12-2012

Boolean and Profinite Loops

Benjamin Andrew Phillips
Western Michigan University, baphil@umd.umich.edu

Boolean and Profinite Loops

by
Benjamin Andrew Phillips

A Dissertation
Submitted to the
Faculty of the Graduate College
in partial fulfillment of the
requirements for the
Degree of Doctor of Philosophy
Department of Mathematics
Advisor: Clifton Ealy, Ph.D.

Western Michigan University
Kalamazoo, Michigan
December 2012

BOOLEAN AND PROFINITE LOOPS

Benjamin Andrew Phillips, Ph.D.

Western Michigan University, 2012

A *Quasigroup* G consists of a set G together with a binary operation $\star : G \times G \to G$ such that, for any elements $a, b \in G$ there are unique solutions to the equations $a \star x = b$ and $y \star a = b$ within G. A *loop* is a quasigroup which also contains a 2-sided identity element. More heuristically, loops are essentially non-associative groups. However, without an associative binary operation, some of the familiar properties found in groups, such as 2-sided inverse, need not be present in loops.

The study of quasigroups and loops emerges from a variety of fields, including algebra, combinatorics, geometry, topology and even quantum field theory. In the past, the study of non-associative objects has often been limited by computational complexity. However, the connections to such a diversity of fields, combined with new computation tools have led to an increased interest in the study of loops and quasigroups of late. Over the past decade, great strides have been made in this area, particularly in finite loop theory. Studies of infinite loops have been somewhat less common, and largely done from a Lie-Theory perspective.

Here, we focus on a kind of loop which is built from finite loops by means of a projective limit. Such loops are called *profinite* and have a topological structure closely resembling that of finite loops. We use topological structures as a means of partially circumventing the lack of associativity and show that the resemblance to finite loops holds for important algebraic properties as well. We discuss numerous examples and show that analogues of Lagrange's Theorem, Sylow's Theorem and Hall's Theorem all hold, at least for certain kinds of profinite loops. We also show that the study of profinite loops is inherently tied up with the study of profinite groups, though the two have some interesting differences as well.

ACKNOWLEDGEMENTS

This work would likely not have been possible without the help and support of a great many people. I would especially like to thank Dr. Clifton Ealy for introducing me to the topics of loops and profinite groups and for his support during the writing of this thesis. I would also like to thank my family for all their patience and support, and my wife Nesrin for her tireless encouragement. Also, though it may seem somewhat silly, I'd like to thank my dog, Doc, for his constant need to get outside and walk. While I suspect most dogs have a similar need, I found these walks quite helpful in clearing my head and helping me to think.

I have had the good fortune to have many helpful classmates and instructors from whom I have learned much (not only about mathematics!). While there are too many to list them all, I wish to thank some in particular. Thanks go to Nick Scoville for allowing me to share his passion for mathematics (and his sense of humor); the entire team of the "Gaussian Eliminators" for all the good times; David Erwin for his encouragement; and Allan Bickle for his great passion for games, politics and mathematics. It is quite difficult for me to imagine a path to becoming a mathematician without it including the excellent teaching of John Martino and Jeff Strom, who together taught more than half of the mathematics classes I most enjoyed and helped me to understand what it means to be a mathematician. I also wish to thank my committee members, Dr. Annegret Paul, Dr. Petr Vojtěchovský and Dr. Jay Wood, for all their hard work, support and their many helpful suggestions.

Finally, I wish to dedicate this work to my son, Patrick, who has filled my life with joy, and whose timely arrival encouraged me to actually finish writing.

Benjamin Andrew Phillips

Contents

0.1 Introduction

Although the history of group theory reaches back at least to the mid 19th century, much of how we conceptualize the subject is more recent, going back only to the early 20th century in many cases. Still, throughout the 19th century many of the notable mathematicians were certainly aware of the concepts of various algebraic structures, even if not in their most general forms. It is equally certain that the ideas of non-associative operations have been known far longer; subtraction, for example, is one of the oldest known mathematical operations. Yet, it was not until the 1920s that the two ideas were more rigorously combined.

Often the identities of the originators of important mathematical ideas are lost to history, and this may well be one of those cases, but what is known is that in 1929, a paper titled *On a Generalization of the Associative Law* (see [28]) was published by Anton Suschkewitsch, who was a Russian professor of mathematics in Voronezh. In his paper, Suschkewitsch noted the curious observation that in the proof of Lagrange's Theorem for groups, the idea of associativity is perhaps not needed.

It is difficult to say where Suschkewitsch's ideas might have led, but from other works he published it becomes clear that he was beginning to think about topics which would later become known as quasigroups and isotopy. However, for largely political reasons, he was not allowed to supervise doctoral dissertations. This undoubtedly affected the wider spread of his ideas. Several years later, the algebraic study of non-associative objects seems to have come from looking at alternative algebras. Around the same time, students of differential geometry began looking at so called "web structures". Later it was realized that the geometric creations were in certain ways connected to the algebraic structures of alternative algebras.

The turbulence of a world at war did its best to interrupt efforts at a more coherent view of non-associative structures, but finally (and largely in the post war period) the foundational work would come largely out of the University of Chicago (which is allegedly how the structure known as a loop got its name: from the famous Chicago loop). European and American mathematicians began to see that there were in fact many different viewpoints of non-associative structures, coming from algebra, geometry, combinatorics and topology. While a monumental amount of work was done at this time, particularly by A.A. Albert, R. Bruck and their students, a number of important results concerning the nature of loops and quasigroups have not been

proved until even the last 10 years. For more about the history of quasigroups and loops, see [24]. The subject has enjoyed somewhat of a resurgence of late, largely due to the work of Drápal, Kinyon, Nagy and Vojtěchovský. This dissertation aims to continue that.

Unlike loops, groups have been widely studied, largely because associativity makes them vastly easier to study using traditional set theory. Even topological groups are generally well understood, particularly those with certain user-friendly structure. Among these are the topological groups which are compact, Hausdorff and totally disconnected. These are the profinite groups, and they are of note largely because they share many structural properties with finite topological groups (for more about profinite groups, see [30], [25]). A notable observation is that many of the results in the theory of profinite groups are more topological in nature and do not expressly require an associative binary operation. This suggests that profinite loops may be an approachable topic.

In recent years we have seen a great deal of development in topics concerning finite loops (and to a lesser extent finite quasigroups), particularly in the field of Moufang loops (see [19], [9], [12], [13], [14]). Despite that fact, examples of loops are still often difficult to describe, excessively specific, or collected from other areas of mathematics where certain constructions were useful and which turned out to produce loops. Finally, though, the study of finite loops has mostly been put on a firm footing. Study of infinite loops has at times lagged behind, in part due to a lack of computational tools. One of our goals in this work is to broaden the knowledge of a certain kind of infinite loop which is built from finite loops and ultimately shares many of the hallmark properties of finite algebraic structures. To supplement the non-associative nature of this study, we resort instead to using topological principles to circumvent the lack of associativity where possible.

0.2 Chapter Summary

Chapter one will be devoted to a basic review of general topology. We collect and prove scattered results which will be of use here. We also provide a very watered down summary of certain categorical principles in order to help us better organize and describe certain topics later on. For more on general topology and category theory, see [22], [8], [18].

Chapter two will begin by introducing some of the basic background con-

cepts important to loops. Once more, we collect results which are often scattered but generally well known for Sections 2.1 though 2.5. In Section 2.6 we look at the notion of topological loops. While this topic is not new, the existing work has tended to be in studying loops from a Lie theory perspective. As such, much of the existing work has focused on loops which are compact, Hausdorff and connected. Here we depart somewhat from the existing work and focus on loops which are compact, Hausdorff and totally disconnected. Section 2.7 explores the concept of profinite loops, as well as its categorical dual, Ind-finite loops. Propositions 83 and 84 are generalizations of well known results for profinite groups, but may not be generally known either to loop theorists or group theorists. It is here that we begin to recognize the divergence of profinite group theory and profinite loop theory. The remainder of Section 2.7 is devoted to general results about profinite and ind-finite loops, with some emphasis on how profinite loops and profinite groups may differ. For a basic introduction on the theory of loops and topological loops, see [5], [23], [16].

Chapter three provides numerous examples of profinite, and boolean loops, as well as one new example of an ind-finite loop. In Section 3.1 we highlight some work of Paige and Wells on general linear loops, and show that when these are built from profinite coefficient rings that the profiniteness is preserved in loop form. This is also discussed for the special linear loops. Using the p-adic integer ring, we provide two specific infinite families of profinite loops. In section 3.2 we consider semi-direct and twisted semi-direct products of loops. We show that if we start from a profinite group G and a specific kind of subgroup of $\mathrm{Aut}(G)$ we can build boolean loops using semidirect and twisted semi-direct constructions. We also lay a foundation for looking at the structure of $\mathrm{Aut}(G)$ when G is a profinite loop. This will be discussed further in Chapter 4. Section 3.3 introduces an infinite family of loops which do not seem to have been previously studied in any great detail, though they were hinted at in work by Bruck. We prove a variety of new results about this family and discuss some interesting structural findings. In section 3.4 we use this family to build examples of ind-finite loops, and note that there is a categorical dual of this idea that leads in some cases to further examples of profinite loops. In section 3.5, we mention a construction of Solarin and Sharma of finite Bol loops (see [27]), and use it to construct examples of profinite Bol loops.

In Chapter 4, we attempt to make some interesting connections between group theory and loop theory. In particular, we show that profinite loops

both give rise to, and can be constructed from, profinite groups using the traditional notion of sharply transitive sections. In section 4.1 we show that the multiplication group(s), as well as the inner mapping groups(s) of a profinite loop are profinite. We also show that the nuclei and center of a profinite loop are profinite. Finally, we discuss the multiplication groups of profinite Moufang loops in an effort to detect whether or not their automorphism groups are profinite. In Section 4.2 we show that sharply transitive sections provide a way to build profinite loops from profinite groups and vice-versa. We also note that being a boolean loop is in fact an isotopy invariant, which suggests that it may also be the case that profiniteness is an isotopy invariant. In section 4.3, we look at profinite Moufang loops. We show, with a suitably modified idea of index, that both Lagrange's and Sylow's theorems can be extended to profinite Moufang loops in some measure. Finally, we show that Hall's theorem is essentially true for profinite Moufang loops as well.

Chapter 1

Preliminaries

Since the study of both Boolean and Profinite loops involves elements from a variety of fields, our first goal will be to review those topics which will be relevant to the current study. First, we shall begin with a study of basic topological principles so that the reader will better understand how these principles are applied to the current setting. In this chapter, we collect results which are previously known, but are often scattered throughout the literature. Proofs of these results are provided for the benefit of those readers who lack a sufficient background in topology. For more on these topics, we refer the reader to [8], [22], [18], [30], and [25].

1.1 Topological Spaces

Definition 1. A *topological space* is a set X together with a family of subsets, called *open sets*, satisfying the following conditions:

1. the empty set $\emptyset$ and X are both open sets;
2. the intersection of any two open sets is an open set;
3. the union of any collection of open sets is an open set.

The family of open sets is usually referred to as a *topology* on X. When necessary, we shall denote a topological space by (X, T), where X is the underlying set and T is the topology on X. However, we shall suppress the mention of T whenever possible to avoid excess notation. A subset of X will be called *closed* if its complement is open, that is, if its complement is in T.

It is easily seen that every set X has at least one non-trivial topology. For example, take the collection of open sets to be simply the power set of X. This is generally called the *discrete topology*, and when we consider X as a topological space with the discrete topology, we will refer to X as a *discrete space*.

It often suffices to describe the topology on a set using only a small collection of the open sets. A *base* or *basis* for the topology on a set X is a collection $\{U_\lambda : \lambda \in \Lambda\}$ of open sets such that every open set is a union of some of the sets U_α. We shall also, at times, describe a set which is not a basis, but which can be used to generate a topology in a similar fashion. We shall call a collection B of subsets of X a *subbase* if the collection of open sets consisting of all finite intersections of elements in B, together with X and $\emptyset$ form a base for the topology on X.

Often of interest will be the minimal closed set containing a set Y of interest. Thus we shall denote by $\overline{Y}$ the *closure* of Y. That is, $\overline{Y}$ is the intersection of all closed sets containing Y. If it should be that $\overline{Y} = X$ for some subset Y of X then we say Y is *dense* in X.

If Y is a subset of X then the collection of all subsets of the form $Y \cap U$ where U is an open set of X forms a topology on Y. This topology is inherited from X and so we call this the *subspace topology* on Y. It is also customary to refer to Y under this topology as a *subspace* of X.

Definition 2. A topological space X is called *compact* if given any family $\{U_\alpha\}$ of open sets whose union is X, there is a finite subfamily $\{U_{\alpha_i}\}$, $i = 1, 2, \cdots, n$ for some $n \in \mathbb{N}$ whose union is X.

This says that any *open covering* of X has a finite subcovering.

Definition 3. A space X is called *Hausdorff* if given any two distinct elements $x, y \in X$ there exist open sets U, V containing x and y respectively such that $U \cap V = \emptyset$.

Definition 4. A space X is called *connected* if it cannot be written as the disjoint union of two non-empty open subsets. A space X will be called *totally disconnected* if every connected subset has at most one element. The maximally connected subsets of X are called the *connected components* of X. If $x \in X$ we say the connected component of x is the connected component of X which contains x.

Equivalently, we may define a totally disconnected space X to be a topological space for which, given any pair of distinct elements $x, y \in X$ there are disjoint open sets A and B of X such that $x \in A$, $y \in B$ and $A \cup B = X$.

Most of the spaces we shall find of interest here will be compact, Hausdorff and totally disconnected. Such a space is sometimes called a *Boolean* space. The following Proposition is generally proved in an introductory topology course. A proof can be found in [30], and [8], as well as many others.

Proposition 5. *Let X be a compact Hausdorff space. If A, B are closed subsets such that $A \cap B = \emptyset$ then there exist open subsets U, V such that $A \subseteq U$, $B \subseteq V$ and $U \cap V = \emptyset$.*

Proposition 6. *Let X be a compact Hausdorff space and let $x \in X$. The intersection of all sets containing x that are closed and open is the connected component of x.*

Proof. Let $\{U_i\}$ be the collection of all open and closed sets of X which contain x. Let $C = \bigcap U_i$. Since the connected component of x is contained in every open and closed set containing x, it suffices to show that C is connected. Assume to the contrary that C is disconnected. Then there are closed sets U and V of X with $C = U \cup V$ and $U \cap V = \emptyset$. Since X is compact and U, V are disjoint, by Proposition 5 there are open sets U' and V' in X with $U \subseteq U'$, $V \subseteq V'$ and $U' \cap V' = \emptyset$. So, we have that

$$\Big[X - (U' \bigcup V')\Big] \bigcap C = \emptyset.$$

Additionally, the set $X - (U' \cup V')$ is closed. Thus, by the compactness of X, there is a finite subcollection, $\{U_{i_j}\}_{j=1}^{n}$ of $\{U_i\}$ such that

$$\Big[X - (U' \bigcup V')\Big] \bigcap \left[\bigcap_{j=1}^{n} U_{i_j}\right] = \emptyset.$$

Observe that $B = \bigcap_{j=1}^{n} U_{i_j}$ is a closed and open set which contains x. We have, $x \in (B \cap U') \cup (B \cap V') = B$, and so either $x \in B \cap U'$ or $x \in B \cap V'$. Suppose that $x \in B \cap U'$. This set is clearly open, but since $B \cap V'$ is also open and $(X - B \cap V') \cap B = B \cap U'$, it follows that it is also closed. Then $C \subseteq B \cap U' \subseteq U'$ and hence $C \cap V \subseteq C \cap V' = \emptyset$ from which we conclude that $V = \emptyset$. A similar argument applies when $x \in B \cap V'$. Thus we find that C is in fact connected, and the proof is complete. □

Proposition 7. *If X is compact, Hausdorff and totally disconnected then every open set is a union of sets which are both closed and open.*

Proof. Let $x \in X$ and let U be an open set of containing x. We need only show that U contains a subset containing x which is both open and closed. Let $\{O_i\}$ be the collection of all sets containing x which are both open and closed. By Proposition 6, we have that

$$\bigcap O_i = \{x\}$$

since X is totally disconnected. Since $X - U$ is closed and disjoint from $\cap O_i$, it follows from the compactness of X that there is a finite subcollection $\{O_{i_j}\}_{j=1}^n$ of the O_i sets such that

$$(X - U) \bigcap \left(\bigcap_{j=1}^{n} O_{i_j} \right) = \emptyset.$$

Thus $\cap_{j=1}^n O_{i_j}$ is a set which is both closed and open, and which contains x. This set is clearly contained in U, and thus we find that X has a basis of both closed and open sets for its topology. Thus the result follows. □

Definition 8. Let X and Y be topological spaces. A map $f : X \to Y$ is said to be *continuous* if for each open set U of Y, the set $f^{-1}(U) = \{x \in X : f(x) \in U\}$ is open in X.

An alternative, but equivalent, definition of a continuous mapping is that $f^{-1}(C)$ is closed in X for every closed subset C of Y. It is important to note that the notation $f^{-1}(U)$ is not intended to suggest that f has an inverse, but rather that $f^{-1}(U)$ represents the *pre-image* of the set U under f. If f is bijective then of course f^{-1} exists. When f is bijective and both f, f^{-1} are continuous, we call f a *homeomorphism*.

Proposition 9. *Each closed subset of a compact space is compact.*

Proof. Let X be a compact space and C a closed subset of X. Let $\{U_\alpha\}$ be an open covering of C. As C is closed, $X - C$ is open. Thus $\{U_\alpha\} \cup (X - C)$ is an open covering of X. As X is compact, this has a finite subcover $\{U_{\alpha_1}, \cdots U_{\alpha_n}\} \cup (X - C)$. But then $\{U_{\alpha_1}, \cdots U_{\alpha_n}\}$ is a finite subcover of C, and so C is compact. □

Proposition 10. *Each compact subset of a Hausdorff space is closed.*

Proof. Let X be a Hausdorff space and let Y be a compact subset of X. Then for a fixed $x \in X - Y$ and any $y \in Y$ there are open sets V_y and U_y, containing y and x respectively, with $U_y \cap V_y = \emptyset$. Then $\{V_y\}_{y \in Y}$ is an open cover of Y, and hence has a finite subcover $\{V_{y_1}, \cdots, V_{y_n}\}$. Consider the following set:

$$U = \bigcap_{i=1}^{n} U_{y_i}.$$

We have that U is open, being a finite intersection of open sets, and that $x \in U$. Also, U is pairwise disjoint with V_y for each y, and thus is disjoint from Y. The union of all such sets over all $x \in X - Y$ is thus open, and disjoint from Y, meaning this union is the complement of Y. Hence Y is closed. □

Proposition 11. *If $f : X \to Y$ is continuous and X is compact, then $f(X)$ is compact.*

Proof. Let $\{O_\alpha\}$ be an open covering of $f(X)$. Then $f^{-1}(O_\alpha)$ is open in X for each α, and hence $\{f^{-1}(O_\alpha)\}$ is an open covering of X. As X is compact, it follows that there is a finite subcovering $\{f^{-1}(O_{\alpha_1}), \cdots, f^{-1}(O_{\alpha_n})\}$ of X. But this implies that $\{O_{\alpha_1}, \cdots, O_{\alpha_n}\}$ is a finite subcovering of $f(X)$. Thus $f(X)$ is compact. □

Proposition 12. *If $f : X \to Y$ is continuous and bijective, and if X is compact and Y is Hausdorff, then f is a homeomorphism.*

Proof. Let C be a closed subset of X. Then C is compact by Proposition 9. Since f is continuous, it follows that $f(C)$ is compact by Proposition 11. As $f(C) \subseteq Y$ and Y is Hausdorff, we get from Proposition 10 that $f(C)$ is closed. But this implies that f^{-1} is continuous, as the pre-image of a closed set under f^{-1} is closed. □

Proposition 13. *If $f : X \to Y$ and $g : X \to Y$ are continuous and Y is Hausdorff then the set $\{x \in X : f(x) = g(x)\}$ is closed in X.*

Proof. Let $N = \{x \in X \mid f(x) \neq g(x)\}$ and let $y \in N$. Then there are open sets U and V containing $f(y)$ and $g(y)$ respectively such that $U \cap V = \emptyset$. Then $f^{-1}(U) \cap g^{-1}(V)$ is an open set in X containing y. Furthermore, this open set is contained in N. Thus N is a union of open sets, and so is open, and so its complement is closed. □

Proposition 14. *Let X be a totally disconnected space. Then $\{x\}$ is closed in X for each $x \in X$.*

Proof. Let C be the closure of $\{x\}$ for some $x \in X$. Suppose that C were disconnected. Then there exist disjoint open sets A, B of X such that $C = A \cup B$. Without loss of generality, suppose that $x \in A$. Then the complement of A is open in C and thus A is closed in C. Since C is closed in X, a subset of C is closed in C if and only if it is closed in X. Thus A is closed in X. As A is a closed, non-empty set containing x and lying within the closure of $\{x\}$, it follows that $A = C$. Thus we have a contradiction, and conclude that C is in fact connected. As X is totally disconnected, the fact that C is connected insures that $C = \{x\}$. □

1.2 Cartesian Products of Spaces

In this section, we continue to highlight results which are previously known, but are often scattered throughout the literature. Proofs of these results are provided for the benefit of those readers who lack a sufficient background in topology. For more on these topics, we refer the reader to [8], [22], [18], [30], and [25].

Recall that the *Cartesian Product* of a family $\{X_\alpha\}_{\alpha\in\Lambda}$ of sets is the set, denoted $\prod_{\alpha\in\Lambda} X_\alpha$, of all vectors $(x_\alpha)_{\alpha\in\Lambda}$ where $x_\alpha \in X_\alpha$ for all $\alpha \in \Lambda$. The *projection map* π_β is the map from $\prod_{\alpha\in\Lambda} X_\alpha$ to X_β which takes the vector $(x_\alpha)_{\alpha\in\Lambda}$ to x_β.

Now, suppose that $\{(X_\alpha, T_\alpha)\}_{\alpha\in\Lambda}$ is a family of topological spaces. We shall use the topologies on each X_α to build a topology on $X = \prod_{\alpha\in\Lambda} X_\alpha$, called the *product topology*. A subset A of X is open if and only if A is a union of sets of the form $\prod_{\alpha\in\Lambda} U_\alpha$ where U_α is an open subset of X_α for each $\alpha \in \Lambda$ and such that $U_\alpha \neq X_\alpha$ for only finitely many α. This is equivalent

to saying that the collection $\{\pi_\alpha^{-1}(U)\}$ such that $\alpha \in \Lambda$ and U is open in X_α is a subbase for the product topology.

The product topology is the smallest topology (that is, the one with the fewest open sets) for which the projection maps π_α are continuous. In fact, it can be shown that if Y is another topological space and $f : Y \to X$ then f is continuous if and only if $\pi_\alpha \circ f$ is continuous for each $\alpha \in \Lambda$.

Theorem 15. *Let $\{X_\alpha \mid \alpha \in \Lambda\}$ be a family of topological spaces, and let X be their Cartesian product.*

1. *If X_α is Hausdorff for each α, then so is X.*
2. *If X_α is totally disconnected for each α, then so is X.*

Proof.

1. Suppose X_α is Hausdorff for each $\alpha \in \Lambda$. Let $x = (x_\alpha)$ and $y = (y_\alpha)$ be elements of X with $x \neq y$. Then there exists an index, say $\alpha = n$, for which $x_n \neq y_n$. In X_n there exist disjoint open sets U and V such that $x_n \in U$ and $y_n \in V$. It then follows that $\pi_n(x) \in U$ and $\pi_n(y) \in V$. Thus we get that $x \in \pi_n^{-1}(U)$ and $y \in \pi_n^{-1}(V)$. As the projections are continuous, these are open sets in X. Finally, we see that $\pi_n^{-1}(U) \cap \pi_n^{-1}(V) = \pi_n^{-1}(U \cap V) = \emptyset$. Thus X is Hausdorff.

2. Suppose that C is a non-empty connected component of X. As continuous functions preserve connectedness, it follows that $\pi_\alpha(C)$ is connected for each $\alpha \in \Lambda$. But as X_α is totally disconnected, it follows that $\pi_\alpha(C)$ is a singleton for each α. Thus, we get that C too is a singleton, and so X is totally disconnected.

□

Lemma 16. *Suppose X_α is a compact topological space for each $\alpha \in \Lambda$ and let $X = \prod_{\alpha\in\Lambda} X_\alpha$. Then any open cover of X consisting solely of elements of the form $\pi_\alpha^{-1}(O)$, where O is an open set of X_α, contains a finite subcover.*

Proof. Let U be such an open cover and let U_α denote the set of all open sets O of X_α for which $\pi_\alpha^{-1}(O)$ is in U. We claim there is at least one $\alpha \in A$ for which U_α covers X_α. If this is not the case then for each $\alpha \in A$ there is a point $x_\alpha \in X_\alpha$ such that x_α is not in the union of all the elements in U_α. Then the element $(x_\alpha)_{\alpha\in A}$ of X would not be contained

in any element of U, which contradicts the assumption that U is an open cover of X. Thus, we may choose α such that U_α is a cover of X_α. By compactness, there is a finite subcover $\{O_1, O_2, \cdots, O_n\} \subset U_\alpha$. Then it follows that $\{\pi_\alpha^{-1}(O_1), \pi_\alpha^{-1}(O_2), \cdots, \pi_\alpha^{-1}(O_n)\}$ is a finite subcover of U. □

We shall omit the proof of the following well known result, as it adds little to the current discussion. The proof can be found in many point-set topology texts, including [22].

Theorem 17 (Alexander's Subbase Theorem)**.** *Let X be a topological space with a subbasis B. If every subbasic cover from B has a finite subcover, then X is compact.*

Corollary 18 (Tychonoff's Theorem)**.** *Let $\{X_\alpha\}_{\alpha\in\Lambda}$ be a collection of compact topological spaces and let X be the Cartesian product of this collection of spaces. Then X is compact.*

Proof. The set

$$\{\pi_\alpha^{-1}(O) \mid \alpha \in \Lambda, O \text{ is open in } X_\alpha\}$$

is a subbase of the product topology on X. Any sub-collection of this set that covers X has a finite subcover by Lemma 16. Then by the Alexander Subbase Theorem, the result follows. □

1.3 Categories and Functors

The fairly recent notion of a *category* can provide a convenient conceptual language for many fundamental concepts in mathematics. While much of the work contained in this discourse will be presented in the language of set theory, certain topics which are very categorical in nature will be treated as such. Thus, here we shall see a short introduction to basic definitions of category theory. For a more thorough treatment, we refer the reader to [18].

Definition 19. Let $\mathcal{C}$ consist of a collection $\mathrm{Ob}(\mathcal{C})$ of *objects*, a collection $\mathrm{Morph}(\mathcal{C})$ of *morphisms* and a binary operation $\circ$ called *composition*. Suppose that each morphism has a unique source object and a unique target object in $\mathcal{C}$. The notation $f : a \to b$ will be used to describe the morphism f

having source object a and target object b. If the composition operation is associative, that is when $f : a \to b$, $g : b \to c$ and $h : c \to d$ are morphisms of $\mathcal{C}$ then $h \circ (g \circ f) = (h \circ g) \circ f$, and if there exists an identity morphism for each object a, i.e. a morphism $id_a : a \to a$ such that if $f : a \to b$ is any other morphism from a to b then $id_b \circ f = f = f \circ id_a$, then we call $\mathcal{C}$ a *category*.

Equivalently, a category can be viewed as a directed multigraph (not necessarily finite), where each vertex represents an object of the category and each directed edge represents a morphism. In this model, composition can simply be viewed as a directed walk within the directed multigraph.

A morphism $f : a \to b$ in a category $\mathcal{C}$ is called a *monomorphism* if, for any two morphisms $g, h : d \to a$, $f \circ g = f \circ h$ implies that $g = h$. A morphism $f : a \to b$ in a category is called an *epimorphism* if, for any two morphisms $g, h : b \to c$, $g \circ f = h \circ f$ implies $g = h$. A morphism which is both a monomorphism and an epimorphism is called a *bijective* morphism.

Many heavily studied areas of mathematics can, of course, be viewed in categorical terms. In order to avoid some of the more annoying meta-logical concerns such as issues arising with the "set of all sets", it is customary to use the notion of a *small* set in category theory. A small set is essentially one in a fixed universe of sets, or in other words, simply the set of things one cares to discuss. Some specific categories that will be useful for our purposes are:

•**Sets**: the category with object set consisting of all (small) sets and morphism set consisting of all corresponding set maps.

• **Top**: the category with object set consisting of all (small) topological spaces and morphism set consisting of the corresponding continuous maps.

• **Grps**: the category with object set consisting of all (small) groups and morphism set consisting of the corresponding group homomorphisms.

Often it can be useful to translate the conceptual topics of one category to another. Setting aside meta-logical concerns, we may wish to consider a category where the objects are categories themselves. As it turns out, there is a natural choice for the morphisms in this setting.

Definition 20. Suppose that $\mathcal{C}$ and $\mathcal{D}$ are categories. Then a *(covariant) functor* $F : \mathcal{C} \to \mathcal{D}$ consists of two suitably related functions:

• an *object function* $F : \mathrm{Ob}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{D})$ which assigns each object of $\mathcal{C}$ to an object of $\mathcal{D}$ and

• a *morphism function* also called F, which assigns to every morphism $f : a \to b$ of $\mathrm{Morph}(\mathcal{C})$ a morphism $F(f) : F(a) \to F(b)$ of $\mathrm{Morph}(\mathcal{D})$ in such a way that $F(id_a) = id_{F(a)}$ for each object $a \in \mathrm{Ob}(\mathcal{C})$ and $F(g \circ f) = F(g) \circ F(f)$ for any two morphisms of $\mathcal{C}$ where $g \circ f$ is defined.

Functors were first explicitly used in algebraic topology, where they arose naturally by studying geometric properties using algebraic ones. We shall see them being used in a similar way in this work, but also to study certain algebraic structures using other algebraic structures.

A functor $F : \mathcal{C} \to \mathcal{D}$ is called *faithful* when to every pair a, b of objects of $\mathcal{C}$ and to every pair $f_1, f_2 : a \to b$ of "parallel" morphisms of $\mathcal{C}$, the equality $F(f_1) = F(f_2)$ implies that $f_1 = f_2$. In this case, the functor F is often called an *embedding* of $\mathcal{C}$ into $\mathcal{D}$.

The functor F is called *full* when to every pair a, b of objects in $\mathcal{C}$ and to every morphism $g : F(a) \to F(b)$ of $\mathcal{D}$ there is a morphism $f : a \to b$ of $\mathcal{C}$ with $g = F(f)$.

Definition 21. Let $\mathcal{C}$ be a category. If $\mathcal{S}$ is a category with $\mathrm{Ob}(\mathcal{S}) \subset \mathrm{Ob}(\mathcal{C})$, $\mathrm{Morph}(\mathcal{S}) \subset \mathrm{Morph}(\mathcal{C})$, and which utilizes the composition operation of $\mathcal{C}$ then $\mathcal{S}$ is called a *subcategory* of $\mathcal{C}$.

If $\mathcal{S}$ is a subcategory of $\mathcal{C}$ there is an obvious inclusion map $\mathcal{S} \to \mathcal{C}$ which sends objects and morphisms to themselves. This inclusion is itself a functor and is automatically faithful. If it is also full, we say $\mathcal{S}$ is a *full subcategory* of $\mathcal{C}$. Thus, if $\mathcal{C}$ is given, a full subcategory $\mathcal{S}$ is determined just by its object set.

We shall finish this section with two basic, but important results regarding functors. Each of these facts follows immediately from the definition of functor.

Proposition 22. *Suppose that D is a commutative diagram of objects and morphisms from the category $\mathcal{C}$ and that $F : \mathcal{C} \to \mathcal{D}$ is a functor. Then F transforms D to a commutative diagram $F(D)$ of objects and morphisms in the category $\mathcal{D}$.*

Proposition 23. *If $f : a \to b$ is a bijective morphism of $\mathcal{C}$ and $F : \mathcal{C} \to \mathcal{D}$ is a functor then $F(f)$ is a bijective morphism of $\mathcal{D}$.*

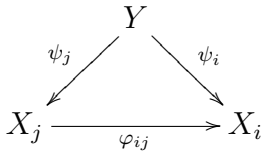
1.4 Direct Limits and Inverse Limits

We shall next discuss a mechanism which allows us to build larger objects from smaller ones. As we shall see, this concept is strongly related to Cartesian products but is less intuitive. For this section, we shall focus on the category of topological spaces and continuous maps, but many of the results are still true in other settings. Again, these results are generally well known, but we collect them and their proofs for the aid of the reader. See [8], [22], [18], [30], and [25] for more information.

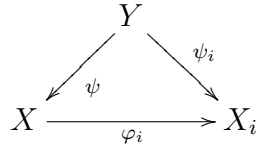
Definition 24. A *directed set* is a partially ordered set I such that for all $i_1, i_2 \in I$ there exists an element $j \in I$ with $i_1 \leq j$ and $i_2 \leq j$.

Definition 25. An *inverse system* (X_i, φ_{ij}) in the category $\mathcal{C}$, indexed by a directed set I, consists of a family $\{X_i : i \in I\}$ of objects in $\mathcal{C}$ and a family $\{\varphi_{ij} : X_j \to X_i \mid i, j \in I, i \leq j\}$ of morphisms in $\mathcal{C}$ such that φ_{ii} is the identity map on X_i for each i, and $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$ whenever $i \leq j \leq k$.

Now, let (X_i, φ_{ij}) be an inverse system in the category $\mathcal{C}$ and let Y be an object in $\mathcal{C}$. We shall call a family of $\mathcal{C}$-morphisms $\{\psi_i : Y \to X_i \mid i \in I\}$ *compatible* with (X_i, φ_{ij}) if $\varphi_{ij} \circ \psi_j = \psi_i$ whenever $i \leq j$. In other words, the family is compatible if the following diagram commutes.



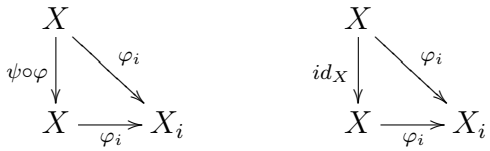
Definition 26. An *inverse limit* (X, φ_i) of an inverse system (X_i, φ_{ij}) in the category $\mathcal{C}$ is an object X in $\mathcal{C}$ together with a compatible family of morphisms $\{\varphi_i\}$ in $\mathcal{C}$ such that whenever $\{\psi_i : Y \to X_i \mid i \in I\}$ is a compatible family of morphisms in $\mathcal{C}$ from an object Y in $\mathcal{C}$ there is a unique morphism $\psi : Y \to X$ such that $\varphi_i \circ \psi = \psi_i$ for each i. In other words, there is a unique morphism ψ such that each of the following diagrams is commutative.



The maps φ_i are called *projections*, though they need not be surjective. In an abuse of notation, we shall sometimes describe an inverse limit by suppressing mention of both the directed set and the morphisms, at least so long as the context is clear. Inverse limits are a special case of the more general idea of a *categorical limit* which need not specifically use an inverse system. Next we shall show that, when an inverse limit exists, it is essentially unique.

Proposition 27. *Suppose (X_i, φ_{ij}) is an inverse system in the category $\mathcal{C}$ indexed by the directed set I. If (X, φ_i) and (Y, ψ_i) are two inverse limits of this system then there is a unique isomorphism $\varphi : X \to Y$ such that $\psi_i \circ \varphi = \varphi_i$ for each $i \in I$.*

Proof. Since the family $\{\psi_i : Y \to X_i \mid i \in I\}$ is compatible with the inverse system, we get by the definition of an inverse limit that there exists a unique morphism in $\mathcal{C}$, $\psi : Y \to X$ such that $\varphi_i \circ \psi = \psi_i$ for all $i \in I$. Similarly, the assumption that Y is an inverse limit insures the existence of a unique morphism $\varphi : X \to Y$ in $\mathcal{C}$ such that $\psi_i \circ \varphi = \varphi_i$ for each $i \in I$. Notice that the following diagrams commute for each $i \in I$:



By definition, there is only one morphism which satisfies this property and so we conclude that $\psi \circ \varphi = id_X$. A similar argument shows that $\varphi \circ \psi = id_Y$ and thus φ is an isomorphism in $\mathcal{C}$. □

While inverse limits need not always exist in a general category $\mathcal{C}$, we shall see that in many familiar categories they do. In fact, we can often even describe the structure of the limit up to isomorphism. We shall do this for the category **Top** of topological spaces and continuous functions explicitly, but it should be noted that a nearly identical proof will work for several other well studied categories.

Theorem 28. *Let (X_i, φ_{ij}) be an inverse system in the category **Top**. Then there exists an inverse limit (X, φ_i) of this system in **Top**.*

Proof. Define X as the subspace of the direct product $\prod_{i\in I} X_i$ of topological spaces consisting of those tuples (x_i) that satisfy the condition $\varphi_{ij}(x_j) = x_i$ if $i \leq j$. Let φ_i denote the restriction of the canonical projection $\pi_i : \prod_{i\in I} X_i \to X_i$ to X. Then φ_i is continuous for each $i \in I$. We must verify (X, φ_i) is an inverse limit.

Suppose that $\{\psi_i : Y \to X_i\}$ is a compatible family of continuous maps. Let $\psi : Y \to \prod_{i\in I} X_i$ be the map which takes the element $y \in Y$ to the tuple $(\psi_i(y))_{i\in I}$. Then we see that $\pi_i \circ \psi = \psi_i$ for each $i \in I$, and so ψ is continuous. By compatibility, we have that $\psi_i = \varphi_{ij} \circ \psi_j = \varphi_{ij} \circ \pi_j \circ \psi$ whenever $i \leq j$. Thus we see that ψ maps into X. Finally, if $\theta : Y \to X$ is any other map satisfying $\varphi_i \circ \theta = \psi_i$ for all $i \in I$ and $y \in Y$ then $\pi_i \circ \theta(y) = \psi_i(y)$ for all $i \in I$ and thus $\theta(y) = \psi(y)$. This completes the proof. □

In light of Proposition 27 and Theorem 28, we may without loss of generality assume that a given inverse limit is as described in Theorem 28. We shall make this assumption unless otherwise specified.

If (X_i, φ_{ij}) is an inverse system in the category $\mathcal{C}$, we shall denote its inverse limit by $\varprojlim X_i$, assuming it exists. For our purposes, we shall mostly be concerned with topological spaces which are Hausdorff, compact and totally disconnected. Under these circumstances, we can say more about the inverse limit of a given system.

Lemma 29. *If (X_i, φ_{ij}) is an inverse system of Hausdorff topological spaces, then $\varprojlim X_i$ is a closed subspace of $\prod_{i\in I} X_i$.*

Proof. Let $(x_i) \in \left(\prod_{i\in I} X_i\right) - \left(\varprojlim X_i\right)$. Then there exist $r, s \in I$ with $r \leq s$ and $\varphi_{rs}(x_s) \neq x_r$. Let U be an open neighborhood in X_r containing $\varphi_{rs}(x_s)$ and choose V to be an open neighborhood of x_r which is disjoint from U. Let O be an open neighborhood of x_s in X_s such that $\varphi_{rs}(O) \subset U$. Consider the basic open subset $W = \prod_{i\in I} V_i$ of $\prod_{i\in I} X_i$ where $V_s = O$, $V_r = V$ and $V_i = X_i$ for $i \neq r, s$. Then W is an open neighborhood of (x_i) in $\prod_{i\in I} X_i$, disjoint from $\varprojlim X_i$. Thus $\varprojlim X_i$ is closed. □

Proposition 30. *Let (X_i, φ_{ij}) be an inverse system of nonempty compact Hausdorff spaces indexed by the directed set I. Then $\varprojlim X_i$ is nonempty.*

Proof. For each $j \in I$, set

$$D_j = \{(x_i) \in \prod_{i \in I} X_i \mid \varphi_{kj}(x_j) = x_k\}$$

whenever $k \leq j$. By the argument applied in Lemma 29, we see that D_j is closed for each j, compact and is non-empty. Furthermore, observe that if $j \leq j'$ it follows that $D_{j'} \subseteq D_j$. From this and the fact that I is directed, we see that the collection $\{D_j \mid j \in I\}$ has the finite intersection property, that is, that any finite intersection of this collection is non-empty. Given the compactness of $\prod_{i \in I} X_i$, it follows that $\cap D_j$ is non-empty. Finally, we have that

$$\varprojlim X_i = \bigcap_{j \in I} D_j$$

and so the result follows. □

We shall next consider a category of inverse systems. Suppose (X_i, φ_{ij}) and (Y_i, θ_{ij}) are inverse systems of topological spaces over the same directed set I. We define a *morphism* of inverse systems $\Upsilon : (X_i, \varphi_{ij}) \to (Y_i, \theta_{ij})$ to be a collection of continuous mappings $\{\upsilon_i : X_i \to Y_i\}$ such that if $i \leq j$ then the following diagram commutes:

$$\begin{array}{ccc} X_j & \xrightarrow{\varphi_{ij}} & X_i \\ \downarrow{\scriptstyle \upsilon_j} & & {\scriptstyle \upsilon_i}\downarrow \\ Y_j & \xrightarrow[\theta_{ij}]{} & Y_i \end{array}$$

The maps υ_i are called the *components* of the morphism Υ. If each component map of a given morphism $\Upsilon : (X_i, \varphi_{ij}) \to (X_i, \varphi_{ij})$ from an inverse system to itself is the identity map, we say Υ is the identity morphism. Composition of these morphisms is defined in the natural way, that is, through composition of the component maps. Thus, we obtain a category **InvTop** of inverse systems of topological spaces. The reader should also note that this process works just as well in other important categories besides **Top**, giving rise to categories of inverse systems of topological groups, etc.

Let (X_i, φ_{ij}) and (Y_i, θ_{ij}) be inverse systems of topological spaces indexed by the directed set I and assume that $X = \varprojlim X_i$ and $Y = \varprojlim Y_i$. Assume that $\Upsilon : (X_i, \varphi_{ij}) \to (Y_i, \theta_{ij})$ is a morphism of inverse systems, having components $\upsilon_i : X_i \to Y_i$. Then the collection $\{\upsilon_i \circ \varphi_i : X \to Y_i\}$ is a compatible

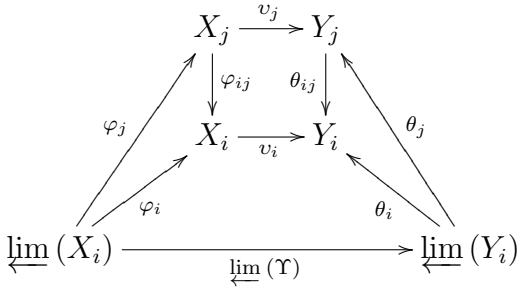
family of continuous mappings and thus induces a continuous map from X to Y. We shall denote this map by $\varprojlim \Upsilon := \varprojlim \upsilon_i : \varprojlim X_i \to \varprojlim Y_i$.

From the above discussion, we see that there is a functor $\varprojlim$ from the category of inverse systems of topological spaces over I to the category of topological spaces. That is, if Υ and Ψ are morphisms in **InvTop**, we have that $\varprojlim (\Psi \circ \Upsilon) = \varprojlim (\Psi) \circ \varprojlim (\Upsilon)$. If $id : (X_i, \varphi_{ij}) \to (X_i, \varphi_{ij})$ is the identity morphism of **InvTop** then $\varprojlim (id)$ is just the identity map on $\varprojlim X_i$.

Suppose that $\Upsilon : (X_i, \varphi_{ij}) \to (Y_i, \theta_{ij})$ is a morphism of inverse systems, and suppose the components υ_i of Υ are all injective. Then it is clear that $\varprojlim (\Upsilon)$ is also injective. However, if instead the component maps are surjective, $\varprojlim (\Upsilon)$ need not be surjective. Luckily, for the kinds of topological spaces we shall be most interested in, we have the following result.

Theorem 31. *Let $\Upsilon : (X_i, \varphi_{ij}) \to (Y_i, \theta_{ij})$ be a morphism of inverse systems of compact Hausdorff topological spaces. If each component map $\upsilon_i : X_i \to Y_i$ is surjective, then the induced map $\varprojlim (\Upsilon) : \varprojlim (X_i) \to \varprojlim (Y_i)$ is also surjective.*

Proof. Let $(y_i) \in \varprojlim (Y_i)$. For each $i \in I$, let P_i denote the pre-image of y_i under υ_i. From the continuity of the component maps, we see that P_i is closed for each i, and hence compact. We have the following commutative diagram:



Thus we see that $\varphi_{ij}(P_j) \subseteq P_i$ for $i \leq j$. Then we have that (P_i, φ_{ij}) is an inverse system of non-empty compact topological spaces. Thus, by Proposition 30, we get that $\varprojlim (P_i) \neq \emptyset$ and see also that $\varprojlim (P_i) \subset \varprojlim (X_i)$. Finally, we note that, by construction, $\varprojlim (\Upsilon)(x_i) = (y_i)$ for any $(x_i) \in \varprojlim (P_i)$. Thus $\varprojlim (\Upsilon)$ is onto. $\square$

Corollary 32. *Let (X_i, φ_{ij}) be an inverse system of compact Hausdorff spaces. Suppose that X is a compact topological space and that $\{\theta_i : X \to X_i\}$ is a continuous family of compatible mappings which are also onto. Then the induced mapping $\theta : X \to \varprojlim (X_i)$ is onto.*

Proof. The collection $\{\theta_i\}$ can be thought of as a morphism from the inverse system (X, id) to the inverse system (X_i, φ_{ij}). Then $\theta = \varprojlim (\theta_i)$ and so the result follows from Theorem 31. □

Corollary 33. *Let (X_i, φ_{ij}) be an inverse system of compact Hausdorff spaces and let $X = \varprojlim X_i$. If Y is a closed subspace of X, then $Y = \varprojlim (\varphi_i(Y))$.*

Proof. There is an obvious embedding of Y into $\varprojlim (\varphi_i(Y))$. Since Y is compact and Hausdorff, the previous corollary implies that the induced mapping of Y to $\varprojlim (\varphi_i(Y))$ is onto, and by uniqueness this mapping is the afore mentioned embedding. Thus we find that $Y = \varprojlim (\varphi_i(Y))$. □

Suppose that (X_i, φ_{ij}) is an inverse system of topological spaces. If φ_{ij} is a surjection for all $i \leq j$, we say (X_i, φ_{ij}) is a *surjective inverse system.* In light of the previous corollary, we find that if (X_i, φ_{ij}) is an inverse system of compact Hausdorff spaces, then there is a corresponding surjective inverse system with the same limit, namely $(\varphi_i(\varprojlim (X_i)), \overline{\varphi}_{ij})$ where $\overline{\varphi}_{ij}$ is the restriction of φ_{ij} to $\varphi_i(\varprojlim (X_i))$. We also have the following Proposition.

Proposition 34. *Let (X_i, φ_{ij}) be a surjective inverse system of nonempty, compact Hausdorff spaces over a directed set I. Then, for each $i \in I$, the projection map $\varphi_i : \varprojlim (X_i) \to X_i$ is onto.*

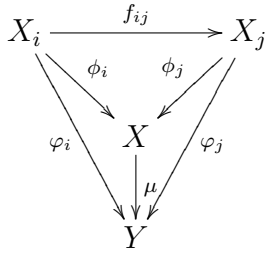
Proof. Fix an arbitrary $i \in I$ and let $x_i \in X_i$. Set $P_j = \varphi_{ij}^{-1}(x_i)$ for $j \in I$ with $i \leq j$. Since φ_{ij} is continuous and surjective for all i, j with $i \leq j$, we get that P_j is a nonempty, compact subset of X_j for each j with $i \leq j$. Furthermore, we find that $\varphi_{sr}(P_r) \subset P_s$ when $i \leq s \leq r$. Thus we find that (Y_i, φ_{ij}) is an inverse system over I where $Y_j = P_j$ for $j \geq i$ and is equal to X_i otherwise. Then the limit Y of this system is non-empty, and by construction for any tuple $(y_i) \in Y$ we have that $\varphi_i(y_i) = x_i$. Thus the ith projection is onto. □

In light of the work above, we see that when we are dealing with compact Hausdorff spaces, we may assume that all inverse systems are surjective, the projection maps from the inverse limit are surjections and that the induced map from the inverse limit obtained from a compatible family of continuous maps is also a surjection. Thus, we see that $\varprojlim$ can be viewed as a functor from the category of inverse systems of compact Hausdorff spaces where the morphisms are surjective continuous maps to the category of topological spaces.

We shall finish this chapter by discussing the categorical *dual* to inverse limits. Generally speaking, this is done by interchanging the role of target and domain. Thus, where inverse limits are good for mapping *to* an inverse system, the dual concept will be useful for mapping *from* a direct system.

Definition 35. Let I be a directed set. A *direct system* (X_i, f_{ij}) in the category $\mathcal{C}$, indexed by I consists of a family $\{X_i : i \in I\}$ of objects in $\mathcal{C}$ and a family $\{f_{ij} : X_i \to X_j : i, j \in I, i \leq j\}$ of morphisms in $\mathcal{C}$ such that φ_{ii} is the identity map on X_i for each i and $f_{ik} = f_{jk} \circ f_{ij}$ whenever $i \leq j \leq k$.

Definition 36. Let (X_i, f_{ij}) be a direct system in the category $\mathcal{C}$. The *direct limit* of this system is an object $X \in \mathrm{Ob}(\mathcal{C})$ together with morphisms $\phi_i : X_i \to X$ satisfying $\phi_j \circ f_{ij} = \phi_i$ whenever $i \leq j$ if for any other such pair (Y, φ_i) there exists a unique morphism $\mu : X \to Y$ which makes the following diagram commute for all i, j with $i \leq j$:



For a given category $\mathcal{C}$, and a given direct system (X_i, f_{ij}) in that category, the direct limit may not exist. When it does, however, it can be shown that any two such limits are categorically isomorphic.

In any category $\mathcal{C}$ where $\mathrm{Ob}(\mathcal{C})$ is a set and where $\mathrm{Morph}(a, b)$ is a set for each pair of objects $a, b \in \mathrm{Ob}(\mathcal{C})$ (this is called a *locally small* category) we may define the so called *Hom-functors* $\mathrm{Hom}_{\mathcal{C}}(A, -)$ and $\mathrm{Hom}_{\mathcal{C}}(-, B)$ by

sending objects to morphism sets and morphisms to induced maps between morphism sets. For more details about this, see [18]. Due in part to the inherently dual nature of direct limits and inverse limits, these two ideas enjoy a special relationship, which is best expressed through use of the above hom-functors.

Suppose (X_i, f_{ij}) is a direct system in the category $\mathcal{C}$ which has a direct limit, (X, ϕ_i) in $\mathcal{C}$. If $\alpha \in \mathrm{Hom}(X, Y) = \mathrm{Morph}(X, Y)$ where Y is some object of $\mathcal{C}$ then it follows that $\alpha \circ \phi_i : X_i \to Y$ is an element of $\mathrm{Morph}(X_i, Y)$. Similarly, due to the universal property of direct limits, for any morphism $g_i : X_i \to Y$ there is a unique map $\alpha : X \to Y$ such that $g_i = \alpha \circ \phi_i$. We may thus build an inverse system $(\mathrm{Hom}(X_i, Y), (f_{ij})_*)$ where $(f_{ij})_*$ is induced by f_{ij} via composition. That is, $(f_{ij})_*(g) = \alpha \circ \phi_j \circ f_{ij}$. It is easily checked that this satisfies the necessary conditions of an inverse system (reversing the ordering on I as needed). We have the following (the proof can be found in [18]):

Proposition 37. *If (X_i, f_{ij}) is a direct system in $\mathcal{C}$ and $X = \varinjlim X_i$ is an direct limit for this system in $\mathcal{C}$, we may form an inverse system $(\mathrm{Hom}(X_i, Y), (f_{ij})_*)$ as described above. If this inverse system has an inverse limit in $\mathcal{C}$ we have that*

$$\mathrm{Hom}(\varinjlim X_i, Y) = \varprojlim \mathrm{Hom}(X_i, Y).$$

We shall find this connection useful in Chapter 3 for generating examples of inverse limits.

Chapter 2

Quasigroups and Loops

For this chapter, we shall continue to discuss known results (and their proofs) for the benefit of the reader. In this case, we begin by trying to present a quick but thorough introduction to the theory of loops, which are inherently algebraic objects. While several of the results in the first six sections are possibly unpublished, it is likely that they are all known to experts of the field. Beginning with Theorem 78, however, the results should be viewed as original (unless otherwise stated). The reader may consult and [23], [5] for additional information.

2.1 Introduction

As our main concern in this discussion will be various algebraic structures, we will begin with some precursory definitions.

Definition 38. A *quasigroup* is a set Q together with a binary operation $\cdot$ such that for any two elements $a, b \in Q$ the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions in Q.

If we consider the equation $a \cdot x = b$, it is customary to denote the unique solution for x as $a\backslash b$. Similarly, it is customary to say $y = b/a$ is the unique solution to the equation $y \cdot a = b$. In this way we define binary operations $/$ and $\backslash$ on Q, usually called right and left division respectively. We also see that the uniqueness of these solutions means that a quasigroup Q has both left and right cancellation laws.

As should be quickly noted, any group is a quasigroup, yet there are many quasigroups which are not groups. For one thing, no assumption is made that a quasigroup must have an identity (and so it may not even make sense to discuss inverses), and even more nefarious, the operation $\cdot$ need not be associative (meaning even such simple ideas as powers need not be well defined). Of particular concern in this work shall be a special kind of quasigroup.

Definition 39. A quasigroup $(L, \cdot)$ which contains an element e such that $a \cdot e = a$ and $e \cdot a = a$ for every $a \in L$ is called a *loop*.

Proposition 40. *A quasigroup may contain at most one 2-sided identity. Furthermore, if a quasigroup Q has a left identity e and a right identity f then $e = f$.*

Proof. If Q is a quasigroup which contains no identity element e then there is nothing to prove. Then suppose Q contains a 2-sided identity element e. Then clearly e is the unique solution to any equation of the form $a \cdot x = a$. The uniqueness of this solution insures that no other 2-sided identity can exist.

Now, if e is a right identity for Q and f is a left identity for Q, it follows that $a \cdot e = a$ for any $a \in Q$ and $f \cdot a = a$ for any $a \in Q$. But then we have that $f = f \cdot e = e$ and this concludes the proof. □

Definition 41. We shall call a quasigroup $(Q, \cdot)$ (or loop) *commutative* if $a \cdot b = b \cdot a$ for all $a, b \in Q$.

Now, let $(Q, \cdot)$ be a quasigroup. Then the fact that there are unique solutions to equations of the form $a \cdot x = b$ and $y \cdot a = b$ for all $a, b \in Q$ insures that in the multiplication table of Q, each element must appear exactly once in every row and every column. Thus we see a connection to a well known combinatorial object.

Definition 42. A standard *Latin square* of order n is an $n \times n$ array in which the symbols $1, 2, \cdots, n$ have been arranged so that each of these appears exactly once in each row and each column of the array.

More generally, we do not require a Latin square to use the symbols $1, 2, \cdots, n$, but rather any set of n distinct symbols. It is clear than any Latin square of order n is isomorphic to a standard Latin square of order n.

Given a standard Latin square of order n we can construct a quasigroup having that Latin square as its multiplication table. The (i, j) entry in the Latin square can be considered to be the product $i \cdot j$. This shall be referred to as the canonical quasigroup built from such a square. Still, there are potentially other quasigroups on the same symbol set that could be constructed in a similar way. It is also quite obvious that for any quasigroup of order n, its multiplication table is a Latin square of order n. As such, some authors recognize no difference between a Latin square of order n and the quasigroup of order n constructed as above. We have chosen to refrain from this, however, as it can be beneficial to view Latin squares in their own right, without any underlying idea of a product. A bijection φ on the set $\{1, 2, \cdots, n\}$ induces a *Latin square isomorphism* by simply relabeling the entries according to φ. This process will also come in handy when dealing with quasigroups.

A *framed* (also sometimes called a *normalized*) Latin square is one in which the first row and first column are both $1, 2, \cdots, n$. That is, the $(1, i)th$ entry is i and the $(j, 1)st$ entry is j. The construction of a quasigroup described above will result in a loop if used on a framed Latin square. Similarly, the multiplication table of a loop L can always be written as a framed Latin square.

Various additional assumptions can be made when studying loops. Many of the more heavily studied such assumptions involve a weakened form of associativity.

Definition 43. A loop G is said to be *Moufang* if it satisfies any one of the following (equivalent) identities:

$$z \cdot (x \cdot (z \cdot y)) = ((z \cdot x) \cdot z) \cdot y$$

$$x \cdot (z \cdot (y \cdot z)) = ((x \cdot z) \cdot y) \cdot z$$

$$(z \cdot x) \cdot (y \cdot z) = (z \cdot (x \cdot y)) \cdot z$$

$$(z \cdot x) \cdot (y \cdot z) = z \cdot ((x \cdot y) \cdot z)$$

It is clear that every group is a Moufang loop. The Moufang identities are not quite strong enough to insure associativity, however. Still, Moufang

loops share much in common with groups, and are historically some of the most well studied. Well known group theoretic results such as Lagrange's Theorem hold for finite Moufang loops, as do some limited Sylow Theorems. We shall discuss this more in Chapter 4.

2.2 Substructures and Products

In this section we continue to summarize known results about quasigroups and loops. For a more thorough treatment, see [23], [5] and others.

Definition 44. Let $(Q, \cdot)$ be a quasigroup and let H be a non-empty subset of Q. Then we say H is a *subquasigroup* of Q if $(H, \cdot)$ is a quasigroup. If $(Q, \cdot)$ and $(H\cdot)$ are both loops, we say H is a *subloop* of Q.

Proposition 45. *Let $(L, \cdot)$ be a loop and H a subquasigroup of L. Then H is a subloop of L. Furthermore, the identity of H is the same as the identity of L.*

Proof. By assumption, H is a subquasigroup of L. Then for $a, b \in H$ the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions in H. If we set $a = b$ we see that for every $a \in H$ there is an element $e_a \in H$ such that $a \cdot e_a = a$. But then e_a must be the identity of L, otherwise the equation $a \cdot x = a$ does not have a unique solution in L. Clearly the identity of L serves also as an identity of H, so the result follows. □

When H is a subquasigroup of Q, we shall write $H \leq Q$. If Q is a loop, this notation will be used to indicate that H is a subloop of Q (and also a subquasigroup of Q).

Proposition 46. *Let $(Q, \cdot)$ be a quasigroup. If H and G are subquasigroups of Q, then $H \cap G$ is a subquasigroup of Q.*

Proof. Consider an equation of the form $a \cdot x = b$ where $a, b \in G \cap H$. As G and H are subquasigroups of Q, this equation has a unique solution for x, and this solution lies in both G and H. Thus it also lies in the intersection of G and H. Similarly, equations of the form $y \cdot a = b$ has a unique solution for y in $G \cap H$ whenever $a, b \in G \cap H$. Thus $G \cap H$ is a subquasigroup. □

Definition 47. Let $(Q, \cdot)$ be a quasigroup. Then if S is a non-empty subset of Q, we define $\langle S \rangle = \bigcap H$ where the intersection is taken over all subquasigroups H of Q that contain S. We call $\langle S \rangle$ the subquasigroup *generated* by S. If $\langle S \rangle = Q$ we say that S *generates* Q. We shall call a quasigroup Q finitely generated if there is a finite set $S \subseteq Q$ such that $\langle S \rangle = Q$.

Because quasigroups and loops may not have an associative operation, working with these structures can feel quite different from the more familiar structure of a group. It can be quite useful to study exactly how close a quasigroup (resp. loop) is to being a group.

Definition 48. Let $(Q, \cdot)$ be a quasigroup. Define the following sets:

$$N_l(Q) = \{a \in Q \mid a \cdot (x \cdot y) = (a \cdot x) \cdot y \ \ \forall x, y \in Q\}$$

$$N_r(Q) = \{a \in Q \mid x \cdot (y \cdot a) = (x \cdot y) \cdot a \ \ \forall x, y \in Q\}$$

$$N_m(Q) = \{a \in Q \mid x \cdot (a \cdot y) = (x \cdot a) \cdot y \ \ \forall x, y \in Q\}$$

The set $N_l(Q)$ is called the *left nucleus* of Q, $N_r(Q)$ is called the *right nucleus* of Q and $N_m(Q)$ is called the *middle nucleus* of Q. The intersection of these three nuclei is called the *nucleus* of Q, and will be denoted by $N(Q) = N_l(Q) \cap N_r(Q) \cap N_m(Q)$.

It should be noted that, for a given quasigroup, there is no guarantee that its left, right or middle nucleus is non-empty. For example, consider the quasigroup Q whose multiplication is given by the following Cayley table:

$\cdot$	1	2	3
1	1	3	2
2	3	2	1
3	2	1	3

Notice that $(1 \cdot 2) \cdot 3 = 3$, whereas $1 \cdot (2 \cdot 3) = 1$. Similarly, $(2 \cdot 1) \cdot 3 \neq 2 \cdot (1 \cdot 3)$ and $(3 \cdot 1) \cdot 2 \neq 3 \cdot (1 \cdot 2)$. Thus we find that $N_l(Q) = \emptyset$. In fact, for the given quasigroup, all three nuclei are empty. If it should occur that a left, right or middle nucleus is non-empty however, then said nucleus has a familiar structure.

Theorem 49. *Let $(Q, \cdot)$ be a quasigroup. Let $x \in \{l, r, m\}$. If $N_x(Q) \neq \emptyset$ then $N_x(Q)$ is a subgroup of Q. In the case where $x = m$, the identity element*

of $N_x(Q)$ serves as a 2-sided identity for Q. If $x = l$, the identity of $N_x(Q)$ serves as a left identity for Q. If $x = r$ the identity of $N_x(Q)$ serves as a right identity for Q.

Corollary 50. *If Q is a quasigroup for which $N_m(Q) \neq \emptyset$ then Q is a loop.*

The reader will also note that a quasigroup Q is a group if and only if $N(Q) = Q$.

Definition 51. Let $(Q, \cdot)$ be a quasigroup. We define the *center* of Q, denoted $Z(Q)$, to be the set $\{a \in N(Q) \mid a \cdot x = x \cdot a \ \ \forall x \in Q\}$.

Theorem 52. *Let Q be a quasigroup. If $N(Q) \neq \emptyset$ then $Z(Q) \neq \emptyset$ and $N(Q), Z(Q)$ are subgroups of Q. Furthermore, $Z(Q)$ is an abelian group.*

Just as for groups, we may define a *Cartesian product* of quasigroups. That is, if $(Q, \cdot)$ and $(G, \diamond)$ are quasigroups, we define the Cartesian product $(Q \times G, \star)$ where $(q_1, g_1) \star (q_2, g_2) = (q_1 \cdot q_2, g_1 \diamond g_2)$. It is clear that the Cartesian product of quasigroups (resp. loops) is again a quasigroup (resp. loop).

Next we see that the nuclei respect products of loops. We shall prove this for the left nucleus, but the reader should note that a similar argument shows this to be true for the right nucleus as well as the full nucleus.

Proposition 53. *Let L_1 and L_2 be loops. Then $N_l(L_1 \times L_2) = N_l(L_1) \times N_l(L_2)$.*

Proof. We note that

$$N_l(L_1 \times L_2) = \{l \in L_1 \times L_2 \mid l \cdot (x \cdot y) = (l \cdot x) \cdot y \text{ for all } x, y \in L_1 \times L_2\}.$$

Then if $(l_1, l_2) \in N_l(L_1 \times L_2)$ we get that $[(l_1, l_2) \cdot (x_1, x_2)] \cdot (y_1, y_2) = (l_1, l_2) \cdot [(x_1, x_2) \cdot (y_1, y_2)]$ which implies that $(l_i \cdot x_i) \cdot y_i = l_i \cdot (x_i \cdot y_i)$ for $i = 1, 2$ and for all $x_i, y_i \in L_i$. Thus $l_i \in N_l(L_i)$ for $i = 1, 2$. It is easily seen that $N_l(L_1) \times N_l(L_2)$ is contained in $N_l(L_1 \times L_2)$, and so the result has been shown. $\square$

Cartesian products are, of course, one standard way to build a quasigroup (resp. loop) from others. In group theory, products and quotients enjoy a fruitful relationship. We next explore the possibility of quotients of quasigroups.

Definition 54. Let Q be a quasigroup and H a subquasigroup of Q. For a given $a \in Q$, define the set $aH = \{a \cdot h \mid h \in H\}$ to be the *left coset of a with respect to H*. Right cosets are defined similarly. We shall denote the set of all left cosets with respect to H by Q/H. The set of right cosets will be denoted $H\backslash Q$.

Unlike the situation with groups, quasigroup cosets need not partition the set Q. For example, consider the quasigroup Q with multiplication defined by the following Cayley table:

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	1	5	2
4	4	5	2	1	3
5	5	3	4	2	1

We see that the set $H = \{1, 2\}$ is a subquasigroup of Q. However, we see that the left cosets with respect to H are

$$1H = 2H = H, \;\; 3H = \{3, 4\}, \;\; 4H = \{4, 5\}, \;\; 5H = \{3, 5\}$$

It is easy to see by inspection that the cosets do not form a partition of Q, as $3H$ and $4H$ have a non-empty intersection, but are not equal. In fact, the above quasigroup is also a loop, as 1 serves as a 2-sided identity, thus we see that even for loops cosets do not partition the loop. Moreover, since Q has order 5 and contains a subloop of order 2, we see that Lagrange's Theorem may not hold. Regarding coset decompositions, however, there is a weaker relationship for loops.

Proposition 55. *Let L be a loop and H a subloop of L. Then $lH \bigcap H = \emptyset$ for any $l \in L - H$. Furthermore, $L - H = \bigcup lH$ where the union is taken over all $l \in L - H$.*

Proof. Let $l \in L - H$ and suppose to the contrary that $lH \cap H \neq \emptyset$. Then there exists some $h_1 \in H$ such that $h_1 = l \cdot h_2$ where $h_2 \in H$. But this implies that $l = h_1/h_2$, which is an element of H since H is a subloop. Finally, since $lH \cap H = \emptyset$ for all $l \in L - H$, we get that the union of all such cosets must be disjoint from H. As $l \in lH$, as H contains the identity, we find that the above union is in fact the complement of H. □

Definition 56. Let L be a loop and H a subquasigroup of L. We say that L has a *left coset decomposition with respect to* H if the left cosets of L with respect to H form a partition of L. A right coset decomposition is defined similarly.

It is possible to classify the kinds of subloops that induce a left (resp. right) coset decomposition.

Theorem 57. *Let L be a loop and H a subloop of L. Then L has a left coset decomposition with respect to H if and only if $(a \cdot h)H = aH$ for all $a \in L$ and all $h \in H$.*

Proof. First, assume that L has a left coset decomposition with respect to H. Then L/H is a partition of L. We have that, for any $a \in L$ and any $h \in H$ that $(ah) = (ah)e$, where e denotes the identity element of L. Thus, $(ah)H \cap aH$ contains (ah). Since L/H is a partition, it follows that $(ah)H = aH$.

Now, suppose that $(ah)H = aH$ for all $a \in L$ and all $h \in H$. We must show that L/H is a partition of L. Notice that since $l = le$ for any $l \in L$, we get that $l \in lH$ and hence

$$L \subseteq \bigcup_{X \in L/H} X.$$

We also see that $lH \neq \emptyset$ for each $l \in L$. Suppose that $aH \cap bH \neq \emptyset$ for some $a, b \in L$. Then there exists $c \in aH \cap bH$ and so $c = ah_1 = bh_2$ for some $h_1, h_2 \in H$. But then we have that $aH = (ah_1)H = (bh_2)H = bH = cH$. Thus, any two cosets of L/H are either disjoint or equal, and so L/H is a partition of L. □

We also note that there is a corresponding result for right coset decompositions.

Definition 58. Let L be a finite loop and let H be a subloop of L. We say H is *Lagrange-like* if $|H|$ divides $|G|$. We say L satisfies the *weak Lagrange* property if every subloop of L is Lagrange-like; we say L has the *strong Lagrange* property if every subloop of L satisfies the weak Lagrange property.

Theorem 59. *Let L be a finite loop and let H be a subloop of L. If L has a left (or right) coset decomposition with respect to H, then H is Lagrange-like.*

Proof. Suppose that L has a left coset decomposition with respect to H. Let P be the set of all the left H-cosets. As P is a partition of L, it follows that

$$|L| = \sum_{X \in P} |X|.$$

Since each such X is a left coset, it follows that $X = aH$ for some $a \in L$. We have that $\lambda_a : L \to L$ given by $x \mapsto ax$ is a bijection for each $a \in L$, and so $|H| = |aH|$ for each $a \in L$. Thus, each coset in P has the same size, insuring that $|L| = m|H|$ where m is the number of elements of P. It follows that $|H|$ divides $|L|$, and thus H is Lagrange-like. A similar argument shows the result holds for right coset decompositions, and so the proof is complete. □

Definition 60. Let L be a loop and H a subloop of L. Then we call H a *normal subloop* if

$$xH = Hx, \;\; (xH)y = x(Hy) \;\; \textit{and} \;\; x(yH) = (xy)H$$

for all $x, y \in L$.

It is elementary to show that if H is a normal subloop of a finite loop L, then H is Lagrange-like.

Now, if H is a normal subloop of $(L, \cdot)$ and $x, y \in L$, we have that for any $h_1, h_2 \in H$ that

$$\begin{aligned} (x \cdot h_1) \cdot (y \cdot h_2) &= ((x \cdot h_1) \cdot y) \cdot h_3 \\ &= ((x \cdot (y \cdot h_4)) \cdot h_3 \\ &= ((x \cdot y) \cdot h_5) \cdot h_3 \\ &= (x \cdot y) \cdot (h_6 \cdot h_3) \in (x \cdot y)H \end{aligned}$$

Then we see that we may define a multiplication $\star$ on L/H by $(xH) \star (yH) = (x \cdot y)H$. Under this operation, we see that the equations $aH \star xH = bH$ and $yH \star aH = bH$ have unique solutions in L/H, namely $xH = (a\backslash b)H$ and $yH = (b/a)H$. Thus L/H is a quasigroup. Furthermore, we have that $eH \star xH = xH = xH \star eH$ for any $x \in L$ where e is the identity of L. Thus in fact L/H is a loop. We shall call this the *quotient loop* of L by H.

2.3 Important Maps

In this section, we continue to discuss known results for the benfit of the reader. See [23] and [5] for more on these topics.

Let $(Q, \cdot)$ be a quasigroup. From the observation that each element of Q appears exactly once in every row and every column of the multiplication table of Q comes find a useful tool for studying these possibly non-associative structures.

Definition 61. Let $(Q, \cdot)$ be a quasigroup and $a \in Q$. Then the map $\lambda_a : Q \to Q$ given by $\lambda_a(x) = a \cdot x$ is called the *left translation* by a, or the *left multiplication* by a. Similarly, the map $\rho_a : Q \to Q$ given by $\rho_a(x) = x \cdot a$ is called the right translation or right multiplication by a.

One immediate observation is that if Q is a quasigroup, these maps are bijections and thus are invertible. If Q is a loop with identity e, then clearly $\lambda_e = \rho_e$ and this map is just the identity map on Q. Even though the multiplication on Q may not be associative, composition of the translation maps is associative. That is, we can conclude that for any $a, x \in L$ we have that $x = \lambda_a \circ \lambda_a^{-1}(x) = a \cdot (\lambda_a^{-1}(x))$ and similarly, $x = (\rho_a^{-1}(x)) \cdot a$. From the uniqueness of solutions in a loop, we can conclude that $\lambda_a^{-1}(x) = a\backslash x$ and $\rho_a^{-1}(x) = x/a$. The following Proposition is useful when dealing with quasigroup calculations.

Proposition 62. *Let Q be a quasigroup. Then, for all $x, y \in Q$ we have that*

$$x \cdot (x\backslash y) = y \qquad (x/y) \cdot y = x$$

$$x\backslash(x \cdot y) = y \qquad (x \cdot y)/y = x$$

$$(x/y)\backslash x = y \qquad x/(y\backslash x) = y$$

Proof. The first two equations follow immediately from the definition of / and \. The expression $x\backslash(x \cdot y)$ is equivalent to $\lambda_x^{-1}(x \cdot y) = \lambda_x^{-1} \circ \lambda_x(y) = y$. The 4th equation follows similarly. For the fifth equation, note that

$$\lambda_{(x/y)}(y) = x = \lambda_{(x/y)} \circ \lambda_{(x/y)}^{-1}(x)$$

Thus, by left cancellation, we find that $y = \lambda_{(x/y)}^{-1}(x) = (x/y)\backslash x$. The sixth and final equation follows by an argument similar to that of the fifth. This completes the proof. □

Definition 63. Let Q_1 and Q_2 be quasigroups. Then a map $\varphi : Q_1 \to Q_2$ is called a *quasigroup homomorphism* if $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in Q_1$. If Q_1 and Q_2 are both loops, then φ is called a *loop homomorphism*. A quasigroup (resp. loop) homomorphism which is bijective is called a *quasigroup (resp. loop) isomorphism*.

Proposition 64. *Let $\varphi : Q_1 \to Q_2$ be a quasigroup homomorphism. Then $\varphi(x/y) = \varphi(x)/\varphi(y)$ and $\varphi(x\backslash y) = \varphi(x)\backslash\varphi(y)$. In other words, φ preserves both left and right multiplication as well as left and right division.*

Proof. Let $\varphi : Q_1 \to Q_2$ be a homomorphism of quasigroups. Let $x, y \in Q_1$. Then we have that $\varphi(y) = \varphi(x \cdot x\backslash y) = \varphi(x) \cdot \varphi(x\backslash y)$. But then $\varphi(x\backslash y)$ is the unique solution to the equation $\varphi(x) \cdot z = \varphi(y)$ and so $z = \varphi(x\backslash y) = \varphi(x)\backslash\varphi(y)$. A similar argument shows that $\varphi(x/y) = \varphi(x)/\varphi(y)$. □

Proposition 65. *Let $\varphi : Q_1 \to Q_2$ be a homomorphism of quasigroups (resp. loops). Then $\varphi(Q_1)$ is a subquasigroup (resp. subloop) of Q_2. If Q_1 and Q_2 are both loops, then $\varphi(1_{Q_1}) = 1_{Q_2}$.*

Proof. Let $a, b \in \varphi(Q_1)$. Then there exist $c, d \in Q_1$ such that $\varphi(c) = a$ and $\varphi(d) = b$. Since Q_1 is a quasigroup, both $c\backslash d$ and d/c are in Q_1. Then by the previous Proposition, $\varphi(c/d) = \varphi(c)/\varphi(d)$ and so the equation $a \cdot x = b$ has a solution in $\varphi(Q_1)$. As φ is onto $\varphi(Q_1)$, uniqueness is assured. A similar argument shows that $a \cdot x = b$ has a unique solution, and so $\varphi(Q_1)$ is a quasigroup.

Now, if Q_1 and Q_2 are loops, note that $\varphi(1_{Q_1}) \cdot \varphi(x) = \varphi(x) = \varphi(x) \cdot \varphi(1_{Q_1})$ for any $x \in Q_1$. Thus $\varphi(1_{Q_1})$ serves as an identity in $\varphi(Q_1)$. But as this is a subloop of Q_2, it follows that $\varphi(1_{Q_1}) = 1_{Q_2}$. □

Definition 66. Let Q_1 and Q_2 be quasigroups. Then a triple of maps (α, β, γ) is called a *homotopy*, where $\alpha, \beta, \gamma : Q_1 \to Q_2$, if $\alpha(x)\beta(y) = \gamma(xy)$ for all $x, y \in Q_1$. If α, β and γ are all bijections, then the triple is called an *isotopy*. In this case, Q_2 is called an *isotope* of Q_1.

If $(\alpha, \beta, \gamma) : (Q_1, \cdot) \to (Q_1, \star)$ is an isotopy for which γ is the identity map we call this a *principal isotopy*. As it turns out, any isotope of a quasigroup can be obtained as a principal isotope. The following can be found in [23].

Theorem 67. *Let $(Q_1, \cdot)$ be a quasigroup and $(Q_2, *)$ an isotope of Q_1. Then there exist $a, b \in Q_1$ such that Q_2 is isomorphic to the quasigroup $(Q_1, \star)$ where $\star$ is defined by $x \star y = x/a \cdot b\backslash y$.*

2.4 The Bruck Functor

In this section we continue to provide results for the benefit of the reader. In some cases, the terminology of the original source has been updated to better fit with the currently used terminologies. See [23], [5], [1] and [18].

Since the translation maps are associative as functions, they can be used to study the multiplication properties of a quasigroup or loop using a group generated by the translations themselves.

Definition 68. Let $(Q, \cdot)$ be a quasigroup. Then we define the *left multiplication, right multiplication* and *multiplication groups* of Q as follows:

$$M_\lambda(Q) = \langle \lambda_a, \mid a \in Q \rangle$$

$$M_\rho(Q) = \langle \rho_a, \mid a \in Q \rangle$$

$$M(Q) = \langle \lambda_a, \rho_a, \mid a \in Q \rangle$$

Thus the left multiplication group is the group under composition, generated by all left translations of Q (and their inverses), etc.

The multiplication groups can be useful for understanding certain structural properties of the underlying quasigroup. The following result is mostly due to Bruck (see [5]), though we have interpreted it into the language of category theory.

Theorem 69. *Let $\mathcal{C}$ be the category of loops and surjective loop homomorphisms, and $\mathcal{D}$ the full subcategory of groups and group homomorphisms. Then there exists a covariant functor $M : \mathcal{C} \to \mathcal{D}$ which takes a loop to its multiplication group.*

Proof. Let $\varphi : L_1 \to L_2$ be a loop homomorphism. Then, for all $x, y \in L_1$ we have that $\varphi(xy) = \varphi(x)\varphi(y)$. That is, $\varphi \circ \rho_y(x) = \rho_{\varphi(y)} \circ \varphi(x)$. Similarly $\varphi \circ \lambda_x(y) = \lambda_{\varphi(x)} \circ \varphi(y)$. As φ is a homomorphism, it follows that $\varphi(x/y) = \varphi(x)/\varphi(y)$ and $\varphi(x\backslash y) = \varphi(x)\backslash\varphi(y)$. These allow us to conclude similar statements about the inverses of the left and right translations.

Then if $\alpha \in M(L_1)$ we get that $\alpha = f(x_1) \circ f(x_2) \circ \cdots \circ f(x_r)$ for some finite r, where $f(x_i)$ is one of $\lambda_{x_i}, \rho_{x_i}, \lambda_{x_i}^{-1}$ or $\rho_{x_i}^{-1}$ for each i. Thus we find that

$$\begin{aligned} \varphi \circ \alpha &= \varphi \circ (f(x_1) \circ \cdots \circ f(x_r)) \\ &= f(\varphi(x_1)) \circ f(\varphi(x_2)) \circ \cdots \circ f(\varphi(x_r)) \circ \varphi \end{aligned}$$

Denote the map $f(\varphi(x_1)) \circ \cdots \circ f(\varphi(x_r))$ by f_φ. If α has a second factorization, $\alpha = g(y_1) \circ \cdots \circ g(y_s)$ for some finite s, we get a corresponding map g_φ. It then follows that $f_\varphi(\varphi(x)) = g_\varphi(\varphi(x))$ for any $x \in L_1$. From the surjectivity of φ, it follows that f_φ and g_φ agree on all of $L_2 = \varphi(L_1)$.

Thus, for any $\alpha \in M(L_1)$ there is a unique map $\alpha_\varphi \in M(L_2)$ making the following diagram commute:

$$\begin{array}{ccc} L_1 & \xrightarrow{\varphi} & L_2 \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha_\varphi} \\ L_1 & \xrightarrow[\varphi]{} & L_2 \end{array}$$

Then we define a categorical map M from the category of loops and loop homomorphisms to the full subcategory of groups and group homomorphisms as follows: If L is a loop, then $M(L)$ is its multiplication group. If $\varphi : L_1 \to L_2$ is a loop homomorphism, then $M(\varphi) = \overline{\varphi}$ where $\overline{\varphi} : M(L_1) \to M(L_2)$ is given by $\overline{\varphi}(\alpha) = \alpha_\varphi$. We see that $\overline{\varphi}(\alpha\beta) = (\alpha\beta)_\varphi = \alpha_\varphi\beta_\varphi = \overline{\varphi}(\alpha)\overline{\varphi}(\beta)$ and thus $\overline{\varphi}$ is a group homomorphism.

We must now show that M is indeed a functor. Let φ be the identity homomorphism from a loop L to L. Then $M(\varphi) = \overline{\varphi}$ where $\overline{\varphi}(\alpha) = \alpha_\varphi = \alpha$.

Thus $\overline{\varphi}$ is the identity on $M(L)$, so M preserves identity maps. Finally, consider the following commutative diagram of loops and loop homomorphisms, where $\alpha \in M(L_1)$:

$$\begin{array}{ccccc} L_1 & \xrightarrow{\psi} & L_2 & \xrightarrow{\varphi} & L_3 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha_\psi} & & \downarrow{\scriptstyle (\alpha_\psi)_\varphi} \\ L_1 & \xrightarrow[\psi]{} & L_2 & \xrightarrow[\varphi]{} & L_3 \end{array}$$

From the diagram we see clearly that $\alpha_{\varphi\circ\psi} = (\alpha_\psi)_\varphi$ and thus $M(\varphi \circ \psi) = M(\varphi) \circ M(\psi)$. Thus M respects composition of loop homomorphisms, and so M is a functor. □

Proposition 70. *Let L_1 and L_2 be loops. Then $M(L_1 \times L_2) = M(L_1) \times M(L_2)$, where $M(L)$ indicates the multiplication group of L.*

Proof. This is a straightforward exercise. □

While the various multiplication groups can be an asset when studying the underlying loop, it is not uncommon for these groups to be extremely large. For a finite loop of order n, it is all too common that at least one of these (and frequently all of them) turn out to be the symmetric group S_n. If L is a loop then an element $\alpha \in M(L)$ is called an *inner mapping* if $\alpha(e) = e$ where e denotes the identity of L. We may define *left inner mappings* and *right inner mappings* similarly. The set of all inner mappings (respectively left or right inner mappings) forms a subgroup of $M(L)$ (resp. $M_\lambda(L)$ or $M_\rho(L)$), which is called the *inner mapping group* of L (resp. left or right inner mapping group), and will be denoted here by $I(L)$ (resp. $I_\lambda(L)$ or $I_\rho(L)$). Generators for these groups are generally well known and can be found in [23], [7]. Additionally, if H is a subloop of L then H is normal if and only if $\alpha(H) \subseteq H$ for each $\alpha \in I(L)$.

2.5 Sharply Transitive Sections

In this section, we shall discuss a means by which a loop can be studied using a related group. These ideas are generally well known within the field, but have been collected here for the benefit of the reader. See [23], [5], [20].

Let G be a group and H a subgroup of G. Let $\pi : G \to G/H$ denote the natural mapping which takes an element of G to its left coset by H. That is, $\pi(g) = gH$. Recall that a map $\sigma : G/H \to G$ is called a *section* if the composition $\pi \circ \sigma$ is the identity map on G/H. Here, we shall be particularly interested in a special kind of section.

Definition 71. Suppose G is a group with $H \leq G$. Suppose $\sigma : G/H \to G$ is a section for which

1. $\sigma(H) = 1_G$ and $\sigma(G/H)$ generates G.
2. for each pair (xH, yH) there exists exactly one $z \in \sigma(G/H)$ for which $(zx)H = yH$.

Then we say σ is a *sharply transitive* section. If σ satisfies only the second condition, then we say σ *acts sharply transitively* (or that $\sigma(G/H)$ acts sharply transitively) on G/H.

Since $\pi \circ \sigma$ is the identity function on G/H, it follows that for any $x \in G$, we have that $\pi \circ \sigma(xH) = xH$, which in turn implies that $\sigma(xH) \in xH$. Thus, we see that a sharply transitive section is a special way of selecting coset representatives for the cosets of G by H. Starting with a sharply transitive section, we may build a loop. Specifically, suppose $\sigma : G/H \to G$ is a sharply transitive section, and let $x, y \in \sigma(G/H)$. We define an operation $*$ on $\sigma(G/H)$ by $x * y = \sigma((xy)H)$.

Proposition 72. *With the operation $*$ defined above, $(\sigma(G/H), *)$ is a loop.*

Proof. Let $a, b \in \sigma(G/H)$. We must first show there are unique solutions to the equations $a * x = b$ and $y * a = b$ in $\sigma(G/H)$. Consider the equation $a * x = b$. This is equivalent to $\sigma((ax)H) = b$. We claim that $x = \sigma((a^{-1}b)H)$ is the unique solution to this equation. Note that $x = (a^{-1}b)h$ for some $h \in H$ and thus $a * x = a * (a^{-1}bh) = \sigma(a(a^{-1}bh)H) = \sigma(bhH) = \sigma(bH) = b$. Thus the given value for x is a solution. This solution is unique since σ is a function.

For the equation $y * a = b$, we note that this is equivalent to $\sigma((ya)H) = b$. From the assumption that σ is a sharply transitive section, there is exactly one $y \in \sigma(G/H)$ such that $yaH = bH$, and this y is thus the unique solution we seek.

Finally, since $\sigma(H) = 1_G$, and since $1_G * a = a * 1_G = \sigma(aH) = a$ we have that 1_G serves as a 2-sided identity for $(\sigma(G/H), *)$. Thus the proof is complete. □

We may also define a product on the coset space G/H. Define $\star : G/H \times G/H \to G/H$ by $xH \star yH = \sigma(xH)yH$. Using an argument similar to that of Proposition 72, it is easy to show that $(G/H, \star)$ is a loop. Since both $(G/H, \star)$ and $(\sigma(G/H), *)$ are loops built from the sharply transitive section σ, it is natural to question how these two loops are related.

Proposition 73. *Let $\sigma : G/H \to G$ be a sharply transitive section. Then the loops $(\sigma(G/H), *)$ and $(G/H, \star)$ are isomorphic.*

Proof. We first note that $\sigma : G/H \to \sigma(G/H)$ is a bijection. We have that

$$\begin{aligned} \sigma(xH \star yH) &= \sigma(xH \star \sigma(yH)H) \\ &= \sigma((\sigma(xH)\sigma(yH))H) \\ &= \sigma(xH) * \sigma(yH) \end{aligned}$$

and so we see that σ is a loop isomorphism. □

Generally speaking, finding a sharply transitive section seems to be quite difficult. However, in [4], R. Baer gave the following characterization of sections which act sharply transitively.

Proposition 74. *Let $\sigma : G/H \to G$ be a section with $\sigma(H) = 1_G$. Then $\sigma(G/H)$ acts sharply transitively on G/H if and only if $\sigma(G/H)$ forms a system of representatives in G for the cosets of each conjugate subgroup gHg^{-1} where $g \in G$.*

Proof. First, let us assume that σ acts sharply transitively. We must show that, for any $a, g \in G$, there is a unique coset bH with $\sigma(bH) \in a(gHg^{-1})$. The expression $\sigma(bH) \in a(gHg^{-1})$ is true if and only if $\sigma(bH) = aghg^{-1}$ for some $h \in H$, that is, if and only if $\sigma(bH)g = agh$ for some $h \in H$. But this says that $(\sigma(bH)g)H = (ag)H$. Since σ acts sharply transitively, there is a unique solution $\sigma(bH)$ to this equation in $\sigma(G/H)$.

The converse follows essentially by a reversal of the above argument. □

We conclude this section by showing that any loop can be constructed in one of the ways described above. If L is a loop then $M(L)$ is a group which acts on the elements of L by function evaluation. Recall that the *stabilizer of* x of an element of $x \in L$ is a subgroup of $M(L)$ that consists of all the elements of $M(L)$ that fix x with respect to this action.

Theorem 75. *Let $(L, \cdot)$ be a loop and let $G = (M_\lambda(L), \circ)$ be the left multiplication group of L. If H denotes the stabilizer of 1_L in G then*

$$(L, \cdot) \cong (\sigma(G/H), *) \cong (G/H, \star)$$

where $\sigma : G/H \to G$ is the sharply transitive section given by $\sigma(\lambda_x H) = \lambda_x$.

Proof. We first note that every element in any coset xH of G/H maps the identity of L to the same element. Thus we see by left cancellation that each such coset contains exactly one left translation. Thus σ is well defined. Clearly σ is a section, and we have that $\sigma(\lambda_{1_L} H) = \sigma(H) = \lambda_{1_L} = 1_G$. For a given pair λ_x, λ_y of left translations, we see that $\lambda_x \circ \lambda_y(1_L) = x \cdot y = \lambda_{x \cdot y}(1_L)$ and so $(\lambda_x \circ \lambda_y)H = \lambda_{x \cdot y} H$. Then, for a given pair $(\lambda_x H, \lambda_y H)$ there is exactly one element λ_z of $\sigma(G/H)$ for which $(\lambda_z \circ \lambda_x)H = \lambda_y H$, namely $\lambda_z = \sigma((\lambda_{(y/x)} H)$. Thus σ acts sharply transitively.

Define $\varphi : \sigma(G/H) \to L$ by $\varphi(\lambda_x) = \lambda_x(1_L) = x$. By the discussion above, we see that φ is a bijection. Also, we have that

$$\begin{aligned} \varphi(\lambda_x * \lambda_y) &= \varphi(\sigma((\lambda_x \circ \lambda_y)H)) \\ &= \varphi(\sigma(\lambda_{x \cdot y} H)) \\ &= \varphi(\lambda_{x \cdot y}) \\ &= x \cdot y \\ &= \varphi(\lambda_x) \cdot \varphi(\lambda_y) \end{aligned}$$

and so φ is a loop isomorphism. The second isomorphism has been shown previously. □

2.6 Topological Loops

The aim of this work is ultimately to study algebraic objects using additional topological properties they may have. As such, this section will be devoted to basic definitions and results which will be useful towards that end. While some of these ideas have been published previously, others seem to be either not previously studied or known within the Mathematical folklore. See [16] for additional reading. We begin with a definition of topological quasigroup that is inspired by the traditional definition of topological group.

Definition 76. A *topological quasigroup* is a quasigroup $(Q, \cdot)$ together with a topology on Q such that the binary operations of left multiplication, right multiplication, left division and right division are all continuous. A *topological loop* is a loop L which is also a topological quasigroup.

The following result is due to Hofmann and Strambach (see [16]). Recall that a topological space X is said to satisfy axiom T_0 if given any two distinct points of X, there is an open set containing exactly one of those points.

Theorem 77. *If a topological quasigroup satisfies axiom T_0 then it is a Hausdorff space.*

The following four results do not seem to have been previously published, but they are all known for topological groups. The results for groups can be found in [30].

Theorem 78. *Let L be a topological loop. If H is an open (resp. closed) subloop of L then every coset Hl or lH of L is open (resp. closed).*

Proof. If H is an open (resp. closed) subloop then $Hl = \{h \cdot l \mid h \in H\} = \rho_l(H)$. But as ρ_l is a homeomorphism, it follows that it takes open (resp. closed) sets to open (resp. closed) sets. Thus Hl is open (resp. closed) for each $l \in L$. The result for left cosets is shown similarly. □

Theorem 79. *Let L be a topological loop. Let H be a subloop of L. If H is open then H is also closed. If H is closed and has finite index then H is open. If L is compact, H is open and H is Lagrange-like then H has finite index.*

Proof. We have that $L - H = \cup lH$ where the union is taken over all $l \notin H$. If H is open, this is a union of open sets, and thus H is closed. If H has finite index, then $L - H$ is a finite union of cosets, each of which are closed since H is closed. Then $L - H$ is closed, and so H is open.

Finally, suppose that L is compact and H is open. Then the sets Hl are open and their union is L. Thus this is an open cover of L. From the compactness of L, it follows that there is a finite subcover, and hence H has finite index. □

Theorem 80. *Let L be a topological loop. If H is a subloop of L containing a non-empty open subset U of L then H is open.*

Proof. Let $hU = \{h \cdot u \mid u \in U\}$. Then since U is open, it follows that hU is as well. Furthermore, we claim that $H = \cap hU$ where the union is taken over all $h \in H$. Clearly $hU \subset H$ for each $h \in H$, as $U \subset H$ and H is a subloop. Now, let $h \in H$. We wish to show that $h \in h_1 U$ for some $h_1 \in H$. That is, that $h = h_1 \cdot u$ for some $u \in U$. But this is equivalent to saying that $h_1 = h/u$ which is an element of H since both h and u are. Thus we find that $H = \cup hU$, and so H is a union of open sets, and so is open in L. □

Theorem 81. *Let L be a topological loop. Then L is Hausdorff if and only if $\{1_L\}$ is a closed set. If N is a normal subloop of L, then L/N is Hausdorff if and only if N is closed in L.*

Proof. By Proposition 10, if L is Hausdorff, then any one element subset of L is closed, since such a subset is compact. Thus we must only show that if $\{1_L\}$ is a closed subset of L then L is Hausdorff. We shall do this by showing that axiom T_0 is satisfied. If $\{1_L\}$ is closed this implies that $\{a\} = \{\lambda_a(1_L)\}$ is closed for any $a \in L$. Then if $a, b \in L$ with $a \neq b$ we have that $L - \{a\}$ is an open set containing b, but not containing a. Thus L satisfies T_0. Then by Theorem 77 the result follows. □

The following result of Scheerer and Strambach will be useful for our purposes, especially since most of our attention is restricted to compact spaces. A proof can be found in [26].

Proposition 82. *Suppose Q is a quasigroup and that Q is a topological space. If Q is compact and the map $Q \times Q \to Q$ given by $(x, y) \mapsto x \cdot y$ is continuous then Q is a topological quasigroup.*

2.7 Profinite and Ind-finite Loops

The object of this section is to show some basic facts about inverse and direct limits of loops. Specifically, we shall focus our attention on inverse or direct limits of systems of finite loops. In light of Theorem 28, the following result should come as no surprise.

Proposition 83. *Suppose that (G_i, φ_{ij}) is an inverse system of compact, Hausdorff and totally disconnected topological loops and continuous loop homomorphisms. Then $\varprojlim G_i$ is a topological loop.*

Proof. Since each loop G_i is a topological space, we have that $\varprojlim G_i$ exists as a topological space and that

$$\varprojlim G_i \cong \{(g_i)_{i\in I} \in \prod G_i \mid \varphi_{ij}(g_j) = g_i \forall i \leq j\}.$$

Furthermore, the above set is non-empty and clearly contains the identity element of $\prod G_i$. We shall show that this set is in fact a subloop of the Cartesian product $\prod_{i\in I} G_i$. Suppose that $(a_i)_{i\in I}$ and $(b_i)_{i\in I}$ are elements of $\varprojlim G_i$. Consider an equation of the form $(a_i)_{i\in I} \cdot (x_i)_{i\in I} = (b_i)_{i\in I}$. Since the operation is computed coordinate wise, it follows that this is equivalent to $a_i \cdot x_i = b_i$ for all $i \in I$. Then we have that $x_i = a_i \backslash b_i$ is the unique solution to this equation in G_i for each i. Notice that for $i \leq j$ we have

$$\begin{aligned} \varphi_{ij}(x_j) &= \varphi_{ij}(a_j \backslash b_j) \\ &= \varphi_{ij}(a_j) \backslash \varphi_{ij}(b_j) \\ &= a_i \backslash b_i \\ &= x_i \end{aligned}$$

Thus we find that $(a_i \backslash b_i)_{i\in I}$ is an element of $\varprojlim G_i$. A similar computation shows that equations of the form $(y_i)_{i\in I} \cdot (a_i)_{i\in I} = (b_i)_{i\in I}$ also have unique solutions in $\varprojlim G_i$. Thus $\varprojlim G_i$ is a loop.

Finally, note that since multiplication, as well as left and right division, is continuous coordinate wise, it follows that $\varprojlim G_i$ is a topological loop under a subspace topology of the product topology on $\prod G_i$. This completes the proof. □

When each G_i is a finite loop with the discrete topology, we shall call $\varprojlim G_i$ a *profinite loop*. Next we shall see that a profinite loop never has countably infinite cardinality. This result is previously known both for both profinite groups and topological spaces arising as an inverse limit of finite topological spaces. See [30].

Theorem 84. *Let G be a profinite loop. Let $\{C_i\}$ be a countably infinite set of distinct non-empty closed subsets of G having empty interior. Then*

$$G \neq \bigcup_{i=1}^{\infty} C_i.$$

Thus, the cardinality of G is either finite or uncountable.

Proof. Assume to the contrary that

$$G = \bigcup_{i=1}^{\infty} C_i$$

for some collection $\{C_i\}$ of distinct closed subsets of G which have empty interior. Then $D_i = G - C_i$ is an open dense set of G for each i.

Suppose that U_0 is a non-empty open subset of G. Then $U_0 \cap D_1$ is open and non-empty. Then by Proposition 7 there is a basis for G consisting of closed and open subsets, and so there is a nonempty open and closed subset U_1 of $U_0 \cap D_1$. Similarly, there is a non-empty closed and open subset U_2 of $U_1 \cap D_2$, and so on. Thus we obtain a nested sequence of nonempty open and closed subsets

$$U_1 \supseteq U_2 \supseteq \cdots \supseteq U_i \supseteq \cdots$$

such that $U_i \subseteq D_i \cap U_{i-1}$ for each i. As G is compact, we have that

$$\bigcap_{i=1}^{\infty} U_i \neq \emptyset$$

by the finite intersection property. However, we also have that

$$\begin{aligned}\bigcap_{i=1}^{\infty} U_i &\subseteq \bigcap_{i=1}^{\infty} D_i \\ &= \bigcap_{i=1}^{\infty} (G - C_i) \\ &= G - \bigcup_{i=1}^{\infty} C_i \\ &= \emptyset\end{aligned}$$

Thus we arrive at a contradiction, and so we conclude that

$$G \neq \bigcup_{i=1}^{\infty} C_i$$

for any such collection. Since G is not a countably infinite union of singletons, it follows that G is either finite or uncountable. □

There are several known equivalent notions for profinite groups. See [30] and [25]. In the case of loops, however, we find that some of these are either not meaningful or not true. Still, motivated by the group theoretic work, we have the following result.

Theorem 85. *Let G be a topological loop. The following are equivalent:*

1. *G is profinite.*
2. *G is isomorphic (as a topological loop) to a closed subloop of a Cartesian product of finite loops.*
3. *G is compact and the intersection of all open normal subloops of G is trivial.*

Proof. (1) ⇒ (2): This follows immediately from Lemma 29 since a finite topological loop with the discrete topology is compact, Hausdorff and totally disconnected.

(2) $\Rightarrow$ (3): Suppose G is isomorphic to a closed subloop $\widehat{G}$ of $\prod G_i$, where each G_i is a finite loop. For each i, let K_i be the kernel of the projection map from $\prod G_i$ to G_i. Since G_i is finite, we get that it is compact for each i, and thus so is $\prod G_i$. As $\widehat{G}$ is closed in the product space, we find that it too is compact. For each i, let $N_i = K_i \cap \widehat{G}$. Since K_i is an open normal subloop of $\prod G_i$ for each i, it follows that N_i is an open normal subloop of $\widehat{G}$. Since $\bigcap K_i = 1$ it follows that $\bigcap N_i = 1$ as well. Thus, the intersection of all open normal subloops of L must be trivial.

(3) $\Rightarrow$ (1): Let $\mathcal{U}$ denote the collection of all open normal subloops of G. Define a relation $\leq$ on $\mathcal{U}$ by $V \leq U$ if U is a subloop of V and let $\varphi_{UV} : G/U \to G/V$ be the natural projection whenever $U \leq V$. It follows that $(G/U \ \ (U \in \mathcal{U}), \varphi_{UV})$ is an inverse system of finite loops. If π_U denotes the canonical projection from G to G/U, it follows that these maps are compatible with the above inverse system. As such, we have a unique map $\psi : G \to \varprojlim G/U$, which is onto since the system is surjective. We shall show ψ is a topological isomorphism. Since G is compact, we need only show that ψ is injective. Let $x \in \ker(\psi)$. Then $\pi_U(x) = \varphi_U \circ \psi(x) = 1$ and thus $x \in U$ for every open subloop U of G. Since the intersection of all such subloops is trivial, it follows that $x = 1$, and so $\ker(\psi)$ is trivial. Thus ψ is injective, and we find that $G \cong \varprojlim G/U$, so G is profinite. $\square$

Note if G is a profinite loop, it is the inverse limit of an inverse system of finite loops. Such loops are compact, Hausdorff and totally disconnected under the discrete topology, and thus any profinite loop is a topological loop which is compact, Hausdorff and totally disconnected. A loop (or group) with these three properties is called a *Boolean* loop (respectively group). When G is a topological group, it can be shown (see [30], [25]) that if G is compact, Hausdorff and totally disconnected then G is a profinite group. That is, a Boolean group is also profinite. The proof of this is dependent on being able to find an open normal subgroup in any open and closed neighborhood of the identity, a result which holds for all compact groups. However, it is currently unknown whether loops enjoy the same property. The construction of such a normal subgroup in the group case is heavily dependent on an associative binary operation, and so this construction does not apply to loops in general. Still, based on the known examples, we have the following Conjecture.

Conjecture 86. *If G is a topological loop which is compact, Hausdorff and totally disconnected then G is profinite.*

Some work has been done to try to prove this Conjecture, but the problem remains open. In [15], Herfort and Plaumann show that if G is a Boolean loop for which the inner mapping group $I(G)$ is finite, then G is profinite.

Proposition 87. *If G is a Boolean loop which has a basis $\beta = \{H_\lambda\}_{\lambda\in\Lambda}$ of subloops for which $\bigcap_{\alpha\in I(G)} \alpha(H_\lambda)$ is open for each λ then G is profinite.*

Proof. The given hypothesis is enough to insure that G has a basis of open normal subloops, for if H_λ is a subloop of G then $K = \bigcap_{\alpha\in I(G)} \alpha(H_\lambda)$ is a normal subloop of G, which by assumption is open. It follows then, that $G \cong \varprojlim G/K$ where the inverse limit runs over all such K. □

From Corollary 33, we also have that any closed subloop of a profinite loop is profinite.

Proposition 88. *Let G be a profinite loop. Then the left, right and middle nuclei of G are profinite. Additionally, the nucleus $N(G)$ is profinite.*

Proof. We have that the left nucleus of G is the set

$$\begin{aligned} N_l(G) &= \{x \in G \mid x(yz) = (xy)z \ \ \forall y, z \in G\} \\ &= \{x \in G \mid \rho_{(yz)}(x) = \rho_z \circ \rho_y(x) \ \ \forall y, z \in G\} \\ &= \bigcap_{y,z\in G} \{x \in G \mid \rho_{(yz)}(x) = \rho_z \circ \rho_y(x)\} \end{aligned}$$

Given that $\rho_a : G \to G$ is a continuous map to a Hausdorff space for any $a \in G$, it follows from Proposition 13 that the sets $\{x \in G \mid \rho_{(yz)}(x) = \rho_z \circ \rho_y(x)\}$ are closed, and hence the intersection of these sets is closed as well. Similar arguments show the result to be true for the right and middle nuclei as well. As the nucleus is the intersection of the left, middle and right nuclei, it too is closed in G and hence profinite. □

Proposition 89. *If G is profinite, then the center, $Z(G)$, of G is also profinite.*

Proof. We have that the center of G is the set

$$\begin{aligned} Z(G) &= \{x \in N(G) \mid yx = xy \ \ \forall y \in G\} \\ &= \{x \in N(G) \mid \lambda_y(x) = \rho_y(x) \ \ \forall y \in G\} \\ &= \bigcap_{y \in G} \{x \in N(G) \mid \lambda_y(x) = \rho_y(x)\} \end{aligned}$$

and since λ_a, ρ_a are continuous maps to a Hausdorff space, it follows that $Z(G)$ is the intersection of closed sets of G, and hence is closed in G (and $N(G)$). □

Proposition 90. *Suppose G and H are profinite loops. Then the Cartesian product $G \times H$ is profinite with respect to the product topology.*

Proof. First, note that if N is an open normal subloop of G and K is an open normal subloop of H then $N \times K$ is an open normal subloop of $G \times H$, since open sets are unions of sets of the form $U \times V$ where U and V are open in G and H respectively. Since the intersection of all open normal subloops in G is trivial, and the intersection of all open normal subloops in H is also trivial, it follows that the intersection of the open normal subloops in $G \times H$ of the form $N \times K$ is also trivial. Thus $G \times H$ is profinite. □

We shall finish this section with a discussion of the dual concept of profinite loops.

Let (G_i, f_{ij}) be a direct system of loops indexed by a directed set I. Similar to the case of inverse limits, in the category of loops and loop homomorphisms this system has a direct limit which is unique up to isomorphism. If $a_i \in G_i$ and $b_j \in G_j$, define a relation by $a_i \sim b_j$ if there is an index $k \geq i, j$ such that $f_{ik}(a_i) = f_{jk}(b_j)$. Then $\sim$ is an equivalence relation. We shall use this relation to build a direct limit for the system. Denote the equivalence class of a for this relation by $[a]$.

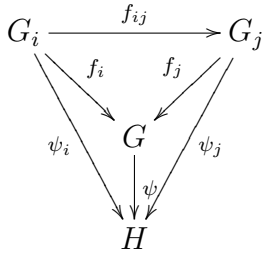
Proposition 91. *Let (G_i, f_{ij}) be a direct system of loops. Then*

$$G = \left(\bigsqcup_i G_i \right) / \sim$$

is a direct limit of the system, where $\sqcup$ denotes the disjoint union, and this limit is unique up to isomorphism.

Proof. We must first show that G is a loop. Let $[a], [b] \in G$. Consider an equation of the form $[a][x] = [b]$. If $a_i \in G_i$ is some representative for $[a]$ and $b_j \in G_j$ is some representative for $[b]$ there is some index k with $k \geq i, j$ such that $f_{ik}(a_i) \cdot (f_{ik}(a_i) \backslash f_{jk}(b_j)) = f_{jk}(b_j)$. Furthermore, we see that if l is any other index with $l \geq k \geq i, j$ then $f_{kl}(f_{ik}(a_i) \backslash f_{jk}(b_j)) = f_{il}(a_i) \backslash f_{jl}(b_j)$ and thus we see that the unique solution to the equation $[a][x] = [b]$ is the equivalence class of $f_{ik}(a_i) \backslash f_{jk}(b_j)$. A similar argument shows that equations of the form $[y][a] = [b]$ also have unique solutions, and so G is a quasigroup. Notice that the equivalence class of the identity in any G_i serves as a two sided identity for G, and so G is a loop.

We must next show that G is a direct limit of the direct system. Let $f_i : G_i \to G$ be given by $f_i(x) = [x]$. Then it follows from the definition of the binary operation on G that f_i is a loop homomorphism. Suppose $\{\psi_i : G_i \to H\}$ is a collection of compatible maps to the loop H. We must show the existence of a unique map $\psi : G \to H$ making the following diagram commute whenever the relevant maps are defined:



Now, if $g \in G$ then $g = f_i(x)$ for some $x \in G_i$ and some i. Define $\psi(g) = \psi_i(x)$. It is evident that ψ is a loop homomorphism. Then we have that $\psi_i(x) = \psi(g) = \psi \circ f_i(x)$ and thus the diagram above commutes. Additionally, by the nature of the above requirements, we see that this is the only possible function satisfying the necessary conditions.

If G and H are two direct limits of the given system, then in addition to the maps in the diagram above, there is a map $\sigma : H \to G$ making the diagram commute. That is, we have $\psi_i = \psi \circ f_i$ and $f_i = \sigma \circ \psi_i$ for each i. But this implies that $\psi_i = \psi \circ \sigma \circ \psi_i$ for each i and $f_i = \sigma \circ \psi \circ f_i$ for each i. Thus, it follows that $\psi \circ \sigma$ is the identity on $\psi_i(G_i)$ for each i and that $\sigma \circ \psi$ is the identity on $f_i(G_i)$ for each i, from which it follows that $\psi \circ \sigma$ and $\sigma \circ \psi$ are the identity maps on H and G respectively. Thus G and H are isomorphic. This completes the proof. $\square$

If (G_i, f_{ij}) is a direct system of loops, we denote its direct limit by $\varinjlim G_i$, suppressing mention of the maps whenever the context is clear. If G is the direct limit of a direct system of finite loops, we say G is an *Ind-finite* loop.

Chapter 3

Examples

3.1 General Linear Loops

Let R be a commutative ring with identity. Then the set of 2×2 *Zorn Matrices* on R is the set

$$\mathrm{Zorn}(R) = \left\{ \begin{bmatrix} a & \overline{x} \\ \overline{y} & b \end{bmatrix} : a, b \in R \text{ and } \overline{x}, \overline{y} \in R^3 \right\}.$$

To represent the split-octonians using matrices, Max Zorn defined an operation $\star$ on the above set as follows:

$$\begin{bmatrix} a_1 & \overline{x}_1 \\ \overline{y}_1 & b_1 \end{bmatrix} \star \begin{bmatrix} a_2 & \overline{x}_2 \\ \overline{y}_2 & b_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 + (\overline{x}_1 \cdot \overline{y}_2) & a_1 \overline{x}_2 + b_2 \overline{x}_1 - (\overline{y}_1 \times \overline{y}_2) \\ a_2 \overline{y}_1 + b_1 \overline{y}_2 + (\overline{x}_1 \times \overline{x}_2) & b_1 b_2 + (\overline{y}_1 \cdot \overline{x}_2) \end{bmatrix}$$

where $\cdot$ indicates the standard dot product on R^3 and $\times$ indicates the cross product on R^3.

Recall that an *alternative algebra* is an algebra A for which the multiplication satisfies $x(xy) = (xx)y$ and $(yx)x = y(xx)$ for all elements $x, y \in A$. The following result is well known (see [21], [29], [11]).

Proposition 92. *Let R be a commutative ring with identity. Then* $\mathrm{Zorn}(R)$ *is a non-associative alternative algebra with addition defined coordinate-wise and multiplication defined as above.*

In fact, Albert showed in [2] that every simple alternative algebra containing a non-trivial idempotent is either associative or isomorphic to the

above construction for some R. Recall that an element a of an algebra A is called a *unit* if there exist $x, y \in A$ such that $ax = 1 = ya$. The following was hinted at by Paige in [21] and expressly shown by Wells in [29].

Proposition 93. *An element*

$$\begin{bmatrix} a & \overline{x} \\ \overline{y} & b \end{bmatrix}$$

in $\mathrm{Zorn}(R)$ *is a unit if and only if* $ab - \overline{x} \cdot \overline{y}$ *is a unit in* R.

As such, it is natural to define a map $\det : \mathrm{Zorn}(R) \to R$ given by

$$\begin{bmatrix} a & \overline{x} \\ \overline{y} & b \end{bmatrix} \mapsto ab - \overline{x} \cdot \overline{y}.$$

It then follows that an element of $M \in \mathrm{Zorn}(R)$ is invertible if and only if $\det(M)$ is a unit in R. The map det is multiplicative on $\mathrm{Zorn}(R)$. Analogous to a general linear group over a commutative ring with identity, define $GLL(R)$ to be the set of all invertible elements of $\mathrm{Zorn}(R)$. This is called the *general linear loop* over R. From the work of Paige, Bruck and Kleinfeld (see [21], [6]) we have the following:

Theorem 94. *The subset* $GLL(R)$ *of* $\mathrm{Zorn}(R)$ *is a Moufang loop under the multiplication of* $\mathrm{Zorn}(R)$. *Furthermore, the set* $SLL(R) = \{M \in GLL(R) : \det(M) = 1\}$ *is a normal Moufang subloop of* $GLL(R)$.

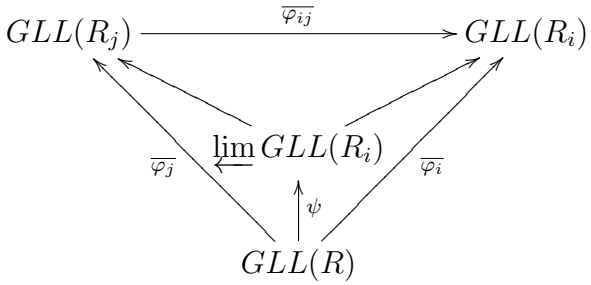
Theorem 95. *Suppose* (R_i, φ_{ij}) *is an inverse system of finite commutative rings with identity and ring homomorphisms. Suppose that* $R = \varprojlim R_i$. *Then* $GLL(R)$ *is a profinite Moufang loop and*

$$GLL(R) \cong \varprojlim GLL(R_i).$$

Proof. The ring homomorphisms $\varphi_{ij} : R_j \to R_i$ (where $i \leq j$) can be extended to maps $\overline{\varphi_{ij}} : GLL(R_j) \to GLL(R_i)$ by

$$\overline{\varphi_{ij}}\left(\begin{bmatrix} a & \overline{x} \\ \overline{y} & b \end{bmatrix}\right) = \begin{bmatrix} \varphi_{ij}(a) & \varphi_{ij}^3(\overline{x}) \\ \varphi_{ij}^3(\overline{y}) & \varphi_{ij}(b) \end{bmatrix}$$

where φ_{ij}^3 denotes that map $\varphi_{ij} \times \varphi_{ij} \times \varphi_{ij}$. Since φ_{ij} is a ring homomorphism for each $i \leq j$, it follows that $\overline{\varphi_{ij}}$ respects coordinate wise addition, multiplication and units, and hence preserves dot and cross products as well. Thus $\overline{\varphi_{ij}}$ is a loop homomorphism for each $i \leq j$. In a similar way, we are able to obtain maps $\overline{\varphi_i} : GLL(R) \to GLL(R_i)$ from the projection mappings $\varphi_i : R \to R_i$. Then we have the following commutative diagram:



where ψ is the unique homomorphism making the entire diagram commute. It is evident that ψ may be viewed as nothing more than the coordinate wise projections, and thus we conclude that this is an isomorphism. □

From the above argument, we see that since ring homomorphisms also preserve the multiplicative identity (where applicable), it follows that a similar result holds for the special linear loops. Alternatively, we note that the special linear loops are a closed subspace of the general linear loops.

Corollary 96. *If R is a profinite commutative ring with identity then $SLL(R)$ is profinite.*

Corollary 97. *Let p be a prime and let $\mathbb{Z}_{\boldsymbol{p}}$ denote the p-adic integers. Then $GLL(\mathbb{Z}_{\boldsymbol{p}})$ and $SLL(\mathbb{Z}_{\boldsymbol{p}})$ are profinite Moufang loops.*

3.2 Semidirect and Twisted-Semidirect Products

In this section, we shall see two variations of what is, in group theory, called a semidirect product. We can use both of these products to find Boolean loops.

First, let $(K, \cdot)$ be a loop, and choose H to be a subgroup of $\mathrm{Aut}(K)$, the group of automorphisms on K. Echoing a well known construction in group theory, we may define an operation $*$ on the set $H \times K$ by $(f, a) * (g, b) = (f \circ g, a \cdot f(b))$.

Proposition 98. *With the operation $*$ defined above, $(H \times K, *)$ is a loop.*

Proof. First, consider the equation $(f, a) * (\varphi, x) = (g, b)$. This is equivalent to $(f \circ \varphi, a \cdot f(x)) = (g, b)$. Thus, $f \circ \varphi = g$ and $a \cdot f(x) = b$. Then $\varphi = f^{-1} \circ g$ and $f(x) = a \backslash b$. Thus, the element $(\varphi, x) = (f^{-1} \circ g, f^{-1}(a \backslash b))$ is a unique solution to the above equation.

For equations of the form $(\phi, y) * (f, a) = (g, b)$, we see this is equivalent to $(\phi \circ f, y \cdot \phi(a)) = (g, b)$. Then $\phi \circ f = g$ and $y \cdot \phi(a) = b$. Thus, we have that $\phi = g \circ f^{-1}$ and $y = b / \phi(a) = b / (g \circ f^{-1}(a))$, and so we see this equation also has a unique solution. This shows that $(H \times K, *)$ is a quasigroup.

Finally, we see that for any $(f, a) \in H \times K$ it follows that $(1_H, 1_K) * (f, a) = (1_H \circ f, 1_K \cdot 1_H(a)) = (f, 1_K \cdot a) = (f, a)$ and that $(f, a) * (1_H, 1_K) = (f \circ 1_H, a \cdot f(1_K)) = (f, a \cdot 1_K) = (f, a)$. Thus, $(1_H, 1_K)$ is a 2-sided identity for $(H \times K, *)$. □

The above construction should be familiar to any observer well acquainted with group theory. If K is a group, the above construction is one means of obtaining a semidirect product of the groups H and K. In fact, we see that even when K is a loop, this construction has some familiar properties.

Proposition 99. *In the loop $(H \times K, *)$, there is a normal subloop which is isomorphic to K.*

Proof. Define a function $\varphi : (H \times K, *) \to (H, \circ)$ by $(h, k) \mapsto h$. We have that $\varphi((f, a) * (g, b)) = \varphi((f \circ g, a \cdot f(b))) = f \circ g = \varphi((f, a)) \circ \varphi((g, b))$, and so φ is a loop homomorphism. The kernel of φ is a normal subloop of $(H \times K, *)$, and this kernel is the set $\{(1_H, k) : k \in K\}$ which is clearly isomorphic to K. This completes the proof. □

As a result of Proposition 99, from this point on, we refer to $(H \times K, *)$ as $H \ltimes K$, a semidirect product of loops. A simple calculation shows that $H \ltimes K$ is a group if and only if K is a group.

Following [31], we discuss a similar product. Let G be group and H a subgroup of $\mathrm{Aut}(G)$. Define an operation $\star$ on $G \times H$ by $(h_1, g_1) \star (h_2, g_2) = (h_1 \circ h_2, h_2(g_1) \cdot g_2)$.

Proposition 100. *Under the operation $\star$ defined above, we have that $(H \times G, \star)$ is a loop.*

Proof. Consider an equation of the form $(f, a) \star (\varphi, x) = (g, b)$. This is equivalent to $(f \circ \varphi, \varphi(a) \cdot x) = (g, b)$. Then we have that $f \circ \varphi = g$ and $\varphi(a) \cdot x = b$. Thus $\varphi = f^{-1} \circ g$ and $x = \varphi(a) \backslash b = (f^{-1} \circ g(a)) \backslash b$. Each of these are seen to be unique, so the given expression has a unique solution in $H \times G$.

For an equation of the form $(\phi, y) \star (f, a) = (g, b)$ we find this to be equivalent to $(\phi \circ f, f(y) \cdot a) = (g, b)$. Then it follows that $\phi \circ f = g$ and $f(y) \cdot a = b$. Then $\phi = g \circ f^{-1}$ and $f(y) = b/a$. Taking $y = f^{-1}(b/a)$, we obtain unique solutions to these two equations, and thus $(H \times G, \star)$ is a quasigroup.

Finally, we see that $(1_H, 1_G)$ serves as a 2-sided identity in $(H \times G, \star)$ and so it is a loop. □

Proposition 101. *The loop $(H \times G, \star)$ contains a normal subloop which is isomorphic to G.*

Proof. Let $\varphi : (H \times G, \star) \to (H, \circ)$ be given by $(h, g) \mapsto h$. We have that

$$\begin{aligned} \varphi((f, a) \star (g, b)) &= \varphi((f \circ g, g(a) \cdot b)) \\ &= f \circ g \\ &= \varphi((f, a)) \circ \varphi((g, b)) \end{aligned}$$

and thus φ is a loop homomorphism. The kernel of φ is the set $\{(1_H, g) : g \in G\}$ which is clearly isomorphic to G. □

In light of the above Proposition, it is clear that $(H \times G, \star)$ is a variant of a semi-direct product. We shall denote this as $H \propto G$ and call it the *twisted semidirect product*.

Proposition 102. *The loop $H \propto G$ is a group if and only if H is an abelian subgroup of* $\mathrm{Aut}(G)$.

Proof. This follows from a lengthy but straightforward calculation. □

It should be noted that the two loop constructions above are purely algebraic. As we wish to discuss possible examples and constructions of profinite gadgets, we need to first discuss how these two constructions can be viewed as topological loops. The first concern is what sort of topology (if any) we can ascribe to an automorphism group of a loop (or group). For categorical reasons, we first limit our attention to only automorphisms which are continuous maps. When the context is clear, we shall use $\mathrm{Aut}(G)$ to mean the group of continuous automorphisms of the topological loop (or group) G. For more on viewing a set of continuous maps as a topological space, see [22], [8] and others.

Definition 103. Let G be a topological loop and $\mathrm{Aut}(G)$ the group of continuous automorphisms of G. Given a compact subset K of G and an open subset U of G, let $V(K, U)$ be the set of all elements $f \in \mathrm{Aut}(G)$ such that $f(K) \subset U$. Then the *compact open topology* on $\mathrm{Aut}(G)$ is the topology generated by the set of all such sets $V(K, U)$.

The following are well known results about the compact open topology. Proofs can be found is most elementary topology texts, such as [8].

Proposition 104. *If G is a locally compact Hausdorff space then* $\mathrm{Aut}(G)$ *is a Hausdorff topological group under the operation of function composition when equipped with the compact open topology.*

Proposition 105. *If G is locally compact and Hausdorff then the evaluation map $e : \mathrm{Aut}(G) \times G \to G$ given by $e(f, g) = f(g)$ is continuous. Furthermore, the compact open topology is the weakest topology on* $\mathrm{Aut}(G)$ *for which this is true.*

Proposition 106. *If K is a profinite loop,* $\mathrm{Aut}(K)$ *is a profinite group and H is a closed subgroup of* $\mathrm{Aut}(K)$*, then $H \ltimes K$ is a Boolean loop with respect to the product topology.*

Proof. Since $H \ltimes K$ is defined on the set $H \times K$, it will be a Boolean loop with respect to the product topology if both H and K are profinite. Since K and $\mathrm{Aut}(K)$ are profinite by assumption, and H is a closed subgroup of $\mathrm{Aut}(K)$, the required conditions are satisfied. □

Proposition 107. *If G and $\mathrm{Aut}(G)$ are profinite groups with H a closed subgroup of $\mathrm{Aut}(G)$, then $H \propto G$ is a Boolean loop.*

The two Propositions naturally give rise to the question of when exactly $\mathrm{Aut}(G)$ is profinite when G is a profinite group/loop. Unfortunately, $\mathrm{Aut}(G)$ may not be profinite, even when G is a profinite group, as can be seen from example 4.4.6 in [25]. While it is generally not known, Ribes and Zalesski give some conditions on a group G which insure that $\mathrm{Aut}(G)$ is profinite. Recall that $\mathcal{U}$ is a *fundamental system of open neighborhoods of x* if for every open neighborhood U of x there exists a $V \in \mathcal{U}$ such that $V \subset U$.

Proposition 108. *Suppose that G is a profinite group which admits a fundamental system $\mathcal{U}$ of open neighborhoods of 1_G such that $U \in \mathcal{U}$ is a characteristic subgroup of G, that is, a subgroup that is left invariant by each element of $\mathrm{Aut}(G)$. Then $\mathrm{Aut}(G)$ is profinite.*

Ribes and Zalesski also prove the following result, which, when used in tandem with Proposition 108, describes a significant class of profinite groups G for which $\mathrm{Aut}(G)$ is profinite.

Proposition 109. *Let G be a finitely generated profinite group. Then 1_G has a fundamental system of open neighborhoods consisting of a countable chain of characteristic subgroups*

$$G = V_0 \geq V_1 \geq V_2 \geq \cdots .$$

Thus, we see that for any finitely generated profinite group G, $\mathrm{Aut}(G)$ is also profinite. This can be of use when dealing with multiplication groups of loops. We shall see an example of this in chapter 4.

3.3 The Construction of T_{n+1}

Our immediate goal in this section is to describe the construction of an infinite family of commutative, non-associative loops. We shall use these loops in the next section to find a class of approachable profinite loops.

Recall that $\mathbb{Z}/n\mathbb{Z}$ denotes the cyclic group of order n, where the elements are considered to be equivalence classes $\mod n$ and the operation is addition. The following result is a standard exercise, yet we discuss it to highlight its importance for the task at hand.

Proposition 110. *If n is odd, the map $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $\varphi(x) = x + x$ is an isomorphism.*

Proof. We first note that

$$\begin{aligned} \varphi(x+y) &= (x+y)+(x+y) \\ &= (x+x)+(y+y) \\ &= \varphi(x)+\varphi(y) \end{aligned}$$

and thus we see that φ is a homomorphism. Now, if $x + x = y + y$ then it follows that $x - y = -(x - y)$, and since n is odd, it follows that $x - y = 0$. Thus φ is one-to-one. As $\mathbb{Z}/n\mathbb{Z}$ is finite, we find that φ is onto. □

Corollary 111. *Division by 2^m where $m \in \mathbb{N}$ is an automorphism of $\mathbb{Z}/n\mathbb{Z}$ for n odd.*

Proof. The Proposition above shows this is true for $m = 1$. The result then follows by composing automorphisms. □

We now construct a family of loops. For $\mathbb{Z}/n\mathbb{Z}$ with n odd we have that every element must occur on the main diagonal of its Cayley table, which in turn is a Latin square. We may use the bijection σ, given by $\sigma(x) = x/2$ on $\mathbb{Z}/n\mathbb{Z}$ to produce a new Latin square having the property that the $(i, i)th$ entry is the equivalence class of $i - 1 \mod n$. We shall use this Latin square of order n to construct one of order $n + 1$ which shares most of the entries.

The new Latin square can be constructed in such a way so as to insure that it is framed.

Let S be the Latin square of order n. Then construct a new square S' by taking the $(1,i)th$ entry to be the equivalence class of $i-2$ mod n for $2 \leq i \leq n+1$, the $(j,1)st$ entry to be the equivalence class of $j-2$ mod n with $2 \leq j \leq n+1$, the $(i,i)th$ entry to be a new element e, and the entry (i,j) not fitting any of the above descriptions will be the $(i-1,j-1)th$ entry of S. An example of this process is seen below for the case $n=3$.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\rightarrow$

0	2	1
2	1	0
1	0	2

$\rightarrow$

e	0	1	2
0	e	2	1
1	2	e	0
2	1	0	e

Finally, from S' we construct a loop in the standard way. That is, we take the first row to be the products $e \cdot e$, $e \cdot 0$, etc.; the second row to be the products $0 \cdot e$, $0 \cdot 0$, etc. and so on for each row. It is quickly seen that S' represents the multiplication table of a loop, which we shall call T_{n+1}.

For a more algebraic construction, let $T_{n+1} = \{e\} \cup \mathbb{Z}/n\mathbb{Z}$ as a set. We define an operation on this set as follows:

$$a \cdot b = \begin{cases} a & \text{if } b = e \\ b & \text{if } a = e \\ e & \text{if } a = b \\ a/2 + b/2 & \text{otherwise} \end{cases}.$$

This description of the product is seen to match the combinatorial construction above, and so can be taken as an equivalent definition of T_{n+1}.

Proposition 112. *T_{n+1} is a loop under the operation $\cdot$ described above.*

Proof. It is immediately clear that e serves as an identity, so we must only verify that T_{n+1} is a quasigroup. Consider the equation $a \cdot x = b$ for $a, b \in T_{n+1}$. If $b = e$ then clearly $x = a$ is the unique solution. If $b = a$ then $x = e$, otherwise we find that $x = b + b - a$. A similar argument shows that the equations $y \cdot a = b$ also have unique solutions for y. Thus the result holds. $\square$

Theorem 113. *Let H be a subgroup of $\mathbb{Z}/n\mathbb{Z}$, with n odd. Then $H \cup \{e\}$ is a subloop of T_{n+1}.*

Proof. Consider an equation of the form $a \cdot x = b$ with $a, b \in H \cup \{e\}$. If $a = e$, then clearly $x = b$ is the unique solution to this equation and lies in $H \cup \{e\}$. If $b = e$ then $x = a$ is the unique solution, and again a lies in $H \cup \{e\}$. Then assume neither a nor b is I. Then $x = 2b - a$, and as H is a subgroup, it follows that this value for x is also in H. Thus the equation $a \cdot x = b$ has a unique solution in $H \cup \{e\}$. A similar argument holds for equations of the form $y \cdot a = b$. Clearly e still serves as an identity element, and thus $H \cup \{e\}$ is a subloop of T_{n+1}. □

Theorem 114. *The only subloops of T_{n+1} are either trivial or of the form $(x + H) \cup \{e\}$ for some subgroup H of $\mathbb{Z}/n\mathbb{Z}$.*

Proof. First, let $H = \langle a \rangle$ be a subgroup of $\mathbb{Z}/n\mathbb{Z}$ and let $b \in \mathbb{Z}/n\mathbb{Z}$. Set $K = (b + H) \cup \{e\}$. If $c, d \in K$ consider the equation $c \cdot x = d$. If $c = e$ or if $d = e$ the unique solution for x is obvious. If neither of these is the case then $c \cdot x = \frac{c+x}{2}$ and thus $x = 2d - c$ is the unique solution in T_{n+1} to this equation. We have that $c = b + ma$ for some integer m and that $d = b + la$ for some integer l. Thus, $2d - c = b + (2l - m)a$ which is an element of $(b + H)$ and hence an element of K. A similar argument shows that equations of the form $y \cdot c = d$ have unique solutions in K. Finally, since $e \in K$ we get that K is a subloop.

For the converse, suppose that K is a nontrivial subloop of T_{n+1}. We claim that $K - \{e\} = a + H$ for some $a \in \mathbb{Z}/n\mathbb{Z}$ and some subgroup $H \leq \mathbb{Z}/n\mathbb{Z}$. Let $a \in K - \{e\}$ and set $H = \{k - a \mid k \in K - \{e\}\}$. We see immediately that H contains 0. If $h \in H$ then it follows that $h + a \in K - \{e\}$. Since n is odd, the equation $h = -h$ implies that $h = 0$, so assume $h \neq -h$. Then notice that $(h + a) \cdot (-h + a) = 2a/2 = 0 + a$ and thus we see that $-h \in H$ whenever $h \in H$, since K is a subloop. Lastly, we must show that H is closed under addition. If $g, h \in H$ we have that $g + a, h + a \in K - \{e\}$. Since $(g + a) \cdot (h + a) = \frac{g+h}{2} + a$ it follows that $\frac{g+h}{2} \in H$ for any $g, h \in H$. But as $0 \in H$, this implies that $g/2 \in H$ for any $g \in H$. That is, we have that H is its own image under the automorphism described in Proposition 110, and hence if $g \in H$ it follows that $2g \in H$. Finally, since $(2g + a) \cdot (2h + a) = (g + h) + a$,

we get that $g + h \in H$, and so H is a subloop of $\mathbb{Z}/n\mathbb{Z}$. The rest follows immediately. □

Corollary 115. *The loop T_{n+1} has a subloop of order $k+1$ if and only if k divides n.*

Proof. This follows from the fact that $\mathbb{Z}/n\mathbb{Z}$ has a subgroup of order k if and only if k divides n. From Theorem 114 we see that the only subloops that can exist must have order $k+1$ where k divides n, and that in fact multiple subloops exist for each such k. □

Thus we see that each proper subgroup H of $\mathbb{Z}/n\mathbb{Z}$ in fact gives rise to $[\mathbb{Z}/n\mathbb{Z} : H]$ subloops of T_{n+1}. One important question is whether or not any (or all?) of these subloops are normal in T_{n+1}. In some cases we can answer with a definitive 'not' simply based on divisibility considerations. For example, the subgroup $H = \langle 3 \rangle$ of $\mathbb{Z}/9\mathbb{Z}$ has the property that $|H| = 3$, but $|H| + 1$ does not divide $9 + 1 = 10$. Thus any of the $[\mathbb{Z}/9\mathbb{Z} : H]$ subloops we obtain in T_{10} do not satisfy the Lagrange property, and hence cannot be normal. This kind of argument cannot always be used however. For example, the trivial subgroup of $\mathbb{Z}/n\mathbb{Z}$ is associated with n different subloops of order 2, and 2 certainly divides $n+1$ for every odd n.

Proposition 116. *For elements $a, b \in T_{n+1}$ the relation $a \cdot (a \cdot b) = b$ holds if and only if either $a = e$, $b = e$, $a = b$ or $3a = 3b \mod n$. Further more, $a \cdot (a \cdot x) = a \cdot (a \cdot y)$ if and only if $x = y$.*

Proof. The first statement follows from tedious case work. In general, we have that

$$a \cdot (a \cdot b) = \begin{cases} b & \text{if } a = b \text{ or } a = e \text{ or } b = e \text{ or } 3a = 3b \\ \frac{3a+b}{4} & \text{otherwise} \end{cases}$$

For the second, note that the claimed equality is equivalent to saying that $\lambda_a(\lambda_a(x)) = \lambda_a(\lambda_a(y))$. But this is true if and only if $x = y$, since λ_a is a bijection for any $a \in T_{n+1}$. □

Corollary 117. *If $n > 3$ then any nontrivial cyclic subloop K of T_{n+1} is not normal.*

Proof. Let K be a cyclic subloop. Then $K = \langle a \rangle = \{e, a\}$ for some $a \in T_{n+1}$ with $a \neq e$. Then $x \cdot (x \cdot H) = (x \cdot x) \cdot H = H$ if and only if $x \cdot (x \cdot a) = a$. This can happen if and only if either $a = x$, $x = e$ or $3a = 3x$. If $n > 3$ then there exists some $x \in \mathbb{Z}/n\mathbb{Z}$ such that $a \neq x$ and $3a \neq 3x$. Thus K can not be normal. □

Notice that if $n = 3$, we find that subloops of order 2 in T_4 are normal. This is a consequence of the fact that multiplication by 3 annihilates all of $\mathbb{Z}/n\mathbb{Z}$. Additionally, we see that $T_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

A well known result for groups is that any subgroup of index 2 is automatically normal. In fact, the same is true of loops. Thus, if T_{n+1} should ever have a subloop of order $\frac{n+1}{2}$, its normality would be assured. However, this generally can't happen.

Proposition 118. *If $n > 3$ then T_{n+1} has no subloops of index 2.*

Proof. If such a subloop did exist, it would have order $\frac{n+1}{2}$ and thus would imply the existence of a subgroup of order $\frac{n-1}{2}$ in $\mathbb{Z}/n\mathbb{Z}$. However, since $2\left(\frac{n-1}{2}\right) + 1 = n$, we see that this can only happen when $n = 1$ or $n = 3$. □

Theorem 119. *Let K be a subloop of T_{n+1}. Then for any $a \in T_{n+1}$ the map $\theta_a : K \to a(aK)$ given by $x \mapsto a \cdot (a \cdot x)$ is a bijection which preserves multiplication.*

Proof. From Proposition 116 we see that θ_a is injective for any $a \in T_{n+1}$. Thus, by finiteness θ_a is a bijection. It remain to show, then, that θ_a preserves multiplication. By direct calculations we find that

$$\theta_a(x \cdot y) = a \cdot (a \cdot (x \cdot y)) = \begin{cases} x \cdot y & \text{if } a = e \text{ or } a = (x \cdot y) \\ e & \text{if } x = y \\ \frac{3a + (x \cdot y)}{4} & \text{otherwise} \end{cases}.$$

Similarly, we find that

$$\theta_a(x)\cdot\theta_a(y)=\begin{cases} x\cdot y & \text{if } a=e \\ e & \text{if } x=y \\ x\cdot(x\cdot(x\cdot y)) & \text{if } a=x \\ y\cdot(y\cdot(y\cdot x)) & \text{if } a=y \\ \frac{6a+x+y}{8} & \text{otherwise} \end{cases}$$

By examining the different possibilities, we see that in each possible instance, $\theta_a(x\cdot y)=\theta_a(x)\cdot\theta_a(y)$. Thus the statement in proven. □

In fact, something stronger is true. The map given above is actually a loop homomorphism. To verify this, we need only show that $a\cdot(aK)$ is a subloop.

Proposition 120. *If K is a nontrivial subloop of T_{n+1} then so is $a\cdot(aK)$ for any $a\in T_{n+1}$.*

Proof. Consider an equation of the form $[a\cdot(a\cdot k_1)]\cdot x=[a\cdot(a\cdot k_2)]$ where $k_1,k_2\in K$. Since K is a subloop, there is a unique element y in K for which $k_1\cdot y=k_2$. But this implies that $a\cdot(a\cdot(k_1\cdot y))=a\cdot(a\cdot k_2)$. By the previous Theorem, we see that this is equivalent to $[a\cdot(a\cdot k_1)]\cdot[a\cdot(a\cdot y)]=a\cdot(a\cdot k_2)$ and so the given equation has a unique solution in $a(aK)$. The other equation form follows by similar argument, and thus $a(aK)$ is a quasigroup. Since $a\cdot(a\cdot e)=e$, it follows that $a(aK)$ is in fact a loop. □

The subloop described in the previous two results is of some significance. Given that we know the exact structure of any subloop K in T_{n+1}, it is natural to ask whether or not we can describe $a(aK)$ using knowledge of K. We have the following result.

Theorem 121. *Assume that $K_x=(x+H)\cup\{e\}$ is a subloop of T_{n+1} and that $|K_x|$ divides $n+1$. Then for any $a\in T_{n+1}$ we have that $a(aK_x)=K_{a\cdot(a\cdot x)}=((a\cdot(a\cdot x)+H)\cup\{e\}$.*

Proof. Since $|K_x|$ divides $n+1$, it follows that $n/(|K_x|-1)$ is an integer, say m. Thus, we have that $K_x = \{e, x, x+m, x+2m, \cdots\}$ and so $aK_x = \{a, a\cdot x, a\cdot(x+m), \cdots\}$ and thus $a(aK_x) = \{e, a\cdot(a\cdot x), \cdots\}$. By the previous proposition, we have that $a(aK_x)$ is a subloop, and since θ_a is a bijection, it must be a coset of H together with e. Since it clearly contains $a\cdot(a\cdot x)$, the result follows. □

Corollary 122. *For $n > 3$ we have that T_{n+1} is a simple loop.*

Proof. Suppose to the contrary that $K_x = (x+H)\cup\{e\}$ is a normal subloop of T_{n+1}. Then $|K_x|$ divides $n+1$ since normal subloops are lagrange-like. Since there exists at least one $a \in T_{n+1}$ for which $a\cdot(a\cdot x) \neq x$, we have that

$$a(aK_x) = K_{a\cdot(a\cdot x)} \neq (a\cdot a)K_x = K_x$$

and thus we have a contradiction. □

The loop T_{n+1} would seem to not be of any family of loop previously studied. For example, it is neither a Bol loop, nor a Moufang loop. It can also be shown that it is not an automorphic loop. Yet, as we see from Corollary 115, it does satisfy a Sylow like Theorem regarding the existence of certain subloops despite the fact that Lagrange's Theorem need not hold. In the next section, we shall use T_{n+1} to build an Ind-finite loop and the use categorical duality to construct a profinite loop.

3.4 A Pro-finite Loop built from an Ind-finite Loop

In this section, we shall see that T_{n+1} may be used to construct profinite loops which are loops of homomorphisms. We shall accomplish this by constructing an ind-finite loop and using categorical duality.

Proposition 123. *Let p be an odd prime and let $i, j \in \mathbb{N}$ with $i \leq j$. Define a map $f_{ij} : T_{p^i+1} \to T_{p^j+1}$ by*

$$f_{ij}(x) = \begin{cases} e & \text{if } x = e \\ p^{j-i}x & \text{otherwise} \end{cases}.$$

Then f_{ij} is a loop homomorphism for any $i \leq j$.

Proof. First, note that if $x = y$ we have $f_{ij}(x \cdot y) = f_{ij}(e) = f_{ij}(x) \cdot f_{ij}(x)$. If $x = e$ then $f_{ij}(x \cdot y) = f_{ij}(y) = f_{ij}(e) \cdot f_{ij}(y)$. The case of $y = e$ is similar. Otherwise, we have that

$$\begin{aligned} f_{ij}(x \cdot y) &= f_{ij}\left(\frac{x+y}{2}\right) \\ &= p^{j-i}\left(\frac{x+y}{2}\right) \\ &= \frac{p^{j-i}x + p^{j-i}y}{2} \\ &= \frac{f_{ij}(x) + f_{ij}(y)}{2} \\ &= f_{ij}(x) \cdot f_{ij}(y) \end{aligned}$$

where the last equation follows from the fact that f_{ij} is injective and that $f_{ij}(x) = e$ only if $x = e$. This completes the proof. □

For the above collection of loop homomorphisms, we have that f_{ii} is the identity on T_{p^i+1} for each i and that if $i \leq j \leq k$ then $f_{jk} \circ f_{ij} = f_{ik}$. Thus, (T_{p^i+1}, f_{ij}) is a direct system of commutative loops. We shall denote the direct limit of this system by $T_{p^\infty+1}$. It should also be noted that this loop is similar in construction to the *Prüfer Group* $\mathbb{Z}(p^\infty)$ (see [17]) and likely shares some of the same properties.

Recall that in general $\mathrm{Hom}(X, Y)$ denotes the set of maps from an object X to an object Y in some category. If X and Y are loops, we may use $\mathrm{Hom}(X, Y)$ to describe the set of loop homomorphisms between X and Y. However, this may or may not have the structure of a loop. If we consider $\mathrm{Hom}(X, Y)$ to be simply the set of all set maps from X to Y, however, it is possible to show that $\mathrm{Hom}(X, Y)$ has the structure of a loop. To do this, we define an operation $*$ by $f * g(x) = f(x) \cdot g(x)$ where f, g are set maps from X to Y and $\cdot$ is the loop operation on Y. With this operation, we may define a map $(f/g) : X \to Y$ by $(f/g)(x) = f(x)/g(x)$ and similarly for $f\backslash g$. The identity element of $\mathrm{Hom}(X, Y)$ then is just the map $e : X \to Y$ which maps every element of X to the identity element of Y.

Proposition 124. *Let Y be a finite topological loop. Then $\mathrm{Hom}(T_{p^i+1}, Y)$ is a finite loop and so $\mathrm{Hom}(\mathbb{Z}_{p^\infty+1}, Y)$ is a profinite loop.*

Proof. This follows immediately from Proposition 37, since the set $\mathrm{Hom}(T_{p^i+1}, Y)$ is finite whenever Y is a finite loop. $\square$

3.5 Some Profinite Bol Loops

In [27], Solarin and Sharma used non-abelian and cyclic groups to construct loops of order $2n^2$ and $4n$ which satisfy a certain associativity-like condition. A loop $(L, \cdot)$ is called a *(right) Bol loop* if

$$((x \cdot y) \cdot z) \cdot y = x \cdot ((y \cdot z) \cdot y)$$

for all $x, y, z \in L$.

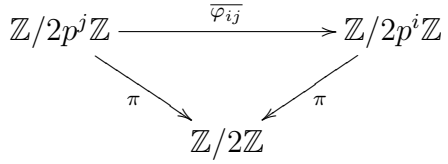
Let n be an integer greater than 2. Following [27], we define a product $*$ on the set $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ by

$$(a,b) * (c,d) = \begin{cases} (a+c, b+d) & \text{if } b \equiv 0 \mod 2 \\ (a-c, b+d-2c) & \text{if } b \equiv 1 \mod 2 \text{ and } d \equiv 0 \mod 2 \\ (a-c, b+d+2c) & \text{if } b \equiv 1 \mod 2 \text{ and } d \equiv 1 \mod 2 \end{cases}.$$

Then $(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, *)$ is a (right) Bol loop of order $2n^2$. To avoid confusion with the group $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, we shall denote this loop by $\mathbb{Z}/n\mathbb{Z} \boxtimes \mathbb{Z}/2n\mathbb{Z}$. Solarin and Sharma went further and showed that although this loop is a (right) Bol Loop, it is not a Moufang loop.

Proposition 125. *Let p be an odd prime. For $i, j \in \mathbb{N}$ with $i \leq j$, define a map $\varphi_{ij} : \mathbb{Z}/p^j\mathbb{Z} \boxtimes \mathbb{Z}/2p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z} \boxtimes \mathbb{Z}/2p^i\mathbb{Z}$ given by $(a + p^j\mathbb{Z}, b + 2p^j\mathbb{Z}) \mapsto (a + p^i\mathbb{Z}, b + 2p^i\mathbb{Z})$. Then φ_{ij} is a loop homomorphism.*

Proof. First, notice that since p is odd, it follows that φ_{ij} preserves equivalence mod 2 in the second coordinate. That is, the following diagram is commutative:



where $\overline{\varphi_{ij}}$ denotes the restriction of φ_{ij} to the second coordinate and π denotes reduction mod 2. Then, if $b \equiv 0 \mod 2$ we have that

$$\begin{aligned}
& \varphi_{ij}((a + p^j\mathbb{Z}, b + 2p^j\mathbb{Z})) * \varphi_{ij}((c + p^j\mathbb{Z}, d + 2p^j\mathbb{Z})) \\
= \; & (a + p^i\mathbb{Z}, b + 2p^i\mathbb{Z}) * (c + p^i\mathbb{Z}, d + 2p^i\mathbb{Z}) \\
= \; & (a + c + p^i\mathbb{Z}, b + d + 2p^i\mathbb{Z}) \\
= \; & \varphi_{ij}((a + c + p^j\mathbb{Z}, b + d + 2p^j\mathbb{Z}) \\
= \; & \varphi_{ij}((a + p^j\mathbb{Z}, b + 2p^j\mathbb{Z}) * (c + p^j\mathbb{Z}, d + 2p^j\mathbb{Z})).
\end{aligned}$$

The other cases are similar, so we conclude that φ_{ij} is a homomorphism of loops for $i \leq j$. □

Using the collection of homomorphisms described above, we may form an inverse system $(\mathbb{Z}/p^i\mathbb{Z} \boxtimes \mathbb{Z}/2p^i\mathbb{Z}, \varphi_{ij})$ indexed by the natural numbers, as φ_{ii} is the identity function and $\varphi_{ik} = \varphi_{ij} \circ \varphi_{jk}$ whenever $i \leq j \leq k$. We shall denote the inverse limit of this system by $\mathbb{Z}_{\mathbf{p}} \boxtimes \mathbb{Z}_{\mathbf{2p}}$. This is a profinite loop which properly contains a subgroup which is isomorphic to the p-adic integers.

Chapter 4

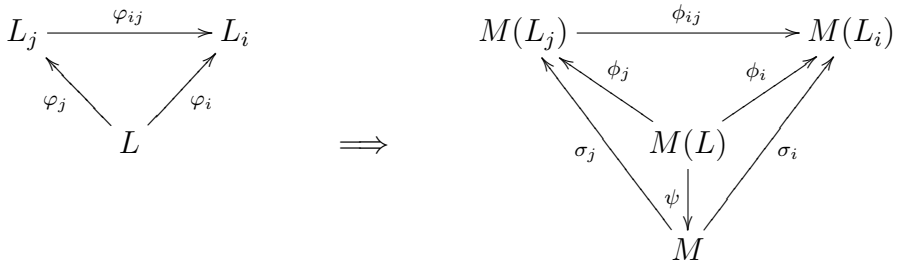
Profinite Loops and Related Groups

4.1 Multiplication Groups of Profinite Loops

In this section, we shall see that if G is a profinite loop, it is closely associated with several profinite groups. While profinite groups have been reasonably well studied in the recent years, much is still unknown about multiplication groups, such as even the basic question of which groups are multiplication groups of loops.

Theorem 126. *If L is a profinite loop, then the multiplication group of L, $M(L)$ is a profinite group.*

Proof. Let $L = \varprojlim (L_i, \varphi_{ij})$ where L_i is a finite loop for each i, and $\varphi_{ij} : L_j \to L_i$ is a loop homomorphism. Without loss of generality, we may assume that this system is an onto system. Applying the Bruck functor, F, to this system yields an inverse system $(F(L_i), F(\varphi_{ij}))$ of groups and surjective group homomorphisms, where $F(L_i) = M(L_i)$. Let $F(\varphi_{ij}) = \phi_{ij}$. We note that the finiteness of L_i implies the finiteness of $M(L_i)$, and so this is an inverse system of finite topological groups. Let $M = \varprojlim (M(L_i), \phi_{ij})$. By applying the functor to L, and the limiting maps $\varphi_i : L \to L_i$, we obtain a compatible family of surjective maps $\{\phi_i : M(L) \to M(L_i)\}$, and as M is an inverse limit, we thus obtain a unique surjective group homomorphism $\psi : M(L) \to M$ such that $\sigma_i \circ \psi = \phi_i$, where $\sigma_i : M \to M(L_i)$ is the ith projection map.



Now, if $\widehat{\pi}_i$ represents the projection from $\prod M(L_i)$ to $M(L_i)$, then without loss of generality we have that

$$M = \{f \in \prod M(L_i) \mid \phi_{ij} \circ \widehat{\pi}_j(f) = \widehat{\pi}_i(f) \forall\ i, j \text{ with } i \leq j\}$$

and that

$$L = \{p \in \prod L_i \mid \varphi_{ij} \circ \pi_j(p) = \pi_i(p) \forall\ i, j \text{ with } i \leq j\}.$$

We shall show that in fact, $M(L)$ is contained in M. Let $p \in L$. Then $p = (p_i)_{i \in I}$ where $p_i \in L_i$ for each $i \in I$. Then if λ_p is left multiplication of L, we get that $\lambda_p = \prod_{i \in I} \lambda_{p_i}$ as the multiplication is performed coordinate-wise. Thus $\lambda_p \in \prod M(L_i)$, since λ_{p_i} is an element of $M(L_i)$ for each $i \in I$. As $p \in L$ we have that $\varphi_{ij}\pi_j(p) = \pi_i(p)$, which is equivalent to saying that $\varphi_{ij}(p_j) = p_i$. From this it follows that $\lambda_{\varphi_{ij}(p_j)} = \lambda_{p_i}$ which is equivalent to saying that $\phi_{ij}(\lambda_{p_j}) = \lambda_{p_i}$. Thus we see that $\lambda_p \in M$. Similar arguments show the same for λ_p^{-1}, ρ_p and ρ_p^{-1}. Then, as M is a group, we get that $M(L)$ is contained in M, since M contains the generators of $M(L)$.

Finally, we have that $\phi_i = \sigma_i \circ \psi$ for all $i \in I$. For any element $f \in M(L)$ there is a finite r such that $f = f_{x_1} \circ \cdots \circ f_{x_r}$ where each $x_n \in L$ and f_{x_i} is one of $\lambda_{x_i}^{\pm 1}$ or $\rho_{x_i}^{\pm 1}$ for each $i \in I$. As $\phi_i = F(\varphi_i)$, it follows that $\phi_i(f) = f_{\varphi_i(x_1)} \circ \cdots \circ f_{\varphi_i(x_r)}$. But as each $x_n \in L$, we have that $x_n = (p_{i,n})_{i \in I}$ for each n with $1 \leq n \leq r$. Thus, it follows that $\phi_i(f) = f_{p_{i,1}} \circ \cdots \circ f_{p_{i,r}} = \sigma_i \circ \psi(f)$. But since σ_i is the restriction of $\widehat{\pi}_i$ to M, it follows that $\psi(f) = (f_{p_{i,1}} \circ \cdots \circ f_{p_{i,r}})_{i \in I}$. Thus, if $\psi(f) = \psi(g)$ for elements $f, g \in M(L)$ then $f_{p_{i,1}} \circ \cdots \circ f_{p_{i,r}} = g_{q_{i,1}} \circ \cdots \circ g_{q_{i,s}}$ for each $i \in I$. But this says that f and g are the same on each coordinate of L, and thus $f = g$. Thus ψ is a bijection, and thus $M(L)$ is profinite. $\square$

A similar argument shows that

Theorem 127. *Let L be a profinite loop. Then $M_\rho(L)$ and $M_\lambda(L)$ are profinite groups.*

Definition 128. Let G be a profinite group and X a topological space. We say X is a *G-space* if there exists a continuous map $G \times X \to X$, denoted $(g, x) \mapsto g \cdot x$ such that $(gh) \cdot x = g \cdot (h \cdot x)$ and $1 \cdot x = x$ for all $g, h \in G$ and for all $x \in X$.

Proposition 129. *If G is a profinite loop and $M(G)$ is its multiplication group, then G is an $M(G)$-space.*

Proof. Define a map $e : M(G) \times G \to G$ by $e(\alpha, g) = \alpha(x)$. Then we have that $(\alpha \circ \beta)(g) = \alpha(\beta(g))$ and that $1_{M(G)}(g) = g$ for all $\alpha, \beta \in M(G)$ and all $g \in G$. It remains to show that e is continuous. As G is profinite, we have that G is topologically isomorphic to a closed subspace of the product space $\prod_{i \in I} G_i$ where G_i is a finite group for each i in the directed set I. Similarly, $M(G)$ is isomorphic to a closed subspace of $\prod M(G_i)$. The map e is a restriction of the map

$$\overline{e} : \prod M(G_i) \times \prod G_i \to \prod G_i$$

and we have that $\prod M(G_i) \times \prod G_i$ is isomorphic to $\prod (M(G_i) \times G_i)$ as topological groups. We have the following commutative diagram:

$$\begin{array}{ccc} \prod (M(G_i) \times G_i) & \xrightarrow{\overline{e}} & \prod G_i \\ \downarrow{\scriptstyle \pi_i} & & \downarrow{\scriptstyle \pi_i'} \\ M(G_i) \times G_i & \xrightarrow[e_i]{} & G_i \end{array}$$

where $e_i : M(G_i) \times G_i$ is function composition for each i and π_i, π_i' are projections to the ith coordinate. Since the spaces in the top row of the above diagram are imbued with the product topology, it follows that the vertical maps are continuous. The space $M(G_i)$ is a topological group under the compact open topology, and thus the map e_i is continuous for each i as well. It then follows that $\overline{e}$ is continuous, and thus its restriction, e, to a subspace is also continuous. This completes the proof. □

Proposition 130. *If G is a profinite loop and U is an open subset of $M(G)$ with respect to the compact open topology, then U is open in $M(G)$ with respect to the profinite topology.*

Proof. This follows from the fact that function evaluation is continuous with respect to the profinite topology on $M(G)$, since the compact open topology is the weakest topology with this property. Hence the open subsets with respect to the compact open topology are open with respect to the profinite topology. □

Corollary 131. *Let G be a profinite loop and H a subset of G which is both open and closed. Then the set $\{\alpha \in M(G) \mid \alpha(H) \subset H\}$ is open in $M(G)$, as is the subgroup it generates, which we shall denote $N_{M(G)}(H)$.*

Proof. Since H is closed and G is profinite, it follows that H is compact. Thus the given set is a subbasic set with respect to the compact open topology (it is in fact one of the generators of said topology) and thus is open. Since this open set is contained in the subgroup $N_{M(G)}(H)$, it follows that this group is open in $M(G)$. □

Theorem 132. *Let G be a profinite group and let X be a Hausdorff G-space. Then for $x \in X$, the G-stabilizer $G_x = \{g \in G \mid g \cdot x = x\}$ of x is a closed subgroup of G.*

Proof. Since G is compact and the action of function evaluation is continuous, this result follows from Proposition 13. □

Corollary 133. *Let G be a profinite loop. Then the group of inner mappings of G, $I(G)$, is also profinite.*

Proof. We have that $M(G)$ acts continuously on G, making G a $M(G)$-space. Then, by the Theorem, the $M(G)$-stabilizer of the identity element e of G is closed in G. The $M(G)$-stabilizer of e is the set of all elements of $M(G)$ which fix e, and thus is the inner mapping group $I(G)$. Since G is profinite and $I(G)$ is closed in $M(G)$, it follows that $I(G)$ is profinite. □

We now return to the question of when $\mathrm{Aut}(G)$ is profinite for a given profinite loop G. Although this remains an open question, we may offer some insight into the case of commutative Moufang loops.

Theorem 134. *If G is a commutative Moufang loop which is finitely generated then $M(G)$ is finitely generated.*

Proof. This is a special case of Theorem 2 in [3]. □

Corollary 135. *If G is a profinite, finitely generated commutative Moufang loop then $\mathrm{Aut}(M(G))$ is a profinite group.*

Proof. Since $M(G)$ is profinite and finitely generated, this follows from Proposition 108 and Proposition 109. □

We combine the above result with a basic result found in [23].

Theorem 136. *Let Q be a quasigroup. Then $\mathrm{Aut}(Q)$ is isomorphic to a subgroup of $\mathrm{Aut}(M(G))$.*

We therefore have that if G is a finitely generated, profinite commutative Moufang loop then $\mathrm{Aut}(G)$ is naturally isomorphic to a subgroup A of $\mathrm{Aut}(M(G))$ which is profinite. Thus, if A is closed, we have that $\mathrm{Aut}(G)$ is profinite.

4.2 Sharply Transitive Sections and Profinite Groups

In this section, we shall explore the types of loops that can be constructed from profinite groups via continuous sharply transitive sections. First, however, we must establish certain basic facts about topological quotients.

Let X be a topological space and $\sim$ an equivalence relation on X. We shall denote the set of equivalence classes of $\sim$ by $X/\sim$. There is a natural topology on $X/\sim$ known as the *quotient topology* where a set of equivalence classes is open if and only if the union of those classes is open in X. The quotient topology is the finest topology that makes the projection map π :

$X \to X/\sim$ given by $x \mapsto [x]$ continuous. The next three results are standard, but we include them for the benefit of the reader. For more details, see [8], [22], and others.

Proposition 137. *If X is a compact topological space and $X/\sim$ is a quotient of X then $X/\sim$ is compact with respect to the quotient topology.*

Proof. Suppose $\{O_i\}$ is an open cover of $X/\sim$. Then $\{\pi^{-1}(O_i)\}$ is an open cover of X. As X is compact, this open cover has a finite subcover, say $\{\pi^{-1}(O_i)\}_{i=1}^n$, relabeling the indices as needed. Then $\{O_i\}_{i=1}^n$ is a finite subcover of $X/\sim$ and so we find that $X/\sim$ is compact. □

Recall that a space X is said to satisfy axiom T_1 if for $x, y \in X$ there are open sets A and B with $x \in A$, $y \in B$ and also with $x \notin B$ and $y \notin A$. It is immediate that any space satisfying axiom T_1 also satisfies axiom T_0.

Proposition 138. *A quotient space $X/\sim$ is a T_1 space if and only if every equivalence class of $\sim$ is closed.*

Proof. Let $[x], [y] \in X/\sim$ and assume all equivalence classes of $\sim$ are closed in X. Since the sets $\{[x]\}$ and $\{[y]\}$ are closed in $X/\sim$, it follows that $A = X/\sim - \{[x]\}$ and $B = X/\sim - \{[y]\}$ are open in $X/\sim$. Furthermore, A contains $[y]$ but not $[x]$ and B contains $[x]$ but not $[y]$. Thus $X/\sim$ satisfies T_1.

On the other hand, if $X/\sim$ satisfies axiom T_1 then for a fixed point $[x] \in X/\sim$ and any other point $[y] \neq [x]$ there is an open set $A_{[y]}$ which contains $[y]$ but not $[x]$. But then we have that the set

$$\bigcup_{[y]\neq[x]} A_{[y]}$$

is an open set which contains every point of $X/\sim$ but $[x]$. Thus, its complement $\{[x]\}$ is closed. Since $[x]$ is arbitrary, we have that any equivalence class of $\sim$ is closed. □

Proposition 139. *Let X be a compact, totally disconnected space. Then any quotient of X obtained by identifying a closed subset of X to a point is totally disconnected.*

Next, we obtain a partial converse of Theorem 126.

Theorem 140. *Let G be a profinite group, H a closed subgroup of G and $\sigma : G/H \to G$ a continuous sharply transitive section. Then G/H is a profinite loop under the operation $xH * yH = \sigma(xH)yH$.*

Proof. Suppose $G = \varprojlim (G_i, \varphi_{ij})$ where G_i is a finite group for each i. Since H is closed and G is profinite, we have that $H = \varprojlim \phi_i(H)$ where $\phi_i : G \to G_i$ is the ith projection map. Let $H_i = \phi_i(H)$, so that H_i is a subgroup of G_i for each i. For each i, define a map $\sigma_i : G_i/H_i \to G_i$ by $\sigma_i(g_iH_i) = x_i$ where $\sigma((g_i)_{i\in I}H) = (x_i)_{i\in I}$. That is, σ is the Cartesian product of the maps σ_i. It follows that σ_i is a sharply transitive section for each $i \in I$, and so G_i/H_i is a finite loop for each i.

For each pair i, j with $i \leq j$, define $\overline{\varphi_{ij}} : G_j/H_j \to G_i/H_i$ by $\overline{\varphi_{ij}}(g_jH_j) = \varphi_{ij}(g_j)H_i = g_iH_i$. We first check that this map is well defined. Suppose that $a_jH_j = b_jH_j$. Then $a_j^{-1}b_j \in H_j$. Thus, $\varphi_{ij}(a_j^{-1}b_j) = a_i^{-1}b_i$ and since $\varphi_{ij}(H_j) \subset H_i$ this is an element of H_i. Thus $a_iH_i = b_iH_i$, and so $\overline{\varphi_{ij}}$ is well defined. Next, notice that for $i \leq j$ we have

$$\begin{aligned}
\varphi_{ij} \circ \sigma_j(g_jH_j) &= \varphi_{ij}(x_j) \\
&= x_i \\
&= \sigma_i(g_iH_i) \\
&= \sigma_i \circ \overline{\varphi_{ij}}(g_jH_j)
\end{aligned}$$

Thus, $\varphi_{ij}\sigma_j = \sigma_i \circ \overline{\varphi_{ij}}$ whenever $i \leq j$. Then, we have that

$$\begin{aligned}
\overline{\varphi_{ij}}(a_jH_j * b_jH_j) &= \overline{\varphi_{ij}}(\sigma_j(a_jH_j)b_jH_j) \\
&= \varphi_{ij}(\sigma_j(a_jH_j)b_j)H_i \\
&= \varphi_{ij}(\sigma_j(a_jH_j))\varphi_{ij}(b_j)H_i \\
&= \sigma_i \circ \overline{\varphi_{ij}}(a_jH_j)y_iH_i \\
&= \sigma_i(a_iH_i)y_iH_i \\
&= \overline{\varphi_{ij}}(a_jH_j) * \overline{\varphi_{ij}}(b_jH_j)
\end{aligned}$$

and thus we have that $\overline{\varphi_{ij}}$ is a loop homomorphism for each $i \leq j$. It is easily checked that $(G_i/H_i, \overline{\varphi_{ij}})$ is an inverse system of finite loops and loop homomorphisms.

Let $\psi_i : G/H \to G_i/H_i$ be the map given by $\psi_i(gH) = g_iH_i$ where $g = (g_i)_{i\in I}$ and hence $gH = \{(g_ih_i)_{i\in I} \mid (h_i) \in H\}$. We check this map is well defined. If $aH = bH$ then $\{(a_ih_i) \mid (h_i) \in H\} = \{(b_ik_i) \mid (k_i) \in H\}$ and thus, for each i, we have that $a_i \in b_iH_i$. Thus $\psi_i(aH) = \psi_i(bH)$ and so these maps are well defined. We also see that these maps are compatible with the inverse system given above. Thus, we induce a unique map $\psi : G/H \to \varprojlim G_i/H_i$ which makes the entire collection of maps commute. Since ψ must effectively split a coset into its coordinate-wise components, we see that ψ is in fact a bijection, and thus we have that $\varprojlim G_i/H_i \cong G/H$ as loops. Since G_i is finite for each i, we have shown that G/H is a profinite loop and the proof is complete. □

Corollary 141. *If G is a loop for which $M_\lambda(G)$, its left multiplication group, is profinite, then G is profinite.*

Proof. The loop G is isomorphic (see [20]) to the loop formed on the set $M_\lambda(G)/H$ where H is the left inner mapping group of G using the sharply transitive section σ given by $x \mapsto \lambda_x$. □

When dealing with isotopes of topological loops, we have that the three isotopy maps are continuous bijections. Thus, if either of the two loop isotopes are Hausdorff spaces, it follows that these maps are homeomorphisms. We therefore have that:

Proposition 142. *Let G be a Boolean topological loop and H a topological loop which is an isotope of G. Then H is a Boolean loop.*

Furthermore, if it is indeed the case that Boolean loops are profinite, as Conjecture 86 suggests, this would insure that all loop isotopes of a profinite loop are profinite.

Proposition 143. *Let G be a Boolean topological loop. Then its multiplication group $M(G)$ is a totally disconnected Hausdorff group.*

Proof. That $M(G)$ is Hausdorff has been previously established. Since G is totally disconnected, it follows that for any pair of distinct points $x, y \in G$ there is a separation $G = A \cup B$ with A and B open and disjoint, and $x \in A$, $y \in B$. Let $\alpha, \beta \in M(G)$ with $\alpha \neq \beta$. Then there exists some $x \in G$ with $\alpha(x) \neq \beta(x)$. Thus there are disjoint open sets A_α, B_β with $\alpha(x) \in A_\alpha$, $\beta(x) \in B_\beta$ and $A_\alpha \cup B_\beta = G$. Then the subbasic sets $V(\{x\}, A_\alpha) = \{f \in M(G) : f(x) \in A_\alpha\}$ and $V(\{x\}, B_\beta) = \{f \in M(G) : f(x) \in B_\beta\}$ are disjoint open sets in $M(G)$. Furthermore, it is evident that $V(\{x\}, A_\alpha) \cup V(\{x\}, B_\beta) = M(G)$ and thus we have a separation of $M(G)$ as desired. Thus $M(G)$ is totally disconnected. □

In light of the above results, we see that Conjecture 86 can be established by showing that if G is a Boolean loop then $M(G)$ is compact. Equivalently, it would be enough to show that either $M_\lambda(G)$ or $M_\rho(G)$ is compact as well. Unfortunately, there are very few known conditions about when a space of homeomorphisms is compact under the compact open topology. This would seem to be a vital component for proving Conjecture 86, and will be an area of future research.

4.3 Profinite Moufang Loops

One of the major topics of study in loop theory is the question of when a loop satisfies certain well known group theoretic results, such as Lagrange's Theorem and the Sylow Theorems. In this section we shall see that for a special family of loops, we may extend these results from finite loops to profinite loops in a natural way.

Given that the cardinality of a profinite loop is either finite or uncountable, when G is an infinite profinite loop, knowledge about its cardinality is somewhat unhelpful. However, there is a useful generalization of the natural numbers which can be used to describe various algebraic properties of G. This idea has been used to study profinite groups (see [30], [25]), and we find that in some cases it may be applied to our setting as well.

Definition 144. A *supernatural number* is a formal product

$$n = \prod_p p^{n(p)}$$

where p runs through the set of all prime numbers, and $n(p)$ is a nonnegative integer or ∞ for each prime p.

By convention, we say $n < \infty$, and that $\infty + \infty = \infty + n = n + \infty = \infty$ for all $n \in \mathbb{N}$. If

$$n = \prod_p p^{n(p)} \qquad \text{and} \qquad m = \prod_p p^{m(p)}$$

are supernatural numbers and $m(p) \leq n(p)$ for all primes p, we say m *divides* n. Many familiar concepts from the natural numbers may be defined in a natural way for the supernatural numbers.

Definition 145. Suppose that

$$n_i = \prod_p p^{n_i(p)}$$

is a supernatural number for each i in some index set I. Define the *least common multiple* of the numbers $\{n_i\}_{i \in I}$ to be the supernatural number

$$\prod_p p^{n(p)}$$

where $n(p) = \max_i \{n_i(p)\}$.

Building on [30] and [25] for groups, we define a modified concept of index for profinite loops. Note that if U is an open subloop of a profinite loop G, it follows from compactness that the index of U in G, denoted $|G : U|$, is finite. To avoid confusion, we shall denote the profinite concept of index by $[G : H]$ and the traditional concept of index by $|G : H|$.

Definition 146. Let G be a profinite loop which satisfies both the weak and the strong Lagrange properties. Let H be a closed subloop of G. We say the *index* of H in G, denoted $[G : H]$ is the least common multiple of the indices of the open subloops of G containing H. That is,

$$[G : H] = \text{l. c. m.}\{|G : U| \mid H \leq U \leq_O G\}.$$

The *order* (or *cardinality*) of G is the index $[G : I]$ where I denotes the trivial subloop.

Notice that if G is a profinite loop then any open subloop U of G which contains the closed subloop H of G must contain an open normal subloop N.

Lemma 147. *Let G be a profinite loop and let C be an open subset of G which contains the identity. Then C contains an open subloop of G which is normal in G.*

Proof. Let $G = \varprojlim G_i$ where G_i is a finite loop for each i. Then, without loss of generality, we may assume that G is a closed subset of $\prod G_i$ under the product topology. Then, if O is an open set of G which contains the identity, it follows that $O = G \cap U$ where U is some open set of $\prod G_i$. Since $\prod G_i$ has the product topology, it follows that U is a union of sets of the form $\prod U_i$ where U_i is open in G_i for each i and $U_i \neq G_i$ for only finitely many i. Let $N_i = \{1_{G_i}\}$ if $U_i \neq G_i$ and let $N_i = G_i$ otherwise. Then we have that $N := \prod N_i$ is contained in U, and is an open normal subloop of $\prod G_i$. Thus we find that $G \cap N$ is open in G and normal in G. Finally, we see that $G \cap N$ is contained in O as desired, and thus the proof is complete. □

Proposition 148. *Let G be a profinite loop. Then every nonempty open set in G is a union of cosets of open normal subloops.*

Proof. Let O be a non-empty open set of G. Then if $x \in O$ we have that $\lambda_x^{-1}(O) = \{x\backslash o \mid o \in O\}$ is a nonempty open set of G which contains the identity. Then by Lemma 147 we have that $\lambda_x^{-1}(O)$ contains an open normal subloop K_x of G. We claim that

$$O = \bigcup_{x \in O} xK_x.$$

Notice that if $a \in O$ then $a \in aK_a$ since K_a contains the identity, and thus $a \in \cup_{x \in O} xK_x$. On the other hand, if a is in the above union, it follows that $a \in xK_x$ for some $x \in O$. Thus $a = x \cdot y$ for some $y \in K_x$. But $y = x\backslash b$ for some $b \in O$ since K_x is contained in $\lambda_x^{-1}(O)$. Thus, $a = x \cdot (x\backslash b) = b$ which implies that $a \in O$. Thus we find that O is a union of cosets of normal subloops of G. □

We shall next see that if G is a profinite Moufang loop then G enjoys many of the properties that groups have. While Moufang loops are not associative, they do have a more limited form of associativity which turns out to be strong enough to insure certain finite group theoretic properties hold.

Theorem 149. *Suppose G is a finite Moufang loop and H is a subloop of G. Then the order of H divides the order of G.*

Proof. This was shown by Grishkov and Zavarnitsine in [12]. □

Theorem 150. *Let G be a profinite Moufang loop and let H, K be closed subloops of G with $K \leq H \leq G$. Then*

$$[G : K] = [G : H][H : K].$$

Proof. If N is an open normal subloop of G, then we have that

$$\begin{aligned} [G : NK] &= [G : NH][NH : NK] \\ &= [G : NH][H : (N \cap H)K] \end{aligned}$$

and that $N \cap H$ is an open normal subloop of H. Then, as $[G : NK]$ divides $[G : K]$, it follows that $[G : K]$ divides $[G : H][H : K]$.

Now, if N_1 is an open normal subloop of G and N_2 is an open normal subloop of H then $N_2 = O \cap H$ for some open set O of G. Then O is a union of cosets of open normal subloops, and since $1_G \in O$ it follows that there is an open normal subloop M of G such that $M \subseteq O$ and thus $M \cap H \leq H_2$. Set $N = M \cap N_1$. Then we have that N is an open normal subloop of G and that $[G : N_1H][H : N_2K]$ divides $[G : NH][H : (N \cap H)K]$ which is equal to $[G : NK]$. Thus, we have that $[G : H][H : K]$ divides $[G : K]$. □

Lemma 151. *If $\{H_i\}_{i \in I}$ is a family of closed subloops of a profinite Moufang loop G (indexed by I) such that for all $i, j \in I$ there is an element $k \in I$ with $H_k \leq H_i \cap H_j$ then*

$$[G_i \cap H_i] = \text{l. c. m.}\{[G : H_i]\}.$$

Proof. By Theorem 150 we have that the right hand side of the given equality divides the left hand side. Now, if U is an open subloop of G containing $\cap H_i$ then

$$\bigcap (H_i \cap (G - U)) = \emptyset.$$

As H_i and $G - U$ are closed for each i, so too is $H_i \cap (G - U)$, and thus by compactness there is a finite set $\{i_1, i_2, \cdots, i_r\}$ with

$$\bigcap_{n=1}^{r} ((H_{i_n} \cap (G - U)) = \emptyset$$

and $\cap_{n=1}^{r} H_{i_n} \leq U$. Selecting k such that $H_k \leq H_{i_n}$ for $n = 1, 2, \cdots, r$ we find that $H_k \leq U$, and so $[G : U]$ divides $[G : H_k]$ which implies that the left hand side of the given equality divides the right hand side. Thus the proof is complete. □

Definition 152. If G is a profinite loop, a p-Sylow subloop of G is a subloop P of G such that the order of P is a power of p (not necessarily finite) and $[G : P]$ is a supernatural number which is relatively prime to p.

We have previously noted that in general Sylow subloops of a given loop (even a finite one) may not exist. Even for the case of the relatively group-like Moufang loops, we can find a loop G and a prime p for which no p-Sylow subgroups exist in G. However, for the case of finite Moufang loops, some recent and definitive progress has been made by Grishkov and Zavarnitsine in [13]. Following Grishkov and Zavarnitsine, we have the following definition.

Definition 153. Let G be a Moufang loop. A prime p is called a *Sylow prime* for G if, for every composition factor of G that is isomorphic to $M(q)$ for some q we have $p \nmid \frac{q^2+1}{\gcd(2,q-1)}$, where $M(q)$ denotes the finite simple Paige loop over the finite field $\mathbb{F}_q$.

Recall that a loop G is said to be *solvable* if there exists a normal series $1 = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G$ of subloops G_i such that each factor G_i/G_{i-1} is an abelian group. Among the many important results found in [13] are the following:

Theorem 154. *Let G be a finite solvable Moufang loop. Then every prime is a Sylow prime for G.*

Theorem 155. *Let G be a finite Moufang loop and let p be a prime. Then G contains a p-Sylow subloop if and only if p is a Sylow prime for G.*

Since these results are now known for finite Moufang loops, we can extend them to profinite loops. Thus we have a profinite version of the first Sylow theorem for certain types of profinite Moufang loops, such as those obtained as an inverse limit of finite solvable Moufang loops (such loops are sometimes called pro-solvable).

Theorem 156. *Let $G = \varprojlim G_i$ where G_i is a finite solvable Moufang loop for each i, and let p be a prime. Then G has a p-Sylow subloop.*

Proof. Let S be the set of subloops of G whose index is relatively prime to p. Certainly we have that $S \neq \emptyset$ since $G \in S$. Furthermore, S is partially ordered with respect to inclusion. Let C be a chain in S. That is, for all $H_1, H_2 \in C$ either $H_1 \leq H_2$ or $H_2 \leq H_1$. Then, by Lemma 151 we have that

$$\bigcap \{H \mid H \in C\}$$

is an element of S. By Zorn's Lemma, S has a minimal element, say P, and we have that $[G : P]$ is relatively prime to p. If $|P| \neq p^\alpha$ for some (possibly infinite) α then there is an open normal subloop M of P such that $|P/M|$ is not a power of p. But then, by Theorem 154 P/M has a p-Sylow subloop $Q/M < P/M$. As Q is a union of finitely many cosets of M and as M is closed in P, it follows that Q is closed in both P and G. Thus, by Theorem 150 we have that $[G : Q] = [G : P][P : Q]$ and so $[G : Q]$ is relatively prime to p. But this contradicts the minimality of P, so we conclude that P is a p-Sylow subloop. □

It should be noted that in [10], Glaubermann proved that every finite Moufang loop of odd order is solvable; a result shown for odd ordered groups several years previously by Feit and Thompson. Thus the requirement of solvability above is far from excessive. Employing a very similar argument to the one used in the previous Theorem, we may also show the following:

Theorem 157. *Let $G = \varprojlim G_i$ where G_i is a finite Moufang loop for each i and let p be a prime which is a Sylow prime for each G_i. Then G contains a p-Sylow subloop.*

We shall end with a short discussion of Hall subloops. Let π be a set of primes and G a profinite loop. A subloop H of G is called a π-Hall subloop if $|H|$ is divisible only by primes in π and $[G : H]$ is divisible only by primes not in π. It is clear that π-Hall subloops are a natural generalization of p-Sylow subloops, since a $\{p\}$-Hall subloop is precisely a p-Sylow subloop. It has recently been shown by Gagola in [9] that a finite Moufang loop G is solvable if and only if it contains a π-Hall subloop for any set π of primes. This generalizes a result shown by Philip Hall for finite solvable groups. Combining the result of Gagola with the argument from Theorem 156, we obtain the following result.

Theorem 158. *Let $G = \varprojlim G_i$ where each G_i is a finite solvable Moufang loop and let π be a set of primes. Then G has a π-Hall subloop.*

Proof. The argument is almost identical to the proof of Theorem 156, except that Gagola's generalization of Hall's theorem (mentioned above) stands in for the Sylow theorem of finite solvable Moufang loops. □

We shall conclude by noting that many of the results in this section are not special to Moufang loops. In fact, for any variety of finite loops which satisfies the Lagrange, Sylow and Hall Theorems, the analogues of the above results ought to hold. There are in fact a number of varieties of finite loops for which this is true. The previous results ought to hold (with small modifications at best) for varieties such as odd ordered Bruck loops, Automorphic loops, as well as others. While we do not explicitly prove these results, this section could be viewed as a template for doing so.

Bibliography

[1] A.A. Albert. Quasigroups. 1. *Transactions of the American Mathematical Society*, 54(3):507–519, 1943.

[2] A.A. Albert. On simple alternative rings. *Canadian Journal of Mathematics*, 4:129–135, 1952.

[3] A. Babiy and N. Sandu. Commutative Moufang loops with maximum conditions for subloops. *Buletinul Academiei de Ştinţe A Republich Moldova Mathematica*, 51(2):53–61, 2006.

[4] R. Baer. Nets and groups. *Transactions of the American Mathematical Society*, 46:110–141, 1939.

[5] R.H. Bruck. *A Survey of Binary Systems*. Springer-Verlag, 1958.

[6] R.H. Bruck and E. Kleinfeld. The structure of alternative division rings. *Proceedings of the American Mathematical Society*, 2:878–890, 1951.

[7] R.H. Bruck and L.J. Paige. Loops whose inner mappings are automorphisms. *Annals of Mathematics*, 63(2), 1956.

[8] J. Dugundji. *Topology*. Allyn and Becon, 1966.

[9] S. Gagola. Hall's theorem for Moufang loops. *Journal of Algebra*, 323(12):3252 – 3262, 2010.

[10] G. Glauberman. On loops of odd order ii. *Journal of Algebra*, 8(4):393 – 414, 1968.

[11] E.G. Goodaire, E. Jespers, and C. Polcino Milies. *Alternative Loop Rings*, volume 84. North-Holland Mathematics Studies, 1996.

[12] A. Grishkov and A. Zavarnitsine. Lagrange's theorem for Moufang loops. *Mathematical Proceedings of the Cambridge Philosophical Society*, 139(1):41–57, 2005.

[13] A. Grishkov and A. Zavarnitsine. Sylow's theorem for Moufang loops. *The Journal of Algebra*, 321(7):1813–1825, 2009.

[14] A.N. Grishkov and A.V. Zavarnitsine. Sylow's theorem for Moufang loops. *Journal of Algebra*, 321:1813–1825, 2009.

[15] W. Herfort and P. Plaumann. Boolean and profinite loops. *Topology Proceedings*, 37:1–5, 2011.

[16] K.H. Hofmann and K. Strambach. Topological and analytical loops. In *Quasigroups and Loops: Theory and Applications*. Heldermann Verlag Berlin, 1990.

[17] N. Jacobson. *Basic Algebra*, volume 2. Dover, 2009.

[18] S. Mac Lane. *Categories for the Working Mathematician (2nd Edition)*. Springer Graduate Texts in Mathematics, 1998.

[19] K. Kunen M.K. Kinyon and J.D. Phillips. Every diassociative A-Loop is Moufang. *Proceedings of the American Mathematical Society*, 130(3):619–624, 2002.

[20] P.T. Nagy and K. Strambach. *Loops in Group Theory and Lie theory*, volume 35. De Gruyter Expositions in Mathematics, 2002.

[21] L.J. Paige. A class of simple Moufang loops. *Proceedings of the American Mathematical Society*, 7:471–482, 1956.

[22] C.W. Patty. *Foundations of topology (2nd Edition)*. Jones and Bartlett, 2009.

[23] H. Pflugfelder. *Quasigroups and Loops: Introduction*. Heldermann Verlag Berlin, 1990.

[24] H. Pflugfelder. Historical notes on loop theory. *Commentationes Mathematicae Universitatis Carolinae*, 41(2):359–370, 2000.

[25] L. Ribes and P. Zalesskii. *Profinite Groups (Second Edition)*. Springer, 2010.

[26] H. Scheerer and K. Strambach. Idempotente multiplikationen. *Mathematische Zeitshrift*, 182:95–119, 1983.

[27] A.R.T. Solarin and L. Sharma. On the construction of Bol loops. *Analele ştiinţifce ale Universităţii Al. I. Cuza. Univ din Iaşi*, 1:13–17, 1981.

[28] A.K. Suschkewitsch. On a generalization of the associative law. *Transactions of the American Mathematical Society*, 31, 1929.

[29] A. Wells. Moufang loops arising from Zorn vector matrix algebras. *Commentationes Mathematicae Universitatis Carolinae*, 51:371–388, 2010.

[30] J. Wilson. *Profinite Groups*. Oxford Science Publications, 1998.

[31] E. Zizioli. Semidirect product of loops and fibrations. *Results in Mathematics*, 51(3-4):373–382, 2008.