University of the Witwatersrand

Ramsey functions for spaces with symmetries

Author:
Eleftherios Kyriazis

Supervisor:
Yuliya Zelenyuk

March 22, 2012

Abstract

In this dissertation we study the notion of symmetry on groups, topological spaces, et cetera. The relationship between such structures with symmetries and Ramsey Theory is reflected by certain natural functions. We give a general picture of asymptotic behaviour of these functions.

I warrant that the content of this dissertation is the direct result of my own work. Any use of published or unpublished material is fully and correctly referenced.

Signature .....

Date .....

Contents

Chapter 1

Introduction

Astrologers look to the heavens and see all types of animals in the stars such as lions, bulls and half bull-half lions. Frank Plumpton Ramsey, an English mathematician, proved that such patterns are actually implicit in any large structure, whether it is a group of stars or a series of numbers. For instance, given enough stars, we can always find a group that forms any type of peculiar pattern. Ramsey Theory states that any structure will necessarily contain an orderly substructure. As the late mathematician Theodore Motzkin first proclaimed, Ramsey Theory implies that complete disorder is an impossibility.

Chapter 2 and 3 provides the necessary background for Ramsey type Theorems and Ramsey functions. Chapter 2 introduces filters and ultrafilters and describes how they relate to topological spaces. The set of all ultrafilters on a topological space βX is defined and examined. βX is also the largest compactification, or Stone-Čech Compactification, of the discrete space X. Chapter 3 provides an introduction to semigroups, where we extend the notion of a Stone-Čech Compactification to the semigroup S obtaining βS. βS is interesting for its own sake and its applications to Ramsey Theory.

Chapter 4 introduces Ramsey Theory with Theorems from Hilbert, Schur, van der Waerden and Ramsey. Ramsey Theory can be described as the study of the preservation of properties under set partitions [18]. Ramsey's Theorem deals with colourings on natural numbers or graphs, Schur's Theorem deals with colourings on the simple plane and van der Waerden's Theorem deals with colourings on arithmetic progressions. Finite type examples are illustrated.

Chapter 5 provides background in group theory which is necessary for Chapter 6. The relevant notions include cyclic groups, direct sums, semidirect products and importantly, compact groups. The Haar measure is also examined in some detail.

Chapter 6 concerns Ramsey functions and draws on definitions, theorems and concepts from all previous chapters. The vital notion of symmetry is identified and explained. Ramsey functions are analysed for finite Abelian groups and then compact Abelian groups. A general picture of the asymptotic behaviour of $s_r(G)$, the most asymmetrical maximal measure of a monochromatic symmetric subset, for compact Abelian groups is provided.

The following quote appeared in the 1983 article titled *A Tribute to F. P. Ramsey* and epitomizes the field of Ramsey Theory [12].

Unsolved problems abound, and additional interesting open questions arise faster than solutions to the existing problems. - F. Harary

Chapter 2

Spaces

2.1 Filters and ultrafilters

Filters were introduced by Frigyes Riesz [27] in 1908 and Stanislaw Ulam [33] in 1929. Filters are important as they provide us with ultrafilters which have been used to prove all the fundamental results in Ramsey Theory.

In set theory, a filter is a subset of a partially ordered set (or poset). A poset is a set whose elements are ordered but not all elements are required to be comparable in the order. Filters appear in topology, order theory and lattice theory. Ultrafilters are very useful and have multiple applications in topology (especially with compact Hausdorff spaces), set theory and with Boolean algebras and general partial orders.

Throughout the dissertation we work in ZFC (Zermelo-Fraenkel system of axioms with axiom of choice). Results (all definitions, theorems, lemmas, corollaries, propositions and proofs) from Chapter 2 can be found in [14], [21], [23] and [36].

Definition 2.1.1. A family $\mathcal{F}$ of subsets on a set X is called a *filter* if the following conditions hold:

1. $\emptyset \notin \mathcal{F}$ and $X \in \mathcal{F}$;
2. If $A, B \in \mathcal{F}$, then $A \cap B \in \mathcal{F}$;
3. If $A \in \mathcal{F}$ and $A \subseteq B \subseteq X$, then $B \in X$.

An example of a filter is the set of neighbourhoods of a point in a topological space. A family $\mathcal{F}$ of subsets on a set X is called centered if the intersection of any finite

number of its sets is nonempty.

The smallest filter that contains a given element is known as a principal filter, i.e.: if $x \in X$, then the principal filter is $\mathcal{F}_x = \{A \subseteq X : x \in A\}$. Thus for each $x \in X$, $\mathcal{F}_x$ is the principal filter corresponding to x, the principal element. For sets, principle filters contain a least element and are exactly the one element sets.

The family of all filters on the set X is partially ordered by the relation $\mathcal{F}_1 \subseteq \mathcal{F}_2$. A filter which is maximal with respect to this order is known as an ultrafilter. All other subsets of X are considered either almost everything or almost nothing.

Definition 2.1.2. An *ultrafilter* on the set X is a filter which is not properly contained in any other filter on X.

We denote ultrafilters using lower case letters. If p and q are ultrafilters on X, then $p = q$ if and only if $p \subseteq q$.

There are two types of ultrafilters, namely principal and free. A principle ultrafilter on X is a filter containing a least element. All principal filters are ultrafilters. Non-principal ultrafilters are known as free ultrafilters. An ultrafilter is free if and only if $\bigcap \mathcal{F} = \emptyset$ and can therefore only exist on infinite sets. Free ultrafilters were introduced by Alfred Tarski in 1930. Almost all ultrafilters on an infinite set are free while all ultrafilters of a finite set are principle. We are unable to state examples of free ultrafilters but we can show that they do exist using the Kuratowski-Zorn Lemma and by proving the Ultrafilter Theorem below.

Lemma 2.1.3. (Kuratowski-Zorn). *If every chain (linearly ordered set) in a partially ordered set has an upper bound, then the set has a maximal element.*

Theorem 2.1.4. (Ultrafilter Theorem). *Every filter on a set is contained in an ultrafilter.*

Proof:
Let $\mathcal{F}'$ be a filter on the set X and consider the collection of all filters $\mathcal{F}$ on X that contain $\mathcal{F}'$. Let this collection be δ with the chain γ. There exists a filter $\{F \in \mathcal{F} : \mathcal{F} \in \gamma\}$ on X that is an upper bound for the chain γ. By the Kuratowski-Zorn lemma, δ has a maximal element. This means that there is an ultrafilter that contains $\mathcal{F}'$.

□

Consider an ultrafilter on the infinite set X which contains
$\mathcal{F}_x = \{F \subseteq X : X \backslash F \text{ is finite}\}$, known as the Fréchet filter. Then there exists a free ultrafilter on X. We now provide some theorems to describe some properties and the structure of filters and ultrafilters.

Theorem 2.1.5. (Ultrafilter Criterion). *A filter $\mathcal{F}$ on the set X is an ultrafilter if and only if either $A \in \mathcal{F}$ or $X \backslash A \in \mathcal{F}$ for every subset A of X.*

Proof:
$\Rightarrow$. Let $\mathcal{F}$ be an ultrafilter on X, $A \subseteq X$ and $A \notin \mathcal{F}$. By the definition of a filter, $F \backslash A \neq \emptyset$ for all $F \in \mathcal{F}$. Since $F_1, F_2, \ldots, F_n \in \mathcal{F}$, then $(F_1 \backslash A) \cap (F_2 \backslash A) \cap \ldots \cap (F_n \backslash A) = (F_1 \cap F_2 \cap \ldots \cap F_n) \backslash A = \{F \backslash A : F \in \mathcal{F}\} \neq \emptyset$. By Theorem 2.1.4, there exists an ultrafilter $\mathcal{F}'$ which contains $\{F \backslash A : F \in \mathcal{F}\}$. Since $\mathcal{F} \subseteq \mathcal{F}'$ and hence $\mathcal{F} = \mathcal{F}'$. Since $A \subseteq X$ and $A \notin \mathcal{F}$, then $X \backslash A \in \mathcal{F}'$ and $X \backslash A \in \mathcal{F}$.

$\Leftarrow$. Consider a filter $\mathcal{F}$ satisfying either $A \in \mathcal{F}$ or $X \backslash A \in \mathcal{F}$ and $\mathcal{F}$ is contained in the ultrafilter $\mathcal{F}'$. Now, if $\mathcal{F} \neq \mathcal{F}'$, then there exists a subset $A \in \mathcal{F}'$ such that $A \notin \mathcal{F}$. Since $X \backslash A \in \mathcal{F}$ then $X \backslash A \in \mathcal{F}'$. However, since $A \cap (X \backslash A) = \emptyset$ this contradicts the definition of a filter and so $\mathcal{F} = \mathcal{F}'$. Therefore $\mathcal{F}$ is an ultrafilter.

□

Corollary 2.1.6. *Let $\mathcal{F}$ be an ultrafilter on X and $F = F_1 \cup \ldots \cup F_n$ where $F \in \mathcal{F}$. Then there exists an F_i such that $F_i \in \mathcal{F}$.*

Proof:
Suppose the contrary, i.e.: $F_1 \notin \mathcal{F}, \ldots, F_m \notin \mathcal{F}$. Then by the Ultrafilter Criterion $X \backslash F_1 \in \mathcal{F}, \ldots, X \backslash F_m \in \mathcal{F}$. Now $(X \backslash F_1) \cap \ldots \cap (X \backslash F_m) = X \backslash F \in \mathcal{F}$.
Since $F \in \mathcal{F}$ and $\mathcal{F}$ is a filter, we obtain a contradiction and $F_i \in \mathcal{F}$.

□

Theorem 2.1.7. (Ultrafilter Image Theorem). *Let $\mathcal{F}$ be an ultrafilter on the set X. For every map $f : X \to Y$ the filter $\bar{f}(\mathcal{F})$ is an ultrafilter on the set Y.*

Proof:
If $Y = Y_1 \cup Y_2$, then $X = f^{-1}(\mathrm{Y}_1) \cup f^{-1}(\mathrm{Y}_2)$. By the Ultrafilter Criterion, either $f^{-1}(\mathrm{Y}_1) \in \mathcal{F}$ or $f^{-1}(\mathrm{Y}_2) \in \mathcal{F}$. Suppose that $F = f^{-1}(\mathrm{Y}_1)$ and $F \in \mathcal{F}$. We then have that $f(F) = Y_1$ and $f(F) \in \bar{f}(\mathcal{F})$. Thus, $Y_1 \in \bar{f}(\mathcal{F})$. Using the Ultrafilter Criterion we can verify that $\bar{f}(\mathcal{F})$ is an ultrafilter on Y.

□

2.2 Ultrafilters on topological spaces

Topological spaces are structures that allow formal definitions of many notions.

Definition 2.2.1. A family τ of open subsets on a set X is called a *topology* of X if the following conditions hold:

1. The union of an arbitrary number of sets in τ is also in τ;
2. The intersection of a finite number of sets in τ is also in τ;
3. The empty set and X are both sets in τ.

The elements of X are called points and the complements of members of τ are known as closed sets. (X, τ) is called the topological space. A set W is a neighbourhood of a point $x \in X$ if there is an open subset $U \in \tau$ such that $x \in U \subseteq W$. We denote $B(x)$ as a collection of subsets of X that are neighbourhoods of the point $x \in X$.

If τ contains only the empty set and X then τ forms a trivial topology. If τ contains the power set (the set of all subsets of X) then τ forms a discrete topology.

An equivalent definition is a topology on closed sets. In this case the following conditions must hold:

1. The intersection of an arbitrary number of sets in τ is also in τ;
2. The union of a finite number of sets in τ is also in τ;
3. The empty set and X are both sets of τ.

The empty set and X are both open and closed (or clopen). We now use our knowledge of ultrafilters to define properties of topological spaces. By definition, a filter $\mathcal{F}$ on (X, τ) converges to a point x if $W \in \mathcal{F}$ for every neighbourhood W of x. x is known as the limit of the filter $\mathcal{F}$. A subset $A \subseteq X$ is closed if and only if a limit of any filter containing A belongs to A. Note that the family of all neighbourhoods of x forms a filter. A topological space is called Hausdorff if any two distinct points of the space have disjoint neighbourhoods, i.e.: the points are seperated by open sets.

Theorem 2.2.2. *A topological space (X, τ) is Hausdorff if and only if every filter on X has at most one limit.*

Proof:
Suppose (X, τ) is Hausdorff and $\mathcal{F}$ is a filter on X that converges to two distinct points, say x and y. Choose two distinct neighbourhoods of x and y, say U and V respectively. Then $U \cap V = \emptyset$, a contradiction with the definition of a filter and so every filter on X converges to a single point.

Now suppose that (X, τ) is not Hausdorff but every filter on X converges to a single point. Choose two distinct points $x, y \in X$ with neighbourhoods U of x and V of y such that the $U \cap V \neq \emptyset$. The family $\{U \cap V : U \in B(x), V \in B(y)\}$ is centered and can be completed to a filter $\mathcal{F}$. $B(x) \subseteq \mathcal{F}$ and $B(y) \subseteq \mathcal{F}$ and so $\mathcal{F}$ converges to two distinct points, namely x and y. This is a contradiction.

□

A cover of a topological space is a family of nonempty subsets of X whose union contains X. The Heine-Borel definition of compactness states that a topological space is compact if every open cover of X has a finite subcover, i.e.: if X is the union of a family of open sets, there is a finite subfamily whose union is also X. A cover is a family of nonempty subsets of X whose union contains the given set X. This brings us to a theorem about compactness.

Theorem 2.2.3. *A topological space (X, τ) is compact if and only if every ultrafilter on X is convergent.*

Proof:
Let X be a compact space with an ultrafilter $\mathcal{F}$ that doesn't converge to a point on X. For any point $x \in X$ there is an open neighbourhood U_x of x such that $U_x \notin \mathcal{F}$. Now from the cover of X by open subsets U_x, $x \in X$, select a finite subcover $X = U_{x_1} \cup \ldots \cup U_{x_n}$. By Corollary 2.1.6. at least one of $U_{x_1} \cup \ldots \cup U_{x_n}$ belongs to $\mathcal{F}$, a contradiction to the choice of these sets.

Now suppose all ultrafilters on X converge but (X, τ) is not compact. If (X, τ) is not compact then there exists a cover $U_\alpha, \alpha \in J$ of (X, τ) which has no finite subcover. For every finite subset $F \subseteq J$ let $\mathcal{U}(F) = \bigcup\{\mathcal{U}_\alpha : \alpha \in F\}$ and by our hypothesis $X \backslash \mathcal{U}(F) \neq \emptyset$. The centered family $\{X \backslash \mathcal{U}(F) : F \text{ is a finite subset from } J\}$ can be completed to an ultrafilter $\mathcal{F}$. By the hypothesis $\mathcal{F}$ converges to some point $x \in X$. Let $\mathcal{U}_\alpha$ be an element of the cover containing x. Clearly $\mathcal{U}_\alpha \in \mathcal{F}$. Let $F = \{\alpha\}$. By the construction of $\mathcal{F}$ we have $X \backslash \mathcal{U}(F) \in \mathcal{F}$, a contradiction with $\mathcal{U}(F) \in \mathcal{F}$.

□

We now introduce an important result, Tychonoff's Theorem. It states that the product of any collection of compact topological spaces is compact. The theorem was proved and named after Andrey Nikolayevich Tychonoff who first proved it for powers of the closed unit interval in 1930 and later completed the full theorem in 1935. The theorem relies on the definitions of compactness and the product topology. When the theorem was initially proved, the Balzano-Weierstrass criterion was used as opposed to the Heine-Borel definition of compactness. Tychonoff's Theorem is considered as one of the most important results in general topology as any construction that takes a general object to produce a compact space requires it.

Let (X_α, τ_α), $\alpha \in J$, be a collection of topological spaces. $X = \prod_{\alpha \in J} X_\alpha$ is the Cartesian product of X_α. The elements of X are the functions
$f : J \to \bigcup\{X_\alpha : \alpha \in J\}$ satisfying $f(\alpha) \in X_\alpha$ for all $\alpha \in J$. X equipped with this topology is called the Tychonoff product of the family (X_α, τ_α), $\alpha \in J$. The Tychonoff topology is the weakest topology (the topology with the fewest open sets) on the Cartesian product X such that all projections $pr_\alpha : X \to X_\alpha$, where $pr_\alpha(f) = f(\alpha)$ are continuous. We now prove Tychonoff's Theorem.

Theorem 2.2.4. (Tychonoff's theorem). *The Tychonoff product of any collection of compact topological spaces is compact.*

Proof:
Consider the ultrafilter $\mathcal{F}$ on X. By the Ultrafilter Image Theorem, $\bar{pr}_\alpha(\mathcal{F})$ is an ultrafilter on the compact space (X_α, τ_α). Since we know that a topological space is compact if and only if every ultrafilter on it is convergent, the ultrafilter $\bar{pr}_\alpha(\mathcal{F})$ also converges to some point $x_\alpha \in X_\alpha$. Let $f \in X$ such that $f(\alpha) = x_\alpha$ for all $\alpha \in J$. By definition of the Tychonoff topology the ultrafilter $\mathcal{F}$ converges to the point $f \in X$. Using Theorem 2.2.3 the proof is complete.

□

Let r be a positive integer and the subset $Y \subseteq X$ be partitioned into r parts: $Y = Y_1 \cup Y_2 \cup \ldots \cup Y_r$. A collection $\mathcal{A}$ of subsets of X is called r-regular with respect to Y if for every partition of Y there is a subset $A \in \mathcal{A}$ such that $A \subseteq Y_k$ where $1 \leq k \leq r$. If $A \nsubseteq Y_k$ for every $A \in \mathcal{A}$ then $\mathcal{A}$ is called non-regular.

Theorem 2.2.5. (Compactness Theorem for partitions). *If a collection $\mathcal{A}$ of subsets of X is r-regular with respect to X and every element of $\mathcal{A}$ is a finite subset, then there is a finite subset $Y \subseteq X$ such that $\mathcal{A}$ is r-regular with respect to Y.*

Proof:
Let $R = \{1, \ldots, r\}$ and R_x be a copy of R for every $x \in X$. Consider the Tychonoff product $R^X = \prod\{R_x : x \in X\}$, where each factor is endowed with the discrete topology. Suppose the theorem is invalid. Then for every finite subset $Y \subseteq X$ there is a non-regular partition $Y = Y_1 \cup Y_2 \cup \ldots \cup Y_r$. Define the characteristic function h of this partition letting $h(x) = i$ if and only if $x \in Y_i$. Extend the function h to a map $f_Y \in R^X$.

Let $F_Y = \{f_K : Y \subseteq K, K \text{ is a finite subset of } X\}$. The centered family $\{F_Y : Y \text{ is a finite subset of } X\}$ can be completed (sets are added) to an ultrafilter $\mathcal{F}$. By the Tychonoff theorem, $\mathcal{F}$ converges to a point $f \in R^X$.

Consider $X = X_1 \cup \ldots \cup X_r$ where $X_i = \{x \in X : f(x) = i\}$. By the conditions of the theorem there is k and $A \in \mathcal{A}$ such that $A \subseteq X_k$. Consequently, $f(x) = k$ for all $x \in A$. Since $\mathcal{F}$ converges to f, there is a finite subset $Y \subseteq X$ such that $A \subseteq Y$ and $f_Y(x) = f(x)$ for all $x \in X$.

The restriction of f_Y to the subset Y determines a non-regular partition $Y = Y_1 \cup Y_2 \cup \ldots \cup Y_r$. Since $f_Y(x) = k$ for all $x \in A$, we achieve $A \subseteq Y_k$, contradicting the non-regularity of this partition.

□

2.3 The space βX

Let us define a topology on the set of all ultrafilters on the set X.

Definition 2.3.1. Let X be a discrete topological space.

1. $\beta X = \{p : p \text{ is an ultrafilter on } X\}$.
2. Given $A \subseteq X$, $\bar{A} = \{p \in \beta X : A \in p\}$.

Definition 2.3.2. Let X be a set and let $a \in X$. Then $e(a) = \{A \subseteq X : a \in A\}$.

For each $a \in X$, $e(A)$ is the principal ultrafilter corresponding to a. We denote ultrafilters on X using lower case letters as we can think of them as points in a topological space. The space above is discrete because the set X can be identified with the subset of all principal ultrafilters in βX. If $x \in X$, then $\overline{\{x\}}$ is a neighbourhood of the principal ultrafilter x and $\overline{\{x\}} = x$. Therefore, each point of X is isolated in βX making X a discrete subspace. A base B on a topological space (X, τ) is that every open set in τ can be written as a union of elements of B. We can deduce that $\{\bar{A} : A \subseteq X\}$ forms a basis for a topology on βX. The topology of βX is the topology which has these sets as a basis. The following theorem establishes topological properties of βX.

Theorem 2.3.3. *βX is a compact Hausdorff space.*

Proof:
Firstly, let us prove that βX is compact. Let $\mathfrak{U}$ be an open cover of βX. We know that $\bar{A} = \{p \in \beta X : A \in p\}$, so each open subset of the cover on βX is the union of these $\bar{A}$'s. Therefore $\mathfrak{U} = \{\bar{A} : A \in \mathcal{F}\}$.

Let $\mathcal{F}' = \{X \backslash A : A \in \mathcal{F}\}$. Suppose, to prove a contradiction, that $\mathcal{F}'$ is centered (intersection of any of its sets is nonempty), then $\mathcal{F}'$ must be contained in some ultrafilter p of βX. Since $\mathfrak{U}$ is the cover of βX, there is a subset $A \in \mathcal{F}$ such that $p \in \bar{A}$ (containing $\mathcal{F}'$). Also, since $\mathcal{F}'$ is contained in some ultrafilter p, we have $X \backslash A \in p$. But we know that $A \in p$, so with $X \backslash A \in p$ we have a contradiction. Therefore $\mathcal{F}'$ is not centered.

Now choose subsets $A_1, \ldots, A_n \in \mathcal{F}$ such that $(X \backslash A_1) \cap \ldots \cap (X \backslash A_n) = \emptyset$. Then $A_1 \cup \ldots \cup A_n = X$ and we already know that $\bar{A_1} \cup \ldots \cup \bar{A_n} = \beta X$. Therefore, we can conclude that $\{\bar{A_1}, \ldots, \bar{A_n}\}$ is a finite subcover of $\mathfrak{U}$.

Now let us prove that βX is Hausdorff. Suppose that q and r are distinct elements of βX. Let the set $A \in q \backslash r$. Then $B \backslash A \in r$, where B is an arbitrary set. So $\bar{A}$ and $\overline{B \backslash A}$ are disjoint open subsets of βX containing q and r respectively proving that βX is Hausdorff.

□

Theorem 2.3.4. *Let X be any set.*

1. *The sets of the form $\bar{A}$ are the clopen subsets of βX.*
2. *For every $A \subseteq X$, $\bar{A} = cl_{\beta X}$ e[A].*
3. *For any $A \subseteq X$ and any $p \in X, p \in cl_{\beta X}$ e[A] if and only if $A \in p$.*
4. *The mapping e is injective and* e[X] *is a dense subset of βX whose points are precisely the isolated points of βX.*
5. *If U is an open subset of $\beta X, cl_{\beta X} U$ is also open.*

Proof:

1. Suppose that p and q are distinct elements of βX. If $A \in p \backslash q$, then $X \backslash A \in q$. So $\bar{A}$ and $\overline{X \backslash A}$ are disjoint open subsets containing p and q respectively. Sets of the form $\bar{A}$ are also a base for the closed sets, because $\beta X \backslash \bar{A} = \overline{(X \backslash A)}$. Therefore each set $\bar{A}$ is open and closed (clopen).

Now suppose that C is any clopen subset of βX. Let $\mathcal{A} = \{\bar{A} : A \subseteq X \text{ and } \bar{A} \subseteq C\}$. Since C is open, $\mathcal{A}$ is an open cover of C. Since C is closed, it is also compact and we can pick a finite subfamily $\mathcal{F}$ of X such that $C = \bigcup_{A \in \mathcal{F}}$. Since $(\overline{A \cup B}) = \bar{A} \cup \bar{B}$, $C = \overline{\bigcup \mathcal{F}}$.

2. For each $a \in A$, $e(a) \in A$ and therefore $cl_{\beta X}$ e[A] $\subseteq \bar{A}$. To prove the reverse, let $p \in \bar{A}$. Let $\bar{B}$ denote a neighbourhood of p, then $A \in p$ and $B \in p$. So $A \cap B \neq \emptyset$. Now choose any $a \in A \cap B$. Since $e(a) \in$ e[A] $\cap \bar{B}$, e[A] $\cap \bar{B} \neq \emptyset$ and thus $p \in cl_{\beta X}$ e[A].

3. By 2 and the definition of $\bar{A}$, $p \in cl_{\beta X}$ e[A] $\Leftrightarrow p \in \bar{A} \Leftrightarrow A \in p$.

4. e[X] is a dense subset of βX if any point $x \in \beta X$ belongs to e[X] or is a limit point of e[X]. If $a, b \in X$ are distinct then $X \backslash \{a\} \in e(b) \backslash e(a)$ and hence $e(a) \neq e(b)$. For any $a \in X, e(a)$ is isolated in βX since $\overline{\{a\}}$ is an open subset of βX whose solitary member is $e(a)$. Conversely, if p is an isolated point of βX, then $\{p\} \cap$ e[X] $\neq \emptyset$ and so $p \in$ e[X].

5. If U is the empty set then trivial. We therefore assume that U is not the empty set. Let $A = e^{-1}[U]$ and we claim that $U \subseteq cl_{\beta X}$ e[A]. Now let $p \in U$ and let $\bar{B}$ be a neighbourhood of p. Then $U \cap \bar{B}$ is a nonempty open set and by 4, $U \cap \bar{B} \cap$ e[X] $\neq \emptyset$. Now pick $b \in B$ with $e(b) \in U$ then $e(b) \in \bar{B} \cap$ e[A] and $\bar{B} \cap$ e[A] $\neq \emptyset$. e[A] $\subseteq U$ and so $U \subseteq cl_{\beta X}$ e[A] $\subseteq cl_{\beta X} U$. Therefore $cl_{\beta X} U = cl_{\beta X}$ e[A] $= \bar{A}$ (by 2), and so $cl_{\beta X} U$ is open in βX.

□

2.4 βX as the Stone-Čech compactification

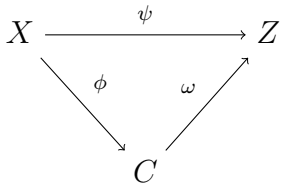
The Stone-Čech Compactification was introduced independently by Marshall Stone [31] and Eduard Čech [5] in 1937. An embedding of a topological space X into a topological space Y is a function $\phi : X \to Y$ which defines a homeomorphism from X onto $\phi[X]$.

Definition 2.4.1. Let X be a topological space. A *compactification* of X is a pair (ϕ, C) such that C is a compact space, ϕ is an embedding of X into C, and $\phi[X]$ is dense in C.

Any completely regular space has a largest compactification called its Stone-Čech Compactification.

Definition 2.4.2. Let X be a completely regular topological space. The *Stone-Čech Compactification* of X is a pair (ϕ, C) such that:

1. C is a compact space;
2. ϕ is an embedding of X into C;
3. $\phi[X]$ is dense in C;
4. given any compact space Z and any continuous function $\psi : X \to Z$, there exists a continuous function $\omega : C \to Z$ such that $\omega \circ \phi = \psi$ (the diagram below commutes).

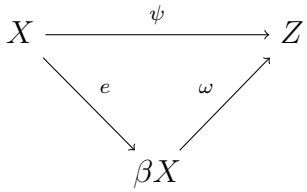


When the space X is discrete, the Stone-Čech Compactification βX can be thought of as the set of all ultrafilters on X. X is regarded as being a subspace of βX.

Theorem 2.4.3. *Let X be a discrete space. Then $(e, \beta X)$ is a Stone-Čech Compactification of X.*

Proof:
Conditions 1,2 and 3 of Definition 2.4.2 hold by Theorems 2.3.3 and 2.3.4.

We must prove condition 4. Let Z be a compact space and let $\psi : X \to Z$. For each $p \in \beta X$, let $\mathcal{A}_p = \{cl_Z\ \psi[A] : A \in p\}$. Then for each $p \in \beta X, \mathcal{A}_p$ has the finite intersection property and so has a nonempty intersection. Now choose $\omega(p) \in \cap\mathcal{A}_p$. Then we have the following diagram:



We need to show that the above are commutative and that ω is continuous. To prove $\omega \circ e = \psi$, let $x \in X$. Then $\{x\} \in e(x)$ so $\omega(e(x)) \in cl_Z\, \psi[\{x\}] = cl_Z\, [\{f(x)\}] = \{\psi(x)\}$. So $\omega \circ e = \psi$.

To prove that ω is continuous, let $p \in \beta X$ and let U be a neighbourhood of $\omega(p)$ in Z. Since Z is regular, we can pick a neighbourhood V of $\omega(p)$ with cl_Z V $\subseteq U$ and let $A = \psi^{-1}[\mathrm{V}]$. We claim that $A \in p$ so suppose instead that $X\backslash A \in p$. Then $\omega(p) \in cl_Z\ \psi[X\backslash A]$ and V is a neighbourhood of $\omega(p)$ so $V \cap \psi[X\backslash A] \neq \emptyset$. This contradicts the fact that $A = \psi^{-1}[\mathrm{V}]$. Thus $\bar{A}$ is a neighbourhood of p. We claim that $\omega[\bar{A}] \subseteq U$, so let $q \in \bar{A}$ and suppose that $\omega(q) \notin U$. Then $Z\backslash cl_Z$ V is a neighbourhood of $\omega(q)$ and $\omega(q) \in cl_Z\ \psi[A]$. So $(Z\backslash cl_Z$ V$) \cap \psi[A] \neq \emptyset$, contradicting the fact that $A = \psi^{-1}[\mathrm{V}]$.

□

Chapter 3

Semigroups

3.1 Semigroups: general notions and facts

We provide some background in Algebra relating to semigroups. The Section concludes with theorems which are necessary for Hindman's and van der Waerden's theorems. We assume all spaces are Hausdorff. Results from Chapter 3 can be found in [14], [15] and [36].

Definition 3.1.1. A *semigroup* is a pair $(S, *)$ where S is a nonempty set and $*$ is an associative binary operation.

For the duration of this Chapter we will use the general binary operation of $*$ and change to the additive operation in Chapter 5 which is required for Abelian groups. There are many examples of semigroups such as $(\mathbb{N}, +)$ and $(\mathbb{R}, \cdot)$. We now list some standard definitions.

Definition 3.1.2. A *group* is a semigroup G containing an element e such that:

1. $e * a = a$ for all $a \in G$;
2. For every $a \in G$, there is an element $b \in G$ with $b * a = e$.

Definition 3.1.3. Let $(S, *)$ and $(T, +)$ be semigroups and $x, y \in S$.

1. A *homomorphism* from S to T is a function $\phi : S \to T$ such that $\phi(x * y) = \phi(x) + \phi(y)$.
2. An *isomorphism* from S to T is a homomorphism from S to T that is both bijective and surjective.

Definition 3.1.4. Let $(S, *)$ be a semigroup and $a, x \in S$.

1. a is known as a *left identity* of S if and only if $a * x = x$.
2. a is known as a *right identity* of S if and only if $x * a = x$.
3. a is known as an *identity* of S if and only if a is both a left and right identity.

We now deal with idempotents which are an important notion. When dealing with arbitrary semigroups we will denote the binary operation $\cdot$ and $x \cdot y$ as xy.

Definition 3.1.5. Let $(S, \cdot)$ be a semigroup.

1. $x \in S$ is an *idempotent* if and only if $xx = x$.
2. $E(S) = \{x \in S : x \text{ is an idempotent } \}$.
3. E is a *subsemigroup* of S if and only if E is a semigroup under the operation of S and $E \subseteq S$.
4. E is a *subgroup* of S if and only if E is a group under the operation of S and $E \subseteq S$.

An idempotent operation or a function is an operation that can be applied multiple times without changing the result. Examples are the union and intersection of a set. If X is a group with identity e, then $E(X) = \{e\}$. The proof of this is simple; assume that $f \in E(X)$. Then $ff = f = fe$. Multiply on the left by the inverse of f and then $f = e$.

Let A and B be subsets of the semigroup S with $AB = \{ab : a \in A \text{ and } b \in B\}$. An ideal is a collection of sets that are considered small. They allow for the generalization of a property such as a multiple of an integer. Every subset of an element of the ideal must be in the ideal and the union of any two elements of the ideal must also be in the ideal. A general example of an the sets that form an ideal are the subsets of K where $K \subseteq X$.

For simplicity of notation let us denote the semigroup $(S, \cdot)$ as S and assume that $\cdot$ is known.

Definition 3.1.6. Let S be a semigroup.

1. The subset L of S is a *left ideal* of S if and only if $SL \subseteq L$, i.e.: $\forall s \in S, l \in L$ we have $sl \in L$.

2. The subset R of S is a *right ideal* of S if and only if $RS \subseteq R$, , i.e.: $\forall s \in S, r \in R$ we have $rs \in R$.

3. The subset I of S is an *ideal* of S if and only if I is a left and right ideal of S.

If $I \neq S$ then I is known as a proper ideal. An ideal I is called a proper ideal of S if $I \neq S$ (if $I = S$ then I is called a unit ideal). A minimal ideal is a left or right ideal which are minimal with respect to the set they are contained within.

Definition 3.1.7. Let S be a semigroup.

1. The subset L of S is a *minimal left ideal* of S if and only if L is a left ideal of S and whenever J is a left ideal of S with $J \subseteq L$ then $J = L$.

2. The subset R of S is a *minimal right ideal* of S if and only if R is a right ideal of S and whenever J is a right ideal of S with $J \subseteq R$ then $J = R$.

A maximal ideal is a proper ideal I if there exists no other proper ideal J with $I \subseteq J$.

Lemma 3.1.8. *Let S be a semigroup.*

1. *Let $x \in S$. Then xS is a right ideal, Sx a left ideal and $S \times S$ an ideal.*

2. *Let $e \in E(S)$. Then e is a left identity for eS, a right identity for Se and an identity for eSe.*

Proof:
1 is immediate. For 2, let $e \in E(S)$. To show that e is a left identity for eS, let $x \in eS$ and pick $p \in S$ such that $x = ep$. Then $ex = eep = ep = x$. Similarly, e is a right identity for Se.

□

Lemma 3.1.9. *Let S be a semigroup, I an ideal of S and L a minimal left ideal of S. Then $L \subseteq I$.*

We now show that minimal left ideals are connected with each other.

Theorem 3.1.10. *Let S be a semigroup with L a minimal left ideal of S and $T \subseteq S$. Then T is a minimal left ideal of S if and only if there is some $a \in S$ such that $T = La$.*

Proof:
For necessity. Pick $a \in T$. By the definition of an ideal $SL \subseteq L$ and so $SLa \subseteq La$. $La \subseteq ST \subseteq T$ giving us that La is a left ideal of S contained in T so $La = T$.

For sufficiency. Since $SLa \subseteq La$, La is a left ideal of S. Now assume that B is a left ideal of S and $B \subseteq La$. Let $A = \{s \in L : sa \in B\}$. Then $A \subseteq L$ and $A \neq \emptyset$. We claim that A is a left ideal of S, so let $s \in A$ and $t \in S$. Then $sa \in B$ and $tsa \in B$. Since $s \in L$, $ts \in L$ and so $ts \in A$ as required. Therefore $A = L$ so $La \subseteq B$ giving $La = B$.

□

Corollary 3.1.11. *Let S be a semigroup. If S has a minimal left ideal of S, then every left ideal of S contains a minimal left ideal.*

Proof:
Let L be a minimal left ideal of S and J a left ideal of S. Pick $a \in J$ and then by Theorem 3.1.10, La is a minimal left ideal which is contained in J.

□

Definition 3.1.12. Let $(S, *)$ be a semigroup.

1. The *centre* of S is $\{x \in S : \text{for all } y \in S, xy = yx\}$.
2. If $x \in S, \lambda_x : S \to S$ is defined by $\lambda_x(y) = xy$.
3. If $x \in S, \rho_x : S \to S$ is defined by $\rho_x(y) = yx$.
4. $L(S) = \{\lambda_x : x \in S\}$.
5. $R(S) = \{\rho_x : x \in S\}$.

The following definition sets out the topological hierarchy.

Definition 3.1.13. 1. A *right topological semigroup* is a triple $(S, \cdot, \tau)$ where $(S, \cdot)$ is a semigroup, (S, τ) is a topological space and $\rho_x : S \to S$ is continuous for all $x \in S$.

2. A *left topological semigroup* is a triple $(S, \cdot, \tau)$ where $(S, \cdot)$ is a semigroup, (S, τ) is a topological space and $\lambda_x : S \to S$ is continuous for all $x \in S$.

3. A *semitopological semigroup* is a right and left topological semigroup.

4. A *topological semigroup* is a triple $(S, \cdot, \tau)$ where $(S, \cdot)$ is a semigroup, (S, τ) is a topological space and $\cdot : S \to S$ is continuous.

5. A *topological group* is a triple $(S, \cdot, \tau)$ where $(S, \cdot)$ is a group, (S, τ) is a topological space, $\cdot : S \to S$ is continuous and $In : S \to S$ is also continuous (where $In(x)$ is the inverse of x in S).

Definition 3.1.14. (*Quotient topology*). $X/\backsim$ of a topological space X with the equivalence relation $\backsim$ on X is defined as the set of equivalence classes of points in X which is under the equivalence relation, together with the following topology given to the subsets U of $X/\backsim$: a subset U of $X/\backsim$ is called open if and only if the union of the subsets is open in X.

The following two theorems are fundamental and deal with compact right topological semigroups.

Theorem 3.1.15. *Every compact right topological semigroup contains an idempotent* (R. Ellis).

Proof:
Let $\mathcal{A} = \{K \subseteq S : K \neq \emptyset, K \text{ is compact}, K.K \subseteq K\}$. Evidently, $\mathcal{A}$ is the set of compact subsemigroups of S. Firstly, we show that $\mathcal{A}$ has a minimal member using the Kuratowski-Zorn Lemma. Since $S \in \mathcal{A}$, $\mathcal{A} \neq \emptyset$ and so let C be a chain in $\mathcal{A}$. C is a collection of closed subsets of the compact space S with the finite intersection property, i.e.: $\cap C \neq \emptyset$. $\cap C$ is compact and a semigroup. Therefore $\cap C \in \mathcal{A}$ and so there is a minimal member $A \in \mathcal{A}$.

Choose an arbitrary element, say $x \in A$. We must show $xx = x$. We first show that $Ax = A$. Let $B = Ax$. $B \neq \emptyset$ and since $B = \rho_x[A]$ (right topological semigroup with $x \in A$), B is the continuous image of a compact space, and thus compact.

Now $BB = AxAx \subseteq AAAx \subseteq Ax = B$. Thus $B \in \mathcal{A}$. Since $B = Ax \subseteq AA \subseteq A$ and A is minimal, we have $B = A$.

Now let $C = \{y \in A : yx = x\}$. Since $x \in A = Ax$, $C \neq \emptyset$. $C = A \cap p_x^{-1}$ [{x}], so C is closed and hence compact. Given $y, z \in C$, we have $yz \in AA \subseteq A$ and $yzx = yx = x$ so $yz \in C$. Therefore $C \in \mathcal{A}$. Since $C \subseteq A$ and A is minimal from above, we achieve $C = A$. So $x \in C$ and $xx = x$ as required.

□

Theorem 3.1.16. *Let S be a compact right topological semigroup. Then every left ideal of S contains a minimal left ideal. Minimal left ideals are closed and each minimal left ideal has an idempotent.*

Proof:
Let L be a left ideal of S. Choose $x \in L$, then $Sx = \rho_x[S]$ is a compact left ideal contained in L. Any minimal left ideal is closed and by the previous theorem, any minimal left ideal contains an idempotent. We must therefore show that any left ideal of S contains a minimal left ideal.

Let L be a left ideal of S, i.e.: $SL \subseteq L$, and let $\mathcal{A} = \{T : T$ is a closed left ideal of S and $T \subseteq L\}$. Using the Kuratowski-Zorn Lemma on $\mathcal{A}$, we get a left ideal N which is minimal with respect to all of the closed left ideals contained in L. Since every left ideal contains a closed left ideal, N must be a minimal left ideal.

□

Definition 3.1.17.
1. A semigroup is *simple* (left simple) if it has no proper ideal (left ideal).
2. A semigroup S is *completely simple* if it is simple and there is a minimal left ideal of S which has an idempotent.

Corollary 3.1.18. *Every compact right topological semigroup has a smallest ideal which is a completely simple semigroup.*

Definition 3.1.19. Let G be a group, I, Λ be nonempty sets, and let $P = (p_{\lambda i}$ be a $\Lambda \times I$ matrix with entries in G. The *Rees matrix semigroup over the group G with $\Lambda \times I$ sandwich matrix P*, denoted $f : \mathcal{M}(G; I, \Lambda; P)$, is the set $I \times G \times \Lambda$ with the operation defined by

$$(i, a, \lambda)(j, b, \mu) = (i, ap_{\lambda j}b, \mu).$$

$\mathcal{M}(G; I, \Lambda; P)$ is a completely simple semigroup. The following theorem is a special case of the Rees-Suschkewitsch theorem proved by A. Suschkewitsch [32] for finite semigroups and D. Rees [26] in the general case. This theorem tells us that every completely simple semigroup is isomorphic to some Rees matrix semigroup.

Theorem 3.1.20. *Let S be a completely simple semigroup. Pick $e \in E(S)$ such that Se is a minimal left ideal. Let $I = E(Se)$, $\Lambda = E(eS)$, $G = eSe$, and $p_{\lambda i} = \lambda i$, and define $f : \mathcal{M}(G; I, \Lambda; P) \to S$ by $f(i, a, \lambda) = ia\lambda$. Then f is an isomorphism.*

Proof:
Let (i, a, λ) and (j, b, μ) be arbitrary elements of $f : \mathcal{M}(G; I, \Lambda; P)$. Then

$$f((i, a, \lambda)(j, b, \mu)) = f(i, a\lambda jb, \mu) = ia\lambda jb\mu = f(i, a, \lambda)f(j, b, \mu),$$

so f is a homomorphism. Since

$$E(Se)eSeE(eS) = E(Se)eSeeSeE(eS) = SeeS = SeS,$$

f is surjective. To see that f is injective, let $ia\lambda = jb\mu$. Then

$$\begin{gathered} a = eae = eia\lambda e = ejb\mu e = ebe = b, \\ i = ie = iaa^{-1} = ia\lambda ea^{-1} = ja\mu ea^{-1} = jaa^{-1} = je = j, \\ \lambda = e\lambda = a^{-1}a\lambda = a^{-1}eia\lambda = a^{-1}eja\mu = a^{-1}a\mu = e\mu = \mu. \end{gathered}$$

Hence f is an isomorphism.

□

3.2 The semigroup βS

We have showed that βX is the Stone-Čech Compactification of the discrete space X. It is possible to extend this notion to semigroups and show that βS is the Stone-Čech Compactification of the discrete semigroup S. An operation used on a semigroup S will be the same as the operation used on βS.

Theorem 3.2.1. *Let S be a discrete space and let $\cdot$ be a binary operation defined on S. There is a unique binary operation $* : \beta S \times \beta S \to \beta S$ satisfying the following three conditions:*

1. *For every $s, t \in S, s * t = s \cdot t$;*
2. *For each $q \in \beta S$, the function $\rho_q : \beta S \to \beta S$ is continuous, where $\rho_q(p) = p * q$;*
3. *For each $s \in S$, the function $\lambda_s : \beta S \to \beta S$ is continuous, where $\lambda_s(q) = s * q$.*

Proof:
Uniqueness and existence are proved concurrently. Let us first define $*$ on $S \times \beta S$. Define $l_s : S \to S \subseteq \beta S$ by $l_s(t) = s \cdot t$ for any $s \in S$. By the Stone-Čech Compactification, there is a continuous function $\lambda_s : \beta S \to \beta S$ such that $\lambda_{s|S} =$l$_s$. Define $s * q =_s (q)$ if $s \in S$ and $q \in \beta S$. Therefore 3 holds and because λ_s extends l_s so does 1. The extension l_s is unique because continuous functions agreeing on a dense subspace are equal. This is the only possible definition of $*$ satisfying 1 and 3.

Now we can define $*$ on $\beta S \times \beta S$. Define $r_q : S \to \beta S$ by $r_q(s) = s * q$ for any $q \in \beta S$. There is a continuous function $\rho_q : \beta S \to \beta S$ such that $\rho_{q|S} =$r$_q$. Define $p * q = \rho_q(p)$ for $\rho \in \beta S \backslash S$ and $\rho_q(s) = r_q(s) = s * q$ if $s \in S$. So $\rho_q(p) = p * q$ for all $p \in \beta S$ and 2 holds. The extension ρ_q is unique just like l_s is unique and this is the only possible definition of $*$ satisfying 2.

□

The following definition follows immediately since λ_s and ρ_q are continuous for all $s \in S$ and $q \in \beta S$ respectively where $s, t \in S$. Operations on βS are distinguished in terms of limits.

Definition 3.2.2. Let $\cdot$ be a binary operation on a discrete space S.

1. If $s \in S$ and $q \in \beta S$, then $s \cdot q \lim_{t \to q} s \cdot t$.
2. If $p, q \in \beta S$, then $p \cdot q = \lim_{s \to p} (\lim_{t \to q} s \cdot t)$.

   This is equivalent to: If $p, q \in \beta S$, let $P \in p$ and $Q \in q$, then $p \cdot q = p - \lim_{s \in P} (q - \lim_{t \in Q} s \cdot t)$.

We now prove that βS is a semigroup if S is a semigroup by proving that the operation on βS is associative.

Theorem 3.2.3. *Let $(S, \cdot)$ be a semigroup. Then the extended operation on βS is associative.*

Proof:

Let $p, q, r \in \beta S$. Consider $\lim_{a \to p} \lim_{b \to q} \lim_{c \to r} (a \cdot b) \cdot c$, where $a, b, c \in S$. Then

$$\lim_{a \to p} \lim_{b \to q} \lim_{c \to r} (a \cdot b) \cdot c = \lim_{a \to p} \lim_{b \to q} (a \cdot b) \cdot r \qquad (\lambda_{a \cdot b} \text{ is continuous})$$

$$= \lim_{a \to p} (a \cdot q) \cdot r \qquad (\rho_r \circ \lambda_a \text{ is continuous})$$

$$= (p \cdot q) \cdot r. \qquad (\rho_r \circ \rho_q \text{ is continuous})$$

$$\lim_{a \to p} \lim_{b \to q} \lim_{c \to r} a \cdot (b \cdot c) = \lim_{a \to p} \lim_{b \to q} a \cdot (b \cdot r) \qquad (\lambda_a \circ \lambda_b \text{ is continuous})$$

$$= \lim_{a \to p} a \cdot (q \cdot r) \qquad (\lambda_a \circ \rho_r \text{ is continuous})$$

$$= p \cdot (q \cdot r). \qquad (\rho_{q \cdot r} \text{ is continuous})$$

We have that $(p \cdot q) \cdot r = p \cdot (q \cdot r)$ and so the operation $\cdot$ on βS is associative.

□

βS is a compact right topological semigroup by virtue of Theorem 3.2.1 and Theorem 3.2.3. If T is a right topological semigroup then denote $\Lambda(T) = \{x \in T : \lambda_x \text{ is continuous}\}$.

Definition 3.2.4. Let S be a semigroup and a topological space. A *semigroup compactification* of S is a pair (ϕ, T) where T is a compact right topological semigroup, $\phi : S \to T$ is a continuous homomorphism, $\phi[S] \subseteq \Lambda(T)$ and $\phi[S]$ is dense in T.

We now discuss commutativity in βS.

Theorem 3.2.5. *If $(S, \cdot)$ is a commutative semigroup, then S is contained in the center of $(\beta S, \cdot)$.*

Proof:
Let $s \in S$ and $p \in \beta S$. Then

$$\begin{aligned} s \cdot q &= \lim_{t \to q} st \\ &= \lim_{t \to q} ts \\ &= (\lim_{t \to q} t) \cdot s \qquad \text{since } \rho_s \text{ is continuous} \\ &= q \cdot s. \end{aligned}$$

□

Theorem 3.2.6. *Let S be a discrete commutative semigroup. Then the topological center of βS coincides with its algebraic center.*

Proof:
Let $p \in \Lambda(\beta S)$ and $q \in \beta S$. Since λ_p is continuous, then

$$\begin{aligned} p \cdot q &= q - \lim_{t \in S} (p \cdot t) \\ &= q - \lim_{t \in S} (t \cdot p) \\ &= q \cdot p \end{aligned}$$

So p is the topological and algebraic center of βS.

□

If S is a discrete semigroup then the operation of S extends uniquely to the Stone-Čech Compactification making βS a compact Hausdorff right topological semigroup with S contained in its topological center.

This means that for each $p \in \beta S$, the right translation $\rho_q : \beta S \ni x \mapsto xq \in \beta S$ is continuous. S is contained in its topological center means that for each $s \in S$, the left translation $\lambda_s : \beta S \ni x \mapsto sx \in \beta S$ is continuous.

M. Day [7] established the initial extension while P. Civin and B. Yood [6] established the operation on the Stone-Čech Compactification. The construction is: for each $s \in S$, the function $\eta_s : S \ni x \mapsto sx \in S$ extends continuously to another function $\bar{\eta_s} : \beta S \mapsto \beta S$. Define $s \circ q = \bar{\eta_s}(q)$ for each $s \in S$ and $q \in \beta S$.

For each $q \in \beta S$, the function $\gamma_q : S \ni x \mapsto xq \in \beta S$ extends continuously to another function $\bar{\gamma_q} : \beta S \mapsto \beta S$. Define $p \cdot q = \bar{\gamma_q}(p)$ for each $q \in \beta S$ and $p \in \beta S \backslash S$. For the extended operation $\lambda_s = \bar{\eta_p}$ and $\rho_q = \bar{\gamma_q}$, all right translations are continuous. R. Ellis (Theorem 3.1.15) introduced the extension of βS as the set of all ultrafilters [8].

βS has multiple applications in Ramsey Theory, specifically van der Waerden's Theorem and Hindman's Theorem. One of the reason's for this is that βS is the largest semigroup compactification of S. The first application of βS to Ramsey Theory was the proof of the Finite Sums Theorem (also known as Hindman's Theorem). The original proof was elementary yet very complicated.

Theorem 3.2.7. (Finite Sums Theorem). *Whenever* $\mathbb{N}$ *is finitely coloured, there is an infinite subset* $A \subseteq \mathbb{N}$ *such that all finite sums of distinct elements of* A *have the same colour* (N. Hindman, 1974).

F. Galvin and S. Glazer provided another proof of the Finite Sums Theorem in 1975 by means of an ultrafilter on $\mathbb{N}$ being an idempotent of $\beta\mathbb{N}$. This proof was short and elegant. Soon after this, new ultrafilter proofs of all the fundamental results in Ramsey Theory have been found using algebra $\beta\mathbb{N}$.

Chapter 4

Ramsey Theory

Ramsey Theory is named after Frank Plumpton Ramsey who made significant contributions to the fields of economics, philosophy and mathematics before his untimely death in 1930 at the age of twenty six. Ramsey only wrote two economics papers, one titled *A Mathematical Theory of Saving*, which the great economist John Maynard Keynes described as "one of the greatest contributions to mathematical economics ever".

Ramsey Theory is the study of the preservation of properties under set partitions. Results in Ramsey Theory have two characteristics. Firstly, a result may show that some structure exists yet the result gives no process for finding this structure. Secondly, a result may say that sufficiently large objects must necessarily contain a given structure. The sufficiently large structures usually have massive bounds which grow exponentially. There are several classical theorems in the field of Ramsey Theory, many of which we will prove using the algebraic structures set out in the preceeding chapters.

The oldest result is that of Hilbert in 1892 followed by Schur in 1916, van der Waerden in 1927 and Ramsey in 1928. Results from Chapter 4 can be found in [11], [18] and [23].

4.1 Ramsey's theorem

There are two versions of Ramsey's Theorem, namely the finite version and an extension of the finite version, the infinite version. Frank Ramsey proved the finite

version in 1928 yet it was only published in 1930 after his death in a paper titled *On a problem of formal logic* [25]. Ramsey's Theorem deals with colourings so let us formalize the definition of a colouring.

Definition 4.1.1. An *r-colouring* of the set of natural numbers is a function $\mathcal{X} : \mathbb{N} \to \{1, \ldots, r\}$.

We first prove the most general form of Ramsey's Theorem; the infinite version. Let $[\mathbb{N}]^k$ denote the family of all k-element subsets of the set of natural numbers.

Theorem 4.1.2. (Infinite Ramsey's Theorem). *Let k, r be natural numbers. For every colouring $\mathcal{X} : [\mathbb{N}]^k \to \{1, \ldots, r\}$, there exists an infinite subset $A \subseteq \mathbb{N}$ such that all its k-element subsets have the same colours.*

Proof:
Consider the case $k = 1$. This is an infinite version of the Pigeonhole principle. One element subsets are merely the elements of the set of natural numbers, of which there are an infinite number. Therefore, if we colour the set of natural numbers using r colours, there will be a colour that occurs an infinite number of times. The elements coloured by this colour represent the elements of our infinite set A and we are done.

Consider the case $k = 2$. We represent the elements of the set $[\mathbb{N}]^2$ as edges of a complete graph with $\mathbb{N}$ vertices. We denote this graph $K_{\mathbb{N}}$. Let the set of points $X_0 = \mathbb{N}$ and fix any point, say $x_0 \in X_0$. By the Pigeonhole principle, of the edges connecting the point x_0 with the points $X_0 \backslash \{x_0\}$, infinitely many have the same colour. Let this colour be r_0. Now let

$$X_1 = \{y \in X_0 \backslash \{x_0\} : \mathcal{X}(x_0, y) = r_0\}.$$

Again, fix any point, say $x_1 \in X_1$. By the Pigeonhole principle, the edges connecting the point x_1 with the points $X_1 \backslash \{x_1\}$, infinitely many edges have the same colour. Let this colour be r_1. Now let

$$X_2 = \{y \in X_1 \backslash \{x_1\} : \mathcal{X}(x_1, y) = r_1\}.$$

Continuing in this manner, we construct a sequence $E = \{x_0, x_1, x_2, \ldots\}$ such that for each edge $\{e, e'\}$ which connect the points of E, the colour of $\{e, e'\}$ depends only on $\min\{e, e'\}$. Let us define a new colouring $\mathcal{X}^*(e) = \mathcal{X}(\{e, e'\})$ where $e' > e$.

By the Pigeonhole principle, there is an infinite monochromatic subset A with respect to $\mathcal{X}$, i.e: $\mathcal{X}^*(a) = r \ \forall \ a \in A$. By our definition of $\mathcal{X}^*$ this means that all two element subsets of the infinite set A, where $A \subseteq E$, have the same colour with respect to $\mathcal{X}$.

Consider the case $k = 3$. Let the set of points $X_0 = \mathbb{N}$ and fix any point, say $x_0 \in X_0$. Any colouring $\mathcal{X} : [\mathbb{N}]^3 \to \{1, \ldots, r\}$ forms a colouring $\mathcal{X}_0$ of pairs from the set $X_0 \backslash \{x_0\}$ due to the rule $\mathcal{X}_0(i, j) = \mathcal{X}(x_0, i, j)$ where i, j are points of the set $X_0 \backslash \{x_0\}$. By our case of $k = 2$, the set $X_0 \backslash \{x_0\}$ contains an infinite subset X_1 such that $\mathcal{X}_0(i, j) = r_1$ for distinct $i, j \in X_1$.

Again, fix any point, say $x_1 \in X_1$ with $x_1 > x_0$. Any colouring $\mathcal{X} : [\mathbb{N}]^3 \to \{1, \ldots, r\}$ forms a colouring $\mathcal{X}_1$ of pairs from the set $X_1 \backslash \{x_1\}$ due to the rule $\mathcal{X}_1(i, j) = \mathcal{X}(x_1, i, j)$ where i, j are points of the set $X_1 \backslash \{x_1\}$. By our case of $k = 2$, the set $X_1 \backslash \{x_1\}$ contains an infinite subset X_2 such that $\mathcal{X}_1(i, j) = r_2$ for distinct $i, j \in X_2$.

Continuing in this manner, we construct a sequence $E = \{x_0, x_1, x_2, \ldots\}$ such that the colour of any three element subset $\{e, e', e''\}$ depends only on $\min\{e, e', e''\}$. Let us define a new colouring $\mathcal{X}^*(e) = \mathcal{X}(\{e, e', e''\})$ where $e'' > e' > e$. By the Pigeonhole principle, there is an infinite subset $A \subseteq E$ which is monochromatic with respect to $\mathcal{X}^*$. By our definition of $\mathcal{X}^*$ this means that all three element subsets of the infinite set A, where $A \subseteq E$, have the same colour with respect to $\mathcal{X}$. The same argument can be applied to any value of k.

□

The finite version can be considered as a refinement of the pigeonhole principle, where there is not only a certain number of pigeons in each pigeonhole, but also a certain relationship between the pigeons.

Theorem 4.1.3. (Finite Ramsey's Theorem). *Let k, r, l be natural numbers with $k \leq l$ and $[1, \ldots, n]^k$ be the family of all k-subsets of $\{1, \ldots, n\}$. There exists a natural number, known as the Ramsey number, $R(k, l, r)$ such that for every $n \geq R(k, l, r)$ and arbitrary colouring $\mathcal{X} : [1, \ldots, n]^k \to \{1, \ldots, r\}$, there exists an l-subset of the set $\{1, \ldots, n\}$ such that all of its k-subsets are monochrome.*

Proof:
Let the family of all k-element subsets from the set of natural numbers equal the

set X, i.e.: $X = [\mathrm{N}]^k$. Let $\mathfrak{U}$ represent the family of all k-element subsets from a set B, where B is a subset of $\mathbb{N}$ with cardinality l, i.e.: $\mathfrak{U} = \{[B]^k : B \subset \mathbb{N}, |B| = l\}$.

Consider the partition $X = A_1 \cup A_2 \cup \ldots \cup A_m$. By the Infinite Ramsey's Theorem, there exists an infinite subset $A \subseteq \mathbb{N}$ such that $[A]^k \subseteq A_i$ where A_i is a random subset of X. Choose an arbitrary subset B such that $B \subset A$. Then we have that $[B]^k \subseteq A_i$. Therefore $\mathfrak{U}$ is r-regular with respect to X and all subsets of $\mathfrak{U}$ are finite since they possess cardinality l.

By the Compactness Theorem for partitions, Theorem 2.2.5, there exists a finite subset $Y \subseteq [\mathbb{N}]^k$ such that the $\mathfrak{U}$ is r-regular with respect to Y. There exists a natural number $R(k, l, r)$ such that $Y \subseteq [1, \ldots, R(k, l, r)]^k$. Then the subset $[1, \ldots, n]^k$ is r-regular with respect to $\mathfrak{U}$ for all $n \geq R(k, l, r)$ and hence there exists an l-subset of the set $\{1, \ldots, n\}$ such that all of its k-subsets are monochrome.

□

An alternative version of the Finite Ramsey's Theorem is as follows:

Theorem 4.1.4. (Finite Ramsey's Theorem Restated). *For any given number of colours $r \in \mathbb{N}$ and $\{n_1, \ldots, n_r\} \in \mathbb{N}$, there is a natural number, known as the Ramsey number $R(n_1, \ldots, n_r; r)$, such that if the edges of a complete graph of order $R(n_1, \ldots, n_r; r)$ are coloured with r different colours, it must contain a complete subgraph of order n_i whose edges are all of colour $i \in r$.*

This version provides us with more practicality for an example and we will use its notation henceforth. There are a limited quantity of Ramsey numbers that have been discovered. For unknown Ramsey numbers, lower and upper bounds are generally computed, but these are usually over large intervals. Let us prove the example of $R(3, 3; 2)$:, i.e.: how many elements are required so that we guarantee either a 3 element red subgraph (triangle) or a 3 element blue subgraph (triangle)?

It is easier to use graph theory where vertices represent elements and edges represent relationships. If we have three vertices, it is possible to have a blue or red triangle, but not necessary. Vertices B and C may know each other but A may know neither. With four or five vertices it is still possible to colour the edges either red or blue without a monochromatic triangle. With six vertices it becomes impossible to colour

the edges without a red or blue monochromatic triangle.

Fix one vertex in a six element complete graph, say A. A has five edges connected to it. By the pigeonhole principle and without a loss of generality, A will have either three blue lines and two red lines or two blue lines and three red lines connected to it. Suppose A has three blue lines connected to B, C and D. Now of these three vertices, each pair can have a blue or red line connecting them. If the lines are all red, then we have a red monochromatic triangle between B, C and D. If any pair between B, C and D has a blue line, say B to C, then we also have a blue monochromatic triangle between A, B and C.

Below is a recent table of the known small Ramsey numbers and selected bounds for two colours [24].

n_1 \ n_2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	6	9	14	18	23	28	36	40 43	46 51	52 59	59 69	66 78	73 88
4		18	25	35 41	49 61	56 84	73 115	92 149	97 191	128 238	133 291	141 349	153 417
5			43 49	58 87	80 143	101 216	125 316	143 442	159 633	185 848	209 1139	235 1461	265 1878
6				102 165	113 298	130 495	169 780	179 1171	253 1804	262 2566	317 3705	5033	401 6911
7					205 540	216 1031	237 1713	289 2826	405 4553	416 6954	511 10581	15263	22116
8						282 1870	317 3583	6090	10630	16944	817 27490	41525	861 63620
9							565 6588	580 12677	22325	39025	64871	89203	
10								798 23556		81200			1265

Upper and lower bounds on $R(n_1, n_2; 2)$

The only known Ramsey number for multiple colours is $R(3, 3, 3; 3) = 17$.

4.2 Schur's theorem

One of the earliest results in the field is credited to Issai Schur in 1916 [30]. He was oddly motivated by the most famous of mathematical problems, Fermats Last Theorem which was only proved in 1995. Consider the points in the simple plane $x+y=z$ and use any finite set of colours to assign a colour to each positive integer. If $x+y=z$ are all the same colour, then colour the point in the plane. Our question is whether it is possible to colour the positive integers so that no point in the plane is coloured. The answer is no, there must be a coloured point.

Theorem 4.2.1. (Infinite Schur's Theorem). *For every colouring $\mathcal{X} : [\mathbb{N}] \to \{1, \ldots, r\}$ of the set of natural numbers into m colours, the equation $x+y=z$ has a monochromatic solution.*

Proof:
Define the colouring $\mathcal{X}^* : [\mathbb{N}]^2 \to \{1, \ldots, r\}$ by the rule

$$\mathcal{X}^*\{i, j\} = \mathcal{X}(|i - j|).$$

By the Infinite Ramsey's Theorem, there exists an infinite set A such that $A \subseteq \mathbb{N}$ and $\mathcal{X}^*\{i, j\} = \textit{constant}$ for all distinct elements $i, j \in A$. Now choose three elements $i, j, k \in A$ where $i < j < k$. Then we have that the two-element subsets all have the same colour, i.e.:

$$\mathcal{X}^*\{i, j\} = \mathcal{X}^*\{j, k\} = \mathcal{X}^*\{i, k\}.$$

But since $(j - i) + (k - j) = (k - i)$, the solution of $x + y = z$ is monochromatic.

□

Theorem 4.2.2. (Finite Schur's Theorem). *There exists a least positive integer $S(r)$ with $S(r) \leq n$, and an arbitrary colouring $\mathcal{X} : \{1, \ldots, n\} \to \{1, \ldots, r\}$ such that the equation $x + y = z$ has a monochromatic solution in the set $\{1, \ldots, n\}$.*

Proof:
Consider the family $\mathfrak{V}$ of distinct natural numbers i, j, k satisfying $i + j = k$. By the Infinite Schur Theorem, $\mathfrak{V}$ is r-regular with respect to $\mathbb{N}$. By the Compactness Theorem for partitions, Theorem 2.2.5, $\mathfrak{V}$ is also r-regular with respect to some finite subset $Y \subseteq \mathbb{N}$.

We can take $S(r)$ as a natural number such that $Y \subseteq \{1, \ldots, S(r)\}$. This means that there exists a monochrome solution of $x + y = z$ for an r-colouring on the interval $\{1, \ldots, S(r)\}$.

□

On the set of integers, the numbers $S(r)$ are called the Schur numbers. As an example, take the case $S(2)$. We would like to find the least positive integer n so that whenever $[1, n]$ is two coloured, there will exist x, y, z (not necessarily distinct), so that $x + y = z$. $S(2)$ must be greater than four, because a two-colouring of four integers will not yield a monochromatic $x + y = z$. Two-colouring the interval $[1, 5]$ does yield a monochromatic $x + y = z$, and we can show why.

Assume the two-colouring of the interval $[1, 5]$ does not yield a monochromatic $x + y = z$. $1 + 1 = 2$ so colour 1 red and 2 blue. $2 + 2 = 4$ so colour 4 red. $1 + 4 = 5$ so colour 5 blue. Now we must colour 3, but whether 3 is red or blue makes no difference as there will always be a monochromatic $x + y = z$ on $[1, 5]$. Therefore $S(2) = 5$.

The only known Schur numbers are $S(1) = 2$, $S(2) = 5$, $S(3) = 14$ and $S(4) = 44$.

4.3 Hindman's theorem

Suppose the natural numbers are coloured with n different colours with each number coloured only once. By this colouring there exists a colour c which is used an infinite amount of times creating an infinite set. Then every finite sum over the infinite set also has colour c. The finite sums of a set I are all those numbers that can be obtained by adding up the elements of some finite nonempty subset of I. This is known as Hindman's Theorem and the set of all finite sums over I is denoted $FS(I)$.

Let $\langle a_n \rangle$ be an infinite sequence of elements of the semigroup S. The notation FP represents "finite products" and FS represents "finite sums" depending on whether the binary operation on S is $\cdot$ or $+$ respectively.

We denote $FP\langle a_n\rangle$ as the collection of elements of the semigroup having the form $\prod_{n=1}^{r} a_n$ and $FS\langle a_n\rangle$ as the collection of elements of the semigroup having the form $\sum_{n=1}^{r} a_n$.

A subset A of S is an FP-set if there exists an infinite sequence $\langle a_n\rangle$ of distinct elements from A such that $FP\langle a_n\rangle \subseteq A$. Alternatively, if the operation is commutative then it is called an FS-set.

Lemma 4.3.1. *If a non-principal ultrafilter p on the semigroup S is an idempotent of the semigroup βS, then any subset $A \in p$ is an FP-set.*

Proof:
Let $A_0 = A$. Since p is idempotent we have that $pp = p$ on βS. We also know that $p \in A_0 = \{p \in \beta S : A \in p\}$. By continuity of multiplication with respect to the second argument there exists a subset $B \in p$, $B \subseteq A_0$, such that $p\bar{B} \subseteq \bar{A}_0$.

Now select an arbitrary element, say $a_1 \in B \in p$. Now, since $pa_1 \in \bar{A}_0$ and $a_1 \in S$, there naturally exists a subset of A_0 which does not contain the element a_1. Let this set be A_1. So now $a_1 \in A_0 \backslash A_1$.

Select another arbitrary element, say $a_2 \in A_1 \in p$. Again, there naturally exists a subset $A_2 \in p$ which does not contain a_2. Continuing this process we can construct a sequence $\langle a_n\rangle$ and decreasing subsets $A_0 \supseteq A_1 \supseteq \ldots \supseteq A_n \supseteq \ldots$ such that the element a_n is contained in $A_{n-1} \backslash A_n$ for all $n \in \mathbb{N}$. All elements of $\langle a_n\rangle$ are distinct and $FP\langle a_n\rangle \subseteq A$.

□

Theorem 4.3.2. (Hindman's Theorem for semigroups). *Suppose an infinite semigroup S is either a semigroup without idempotents or a right cancellative semigroup. Then for every finite partition $S = A_1 \cup \ldots \cup A_r$ at least one of the elements of the partition is an FP-set.*

Proof:
By Lemma 4.3.1, it is sufficient to prove the existence of a free ultrafilter on S which is an idempotent of the semigroup βS. Suppose S contains no idempotent. By Theorem 3.1.15, there exists an idempotent element p of the semigroup βS. By

the condition, the ultrafilter p cannot be principal and consequently, $p \in \beta S \backslash S$.

Now let S be a right cancellative semigroup. We know that $\beta S \backslash S$ is a closed subsemigroup of the semigroup βS. Applying Theorem 3.1.15 to $\beta S \backslash S$ we find an idempotent $p \in \beta S \backslash S$.

□

From Hindman's Theorem for semigroups it follows that for every partition $\mathbb{N} = A_1 \cup \ldots \cup A_r$ there exists an FS-set A_i and an FP-set A_j. The following theorem, Hindman's Theorem for natural numbers, shows that i and j can be equal.

Theorem 4.3.3. (Hindman's Theorem for natural numbers). *For every partition of the natural numbers $\mathbb{N} = K_1 \cup K_2 \cup \ldots \cup K_r$ there exists a subset K_i which is an FS-set and an FP-set.*

Proof:
Let J be the family of all ultrafilters on the set of natural numbers $\mathbb{N}$ such that all of its elements form an FS-set. By Lemma 4.3.1, J contains all idempotents of the semigroup $\beta(\mathbb{N}, +)$ and $J \neq \emptyset$. J is also a closed subset in the semigroup $\beta\mathbb{N}$.

We show that J is a right ideal of the semigroup $\beta(\mathbb{N}, \cdot)$. Let $p \in J$ and $q \in \beta\mathbb{N}$. We fix a random subset $K \in pq$, then we choose a subset $Q \in q$ such that $p\bar{Q} \subseteq \bar{K}$. Now select a random element $a \in Q \in q$. Now $pa \in \bar{K}$, and therefore there exists a subset $P \in p \in J$ such that $P_a \subseteq K$. Since $p \in J$, P is also an FS-set, and there exists an infinite sequence $\langle a_n \rangle$ of distinct elements from P such that $FS\langle a_n \rangle \subseteq P$. Also, $Pa \subseteq K$ and this implies that K is an FS-set aswell. We stated that $K \in pq$ and can conclude that $pq \in J$, the family of all ultrafilters on $\mathbb{N}$.

So we have that J is a right ideal and also a subsemigroup of $\beta(\mathbb{N}, \cdot)$ since $J \subseteq \beta\mathbb{N}$. By Theorem 3.1.15, J contains an idempotent p of $\beta(\mathbb{N}, \cdot)$ and by definition, J contains non-principal (free) ultrafilters. It therefore follows from the previous lemma that every subset $K \in p$ is an FP-set. So now every subset K is both a FP-set and a FS-set. Now we choose a subset K_i of $\mathbb{N} = K_1 \cup K_2 \cup \ldots \cup K_r$ that is an element of the ultrafilter p and we are done.

□

4.4 van der Waerden's theorem

Ramsey's Theorem was preceeded by three other theorems all dealing with colouring of the integers. van der Waerden's Theorem was an unexpected result when proved by the Dutch mathematician, Bartel Leendert van der Waerden, in 1927 in the paper *Beweis einer Baudetschen Vermutung* [34]. The theorem states that if the positive integers are partitioned into a finite number of subsets then at least one of the subsets must contain arbitrarily long arithmetic progressions. Alternatively, on the set of integers, it states that for any given colouring of the positive integers, monochromatic arithmetic progressions cannot be avoided.

An arithmetic progression (AP) is a sequence in which each term (except the first) differs from the previous one by a constant amount. An n-term AP is of the form $a, a+d, a+2d, \ldots, a+(n-1)d$, where $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Note that the existence of arbitrarily long arithmetic progressions does not imply that infinitely long monochromatic arithmetic progressions exist, only that for a finite number k we can find monochromatic arithmetic progressions of length k. Arithmetic progressions provide us with a very well organised structure.

Let S be the Tychonoff product of r copies of the semigroup $\beta(\mathbb{N}, +)$ where r is a natural number. We represent the elements of S as vectors, i.e.: $\vec{p} = (p_1, \ldots, p_r)$. Note that S is a compact left topological semigroup with respect to the addition of vectors. Let

$$E^* = \{(a, a+d, \ldots, a+(r-1)d) : a \in \mathbb{N}, d \in \mathbb{N} \cup 0\},$$
$$\mathrm{I}^* = \{(a, a+d, \ldots, a+(r-1)d) : a \in \mathbb{N}, d \in \mathbb{N}\}.$$

Let E and I be the closures in the semigroup S of the subsets E^* and I^* respectively.

Lemma 4.4.1. *E is a subsemigroup of S and I is an ideal of the semigroup E.*

Proof:
Let $\vec{p} = (p_1, \ldots, p_r)$ and $\vec{q} = (q_1, \ldots, q_r)$ where $\vec{p}, \vec{q} \in E$. Take an arbitrary neighbourhood of $\vec{p} + \vec{q}$, say $V_1 \times \ldots \times V_r$. Using the continuity of the addition with respect to the second argument, we can choose a neighbourhood $U_1 \times \ldots \times U_r$ of $\vec{q}$ such that

$$\vec{p} + (U_1 \times \ldots \times U_r) \subseteq V_1 \times \ldots \times V_r.$$

Now choose $a \in \mathbb{N}, d \in \mathbb{N} \cup \{0\} (d \in \mathbb{N}$ if $q \in I)$ such that

$$(a, a+d, \ldots, a+(r-1)d) = \vec{x} \text{ where } \vec{x} \in U_1 \times \ldots \times U_r.$$

Since $\vec{p} + \vec{x} \in V_1 \times \ldots \times V_r$ and $a, a+d, \ldots, a+(r-1)d \in \mathcal{N}$, there exists a neighbourhood $W_1 \times \ldots \times W_r$ of $\vec{p}$ such that

$$(W_1 \times \ldots \times W_r) + \vec{x} \subseteq V_1 \times \ldots \times V_r.$$

Again, choose $b \in \mathbb{N}, e \in \mathbb{N} \cup \{0\} (e \in \mathbb{N}$ if $p \in I)$ such that

$$(b, b+e, \ldots, b+(r-1)e) = \vec{y} \text{ where } \vec{y} \in W_1 \times \ldots \times W_r.$$

Then $\vec{y} + \vec{x} \in V_1 \times \ldots \times V_r$. Now

$$\vec{y} + \vec{x} = (a+b, a+b+d+e, \ldots, a+b+(r-1)(d+e)).$$

Therefore, $\vec{y} + \vec{x} \in E^*$ and if either $\vec{p} \in I$ or $\vec{q} \in I$, then we have $\vec{y} + \vec{x} \in I^*$.

□

Lemma 4.4.2. *If $p \in \beta\mathbb{N}$ and $\vec{p} = (p, \ldots, p)$ then $\vec{p} \in E$.*

Proof:
Let $\vec{p}$ have the arbitrary neighbourhood $U_1 \times \ldots \times U_r$. $U = U_1 \cap \ldots \cap U_r$ is a neighbourhood of the element p. Now choose an arbitrary element $a \in \mathbb{N} \cap U$ and we get $(a, \ldots, a) \in (U_1 \cap \ldots \cap U_r) \cap E^*$.

□

Lemma 4.4.3. *If R be is a minimal right ideal of $\beta(\mathbb{N}, +)$ with $p \in R$ and $\vec{p} = (p, \ldots, p)$, then $\vec{p} \in I$.*

Proof:
By Theorem 3.1.16 there exists a minimal right ideal, say F, in the right ideal $\vec{p} + E$ of the semigroup E. Again, by Theorem 3.1.16, F is a closed subsemigroup of E and contains an idempotent $\vec{q} \in F$. Since $\vec{q} \in \vec{p} + E$, we can say that $\vec{q} = \vec{p} + \vec{r}$ for some element $\vec{r} \in E$.

Let $\vec{q} = (q_1, \ldots, q_r)$ and $\vec{r} = (r_1, \ldots, r_r)$. Then $q_i = p + r_i \in p + \beta\mathbb{N}$. Since R is a minimal right ideal of $\beta\mathbb{N}$ and $p \in R$, we get

$$R = p + \beta\mathbb{N} = q_i + \beta\mathbb{N}.$$

Now choose an element $t_i \in \beta\mathbb{N}$ such that $q_i + t_i = p$. Then $q_i + q_i + t_i = q_i + t_i = p$. Consequently, $\vec{q} + \vec{p} = \vec{p}$ and $\vec{p} \in F$.

We now need to show that $F \subseteq I$. Since $FI \subseteq F$ and $FI \subseteq I$, we have $FI \subseteq F \cap I$. Consequently, $F \cap I \neq \emptyset$ and since I is an ideal and F a right ideal, we see that $F \cap I$ is a right ideal of the semigroup E and by minimality of F, $F \subseteq I$.

□

Theorem 4.4.4. *If R is a minimal right ideal of $\beta(\mathbb{N}, +)$ where $p \in R$, then every subset $A \in p$ contains arbitrarily long arithmetic progressions.*

Proof:
Fix a natural number, say r and consider the element $\vec{p} = (p, \ldots, p)$ and its neighbourhood $\bar{A} \times \ldots \times \bar{A}$. By the Lemma 4.4.3 there exists $x \in I^* \cap (\bar{A} \times \ldots \times \bar{A})$. Then $\vec{x} = (a, a + d, \ldots, a + (r-1)d)$ where $a, d \in \mathbb{N}$, while $(a, a + d, \ldots, a + (r-1)d) \in A$.

□

Theorem 4.4.5. (Infinite van der Waerden's Theorem). *If the set of natural numbers is partitioned into a finite number of subsets then at least one of the subsets contains arbitrarily long arithmetic progressions.*

Proof:
By Theorem 3.1.16, the semigroup $\beta\mathbb{N}$ contains minimal right ideals. Suppose one of them is R. Select an ultrafilter $p \in R$ and a subset of the partition being an element of p. Apply Theorem 4.4.4 and we are done.

□

Theorem 4.4.6. (Finite van der Waerden's Theorem). *For all $k, r \in \mathbb{N}$ there exists a unique number, known as the van der Waerden number $w = w(r, k)$, satisfying the condition: if $n \geq w$ and $\{1, \ldots, n\} = \{A_1, \ldots, A_r\}$ then the subset A_i contains an arithmetic progression of length k.*

The finite version of van der Waerden's Theorem can be explained in terms of colourings. There exists a least positive integer, known as the van der Waerden number, $w = w(r, k)$, such that for every r-colouring of $[1, n]$ there is a monochromatic arithmetic progression of length k.

Proof:
Consider the family $\mathfrak{U}$ of all k-subsets of $\mathbb{N}$ that are arithmetic progressions. By the Infinite version of van der Waerden's Theorem $\mathfrak{U}$ is r-regular with respect to $\mathbb{N}$. By the Compactness Theorem for partitions, Theorem 2.2.5, $\mathfrak{U}$ is r-regular with respect to a finite subset $Y \subset \mathbb{N}$. The required number $w = w(r, k)$ can be determined by the condition $Y \subseteq \{1, \ldots, w(r, k)\}$.

□

Van der Waerden numbers are notoriously difficult to calculate. Let us prove the example of $w(2, 3)$. This is equivalent to saying that every two colouring of $[1, w(2, 3) = n]$ yields a monochromatic arithmetic progression of length three. We must find $w(2, 3)$ which is proved by elimination until the desired property is satisfied.

Case 1: Lower bound Prove $w \geq 9$. We must show that a two colouring of the interval $[1, 8]$ yields an instance where there is no monochromatic three term AP. This is easily illustrated as follows: colour 2,3,6,7 red and 1,4,5,8 blue. This avoids any three term monochromatic AP. We could alternatively coloured 2,3,6 red and 1,4,5,7,8 blue still providing no monochromatic three term AP. Of course, we could of coloured 1,2,3,4 red and 5,6,7,8 blue having monochromatic three term AP for both colours. These are all wrong since a lower bound states that we only need one instance where there is no monochromatic three term AP for a number to be a lower bound. We therefore have $w \geq 9$.

Case 2: Upper bound Prove $w \leq 9$. We must show that every two colouring of the interval $[1, 9]$ allows monochromatic three term AP's. Let us prove this by contradiction. Assume there exists a two colouring of $[1, 9]$ with no monochromatic three term AP. Let us find this colouring. Consider the integers 4 and 6. Can they both be coloured red? If 4 and 6 are coloured red then 2 must be blue since 2,4,6 cannot be monochromatic. 5 and 8 must also be blue since 4,5,6 and 4,6,8 cannot

be monochromatic. But now 2,5,8 are all blue, a monochromatic three term AP. Therefore 4 and 6 must be different colours. Similarly neither 5 and 7 nor 3 and 5 cannot have the same colour.

Assume the colour of 3 is red. We then only have two options for the colourings of 3,4,5,6,7 namely $\mathcal{X}_1$ = red,blue,blue,red,red or $\mathcal{X}_2$ = red,red,blue,blue,red. If $\mathcal{X}_1$ is the colouring of 3,4,5,6,7 then 8 must be blue due to 6,7,8 and 9 must be blue due to 3,6,9. 1 must be red due to 1,5,9 and hence 2 must be blue due to 1,2,3. But now 2,5,8 are blue, an unavoidable monochromatic three term AP and a contradiction. If $\mathcal{X}_2$ is the colouring of 3,4,5,6,7 then 2 must be blue due to 2,3,4 and 8 must be red due to 2,5,8. 9 must be blue due to 7,8,9 and hence 1 must be red due to 1,5,9. But now 1,4,7 are red, an unavoidable monochromatic three term AP and a contradiction. Therefore, every two colouring of $[1, 9]$ yields a three term monochromatic AP and we have $w \leq 9$.

So $w \geq 9$ and $w \leq 9$. Therefore $w(2, 3) = 9$, the least positive integer that enables us to have a monochromatic three term arithmetic progression using two colours.

Besides this example, other van der Waerden numbers known are $w(3, 3) = 27$, $w(4, 3) = 76$, $w(2, 4) = 35$, $w(2, 5) = 178$ and $w(2, 6) = 1132$. Trivially, $w(r, 1) = 1$, $w(r, 2) = r + 1$ and $w(1, k) = k$.

We use the notation $a \uparrow b$ for a^b with evaluation proceeding from the right, i.e.: $a \uparrow b \uparrow c = a \uparrow (b \uparrow c)$. General upper bounds for $w(r, k)$ are:

1. For $k \geq 2$ and $r = 2$ [10],

$$w(2, k) \leq 2 \uparrow 2 \uparrow 2 \uparrow 2 \uparrow 2 \uparrow (k + 9).$$

2. For $k = 3$ and $r \geq 5$ [13],

$$w(r, 3) < \left(\frac{r}{4}\right)^{3^r}.$$

Chapter 5

Compact groups

A subset C of P is called a chain if $a, b \in C$ implies either $a \leq b$ or $b \leq a$. The element $u \in P$ is an upper bound for C if $c \leq u$ for all $c \in C$, and P is called inductive if every chain in P has an upper bound in P [9].

In the case of multiplicative groups we abbreviate $a * b$ to ab and e to 1 and in the case of additive groups $a * b$ to $a + b$ and e to 0. We will use additive notation for our groups. Abelian groups are commutative groups, i.e.: $a + b = b + a \; \forall \; a, b \in A$. A group A is divisible if there is $x \in A$ such that $nx = a$ for all $a \in A$ and $n \in \mathbb{N}$. Examples of divisible groups are the sets of real and rational numbers. A group is never empty since it contains a zero.

The order of group A is denoted $|A|$ and is the number of elements in a group. The order of an element $a \in A$ is the least positive integer n such that $na = 1$. A subset B of A is a subgroup, denoted $B \leqq A$, if and only if $a, b \in B$ implies $a + b \in B$ and $a \in B$ implies $-a \in B$. A subgroup of A always contains the zero of A. By Lagrange's theorem, $|B|$ is a divisor of $|A|$. Trivial subgroups are A and $\{0\}$ while all other subgroups are called proper subgroups.

A group A is a torsion group if every element of A is of finite order and torsion free if every element except 0 are of infinite order. A group A is a cyclic group if the group is generated by a single element, say a. A group A is a primary group if the orders of its elements are powers of a fixed prime p.

Results in Chapter 5 can be found in [9], [16], [28] and [35]. We now introduce

a normal subgroup. These are subgroups that are invariant under conjugation by members of the group.

Definition 5.0.7. A subgroup S of G is a *normal subgroup* of G, denoted $S \lhd G$, if aSa^{-1}=S for all $a \in G$ ($S \lhd G \leftrightarrow \forall\ s \in S, a \in G, aSa^{-1} \in S$).

Examples of normal subgroups are: a center of a group, the subgroup consisting of only the identity element (trivial subgroup) and the subgroup consisting of the entire group.

If $B \leqq A$ and $a \in A$, the set $a + B = \{a + b \mid b \in B\}$ is called a left coset of A modulo B while $B + a = \{b + a \mid b \in B\}$ is called a right coset of A modulo B. Let us examine an example in order to identify the properties of cosets. Take the multiplication table for the known group $G = S_3$. The six elements of S_3 may be denoted by $\{e, b, b^2, a, ab, ab^2\}$ where

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

$$b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132),$$

$$b^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123),$$

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12),$$

$$ab = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13),$$

$$ab^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23).$$

We can compute that $e = a^2 = b^3$ and $ba = ab^2$. For example $ba := b \circ a = (12) \rightarrow (132)$ which is equivalent to $(23) = ab^2$. From these relations we can complete the multiplication table of S_3:

$\circ$	e	b	b^2	a	ab	ab^2
e	e	b	b^2	a	ab	ab^2
b	b	b^2	e	ab^2	a	b
b^2	b^2	e	b	ab	ab^2	a
a	a	ab	ab^2	e	b	b^2
ab	ab	ab^2	a	b^2	e	b
ab^2	ab^2	a	ab	b	b^2	e

If $B = \langle a \rangle = \{1, a\}$, then the right cosets of H in S_3 are:

$$B = \{1, a\}, Bb = \{b, ab\}, Bb^2 = \{b^2, ab^2\},$$

and the left cosets are:

$$B = \{1, a\}, bB = \{b, ba\} = \{b, ab^2\}, b^2B = \{b^2, ab\}.$$

From this example we can conclude that:

1. all elements of S_3 are contained in both the right and left cosets;
2. any two right (or left) cosets are either equal or disjoint;
3. the number of right cosets equals the number of left cosets;
4. right cosets are different from left cosets.

The index, denoted $|A : B|$, is the number of left (or right) cosets of B in A. The cosets of A mod B form a group A/B known as a quotient or factor group. Normal subgroups can be used to construct quotient groups from a given group. The zero element of A/B is B and the inverse of a coset C is $-C$. A/B is a proper quotient group of A if $B \neq 0$.

A map $\alpha : A \to B$ is a homomorphism (structure preserving) of A onto B if it preserves addition, i.e.: $\alpha(a_1 + a_2) = \alpha a_1 + \alpha a_2$ for all $a_1, a_2 \in A$. Every homomorphism gives rise to two subgroups, namely the kernel and the image. The kernel of α is the set $\mathrm{Ker}(\alpha) = \{a \in A \mid \alpha(a) = 0\}$ while the image of α is the set $\mathrm{Im}(\alpha) = \{b \in B \mid \alpha(a) = b \text{ for some } a \in A\}$.

Proof that Ker$(\alpha) \leqq A$:
We know that $\mathrm{Ker}(f)$ is nonempty since it contains 0.
If $\alpha(a) = 0$, then $\alpha(a^{-1}) = \alpha(a)^{-1} = 0$.
If $\alpha(a) = 0 = \alpha(b)$, then $\alpha(ab) = \alpha(a) + \alpha(b) = 0 + 0 = 0$.
So $\mathrm{Ker}(\alpha) \leqq A$.

Proof that Im$(\alpha) \leqq A$:
If $\alpha(a) \in A$, then $a \in A$ and so $a^{-1} \in A$. Since G is a group, there exists the identity element $e_A \in A$ and $\alpha(e_A) = e_B$. Now $\alpha(a^{-1}) \in \alpha(A)$ and $\alpha(a)\alpha(a^{-1})$=$\alpha(aa^{-1})$=$\alpha(e_A) = e_B$. So $a \in \mathrm{Im}(\alpha)$ implies $a^{-1} \in \mathrm{Im}(\alpha)$.
If $\alpha(a), \alpha(b) \in \alpha(A)$, then $\alpha(a)\alpha(b) = \alpha(ab) \in \alpha(A)$ since $a, b \in G \to ab \in A$. So $a, b \in \mathrm{Im}(\alpha)$ implies $ab \in \mathrm{Im}(\alpha)$.

□

If $\mathrm{Im}(\alpha) = B$, α is said to be surjective and we say α is an epimorphism. If $\mathrm{Ker}(\alpha) = 0$, α is said to be injective and we say α is a monomorphism. An automorphism is an isomorphism from an object to itself. If both $\mathrm{Ker}(\alpha) = 0$ and $\mathrm{Im}(\alpha) = B$, then α is one-to-one between A and B (i.e.: bijective), and we call α an isomorphism between A and B. Two groups are isomorphic (structurally identical), denoted $A \cong B$, if there is an isomorphism $\alpha : A \to B$. In this case the inverse mapping α^{-1}: B $\to A$ exists and is also an isomorphism.

The Kernel and Image are useful to describe the relationship between quotient groups, homomorphisms and subgroups. The following theorem says that there is no significant difference between a quotient group and a homomorphic image.

Theorem 5.0.8. (First Isomorphism Theorem). *Let $\alpha : A \to B$ be a homomorphism with* $\mathrm{Ker}(\alpha) = K$. *Then K is a normal subgroup of G and $G/K \cong \mathrm{Im}(\alpha)$.*

Proof:
We know that K is a subgroup of G. To see that K is a normal subgroup, we must show $aKa^{-1} \subset K$ for every $a \in A$.

$$\begin{aligned}
\alpha(aKa^{-1}) &= \alpha(a)\ \alpha(K)\ \alpha(a)^{-1} && \alpha \text{ is a homomorphism} \\
&= \alpha(a)\ 1_H\ \alpha(a)^{-1} && \text{definition of } K \\
&= 1_H
\end{aligned}$$

Hence aKa^{-1} is in K. Therefore K is a normal subgroup of G and G/K is well defined. To prove the theorem we will define a map from G/K to the image of α and show that it is a function, a homomorphism and an isomorphism.

Let $\theta : G/K \to \mathrm{Im}(\alpha)$ be a map that sends the coset aK to $\alpha(a)$. Since θ is defined on representatives we need to show that it is well defined. Let a_1 and a_2 be elements of G that belong to the same coset. Then $a_1^{-1}a_2$ is an element of K and $\alpha(a_1^{-1}a_2) = 1$ since K is the kernel of G. The rules of homomorphism show that $\alpha(a_1)^{-1}\alpha(a_2) = 1$ which is equivalent to $\alpha(a_1) = \alpha(a_2)$ which implies $\theta(a_1K) = \theta(a_2K)$. We now show that θ is a homomorphism,

$$\begin{aligned}
\theta(a_1K \cdot a_2K) &= \theta(a_1a_2K) \\
&= \alpha(a_1a_2K) \\
&= \alpha(a_1)\alpha(a_2) \\
&= \theta(a_1K)\theta(a_2K).
\end{aligned}$$

We now show that θ is an isomorphism. The kernel of θ consists of all cosets aK in G/K such that $\alpha(a) = 1$. These are exactly the elements a that belong to K so only the coset K is in the kernel of θ. This implies that θ is an injection. Let c be an element of $\mathrm{Im}(\alpha)$ and a is pre-image. Then $\theta(aK) = \alpha(a)$ and $\theta(aK) = c$. Therefore θ is surjective. So θ is an isomorphism and the theorem is proved.

□

5.1 Direct sums

Direct sums allow us decompose complicated groups into simpler individual parts. If a group can be broken down into these simpler parts, the group can be studied by investigating each component of the direct sum. We can also construct new groups from the direct sums of known groups. Almost all structure theorems on Abelian groups involve decomposition.

Definition 5.1.1. Let B_i be a family of subgroups of A satisfying:

1. $\sum B_i = A$;
2. $B_i \cap \sum_{j \neq i} B_j = 0$ for every $i \in I$ where $I = \{1, \ldots, n\}$.

Then A is said to be the *direct sum* of its subgroups B_i, denoted:

$$\mathrm{A} = \bigoplus_{i \in I} \mathrm{B}_i.$$

Each B_i is referred to as a direct summand of A. Every $a \in A$ can be written in the unique form $a = b_{i_1} + \ldots + b_{i_k}$ with $b_{i_j} \neq 0$ belonging to different components $B_{i_j} (j = 1, \ldots, k)$. The maps

$$\pi := a \mapsto b \text{ and } \theta : a \mapsto c$$

are epimorphisms ($\mathrm{Im}(\alpha) = B$ and $\mathrm{Im}(\alpha) = C$). Since $\pi b = b, \theta c = c, \pi c = 0, \theta b = 0, \pi a + \theta a = a$ and $\pi b + \theta b = b$, the endomorphisms (a homomorphism into itself) π, θ of A satisfy

$$\pi^2 = \pi, \theta^2 = \theta, \theta\pi = \pi\theta = 0, \pi + \theta = 1_A. \tag{5.1}$$

We know that each B_i is referred to as a direct summand of A. If there is a subgroup C of A such that $A = B \oplus C$ then C is a complementary direct summand or a complement of B in A. Some properties of direct summands are:

1. If $A = B \oplus C$, then $C \cong A/B$. Thus the complement of B in A is unique up to isomorphism (it possesses a trivial automorphism group);
2. If $A = B \oplus C$ and if D is a subgroup of A containing B, then $D = B \oplus (D \cap C)$;

3. If $A = B \oplus C$ and $a = b + c$ with $a \in A, b \in B, c \in C$, then $o(a)$ is the least common multiple of $o(b)$ and $o(c)$;

4. If $A = \oplus_i B_i$ and if for every i, $C_i \leqq B_i$ then $\sum C_i = \oplus C_i$. This is a proper subgroup if A if $C_i < B_i$ for at least one i;

5. If $A = \oplus_i B_i$, where each B_i is a direct sum, $B_i = \oplus_j B_{ij}$, then $A = \oplus_i \oplus_j B_{ij}$, called a refinement of the first decomposition of A;

6. If $A = \oplus_i \oplus_j B_{ij}$, then $A = \oplus_i B_i$ with $B_i = \oplus_j B_{ij}$.

Two direct decompositions of A, $A = \oplus_i B_i$ and $A = \oplus_j C_j$ are called isomorphic if we can find a one-to-one correspondence between B_i and C_j such that the corresponding components are isomorphic.

Given the groups B and C, we would like to have a group A that is the direct sum of two of its subgroups, B' and C', such that $B' \cong B$ and $C' \cong C$. The set of all pairs of $b \in B$ and $c \in C$ forms a group A under the rules:

1. $(b_1, c_1) = (b_2, c_2)$ if and only if $b_1 = b_2$ and $c_1 = c_2$;

2. $(b_1, c_1) + (b_2, c_2) = (b_1 + b_2, c_1 + c_2)$.

The correspondences $b \mapsto (b, 0)$ and $c \mapsto (c, 0)$ are isomorphisms of B, C with subgroups B', C' of A. We have $A = B' \oplus C'$ and if we think of B, C as being identified with B', C' under the above isomorphisms, then $A = B \oplus C$ and we call A the external direct sum of B and C.

An important application of direct sums is the following theorem.

Theorem 5.1.2. *A torsion group A is the direct sum of primary groups A_p belonging to different primes p. The A_p are uniquely determined by A.*

Proof: Let A_p consist of all $a \in A$ whose order is a power of the prime p. In view of $0 \in A_p$, A_p is nonempty. If $a, b \in A_p$, i.e.: $p^m a = p^n b = 0$ for integers $m, n \geq 0$, then $p^{max(m,n)}(a - b) = 0, a - b \in A_p$, and A_p is a subgroup. Every element in $A_{p_1} + \ldots + \mathrm{A}_{p_k}$ is cancelled by a product of powers of $p_1, \ldots, p_k$ and so

$$A_p \cap (A_{p_1} + \ldots + A_{p_k}) = 0 \text{ when } p \neq p_1, \ldots, p_k.$$

Therefore the A_p generate by their direct sum $\oplus_p A_p$ in A. To show that every $a \in A$ lies in this direct sum, let $o(a) = m = p_1^{r_1} \ldots \mathrm{p}_n^{r_n}$ with different primes p_i. The numbers $m_i = mp_i^{-r_i}$ where $i = 1, \ldots, n$ are relatively prime (gcd=1), and hence there are integers $s_1, \ldots, s_n$ such that $s_1 m_1 + \ldots s_n m_n = 1$. Thus $a = s_1 m_1 a + s_n m_n a$ where $m_i a \in A_{p_i}$. This is due to $p_i^{r_i} m_i a = ma = 0$ and so $a \in A_{p_1} + \ldots + \mathrm{A}_{p_n} \leq \oplus_p A_p$. If $A = \oplus_p B_p$ is any direct decomposition of A into p-groups B_p with different primes p, then by definition of the A_p, we have $B_p \leq A_p$ for all p. Since the B_p and the A_p generate direct sums which are both equal to A, we naturally have $B_p = A_p$ for every p.

□

Theorem 5.1.3. *An elementary p-group is the direct sum of cyclic groups of order p.*

Proof: We must show that an elementary p-group A is in the natural way a vector space over the field F_p of p elements. $pa = 0$ for $a \in A$ and so for $n, m \in \mathbb{Z}$, we have $na = ma$ if $n \equiv m \mod p$ ((n, m) represent the same element of F_p). It is now fairly straightforward to check the vector space axioms. Therefore, A as a vector space over a field F_p has a basis, say $\{a_i\}_{i \in I}$. It follows that $A = \oplus_{i \in I} \langle a_i \rangle$.

□

We have called a subgroup B of A a direct summand of A if $A = B \oplus C$ for some $C \leqq A$. For the projections $\pi : A \to B$ and $\theta : B \to C$, the projections of (5.1) hold. Our attention is now turned to B. Note that B alone does not define π uniquely unless C is known.

Lemma 5.1.4. *If there is a projection π of A onto its subgroup B, then B is a direct summand of A.*

Proof: The map $\theta : 1_A - \pi$ is an endomorphism of A, satisfying (5.1). Therefore we have $A = B \oplus \theta A$ where θA is the kernel of π.

□

Lemma 5.1.5. *If the quotient group A/B is a direct sum, $A/B = \oplus_i (A_i/B)$, and if B is the direct summand of every $A_i = B \oplus C_i$, then B is a direct summand of A, $A = B \oplus (\oplus_i C_i)$* (Kaplansky).

Proof: B and C_i generate A. Assume that we have $b+c_1+\ldots+c_n = 0$ for some $b \in B$ and $c_j \in C_j$ where $j = 1, \ldots, n$. With mod B, we obtain $(c_1+B)+\ldots+(c_n+B) = B$. Since $c_j + B \in A_j/B$, $c_1 + B = \ldots = c_n + B = B$. Thus $c_j \in B$ for every j, and so $c_j \in B \cap C_j = 0$ giving $b = 0$. Consequently, B and the C_i generate their direct sum.

□

If a subgroup B of a group A is shown to be a direct summand of A, then generally it is not possible to find directly a projection $A \to B$. One would then try to find the complement D to B among the subgroups G of A satisfying $G \cap B = 0$. A B-high subgroup is a subgroup H of A satisfying

$$H \cap B = 0, \text{ and if } H < H' \leqq A \Rightarrow H' \cap B \neq 0.$$

H is maximal with respect to the property of being disjoint from B and we can say that $H + B = H \oplus B$. The existence of these B-high subgroups is guaranteed by the Kuratowski-Zorn Lemma. A subgroup D of A is an absolute direct summand of A if for every D-high subgroup H of A we have $A = D \oplus H$. We now prove two lemmas which are essential for later on.

Lemma 5.1.6. *If B is a subgroup of A and C is a B-high subgroup of A, then $a \in A, pa \in C$ implies $a \in B \oplus C \leq A$ where p is a prime.*

Proof: There are two cases: when $a \in C$ and $a \notin C$. When $a \in C$ there is nothing to be proved. When $a \notin C$, then $\langle C, a\rangle$ contains, owing to the choice of C, an element $b \in B$ with $b \neq 0$ i.e.: $b = c + ka$ for some $c \in C$ and $k \in \mathbb{Z}$. $(k, p) = 1$ because of $pa \in C$ and $B \cap C = 0$. Therefore, $rk + sp = 1$ for $r, s \in \mathbb{Z}$ and so $a = r(ka) + s(pa) = r(b - c) + s(pa) \in B \oplus C$.

□

Lemma 5.1.7. *Let A, B, C be as in the previous lemma. Then $A = B \oplus C$ if and only if $pa = b + c$ implies $pb' = b$ for some $b' \in B$ and where $a \in A, b \in B, c \in C$* (G. Gratzer).

Proof: If $A = B \oplus C$ and $a' = b' + c'$ where $b' \in B$ and c inC, then $pa = pb' + pc' = b + c$ which implies $pb' = b$. Conversely, if $pa = b + c$ implies $pb' = b$ for some $b' \in B$, then $a - b'$ satisfies the hypotheses of the previous lemma, and so $a - b' \in B \oplus C, a \in B \oplus C$. This demonstrates that the quotient group $A/(B \oplus C)$ contains no elements of prime order, and is torsion-free. But if $x \in A$ is arbitrary, not in $B \oplus C$, then $\langle C, x\rangle$ intersects B in a nonzero element $b'' = c'' + lx$ where $c'' \in C$ and an integer l. $l \neq 0$ since $B \cap C = 0$ giving $lx = b'' - c'' \in B \oplus C$ and $A/(B \oplus C)$ is a torsion group and we can conclude that $A = B \oplus C$.

□

5.1.1 Direct sums of cyclic groups

An important type of group are cyclic groups. They are Abelian groups and are generated by a single element, such as a, called the generator, and all other elements are multiples of a when using additive notation. A cyclic group of the element a is denoted $\langle a\rangle$ and represented by $\langle a\rangle = \{na \mid n \in \mathbb{Z}\}$.

If $A = \langle a\rangle$ is an infinite cyclic group, then it is isomorphic to the additive group Z of rational integers $0, \pm 1, \pm 2, \ldots$. Therefore, all infinite cyclic groups are isomorphic and we denote them using Z. If $A = \langle a\rangle$ is a finite cyclic group of order m, it consists of the elements $0, a, 2a, \ldots, (m-1)a$. Since $ma = 0$, A is isomorphic to the additive group $Z(m)$, the rational integers mod m. Therefore, all finite cyclic groups of the same order m are thus isomorphic and we denote them $Z(m)$.

Let $A = \langle a\rangle$ be a cyclic group of order m. Every ka with $(k, m) = 1$ generates A. If $n > 0$ is an integer with $n(ka) = 0$, then $m|nk$ and hence $m|n$. This means $o(ka) = m$, and $\langle ka\rangle = \langle a\rangle$. Conversely, if ka generates $\langle a\rangle$, then $o(ka) = m$ and if we say $(k, m) = d$, then $md^{-1}ka = kd^{-1}ma = 0$ from $o(ka) \leq md^{-1}$ and hence $d = 1$. Therefore $\langle ka\rangle = \langle a\rangle$ if and only if $(k, m) = 1$.

Theorem 5.1.8. (Fundamental Theorem of Cyclic groups). *Subgroups of cyclic groups are cyclic.*

Proof:
Let B be a nonzero subgroup of the cyclic group $\langle a \rangle$ and n be the smallest positive integer with $na \in B$. Now all the multiples of na belong to B, and if $sa \in B$ with an integer $s = qn + r$ $(0 \leq r < n)$, then $ra = sa - q(na) \in B$ implies $r = 0$ and hence $B = \langle na \rangle$.

If a is of finite order m, then $n|m$. Now, if u, v are integers such that $mu + nv = (m, n)$, then $(m, n)a = mua + nva = v(na) \in B$ and hence $n \leq (m, n)$. For alternate divisors $n \geq 0$ of m, the subgroups $\langle na \rangle$ are different, and so $Z(m)$ has as many subgroups as m has divisors. Of two subgroups of $Z(m)$, one contains the other if and only if the corresponding divisor of m divides the other. If a is of infinite order, then so is na, and every nonzero subgroup of Z is an infinite cyclic group. $\langle na \rangle$ is of index n in $\langle a \rangle$, and it is the only subgroup of index n.

Let $A = \langle a \rangle$ and $B = \langle na \rangle$, with $n \geq 0$ a divisor of the order of a if this is finite. Then the quotient group A/B may be generated by the coset $a+B$ which is evidently of order n, thus $A/B \cong Z(n)$. Consequently, all proper quotient groups of a cyclic group are finite cyclic groups.

□

Lemma 5.1.9. *Let G be a cyclic group of order n. For each divisor d of G, there exists a unique subgroup G of order d.*

Proof:
If a is a generator of G, then $\langle a^{n/d} \rangle$ is a subgroup of order d. Assume $\langle b \rangle$ is a subgroup of order d. Now $b^d = 1$ and $b = a^m$ for some m. Hence $a^{md} = 1, md = nk$ for some k, and $b = a^m = (a^{n/d})^k$. Therefore $\langle b \rangle \subset \langle a^{n/d} \rangle$, and the inclusion is an equality because both subgroups have order d.

□

Definition 5.1.10. The *Euler φ-function* is defined as follows: $\varphi(1) = 1$; if $h > 1$, then $\varphi(h)$ is the number of integers k such that $1 \leq k < h$ and $(k, h) = 1$.

Theorem 5.1.11. *If n is a positive integer, then $n = \sum_{d|n} \varphi(d)$, where the sum is over all divisors d of n $(1 \leq d \leq n)$.*

Proof:
If C is a cyclic subgroup of a group G, let $g(C)$ denote the set of its generators. It is clear that $G = \cup g(C)$ where C varies over all the cyclic subgroups of G. When G is cyclic of order n, we have just seen that there is a unique cyclic subgroup C_d of order d for every divisor d of n. Therefore, $n = |G| = \sum_{d|n} |g(C_d)|$.

□

We can now characterize finite cyclic groups.

Theorem 5.1.12. *A group G or order n is cyclic if and only if, for each divisor d of n, there is at most one cyclic subgroup of G of order d.*

Proof:
If G is cyclic, the result is Lemma 5.1.9. Conversely, since $G = \cup g(C)$, where C ranges over all the cyclic subgroups of G, whence $n = |G| = \sum |g(C)|$. By hypothesis, for each divisor d of n, there is at most one such C of order d (and $|g(C)| = \varphi(d)$). Hence $\sum |g(C)| \leq \sum_{d|n} \varphi(d) = n$ by Theorem 5.1.11. We conclude that G must have exactly one cyclic subgroup of order d for every divisor d of n. In particular, G has a cyclic subgroup of order $d = n$ and G is cyclic.

□

A finitely generated Abelian group is the direct sum of cyclic groups. A free Abelian group is the direct sum of infinite cyclic groups. If the cyclic groups are generated by x_i $(i \in I = \{1, \ldots, n\})$, then the free group, denoted F, is: $F = \oplus_{i \in I} \langle x_i \rangle$.

F consists of all finite linear combinations

$$g = n_1 x_{i_1} + \ldots + n_k x_{i_k}$$

with different $x_{i_1}, \ldots, x_{i_k}$ where n_j are integers $\neq 0$ and k is a nonnegative integer. Equivalently, a free Abelian group has elements that can be written in only a single way as a finite linear combination of elements of a basis. The rank is the cardinality

of a basis. Therefore, if m is the cardinal of F, we say F is of rank m.

We could also define F by starting with the nonempty set $X = \{x_i\}_{i \in I}$ called a free set of generators, and then declaring F as the collection of all formal expressions of the form $g = n_1 x_{i_1} + \ldots + n_k x_{i_k}$. F is then called the free group on the set X. F, up to isomorphism, is uniquely determined by the cardinal number of the index set I. Therefore, we write F_m for a free group with m generators.

To select a basis in a direct sum of cyclic groups we require the concepts of linear independence and rank. A system $\{a_1, \ldots, a_k\}$ of nonzero elements of a group A is linearly independent if

$$n_1 a_1 + \ldots + n_k a_k = 0 \; n_i \in \mathbb{Z}.$$

This, in effect, means that all coefficients n_i are equal to zero (the sum is finite) if $o(a_i) = \infty$ and $o(a_i)|n_i$ if $o(a_i)$ is finite. Any two maximal linearly independent sets in A have identical cardinality, known as the rank of A. For Abelian groups, the rank is defined using modules over $\mathbb{Z}$. A system is dependent if it is not independent.

An element of A is torsion if its order is finite and the set of all torsion elements is a subgroup denoted $T(A)$. The quotient group $A/T(A)$ is the unique maximal torsion free quotient of A and it has the same rank as A. Independence is a property of finite character since an infinite system is independent if every finite subset is independent. An independent system cannot contain equal elements and is therefore a set.

An infinite system $L = \{a_i\}_{i \in I}$ of elements A is independent if every finite subsystem of L is independent. Independence is a therefore a finite characteristic. An independent system can't contain equal elements and hence it is a set.

Proposition 5.1.13. *The free groups F_m and F_n are isomorphic if and only if $m = n$ for cardinals m, n.*

Proof:
Let p be a prime and F a free group with m free generators x_i. Since every element $g \in F$ has the unique form $g = n_1 x_{i_1} + \ldots + n_k x_{i_k}$, it is evident that $g \in pF$ is

quivalent to the simultaneous fulfillment of the divisibility relations $p|n_1, \ldots, p|n_k$. Hence $F|pF$ as a vector space over the prime field of characteristic p, has a basis $\{x_i + pF\}$ with dimension m. The assertion follows.

□

There is a one-to-one correspondence between cardinal numbers and nonisomorphic free groups. A basic property of free groups is as follows.

Theorem 5.1.14. *A set $X = \{x_i\}_{i \in I}$ of generators of a free group F is a free set of generators if and only if every mapping ϕ of X into a group A can be extended to a unique homomorphism $\psi : F \to A$.*

Proof:
Let X be a free set of generators of F. If $\phi : x_i \mapsto a_i$ is a mapping of X into a group A, then let us define $\psi : F \to A$ as

$$\psi(n_1 x_{i_1} + \ldots + n_k x_{i_k}) = n_1 a_{i_1} + \ldots + n_k a_{i_k}.$$

The uniqueness of $g = n_1 x_{i_1} + \ldots + n_k x_{i_k}$ guarantees that ψ is well defined and it preserves addition. Conversely, assume that the subset X in F has the stated property. Then let G be a free group with a free set $\{y_i\}_{i \in I}$ of generators, where I is the same as for X. By hypothesis, $\phi : x_i \mapsto y_i$ can be lifted to a homomorphism $\psi : F \to G$, which cannot be anything else bar the map $\psi : n_1 x_{i_1} + \ldots + n_k x_{i_k} \mapsto n_1 y_{i_1} + \ldots + n_k y_{i_k}$. It is evident that ψ must be a homomorphism.

□

Theorem 5.1.15. *If B is a subgroup of A such that A/B is free, then B is a direct summand of A.*

Proof:
By Lemma 5.1.5, it suffices to merely prove this for the case where A/B is an infinite cyclic group, say $A/B = \langle a' \rangle$. Select an $a \in a'$ in A. Then the cosets na' mod B where $n = 0, \pm 1, \pm 2, \ldots$ are represented by the elements na of $\langle a \rangle$. Hence $A = B \oplus \langle a \rangle$.

□

The following theorem provides complete information about the structure of subgroups of free groups.

Theorem 5.1.16. *A subgroup of a free group is free.*

Proof:
Let $F = \oplus_{i\in I} \langle a_i\rangle$ be a free group and suppose that the index set I is the set of ordinals $< \tau$ and well ordered in some way. For $\sigma \leqq \tau$, we define $F_\sigma = \oplus_{\rho<\sigma}\langle a_\rho\rangle$. If G is a subgroup of F, then let $G_\sigma = G \cap F_\sigma$. Now $G_\sigma = G_{\sigma+1} \cap F_\sigma$, and so $G_{\sigma+1}/\mathrm{G}_\sigma \cong (G_{\sigma+1} + \mathrm{F}_\sigma)/F_\sigma$.

The quotient group $(G_{\sigma+1} + \mathrm{F}_\sigma)/F_\sigma$ is a subgroup of $F_{\sigma+1}/\mathrm{F}_\sigma \cong \langle a_\sigma\rangle$. We have that either $G_{\sigma+1} = \mathrm{G}_\sigma$ or $G_{\sigma+1}/\mathrm{G}_\sigma$ is an infinite cyclic group. By the previous theorem, we have $G_{\sigma+1} = \mathrm{G}_\sigma \oplus \langle b_\sigma\rangle$ for some $b \in G_{\sigma+1}$, which is zero if $G_{\sigma+1}$=G_σ. It follows that the elements b_σ generate the direct sum $\oplus\langle b_\sigma\rangle$. This direct sum must be G, since G is the union of G_σ.

□

If A is finite, then a group $G = \langle A\rangle$ is called finitely generated. The following two theorems describe finite groups.

Lemma 5.1.17. *Let A be a primary group and assume that A contains an element g of maximal order p^k. Then $\langle g\rangle$ is a direct summand of A.*

Proof:
Let B be a $\langle g\rangle$-high subgroup of A. We must show that $A = \langle g\rangle \oplus B$. We recall Lemma 5.1.7 and show that $pa = mg + b$ where $a \in A, b \in B, m \in \mathbb{Z}$ implying $p|m$. Due to the maximality of the order of $\langle g\rangle$, we have $p^{k-1}mg + p^{k-1}b = p^k a = 0$. Hence $p^{k-1}mg = 0$ and p divides m.

□

The following theorem is the first proper structure theorem in the history of group theory.

Theorem 5.1.18. *A finite group is the direct sum of a finite number of cyclic groups of prime power orders* (Frobenius and Stickelberger).

Proof:
Due to Theorem 5.1.2, we can immediately restrict ourselves to p-groups. If the set $A \neq 0$ is a finite p-group, then we select an element $a \in A$ of maximal order p^k. By the previous lemma, $A = \langle a \rangle \oplus B$ for some $B < A$. Since B is of smaller order than A, a trivial induction completes the proof.

□

Theorem 5.1.19. *A p-group A is a direct sum of cyclic groups if and only if A is the union of an ascending chain of subgroups $A_1 \leqq A_2 \leqq \ldots \leqq A_n \leqq \ldots$, $\bigcup_{n=1}^{\infty} A_n = A$, such that the heights of elements not equal to zero of A_n are less than a finite bound k_n* (Kulikov).

Theorem 5.1.20. *Subgroups of direct sums of cyclic groups are again direct sums of cyclic groups* (Kulikov).

Proof:
Let A be a direct sum of cyclic p-groups with B a subgroup of A. A is the union of the ascending chain $A_1 \leqq \ldots \leqq A_n \leqq \ldots$ of its subgroups, where the height of A_n are bounded by k_n. B is the union of the ascending chain $B_1 \leqq \ldots \leqq B_n \leqq \ldots$ with $B_n = B \cap A_n$, where the height of B_n do not exceed k_n. By the previous theorem, B is the direct sum of cyclic groups. Therefore, the theorem holds for torsion groups.

Let A be a random direct sum of cyclic groups. If T is its torsion part, then $B \cap T$ is the torsion part of the subgroup B of A. Now $B/(B \cap T) \cong (B+T)/T \leqq A/T$ is a free group. By Theorem 5.1.16, $B/(B+T)$ is free, and so Theorem 5.1.15 implies $B = (B \cap T) \oplus C$ for some free subgroup C of B. $B \cap T$ is a direct sum of cyclic p-groups and B is therefore a direct sum of cyclic groups.

□

5.2 Semidirect product

A semidirect product is another way that a group can be put together from two subgroups, one of which is normal.

Definition 5.2.1. A group G is a *semidirect product* of H by K, denoted $G = H \rtimes K$, if G contains subgroups H and K such that:

1. $H \lhd G$;
2. $HK = G$;
3. $H \cap K = 1$.

Semidirect products are similar to direct products (a direct product is when both subgroups are normal). A note for Chapter 6: the Quarternion group is not a semidirect product because all subgroups of the Quarternion group are normal. Unlike direct products, semidirect products require a homomorphism from K to the group of automorphisms of H to get back to G, $\phi : K \to \mathrm{Aut}(H)$.

The result of applying the automorphism $\phi(k)$ for $k \in K$ to $h \in H$ is denoted as ϕ_k. ϕ_k is defined to be the automorphism of H given by the conjugation:

$$\phi_k : H \to H, \phi_k(h) = khk^{-1}$$

which gives a homomorphism.

Theorem 5.2.2. *The map $k \mapsto \phi_k$ is a homomorphism $\phi : K \to \mathrm{Aut}(H)$.*

Proof:
We must show $\phi_{k_1}\phi_{k_2} = \phi_{k_1k_2}$ for any $k_1, k_2 \in K$. We need to show that the $\phi_{k_1}\phi_{k_2}(h) = \phi_{k_1k_2}(h)$ for any $h \in H$.

LHS: $\phi_{k_1}\phi_{k_2}(h) = \phi_{k_1}(k_2hk_2^{-1}) = k_1k_2hk_2^{-1}k_1^{-1}$.
RHS: $\phi_{k_1k_2}(h) = k_1k_2h(k_1k_2)^{-1} = k_1k_2hk_2^{-1}k_1^{-1}$.

□

$G = HK$, so every $g \in G$ can be written in the form hk for $h \in H$ and $k \in K$. Given any two elements $hk, h'k' \in G$, we can write their product and the inverse of hk in the same form.

Theorem 5.2.3. *If $h, h' \in H$ and $k, k' \in K$ then*

$$hkh'k' = h''k'' \text{ and } (hk)^{-1} = \phi_{k^{-1}}(h^{-1})(k^{-1}), \text{ where } h'' = h\phi_k(h') \text{ and } k'' = kk'.$$

Proof:
$hkh'k' = hkh'(k^{-1}k)k' = h(kh'k^{-1})kk' = h\phi_k(h')kk' = h''kk' = h''k''$ and
$(hk)^{-1} = k^{-1}h^{-1} = k^{-1}h^{-1}kk^{-1} = \phi_{k^{-1}}(h^{-1})k^{-1}$.

□

If we had begun with H and K and a homomorphism $\phi : K \to \text{Aut}(H)$ given by $k \mapsto \phi_k$ we can always find some semidirect product group.

Theorem 5.2.4. *Given groups H and K and a homomorphism $K \to \text{Aut}(H)$ there is a semidirect product group G. We can construct it as follows: The underlying set of G is the set of pairs (h, k) where $h \in H$ and $k \in K$. The multiplication on this set is given by the rule*

$$(h, k)(h', k') = (h\phi_k(h'), kk'),$$

the identity element is $(1, 1)$ and inverse is given by

$$(h, k)^{-1} = (\phi_{k^{-1}}(h^{-1}), k^{-1}).$$

Proof:
It is easy to prove that G is a group by showing that multiplication is associative and the identity and inverse laws hold. Since G is a group, we need to show that it is the desired semidirect product of H and K.

We have the injective maps $H \to G$ and $K \to G$ given by $h \mapsto (h, 1)$ and $k \mapsto (1, k)$ respectively. Both these maps are homomorphisms and allow us to think of H and K as subgroups of G. $H \cap K = \{(1, 1)\}$ and $HK = G$ since $(h, 1)(1, k) = (h, k)$.

We need to show that H is normal in G and the action of K on H by conjugation in G is given by the original homomorphism ϕ. Both follow from:

$$(1, k)(h, 1)(1, k)^{-1} = (1, k)(h, 1)(1, k^{-1}) = (\phi_k(h), k)(1, k^{-1}) = (\phi_k(h), 1).$$

□

5.3 Compact groups

Definition 5.3.1. 1. A *topological group* G is a group together with a topology such that multiplication $(x, y) \mapsto xy : G \times G \to G$ and inversion $x \mapsto x^{-1} : G \to G$ are continuous functions.

2. A *compact group* is a topological group whose topology is compact Hausdorff.

3. A *locally compact group* is a topological group whose topology is a Hausdorff space where the identity has a compact neighbourhood.

Note that if H is a subgroup of a topological group G, then H is also a topological group with the induced topology.

Definition 5.3.2. A *morphism* of topological groups is a continuous function $f : G \to H$ between two topological groups that is also a group homomorphism. It is called an *isomorphism* of topological groups, denoted $G \cong H$, if it has an inverse morphism of topological groups.

If G is a group and X a set, we say that G acts on X if there is a function $(g, x) \mapsto gx : G \times X \to X$ such that $1x = x$ and $g(hx) = (gh)x$. The act is transitive if Gx X for all $x \in X$. $G_x = \{g \in G \mid gx = x\}$ for all $x \in X$ is a subgroup called the stability subgroup of G at x. A subgroup H of G gives rise to the set G/H of cosets gH where $g \in G$. G is transitive on G/H through $(g, g^{'}H) \mapsto gg^{'}H : G \times G/H \to G/H$ and the stability group of G at H is H.

Definition 5.3.3. *A topological group G acts on a topological space X* if there is a continuous function $(g, x) \mapsto gx : G \times X \to X$ which is a group action on X.

Definition 5.3.4. If H is a subgroup of a topological group G, then the set G/H of cosets gH, where $g \in G$ is a topological space with respect to the quotient topology, is called the *quotient space* of G modulo H or the *homogeneous space* of G modulo H. If N is a normal subgroup of G, then G/N with the quotient topology is called the *quotient group* of G modulo N. The quotient group $\mathbb{R}/\mathbb{Z}$ will be denoted as $\mathbb{T}$.

The following proposition shows invariant objects for the action of compact groups.

Proposition 5.3.5. *If a compact group G acts on a topological space X and x is a fixed point, that is $Gx = \{x\}$, then x has a basis of G-invariant neighbourhoods. Specifically, if U is any neighbourhood of x, then the set $V = \bigcap_{g\in G} gU$ is a G-invariant neighbourhood of x contained in U.*

Proof:
Since all functions $y \mapsto hy : X \to X, h \in G$, are bijective and $hG = G$ we find

$$\begin{aligned} hV &= h \bigcap_{g\in G} gU \\ &= \bigcap_{g\in G} hgU \\ &= \bigcap_{g\in G} gU \\ &= V. \end{aligned}$$

Therefore, V is G-invariant. Also, $V \subseteq U$ since $1 \in G$ and $1U = U$.

We now suppose that V is not a neighbourhood of $x \in X$ and derive a contradiction which will complete the proof. We assume that U is open. For any subset W of X we define

$$G_W = \{g \in G \mid gW \neq \emptyset\}.$$

By our supposition that V is not a neighbourhood of x, for any neighbourhood W of x we compute

$$\begin{aligned} \emptyset &\neq W \backslash V \\ &= W \backslash \bigcap_{g\in G} gU \\ &= \bigcup_{g\in G} (W \backslash gU). \end{aligned}$$

So there is some $g \in G$ with $W\backslash gU \neq \emptyset$ and then $g^{-1}W\backslash U \neq \emptyset$. Therefore $G_W \neq \emptyset$. Let $\mathcal{U}$ denote the neighbourhood filter of x. Since $W \subseteq W' \Rightarrow G_W \subseteq G'_W$, the family $\{G_W \mid W \in \mathcal{U}\}$ is a filter basis on G. By the compactness of G, there is an element $g \in \bigcap_{W\in\mathcal{U}} \overline{G_W}$. Then, for all neighbourhoods N of 1 in G, we have $gN \bigcap G_W \neq \emptyset$,

that is, $gNW \backslash U \neq \emptyset$.

By the continuity of the the action, given an arbitrary neighbourhood W_0 of x, we find N and W so that $NW \subseteq W_0$. Hence $gW_0 \neq \emptyset$. Therefore, every neighbourhood W_0 of x meets the set $X \backslash g^{-1}U$. This last set is closed as U and hence $g^{-1}U$ is open. Therefore $x \in X \backslash g^{-1}U$ and so $gx \notin U$. But $x = gx$ since x is a fixed point. Thus $x \notin U$ which is the required contradiction since U is a neighbourhood of x.

□

Corollary 5.3.6. *If G is a compact group and U any neighbourhood of the identity, then $V = \bigcap_{g \in G} gUg^{-1}$ is a neighbourhood of the identity which is contained in U and is invariant under all inner automorphisms.*

Proof:
Since the group G acts on G through $(g, x) \mapsto gxg^{-1}$ and 1 is a fixed point for this action, we can apply Proposition 5.3.5 and the Corollary is proved.

□

We can construct many compact groups using products.

Proposition 5.3.7. *If $\{G_j \mid j \in J\}$ is an arbitrary family of compact groups, then the product $G = \prod_{j \in J} G_j$ with the product topology is a compact group. Every closed subgroup H of G is a compact group.*

Proof:
We can observe that the product topology makes the cartesian product of any family of topological groups into a topological group. Due to Tychonoff's Theorem, the product space of any family of compact spaces is compact and therefore G is a compact group. We also already know that any closed subgroup H of G is a compact group.

□

For two sets X and Y, the set of all functions $f : X \to Y$ will be denoted Y^X.

Definition 5.3.8. If A is an Abelian group, then the group

$$\mathrm{Hom}(A, \mathbb{T}) \subseteq \mathbb{T}^A$$

of all morphisms of Abelian groups into the underlying Abelian group of the circle group given the induced group structure and topology of the product group $\mathbb{T}^A$, is called the *character group* of A and is denoted $\hat{A}$. Its elements are called *characters* of A.

For any Abelian group there is always a large supply of characters.

Proposition 5.3.9. *The character group $\hat{A}$ of any Abelian group A is a compact Abelian group.*

Proof:
By Proposition 5.3.7, the product $\mathbb{T}^A$ is a compact Abelian group. For any pair $(a, b) \in A \times A$, the set $M(a, b) = \{\mathcal{X} \in \mathbb{T}^A \mid \mathcal{X}(a+b) = \mathcal{X}(a) + \mathcal{X}(b)\}$ is closed since $\mathcal{X} \mapsto \mathcal{X}(c) : \mathbb{T}^A \to \mathbb{T}$ is continuous by the definition of the product topology. But then $\hat{A} = \bigcap_{(a,b)\in A\times A} M(a, b)$ is closed in $\mathbb{T}^A$ and therefore compact.

□

A topological space in which all components are singletons (sets with exactly one element) is called totally disconnected. Discrete spaces are totally disconnected and so are products of totally disconnected spaces.

Definition 5.3.10. Let X and Y be sets with $F \subseteq Y^X$. We say that f seperates the points of X if for any two different points x_1 and x_2 in X, there is an $f \in F$ such that $f(x_1) = f(x_2)$.

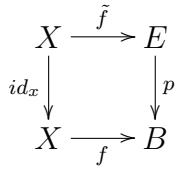
We now define coverings and simple connectivity.

Definition 5.3.11. A function $f : X \to Y$ is called a *covering* (covering map) if Y has an open cover $\{U_j \mid j \in J\}$ such that for each $j \in J$ there is a nonempty discrete space F_j and a homeomorphism $h_j : F_j \times U_j \to f^{-1}(U_j)$ such that the following diagram commutes:

$$\begin{array}{ccc} F_j \times U_j & \xrightarrow{h_j} & f^{-1}(U_j) \\ {\scriptstyle pr_2}\downarrow & & \downarrow{\scriptstyle f|f^{-1}(U_j)} \\ U_j & \xrightarrow[id\,U_j]{} & U_j \end{array}$$

Note that coverings are continuous, open and surjective.

Definition 5.3.12. A topological space X is called *simply connected* if it is connected and has the following universal property: For any covering map $p : E \to B$ between topological spaces, any point $e_0 \in E$ and any continuous function $f : X \to B$ with $p(e_0) = f(x_0)$ for some $x_0 \in X$, there is a continuous map $\tilde{f} : X \to E$ such that $p \circ \tilde{f} = f$ and $\tilde{f}(x_0) = e_0$. This can be represented diagrammatically as:



5.4 Haar measure

The Haar measure was introduced by Alfréd Haar, a Hungarian mathematician, in 1933. He proved that there exists an invariant measure on any seperable compact group. Results from Section 5.4 can be found in [29]. Let E be a topological vector space. A topological vector space is a vector space E over $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$ which is a topological group with respect to addition and for which scalar mulitplication is continuous, i.e.: $(y, x) \mapsto y \cdot x : \mathbb{K} \times EE$ is continuous. Let G denote a compact Hausdorff space.

The Haar measure is written as the number $\mu(f)$ or $\int f \, d\mu = \int_G f(g) \, d\mu(g)$.

Definition 5.4.1. Let G denote a compact group. A measure μ is called *invariant* if $\mu_g(f) = \mu(f)$ for all $g \in G$ and $f \in E = (C, \mathbb{K})$. It is called a *Haar measure* if it is invariant and positive, that is, $\mu(f) \geq 0$ for all $f \geq 0$. μ is called *normalized* if $\mu(1) = 1$.

The following theorem is a crucial aspect of the Haar measure. The proof of it is long and tedious.

Theorem 5.4.2. (Existence and Uniqueness Theorem of the Haar measure). *For each compact group G, there is a unique normalized Haar measure.*

The first person to prove uniqueness of the Haar measure was John von Neumann in 1934 while André Weil proved existence. Weil's proof made use of the Axiom of Choice in the form of Tychonoff's Theorem. Before we prove the theorem (using Tychonoff's Theorem), let us introduce some necessary definitions.

Definition 5.4.3. Let X be a topological space, and let $A \subset X$. Then A is *σ-bounded* if it is possible to find a sequence of compact sets $\{K_n\}_{n=1}^{\infty}$ with the property that $A \subset \bigcup_{n=1}^{\infty} K_n$.

Definition 5.4.4. A *left Haar measure* μ on a topological group G is a Radon measure which is invariant under left translation, i.e. $\mu(gB) = \mu(B)$ for all $g \in G$. A *right Haar measure* μ on a topological group G is a Radon measure which is invariant under right translation, i.e. $\mu(Bg) = \mu(B)$ for all $g \in G$.

A Radon measure is a measure on the σ-algebra of Borel sets of a Hausdorff topological space X that is locally finite and inner regular (measure of a set can be approximated from within by compact subsets).

Definition 5.4.5. A *content* λ is a set function that acts on the set of compact sets $\mathcal{C}$ that is finite, nonnegative, additive, subadditive and monotone. A content induces an inner content and an outer measure. The inner content λ_* is defined by $\lambda_* = \sup\{\lambda(K) \,|\, K \in \mathcal{C}, K \subset A\}$. Let $\mathcal{O}$ denote the set of open sets. The outer measure μ_e is defined by $\mu_e(A) = \inf\{\lambda_*(O) \,|\, O \in \mathcal{O}, A \subset O\}$.

Definition 5.4.6. If μ_e is an outer measure, then a set A is said to be μ_e-*measurable* if for all sets B, $\mu_e = \mu_e(A \cap B) + \mu_e(A^c \cap B)$.

We now prove the existence and uniqueness of the Haar measure using the equivalent form:

Theorem 5.4.7. *On any locally compact group G, there exists a nonzero left Haar measure μ, and this Haar measure is unique up to a positive multiplicative constant of proportionality.*

The proof relies on four lemmas.

Lemma 5.4.8. *Let λ be a content, and let λ_* and μ_e be the inner content and outer measure, respectively, induced by λ. Then for all $O \in \mathcal{O}$ and for all $K \in \mathcal{C}, \lambda_*(O) = \mu_e(O)$ and $\mu_e(\text{int}(K)) \leq \lambda(K) \leq \mu_e(K)$.*

Proof:
For any $O \in \mathcal{O}$, it is clear that $\mu_e(O) \leq \lambda_*(O)$ since we can pick O as an open superset of O in the definition of μ_e. Now if $O' \in \mathcal{O}$ with $O \subset O'$, then $\lambda_*(O) \leq \lambda_*(O')$. Hence

$$\lambda_*(O) \leq \inf_{O'} \lambda_*(O') = \mu_e(O).$$

Therefore $\lambda_*(O) = \mu_e(O)$.

Now if $K \in \mathcal{C}$ and $O \in \mathcal{O}$ with $K \subset O, \lambda(K) \leq \lambda_*(O)$. Thus

$$\lambda(K) \leq \inf_O \lambda_*(O) = \mu_e(K).$$

If $K^{'} \in \mathcal{C}$ with $K^{'} \subset \text{int}(K)$, then $\lambda(K^{'}) \leq \lambda(K)$, so

$$\begin{aligned}\mu_e(\text{int}(K)) &= \lambda_*(\text{int}(K)) \\ &= \sup_{K'} \lambda(K^{'}) \\ &\leq \lambda(K).\end{aligned}$$

□

Lemma 5.4.9. *Let λ be a content, and let μ_e be the outer measure induced by λ. Then a σ-bounded set A is measurable with respect to μ_e if and only if for all $O \in \mathcal{O}$, $\mu_e(A \cap O) + \mu_e(A^c \cap O) \leq \mu_e(O)$.*

Proof:
Let λ_* be the inner content induced by λ, let B be a σ-bounded set and let $O \in \mathcal{O}$ satisfying $B \subset O$. Since

$$\begin{aligned}\lambda_*(O) = \mu_e(O) &\geq \mu(A \cap O) + \mu_e(A^c \cap O) \\ &\geq \mu(A \cap B) + \mu_e(A^c \cap B)\end{aligned}$$

we have

$$\mu_e(B) = \inf_O \lambda_*(O) \geq \mu(A \cap B) + \mu_e(A^c \cap B).$$

The other direction and the converse follow from the definition of subadditivity and μ_e measurability.

□

Lemma 5.4.10. *Let μ_e be the outer measure induced by a content λ. Then the measure μ that satisfies $\mu(A) = \mu_e(A)$ for all Borel sets A is a regular Borel measure. μ is called the induced measure of λ.*

Proof:
It suffices to show that each $K \in \mathcal{C}$ is μ_e measurable. By the previous lemma, this would follow from showing that $\mu_e(O) \geq \mu_e(O \cap K) + \mu_e(O \cap K^c)$ for all $O \in \mathcal{O}$.

Let $K^{'} \in \mathcal{C}$ be a subset of $O \in K^c$, and let $\tilde{K} \in \mathcal{C}$ be a subset of $O \cap K^{'c}$. Clearly $O \cap K^c \in \mathcal{O}$ and $O \cap K^c \in \mathcal{O}$. Because $K^{'} \cap \tilde{K} = \emptyset$ and $K^{'} \cup \tilde{K} \subset O$,

$$\mu_e(O) = \lambda_*(O) \geq \lambda(K^{'} \cup \tilde{K}) = \lambda(K^{'}) + \lambda(\tilde{K}).$$

Thus,

$$\begin{aligned}
\mu_e(O) &\geq \lambda(K^{'}) + \sup_{K^{'}} \lambda(\tilde{K}) \\
&= \lambda(K^{'}) + \lambda_*(O \cap K^{'c}) \\
&= \lambda(K^{'}) + \mu_e(O \cap K^{'c}) \\
&\geq \lambda(K^{'}) + \mu_e(O \cap K).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\mu_e(O) &\geq \mu_e(O \cap K) + \sup_{K^{'}} \lambda(K^{'}) \\
&= \mu_e(O \cap K) + \lambda_*(O \cap K^c) \\
&= \lambda(K^{'}) \\
&= \mu_e(O \cap K) + \mu_e(O \cap K^c).
\end{aligned}$$

Now it is necessary to show that $\mu(K)$ is finite. To do so, take $L \in \mathcal{C}$ with $K \subset \text{int}(L)$. Then

$$\mu(K) = \mu_e(K) \leq \mu_e(\text{int}(L)) \leq \lambda(L) < \infty.$$

Regularity follows from

$$\begin{aligned}
\mu(K) &= \mu_e(K) \\
&= \inf_O \{\lambda_*(O) \mid K \subset O, O \in \mathcal{O}\} \\
&= \inf_O \{\mu_e(O) \mid K \subset O, O \in \mathcal{O}\} \\
&= \inf_O \{\mu(O) \mid K \subset O, O \in \mathcal{O}\}.
\end{aligned}$$

□

Lemma 5.4.11. *Let Ω be a measurable space and let $h : \Omega \to \Omega$ be a homeomorphism. Let λ and κ be contents on Ω such that for all $K \in \mathcal{C}$, $\lambda(h(K)) = \kappa(K)$. Suppose that μ and v are the induced measures of λ and κ respectively. Then $\mu(h(A)) = v(A)$ for any Borel measurable set $A \in \Omega$.*

Proof:
Let λ_* and κ_*be the inner contents induced by λ and κ respectively. Let μ_e and v_e be their respective outer measures. If $O \in \mathcal{O}$ then

$$\begin{aligned}\{\kappa(K) \mid K \subset O, K \in \mathcal{C}\} &= \{\lambda(h(k)) \mid K \subset O, K \in \mathcal{C}\} \\ &= \{\lambda(A) \mid A = h(k)K \subset O, K \in \mathcal{C}\} \\ &= \{\lambda(A) \mid h^{-1}(A) \subset O, h^{-1}(A) \in \mathcal{C}\} \\ &= \{\lambda(A) \mid A \subset h(O), A \in \mathcal{C}\}.\end{aligned}$$

Thus $\kappa_*(O) = \lambda_*(h(O))$. Now let B be a σ bounded set. Then

$$\begin{aligned}\{\kappa_*(O) \mid B \subset O, O \in \mathcal{C}\} &= \{\lambda_*(h(O)) \mid B \subset O, O \in \mathcal{O}\} \\ &= \{\lambda_*(C) \mid C = h(O), B \subset O, O \in \mathcal{O}\} \\ &= \{\lambda_*(C) \mid h^{-1}(C) \mid h^{-1}(C) \subset B, h^{-1}(C) \in \mathcal{O}\} \\ &= \{\lambda_*(C) \mid C \subset h(B), C \in \mathcal{O}\}.\end{aligned}$$

Thus $v_e(B) = \mu_e(h(B))$. By the result of the previous lemma, if A is any Borel set, then $\mu(h(A)) = v(A)$.

□

For the existence of the Haar measure, we must find a content λ on G which is invariant under left translation due to Lemma 5.4.11. By Lemma 5.4.8, the induced measure of λ will be nonzero.

Proof of Theorem 5.4.7:
Let $A \subset G$ be a bounded set and $B \subset G$ be a set with nonempty interior. Then let $A : B$ senote the lowest positive integer n such that there exists a set $\{g_j\}_{j=1}^n \subset G$ with the property that $A \subset \bigcup_{j=1}^n g_j B$. Now let $A \in \mathcal{C}$ be a set with nonempty interior. Let $\mathcal{N}$ denote the set of all neighbourhoods of the identity element of G. Fix $O \in \mathcal{N}$.

Define

$$\lambda_O K = \frac{K : O}{A : O} \text{ for } K \in \mathcal{C}.$$

$\lambda_O K$ satisfies $0 \leq \lambda_O(K) \leq K : A$. $\lambda_O K$ satisfies all the properties of a content other than additivity.

For each $K \in \mathcal{C}$, consider the interval $I_K = [0, K : A]$ and let $\Xi = \prod I_K$. By Tychonoff's Theorem, Ξ is compact. Ξ consists of points that are direct products of functions ϕ acting on $\mathcal{C}$ with the property that $0 \leq \phi(K) \leq K : A$. $\lambda_O \in \Xi$ for all $O \in \mathcal{N}$.

Now define $\Lambda(O) = \{\lambda_{O'} | O' \subset O, O' \in \mathcal{N}\}$ given $O \in \mathcal{N}$. If $\{O_j\}_{j=1}^n \subset \mathcal{N}$, then

$$\Lambda(\bigcap_{j=1}^{n} O_j) \subset \bigcap_{j=1}^{n} \Lambda(O_j).$$

Clearly $\Lambda(\bigcap_{j=1}^{n} O_j)$ is nonempty. Since Ξ is compact, there is some point in the intersection of the closures of all the Λ's

$$\lambda \in \bigcap_{O} \{\overline{\Lambda(O)} \mid O \in \mathcal{N}\}.$$

It is now necessary to prove that λ is in fact a content. For any $K \in \mathcal{C}$, $\lambda(K)$ is finite and nonnegative since $0 \leq \lambda(K) \leq K : A < \infty$. To prove monotonicity and subadditivity, let $\xi_K(\phi) = \phi(K)$. Then ξ_K is a continuous function. Thus if K_1 and K_2 are compact sets, then

$$\Theta = \{\phi \mid \phi(K_1) \leq \phi(K_2)\} \subset \Xi \text{ is closed.}$$

Then let $K_1 \subset K_2$ and $O \in \mathcal{N}$. Then $\lambda_O \in \Theta$ and hence $\Lambda(O) \subset \Theta$. Since Θ is closed, $\lambda \in \overline{\Lambda(O)} \subset \Theta$, which imples that λ is monotone and subadditive.

Now to prove additivity, first note the restricted additivity of λ_O. Let gO be a left translation of O, and fix $K_1, K_2 \in \mathcal{C}$ so that $K_1 O^{-1} \cap K_2 O^{-1} = \emptyset$. If $K_1 \cap gO \neq \emptyset$, then $g \in K_1 O^{-1}$. If $K_2 \cap gO \neq \emptyset$, then $g \in K_2 O^{-1}$. Thus there are no left translations of O that do not intersect either K_1 or K_2, and so λ_O has additivity given

that $K_1O^{-1} \cap K_2O^{-1} = \emptyset$.

Let $K_1, K_2 \in \mathcal{C}$ with $K_1 \cap K_2 = \emptyset$. Then there is some $O \in \mathcal{N}$ satisfying $K_1O^{-1} \cap K_2O^{-1} = \emptyset$. If $O' \in \mathcal{N}$ and $O' \subset O$, then $K_1O'^{-1} \cap K_2O'^{-1} = \emptyset$ as well. Thus $\lambda_{O'}(K_1 \cup K_2) = \lambda_{O'}(K_1) + \lambda_{O'}(K_2)$. Then if $O' \subset O$,

$$\lambda_{O'} \in \Theta' = \{\phi \mid \phi(K_1 \cup K_2) = \phi(K_1) + \phi(K_2)\}.$$

Thus λ is additive. Therefore we have established the existence of the Haar measure on any locally compact group.

Now we need to prove uniqueness of the Haar measure. Let μ be a left Haar measure. Consider a nonnegative continuous function f on a locally compact group G that is not identically zero. Since

$$\int_G (f)\ d\mu > 0 \text{ we may assume that } \int_G (f)\ d\mu = 1.$$

We write

$$\Psi(g) = \int_G f(xg^{-1})\ d\mu(x) \text{ where } g \in G.$$

Then $\Psi : G \to \mathbb{R}^+$ is a continuous function and also a homomorphism. Now select a continuous function h on G and consider the convolution,

$$\begin{aligned}(f * h)(g) &= \int_G f(x)h(x^{-1}g)\ d\mu(x) \\ &= \int_G f(gx)h(x^{-1})\ d\mu(x).\end{aligned}$$

By the definition of Ψ and $\int_G (f)\ d\mu = 1$, we have

$$h(x)\ d\mu(x) = \int_G h(x^{-1})\Psi(x^{-1})\ d\mu(x).$$

A right translation of h give us

$$\begin{aligned}\int_G h(xg^{-1})\ d\mu(x) &= \int_G h(x^{-1}g^{-1})\Psi(x^{-1})\ d\mu(x) \\ &= \Psi(g) \int_G h((gx)^{-1})\Psi((gx)^{-1})\ d\mu(x) =\end{aligned}$$

$$= \Psi(g) \int_G h(x^{-1})\Psi(x^{-1})\ d\mu(x)$$

Therefore

$$\Psi(g) = \frac{\displaystyle\int_G h(xg^{-1})\ d\mu(x)}{\displaystyle\int_G h(x)\ d\mu(x)}.$$

Now let v and ϕ be continuous functions on G and let Ψ be defined as before. Let v be another left Haar measure. Then

$$\begin{aligned}
\int_G v(x)\ d\mu(x) \int_G \phi(y)\ dv(y) &= \int_G \int_G v(x)\ d\mu(x)\ \phi(y)\ dv(y) \\
&= \int_G \int_G v(xy)\ d\mu(x)\ \Psi(y)\ \phi(y)\ dv(y) \\
&= \int_G \int_G v(xy)\ \phi(y)\ \Psi(y)\ dv(y)\ d\mu(x) \\
&= \int_G \int_G v(y)\ \phi(x^{-1}y)\ \Psi(x^{-1}y)\ dv(y)\ d\mu(x) \\
&= \int_G \int_G \phi((y^{-1}x)^{-1})\ \Psi((y^{-1}x)^{-1})\ d\mu(x)\ v(y)\ dv(y) \\
&= \int_G \int_G \phi(x^{-1})\ \Psi(x^{-1})\ d\mu(x)\ v(y)\ dv(y) \\
&= \int_G d\mu(x) \int_G v(y)\ dv(y).
\end{aligned}$$

Therefore

$$\int_G v\ d\mu \int_G \phi\ dv = \int_G \phi\ d\mu \int_G v\ dv.$$

Now letting v be a positive continuous function and setting

$$c = \frac{\displaystyle\int_G v\ dv}{\displaystyle\int_G v\ d\mu},$$

we have

$$\int_G \phi \, dv = c \int_G \phi \, d\mu.$$

The Haar measure is unique.

□

5.5 Algebraic structure of compact Abelian groups

For the purposes of torsion and divisibility we must introduce some notation and definitions. For Abelian groups we use the endomorphism $\mu_n = \{x \mapsto n \cdot x\} : G \to G$ where $n \cdot x = x + \ldots + x$ (n times).

Definition 5.5.1. For an Abelian topological group G we let:

1. $nG = \mathrm{Im}\,(\mu_n) = \{n \cdot x \mid x \in G\}$;
2. $G[n] = \mathrm{Ker}\,(\mu_n) = \{x \in G \mid n \cdot x = 0\}$;
3. $\mathrm{DIV}(G) = \bigcap_{n \in \mathbb{N}} \overline{nG}$.

We now introduce torsion and divisibility for an Abelian topological group G. The torsion subgroup of G is $\mathrm{tor}(G) = \bigcup_{n \in \mathbb{N}} G[n]$, the union of all the kernels of the endomorphisms. G is called torsion-free if $\mathrm{tor}(G) = 0$. An element $g \in G$ is called divisible if for each $n \in \mathbb{N}$ there is an $x \in G$ with $n \cdot x = g$. The structure theorem on divisible groups shows that there are no divisible groups other than direct sums of $Z(p^\infty)$ (torsion) and Q (torsion-free).

Theorem 5.5.2. *Any divisible group G is a direct sum of quasicyclic and full rational groups. The cardinal numbers of the sets of components $Z(p^\infty)$ (for every p) and Q form a complete independent system of invariants for G.*

The set of all divisible elements is denoted Div(G) and G is divisible if $G \subseteq \mathrm{Div}(G)$. So $\mathrm{Div}(G) = \bigcap_{n \in \mathbb{N}} nG\{g \in G \mid (\forall\, n \in \mathbb{N})\ (\exists\, x \in G)\ n \cdot x = g\}$. Each Abelian group contains a unique largest divisible subgroup which we denote $\mathrm{div}(G)$. Note that $\mathrm{div}(G) \subseteq \mathrm{Div}(G)$. So $\mathrm{div}(G) = \bigcup\{H \mid H \text{ is a divisible subgroup}\}$.

Proposition 5.5.3. *1. If G is a compact Abelian group or a discrete Abelian group, then* $\mathrm{Div}(G) = \mathrm{DIV}(G)$.

2. *If G is a compact Abelian group or a discrete torsion-free Abelian group, then* $\mathrm{div}(G) = \mathrm{Div}(G)$.

Proof:

1. In both cases nG is closed for all $n \in \mathbb{N}$. Hence Div(G) = DIV(G).

2. Observe first that for all $m \in \mathbb{N}$, $\bigcap_{n\in\mathbb{N}} nG \subseteq \bigcap_{n\in\mathbb{N}} mnG$. As $mnG \subseteq (mG \cap nG)$, the family $\{nG \mid n \in \mathbb{N}\}$ is a filter base. The reverse inclusion holds too and therefore $\bigcap_{n\in\mathbb{N}} mnG = \bigcap_{n\in\mathbb{N}} nG = \mathrm{Div(G)}$.

   Now assume that G is torsion-free. Then μ_m is injective and thus maps nG bijectively onto mnG. Hence $\mu_m(\mathrm{Div(G)}) = \bigcap_{n\in\mathbb{N}} mnG$. By our reasoning above, Div(G) is divisible and contained in div(G), i.e. Div(G) $\subseteq$ div(G).

   Now assume that G is compact. If $\mathcal{F}$ is any filter base of compact subsets of G and $f : G \to G$ any continuous self-map, then

$$f(\bigcap \mathcal{F}) = \bigcap_{f\in\mathcal{F}} f(F).$$

   The left side is trivially contained in the right side since if y is an element of the right side, then for each $F \in \mathcal{F}$, the set $\mathcal{X}_F = f^{-1}(y) \cap F$ is nonempty compact. The set $\{X_F : F \in \mathcal{F}\}$ is a filter base of compact sets and thus has an element $x \in \cap\mathcal{F}$ in its intersection. So $f(x) = y$ and thus y is also in the left side.

   Applying this with $\mathcal{F} = \{nG \mid n \in \mathbb{N}\}$ and $f = \mu_m$ we obtain,

$$\mu_m(\bigcap_{n\in\mathbb{N}} nG) = \bigcap_{n\in\mathbb{N}} mnG$$

   and hence Div(G) is divisible as in 1. We can conclude that Div(G) $\subseteq$ div(G).

□

We now provide a proposition, theorem and corollary which we will not prove, since the proofs require work not detailed in this dissertation. Nevertheless, the results are required and shall be stated.

Proposition 5.5.4. *In a locally compact group G, the following hold:*

1. $(nG)^\perp = \hat{G}[n]$;
2. $G[n] = (n\hat{G})^\perp$;
3. $\overline{nG} = (\hat{G}[n])^\perp$;
4. $\mathrm{DIV}(G) = (\mathrm{tor}\,\hat{G})^\perp$;
5. $(\mathrm{DIV}\,G)^\perp = \overline{\mathrm{tor}\,\hat{G}}$.

The following theorem expresses connectivity in algebric terms in a compact Abelian group. The connected component of the identity is the largest divisible subgroup.

Theorem 5.5.5. *Let G denote a compact Abelian group and G_0 is identity component.*

1. $G_0 = \mathrm{Div}(G) = \mathrm{div}(G) = (\mathrm{tor}\,\hat{G})^\perp$.
2. $G_0^\perp = \mathrm{tor}\,\hat{G}$.
3. $\overline{\mathrm{tor}\,G}^\perp = (\mathrm{tor}\,G)^\perp = \mathrm{Div}(\hat{G})$.
4. $(\mathrm{Div}\,\hat{G})^\perp = \overline{\mathrm{tor}\,G}$.

Corollary 5.5.6. *For a compact Abelian group G, the following are all equivalent:*

1. *G is connected;*
2. *G is divisible;*
3. *$\hat{G}$ is torsion-free.*

We now describe the structure of primary groups.

Definition 5.5.7. A compact Abelian group is called a *compact primary group* if its character group is a primary group. A locally compact Abelian group G is called a *primary group* if it is a union of compact primary groups.

Chapter 6

Ramsey functions

Given a compact finite Abelian group G with $r \in \mathbb{N}$, let $s_r(G)$ denote the least upper bound of real $\varepsilon > 0$ such that for every measurable r-colouring of G there exists a monochrome symmetric subset of size $\varepsilon > 0$. Equivalently,

$$s_r(G) = \inf_\phi \sup_{g \in G} \max_{i \in [r]} \mu(\{x \in G : \phi(x) = \phi(gx^{-1}\mathrm{g}) {=} \mathrm{i}\}),$$

where μ is the Haar measure of G, $[r] = \{1, \ldots, r\}$ and $\phi : G \to [r]$ runs over all measurable r-colourings of G. $s_r(G)$ is essentially the most asymmetrical maximal measure of a monochromatic symmetric subset. If G is finite, then

$$s_r(G) = \frac{1}{|G|} \min_\phi \max_{g \in G} \max_{i \in [r]} |\{x \in G : \phi(x) = \phi(gx^{-1}\mathrm{g}) {=} \mathrm{i}\}|.$$

In this Chapter we show $s_r(G) \geq 1/r^2$. We also show that for every measurable $B \subseteq G$, there exists a measurable symmetric subset $B \subseteq A$ such that $\mu(B) \geq (\mu(A))^2$.

We show that the estimate $s_r(G) \geq 1/r^2$ is optimal for Abelian groups. If the group is not Abelian, the estimate fails, and we provide a counter-example for this in Section 6.3.1.

We give a general picture of asymptotic behaviour for $s_r(G)$ for compact Abelian groups using the function $\overline{s}_r(G)$.

6.1 Symmetries in groups and related Ramsey functions

Definition 6.1.1. Let G be a group. A *symmetry* on a group G with respect to a center $g \in G$ is given by the mapping $\eta_g : G \ni x \mapsto gx^{-1}\mathrm{g} \in G$.

This notion appeared in [20]. It is a natural notion since

$$\eta_g = \lambda_g \circ i \circ \lambda_g^{-1} = \rho_g \circ i \circ \rho_g^{-1},$$

where $\lambda_g : G \ni x \mapsto gx \in G$ is the left translation, $\rho_g : G \ni x \mapsto xg \in G$ is the right translation and $i : G \ni x \mapsto x^{-1} \in G$ is the inversion.

It follows from $\lambda_g(x) = gx$ that $\lambda_g^{-1}(gx) = x$ and $\lambda_g^{-1}(x) = g^{-1}x$. Consequently, $\lambda_g^{-1} = \lambda_{g^{-1}}$ and similarly, $\rho_g^{-1} = \rho_{g^{-1}}$. Then

$$\lambda_g \circ i \circ \lambda_g^{-1}(x) = \lambda_g \circ i \circ \lambda_{g^{-1}}(x) = g(g^{-1}x)^{-1} = gx^{-1}g \text{ and}$$
$$\rho_g \circ i \circ \rho_g^{-1}(x) = \rho_g \circ i \circ \rho_{g^{-1}}(x) = (xg^{-1})^{-1}g = gx^{-1}g.$$

Note that a subset $S \subseteq G$ is symmetric if there exists an element $g \in G$, the center of symmetry, such that $gS^{-1}g = S$ [39].

The following are admissible symmetries:

1. The family S of central symmetries where $s : G \to G$ is of the form $s(x) = 2g - x$ for some $g \in G$;
2. The family S_+ of symmetries where $s : G \to G$ is of the form $s(x) = g - x$ for some $g \in G$.

We can immediately conclude that $S \subseteq S_+$.

6.2 Finite Abelian groups

We know that $s_r(G)$ is our most asymmetrical maximal measure of a monochromatic symmetric subset. For a finite Abelian group, we can represent $s_r(G)$ as the greatest number of the form $\frac{k}{|G|}$, such that for every r-colouring of a finite group G, there exists a monochromatic symmetric subset of cardinality k, where $k \in \mathbb{N}$. Results from 6.2 can be found in [39].

We now introduce $\sigma_r(G)$. This is defined as the greatest number of the form $\frac{k}{|G|}$, such that for every r-colouring $\mathcal{X}$ of a finite group G, there exists a subset $X \subseteq G$ of cardinality k and an element g such that $\mathcal{X}(x) = \mathcal{X}(gx^{-1}g)$ for all $x \in X$ and $k \in \mathbb{N}$.

For every r-colouring $\mathcal{X} : G \to \{1, \ldots, r\}$ of a finite group G, let us define

$$S(\mathcal{X}, g) = |\{x \in G : \mathcal{X}(x) = \mathcal{X}(gx^{-1}g)\}|, g \in G$$

$$\sigma_r(G) = \min_{\mathcal{X}:G\to\{1,\ldots,r\}} \frac{1}{|G|} \max_{g\in G} S(\mathcal{X}, g).$$

Theorem 6.2.1. *For every finite Abelian group G and also for every group of odd order*

$$\sigma_r(G) \geq \frac{1}{r}$$

and consequently

$$s_r(G) \geq \frac{1}{r^2}.$$

To prove this theorem we require the following lemma,

Lemma 6.2.2. *Let $A_i = \mathcal{X}^{-1}(i)$. For every $a \in G$, denote $v(a) = |\{x \in G : x^2 = a\}|$. Then*

$$\sum_{g\in G} S(\mathcal{X}, g) = \sum_{i=1}^{r} \sum_{(x,y)\in A_i^2} v(yx^{-1}).$$

Proof:
Compute in two ways the number of all triples $(g, x, y) \in G \times G \times G$ such that gx^{-1}g=y. We obtain

$$\sum_{g\in G} S(\mathcal{X}, g) = \sum_{i=1}^{r} \sum_{(x,y)\in A_i^2} |\{g \in G : gx^{-1}g = y\}|.$$

We notice that

$$\begin{aligned}|\{g \in G : gx^{-1}g = y\}| &= |\{g \in G : gx^{-1}gx^{-1} = yx^{-1}\}| \\ &= |\{x \in G : x.x = yx^{-1}\}| \text{ since } x^2 = g \Rightarrow x = gx^{-1} \\ &= |\{x \in G : x^2 = yx^{-1}\}| \\ &= v(yx^{-1}).\end{aligned}$$

□

We are now able to prove Theorem 6.2.1.

Proof of Theorem 6.2.1:
By Lemma 6.2.2,

$$\sum_{g\in G} S(\mathcal{X}, g) = \sum_{i=1}^{r} \sum_{(x,y)\in A_i^2} v(yx^{-1}).$$

If G has odd order, then $v(yx^{-1})$=1 for all $x, y \in G$. Since the function $x_1^2 + \ldots + x_r^2$, where $x_1 + \ldots + x_r$, attains minimum when $x_1 = \ldots = x_r = \frac{C}{r}$,

$$\sum_{g\in G} S(\mathcal{X}, g) = \sum_{i=1}^{r} |A_i|^2 \geq \underbrace{\left(\frac{|G|}{r}\right)^2 + \ldots + \left(\frac{|G|}{r}\right)^2}_{r} = \frac{|G|^2}{r}.$$

If G is Abelian, then $v(yx^{-1}) > 0$ if and only if $yx^{-1} \in G^2 = \{g^2 : g \in G\}$ and in this case $v(yx^{-1}) = [G : G^2]$. Let C_j $(i \leq j \leq k)$ be cosets of G modulo G^2 and let $C_{j,i} = \mathrm{C}_j \cap A_i$. Then

$$\sum_{g\in G} S(\mathcal{X}, g) = \sum_{i=1}^{r} \sum_{j=1}^{k} |C_{j,i}\ |^2 \cdot k \geq rk\left(\frac{|G|}{rk}\right)^2 \cdot k = \frac{|G|^2}{r}.$$

Therefore, in each case, there exists an element $g \in G$ such that $S(\mathcal{X}, g) \geq \frac{|G|}{r}$ and so $\sigma(\mathcal{X}) \geq \frac{1}{r}$.

□

6.2.1 $\sigma_r(G) = \frac{1}{r}$ and $\sigma_r(G) = 1$

We now describe finite Abelian groups with $\sigma_r(G) = \frac{1}{r}$ and $\sigma_r(G) = 1$.

Theorem 6.2.3. *$\sigma_r(G) = \dfrac{1}{r}$ if and only if r divides $|2G|$.*

Proof:
Define the following subgroups:

$$2G = \{2x : x \in G\};$$
$$B(G) = \{x \in G : 2x = 0\}.$$

Denote $|2G| = m$ and $|B(G)| = k$. Note that $mk = |G|$. Consider the case when $r \nmid m$. Fix any r-colouring $\mathcal{X}$ on a group G. Let C_j $(1 \leq j \leq k)$ be cosets of G modulo $2G$ and let $C_{j,i} = C_j \cap \chi^{-1}(i)$. Then

$$\sum_{i=1}^{r} |C_{j,i}\,|^2 > r\left[\frac{m}{r}\right]^2 = \frac{m^2}{r}.$$

Hence

$$\sum_{g \in G} S(\mathcal{X}, g) = k\sum_{j=1}^{k}\sum_{i=1}^{r} |C_{j,i}\,|^2 > k^2\frac{m^2}{r} = \frac{|G|^2}{r}.$$

So there is an element $g \in G$ such that $S(\mathcal{X}, g) > \dfrac{|G|}{r}$ and so

$$\sigma(\mathcal{X}) > \frac{1}{|G|}.\frac{|G|}{r} > \frac{1}{r}.$$

Now consider the case when $r \mid m$. By Theorem 6.2.1, $\sigma_r(G) \geq \frac{1}{r}$, so it is sufficient to construct a colouring with $\sigma(\mathcal{X}) = \frac{1}{r}$. Select a subgroup F of group G such that $B(G) \subseteq F$ and $[G : F] = r$. Then $[2G : 2F] = r$. Define an r-colouring $\mathcal{X}$ of G as:

1. Every coset of G mod $2F$ is the same colour;
2. Every r cosets of G mod $2F$ which form a coset of G mod $2G$ are coloured in r different colours.

Then

$$\mathcal{X}(x) = \mathcal{X}(2g - x) \Leftrightarrow x - (2g - x) \in 2F \Leftrightarrow$$

$$\Leftrightarrow 2(x-g) \in 2F$$
$$\Leftrightarrow \exists f \in F \text{ s.t. } 2(x-g-f) = 0$$
$$\Leftrightarrow \exists f \in F \text{ s.t. } x-g-f \in B(G)$$
$$\Leftrightarrow x-g \in F + B(G) = F$$
$$\Leftrightarrow x \in g + F.$$

So $S(\mathcal{X}, g) = |F|$ for all $g \in G$. Therefore $\sigma(\mathcal{X}) = \dfrac{S(\mathcal{X}, g)}{|G|} = \dfrac{|F|}{|G|} = \dfrac{1}{|G:F|} = \dfrac{1}{r}$.

□

Theorem 6.2.4. *$\sigma_r(G) = 1$ if and only if:*

1. *$r = 1$, or*
2. *$r = 2$ and G is a cyclic group of order 3 or 5, or*
3. *G is a Boolean group.*

Proof:
Suppose none of the above cases hold. Define the subgroups $2G$ and $B(G)$ as before. Now assume that $|G|$ is even. Then both the subgroups are different from G. Select $x, y \in G$ such that $x + y \notin 2G$ and $x - y \notin B(G)$. Define the colouring $\mathcal{X} : G \to \{1, 2\}$. Now colour the elements x, y using the first colour, and all the other elements of G using the second colour. Set an element $g \in G$ to be an arbitrary center of symmetry of G. Since $x+y \notin 2G$, $2G-x \neq y$. If $2g-x = x$ then $2g-y \neq y$ since $x - y \neq B(G)$. The contradiction $\mathcal{X}(a) \neq \mathcal{X}(2g - a)$ or $\mathcal{X}(b) \neq \mathcal{X}(2g - b)$ follows.

Now assume that $|G|$ is odd. Then $2G = G$. In this case it is evident that the center of symmetry is unique and any two elements of G are symmetric. Since $n \geq 7$, we can select distinct elements $x, y, z \in G$ such that neither of them is a center of symmetry for the other two, i.e.: For any distinct $g \in G$, $s \in \{x, y, z\}, 2g - s \notin \{x, y, z\}$. To see this, pick any distinct $\{x, y\}$. There is a unique colour $g \in G$ such that $y = 2g-x$.

Now pick $z \in G\backslash\{x, y, g, 2x - y, 2y - x\}$. Colour x, y, z with one colour and all the other elements with another colour ($r = 2$). If $g \notin \{x, y, z\}$ and $2g - x = y$ then

$2g - z \notin \{x, y, z\}$, i.e.: x and y are symmetric to each other so z is symmetric to neither. If $g = \{x, y, z\}$ and $g = x$ then $2g - y \notin \{x, y, z\}$, i.e.: x is the center of symmetry g so y is not symmetric to z. It follows that there is $s \in \{x, y, z\}$ such that $\mathcal{X}(s) \neq \mathcal{X}(2g - s)$.

□

Note that each r-colouring in the theorem is symmetric and the number of all r-colourings of a group is r^n. The number of all symmetric r-colourings for finite Abelian groups was established in [41] and for finite groups in [40].

6.3 Compact Abelian groups

Let G be a compact Abelian group with Haar measure μ on it. We assume that G is Hausdorff and that μ is the complete probability measure. The measure of a subset A on a finite group G is naturally $\mu(A) = |A|/|G|$. Results from 6.3 can be found in [1], [2] and [3].

Definition 6.3.1. A subset $A \subseteq G$ is said to be *symmetric* (centrally symmetric) if $s(A) = A$ for some $s \in S_+$ ($s \in S$). We denote $s_r(G)$ for S and $s_r^+(G)$ for S_+.

Since $S \subseteq S_+$, $s_r(G) \leq s_r^+(G)$. Therefore, the lower estimation of $s_r(G)$ is stronger if established for S, and the upper estimation is stronger if established for S_+.

Theorem 6.3.2. *Let $r \geq 2$ and let G be a compact Abelian group with Haar measure μ. Then:*

1. $s_r^+(G) \geq s_r(G) \geq \frac{1}{r^2}$;
2. *if G is a finite group, then $s_r^+(G) > \frac{1}{r^2}$.*

Proof:
1. In every r-colouring there is a one colour subset A of measure $\mu(A) \geq \frac{1}{r}$ and it immediately follows that $\mu(A) \geq \frac{1}{r^2}$.

2. This proof requires the following proposition:

Proposition 6.3.3. *Any measurable set $A \subseteq G$ contains a centrally symmetric subset $B \subseteq A$ of measure $\mu(B) \geq \mu(A)^2$.*

Proof:

The subset $B_g = A \cap (2g - A)$ with any point $g \in G$ is symmetric relative to g. We must show that $\mu(B_g) \geq \mu(A)^2$ holds for $g \in G$. The set $2G = \{2g : g \in G\}$ is a compact subgroup of G and the quotient group $G/2G$ has exponent 2, i.e.: $h = -h$ for all $h \in G/2G$. Let us denote the quotient map $\pi : G \to G/2G$ and the Haar measures on $2G$ and $G/2G$ by μ_1 and μ_2 respectively. μ_1 induces a probability measure that is a copy of itself on each coset $\pi^{-1}(\mathrm{h})$ mod $2G$ where $h \in G/2G$. By [19], the inequality

$$\int_G f(x)\ dx = \int_{G/2G} \int_{\pi^{-1}(h)} f(x)\ d\mu_1(x)\ d\mu_2(h)$$

holds for any measurable function $f : G \to \mathbb{R}$. Let us denote the characteristic function of the set A by $\mathcal{X}_A : G \to \{0, 1\}$ and integrate the relation

$$\mu(A \cap (g - A)) = \int_G \mathcal{X}_A(x)\ \mathcal{X}_A(g - x)\ d\mu(x)$$

with respect to $g \in 2G$ using Fubini's theorem and the Cauchy-Schwarz inequality.

$$\int_{2G} \mu(A \cap (g - A))\ d\mu_1(g)$$

$$= \int_{2G} \int_G \mathcal{X}_A(x)\ \mathcal{X}_A(g - x)\ d\mu(x)\ d\mu_1(g)$$

$$= \int_{2G} \int_G \mathcal{X}_A\ (x) \mathcal{X}_A(g - x)\ d\mu_1(g)\ d\mu(x)$$

$$= \int_{G/2G} \left(\int_{\pi^{-1}(h)} \left(\int_{2G} \mathcal{X}_A(x)\ \mathcal{X}_A(g - x)\ d\mu_1(g) \right) d\mu_1(x) \right) d\mu_2(h)$$

$$= \int_{G/2G} \left(\int_{\pi^{-1}(h)} \mathcal{X}_A(x) \left(\int_{2G} \mathcal{X}_A(g - x)\ d\mu_1(g) \right) d\mu_1(x) \right) d\mu_2(h)$$

$$= \int_{G/2G} \int_{\pi^{-1}(h)} \mathcal{X}_A(x) \int_{\pi^{-1}(-h)} \mathcal{X}_A(g)\ d\mu_1(g)\ d\mu_1(x)\ d\mu_2(h)$$

$$= \int_{G/2G} \left(\int_{\pi^{-1}(h)} \mathcal{X}_A(x)\ d\mu_1(x) \right)^2 d\mu_2(h)$$

$$\geq \left(\int_{G/2G} \int_{\pi^{-1}(h)} \mathcal{X}_A(x)\ d\mu_1(x)\ d\mu_2(h) \right)^2 =$$

$$= \left(\int_G \mathcal{X}_A(x)\ d\mu_(x) \right)^2$$

$$= \mu(A)^2.$$

By the Mean Value Theorem, there is an element $2g \in 2G$ such that
$\mu(A \cap (2g - A)) = \mu(B) \geq \mu(A)^2$.

□

We can now prove 2 of Theorem 6.3.2 by applying the following Proposition to an arbitrary finite Abelian group G.

Proposition 6.3.4. *Any measurable set $A \subset G$ of measure $\mu(A)$, $0 < \mu(A) < 1$, contains a symmetric measurable subset $B \subseteq A$ of measure $\mu(B) > \mu(A)^2$.*

Proof:
The measure of the symmetric subset $B_g = A \cap (g - A)$ will be denoted by $\mu(B_g)$. We must therefore prove that $\mu(B_g) > \mu(A)^2$ for some $g \in G$. As done previously, we integrate the relation

$$\mu(B_g) = \int_G \mathcal{X}_A(x)\ \mathcal{X}_A(g - x)\ d\mu(x)$$

with respect to $g \in G$ (extended symmeteries). Note that in Proposition 6.3.3 this integration was done with respect to $g \in 2G$.

$$\begin{aligned}
\int_G \mu(B_g)\ d\mu(g) &= \int_G \int_G \mathcal{X}_A(x)\ \mathcal{X}_A(g - x)\ d\mu(x)\ d\mu(g) \\
&= \int_G \mathcal{X}_A(x) \int_G \mathcal{X}_A(g - x)\ d\mu(g)\ d\mu(x) \\
&= \int_G \mathcal{X}_A(x)\ \mu(A)\ d\mu(x) \\
&= \mu(A)^2.
\end{aligned}$$

If we suppose that $\mu(B) \leq \mu(A)^2$ for all $g \in G$ and since
$\int_G \mu(B_g)\ d\mu(g) = \mu(A)^2$, then $\mu(B_g)$ is almost equal to $\mu(A)^2$; a contradiction.

□

Proposition 6.3.5. *Let H be a closed subgroup of a compact Abelian group G. Then $s_r^+(G) \leq s_r^+(G/H)$.*

Proof:
Let us denote the Haar measures on G and G/H by μ and λ respectively. By definition, the uniqueness of the Haar measure on G/H implies that the relation $\lambda(A) = \mu(\pi^{-1}(A))$, where $\pi : G \to G/H$ is the quotient map, holds for any measurable subset $A \subseteq G/H$.

Now let $\mathcal{X} : G/H \to [r]$ be an arbitrary colouring of the quotient group G/H. It suffices to prove that G/H contains a one colour symmetric set A of measure arbitrarily close to $s_r^+(G)$.

Let us consider the colouring $\mathcal{X} \circ \pi$ of G. If $A_1, \ldots, A_r$ are the monchromatic classes of $\mathcal{X}$, then let us denote $B_i = \pi^{-1}(A_i)$ as the monochromatic classes of $\mathcal{X} \circ \pi$ where $i \leq r$. Now fix an arbitrary positive ε. By the definition of $s_r^+(G)$, the measure of the one colour symmetric subset $B = B_i \cap (g - B_i)$ in G must exceed $s_r^+(G) - \varepsilon$.

Consider the one colour symmetric subset $A = A_i \cap (\pi(g) - A_i)$ in G/H for the same values of i and g. Since $B \subseteq \pi^{-1}(A)$, the measure of A satisfies the bound $\lambda(A) = \mu(\pi^{-1}(A)) \geq \mu(B) > s_r^+(G) - \varepsilon$. Since our chosen ε can be arbitrarily small, $s_r^+(G) \leq s_r^+(G/H)$ is proved.

□

Proposition 6.3.6. *The relation $s_r^+(G) \leq s_r^+(H)$ holds for any compact Abelian group G.*

Proof:
We first prove the existence of a Borel set U that intersects each coset of G relative to H in exactly one point. Consider a neighbourhood V of zero in G such that the neighbourhoods of $h + V$ and $h' + V$ of different elements h and h' in H do not intersect. Now take the finite subcovering $V_1, \ldots, V_k$ of the covering $\{g + V\}_{g \in G}$ of G. The set U will belong to the algebra generated by the family of open set $\{h + V_i\}_{h \in H}$ where $i \leq k$. Set

$$U_0 = \emptyset, W_0 = \emptyset, U_i = U_{i-1} \cup (V_i \backslash W_{i-1}), W_i = \bigcup_{0 \neq h \in H} (h + U_i), \text{ and } U = U_k.$$

U_i and W_i do not intersect for $i \leq k$ and $U_k \cap W_k = G$. Therefore, U is a Borel set. Note that each $g \in G$ can be uniquely represented as the sum $g = h + u$, where $h \in H$ and $u \in U$.

Let us denote the Haar measures on G and H by μ and λ respectively. Since H is finite, it has a colouring $\mathcal{X} : H \to [r]$ for which the number of elements in any one colour subset does not exceed $|H|\, s_r^+(G)$. Let $A_i = \mathcal{X}^{-1}(i)$ for $i \in [r]$.

Now define a colouring $\mathcal{X}^{'} : G \to [r]$ of G by setting $\mathcal{X}^{'}(g) = \mathcal{X}(h)$ for $g = h + u$, where $h \in H$ and $u \in U$. Under the colouring $\mathcal{X}^{'}$, the maximal monochromatic set that has the colour i and is symmetric with respect to the transformation $s(x) = g - x$ has the form $B_g = (A_i + U) \bigcap (g - (A_i + U))$. By the definition of $s_r^+(G)$, the inequality

$$\mu(B_g) > s_r^+(G) - \varepsilon$$

holds for some arbitrary $\varepsilon > 0$, $i \in [r]$ and $g \in G$. We must show that

$$\mu(B_g) \leq s_r^+(H)$$

which with $\mu(B_g) > s_r^+(G) - \varepsilon$ will prove the proposition.

Using the relation $\mathcal{X}_{A_i+U}(x) = \sum\limits_{a \in A_i} \mathcal{X}_U(x - a)$, we write

$$\mu(B_g) = \int_G \sum_{a \in A_i} \mathcal{X}_U(x - a) \sum_{a^{'} \in A_i} \mathcal{X}_U(g - x - a^{'})\, dx.$$

Changing the order of integration and summation and setting $x = y + a$ gives us

$$\mu(B_g) = \int_U \sum_{a, a^{'} \in A_i} \mathcal{X}_U(g - (a + a^{'}) - y)\, dy.$$

Since U intersects each coset in a single point, there exists a unique element $h(y) \in H$ such that $g - h(y) - y \in U$. In light of this, our previous relation becomes

$$\begin{aligned} \mu(B_g) &= \int_U \sum_{\substack{a, a^{'} \in A_i \\ a + a^{'} = h(y)}} 1\, dy \\ &= \int_U |A_i \cap (h(y) - A_i)|\, dy \leq \end{aligned}$$

$$\leq \int_U |H| s_r^+(H))\ dy$$
$$= s_r^+(H).$$

Therefore $\mu(B_g) \leq s_r^+(H)$.

□

6.3.1 Counter-example for non-Abelian groups

The estimate of $s_r(G) \geq \frac{1}{r^2}$ is optimal as we have seen for Abelian groups. For non-Abelian groups, the estimate fails, for which we provide the only known counter example [37]. The example requires the use of the quarternion group, $Q = \{\pm 1, \pm i, \pm j, \pm k\}$.

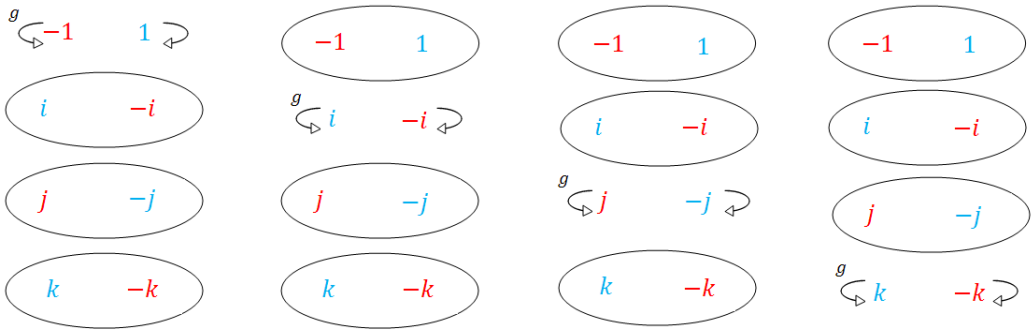
Q is an eight element, non-commutative group and defined by
$(-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1$, where 1 is the identity element and -1 commutes with all other elements of the group. This group provides a very interesting Cayley table.

Quarternion multiplication is non-commutative, since, for example, the multiplication of basis elements yields $jk = i$ but $kj = -i$. Using $ijk = -1$, we can right or left multiply this by one of i, j, k giving us all the following possible products:

$$\begin{aligned} ij &= k \qquad & ji &= -k \\ jk &= i \qquad & kj &= -i \\ ki &= j \qquad & ik &= -j \end{aligned}$$

Note that any two elements of i, j, k can generate the entire group.

Now consider the 2-colouring of the quarternion group as a counter-example as to why $s_r(Q) \not\geq \frac{1}{r^2}$. The symmetry $x \mapsto gx^{-1}g$ becomes less clear due to the groups non-commutativity. Elements of the group are only symmetric with themselves and their negative, i.e.: 1 is only symmetric with 1 and -1, i is only symmetric with i and $-i$, j is only symmetric with j and $-j$ and k is only symmetric with k and $-k$. Therefore, from $s_2(Q)$ we can identify the following colouring:



A selected 2-colouring of the Quarternion group

It is evident that for the above arrangement and colouring, whichever element is chosen as the center g, we are always left with two different colour monochromatic subsets of equal measure (due to the elements being symmetric to themselves). Each center g provides us with a subset of measure $\frac{1}{8}$ and its symmetric element also provides us with a subset of measure $\frac{1}{8}$. The other elements which are symmetric to each other do not provide monochromatic subsets.

From the definition of $s_r(Q)$ and the diagram above, $\max_{i\in[r]} = \frac{1}{8}$ for each colouring. All other symmetric subsets are not monochromatic. Therefore, our maximum monochromatic colouring of all the centers $g \in Q$ is $\max_{g\in Q} = \frac{1}{8}$.

Alternative colourings of Q will provide larger maximum monochromatic colourings and hence $\max_{g\in Q} > \frac{1}{8}$. However, the function $s_2(Q)$ requires the most asymmetrical maximum monochromatic colouring. This is evidently achieved from the colouring above and so $\min_\phi = \frac{1}{8}$. Therefore $s_2(Q) = \frac{1}{8}$ which is less than $\frac{1}{2^2}$.

The following results can be found in [37].

Theorem 6.3.7. *Let G be a compact topological group and let $f : G \to G$ be a continuous transformation of G such that $H = \operatorname{Im} f^*$ is a subgroup of G and for every measurable $C \subseteq H, \mu_G((f^*)^{-1}(C)) = \mu_H(C)$. Then for every measurable $C \subseteq G$ there exists $S \subseteq C$ and $g \in G$ such that $f(Sg^{-1}) \subseteq Cg^{-1}$ and $\mu(S) \geq (\mu(C))^2$.*

The proof of Theorem 6.3.7 is based on the following lemma.

Lemma 6.3.8. *Let G be a compact topological group and let $f : G \to G$ be a measurable transformation of G. Then for every measurable $C \subseteq G$ there exists $S \subseteq C$ and $g \in G$ such that $f(Sg^{-1}) \subseteq Cg^{-1}$ and*

$$\mu(S) \geq \int_G \mathcal{X}_C(x) \int_G \mathcal{X}_C(f^*(y)x)\ dy\ dx,$$

where $\mathcal{X}_C(x)$ is the characteristic function of $C \subseteq G$.

Proof:
For every $y \in G$, denote $S(y) = C \cap f^{-1}(Cy^{-1})y$. Then

$$S(y) \subseteq C, \qquad f(S(y)y^{-1}) \subseteq Cy^{-1}, \qquad \mu(S(y)) = \textstyle\int_G \mathcal{X}_{S(y)}(x)\ dx.$$

It is easy to check that

$$\mathcal{X}_{C\cap D}(x) = \mathcal{X}_C(x)\mathcal{X}_D(x), \qquad \mathcal{X}_{C_y}(x) = \mathcal{X}_C(xy^{-1}), \qquad \mathcal{X}_{h^{-1}(C)}(x) = \mathcal{X}_C(h(x)).$$

Consequently, $\mathcal{X}_{S(y)}(x) = \mathcal{X}_C(x)\mathcal{X}_C(f(xy^{-1})y)$ and

$$\mu(S(y)) = \int_G \mathcal{X}_C(x)\mathcal{X}_C(f(xy^{-1})y)\ dx.$$

Integrating this equation we obtain

$$\begin{aligned}
\int_G \mu(S(y))\ dy &= \int_G \int_G \mathcal{X}_C(x)\mathcal{X}_C(f(xy^{-1})y)\ dx\ dy \\
&= \int_G \mathcal{X}_C(x) \int_G \mathcal{X}_C(f(xy^{-1})y)\ dy\ dx \\
&= \int_G \mathcal{X}_C(x) \int_G \mathcal{X}_C(f(y^{-1})yx)\ dy\ dx \\
&= \int_G \mathcal{X}_C(x) \int_G \mathcal{X}_C(f^*(y)x)\ dy\ dx.
\end{aligned}$$

By the theorem of the mean, there exists $g \in G$ such that

$$\mu(S(G)) \geq \int_G \mathcal{X}_C(x) \int_G \mathcal{X}_C(f^*(y)x)\ dy\ dx.$$

Put $S = S(g)$.

□

Proof of Theorem 6.3.7:
By Lemma 6.3.8, it suffices to prove that

$$\int_G \mathcal{X}_C(x) = \int_G \mathcal{X}_C(x + y - f(y))\ dy\ dx \geq (\mu(C))^2.$$

Denote $H = \mathrm{Im}\,(1-f)$ and $F = G/H$. Then

$$\begin{aligned}
&\int_G \mathcal{X}_C(x) \int_G \mathcal{X}_C(x+y-f(y))\ dy\ dx \\
&= \int_G \mathcal{X}_C(x) \int_G \mathcal{X}_C(x+z)\ dz\ dx \\
&= \int_F \int_H \mathcal{X}_C(x+y) \int_H \mathcal{X}_C(x+y+z)\ dz\ dy\ dx \\
&= \int_F \int_H \mathcal{X}_C(x+y) \int_H \mathcal{X}_C(x+z)\ dz\ dy\ dx \\
&= \int_F \left(\int_H \mathcal{X}_C(x+y)\ dy \right)^2 dx \\
&\geq \left(\int_F \int_H \mathcal{X}_C(x+y)\ dy\ dx \right)^2 \\
&= \left(\int_G \mathcal{X}_C(x+y)\ dx \right)^2 \\
&= (\mu(C))^2.
\end{aligned}$$

Theorem 6.3.9. *Let A be a compact topological Abelian group, let f be the inversion of A, and let $G = A \leftthreetimes \mathbb{C}_4$ be the semidirect product with respect to the homomorphism $\mathbb{C}_4 \ni j \mapsto f^j \in \mathrm{Aut}(A)$. Then for every $r \geq 2, 1/2r^2 \leq s_r(G) \leq 1/2s_r(A)$. In particular, if $s_r(A) = 1/r^2$, then $s_r(G) = 1/2r^2$.*

Proof:
Since G contains an Abelian subgroup $H = A \times \mathbb{C}_2$, the first inequality follows from Theorem 6.3.7. To prove the second one, calculate

$$\begin{aligned}
(a, f^i)(a, f^j)^{-1}(a, f^i) &= \begin{cases} (2a-x, f^j) & \text{if } i \equiv j \equiv 0 \bmod (2), \\ (2a-x, f^j) & \text{if } i \equiv j \equiv 1 \bmod (2), \\ (x, f^{j+2}) & \text{if } i \equiv 0 \bmod (2) \text{ and } j \equiv 1 \bmod (2), \\ (x, f^{j+2}) & \text{if } i \equiv 1 \bmod (2) \text{ and } j \equiv 0 \bmod (2), \end{cases} \\
&= \begin{cases} (2a-x, f^j) & \text{if } i - j \equiv 0 \bmod (2), \\ (x, f^{j+2}) & \text{if } i - j \equiv 1 \bmod (2). \end{cases}
\end{aligned}$$

Given any r colouring $\varphi : A \mapsto \mathbb{Z}_r$, define the extension $\overline{\varphi} : G \mapsto \mathbb{Z}_r$ by

$$\overline{\varphi}(x, f^j) = \begin{cases} \varphi(x) & \text{if } j = 0, 1, \\ \varphi(x) + 1 & \text{if } j = 2, 3. \end{cases}$$

Let $S \subseteq G$ be a monochrome (with respect to $\overline{\varphi}$) and let $(a, f^i)S^{-1}(a, f^i) = S$. Then either $S \subseteq H$ or $S \subseteq G \backslash H$. If $S \subseteq G \backslash H$, then $S_H = S \cdot (0, f) \subseteq H$ is also monochrome and $(a, 0)S_H^{-1}(a, 0) = S_H$. So we may assume that $S \subseteq H$.

Put $P = S \cap A, Q = S \cap (H \backslash A), Q_A = Q \cdot (0, f^2)$. Then $P, Q_A \subseteq A$ are monochrome (with respect to φ) and symmetric with respect to $(a, 0)$ and $\mu(S) = \mu(P) + \mu(Q_A) = \frac{1}{4}(\mu_A(P) + \mu_A(Q_A))$. It follows from this that $s_r(G) \leq \frac{1}{2} s_r(A)$.

□

6.3.2 Ramsey functions in compact Abelian groups

We now show a general picture of asymptotic behaviour for $s_r(G)$ for compact Abelian groups. We use the function $\overline{s}_r(G)$ which is defined as

$$\overline{s}_r(G) = \min_\phi \frac{1}{|G|} \sum_{g \in G} \left(\frac{1}{r} \sum_{i \in [r]} |\{x \in G : \phi(x) = \phi(gx^{-1}g) = i\}| \right).$$

If G is infinite, then $\overline{s}_r(G)$ is defined as

$$\overline{s}_r(G) = \inf_\phi \int_G \left(\frac{1}{r} \sum_{i \in [r]} \mu(\{x \in G : \phi(x) = \phi(gx^{-1}g) = i\}) \right) dg.$$

To prove that $s_r(G) \geq \frac{1}{r^2}$ we first prove $\overline{s}_r(G) \geq \frac{1}{r^2}$. Since $\overline{s}_r(G) \leq s_r(G)$ it immediately follows that $\frac{1}{r^2} \leq \overline{s}_r(G) \leq s_r(G)$. Results from Section 6.3.2 can be found in [17].

Lemma 6.3.10. *Let G be an Abelian group and let B be a Boolean subgroup of G. Then B is a direct summand of G if and only if $B \cap 2G = \{0\}$.*

Proof:
Necessity is obvious. Sufficiency: We let $A = 2G + B$. Since $B \cap 2G = \{0\}$, by the definition of a direct sum, we have $A = 2G \oplus B$. Since $G/2G$ is Boolean, $A/2G$ must be a direct summand of $G/2G$ giving us $G/2G = A/2G \oplus C/2G$ where C is some subgroup of G containing $2G$. It follows that $G = B \oplus C$.

□

We denote $B_0(G)$ as our maximal Boolean subgroup of G. We can represent $B_0(G)$ as a direct summand in the following ways: $G = G/B_0(G) \oplus B_0(G)$ and $B_0(G/B_0(G)) = \{0\}$. The following lemma states the intuitive result that the summands in the decomposition $G = G/B_0(G) \oplus B_0(G)$ do not depend, up to isomorphism, on the choice of $B_0(G)$.

Lemma 6.3.11. *Let G be an Abelian group and let B_1 and B_2 be maximal Boolean subgroups of G and direct summands. Then B_1 is isomorphic to B_2 and G/B_1 is isomorphic to G/B_2.*

Proof:
Let $G = A_1 \oplus B_1 = A_2 \oplus B_2$. Then we also have $G = A_1 \oplus B_2 = A_2 \oplus B_1$. By Lemma 6.3.10 and maximality of B_1, $A_1 \cap B_2 = 0$, and by maximality of B_2, $B_1 \subseteq A_1 + B_2$, so $G = A_1 \oplus B_2$.

Now $G = A_1 \oplus B_1 = A_1 \oplus B_2$ implies that B_1 is isomorphic to B_2. Similarly, $G = A_1 \oplus B_1 = A_2 \oplus B_1$ implying that A_1 is isomorphic to A_2.

□

The aim of this Section is to prove the following two theorems:

Theorem 6.3.12. *Suppose that $\varepsilon > 0$ is given and $r \in \mathbb{N}$. Let $n_0, n_1 \in \mathbb{N}$ such that:*

$$\frac{2\sqrt{3 \ln rn_0} + 1}{\sqrt{n_0}} < \varepsilon \text{ and } n_1 \geq \frac{n_0^2}{2}.$$

Then for every finite Abelian group G with $|G| \geq n_1$

$$\frac{1}{r^2} \leq s_r(G) < \frac{1}{r^2} + \varepsilon \text{ if } |G/B_0(G)| \geq n_0$$

and

$$\overline{s}_r(G/B_0(G)) \leq s_r(G) < \overline{s}_r(G/B_0(G)) + \varepsilon$$

otherwise.

Theorem 6.3.13. *For every infinite compact Abelian group G,*

$$s_r(G) = \begin{cases} \dfrac{1}{r^2} & \text{if } G/B_0(G) \text{ is infinite} \\ \overline{s}_r(G/B_0(G)) & \text{otherwise.} \end{cases}$$

Let us use the following notations:

$$S(G,\phi,g,i) = \{x \in G : \phi(x) = gx^{-1}g = i\};$$

$$s(G,\phi,g,i) = \mu(S(G,\phi,g,i));$$

$$s(G,\phi) = \sup_{g\in G} \max_{i\in[r]} \text{s(G,}\phi, g, i);$$

$$\overline{s}(G,\phi) = \int_G \left(\frac{1}{r}\sum_{i\in[r]} \text{s(G,}\phi, g, i)\right) dg; \text{ so}$$

$$s_r(G) = \inf_\phi\ s(G,\phi) \text{ and}$$

$$\overline{s}_r(G) = \inf_\phi\ \overline{s}(G,\phi).$$

Lemma 6.3.14. *Let G be a compact group and let H be a continuous homomorphic image of G. Then $s_r(G) \leq s_r(H)$ and $\overline{s}_r(G) \leq \overline{s}_r(H)$.*

Proof:
Let $f : G \to H$ be a continuous surjective homomorphism and let ψ be a measurable r-colouring of H. Define the colouring ϕ of G by $\phi = \psi \circ f$. We must show that $s(G,\phi) = s(H,\psi)$ and $\overline{s}(G,\phi) = \overline{s}(H,\psi)$.

Let us first show that $s(G,\phi) = s(H,\psi)$. For every $x \in G$ and $i \in [r]$ we have

$$\begin{aligned} s(G,\phi,x,i) &= \mu_G(\{y \in G : \phi(y) = \phi(xy^{-1}x) = i\}) \\ &= \mu_G(\{y \in G : \psi(f(y)) = \psi(f(x)f(y^{-1})f(x)) = i\}) \\ &= \mu_H(\{z \in H : \psi(z) = \psi(f(x)(z^{-1})f(x)) = i\}) \\ &= s(H,\psi,f(x),i). \end{aligned}$$

Therefore,

$$\begin{aligned} s(G,\phi) &= \sup_{x\in G} \max_{i\in[r]} s(G,\phi,x,i) \\ &= \sup_{x\in G} \max_{i\in[r]} s(H,\psi,f(x),i) \\ &= \sup_{y\in H} \max_{i\in[r]} s(H,\psi,y,i) \\ &= s(H,\psi). \end{aligned}$$

Finally, we can show that $\overline{s}(G,\phi) = \overline{s}(H,\psi)$.

$$\begin{aligned}
\overline{s}(G,\phi) &= \frac{1}{r}\sum_{i\in[r]}\int_G s(G,\phi,x,i)\ dx \\
&= \frac{1}{r}\sum_{i\in[r]}\int_G s(H,\psi,f(x),i)\ dx \\
&= \frac{1}{r}\sum_{i\in[r]}\int_H s(H,\psi,y,i)\ dy \\
&= \overline{s}(H,\psi).
\end{aligned}$$

□

Lemma 6.3.15. *Let G be a compact group and let B be a compact Boolean group. Then $\overline{s}_r(G\times B) = \overline{s}_r(G)$.*

Proof:
By Lemma 6.3.14, we only need to prove $\overline{s}_r(G\times B) \geq \overline{s}_r(G)$.

Let $\phi : G\times B \to [r]$ be a measurable r-colouring of $G\times B$. For each $y\in B$, define $\phi_y : G\to[r]$ by $\phi_y(x) = \phi(x,y)$. Then

$$\begin{aligned}
s(G\times B,\phi,(u,v),i) &= \mu_{G\times B}(\{(x,y)\in G\times B : \phi(x,y) = \phi(ux^{-1}u, vy^{-1}v) = i\}) \\
&\qquad \text{Note that } x\mapsto ux^{-1}u \text{ and } y\mapsto vy^{-1}v \\
&= \mu_{G\times B}(\{(x,y)\in G\times B : \phi(x,y) = \phi(ux^{-1}u, y) = i\}) \\
&= \mu_{G\times B}(\{(x,y)\in G\times B : \phi_y(x) = \phi_y(ux^{-1}u) = i\}) \\
&= \int_B \mu_B(\{x\in G : \phi_y(x)\phi_y(ux^{-1}u) = i\})\ dy \qquad \text{by definition} \\
&= \int_B s(G,\phi_y,u,i)\ dy.
\end{aligned}$$

Then

$$\overline{s}(G\times B,\phi) = \int_G\int_B \frac{1}{r}\sum_{i\in[r]} s(G\times B,\phi,(u,v),i)\ du\ dv =$$

$$= \frac{1}{r}\sum_{i\in[r]}\int_G\int_B s(G\times B,\phi,(u,v),i)\ du\ dv$$

$$= \frac{1}{r}\sum_{i\in[r]}\int_G\int_B\left(\int_B s(G,\phi_y,u,i)dy\right)\ du\ dv$$

$$\text{since}\ \ \mathrm{s(G}\times B,\phi,(u,v),i) = \int_B s(G,\phi_y,u,i)\ dy$$

$$= \frac{1}{r}\sum_{i\in[r]}\int_G\left(\int_B s(G,\phi_y,u,i)\ dy\right)\ du$$

$$= \int_B\left(\frac{1}{r}\sum_{i\in[r]}\int_G s(G,\phi_y,u,i)\ du\right)\ dy$$

$$= \int_B \overline{s}(G,\phi_y)\ dy$$

$$\geq \overline{s}(G,\phi_y)\ dy.$$

It follows that for some $y \in B$, $\overline{s}_r(G\times B) \geq \overline{s}_r(G)$. By Lemma 6.3.14, $\overline{s}_r(G\times B) = \overline{s}_r(G)$.

□

Proposition 6.3.16. *Let G be a finite group and let B be a finite Boolean group. Then*

$$s_r(G\times B) \leq \overline{s}_r(G) + \frac{|G|}{|B|}.$$

Proof:
Let $\psi : G \to \mathbb{Z}(r)$ with $\overline{s}_r(G) = \overline{s}(G,\psi)$ and $\{C_k : k < l\}\bigcup\{D\}$ be a partition of B such that $|C_k| = r|G|$ where $r|G| > |D|$. It is possible for D to be the empty set or C_k to be the empty set when $l = 0$.

Enumerate every C_k as $\{c^k_{g,i} : g \in G, i < r\}$. Now define $\phi : G\times B \to \mathbb{Z}(r)$ so that

$$\phi(x,y) = \psi(xg) + i \qquad \text{if } y = c^k_{g,i}$$

and

$$|\phi^{-1} \cap (G\times D)| \leq |G|^2 \qquad \text{for all}\ \ \mathrm{i} \in \mathbb{Z}_r.$$

Then we have

$$
\begin{aligned}
&S(G \times B, \phi, (g^*, b^*), i^*) \cap (G \times \{c^k_{g,i}\}) \\
&\quad = \{(x, c^k_{g,i}) : \phi(x, c^k_{g,i}) = \phi(g^* x^{-1} g^*, 2b^* - c^k_{g,i}) = i^*\} \\
&\quad = \{(x, c^k_{g,i}) : \phi(x, c^k_{g,i}) = \phi(g^* x^{-1} g^*, c^k_{g,i}) = i^*\} \\
&\quad = \{(x, c^k_{g,i}) : \psi(xg) + i = \psi(g^* x^{-1} g^* g) + i = i^*\} \qquad (\text{since } \phi(x, y) = \psi(xg) + i) \\
&\quad = \{(x, c^k_{g,i}) : \psi(xg) = \psi(g^* g (xg)^{-1} g^* g) = i^* - i\} \\
&\quad = \{xg^{-1} : \psi(x) = \psi(g^* g x g^{-1} g^* g) = i^* - i\} \times \{c^k_{g,i}\} \\
&\quad = (S(G, \psi, g^* g, i^* - i) g^{-1}) \times \{c^k_{g,i}\}.
\end{aligned}
$$

It follows that

$$|S(G \times B, \phi, (g^*, b^*), i^*) \cap (G \times \{c^k_{g,i}\})| = |(S(G, \psi, g^* g, i^* - i)|.$$

Now

$$
\begin{aligned}
&|S(G \times B, \phi, (g^*, b^*), i^*) \cap (G \times C_k)| \\
&\quad = \sum_{\substack{g \in G \\ i \in [r]}} |S(G \times B, \phi, (g^*, b^*), i^*) \cap (G \times \{c^k_{g,i}\})| \\
&\quad = \sum_{\substack{g \in G \\ i \in [r]}} |S(G, \psi, g^* g, i^* - i)| \\
&\quad = \sum_{\substack{g \in G \\ i \in [r]}} |S(G, \psi, g, i)| \\
&\quad = r \ |G|^2 \ \overline{s}(G, \psi).
\end{aligned}
$$

This gives us

$$|S(G \times B, \phi, (g^*, b^*), i^*)| = r \, |G|^2 \, \overline{s}(G, \psi) + |S(G \times B, \phi, (g^*, b^*), i^*) \cap (G \times D)|.$$

We can say

$$
\begin{aligned}
&S(G\times B,\phi)-\overline{s}(G\times B,\phi)\\
&\quad\leq \frac{1}{|G|.|B|}\max_{(g^*,b^*)}\max_{i^*}|S(G\times B,\phi,(g^*,b^*),i^*)\cap(G\times D)|\\
&\quad\leq \frac{1}{|G|.|B|}|G|^2\\
&\quad= \frac{|G|}{|B|}.
\end{aligned}
$$

□

Proposition 6.3.17. *For every finite Abelian group G with $B_0(G)=\{0\}$*

$$s_r(G)\leq\frac{1}{r^2}+\frac{2\sqrt{3\ln r|G|}+1}{\sqrt{|G|}}.$$

Proof:

We notice that the maximal Boolean subgroup of G being a direct summand is the empty set. The inequality trivially holds for $|G|=1$. This is because we can only use one colour to colour a single element group and this results in $s_r(G)=1$. For any r-colouring the inequality is thus satisfied. We therefore suppose that $|G|>1$. Let us denote $B=B(G)$ and $|B(G)|=m$. Then $|G|=2n+m$ for some $n\geq 1$. If $m=2$ and $n=1$ then $G=\mathbb{Z}(4)$, and again the inequality immediately holds for all r-colourings. We therefore suppose that if $m=2$, then $n\geq 2$.

Given $\delta>0$, denote $N(\delta)$ to be the number of all colourings $\phi:G\to[r]$ such that

$$s(G,\phi)\geq\frac{1}{r^2}+\delta+\frac{m}{|G|}.$$

Now consider an arbitrary colouring ϕ. We have that $s(G,\phi)=s(G,\phi,g,i)$ where $g\in G$ and $i\in[r]$. The set $g+B$ is the set of fixed points which allow the symmetry $G\ni x\mapsto 2g-x\in G$. The subset $A=s(G,\phi,g,i)\backslash(g+B)$ leads us to $|A|\geq 2n(\frac{1}{r^2}+\delta)$. Hence

$$
\begin{aligned}
\mathrm{N}(\delta)&\leq|G|\sum_{k\geq n(\frac{1}{r^2}+\delta)}\binom{n}{k}r(r^2-1)^{n-k}\ r^m\\
&\leq|G|\ r\ r^{|G|}\sum_{k\geq n(\frac{1}{r^2}+\delta)}\binom{n}{k}\left(\frac{1}{r^2}\right)^k\left(\frac{r^2-1}{r^2}\right)^{n-k}\\
&\leq r^{|G|}\ r|G|\ e^{\frac{-\delta^2 n}{4}}.
\end{aligned}
$$

We used the following inequality from [4],

$$\sum_{k \geq n(p+\delta)} \binom{n}{k} p^k q^{n-k} \leq e^{\frac{-\delta^2 n}{4}}$$

where p and q are non negative reals with $p + q = 1$. Now we solve the inequality

$$r|G|\, e^{\frac{-\delta^2 n}{4}} < 1$$

and obtain

$$\begin{aligned}
e^{\frac{-\delta^2 n}{4}} &< \frac{1}{r|G|} \\
\ln(e^{\frac{-\delta^2 n}{4}}) &< \ln(\frac{1}{r|G|}) \\
\frac{-\delta^2 n}{4} &< \ln(r|G|)^{-1} \\
-\delta^2 &< \frac{4}{n} \ln(r|G|)^{-1} \\
\delta^2 &> \frac{4}{n} \ln(r|G|) \text{ and so} \\
\delta &> 2\sqrt{\frac{\ln(r|G|)}{n}}.
\end{aligned}$$

We now show that $n \geq \frac{|G|}{3}$. It suffices to show that $n \geq m$ since $n \geq \frac{|G|}{3} \Rightarrow n \geq \frac{2n+m}{3} \Rightarrow n \geq m$. The inequality is trivially true for $m = 1$ since $n \geq 1$ or $m = 2$ since we supposed that $n \geq 2$ for $m = 2$. We therefore suppose that $m > 2$.

Let $b_1, \ldots, b_k$ be a basis in B. Since $B_0(G) = \{0\}$, there exists $a_1, \ldots, a_k$ in G such that $2a_1 = b_1, \ldots, 2a_k = b_k$. Let $H = \langle a_1, \ldots, a_k \rangle$. Then $B \subset H \subseteq G, B = \bigoplus_k \mathbb{Z}(2)$ and $H = \bigoplus_h \mathbb{Z}(4)$. Consequently, $|B| = 2^k = m$ and $|H| = 4^k = m^2$. This leads us to

$$2n \geq m^2 - m \Rightarrow n \geq \frac{m(m-1)}{2} \geq m \qquad (n \geq m).$$

It follows that,

$$\delta = 2\sqrt{\frac{3\ln(r|G|)}{|G|}}$$

is a solution of the inequality. Therefore, for δ, $N(\delta) < r^{|G|}$ and there is a colouring $\phi : G \to [r]$ with

$$\begin{aligned} s(G,\phi) &< \frac{1}{r^2} + \delta + \frac{m}{|G|} \\ &= \frac{1}{r^2} + 2\sqrt{\frac{3\ln(r|G|)}{|G|}} + \frac{m}{|G|} \\ &\leq \frac{1}{r^2} + 2\sqrt{\frac{3\ln(r|G|)}{|G|}} + \frac{1}{\sqrt{|G|}} \\ &= \frac{1}{r^2} + \frac{2\sqrt{3\ln(r|G|)}+1}{\sqrt{|G|}}. \end{aligned}$$

□

If we define symmetries on a compact Abelian group G as mappings of the form $G \ni x \mapsto g - x \in G$ (extended symmetries) where $g \in G$ instead of $G \ni x \mapsto 2g - x \in G$ (central symmetries) then we obtain the function $s_r^+(G)$ instead of $s_r(G)$. We already know that $s_r(G) \leq s_r^+(G)$ and therefore

$$s_r(G) \leq s_r^+(G) \leq \frac{1}{r^2} + \frac{2\sqrt{3\ln(r|G|)}+1}{\sqrt{|G|}}.$$

Let us restate Theorems 6.3.12 and 6.3.13 and prove them.

Theorem 6.3.12 Suppose that $\varepsilon > 0$ is given and $r \in \mathbb{N}$. Let $n_0, n_1 \in \mathbb{N}$ such that:

$$\frac{2\sqrt{3\ln rn_0}+1}{\sqrt{n_0}} < \varepsilon \text{ and } n_1 \geq \frac{n_0^2}{2}.$$

Then for every finite Abelian group G with $|G| \geq n_1$

$$\frac{1}{r^2} \leq s_r(G) < \frac{1}{r^2} + \varepsilon \text{ if } |G/B_0(G)| \geq n_0$$

and

$$\overline{s}_r(G/B_0(G)) \leq s_r(G) < \overline{s}_r(G/B_0(G)) + \varepsilon$$

otherwise.

Proof of Theorem 6.3.12:

This is the proof for the finite case. Let us denote $B_0 = B_0(G)$ and $G_0 = G/B_0$. Suppose that $|G_0| \geq n_0$. We already have that $s_r(G) \geq \frac{1}{r^2}$. By Lemma 6.3.14, $s_r(G) \leq s_r(G_0)$ and by Proposition 6.3.17,

$$s_r(G_0) \leq s_r^+(G_0) \leq \frac{1}{r^2} + \frac{2\sqrt{3\ln(r|G_0|)}+1}{\sqrt{|G_0|}}.$$

Since

$$\frac{2\sqrt{3\ln(r|n_0|)}+1}{\sqrt{n_0}} < \varepsilon \text{ and } |G_0| \geq n_0$$

then

$$\frac{2\sqrt{3\ln(r|G_0|)}+1}{\sqrt{|G_0|}} < \varepsilon.$$

Now suppose that $|G_0| < n_0$. We already know that $\overline{s}_r(G) \leq s_r(G)$ and by Lemma 6.3.15, $\overline{s}_r(G) = s_r(G_0)$. Now by Proposition 6.3.16

$$s_r(G) \leq \overline{s}_r(G_0) + \frac{|G_0|}{|B_0|}.$$

Since $|G| \geq n_1$

$$|B_0| \geq \frac{n_1}{|G_0|} > \frac{n_1}{n_0}$$

and so

$$\frac{|G_0|}{|B_0|} < \frac{n_0}{\frac{n_1}{n_0}} = \frac{n_0^2}{n_1} \leq \varepsilon.$$

□

Theorem 6.3.13 For every infinite compact Abelian group G,

$$s_r(G) = \begin{cases} \frac{1}{r^2} & \text{if } G/B_0(G) \text{ is infinite} \\ \overline{s}_r(G/B_0(G)) & \text{otherwise.} \end{cases}$$

Proof of Theorem 6.3.13:
This is the proof for the infinite case. Let us denote $B_0 = B_0(G)$ and $G_0 = G/B_0$. Suppose that $|G_0|$ is infinite. Then either G_0 has arbitrarily big finite continuous homomorphic images or $\mathbb{T}$, the circle group, is a continuous homomorphic image of G_0.

If G_0 has arbitrarily big finite continuous homomorphic images then $s_r(G) = \frac{1}{r^2}$ by Lemma 6.3.14 and Proposition 6.3.17. If $\mathbb{T}$ is a continuous homomorphic image of

G_0 then $s_r(G) = \frac{1}{r^2}$ by Lemma 6.3.14 and the fact that $s_r(\mathbb{T}) = \frac{1}{r^2}$.

Now suppose that $|G_0|$ is finite. Again, we know that $\overline{s}_r(G) \leq s_r(G)$. By Lemma 6.3.15, $\overline{s}_r(G) = s_r(G_0)$. Since G_0 is finite, B_0 is infinite. For every finite Boolean group B, $G_0 \times B$ is a continuous homomorphic image of G. Hence, by Lemma 6.3.14 and Proposition 6.3.16, $s_r(G) = \overline{s}_r(G_0)$.

□

Bibliography

[1] T. Banakh and I. Protasov, *Symmetry and colorings: some results and open problems*, Voprosy Algebry - 17, No 3 **6** (2001), 4-15.

[2] T. Banakh, O. Verbitsky and Y. Vorobets, *A Ramsey treatment of symmetry*, Electron. J. Comb. **7** (2000), Research paper R52, 25 p.

[3] T. Banakh, O. Verbitsky and Y. Vorobets, *Ramsey problems for spaces with symmetries*, Izv. Math. **64** (2000), 1091-1127.

[4] T. Bartoszynski and S. Shelah, *Strongly meager sets do not form an ideal*, Journal of Mathematical Logic, **1** (2001), 1-34.

[5] E. Čech, *On bicompact spaces*, Ann. Math. (2), **38** (1937), 823-844.

[6] P. Civin and B. Yood, *The second conjugate space of a Banach algebra as an algebra*, Pacific J. Math., **11** (1961), 847-870.

[7] M. Day, *Amenable semigroups*, Illinois J. Math., **1** (1957), 509-544.

[8] R. Ellis, *Lectures on topological dynamics*, Benjamin, New York, 1969.

[9] L. Fuchs, *Infinite Abelian Groups: Vol I*, Academic Press, New Orleans, 1970.

[10] T. Gowers, *A new proof of Szemerédi's theorem*, Geometric and Functional Analysis, **11** (2001), 465-588.

[11] R. Graham, B. Rothschild and J. Spencer, *Ramsey Theory*, Wiley, New York, 1990.

[12] F. Harary, *A tribute to Frank P Ramsey*, J. Graph Theory, **7** (1983), 1-7.

[13] Y. Haung and J. Yang, *New upper bounds for van der Waerden numbers* $W(r, n)$, Chinese Annals of Math. Series A, **21** (2000), 631-634 (Chinese).

[14] N. Hindman and D. Strauss, *Algebra in the Stone-Čech Compactification*, De Gruyter, Berlin, 1998.

[15] N. Hindman and D. Strauss, *Algebra in the space of ultrafilters and Ramsey Theory*, Contemporary Mathematics, **530** (2010), 121-145.

[16] K. Hofmann and S. Morris, *The Structure of Compact Groups*, De Gruyter, Berlin, 2006.

[17] M. Korostenski and Yu. Zelenyuk, *Ramsey functions for symmetric subsets in compact groups*, Quaestiones Mathematicae, **33** (2010), 161-169.

[18] B. Landman and A. Robertson, *Ramsey Theory on the Integers*, American Mathematical Society, Rhode Island, 2004.

[19] L. Loomis, *An introduction to abstract harmonic analysis*, Van Nostrand, Toronto-New York-London, 1953.

[20] O. Loos, *Symmetric Spaces*, Benjamin, New York, 1969.

[21] B. Mendelson, *Introduction to Topology*, Dover, New York, 1990.

[22] J. Milne, *Group Theory*, Math. Notes, University of Michigan, 2009.

[23] I. Protasov, *Combinatorics of Numbers*, VNTL, Lviv, 1997.

[24] S. Radziszowski, *Small Ramsey Numbers*, Electron. J. Comb., Dynamic Survey 1, 2009.

[25] F. Ramsey, *On a problem of formal logic*, Proc. London Math. Soc., **30** (1930), 264-285.

[26] D. Rees, *On semi-groups*, Math. Proc. Cambridge Philos. Soc., **36** (1940), 387-400.

[27] F. Riesz, *Stetigkeitsbegriff und abstrakte Mengenlehre*, Atti del Congr. Intern. Mat., (1908), 18-24.

[28] J. Rotman, *An Introduction to the Theory of Groups*, Allyn and Bacon, Massachusetts, 1984.

[29] S. Rubinstein-Salzedo, *On the Existence and Uniqueness of Invariant Measures on Locally Compact Groups*, Math. Notes, 2004, 8 p.

[30] I. Schur, *Uber die Kongruenz* $x^m + y^m = z^m$ (mod p), Jber. Deutsch. Math.-Verein. Notes, **25** (1916), 114-116.

[31] M. Stone, *Applications of the theory of Boolean rings to general topology*, Trans. Amer. Math. Soc., **41** (1937), 375-481.

[32] S. Suschkewitsch, *ber die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit*, Math. Ann., **99** (1928), 30-50.

[33] S. Ulam, *Concerning functions of sets*, Fund. Math., **14** (1929), 231-233.

[34] B. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Archief voor Wiskunde, **15** (1927), 212-216.

[35] Ye. Zelenyuk, *General Topology*, Math. Notes, University of the Witwatersrand.

[36] Ye. Zelenyuk, *Ultrafilters and topologies on groups*, De Gruyter, Berlin, 2011.

[37] Ye. Zelenyuk and Yu. Zelenyuk, *Transformations and colourings of groups*, Can. Math. Bull., **50** (2007), 632-636.

[38] Y. Gryshko (Zelenyuk), *Monochrome symmetric subsets in 2-colorings of groups*, Electron. J. Comb., **10** (2003), Research paper R28, 8 p.

[39] Yu. Zelenyuk, *Monochrome symmetric subsets in colorings of finite Abelian groups*, Symmetry, **3** (2011), 126-133.

[40] Yu. Zelenyuk, *Symmetric colorings of finite groups*, Groups St Andrews in Bath, **388** (2011), LMS Lecture Note Series, 580-590.

[41] Y. Gryshko (Zelenyuk), *Symmetric colorings of regular polygons*, Ars Combinatoria, **78** (2006), 277-281.

[42] Y. Gryshko (Zelenyuk), *Symmetric subsets and colourings of finite Abelian groups*, Visnyk Kyiv Univ., Ser. Fiz.-Mat. No. 3 (1999), 200-202 (Ukranian).