On the Classification of Tarski Monsters

Lisa Liu

June 1, 2021

1 Introduction

This paper presents a type of non-abelian infinite simple p-group, the *Tarski monster*. The existence of Tarski monsters was first proven by Alexander Yu. Olshanskii in 1980 and is significant as Tarski monsters provide counterexamples to Burnside's problem. To understand specific properties of the Tarski monsters, we begin by discussing basic group theory terminologies and theorems. In Section 2, we first introduce definitions related to groups and subgroups and close with two important theorems, Cauchy's Theorem (Theorem 2.5) and Lagrange's Theorem (Theorem 2.19). These theorems lay the foundation for a basic introduction to the Tarski monster and its subgroup lattice in Section 3 and selected proofs of its properties, specifically its characterization as a simple group (Theorem 4.7), in Section 4.

2 Groups and Subgroups

In this section, we begin by looking at what a group is and the axioms that a group must satisfy. We then discuss different kinds of groups and subgroups, as well as their interesting properties. Finally, this section includes two important theorems, Cauchy's Theorem (Theorem 2.5) and Lagrange's Theorem (Theorem 2.19), and lemmas such as the Cancellation Law (Lemma 2.2) and the Subgroup Criterion (Lemma 2.11).

Definition 2.1. A *group* is defined by the ordered pair $(G, \circ)$ where G is a set and $\circ$ is a binary operation that maps $G \times G \to G$, satisfying the following conditions:

1. *Closure*: The binary operation $\circ$ is said to be closed on set G if for any elements $a, b \in G$, $a \circ b$ is also an element of G. Note that closure has been implied in the definition $\circ : G \times G \to G$, but by convention we include closure as one of the four criteria of a group.

2. *Associativity*: The binary operation $\circ$ is associative such that for any elements $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$.

3. *Identity*: There exists a unique identity element $e \in G$ such that for all $a \in G$, $e \circ a = a = a \circ e$. The identity is often represented by e or 1.

4. *Inverse*: For all $a \in G$, there exists a unique inverse $a^{-1} \in G$ such that $a \circ a^{-1} = e = a^{-1} \circ a$.

We often say that G is a group under $\circ$ instead of writing the ordered pair, and we omit $\circ$ when the binary operation is clear. In most cases, we write ab instead of $a \circ b$ for convenience and assume that multiplication is the group operation, where a^m indicates m applications of $\circ$ to a. We will also denote the identity by 1 unless otherwise specified.

Lemma 2.2 (Cancellation Law)**.** *For any elements a, b, c in group G, if $ab = ac$, then $b = c$.*

Proof. We multiply a^{-1} on each side to get $(a^{-1}a)b = (a^{-1}a)c$, which implies $1b = 1c$ and so $b = c$. Note that the law holds similarly for a via right multiplication. □

The first property we introduce is the order of an element and the order of a group. Order is particularly useful for looking at how elements behave within a group and understanding the group structure as a whole. We will also present a powerful theorem on how the orders of elements and the group relate to each other, Cauchy's Theorem.

Definition 2.3. For a group G, the *order* of $x \in G$ is the smallest positive integer m such that $x^m = 1$.

Definition 2.4. The *order* of a group, denoted by $|G|$, is the cardinality of the set G, namely the number of elements in it. G is an infinite group when its order is infinite.

Theorem 2.5 (Cauchy)**.** *For a finite group G, there must be an element of prime order p if p divides $|G|$.*

We will not prove Cauchy's Theorem in this paper, but its proof is outlined in Exercise 9 of [2, p. 96].

Next, we will characterize different types of groups. For the purposes of this paper, we will only define abelian groups and cyclic groups formally, after which we briefly mention dihedral groups and symmetric groups.

Definition 2.6. We say that a group G is *abelian* if $ab = ba$ for all $a, b \in G$.

Definition 2.7. We say that a group G is *generated by* its subset S, denoted $G = \langle S \rangle$, if every element of G can be written as a finite product of elements in S. The elements of S are called *generators* of G.

By convention, we often write the elements of S instead of the set S in the angle brackets. For example, if the generating set of G is $S = \{a, b, c\}$, we can write $G = \langle a, b, c \rangle$. Moreover, we say that G is *finitely generated* if the cardinality of S is finite.

Definition 2.8. We say that a group C_n is *cyclic* if $C_n = \{x^n \mid n \in \mathbb{Z}\}$ for some $x \in C_n$. In other words, C_n is a group of order n generated by a single element x.

Example 2.9. Consider the set of remainders mod 7, in the form of seven equivalence classes, under addition. This is a cyclic group of seven elements, namely $(\mathbb{Z}_7, +)$ with $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. The identity is 0 and each element can be generated by some addition of 1's, where 1 has order 7.

A *dihedral group* is the set of symmetries (rotation and reflection) of a regular polygon under the group operation function composition. Specifically, D_{2n} is the group of symmetries of a regular n-gon.

For a given set A, a *symmetric group* S_n is the set of bijections $A \to A$ under the group operation function composition. There are n elements in A and the order of S_n is $n!$.

We next look at subgroups and related definitions as these are useful for examining the structure of a group. The *Subgroup Criterion* can be conveniently used to check that a given subset of a group G is a subgroup and its proof is adapted from [2, Chapter 2.1].

Definition 2.10. For a group G, we say that a subset H of G is a *subgroup*, denoted $H \leq G$, if H is a group under the operation of G. (Specifically, check that H is closed under the operation and includes the identity and inverses.) We say that $H = \{1\}$ is the *trivial subgroup* and all $H \neq G$ are *proper subgroups* of G.

Lemma 2.11 (The Subgroup Criterion)**.** *For nonempty subset H of a group G, we say that $H \leq G$ if and only if for all $x, y \in H$, we have $xy^{-1} \in H$.*

Proof. If H is a subgroup of G, by definition H is nonempty and contains the inverses of its elements. Since H is closed, xy^{-1} must be in H since x and y^{-1} are in H.

Now we prove the converse direction. Suppose we have subset H satisfying the condition $xy^{-1} \in H$ for all $x, y \in H$. We will prove that H is group by checking inclusion of identities and inverses and closure. There exists an element $x \in H$, which means that $xx^{-1} \in H$, so H contains the identity $1 = xx^{-1}$. By the same logic, we find that for any $x \in H$, its inverse $x^{-1} = 1x^{-1}$ is also in H. Finally, for any $x, y \in H$, we have shown that $y^{-1} \in H$, so $x(y^{-1})^{-1} \in H$. This is equivalent to $xy \in H$, and hence H is closed under the group operation. □

Definition 2.12. For any subgroup $H \leq G$ and element $g \in G$, we say that $gH = \{gh \mid h \in H\}$ is the *left coset* of H in G and $Hg = \{hg \mid h \in H\}$ the *right coset*. Note that the cardinality of the cosets is the same as $|H|$ (this will be shown in the proof for Theorem 2.19).

Definition 2.13. For a group G and elements $x, g \in G$, we say that gxg^{-1} is the *conjugate* of x. Similarly, we say that the conjugate of a subgroup H of G is $gHg^{-1} := \{ghg^{-1} \mid h \in H, g \in G\}$.

Definition 2.14. For a subgroup N of a group G, we say that N is *normal*, denoted by $N \trianglelefteq G$, if N is invariant under conjugation by elements of G. In other words, $gNg^{-1} = N$.

Note that the conditions $gN = Ng$ for all $g \in G$ and $N \trianglelefteq G$ are equivalent by algebraic manipulation.

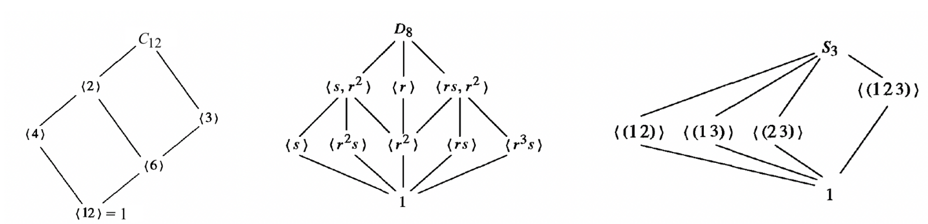
Definition 2.15. A group G is *simple* if $|G| > 1$ and its only normal subgroups are itself and the trivial subgroup.

Definition 2.16. For a group G and a normal subgroup $N \trianglelefteq G$, the *quotient group* of N in G is the set of cosets of N in G, written as G/N.

Notably, lattices are a great method for visualizing the subgroup structures of a group. We will introduce subgroup lattices here with a few examples and illustrate their application to Tarski monsters in the next section.

Definition 2.17. The *lattice of subgroups* of a group G is a plot of all subgroups as points positioned such that the subgroup H is higher than K if and only if $|H| > |K|$ and a path is drawn from subgroups H to K if and only if $H \leq K$.

Example 2.18. Below are the subgroup lattices of C_{12}, D_8, and S_3, respectively [2]. Notice that the bottom of a lattice is always the trivial group as it is the subgroup with the smallest order.



Lastly, we introduce Lagrange's Theorem with a proof based on [2, Chapter 3.1-3.2] and a related lemma, which will be useful for proving properties of Tarski monsters in the following sections.

Theorem 2.19 (Lagrange)**.** *If G is a finite group and H is a subgroup of G, the order of H divides the order of G. Specifically, $\frac{|G|}{|H|}$ is the number of left cosets of H in G.*

Proof. We first show that for a subgroup H of G, all the left cosets of H form a partition of G. Since the operation is closed on G and its subgroups, $G = \bigcup_{g \in G} gH$ as each g shows up in gH ($g = g \cdot 1$ and $1 \in H$). Now suppose that we are given distinct elements $a, b \in G$ and $aH \cap bH \neq \emptyset$. We show that $aH = bH$. Let $x \in aH \cap bH$ and write x as $x = ah_1 = bh_2$. Multiplying by the inverse h_1^{-1} on the right, we see that

$$a = b(h_2 h_1^{-1}) = bh_3$$

for some $h_3 \in H$. Thus, for any $ah \in aH$, we have that $ah = b(h_3 h)$, so $ah \in bH$. This shows that $aH \subseteq bH$, and reversing the argument gives $bH \subseteq aH$. Thus $aH = bH$, so distinct left cosets of H must be disjoint and all such cosets gH partition G.

Let the cardinality of a subgroup H be n and the number of its left cosets be m. Notice that the map $f : h \mapsto gh$ is surjective by definition. Moreover, by the

Cancellation Law it is injective, as $gh_1 = gh_2$ implies $h_1 = h_2$. Therefore, we have a bijection and $|gH| = |H| = n$. So $|G| = kn$ and $\frac{|G|}{|H|}$ is the number of left cosets of H in G. ☐

Lemma 2.20. *For any group G of order n and any element $x \in G$ of order k, the order of x must divide the order of the group, meaning that $k \mid n$.*

Proof. Suppose we have a group G and $x \in G$. Let k be the order of x. Consider the cyclic group $\langle x \rangle = \{1, x, x^2, \dots, x^{k-1}\}$. It is easy to see that $\langle x \rangle$ is of order k and is a subgroup of G, since $\langle x \rangle$ is closed under the group operation and contains the identity and inverses. Thus, by Lagrange's Theorem, k divides $|G|$. ☐

3 The Tarski Monster

In this section, we will define Tarski groups and Tarski monsters, named after Alfred Tarski. We will also look into the history of Alexander Yu. Olshanskii's findings and the Burnside problem, in addition to discussing the structure of Tarski monsters via investigation of their subgroup lattices.

Definition 3.1 (Tarski group)**.** We say that a group T is a *Tarski group* if T is infinite and all proper subgroups of T have prime power order.

Definition 3.2 (Tarski monster)**.** Let T be a Tarski group. We say that T is a *Tarski monster* if there exists a prime p such that every nontrivial proper subgroup of T has order p.

In a series of work published in the 1980s, Alexander Yu. Olshanskii proved the existence of Tarski monsters [4] and classified that Tarski monsters are periodic, finitely generated from two non-commuting elements [5]. He further constructed that the Tarski monster exists for all primes $p > 10^{75}$.

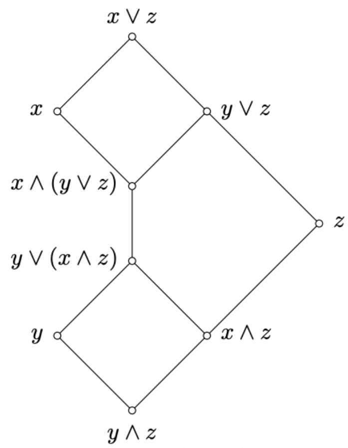
The discovery of Tarski monsters provides an expansive list of counterexamples to the Burnside problem, proposed by William Burnside in 1902. The problem considers whether a group must be finite if it is finitely generated and its elements all have finite order, conditions which the infinite group Tarski monster satisfies. The Tarski monster is an infinite simple non-abelian p-group. A p-group is defined as a group for which all elements have finite order of some power of prime p, though it is commonly understood as the group of prime power order for the finite case. As we will prove in Section 4, Tarski monsters are also simple (Theorem 4.7).

A key feature of Tarski monsters is that they have highly symmetric subgroup lattices. Below we introduce several key properties of lattices [3] and use these to introduce and characterize the Tarski monster's subgroup lattices.

Definition 3.3. For a lattice L and $a, b \in L$, the *meet* of a and b is written as $a \wedge b = z$, where z is the group in L of largest order such that $z \leq a$ and $z \leq b$.

Definition 3.4. For a lattice L and $a, b \in L$, the *join* of a and b is written as $a \vee b = z$, where z is the group in L of smallest order such that $a \leq z$ and $b \leq z$.

Example 3.5. The $\wedge$ and $\vee$ operations may be utilized as shown below [3, p. 99].



Definition 3.6. Let L be a lattice and $x, y \in L$ with $x \leq y$. We define the *interval* from x to y in L as the

$$[x, y] = y/x = \{z \in L \mid x \leq z \leq y\}$$

Definition 3.7. A *sublattice* of a lattice L is a subset $S \subseteq L$ that is a lattice under the same meet and join operations as L. In other words, for all $a, b \in S$, we must have $a \wedge b \in S$ and $a \vee b \in S$.

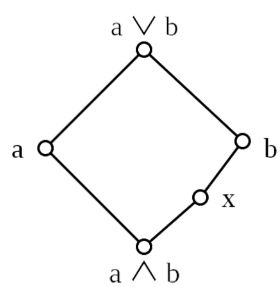
Richard Dedekind devised the *modular law* to introduce modularity as a crucial property of both abelian groups' lattices and lattices of only the normal subgroups. As this property comes from the commutative structures of abelian groups and normal subgroups, it is rare among subgroup lattices of non-abelian groups.

Definition 3.8. A lattice L is *modular* if it satisfies the *modular law*: For $a, b \in L$ with $a \leq b$, we have

$$a \vee (x \wedge b) = (a \vee x) \wedge b \tag{3.9}$$

for all $x \in L$.

Example 3.10. The following pentagon lattice, named $\mathcal{N}_5$, is the smallest non-modular lattice.



Proof. Non-modularity is evident upon consideration of the modular law for x in relation to a and $a \wedge b$. On the lefthand side of (3.9), we have

$$a \vee (x \wedge (a \wedge b)) = a \vee (a \wedge b) = a.$$

On the right hand side, we have

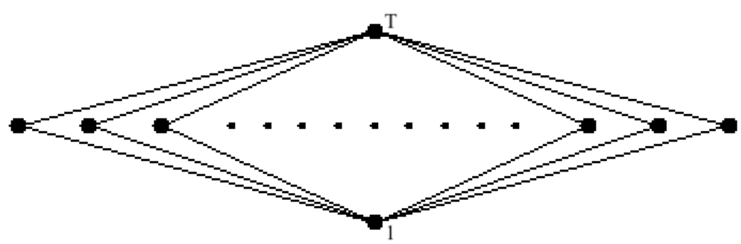
$$(a \vee x) \wedge (a \wedge b) = (a \vee b) \wedge (a \wedge b) = a \wedge b,$$

which is not a. Therefore, $\mathcal{N}_5$ is not modular. □

Theorem 3.11 (Dedekind)**.** *A lattice L is modular if and only if it does not contain $\mathcal{N}_5$ as a sublattice.*

Clearly, a modular lattice must not contain $\mathcal{N}_5$ since $\mathcal{N}_5$ breaks the modular law. The converse can be shown by assuming that L is a non-modular lattice and checking that $\mathcal{N}_5$ exists as a sublattice. A complete proof of Dedekind's Theorem can be found in [3, Chapter 9].

Now we consider the generalized subgroup lattice of a Tarski monster T as shown below.



The subgroups of T are the trivial subgroup, itself, and numerous cyclic subgroups of prime order p. The trivial subgroup is represented as 1 above. It is easy to see that the lattice does not contain $\mathcal{N}_5$, so T must be modular. In fact, we can conveniently check the modular law as well.

As previously discussed, having a modular subgroup lattice is uncommon for non-abelian groups like the Tarski monster. For example, the three subgroup lattices of C_{12}, D_8, and S_3 shown in Example 2.18 are all non-modular by Dedekind's Theorem. Tarski groups in relation to modular subgroup lattices are being further discussed in [1] on the basis of the following extended definition.

Definition 3.12. A group G is an *extended Tarski group* if it has a normal subgroup N such that

1. G/N is a Tarski group
2. for all proper subgroups $H \leq G$, we have $H \leq N$ or $N \leq H$.

4 Properties of Tarski Monsters

As we will see, Tarski monsters have various interesting properties. We will show in particular that all proper subgroups of a Tarski monster are cyclic and build up to a proof for Tarski monsters being simple groups.

Theorem 4.1. *All subgroups of Tarski monster T are cyclic.*

Proof. Let H be a subgroup of a Tarski monster. It must have cardinality prime p. By Cauchy's Theorem, there must be an element $x \in H$ that has order p. The p elements $x, x^2, \dots, x^{p-1}, x^p = 1$ must be all distinct. For if $x^a = x^b$ for some $1 \leq a < b \leq p$, we get that $1 = x^{b-a}$ by the Cancellation Law, which contradicts that the order of x is p. Since there are exactly p elements in H, x is a generator of H and H is cyclic. □

Theorem 4.1 is equivalent to saying that all groups of a prime order are cyclic. We have two corollaries from this result.

Corollary 4.2. *For a group G of prime order p, every non-identity element of G is a generator of the group. That is, $G = \langle x \rangle$ for any $x \in G$ where $x \neq 1$.*

Proof. Suppose we have a group G of prime order p and some $x \in G$ where $x \neq 1$. The order of x must not be 1 as it is not the identity. However, the only divisors of p are 1 and itself, so by Lemma 2.20 we know that the order of x must be p. Now we consider the set $\{x, x^2, \dots x^{p-1}, x^p = 1\}$. As we have discussed in the proof for Theorem 4.1, $\langle x \rangle$ must be G, so any non-identity x can be the generator of G. □

Corollary 4.3. *Let T be a Tarski monster, then for all proper subgroups H and K where $H \neq K$, we have $H \cap K = \{1\}$.*

Proof. For a cyclic group of prime order, every non-identity element is a generator by Corollary 4.2. Thus, if there exists non-identity element $x \in H \cap K$, then $H = \langle x \rangle = K$. Since $K \neq H$, we see that $H \cap K = \{1\}$. □

Definition 4.4. For subgroups H and K of a group G, we define $HK := \{hk \mid h \in H, k \in K\}$.

We now introduce two lemmas, the proofs of which are based on [2, Chapter 3.2]. These lemmas will be used to prove that Tarski monsters are simple groups (Theorem 4.7).

Lemma 4.5. *For subgroups H and K of a group G, the set HK is a subgroup of G if and only if $HK = KH$.*

Proof. If HK is a subgroup of G, note that we have subgroups $K \leq HK$ and $H \leq HK$. Since the three subgroups of G are all closed, we have $KH \subseteq HK$. On the other hand, for any $h_1 \in H$ and $k_1 \in K$, we have $h_1 k_1 = (h_2 k_2)^{-1}$ as an element of the subgroup HK. We also have that $(h_2 k_2)^{-1} = k_2^{-1} h_2^{-1} \in KH$. Hence, $h_1 k_1 \in KH$ so $HK \subseteq KH$. Therefore, $HK = KH$.

For the converse direction, assume that we are given subgroups $H, K \leq G$ such that $HK = KH$. In order to show that HK is a subgroup, we first show that for any $a, b \in HK$, we have $ab^{-1} \in HK$. Let $a = h_1k_1$ and $b = h_2k_2$, so $b^{-1} = k_2^{-1}h_2^{-1}$. Now we consider $ab^{-1} = h_1(k_1k_2^{-1}h_2^{-1})$. We find that

$$k_1k_2^{-1}h_2^{-1} \in KH = HK,$$

so

$$ab^{-1} = h_1(h_3k_3) \in HK$$

since h_1h_3 becomes some $h \in H$. Therefore, HK is a subgroup of G by the Subgroup Criterion. □

Lemma 4.6. *For finite subgroups H and K of a group, the cardinality of HK is*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Proof. Any element of HK is in a left coset hK for some $h \in H$, where each distinct coset is disjoint and has cardinality $|K|$. Therefore, we can simply count the number of distinct left cosets hK for $|HK|$.

For any $h_1, h_2 \in H$, we have $h_1K = h_2K$ if and only if $h_2^{-1}h_1 \in K$. Therefore, this happens when $h_2^{-1}h_1 \in H \cap K$, which similarly is gives an equivalence $h_1(H \cap K) = h_2(H \cap K)$. Note that $H \cap K$ is a subgroup of H, so by Lagrange's Theorem we know that the number of distinct cosets $h(H \cap K)$ is $\frac{|H|}{|H \cap K|}$. We multiply this, which is the number of distinct cosets hK, with the cardinality of K to obtain the above formula. □

Theorem 4.7. *A Tarski monster is a simple group.*

Proof. Let T be a Tarski monster. Assume, for the sake of contradiction, that T is not simple. Then, there exists a proper normal subgroup $N \trianglelefteq T$. Let H be a nontrivial proper subgroup of T different from N. We first show that $HN = NH$. Let $h \in H$ and $n \in N$. By definition, $hnh^{-1} \in N$, so

$$hn = (hnh^{-1})h \in NH.$$

This means that $HN \subseteq NH$. Similarly we can show that $nh = h(h^{-1}nh) \in HN$, so $NH \subseteq HN$. Combining the two results we get $HN = NH$.

Therefore, $HN \leq T$ by Lemma 4.5. On the other hand, by Lemma 4.6 we get that $|HN| = |H| \cdot |N| = p^2$. Note that Corollary 4.3 gives $|H \cap N| = 1$. We reach a contradiction that a subgroup HN of T has order p^2 and not p, so T must be a simple group. □

5 Acknowledgements

First, I would like to thank the PRIMES Circle program and all of its coordinators for providing this wonderful opportunity. I want to especially thank Peter Haine for reviewing drafts of this paper and my mentor Gabrielle Kaili-May Liu for giving feedback on this paper and guiding me in learning about group theory. Finally, I want to thank my Circle group partner Tanvi Ganapathy for supporting me intellectually and my parents for their constant and unconditional support!

References

[1] M. De Falco et al. "Periodic groups with nearly modular subgroup lattice". In: vol. 47. 1-2. Special issue in honor of Reinhold Baer (1902–1979). 2003, pp. 189–205.

[2] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932. ISBN: 0-471-43334-9.

[3] J. B. Nation. "Notes on Lattice Theory".

[4] A. Yu. Olshanskii. "An infinite group with subgroups of prime orders". In: *Izv. Akad. Nauk SSSR Ser. Mat.* 44.2 (1980), pp. 309–321, 479. ISSN: 0373-2436.

[5] A. Yu. Olshanskii. "Groups of bounded period with subgroups of prime order". In: *Algebra i Logika* 21.5 (1982), pp. 553–618. ISSN: 0373-9252.