let G be a finite group, and p a prime. The pole-product, denoted $C_p \triangledown G$, is the group*

$$H = \{gb^i \ : \ g \in G, i = 1, \ldots, p \cdot |g|, (i,p) = 1\} \cup \{g \ : \ g \in G, |g| \neq p^k, k > 0\}.$$

We equipe the group with the following multiplication:

$$(gb^i)(hb^j) = (gh)(b^{i+j+\chi(gh)}),$$

where $\chi(gh)$ is defined as:

$$\chi(gh) = \begin{cases} 0, & |gh| \neq p^s, \\ 1, & h \notin \langle g \rangle, |g| = p^s, |h| = p^t \end{cases}$$

[PENDING: getting it written down correctly is difficult, follow the examples and then correct it.]

Remark VIII.2.5 *There is an obvious dual construction for placing the "pole" atop a group. These extension will be denoted $C_p \triangle G$. The notation $C_p \triangledown G$ is meant to indicate that $C_p \trianglelefteq G$ and the rotation of the triangle upwards indicates that the extension places the normal subgroup bellow G. The dual symbol simply flips the sign as with many dual symbols.*

Notice $b^k = eb^k$ so indeed it is central. Notice also that b^i is not in our group except for $\langle b^k \rangle \cong C_p$.
Example: Consider the pole product of C_2 with itself, $C_2 \triangledown C_2$. Letting the top group be generated by a we attain the following group:

$$C_2 \triangledown C_2 = \{e, b^2, ab, ab^3\}.$$

Now we must check the multiplication table.

$$(ab)(ab) = (a^2)b^{1+1+\chi(a^2)} = b^2.$$

$$(ab)(ab^3) = (a^2)b^{1+3+\chi(a^2)} = (b^2)^2 = e.$$

So $C_2 \triangledown C_2 \cong C_4$ as expected. □

Now in practice it is possible to pick some maximal p-order element in G to be b, and thus b is in the group, but formally we should label every element distinctly. Now let us try a different prime.
Example: Consider the pole product of C_3 with itself, $C_3 \triangledown C_3$. We expect to get C_9 in return, simply by the lattice. Letting the top group be generated by a we attain the following group:

$$C_3 \triangledown C_3 = \{e, b^3, b^6, ab, a^2b^2, ab^4, a^2b^5, ab^7, a^2b^8\}.$$

Now we must check the multiplication table.

$$(ab)^{-1} = (a^2b^8), \qquad (a^2b^2)^{-1} = ab^7, \qquad (ab^5)^{-1} = a^2b^4.$$

Indeed, $(ab)^{-1} = a^{-1}b^{-1}$. Moreover:

$$(ab)^2 = a^2b^2; (ab)^3 = b^3; (ab)^4 = ab^4; (ab)^5 = a^2b^5; (ab)^6 = b^6; (ab)^7 = ab^7; (ab)^8 = a^2b^8; (ab)^9 = e.$$

So correctly we now see $C_3 \triangledown C_2 = \langle ab \rangle$ and is cyclic of order 9. □

Now let us mix pimes.
Example: Describe $C_2 \triangledown C_3$ and $C_3 \triangledown C_2$. We anticipate they are both C_6.

$$C_2 \triangledown C_3 = \{e, b^2, a, a^2, ab^2, a^2b^2\}.$$

Recall we have to add a and a^2 because their orders are not a power of 2. Also, we decorate a with b^2 since the order of a is not a power of 2. Likewise:

$$C_3 \triangledown C_2 = \{e, b^3, b^6, a, ab^3, ab^6\}.$$

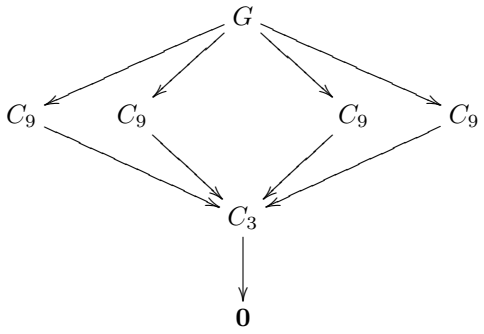
In the first case ab generates the entire group as $(ab^2)^2 = a^2$, and $(ab^2)^5 = a^2b^3$. Similarly for our second group. □

Proposition VIII.2.6

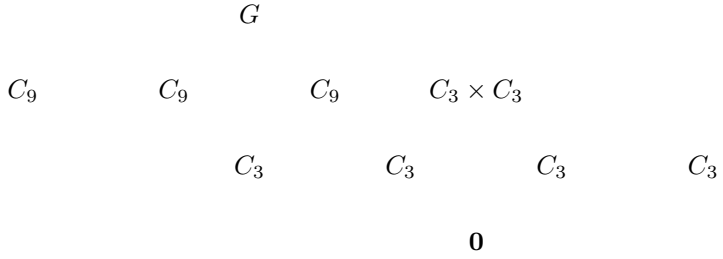
$$C_{p_1^{i_1}\cdots p_k^{i_k}} \cong \left(\bigtriangledown_{j=1}^{i_1} C_{p_1}\right) \triangledown \cdots \triangledown \left(\bigtriangledown_{j=1}^{i_k} C_{p_k}\right).$$

Furthermore, the decomposition is unique up to permutations of the primes.

Example: Central prime extensions for $p \neq 2$ take on different structure. At a first glance it seems possible to build a group of order 27 with the following lattice:



Yet there is no such group of order 27. The analogue with 6 order 25 groups atop a single order 5 group also does not exist, and in general for any prime $p \neq 2$ we cannot repeat the process of the quaternions faithfully. Instead the closest we can get is the following:



Visibly this is now a split extension of C_3 by C_9. Likewise every p^3 group for $p \neq 2$, save C_{p^3}, is a split extension of C_p by C_{p^2} or C_p by $C_p \times C_p$. Thus there is no need for pole extensions for odd primes except to build cyclic groups. □

Why might this be so? The answer lies in parity. Since p^3 is odd for all primes other than 2, it happens that conjugacy classes must be odd. However there are always an even number of generators for any group of order not equal to 2. Thus we cannot divide conjugacy classes amongst generators alone. If the subgroups are conjugate they may only be so with and odd number of groups

which require then that one of the proper subgroups of any $C_p \times C_p$ be left out. What about mixed primes? Is $C_5 \triangledown (C_3 \times C_3)$ viable? Sure, but recall when we do not have any elements of the same prime order in our tup group we get a standard split extension. So in escence, pole products are the domain of even cyclic groups and to build C_{p^n}.

Example: Back to the quaternions. $Q_8 \cong C_2 \triangledown (C_2 \times C_2)$. If we let $C_2 \times C_2 = \langle a, b \rangle$ and

$$\chi(a,b) = -1, \qquad \chi(a,ab) = 1$$

and as usual $\chi(x,x) = 0$, $\chi(x,1) = \chi(1,x) = 0$ and $\chi(x,y) = -\chi(y,x)$ then we can build the quaternions as a pole product. Then we attain the set:

$$C_2 \triangledown (C_2 \times C_2) = \{e, c^2, ac, ac^3, bc, bc^3, abc, abc^3\}.$$

And we multiply as follows:

$$(xc^k)(yc^n) = xyc^{k+n+\chi(x,y)}.$$

Now we must verify the relations.

$$\begin{aligned}
(xc)^2 &= x^2c^{2+\chi(x,x)} = c^2; \\
(xc^3)^2 &= x^2c^{6+\chi(x,x)} = c^2; \\
(c^2)^2 &= e; \\
(ac)(bc) &= abc^{2+\chi(a,b)} = abc; \\
c^2(bc)(ac) &= bac^{4+\chi(b,a)} = abc^{4-\chi(a,b)} = abc.
\end{aligned}$$

So if we let $i = ac$, $j = bc$, $k = abc$, and $c^2 = -1$ then we have:

$$i^2 = j^2 = k^2 = -1; ij == k = -ji.$$

And so these are indeed the quaternions. □

[PENDING: determine if this has anything to do with factor sets and cocycles, looks similar.]

The characteristic function has to have the following properties;

- $\chi : G \times G \to \mathbb{Z}$.
- $\chi(x,y) = -\chi(y,x)$.
- $\chi(x,y) = 0$ if and only if $x \in \langle y \rangle$ or $y \in \langle x \rangle$. Consequently we always have $\chi(x,x) = 0$ and $\chi(x,1) = \chi(1,x) = 0$.

The choice of χ is not arbitrary. It must be choosen so that the multiplication is associative.

VIII.3 Modularity and Consolidation

Beginning with an arbitrary partial ordering makes the the construction of a lattice difficult. A general lattice for an ordering may be infinite, but even when finite, even the relatively small number of 16 elements can complicate the structure increadibly. To study the lattice in detail we can probe for microscopic details, such as: is the lattice modular, or even distributive? Or we can look for macroscopic information such as: do we have a top and bottom element, and is is complemented or complete. Both methods have draw backs. Here I investigate how to reduce the information of lattices and preserve structure.

Definition VIII.3.1 *Given a partially ordered set P, a partition $P/\sim$, the box ordering on $P/\sim$ is defined as $[a] \leq [b]$ if and only if for each $a' \sim a$, there exists a $b' \sim b$ such that $a' \leq b'$. If for each $a \in P$, the class $[a]$ is totally unordered, and for each $b \in P$ where $a \leq b$, it follows $[a] \leq [b]$, then we call $\sim$ a consolidation of P.*

Proposition VIII.3.2 *The boxed ordering of a consolidation is a partial ordering.*

Proof: Suppose $\sim$ is a consolidation of P. Then given any $a, b, a', b' \in P$, suppose $[a] \leq [b]$ and that $a \sim a'$ and $b \sim b'$. Given any $c \sim a$, it follows there exists a $d \sim b$ such that $c \leq d$. But certainly $\sim$ is transitive so that in fact $c \sim a'$ and $d \sim b'$, hence $[a'] \leq [b']$; thus, the boxed ordering is well-defined.

Notice $a \leq a$ for all a, so in fact for all $a' \sim a$, it follows $a' \leq a'$ so $[a] \leq [a]$.

Suppose $[a] \leq [b]$ and $[b] \leq [a]$. Without loss of generality we may take $a \leq b$. All we must show is that $b \leq a$. Well since $[b] \leq [a]$ there exists $a' \sim a$ such that $b \leq a'$. But this means $a \leq a'$, and since $[a]$ is totally unordered, it follows then that $a = a'$. Therefore $a = b$ and so $[a] = [b]$.

Finally let $[a] \leq [b]$ and $[b] \leq [c]$. Taking any $a' \sim a$ there exists a $b' \sim b$ such that $a' \leq b'$; furthermore, there exists a $c' \sim c$ such that $b' \leq c'$, and so $a' \leq c'$. Hence $[a] \leq [c]$. □

Example:

- Given any finite set X, if we equate all subsets of X which are of the same size, then we have a consolidation of the subset lattice of X.
- In any group, conjugation of subgroups is a consolidation of the subgroup lattice.
- In any partially ordered set, the identification of all maximal elements is a consolidation – likewise for all minimal elements.

□

Of particular interest are the consolidations of lattices. We know the structure of a partial ordering is preserved; moreover it is a simple corollary to establish that top and bottom elements of a poset are preserved, as well as connectedness. However it is in fact possible to consolidate elements in such a fashion as to remove greatest lower bounds and least upper bounds form a lattice. We will see such concrete examples with the groups S_n, $n \geq 5$ under the consolidation of conjugation. At some point we will become interested in modularity, specifically, when does a consolidation of a lattice create a modular, or even distributive lattice. We shall then say the lattice is pre-modular, etc. Such information is useful for the study of automorphisms of the set. Each defines very clear subgroups of the automorphism group and many times even normality is acquired.

Bibliography

[Tar95] Alfred Tarski, *Introduction to logic: And to the methodology of deductive sciences*, Dover Publications, Inc., New York, 1995.