Contents

1. Preface

I'll probably add something here later!

This text is mostly written for third year or advanced second year undergraduate students. Many results from undergraduate courses such as complex analysis are taken for granted (although it is clearly mentioned when each result is being invoked, in case the reader would like to refresh their memory). A good background in basic topology is highly beneficial, but I have tried to include most of the important definitions and results in the following two chapters.

2. Background

Definition 2.1 – Topology.
A **topological space** is a nonempty set X endowed with a topology τ, denoted (X, τ). A **topology** is a family τ of subsets of X, such that

(2.1.1). $\varnothing, X \in \tau$ (trivially open sets);
(2.1.2). $\bigcup\limits_{i \in I} V_i \in \tau$, for $\{V_i\}_{i \in I} \subseteq \tau$ (closure under unions);
(2.1.3). $\bigcap\limits_{i=1}^{n} V_i \in \tau$, for $V_1, \ldots, V_n \in \tau$ (closure under finite intersections).

The elements of τ are called **open** (or **$\boldsymbol{\tau}$-open**) sets in X, while a subset $V \subseteq X$ is said to be **closed** if its complement $X \setminus V$ is open. An open set $V \in \tau$ is said to be a **neighbourhood** of a point $x \in X$ if $x \in V$. A point $x \in Y \subseteq X$ is said to be an **interior point** of Y if there exists some $V \in \tau$ such that $x \in V$ and $V \subseteq Y$. A point $x \in X$ is said to be a **boundary point** of $Y \subseteq X$ if every neighbourhood of x intersects both Y and $X \setminus Y$. A point $x \in X$ is said to be a **limit point** of $Y \subseteq X$ if every neighbourhood of x contains an element of Y that is different from x. The **closure** of a set $Y \subseteq X$ is defined to be the set $\mathrm{Cl}(Y) = Y \cup \{\text{limit points of } Y\}$.

Remarks: These definitions should seem familiar; they are actually inherited by vector spaces through metric spaces, which essentially inherit them from topological spaces.

Definition 2.2 – Cover.
Let (X, τ) be a topological space and $Y \subseteq X$. A family of nonempty subsets $\{V_i\}_{i \in I} \subseteq \mathcal{P}(X)$ is said to be a **cover** for Y if $Y \subseteq \bigcup_{i \in I} V_i$. If these sets are open subsets – that is, if $\{V_i\}_{i \in I} \subseteq \tau$ – then it is said to be an **open cover**. A **subcover** of some cover $\{V_i\}_{i \in I}$ is a cover $\{V_i\}_{i \in I'}$ for which $I' \subseteq I$.

Definition 2.3 – Compact Space.
A topological space (X, τ) is said to be **compact** if, for every open cover of X, there exists some finite subcover. That is, given $\{V_i\}_{i \in I} \subseteq \tau$ such that $X \subseteq \bigcup_{i \in I} V_i$, we can find $\{i_1, \ldots, i_n\} \subseteq I$ such that $Y \subseteq \bigcup_{k=1}^{n} V_{i_k}$. A space is said to be **locally compact** if every point has a compact neighbourhood. A subset $Y \subseteq X$ is said to be (locally) compact if it is a (locally) compact space in the **subspace topology**, $\tau|_Y = \{V \cap Y : V \in \tau\}$.

Remarks: Compactness can be thought of as a defining characteristic of the more general idea of finiteness (along with discreteness); for instance, by **Heine-Borel**, a subset of $\mathbb{R}^n$ is closed and bounded if and only if it is compact. This also extends to subsets of $\mathbb{C}^n$, as they are topologically equivalent. For metric spaces in general, compactness is equivalent to complete and totally bounded. There are many quite lovely results following from compactness, especially when complemented with the concept of nets for general topological spaces.

Definition 2.4 – Hausdorff Space.
A topological space (X, τ) is said to be **Hausdorff** if, for any two distinct $x, y \in X$, there exist disjoint, open neighbourhoods of x and y respectively. Hausdorff spaces are sometimes referred to as T_2-spaces, or "topological spaces satisfying the Second Axiom of Separability".

Remarks: One important property of Hausdorff topological spaces is that they *guarantee the uniqueness of limits of convergent sequences*. Note that a Hausdorffness is not strictly necessary for limits of sequences to be unique, and weaker conditions do exist: however, Hausdorffness comes for free when considering the concept of metric spaces, making it remarkably useful.

Definition 2.5 – Metric Space.
A **metric space** is a set X endowed with a **metric** (distance function) $d : X \times X \to \mathbb{F}_{\geq 0}$, where $\mathbb{F}_{\geq 0}$ is a non-negative subset of an **ordered field**, such that

(2.5.1). $d(x, y) = 0$ if and only if $x = y$, for all $x, y \in X$ (identity of indiscernibles);
(2.5.2). $d(x, y) = d(y, x)$, for all $x, y \in X$ (symmetry);
(2.5.3). $d(x, y) + d(y, z) \geq d(x, z)$, for all $x, y, z \in X$ (triangle inequality).

We will denote such a space (X, d). A metric space (X, d) is said to be **complete** if every Cauchy sequence of points in X converges to a limit that also lies within X. A sequence of points $x_1, x_2, \ldots$ in X is a **Cauchy sequence** if, for every real $\varepsilon > 0$, there is some positive integer $K(\varepsilon)$ such that for all integers $m, n > K$, we have

$$d(x_m, x_n) < \varepsilon. \tag{2.5.1}$$

In other words, a complete metric space is just a space where we can *apply the results of calculus*. Note that we require that our field have some kind of **absolute value** function $|\cdot| : \mathbb{F} \to \mathbb{F}_{\geq 0}$. Typically, we will have $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, whence $\mathbb{F}_{\geq 0} = \mathbb{R}_{\geq 0}$.

Remarks: All metric spaces naturally give rise to a corresponding topological space. Indeed, given a metric space (X, d), we may define a **metric topology on *X*** as $\tau = \{V \subseteq X : V \text{ is open under } d\}$. Furthermore, metric topologies are Hausdorff, meaning metric spaces enjoy all of the results that come from Hausdorff spaces.

Definition 2.6 – Normed Space.
A **normed space** is a vector space X over a field $\mathbb{F}$, endowed with a norm $\|\cdot\| : X \to \mathbb{F}_{\geq 0}$. A **norm** is a functional satisfying

(2.6.1). $\|x\| = 0 \implies x = 0$, for all $x \in X$ (positive-definiteness);
(2.6.2). $\|\lambda x\| = |\lambda| \|x\|$, for all $x \in X$, $\lambda \in \mathbb{F}$ (absolute homogeneity);
(2.6.3). $\|x + y\| \leq \|x\| + \|y\|$, for all $x, y \in X$ (triangle inequality).

If we remove the requirement of positive-definiteness, we obtain what is known as a **seminorm**.

Remarks: Suppose we have some normed space X over a field $\mathbb{F}$. It is rather easy to show that we have a **(norm) induced metric**, given by $d(x, y) = \|x - y\|$ for all $x, y \in X$. More precisely put, *all normed spaces induce metrics of this form.*

Definition 2.7 – Uniform Norm.
Let X be a set, and let $\mathcal{B}(X, \mathbb{F})$ denote the set of bounded, $\mathbb{F}$-valued functionals on X. The **uniform norm**, or **Chebyshev norm**, of some $f \in \mathcal{B}(X, \mathbb{F})$ is defined to be

$$\|f\|_\infty \coloneqq \sup\{|f(x)| : x \in X\}. \tag{2.7.1}$$

Remarks: The name of this norm comes from the fact that it characterizes uniform convergence; that is, a sequence of functions $\{f_n\}_{n=1}^{\infty}$ converges to f under the metric induced by this norm if and only if it converges uniformly to f.

Example 2.8 – Examples of Metrics and Norms.
Perhaps the simplest example of a metric space is any non-empty set together with the **discrete metric**

$$d(x, y) \coloneqq \begin{cases} 0, & x \neq y; \\ 1, & x = y. \end{cases}$$

A particularly important set of metric spaces are the **sequence spaces**, ℓ^p. We define ℓ^p to be the set of real sequences $(x_k)_{k\in\mathbb{N}}$ that are "p-summable", in the sense that they have finite norms

$$\left(\sum_{k\in\mathbb{N}} |x_k - y_k|^p \right)^{1/p} < \infty, \quad \text{for } p \in [1, \infty);$$

$$\max_{k\in\mathbb{N}} \{|x_k|\} < \infty, \quad \text{for } p = \infty.$$

These spaces then form complete metric spaces under the ℓ^p metric d_p, defined

$$d_p\left((x_k)_{k\in\mathbb{N}}, (y_k)_{k\in\mathbb{N}}\right) \coloneqq \left(\sum_{k\in\mathbb{N}} |x_k - y_k|^p \right)^{1/p}, \quad \text{for } p \in [1, \infty);$$

$$d_\infty\left((x_k)_{k\in\mathbb{N}}, (y_k)_{k\in\mathbb{N}}\right) \coloneqq \max_{k\in\mathbb{N}} \{|x_k - y_k|\}, \quad \text{for } p = \infty.$$

Note that if we consider sequences of finite length n, we obtain a metric space over $\mathbb{R}^n$. Given the natural bijection between the set of sequences of real numbers and the set of functions mapping from $\mathbb{N}$ to $\mathbb{R}$, one might start to wonder if ℓ^p spaces generalize to metric spaces of functions. Indeed, this is the case: such spaces are known as **Lebesgue spaces**. An example of such a space is, for instance, the set $L^p(\mathbb{R})$ of functions $f : \mathbb{R} \to \mathbb{C}$ that are "p-integrable", in the sense that they have finite norms

$$\left(\int_{\mathbb{R}} |f(x)|^p \, \mathrm{d}x \right)^{1/p} < \infty, \quad \text{for } p \in [1, \infty);$$

$$\sup \{|f(x)| : x \in \mathbb{R}\} < \infty, \quad \text{for } p = \infty.$$

These form a complete metric space under the L^p metric d_p, defined

$$d_p(f, g) \coloneqq \left(\int_{\mathbb{R}} |f(x) - g(x)|^p \, \mathrm{d}x \right)^{1/p}, \quad \text{for } p \in [1, \infty);$$

$$d_p(f, g) \coloneqq \sup \{|f(x) - g(x)| : x \in \mathbb{R}\}, \quad \text{for } p = \infty.$$

Note that the L^∞ norm is actually equivalent to the uniform norm!

Definition 2.9 – Banach Space.
A **Banach space** is a complete normed space, where complete is used in the sense that it induces a complete metric space.

Remarks: The sequence spaces and Lebesgue spaces mentioned above in example 2.8 are both very important examples of Banach spaces. We take the norms to be the canonical norms $\|\cdot\|_p = d_p(\cdot, 0)$.

Definition 2.10 – Inner Product Space.
An **inner product space** is a vector space X endowed with an **inner product** $\langle \cdot, \cdot \rangle : X \times X \to \mathbb{F}$. An **inner product** is a functional satisfying

(2.10.1). $\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle$, for all $x, y, z \in X$ (additivity in the second argument);
(2.10.2). $\langle x, \lambda y \rangle = \lambda \langle x, y \rangle$, for all $x, y \in X$, $\lambda \in \mathbb{F}$ (homogeneity in the second argument);
(2.10.3). $\langle y, x \rangle = \overline{\langle x, y \rangle}$, for all $x, y \in X$ (conjugate symmetry);
(2.10.4). $\langle x, x \rangle \in \mathbb{F}_+$, for all $x \in X$ such that $x \neq 0$ (positive definiteness).

Note that many people use an equally valid pair of linearity conditions, preferring linearity in the first argument and conjugate linearity in the second. However, unless stated otherwise, we will be using the definition provided above, simply because it consistent with vector notation and often prettier.

Remarks: Similarly to how norms induce metrics, inner products induce norms (and hence metrics). In particular, if $\langle \cdot, \cdot \rangle$ is an inner product, then $\|x\|_{\langle \cdot, \cdot \rangle} = \sqrt{\langle x, x \rangle}$ is an induced norm.

Definition 2.11 – Hilbert Space.
A **Hilbert space** is a complete inner product space; that is, it is an inner product space such that the norm $\|x\|_{\langle \cdot, \cdot \rangle} = \sqrt{\langle x, x \rangle}$ induces a complete metric space. Note that all Hilbert spaces are trivially Banach spaces (though the converse is, of course, not necessarily true).

Example 2.12 – Examples of Hilbert Spaces.
On the topic of sequence and Lebesgue spaces, these generate Hilbert spaces *only* for $p = 2$: that is, ℓ^2 and L^2. To see why this is the case, one must look to the parallelogram law, which is not satisfied for $p \neq 2$. The spaces $L^2(\mathbb{R}^n)$ of complex-valued functions are of particular interest in physics.

Theorem 2.13 – Direct Sum Decomposition of Hilbert Spaces.
Let H be a Hilbert space and K a closed vector subspace. Then $H = K \oplus K^\perp$, where we let $K^\perp = \{x \in H : \langle x, k \rangle = 0, \text{ for all } k \in K\}$ denote the **orthogonal complement** of K.

Proof – omitted. This is actually a corollary of the **Hilbert space projection theorem**. While it is not difficult to prove, it is a rabbit hole that is not particularly relevant to us.

Definition 2.14 – Dual Space.
Let X be a vector space over the field $\mathbb{F}$. The **(topological) dual space** of X, denoted X^*, is the set of all bounded (or equivalently, continuous), linear functionals $f : X \to \mathbb{F}$.

Remarks: The topological dual space is a vector subspace of the so-called **algebraic dual space**, the set of all linear functionals on X. We will use dual space to refer to the topological dual space.

3. Introduction to Operators

We will now shift our discussion towards operators, whence we shall conclude the chapter with an important but hopefully somewhat familiar theorem. We will, however, be giving a simplified version that restricts our consideration to Hilbert spaces, as being more general is not particularly relevant to us and would require a treatment of measure theory.

Definition 3.1 – Operator.
Let X, Y be normed spaces over the same field $\mathbb{F}$. An **operator** is a map $T : X \to Y$, where X typically carries with it the implication of being a function space (although this is not always the case). An operator is said to be **(locally) bounded** when there exists some $M \in \mathbb{F}_+$ such that

$$\|T(x)\|_Y \leq M\|x\|_X, \tag{3.1.1}$$

for all $x \in X$.

Definition 3.2 – Operator Norm.
Let X, Y be normed spaces over the same field $\mathbb{F}$, and let $T : X \to Y$ be a bounded, linear operator between them. We define the **operator norm** of T to be

$$\|T\|_{\text{op}} := \begin{cases} 0, & \text{for } T = 0; \\ \inf\{M \in \mathbb{F}_+ : \|T(x)\| \leq M\|x\|, \text{ for all } x \in X\}, & \text{otherwise.} \end{cases} \tag{3.2.1}$$

An alternative, trivially equivalent definition is

$$\|T\|_{\text{op}} := \sup\{\|T(x)\| : x \in X, \|x\| = 1\}. \tag{3.2.2}$$

Remarks: This follows nicely from the definition of boundedness. In fact, suppose we write $x = \lambda\hat{x}$, for some $\hat{x} \in X$, $\lambda \in \mathbb{F}$, where $\|\hat{x}\| = 1$ and $|\lambda| = \|x\|$. Then by linearity, we now see that $\|T(x)\| \leq \|T\||\lambda| = \|T\|\|x\|$! It might be an interesting exercise to compare this to the uniform norm.

Note that if T is a bounded, linear operator with matrix representation A, then $T(x) = Ax$. We actually have that the norm of such a T is the square root of the largest eigenvalue of the symmetric matrix A^*A, where A^* denotes the conjugate transpose of A.

Theorem 3.3 – Bounded and Linear $\iff$ Continuous and Linear.
Let X, Y be normed spaces, and let $T : X \to Y$ be a linear operator between them. Then the following are equivalent:

(3.3.1). T is bounded;
(3.3.2). T is continuous;
(3.3.3). T is continuous at zero.

Proof. It is trivial that (3.3.2) $\implies$ (3.3.3), so we need only show that (3.3.1) $\implies$ (3.3.2) and that (3.3.3) $\implies$ (3.3.1). Furthermore, the result follows immediately for the trivial 0 operator, so we may assume that $T \neq 0$ when proving both directions.

We shall first prove that bounded implies continuous. Suppose $T : X \to Y$ is a bounded, linear operator. Then there exists some $M > 0$ such that for all $x \in X$, $\|T(x)\| \leq M\|x\|$. Now, consider any $x \in X$, $\varepsilon > 0$, and suppose we define $\delta = \varepsilon/M > 0$. It follows that, for all $x' \in X$ satisfying $\|x' - x\| < \delta$, we have

$$\|T(x') - T(x)\| = \|T(x' - x)\| \leq M\|x' - x\| < M\delta = \varepsilon,$$

from the linearity and boundedness of T. Hence T is everywhere continuous by definition.

We shall now prove the converse. Suppose $T : X \to Y$ is a linear operator, continuous at zero. Then there exists some $\delta > 0$ such that, for all $x \in X$, $\|x\| < \delta$ implies $\|T(x)\| < 1$. Well, for all $x \in X$,

$$\left\|\frac{\delta}{2\|x\|}x\right\| = \frac{\delta}{2} < \delta \implies \left\|T\left(\frac{\delta}{2\|x\|}x\right)\right\| = \frac{\delta}{2\|x\|}\|T\,(x)\| < 1 \implies \|T\,(x)\| < \frac{2}{\delta}\|x\|,$$

by the linearity of T. Hence T is bounded by definition. This completes the proof. ■

Remarks: We will henceforth denote by $\mathcal{B}(X, Y)$ the set of bounded, linear operators between the normed spaces X and Y, where $\mathcal{B}(X, X) = \mathcal{B}(X)$. Note that, by theorem 3.3, these are equivalent to the sets of continuous, linear operators between normed spaces.

Theorem 3.4 – Riesz Representation Theorem.
Let H be a Hilbert space and $f \in H^*$ a bounded, linear functional. Then there exists some unique $f \in H$ such that $f(x) = \langle r, x\rangle$, for all $x \in H$. We say that r is the **Riesz representation** of f.

Proof. Let f be a bounded, linear functional on H. We present a general method for constructing an $r \in H$ such that $f(x) = \langle r, x\rangle$, for all $x \in H$. Suppose $f = 0$: then $f(x) = \langle 0, x\rangle = 0$ for all $x \in H$. We shall henceforth assume $f \neq 0$. Well, suppose we let $K = \ker(f) = f^{-1}[\{0\}]$. We know that K will be closed, as f is continuous by theorem 3.3, and continuous preimages of closed sets are closed by definition. Furthermore, K is a subspace of H, as the kernel of a linear map is trivially a subspace. But since K is a closed subspace of a Hilbert space H, we have $H = K \oplus K^\perp$ by theorem 2.13, and since $f \neq 0$, it follows that $K \neq H$, whence $K^\perp$ must contain elements other than the 0 element. Suppose we now let $y \in K^\perp$ such that $\|y\| = 1$ and $f(y) \neq 0$ – which is certainly always possible by linearity – and consider

$$f\left(x - \frac{f(x)}{f(y)}y\right) = f(x) - \frac{f(x)}{f(y)}f(y) = 0,$$

$$\implies x - \frac{f(x)}{f(y)}y \in K.$$

Because this is orthogonal to y by construction, it follows that

$$0 = \left\langle y, x - \frac{f(x)}{f(y)}y\right\rangle = \langle y, x\rangle - \frac{f(x)}{f(y)}\langle y, y\rangle = \langle y, x\rangle - \frac{f(x)}{f(y)},$$

$$\implies f(x) = \langle\overline{f(y)}y, x\rangle.$$

To show that $r = \overline{f(y)}y$ is unique, suppose we let $r_1, r_2 \in H$ such that $f(x) = \langle r_1, x\rangle = \langle r_2, x\rangle$. Then by Cauchy-Schwarz, we have that

$$0 = |f(x) - f(x)| = |\langle r_1, x\rangle - \langle r_2, x\rangle| = |\langle r_1 - r_2, x\rangle| \leq \|r_1 - r_2\|\|x\|$$

for all $x \in H$. If we choose $x \neq 0$ such that it is linearly dependent with respect to $r_1 - r_2$, we in fact have equality, whence $r_1 = r_2$. This completes the proof. ■

Remarks: This is actually a remarkably beautiful theorem: it gives us a simple characterization of bounded, linear functionals on Hilbert spaces – and hence Hilbert dual spaces. Surprisingly, such operators are nothing but inner products! Furthermore, by theorem 3.3, we may happily apply this result to any continuous, linear functional. Note that this result actually does not hold for infinite-dimensional inner product spaces in general; we require the completeness property to ensure that $K^\perp$ is non-trivial. If we were to restrict our attention to finite dimensions, however, we would no longer require completeness, as the Hilbert space decomposition theorem holds for general finite vector spaces.

Another nice thing about the Riesz representation theorem is that it lets us talk about **adjoints of bounded, linear operators between Hilbert spaces**. For instance, suppose we have some such bounded, linear operator $T \in \mathcal{B}(X, Y)$. Suppose we also define some bounded, linear functional $f \in X^*$ by $f(x) = \langle y, T(x)\rangle$, which is a composition of bounded, linear maps and hence is also certainly bounded and linear. By the Riesz representation theorem, there then exists some unique y' such that $f(x) = \langle y', x\rangle$. In order to ensure that $f(x) = \langle T^*(y), x\rangle$, and hence that the adjoint properties are satisfied, it's clear that we only need $T^*(y) = y'$. Hence this is our adjoint map for T. With this in mind, we should find it useful to make one more definition.

Definition 3.5 – Unitary Operator.
A **unitary operator** on a Hilbert space H is a bounded, linear operator $U : H \to H$ such that $U^*U = UU^* = I$, where U^* is the adjoint of U and $I : H \to H$ is the identity operator. Note that the product operation here refers to function composition.

Remarks: Similar to $\mathcal{B}(H)$, we will let $\mathcal{U}(H)$ denote the set of unitary operators on H.

4. Introduction to C^*-Algebras

Definition 4.1 – Algebra Over a Field.
An **algebra** over a field $\mathbb{F}$ is some set A, whose elements satisfy both the vector space axioms (over $\mathbb{F}$) and the ring axioms. More formally, we define over A the following operations:

(4.1.1). λx, for all $\lambda \in \mathbb{F}$, $x \in A$ (scalar multiplication);
(4.1.2). $x + y$, for all $x, y \in A$ (vector addition);
(4.1.3). xy, for all $x, y \in A$ (vector multiplication),

which satisfy the following unifying relations:

(4.1.4). A is a vector space with respect to scalar multiplication and vector addition;
(4.1.5). A is a ring with respect to vector addition and vector multiplication;
(4.1.6). $\lambda(xy) = (\lambda x)y = x(\lambda y)$, for all $\lambda \in \mathbb{F}$, $x, y \in A$.

Note that (4.1.4) unifies (4.1.1) and (4.1.2); (4.1.5) unifies (4.1.2) and (4.1.3); and (4.1.6) unifies (4.1.1) and (4.1.3). An algebra is said to be **Abelian** if $xy = yx$ for all $x, y \in A$. An algebra is said to be **unital** if there exists a necessarily unique element $e \in A$ such that $ex = xe = x$, for all $x \in A$. This element is called the (multiplicative) **unit** or **identity** of A, and is denoted id, I, 1_A or simply 1. An element a is said to be **invertible** if there exists some **inverse** b, such that $ba = ab = 1_A$. This element b is denoted a^{-1}, and is necessarily unique. Sometimes we let $\mathrm{Inv}(A)$ denote the invertible elements in A. We define a **subalgebra** as a subset of A that is itself an algebra.

Definition 4.2 – Banach Algebra.
A **normed algebra** is an algebra equipped with a **submultiplicative** norm $\|\cdot\| : A \to \mathbb{F}_{\geq 0}$, in the sense that

(4.2.1). $\|xy\| \leq \|x\|\|y\|$, for all $x, y \in A$.

A normed algebra is said to be **unital** if the underlying algebra A is unital, and $\|1_A\| = 1_{\mathbb{F}}$. Furthermore, a complete normed algebra – in the sense that the underlying vector space is a Banach space – is said to be **Banach**.

Remarks: Suppose we let $\varepsilon > 0$, and fix some $(x_0, y_0) \in A \oplus A$. Furthermore, let

$$\delta_x = \frac{\min\{1, \varepsilon\}}{\|x_0\| + 1} < 1, \qquad \delta_y = \frac{\min\{1, \varepsilon\}}{\|y_0\| + 1} < 1.$$

Then for all $(x, y) \in A \oplus A$ such that $\|x - x_0\| < \delta_x$ and $\|y - y_0\| < \delta_y$, we have that

$$\|x\| - \|x_0\| \leq \|x - x_0\| < 1 \implies \|x\| < \|x_0\| + 1,$$

$$\|y\| - \|y_0\| \leq \|y - y_0\| < 1 \implies \|y\| < \|y_0\| + 1.$$

Hence by the triangle inequality and condition (4.2.1),

$$\begin{aligned} \|xy - x_0y_0\| = \|x(y - y_0) + (x - x_0)y_0\| &\leq \|x\|\|y - y_0\| + \|x - x_0\|\|y_0\|, \\ &< (\|x_0\| + 1)\delta_y + \delta_x(\|y_0\| + 1), \\ &\leq \varepsilon. \end{aligned}$$

It follows that multiplication on normed algebras is **(jointly) continuous**.

Example 4.3 – Examples of Banach Algebras.
The simplest examples of Banach algebras are the real numbers, $\mathbb{R}$, and the complex numbers, $\mathbb{C}$, under the canonical norms. Actually, both $\mathbb{R}^n$ and $\mathbb{C}^n$ correspond to Banach algebras, with componentwise multiplication and norm given by taking the maximal component. We can generalize this further to the sets of real and complex $n \times n$ matrices, $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$, which admit Banach algebras under the matrix norm (which is essentially the operator norm for matrices). Another rather nice example are the quaternions, denoted $\mathbb{H}$. Their norm is given by the quaternion absolute value.

Definition 4.4 – $*$-Algebra.
A **$*$-algebra** ("star algebra"), denoted $(A, *)$, is an algebra A endowed with a $*$-operation. A **$*$-operation** on an algebra A is a map $x \mapsto x^*$ satisfying

(4.4.1). $(x^*)^* = x$, for all $x \in A$ (involution);
(4.4.2). $(xy)^* = y^* x^*$ (antihomomorphism);
(4.4.3). $(x + y)^* = x^* + y^*$ (additive);
(4.4.4). $(\lambda x)^* = \overline{\lambda} x^*$, for all $\lambda \in \mathbb{F}$, $x \in A$ (conjugate homogeneity).

The $*$-operation of a $*$-algebra is also called the **adjoint operation**, with x^* denoting the **adjoint** of some $x \in (A, *)$. An element $x \in (A, *)$ is said to be **self-adjoint** or **Hermitian** if $x^* = x$. An element $x \in (A, *)$ is said to be **isometric** or an **isometry** if $x^* x = 1_A$ (not to be confused with standard distance-preserving isometries!), and **unitary** if both x and x^* are isometric. Finally, an element is said to be **normal** if $x^* x = x x^*$. We also define a **$*$-subalgebra** in the obvious way.

Remarks: In the usual case where $\mathbb{F} = \mathbb{C}$, we have a unique decomposition for each element x of our $*$-algebra: $x = x_{\mathfrak{R}} + i x_{\mathfrak{I}}$, where $x_{\mathfrak{R}} = (x + x^*)/2$ and $x_{\mathfrak{I}} = (x - x^*)/2i$. In inner product spaces, the $*$-operation may often be taken to be the corresponding adjoint operation of the space.

Example 4.5 – Examples of $*$-Algebras.
Many of the algebras given in example 4.3 admit interesting $*$-algebras. The most obvious of these are the complex numbers, $\mathbb{C}$, which of course have complex conjugation as their $*$-operation. Furthermore, both $M_n(\mathbb{R})$ and $M_n(\mathbb{C})$ admit $*$-algebras under transposition and conjugate transposition, respectively. The quaternions also form a $*$-algebra under their own conjugation operation. Of course, we can technically always create a $*$-algebra from an arbitrary algebra by taking the $*$-operation to be the identity operation, but this is usually not incredibly insightful.

Definition 4.6 – $*$-Homomorphism.
An **algebra homomorphism** is a linear map $\phi : A \to B$ between two algebras A and B over $\mathbb{F}$ that is also a ring homomorphism; that is, an algebra homomorphism is a map satisfying

(4.6.1). $\phi(\lambda x) = \lambda \phi(x)$, for all $\lambda \in \mathbb{F}$, $x \in A$;
(4.6.2). $\phi(x + y) = \phi(x) + \phi(y)$, for all $x, y \in A$;
(4.6.3). $\phi(xy) = \phi(x)\phi(y)$, for all $x, y \in A$.

As expected, we similarly inherit the notions of other kinds of morphisms: endomorphisms ($A = B$), epimorphisms (surjective), monomorphisms (injective), isomorphisms (bijective) and automorphisms (endomorphism and isomorphism). As with rings, an algebra homomorphism ϕ is **unital** if it preserves the unit element; that is, $\phi(1_A) = 1_B$. Finally, a **$*$-homomorphism** ϕ is a homomorphism of $*$-algebras preserving adjoints, such that $\phi(x^*) = \phi(x)^*$ for all $x \in A$.

Definition 4.7 – C^*-Algebra.
A ***C^**-algebra**, or **operator algebra**, is a Banach $*$-algebra A such that

(4.7.1). $\|a^*a\| = \|a\|^2$, for all $a \in A$.

In fact, it actually follows from condition (4.2.1) that adjoint maps on C^*-algebras are isometric:

(4.7.2). $\|a\| = \|a^*\|$, for all $a \in A$.

The set of self-adjoint elements of a C^*-algebra A admit a partial ordering, $(A, \geq)$: that is, an element $a \in A$ is said to be **non-negative** (or **positive**), denoted $a \geq 0$, if there exists some $c \in A$ such that $a = c^*c$. Two self-adjoint elements $a, b \in A$ are said to satisfy $a \geq b$ when $a - b \geq 0$. We will see later on that this definition of positivity is equivalent to requiring that $a^* = a$ and that the **spectrum** of a lie in $\mathbb{F}_{\geq 0}$.

Remarks: If a $*$-algebra admits a norm that turns it into a C^*-algebra, this norm is unique.

The roots of C^*-algebras actually lie in **von Neumann algebras**, an older subset of C^*-algebras that were designed to model rings of bounded, linear operators (representing observables) on Hilbert spaces of wavefunctions in early algebraic formulations of quantum mechanics.

Example 4.8 – $\mathcal{B}(H)$ is a C^*-Algebra.
Consider $\mathcal{B}(H)$, the set of bounded, linear operators on a complex Hilbert space H. Checking axioms, we can easily verify that this is a unital algebra, with function composition being our vector multiplication. This is certainly sensible, as elements of $\mathcal{B}(H)$ map from H to itself. This becomes a unital $*$-algebra under the canonical adjoint operation satisfying $\langle T^*(y), x\rangle = \langle y, T(x)\rangle$, with respect to the inner product of H. This adjoint exists due to theorem 3.4, the Riesz representation theorem. Suppose we now take two operators $T_1, T_2 \in \mathcal{B}(H)$. From boundedness, there exist $M_1, M_2 \in \mathbb{R}_{\geq 0}$ such that we can write $\|T_1(v)\| \leq M_1\|v\|$ and $\|T_2(v)\| \leq M_2\|v\|$, for all $v \in H$. Thus

$$\|T_1T_2\| = \sup_{\|v\|=1} \|T_1(T_2(v))\| \leq M_1 \sup_{\|v\|=1} \|T_2(v)\| = M_1M_2 = \|T_1\|\|T_2\|,$$

whence it follows that $\mathcal{B}(H)$ is a unital Banach $*$-algebra. Finally, note that we also satisfy the additional, rather strong condition $\|T^*T\| = \|T\|^2$, for all $T \in \mathcal{B}(H)$. Thus $\mathcal{B}(H)$ is a C^*-algebra.

Example 4.9 – Continuous Functionals on Compact Spaces.
Let X be a compact space, with $\mathcal{C}(X)$ denoting the space of all continuous, complex-valued functionals on X. Well, $\mathcal{C}(X)$ is certainly an Abelian $*$-algebra under the pointwise operations

scalar multiplication:	$[\lambda f](x) \coloneqq \lambda f(x)$, for all $\lambda \in \mathbb{C}$, $f \in \mathcal{C}(X)$, $x \in X$;
vector addition:	$[f + g](x) \coloneqq f(x) + g(x)$, for all $f, g \in \mathcal{C}(X)$, $x \in X$;
vector multiplication:	$[fg](x) \coloneqq f(x)g(x)$, for all $f, g \in \mathcal{C}(X)$, $x \in X$;
$*$-operation:	$[f^*](x) \coloneqq \overline{f(x)}$, for all $f \in \mathcal{C}(X)$, $x \in X$.

Furthermore, this space is trivially unital, and it is also a Banach $*$-algebra under the uniform norm (which is well-defined, as $f[X]$ is a compact subset of $\mathbb{C}$ and hence bounded by Heine-Borel, so f is itself bounded). Finally, we once again have that $\|f^*f\| = \|f\|^2$ for all $f \in \mathcal{C}(X)$, as $(f^*f)(x) = |f(x)|^2$ for all $x \in X$. Hence $\mathcal{C}(X)$ induces a C^*-algebra. However, $\mathcal{C}(X)$ is not necessarily a Hilbert C^*-algebra.

We will henceforth be assuming that all of our C^*-algebras are over the field $\mathbb{C}$, unless otherwise stated. This is simply the most natural field to us, and will find itself the most relevant in consideration of the coming chapters.

Theorem 4.10 – Unitizing C^*-Algebras.
Let A be a C^*-algebra that is not necessarily unital. Then it admits an embedding into a unital C^*-algebra $\widetilde{A}$, known as the **unitization** of A, such that it is a **maximal ideal** of codimension one.

Proof. Let $\widetilde{A} \coloneqq A \oplus \mathbb{C}$, where we define scalar multiplication and vector multiplication in the obvious ways, with vector multiplication, adjoints and norms as follows:

vector multiplication:	$(a,\lambda)(b,\lambda) \coloneqq (ab + \lambda b + \mu a, \lambda\mu)$, for all $(a,\lambda),(b,\mu) \in \widetilde{A}$;
$*$-operation:	$(a,\lambda)^* \coloneqq (a^*, \overline{\lambda})$, for all $(a,\lambda) \in \widetilde{A}$.
norm:	$\|(a,\lambda)\| \coloneqq \sup\{\|ab + \lambda b\| : b \in A, \|b\| = 1\}$, for all $(a,\lambda) \in \widetilde{A}$.

This is certainly a $*$-algebra; in fact, it is actually a unital Banach $*$-algebra with unit $(0,1)$. This is because the norm is inherited from the space $\mathcal{B}(A)$ of bounded, linear operators on A, given by the $*$-algebra of operators $\{\Lambda_{a,\lambda} : a \in A, \lambda \in \mathbb{C}\}$, where $\Lambda_{a,\lambda}(b) = ab + \lambda b$. We see also that A is a maximal ideal of $\widetilde{A}$ by construction (with codimension $\dim(\widetilde{A}) - \dim(A) = 1$), and that the canonical embedding $a \mapsto (a,0)$ of A into $\widetilde{A}$ is isometric, as

$$\|a\| = \left\| \frac{aa^*}{\|a\|} \right\| \le \|(a,0)\| = \sup_{\|b\|=1} \{\|ab\|\} \le \|a\|,$$

by (4.2.1), (4.7.1) and (4.7.2). We shall thus use this to show that $\widetilde{A}$ also satisfies the C^* condition, (4.7.1). Well, by once again applying (4.2.1) and (4.7.1) on A,

$$\begin{aligned}
\|(a,\lambda)\|^2 &= \sup_{\|b\|=1} \|ab + \lambda b\|^2, \\
&= \sup_{\|b\|=1} \|(ab + \lambda b)^*(ab + \lambda b)\|, \\
&= \sup_{\|b\|=1} \left\|b^*a^*ab + \lambda b^*a^*b + \overline{\lambda} b^*ab + |\lambda|^2 b^*b\right\|, \\
&\le \sup_{\|b\|=1} \left\|a^*ab + \lambda a^*b + \overline{\lambda} ab + |\lambda|^2 b\right\|, \\
&= \left\|(a^*a + \lambda a^* + \overline{\lambda} a, |\lambda|^2)\right\|, \\
&= \|(a,\lambda)^*(a,\lambda)\|, \\
&\le \|(a,\lambda)^*\| \|(a,\lambda)\|.
\end{aligned}$$

Thus $\|(a,\lambda)\| \le \|(a,\lambda)^*\|$. But by starting with $\|(a,\lambda)^*\|^2$, we can obtain the converse. So in fact, $\|(a,\lambda)^*(a,\lambda)\| = \|(a,\lambda)\|^2$ as desired. This completes the proof. ■

5. Elementary Spectral Theory

Definition 5.1 – Spectrum.
Let A be a unital Banach algebra, and let $\mathrm{Inv}(A)$ denote the group of invertible elements in A. The **spectrum** of an element $a \in A$ is then the set

$$\sigma(a) \coloneqq \{\lambda \in \mathbb{C} : \lambda 1_A - a \notin \mathrm{Inv}(A)\}. \tag{5.1.1}$$

The complement of the spectrum, $\rho(a) = \mathbb{C} \backslash \sigma(a)$, is known as the **resolvent set** of a. The function $R_a : \rho(a) \to \mathrm{Inv}(A)$, defined by $\lambda \mapsto (\lambda 1_A - a)^{-1}$, is then the **resolvent function** of a.

Remarks: Compare this to the matrix definition of the spectrum, the set of all eigenvalues of a matrix: the spectrum of an operator is actually nothing but a generalization of this concept, and we see that both definitions are equivalent on matrix spaces. As an additional note, many authors will write simply λ rather than $\lambda 1_A$. This makes sense under the consideration of operators, as $\lambda 1_A$ can be thought of as the scalar operator generated by λ.

Theorem 5.2 – Neumann Series.
Let A be a unital Banach algebra, and suppose a is an element of A with $\|a\| < 1$. Then we have $1_A - a \in \mathrm{Inv}(A)$, and furthermore,

$$(1_A - a)^{-1} = \sum_{k=0}^{\infty} a^k. \tag{5.2.1}$$

This series is known as the **Neumann series** for $(1_A - a)^{-1}$.

Proof. By hypothesis, $\|a\| < 1$, whence it follows by the norm property (4.2.1) that

$$\sum_{k=0}^{\infty} \left\|a^k\right\| \leq \sum_{k=0}^{\infty} \|a\|^k = (1_A - \|a\|)^{-1} < \infty.$$

So the Neumann series is certainly norm convergent for $\|a\| < 1$. Furthermore, by once again appealing to our hypothesis and condition (4.2.1), we know that

$$0 \leq \lim_{n\to\infty} \|a^n\| \leq \lim_{n\to\infty} \|a\|^n = 0,$$

$$\implies \lim_{n\to\infty} a^n = 0_A.$$

So it follows that

$$\begin{aligned}
(1_A - a) \sum_{k=0}^{\infty} a^k &= (1_A - a) \lim_{n\to\infty} \sum_{k=0}^{n} a^k, \\
&= \lim_{n\to\infty} (1_A - a)(1_A + \cdots + a^n), \\
&= \lim_{n\to\infty} 1_A - a^{n+1}, \\
&= 1_A.
\end{aligned}$$

The result follows. This completes the proof. ■

Theorem 5.3 – Invertible Elements Form an Open Subset.
Let A be a unital Banach algebra. Then $\text{Inv}(A)$ is open in A, and the canonical inverse map, given by $\text{inv} : \text{Inv}(A) \to A : a \mapsto a^{-1}$, is differentiable.

Proof. We shall first prove that $\text{Inv}(A)$ is open in A by showing that $B(a, \|a^{-1}\|^{-1})$, the open ball centered at a with radius $\|a^{-1}\|^{-1}$, lies within $\text{Inv}(A)$, for all $a \in \text{Inv}(A)$. Well, let $a \in \text{Inv}(A)$, and suppose that $b \in B(a, \|a^{-1}\|^{-1})$; that is, $\|b - a\| < \|a^{-1}\|^{-1}$. Then by condition (4.2.1), we have that $\|ba^{-1} - 1_A\| \leq \|b - a\|\|a^{-1}\| < 1$. But it then follows by theorem 5.2 that ba^{-1} is invertible, and hence $b \in \text{Inv}(A)$. Because this holds for all $b \in B(a, \|a^{-1}\|^{-1})$, we must in fact have that $B(a, \|a^{-1}\|^{-1}) \subseteq \text{Inv}(A)$ as desired, so $\text{Inv}(A)$ is open in A.

We will now show that the inverse map is differentiable. Well, let $a, b \in \text{Inv}(A)$, with $\|b\| < \frac{1}{2}\|a^{-1}\|^{-1}$. Then $\|a^{-1}b\| < 1/2 < 1$. Suppose we now let $c = a^{-1}b$. Then $1_A + c \in \text{Inv}(A)$ by theorem 5.2, and

$$\left\|(1_A + c)^{-1} - 1_A + c\right\| = \left\|\sum_{n=0}^{\infty} (-1)^n c^n - 1_A + c\right\| = \left\|\sum_{n=2}^{\infty} (-1)^n c^n\right\| \leq \sum_{n=2}^{\infty} \|c\|^n = \frac{\|c\|^2}{1 - \|c\|},$$

by the triangle inequality and condition (4.2.1). Hence, in terms of a and b, we have

$$\left\|\left(1_A + a^{-1}b\right)^{-1} - 1_A + a^{-1}b\right\| \leq \frac{\|a^{-1}b\|^2}{1 - \|a^{-1}b\|} \leq 2\left\|a^{-1}b\right\|^2,$$

as $1 - \|a^{-1}b\| > 1/2$. Suppose we now define a linear operator u on A by $u(z) = a^{-1}za^{-1}$. Then

$$\begin{aligned} \left\|(a+b)^{-1} - a^{-1} - u(b)\right\| &= \left\|\left(1_A + a^{-1}b\right)^{-1} a^{-1} - a^{-1} + a^{-1}ba^{-1}\right\|, \\ &\leq \left\|\left(1_A + a^{-1}b\right)^{-1} - 1_A + a^{-1}b\right\|\left\|a^{-1}\right\| \leq 2\left(\left\|a^{-1}\right\|^3\|b\|^2\right). \end{aligned}$$

Because this naturally continues to be satisfied as $\|b\|$ tends to 0, it follows that

$$\lim_{\|b\| \to 0} \frac{\left\|(a+b)^{-1} - a^{-1} - u(b)\right\|}{\|b\|} = 0$$

Thus we find that the map $\text{inv} : z \mapsto z^{-1}$ is differentiable at $z = a$, with derivative $\text{inv}'(a) = u$. This completes the proof. ■

Lemma 5.4 – Spectrums are Compact.
Let A be a unital Banach algebra. Then for each $a \in A$, the corresponding spectrum $\sigma(a)$ is a compact subset of $\mathbb{C}$, with $\sigma(a) \subseteq \{\lambda \in \mathbb{C} : |\lambda| \leq \|a\|\}$.

Proof. Let $\lambda \in \mathbb{C}$ such that $|\lambda| > \|a\|$. Then $\|\lambda^{-1}a\| < 1$, so $1_A - \lambda^{-1}a$ is invertible by theorem 5.2. This means that $\lambda 1_A - a$ is invertible, as it only involves non-zero scalar multiplication. We therefore have $\lambda \notin \sigma(a)$, whence it follows that $\sigma(a) \subseteq \{\lambda \in \mathbb{C} : |\lambda| \leq \|a\|\}$. Thus $\sigma(a)$ is bounded. Suppose we now define the continuous function $\phi : \mathbb{C} \to A : \lambda \mapsto \lambda 1_A - a$. Then by the definition of the spectrum, it follows that $\phi^{-1}[\text{Inv}(A)] = \mathbb{C} \backslash \sigma(a)$. But by theorem 5.3, we know that $\text{Inv}(A)$ is an open subset of A; hence by the definition of continuity, $\mathbb{C} \backslash \sigma(a)$ must be open, whence we realize that $\sigma(a)$ – the complement with respect to $\mathbb{C}$ – must be closed. So $\sigma(a)$ is a closed and bounded subset of $\mathbb{C}$, and must therefore be compact by Heine-Borel. This completes the proof. ■

Lemma 5.5 – Resolvent Functions are Analytic.
Let A be a unital Banach algebra. Then the resolvent function R_a of each $a \in A$ is analytic. A function $f : X \to Y$ is said to be **analytic** over an open set X if, for every $x_0 \in X$, there exists some neighbourhood of x_0 such that $f(x)$ is the pointwise limit of the Taylor series centered at x_0, for all x in the neighbourhood.

Proof. We have shown in lemma 5.4 that $\mathbb{C}\backslash\sigma(a)$ is open, so it is sensible to think about whether the resolvent function is analytic. Let $\lambda_0 \in \mathbb{C}\backslash\sigma(a)$, and consider the neighbourhood $B(\lambda_0, R)$, where we take $R = \|R_a(\lambda_0)\|^{-1}$ if $\|R_a(\lambda_0)\| \neq 0$ and $R = \infty$ otherwise. We see that, for all $\lambda \in B(\lambda_0, R)$ – that is, λ such that $|\lambda_0 - \lambda| < R$ – we have

$$\lambda 1_A - a = \lambda_0 1_A - a - (\lambda_0 - \lambda)1_A = (\lambda_0 1_A - a)(1_A - R_a(\lambda_0)(\lambda_0 - \lambda)).$$

Thus $\lambda 1_A - a$ is invertible for $\lambda \in B(\lambda_0, R)$ by theorem 5.2, as λ lying in this open ball implies that $\|R_a(\lambda_0)(\lambda_0 - \lambda)\| < 1$ by construction. Taking inverses of both sides, we obtain

$$R_a(\lambda) = R_a(\lambda_0)(1_A - R_a(\lambda_0)(\lambda_0 - \lambda))^{-1}.$$

But this means that, once again by theorem 5.2,

$$R_a(\lambda) = R_a(\lambda_0)\left(\sum_{k=0}^{\infty} (R_a(\lambda_0)(\lambda_0 - \lambda))^k\right) = \sum_{k=0}^{\infty} [R_a(\lambda_0)]^{k+1}(\lambda_0 - \lambda)^k.$$

The result follows, as this is our Taylor series for $R_a(\lambda)$. This completes the proof. ■

Theorem 5.6 – Gelfand's Theorem.
Let A be a unital Banach algebra. Then the spectrum $\sigma(a)$ of each $a \in A$ is non-empty.

Proof. Suppose that $\sigma(a) = \varnothing$. We shall proceed by contradiction. Well, let $\lambda \in \mathbb{C}$ such that $|\lambda| > 2\|a\|$. Then we know that $\|\lambda^{-1}a\| < 1/2$, and hence $1 - \|\lambda^{-1}a\| > 1/2$. So by theorem 5.2 and the triangle inequality,

$$\left\|\left(1_A - \lambda^{-1}a\right)^{-1} - 1_A\right\| = \left\|\sum_{k=1}^{\infty} \left(\lambda^{-1}a\right)^k\right\| \leq \frac{\|\lambda^{-1}a\|}{1 - \|\lambda^{-1}a\|} \leq 2\left\|\lambda^{-1}a\right\| < 1.$$

Therefore, again by the triangle inequality, $\left\|(1_A - \lambda^{-1}a)^{-1}\right\| < 2$. Hence

$$\|R_a(\lambda)\| = \left\|(\lambda 1_A - a)^{-1}\right\| = \left\|\lambda^{-1}\left(1_A - \lambda^{-1}a\right)^{-1}\right\| < 2|\lambda|^{-1} < \|a\|^{-1}.$$

Note that $\|a\|^{-1}$ is well-defined, since $a = 0_A$ would of course imply that $\sigma(a) \neq \varnothing$. We have thus shown that $R_a(\lambda)$ is bounded for $|\lambda| > 2\|a\|$. But because it is obviously continuous on the closed (compact) ball $\overline{B}(0, 2\|a\|)$, it is also bounded for $|\lambda| \leq 2\|a\|$, and is hence bounded on all of $\mathbb{C}$. So there exists some $M \in \mathbb{R}_+$ such that $\|R_a(\lambda)\| \leq M$, for all $\lambda \in \mathbb{C}$. Now, by lemma 5.5, we know that R_a is analytic, and hence **holomorphic**, over $\mathbb{C}\backslash\sigma(a)$. Furthermore, because $\sigma(a) = \varnothing$, we in fact have that R_a is **entire**, as it is holomorphic over the whole complex plane. But **Liouville's theorem** from complex analysis states that bounded, entire functions are constant! This means that $R_a(0) = -a^{-1} = (1_A - a)^{-1} = R_a(1)$, so $a = a - 1_A$: a contradiction. This completes the proof. ■

Remarks: Together with lemma 5.4, we learn that $\sigma(a)$ is a non-empty, compact subset of $\mathbb{C}$!

Theorem 5.7 – Spectral Mapping Theorem.
Let A be a unital Banach algebra and p a polynomial with complex coefficients. Then for each $a \in A$, we have that $\sigma(p_A(a)) = p_{\mathbb{C}}[\sigma(a)]$, where $p_X : X \to X$ denotes the polynomial p implemented over X.

Proof. Suppose first that p is constant; that is, $p_{\mathbb{C}}(z) = C$, for some $C \in \mathbb{C}$. Then $\sigma(a) = \{C\}$, whence the result follows trivially. We may henceforth assume that p is not constant. If we choose such a p and let $\mu \in \mathbb{C}$, then there exist constants $\eta_0, \dots, \eta_n \in \mathbb{C}$, with $\eta_0 \neq 0$, for which

$$p_{\mathbb{C}}(z) - \mu = \eta_0 \prod_{i=1}^{n} (z - \eta_i).$$

In particular, it follows that

$$p_A(a) - \mu 1_A = \eta_0 \prod_{i=1}^{n} (a - \eta_i 1_A).$$

Because each term in this product certainly commutes, we learn that $p_A(a) - \mu 1_A$ will be invertible if and only if each $a - \eta_i 1_A$ is invertible. So it follows from the definition of the spectrum that $\mu \in \sigma(p_A(a))$ if and only if $\mu = p_{\mathbb{C}}(\lambda)$, for some $\lambda \in \sigma(a)$. Therefore, $\sigma(p_A(a)) = p_{\mathbb{C}}[\sigma(a)]$ as desired. This completes the proof. ■

Definition 5.8 – Spectral Radius.
Let A be a unital Banach algebra. From theorem 5.6, the spectrum of any $a \in A$ is always a non-empty, compact subset of $\mathbb{C}$: hence it contains both its infimum and supremum by Heine-Borel. We therefore define the **spectral radius** of $a \in A$ to be

$$r(a) := \sup\{|\lambda| : \lambda \in \sigma(a)\}. \tag{5.8.1}$$

Theorem 5.9 – Beurling-Gelfand Theorem.
Let A be a unital Banach algebra. Then for all $a \in A$, the spectral radius is given by

$$r(a) = \inf_{n \geq 1} \|a^n\|^{1/n} = \lim_{n \to \infty} \|a^n\|^{1/n}. \tag{5.9.1}$$

Proof. One direction is relatively simple. Suppose $\lambda \in \sigma(a)$; then we know that $\lambda^n \in \sigma(a^n)$, for $n \geq 1$. This is because $\lambda 1_A - a$ is a factor of $\lambda^n 1_A - a^n$, as we can always write

$$\lambda^n 1_A - a^n = (\lambda 1_A - a)(\lambda^{n-1} 1_A + \lambda^{n-2} a + \cdots + a^{n-1}).$$

Thus $|\lambda^n| \leq \|a^n\|$ for all $\lambda \in \sigma(a)$ by lemma 5.4, and so

$$r(a) = \sup_{\lambda \in \sigma(a)} |\lambda| = \sup_{\lambda \in \sigma(a)} |\lambda^n|^{1/n} \leq \|a^n\|^{1/n},$$

for all $n \geq 1$. Since $r(a)$ is independent of n, it therefore follows that

$$r(a) \leq \inf_{n \geq 1} \|a^n\|^{1/n} \leq \liminf_{n \to \infty} \|a^n\|^{1/n}.$$

We shall now show the remaining direction. We have shown in lemma 5.5 that the resolvent function R_a is analytic on the resolvent set. In particular, by theorem 5.2, we see that the Laurent series for R_a at infinity is given by

$$R_a(\lambda) = (\lambda 1_A - a)^{-1} = \lambda^{-1}(1_A - a\lambda^{-1})^{-1} = \frac{1}{\lambda}\sum_{k=0}^{\infty}\frac{a^k}{\lambda^k}.$$

Suppose we let $\varphi \in A^*$ be a bounded, linear functional, and $\Lambda = \{\lambda \in \mathbb{C} : |\lambda| > r(a)\} \subseteq \mathbb{C}\backslash\sigma(a)$. It follows that $\varphi(R_a(\lambda)) : \Lambda \to \mathbb{C}$ is also analytic, and furthermore that the Laurent series at infinity for this function is nothing but

$$\varphi(R_a(\lambda)) = \frac{1}{\lambda}\sum_{k=0}^{\infty}\frac{\varphi\left(a^k\right)}{\lambda^k},$$

by linearity. From complex analysis, we also know that this series is uniformly absolutely convergent on the open annulus $|\lambda| > r(a)$. The sequence $(\varphi\left(a^n\right)\lambda^{-n})_{n\geq 1}$ therefore converges to zero, and so is bounded. Because this holds for all $\varphi \in A^*$, the **Banach–Steinhaus theorem** tells us that there is some positive $M(\lambda)$ such that $\|a^n\lambda^{-n}\| \leq M$ for all $n \geq 1$. In other words, $\|a^n\|^{1/n} \leq M^{1/n}|\lambda|$ for all $n \geq 1$, and consequently

$$\limsup_{n\to\infty}\|a^n\|^{1/n} \leq \lim_{n\to\infty} M^{1/n}|\lambda| = |\lambda|.$$

Finally, because this holds for all $r(a) < |\lambda|$, it can be shown by contradiction that we must have

$$\limsup_{n\to\infty}\|a^n\|^{1/n} \leq r(a).$$

Combining this with our previous work, the result follows. This completes the proof. ■

Remarks: This theorem tells us that the spectral radius is actually identical to the so-called **Hadamard radius** of the resolvent function – the radius of convergence of the corresponding Laurent series.

Example 5.10 – Matrix Spectrum.
Suppose A is the algebra of upper-triangular, $n \times n$-matrices, and consider some $a \in A$ with

$$a = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{pmatrix}.$$

From linear algebra, we know that $(\lambda I - a)$ will not be invertible for $\lambda \in \{a_{11}, \ldots, a_{nn}\}$. This is therefore the spectrum of a, which agrees with the typical spectrum observed in linear algebra.

Example 5.11 – Continuous Spectrum.
Let X be a compact Hausdorff space, and $\mathcal{C}(X)$ the C^*-algebra of all continuous, complex-valued functionals on X. Then for all $f \in A$, the spectrum of f is actually nothing but $\sigma(f) = f[X]$; this is rather easy to see by considering which values of λ result in the map $x \mapsto 1/(\lambda - f(x))$ having a singularity. Interestingly, the spectrum is deeply related to the idea of the range of a function.

6. Abelian C^*-Algebras

Definition 6.1 – Non-Zero Homomorphisms.
We denote by $\mathcal{M}(A) \subset A^*$ the set of non-zero, homomorphic functionals on A.

Remarks: This notation is due to the fact that a homomorphism is a multiplicative linear map.

Lemma 6.2 – Properties of Non-Zero Homomorphisms.
Let $\phi \in \mathcal{M}(A)$, for some Abelian, unital C^*-algebra A. Then

(6.2.1). $\phi(a) \in \sigma(a)$, for all $a \in A$;
(6.2.2). ϕ is bounded with $\|\phi\| = 1$;
(6.2.3). $\phi(a^*) = \overline{\phi(a)}$, for all $a \in A$.

Proof. Note that the kernel of ϕ is an ideal in A; this follows rather nicely from the properties of algebra homomorphisms. Furthermore, since ϕ is non-zero, it is actually a proper ideal, and hence can contain no invertible elements (as otherwise it will of course contain the identity, and hence all of A). As a result, for any $a \in A$, we see that $\phi(a)1_A - a$ is clearly in the kernal of ϕ, and so cannot be invertible. Thus $\phi(a)$ lies in the spectrum $\sigma(a)$ by definition.

Because $\phi(a) \in \sigma(a)$, it also follows that $|\phi(a)| \leq r(a) \leq \|a\|$ by definition 5.8 and theorem 5.9, whence ϕ is bounded with $\|\phi\| \leq 1$. To show the other direction, we observe that $\phi(1_A) = 1$. Furthermore, $\|1_A\|^2 = \|1_A^* 1_A\| = \|1_A\|$, implying $\|1_A\| = 1$ and hence that $\|\phi\| \geq |\phi(1_A)| = 1$.

Finally, for (6.2.3), we begin by noting that any $a \in A$ may be decomposed into $a = a_{\mathfrak{R}} + i a_{\mathfrak{I}}$, as in the remark to definition 4.4, where $a_{\mathfrak{R}}$ and $a_{\mathfrak{I}}$ are both self-adjoint. Hence $\phi(a^*) = \phi(a_{\mathfrak{R}}) - i\phi(a_{\mathfrak{I}})$. We need only show that $b^* = b$ implies $\phi(b) \in \mathbb{R}$. Using a power series for the exponential function, we see that $u(t) = e^{itb}$ is a well-defined element of A, for any $t \in \mathbb{R}$. Moreover, by continuity $u(-t) = [u(t)]^*$ and $u(t)u(-t) = 1$. Thus $\|u(t)\| = \sqrt{\|[u(t)]^* u(t)\|} = 1$. Finally, because ϕ is continuous,

$$1 \geq |\phi(u(t))| = \left|e^{it\phi(b)}\right|,$$

for all $t \in \mathbb{R}$. Hence $\phi(b)$ is real, and so

$$\phi(a^*) = \phi(a_{\mathfrak{R}}) - i\phi(a_{\mathfrak{I}}) = \overline{\phi(a_{\mathfrak{R}}) + i\phi(a_{\mathfrak{I}})} = \overline{\phi(a)}.$$

This completes the proof. ■

Lemma 6.3 – Non-Zero Homomorphisms Form a Weak-∗-Compact Subset.
Let A be an Abelian, unital C^*-algebra A. The set $\mathcal{M}(A)$ is a **weak-∗-compact** subset of the unit ball in the dual space A^*. In other words, it is a compact subset with respect to the **weak-∗ topology** on A^*.

Remarks: The weak-∗ topology is essentially a generalization of the usual Hilbert weak topology to duals of arbitrary topological vector spaces. We henceforth endow $\mathcal{M}(A)$ with the weak-∗ topology.

Proof. We know that the unit ball in A^* is weak-$*$ compact by the **Banach-Alaoglu theorem**; hence we need only show that $\mathcal{M}(A)$ is closed. Well, the weak-$*$ topology on A^* is characterized by a more general kind of weak convergence; that is, the net ϕ_λ will converge to ϕ if and only if the net $\phi_\lambda(a)$ converges to $\phi(a)$, for all $a \in A$. But given this, if each net ϕ_λ is multiplicative, so too must ϕ be. Hence the set is closed. This completes the proof. ■

Lemma 6.4 – Continuous Evaluation Map.
Let A be an Abelian, unital C^*-algebra, with $a \in A$. The evaluation map on $\mathcal{M}(A)$ with respect to a, defined by $\phi \mapsto \phi(a)$ for $\phi \in \mathcal{M}(A)$, is a continuous surjection from $\mathcal{M}(A)$ to $\sigma(a)$.

Proof. First, we know that the codomain is correct, as property (6.2.1) ensures that $\phi(a) \in \sigma(a)$, for all $\phi \in \mathcal{M}(A)$. Furthermore, continuity follows directly from the definition of the weak-$*$ topology. We shall now show that the map is surjective.

Let $\lambda \in \sigma(a)$. It can be argued by means of **Zorn's lemma** that $\lambda 1_A - a$ must be contained within some maximal proper ideal $I \subset A$. We claim that this I is closed. Well, its closure is certainly an ideal. Furthermore, $\mathrm{Inv}(A)$ is open by theorem 5.3, and hence the closure of I can contain no invertible elements, as taking the closure of an open set preserves disjointness. But this means that I is itself proper, as it cannot contain 1_A, whence maximality ensures that it must be equal to I. Suppose we now consider the quotient space $B := A/I$. This is actually both a field and a Banach algebra under the quotient norm. For any $b \in A/I$, we know that there is some λ for which $\lambda 1_B - b$ is not invertible, as $\sigma(b) \neq \varnothing$ by Gelfand's theorem. Because A/I is a field, this means $\lambda 1_B - b = 0_B$. Thus every element of A/I is nothing but a scalar multiple of 1_B. In other words, we can identify $A/I \cong \mathbb{C}$! The quotient map from A to $\mathbb{C}$ is then a non-zero homomorphism sending a to λ, as $\lambda 1_A - a$ is in I. Hence the evaluation map must be surjective, as this is possible for any $\lambda \in \sigma(a)$. This completes the proof. ■

Lemma 6.5 – Homeomorphic Evaluation Map.
Let A be an Abelian, unital C^*-algebra generated by the elements a, a^* and 1_A. The evaluation map on $\mathcal{M}(A)$ with respect to a is a homeomorphism from $\mathcal{M}(A)$ to $\sigma(a)$.

Proof. Lemma 6.4 clearly still applies, hence we need only show that the map is injective with a continuous inverse. Well, suppose $\phi, \psi \in \mathcal{M}(A)$, with $\phi(a) = \psi(a)$. Then it follows from property (6.2.3) that $\phi(a^*) = \psi(a^*)$, and also that $\phi(1) = 1 = \psi(1)$. But this means that $\phi = \psi$, as a, a^* and 1_A generate A as a Banach algebra. Hence the evaluation map is injective. Finally, because the evaluation map takes closed subsets to closed subsets, its inverse is naturally continuous by definition. This completes the proof. ■

Theorem 6.6 – Self-Adjoint Spectral Radius.
Let a be a self-adjoint element of a unital C^*-algebra. Then $\|a\| = r(a)$.

Proof. By the C^* condition, (4.7.1), we know that $\|a^2\| = \|a\|^2$. Then by induction, it follows that $\|a^{2^k}\| = \|a\|^{2^k}$, for any $k \in \mathbb{Z}_+$. Thus $r(a) = \lim_{n\geq 1} \|a^n\|^{1/n} = \lim_{k \geq 1} \|a^{2^k}\|^{2^{-k}} = \|a\|$, as desired. This completes the proof. ■

Theorem 6.7 – Structure of Abelian, Unital C^*-Algebras.
Let A be an Abelian, unital C^*-algebra. The map $\hat{}: A \to \mathcal{C}(\mathcal{M}(A)) : a \mapsto \hat{a}$, where $\hat{a}$ is the evaluation map $\hat{a}(\phi) = \phi(a)$, is an isometric $*$-isomorphism from A to $\mathcal{C}(\mathcal{M}(A))$.

Proof. Once again, we know that $\hat{a}$ is a continuous function (that is, it lies in $\mathcal{C}(\mathcal{M}(A))$) due to the definition of the weak-$*$ topology. We also see that $\hat{}$ is not only a homomorphism, but due to property (6.2.3), a $*$-homomorphism. We shall now show that $\hat{}$ is an isometry (and hence also injective). Suppose that a is self-adjoint. From theorem 6.6, definition 5.8 and definition 3.2, it follows that

$$\|a\| = r(a) = \sup_{\phi \in \mathcal{M}(A)} |\phi(a)| = \sup_{\phi \in \mathcal{M}(A)} |\hat{a}(\phi)| = \|\hat{a}\|.$$

Thus, for an arbitrary element,

$$\|a\| = \|a^*a\|^{1/2} = \|\widehat{a^*a}\|^{1/2} = \|\hat{a}^*\hat{a}\|^{1/2} = \|\hat{a}\|.$$

Thus $\hat{}$ is isometric (and injective). All that remains is to show that $\hat{}$ is surjective onto $\mathcal{C}(\mathcal{M}(A))$. First, we see that the range is a unital $*$-algebra of $\mathcal{C}(\mathcal{M}(A))$. Furthermore, for any two distinct $\phi, \psi \in \mathcal{M}(A)$, there must exist some $a \in A$ such that $\phi(a) \neq \psi(a)$. But this means $\hat{a}(\phi) \neq \hat{a}(\psi)$, whence $\hat{a}$ separates ϕ and ψ. Because the range separates points, it must therefore be dense by the **Stone-Weierstrass theorem**. Finally, because $\hat{}$ is isometric and A is complete, the range must also be closed. This gives us surjectivity, whence the result follows. This completes the proof. ■

Proposition 6.8 – Spectrums in Abelian Subalgebras.
Let B be a unital C^*-algebra and A an Abelian C^*-subalgebra of B containing 1_B. An element $a \in A$ has an inverse in A if and only if it has an inverse in B. In particular, $\sigma_A(a) = \sigma_B(a)$.

Proof. The first direction is clear: if a has an inverse in A, then it must also have one in B, and hence $\sigma_B(a) \subseteq \sigma_A(a)$. Assume now that a has an inverse in B. Because $(a^*)^{-1} = (a^{-1})^*$, its adjoint must also have an inverse in B, and so too must a^*a. From lemma 6.4, we then have that $\sigma_A(a^*a) = \{\phi(a^*a) : \phi \in \mathcal{M}(A)\}$. Property (6.2.3) tells us that $\phi(a^*a) = \phi(a^*)\phi(a) = \overline{\phi(a)}\phi(a)$ – a non-negative real number – and property (6.2.2) gives us that $\phi(a^*a) \leq \|a^*a\|$. Thus

$$\sigma_B(a^*a) \subseteq \sigma_A(a^*a) \subseteq [0, \|a^*a\|].$$

But we have assumed that a^*a is invertible, so 0 is not in the spectrum, giving us instead

$$\sigma_B(a^*a) \subseteq [\varepsilon, \|a^*a\|],$$

for some $\varepsilon > 0$. Now, because $\lambda 1_B - (\|a^*a\|1_B - a^*a) = -((\|a^*a\| - \lambda)1_B - a^*a)$, we have that

$$\sigma_B(\|a^*a\|1_B - a^*a) = \|a * a\| - \sigma_B(a^*a) \subseteq [0, \|a^*a\| - \varepsilon].$$

However, $\|a^*a\|1_B - a^*a$ is self-adjoint, so

$$\|(\|a^*a\|1_B - a^*a)\| \leq \|a^*a\| - \varepsilon < \|a^*a\|.$$

It follows from property (6.2.2) that

$$|\phi(\|a^*a\|1_B - a^*a)| = \|a^*a\| - |\phi(a)|^2 < \|a^*a\|,$$

for all $\phi \in \mathcal{M}(A)$. Thus we conclude that $\phi(a) \neq 0$. Lemma 6.4 then implies that $0 \notin \sigma_A(a)$, hence a is invertible in A as desired. This completes the proof. ■

Proposition-Definition 6.9 – Identification of Normal Elements 1.
Let B be a unital C^*-algebra, and a a normal element of B. Let A be the C^*-subalgebra generated by a and 1_B. For each $f \in \mathcal{C}(\sigma(a))$, we let $f(a)$ be the unique element of A such that

$$\phi(f(a)) = f(\phi(a)), \tag{6.9.1}$$

for all $\phi \in \mathcal{M}(A)$.

Proof. Recall that we may use the evaluation map to identify $\mathcal{M}(A)$ with $\sigma(a)$, by lemma 6.5. Thus there is a unique element $f(a) \in A$ whose image under the map $\hat{}$ from theorem 6.7 is precisely f, where we have identified ϕ with $\phi(a)$ for property (6.9.1). This completes the proof. ■

Corollary 6.10 – Identification of Normal Elements 2.
Let B be a unital C^*-algebra, and a a normal element of B. Let A be the C^*-subalgebra generated by a and 1_B. The map $f \mapsto f(a)$ is an isometric $*$-isomorphism from $\mathcal{C}(\sigma(a))$ to A. Furthermore, if

$$f(z) = \sum_{i,j} c_{i,j} z^i \overline{z}^j \tag{6.10.1}$$

is any polynomial in z and $\overline{z}$, then the unique identification from definition 6.9 is characterized by

$$f(a) = \sum_{i,j} c_{i,j} a^i (a^*)^j. \tag{6.10.2}$$

Proof. This is essentially a restatement of theorem 6.7 under the consideration of definition 6.9. ■

Corollary 6.11 – Classification of Normal Elements.
Let B be a unital C^*-algebra, and a a normal element of B. Then a is self-adjoint if and only if $\sigma(a) \subseteq \mathbb{R}$.

Proof. The restriction of the function $f(z) = z$ to the spectrum of a is mapped to a under the isometric $*$-isomorphism from corollary 6.10. Thus a is self-adjoint if and only if $f|_{\sigma(a)} = \overline{f}|_{\sigma(a)}$, which holds if and only if $\sigma(a) \subseteq \mathbb{R}$. This completes the proof. ■

Corollary 6.12 – Homomorphisms on Normal Elements.
Let A and B be unital C^*-algebras, and $\rho : A \to B$ a unital C^*-homomorphism between them. For any normal element $a \in A$, we have $\sigma(\rho(a)) \supseteq \sigma(a)$, and $f(\rho(a)) = \rho(f(a))$, for any $f \in \mathcal{C}(\sigma(a))$.

Proof. Note that unital C^*-homomorphisms must preserve invertability; hence $\sigma(\rho(a)) \supseteq \sigma(a)$ follows immediately. Suppose we now let C be a C^*-subalgebra of A, generated by a and 1_A. Similarly, let D be a C^*-subalgebra of B, generated by $\rho(a)$ and 1_B. Then $\rho|_C : C \to D$ is a unital $*$-homomorphism. Furthermore, for $\psi \in \mathcal{M}(D)$, we have $\psi \circ \rho \in \mathcal{M}(C)$, and hence

$$\psi(\rho(f(a))) = \psi \circ \rho(f(a)) = f(\psi \circ \rho(a)) = f(\psi(\rho(a))).$$

Thus $f(\rho(a)) = \rho(f(a))$ as desired. This completes the proof. ■

7. Finite-Dimensional C^*-Algebras

Definition 7.1 – Projection.
Let A be a C^*-algebra. An element $p \in A$ is a **projection** if $p^2 = p = p^*$; that is, p is a self-adjoint idempotent. An element $u \in A$ is a **partial isometry** if u^*u is a projection.

Lemma 7.2 – Normal Elements in Unital, Finite-Dimensional C^*-Algebras.
Let A be a finite-dimensional, unital C^*-algebra. Then the following properties hold:

(7.2.1). every normal element of A has a finite spectrum;
(7.2.2). every normal element of A is a linear combination of projections.

Proof. Let $a \in A$ be normal. By corollary 6.10, we can say that $\mathcal{C}(\sigma(a))$ is isomorphic to a C^*-subalgebra of A, which of course must also be finite-dimensional. Hence $\sigma(a)$ must be finite.

Suppose we now denote by $p_\lambda : \sigma(a) \to \{0, 1\}$ the function taking $\lambda \in \sigma(a)$ to 1 and everything else to 0. This function is a self-adjoint idempotent, so $p_\lambda(a)$ must be as well, meaning $p_\lambda(a)$ is a projection. Furthermore, because $\sigma(a)$ is finite, it is discrete, so the preimage of any closed subset of $\{0, 1\}$ under p_λ is closed. Thus $p_\lambda \in \mathcal{C}(\sigma(a))$. It is easy to see that, for any $z \in \sigma(a)$,

$$\sum_{\lambda \in \sigma(a)} \lambda p_\lambda(z) = z.$$

Thus by corollary 6.10, we have that

$$\sum_{\lambda \in \sigma(a)} \lambda p_\lambda(a) = a,$$

for any $a \in A$ normal. This completes the proof. ■

Theorem 7.3 – Structure of Finite-Dimensional C^*-Algebras.
Let A be a finite-dimensional, unital C^*-algebra. Then there exist positive integers K and $N_1, \ldots, N_K$ such that

$$A \cong \bigoplus_{k=1}^{K} M_{N_k}(\mathbb{C}). \tag{7.3.1}$$

Furthermore, K is unique, and the $N_1, \ldots, N_K$ are unique up to permutation.

Remarks: Note that the hypothesis that A is unital is not actually necessary here; actually, as it happens, *every* finite-dimensional C^*-algebra is unital. However, we will unfortunately not be proving either of these statements, as the proofs are rather involved (albeit still manageable).

Proof – omitted.

8. Gelfand-Naimark-Segal Construction

Definition 8.1 – Positive, Linear Functional.
Suppose we have some partially ordered vector space $(X, \geq)$ over a field $\mathbb{F}$. A linear functional $\varphi : X \to \mathbb{F}$ is said to be **positive** when $\varphi(x) > 0$ for all $x \in X_+$. Actually, from linearity, we can rewrite this requirement as $\varphi(x) \geq 0$, for all $x \in X_{\geq 0}$, which is more compatible with our characterization of positivity within C^*-algebras.

Remarks: If X is a complex vector space, it is assumed that $\varphi(x)$ is real, for all $x \geq 0$.

Theorem 8.2 – Cauchy-Schwarz Inequality for Positive, Linear Functionals.
Let φ be a positive, linear functional on a unital C^*-algebra A. Then for $a, b \in A$,

$$|\varphi(b^*a)|^2 \leq \varphi(a^*a)\varphi(b^*b). \tag{8.2.1}$$

Proof. Let $a, b \in A$. We begin by showing that $\varphi(a^*) = \overline{\varphi(a)}$. For any $\lambda \in \mathbb{C}$, we have that

$$0 \leq \varphi((\lambda a + b)^*(\lambda a + b)) = |\lambda|^2\varphi(a^*a) + \overline{\lambda}\varphi(a^*b) + \lambda\varphi(b^*a) + \varphi(b^*b),$$

from the positivity and linearity of φ. From positivity, the first and last terms are positive and real, so the sum of the second and third terms must be real. Setting $b = 1_A$ and $\lambda = i$, we see that $\mathfrak{R}(a^*) = \mathfrak{R}(a)$, as $i\varphi(a) - i\varphi(a^*)$ must be real. Setting $b = 1_A$ and $\lambda = 1$, we see that $\mathfrak{I}(a^*) = \overline{\mathfrak{I}(a)}$, as $\varphi(a^*) + \varphi(a)$ must be real. Thus $\varphi(a^*) = \overline{\varphi(a)}$.

We will now use this fact to prove the Cauchy-Schwarz inequality. Because 1_A is positive (since we know $1_A = 1_A^* 1_A$), it follows that $\varphi(1_A)$ must be positive. We also know that $\|1_A\| = 1$; thus $0 \leq |\varphi(1_A)| \leq \|\varphi\|$ from the definition of the operator norm. Well,

$$\begin{aligned} 0 &\leq |\lambda|^2\varphi(a^*a) + \overline{\lambda}\varphi(a^*b) + \lambda\varphi(b^*a) + \varphi(b^*b), \\ &= |\lambda|^2\varphi(a^*a) + \overline{\lambda\varphi(b^*a)} + \lambda\varphi(b^*a) + \varphi(b^*b), \\ &= |\lambda|^2\varphi(a^*a) + 2\mathfrak{R}(\lambda\varphi(b^*a)) + \varphi(b^*b), \\ &\implies -2\mathfrak{R}(\lambda\varphi(b^*a)) \leq |\lambda|^2\varphi(a^*a) + \varphi(b^*b). \end{aligned}$$

If $\varphi(a^*a) = 0$, then it follows that $\varphi(b^*a) = 0$, as we are free to choose any λ we wish. For $\varphi(a^*a) \neq 0$, suppose we choose some $z \in \mathbb{C}$ on the unit circle such that $|z| = 1$ and $z\varphi(b^*a) = |\varphi(b^*a)|$ (which we know must certainly exist!). Finally, we may exercise our freedom in λ to let $\lambda = -z\sqrt{\varphi(a^*a)^{-1}\varphi(b^*b)}$, whence the two sides of the previous inequality become

$$-2\mathfrak{R}(\lambda\varphi(b^*a)) = 2|\varphi(b^*a)|\sqrt{\varphi(a^*a)^{-1}\varphi(b^*b)},$$

$$|\lambda|^2\varphi(a^*a) + \varphi(b^*b) = 2\varphi(b^*b),$$

$$\implies |\varphi(b^*a)| \leq \sqrt{\varphi(a^*a)\varphi(b^*b)}.$$

Note that we have used the fact that $|\varphi(a^*a)| = \varphi(a^*a)$, as both a^*a and φ are respectively positive. The result follows by squaring both sides. This completes the proof. ■

Theorem 8.3 – Norms of Positive, Linear Functionals.
If φ is a positive, linear functional on a unital C^*-algebra A, then $\|\varphi\| = \varphi(1_A)$.

Proof. The first half of this proof is simple: from the definition of the operator norm and the positivity of $\varphi(1_A)$, it follows that $\varphi(1_A) = |\varphi(1_A)| \leq \|\varphi\|$. We would like to now show that $\|\varphi\| \leq \varphi(1_A)$. Consider the Cauchy-Schwarz inequality for positive, linear functionals, with $b = 1_A$:

$$|\varphi(a)| \leq \sqrt{\varphi(a^*a)\varphi(1_A)}.$$

But we know from the definition of the operator norm and boundedness that $\varphi(a^*a) \leq \|\varphi\|\|a^*a\|$; so in fact,

$$|\varphi(a)| \leq \sqrt{\varphi(a^*a)\varphi(1_A)} \leq \sqrt{\|\varphi\|\|a^*a\|\varphi(1_A)} = \sqrt{\|\varphi\|\|a\|^2\varphi(1_A)},$$

where the final equality comes from the C^*-condition. If we now finally take the supremum of both sides with respect to all a of unit norm, we see that $\|\varphi\| \leq \sqrt{\|\varphi\|\varphi(1_A)} \implies \|\varphi\| \leq \varphi(1_A)$, whence the result follows. This completes the proof. ■

Theorem-Definition 8.4 – State.
Suppose that A is a C^*-algebra, and let ϕ be a positive, linear functional with $\|\phi\| = 1$. Then we say that ϕ is a **state**. The set of all states on A is typically denoted $\mathcal{S}(A)$. A state is said to be **faithful** if $\phi(a^*a) = 0$ implies $a = 0_A$. If A is unital, then we necessarily have $\|\phi\| = \phi(1_A) = 1$ by theorem 8.3.

Proof. One direction here is simple: if ϕ is a positive, linear functional with $\phi(1_A) = 1$, then $\|\phi\| = \phi(1_A) = 1$ by theorem 8.3. We shall now prove the converse: that $\|\phi\| = \phi(1_A) = 1$ implies that a linear functional ϕ is positive. We must first show that if a is self-adjoint, then $\phi(a)$ must be real. Well, suppose that $\mathfrak{I}(\phi(a)) \neq 0$, and without loss of generality assume that it is positive. Furthermore, suppose we define the function

$$f(x) \coloneqq \sqrt{\|a\|^2 + x^2} - x.$$

Choosing $0 < r < \mathfrak{I}(\phi(a)) \leq \|a\|$, we see that $f(0) = \|a\| > r$. Multiplying and dividing by factors of $\sqrt{\|a\|^2 + x^2} + x$, we obtain

$$f(x) = \frac{\|a\|^2}{\sqrt{\|a\|^2 + x^2} + x},$$

which clearly tends to 0 as x tends to infinity. Thus we can of course find a positive s such that $f(s) = r$, by the intermediate value theorem. Consider now the complex ball centered at $-is$, with radius $s + r$. We see, by rearranging $f(s) = r$ for the boundary of the ball and using the bound on the spectrum from lemma 5.4, that this ball contains the spectrum of a, but it does not contain $\phi(a)$; that is, $\|a - is1_A\| \leq r + s$, while $|\phi(a) - is| > r + s$. But we now see that

$$|\phi(a - is1_A)| = |\phi(a) - is\phi(1_A)| > r + s,$$

since $\phi(1_A) = 1$, which contradicts $\|\phi\| = 1$! Hence $\phi(a)$ must be strictly real.

We will finally show that $\phi(a) \geq 0$ for positive a. First, note that $\| \|a\| - a\| \leq \|a\|$. Applying ϕ to $\|a\| - a$, and using the fact that $\phi(1_A) = 1 = \|\phi\|$, we obtain

$$|\|a\| - \phi(a)| \leq \|a\|,$$

which implies that $\phi(a) \geq 0$. Thus ϕ is positive. This completes the proof. ■

Remarks: Note that, because $a^*a \geq 0$ for all $a \in A$ by definition, we can just say that a state is a linear functional such that $\phi(a^*a) \geq 0$, for all $a \in A$.

Definition 8.5 – Trace.
A **trace** on a unital $*$-algebra A is a positive, linear functional $\tau : A \to \mathbb{C}$ with $\tau(1_A) = 1$, satisfying the **trace property**: that is, $\tau(ab) = \tau(ba)$, for all $a, b \in A$. A trace is said to be **faithful** if $\tau(a^*a) = 0$ implies $a = 0_A$.

Definition 8.6 – Representation.
Let A be an algebra, and suppose there exists a pair (π, H), where H is a Hilbert space and $\pi : A \to \mathcal{B}(H)$ a homomorphism. We say that π is a **representation** of A on H. Two representations (π_1, H_1), (π_2, H_2) are said to be **unitarily equivalent** if there exists a unitary operator $u : H_1 \to H_2$ such that $u \circ \pi_1(a) = \pi_2(a) \circ u$ for all $a \in A$, whence we write $\pi_1 \sim_u \pi_2$. A representation is said to be **faithful** if it is injective, and **unital** if the underlying homomorphism is unital (such that $[\pi(1_A)](\xi) = \xi$). Finally, if A is a $*$-algebra, we generally require that π be a $*$-homomorphism, and refer to it as a **$*$-representation**.

Definition 8.7 – Non-Degenerate Representation.
A representation (π, H) of an algebra A is said to be **proper** or **non-degenerate** if the only vector $\xi \in H$ such that $[\pi(a)](\xi) = 0_H$, for all $a \in A$, is $\xi = 0_H$. Otherwise, we say that it is **degenerate**.

Proposition 8.8 – Non-Degenerate $\iff$ Unital.
A representation (π, H) of a unital algebra A is non-degenerate if and only if it is unital.

Proof. Let (π, H) be a unital representation on A. This is clearly non-degenerate, as for any non-zero $\xi \in H$, we know that $[\pi(1_A)](\xi) = \xi \neq 0_H$. Conversely, suppose that (π, H) is a non-degenerate representation. Well, denote $[\pi(a)]\xi = \xi_a$, for all $a \in A$ and $\xi \in H$, with $[\pi(1_A)]\xi = \xi_1$. Then from the properties of group homomorphisms, $\xi_a = [\pi(a)](\xi) = [\pi(a) \circ \pi(1_A)](\xi) = [\pi(a)](\xi_1)$. So $[\pi(a)](\xi) = [\pi(a)](\xi_1)$, for all $a \in A$ and $\xi \in H$, whence we obtain $[\pi(a)](\xi - \xi_1) = 0_H$, for all $a \in A$ and $\xi \in H$, by linearity. Because π is non-degenerate, this cannot hold for all $a \in A$ unless $\xi - \xi_1 = 0_H$. Thus $[\pi(1_A)]\xi = \xi_1 = \xi$, whence $\pi(1_A)$ must be the identity. This completes the proof. ■

Definition 8.9 – Cyclic Vector.
Let A be an algebra and (π, H) a representation of A. A vector $\xi \in H$ is said to be **cyclic** if the space $[\pi(A)](\xi)$ is dense in H. A representation is said to be cyclic if it admits a cyclic vector.

Remarks: Note that every cyclic representation is actually non-degenerate. If ξ is a cyclic vector and $[\pi(a)](\eta) = 0_H$ for all a in the $*$-algebra A, then we have $\langle [\pi(a)](\xi), \eta \rangle = \langle \xi, [\pi(a^*)](\eta) \rangle = \langle \xi, 0_H \rangle = 0$. But $[\pi(a)](\xi)$ is dense in H; hence $\eta = 0_H$ as desired.

Theorem 8.10 – Gelfand-Naimark-Segal Construction.
Let A be a C^*-algebra and $\phi : A \to \mathbb{C}$ a state.

(8.10.1). The set $N_\phi := \{a \in A : \phi(a^*a) = 0\}$ is a closed left ideal in A.

(8.10.2). The bilinear form $\langle a + N_\phi, b + N_\phi \rangle = \phi(b^*a)$ is well-defined and non-degenerate on A/N_ϕ. Furthermore, it turns the completion of the quotient space $A/N_\phi := \{a + N_\phi : a \in A\}$ into a Hilbert space, denoted $H_\phi := \overline{A/N_\phi}$.

(8.10.3). The map $[\pi_\phi(a)](b + N_\phi) := ab + N_\phi$, for $a, b \in A$, defines an operator $\pi_\phi(a) \in \mathcal{B}(H_\phi)$.

(8.10.4). The function $\pi_\phi : A \to \mathcal{B}(H_\phi)$ is a $*$-representation of A on H_ϕ.

(8.10.5). The vector $\xi_\phi := 1_A + N_\phi \in A/N_\phi \subset H_\phi$ is a cyclic vector for π_ϕ, with $\|\xi_\phi\| = 1$.

In other words, given a state ϕ, we can generate from it a $*$-representation π_ϕ and a cyclic vector ξ_ϕ. We shall denote such a construction the **GNS representation**.

Proof – omitted.

Definition 8.11 – Gelfand-Naimark-Segal Representation.
Let A be a C^*-algebra and $\phi : A \to \mathbb{C}$ a state. The **GNS representation** of ϕ refers to the triple $(H_\phi, \pi_\phi, \xi_\phi)$, with H_ϕ, π_ϕ and ξ_ϕ as they are defined in theorem 8.10.

Theorem 8.12 – Converse Gelfand-Naimark-Segal Construction.
Let A be a C^*-algebra and $\pi : A \to \mathcal{B}(H_\phi)$ a $*$-representation of A on the Hilbert space H, with cyclic generator $\xi \in H$ of unit norm. Then the map $\phi : A \to \mathbb{C}$, defined by

$$\phi(a) := \langle [\pi_\phi(a)](\xi), \xi \rangle \tag{8.12.1}$$

for all $a \in A$, defines a state on A. Furthermore, all such cyclic GNS representations ϕ are unitarily equivalent to π, in the sense that there is a unitary operator $u : H \to H_\phi$ such that $u(\xi) = \xi_\phi$ and $u \circ \pi(a) \circ u^* = \pi_\phi(a)$, for all $a \in A$.

Proof – omitted.

Theorem 8.13 – Gelfand-Naimark Representation Theorem.
For every C^*-algebra A, there exists a Hilbert space H and a norm-closed $*$-subalgebra $B \subseteq \mathcal{B}(H)$ such that A is isometrically $*$-isomorphic to B.

Proof – omitted. This, along with the Gelfand-Naimark-Segal Construction, is an extremely important result, and historically the definition of a C^*-algebra. What's quite remarkable, however, is that this characterization is equivalent to our abstract definition given in definition 4.7!

Proposition-Definition 8.14 – Hilbert Space Direct Sum.
Let $(H_\lambda)_{\lambda\in\Lambda}$ be a sequence of Hilbert spaces. Then

$$H \coloneqq \left\{ (\xi_\lambda)_{\lambda\in\Lambda} \;:\; \xi_\lambda \in H_\lambda,\ \sum_{\lambda\in\Lambda} \langle \xi_\lambda, \xi_\lambda \rangle < \infty \right\} \tag{8.14.1}$$

is itself a Hilbert space under pointwise operations, with inner product

$$\langle \xi, \eta \rangle \coloneqq \sum_{\lambda\in\Lambda} \langle \xi_\lambda, \eta_i \rangle. \tag{8.14.2}$$

It is known as a **Hilbert space direct sum**, and denoted $H \coloneqq \bigoplus_{\lambda\in\Lambda} H_\lambda$.

Remarks: More generally, the direct sum of Banach spaces is a Banach space.

Proof – omitted.

Definition 8.15 – Universal Representation.
The representation $\pi_U : A \to \mathcal{B}(H_U)$, where

$$H_U \coloneqq \bigoplus_{\phi\in\mathcal{S}(A)} H_\phi, \quad \pi_U \coloneqq \bigoplus_{\phi\in\mathcal{S}(A)} \pi_\phi, \tag{8.15.1}$$

is known as the **universal representation**. That is, it is the direct sum of all GNS representations.

9. Group Representations

Definition 9.1 – Topological Group.
A **topological group** $(G, \cdot, \tau)$ is a group $(G, \cdot)$ endowed with some topology τ, under which the group operation $\cdot : G \times G : (g, h) \mapsto gh$ and inversion map $g \mapsto g^{-1}$ are both continuous.

Definition 9.2 – Locally Compact Group.
A **locally compact space** is a topological space such that that every element belongs to a compact neighbourhood. A **locally compact group** is a topological group for which the underlying topological space is locally compact.

Definition 9.3 – Discrete Group.
A **discrete group** is any group G endowed with the **discrete topology**, $\tau = \mathcal{P}(G)$.

Remarks: Discrete groups have many interesting and useful properties that follow from the discrete topology. In particular, every discrete group is trivially a locally compact Hausdorff space. Most of our discussion will focus on the treatment of these groups.

Definition 9.4 – Unitary Representation.
A **unitary representation** of a discrete group G on a Hilbert space H, sometimes written (u, H), is a group homomorphism of the form $u : G \to \mathcal{U}(H)$. We often let u_g denote the map $u(g)$, the image of g under u. Two unitary representations (u, H_u) and (v, H_v) are said to be **unitarily equivalent** if there exists another unitary operator $w : H_u \to H_v$ such that $w \circ u_g \circ w^{-1} = v_g$, for all $g \in G$. We denote this by $u \sim_w v$. As usual, a representation is said to be **faithful** if it is injective.

Remarks: In the more general locally compact case, we tend to require that our representation be strongly continuous; however, this is automatically satisfied if G is discrete, as every function on a discrete space is trivially continuous. Moreover, if u is a unitary representation, then it follows from the properties of group homomorphisms that $u_{g^{-1}} = u_g^{-1} = u_g^*$, for all $g \in G$.

Definition 9.5 – ℓ^p-Bounded Functionals.
We define the **space of ℓ^p-bounded (complex-valued) functionals** on a set X by

$$\ell^p(X) := \begin{cases} \left\{ \xi : X \to \mathbb{C} : \sum_{x \in X} |\xi(x)|^p < \infty \right\}, & \text{for } 1 \leq p < \infty; \\ \{\xi : X \to \mathbb{C} : \sup\{|\xi(x)| : x \in X\} < \infty\}, & \text{for } p = \infty. \end{cases} \tag{9.5.1}$$

These spaces are also groups under function composition and become Banach spaces (under pointwise operations) when endowed with their respective **ℓ^p-norm**, defined to be

$$\|\xi\|_p := \begin{cases} \left(\sum_{x \in X} |\xi(x)|^p \right)^{1/p}, & \text{for } 1 \leq p < \infty; \\ \sup\{|\xi(x)| : x \in X\}, & \text{for } p = \infty, \end{cases} \tag{9.5.2}$$

for $\xi \in \ell^p(X)$. In the case where $p = 2$, the space can made into a Hilbert space by endowing it with the inner product $\langle \xi_1, \xi_2 \rangle := \sum_{x \in X} \overline{\xi_1(x)} \xi_2(x)$.

Remarks: If A is a subset of X, we let $\chi_A \in \ell^p(X)$ be the indicator function of the form

$$\chi_A(x) := \begin{cases} 1, & \text{if } x \in A; \\ 0, & \text{if } x \notin A. \end{cases}$$

We also generally let $\delta_a \in \ell^p(X)$, for $a \in X$, be the Kronecker delta function of the form

$$\delta_a(x) := \begin{cases} 1, & \text{if } x = a; \\ 0, & \text{if } x \neq a. \end{cases}$$

Note that $\{\delta_x\}_{x\in X}$ is rather trivially an orthonormal linear basis for $\ell^p(X)$.

Proposition-Definition 9.6 – Left Regular Representation.
Suppose we define a group action of a discrete group G on $\ell^2(G)$ by $(g \cdot \xi)(x) := \xi(g^{-1}x)$, for all $\xi \in \ell^2(G)$ and all $g, x \in G$. Then the **left regular representation** of G is the unitary representation

$$\lambda : G \to \mathcal{U}(\ell^2(G)) : g \mapsto \lambda_g,$$

where $\lambda_g : \ell^2(G) \to \ell^2(G)$ is the the unitary convolution map on $\ell^2(G)$, defined by $\lambda_g : \xi \mapsto g \cdot \xi$.

Remarks: We have the following interaction between λ and the delta map: $\lambda_g \circ \delta_h = \delta_{gh}$. Although we are currently treating λ as a unitary representation on $\ell^2(G)$, we will often find it useful later on to relax this definition to arbitrary function spaces, such as $\ell^\infty(G)$.

Proof. We would like to show that the left regular representation is a unitary representation. We shall first show that λ_g is a unitary operator, by showing that it is an invertible isometry. Well, it is immediately clear that λ_g is linear, as $(\mu_1\xi_1+\mu_2\xi_2)(x) = \mu_1\xi_1(g^{-1}x)+\mu_2\xi_2(g^{-1}x)$ for all $\xi_1, \xi_2 \in \ell^2(G)$ and $\mu_1, \mu_2 \in \mathbb{C}$. Consider now the orthonormal basis $\{\delta_a\}_{a\in G}$ for $\ell^2(G)$. We see that

$$\begin{aligned} \langle \lambda_g(\delta_a), \lambda_g(\delta_b)\rangle &= \begin{cases} 0, & a \neq b; \\ 1, & a = b; \end{cases} \\ &= \langle \delta_a, \delta_b\rangle. \end{aligned}$$

This holds for all δ_a, δ_b in our basis; hence by linearity it must hold for all elements of $\ell^2(G)$, so λ_g is an isometry. Furthermore, it is also clearly invertible; in particular, we see that $\lambda_g^{-1} : \xi(g^{-1}x) \mapsto \xi(x)$, whence it follows that $\lambda_g^{-1} = \lambda_{g^{-1}}$. Thus $\lambda_g \in \mathcal{U}(\ell^2(G))$. The only remaining step is to show that λ is a group homomorphism. To see this, we simply observe that

$$(\lambda_g \circ \lambda_h)(\xi(x)) = \lambda_h(\xi(g^{-1}x)) = \xi(h^{-1}g^{-1}x) = \xi((gh)^{-1}x) = \lambda_{gh}.$$

Hence the left regular representation is a unitary representation. This completes the proof. ■

Example 9.7 – Left Regular Representations on Cyclic Groups.
Consider the discrete cyclic group given by endowing some $G = \mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ with the discrete topology, where we denote $\mathbb{Z}_n = \mathbb{Z}$ when $n = 0$. We would like to find the left regular representation on G. We see that this maps the integer $p \in \mathbb{Z}_n$ to the unitary function $\lambda_p : \xi(q+n\mathbb{Z}) \mapsto \xi(q-p+n\mathbb{Z})$. In other words, it behaves as a translation map!

Definition 9.8 – Topologically Irreducible Representation.
Let (u, H) be a unitary representation of a discrete group G. A closed subspace $N \subseteq H$ is said to be an **invariant subspace** of u if $u_g(N) \subseteq N$, for all $g \in G$. We say that the representation is **(topologically) irreducible** if its only invariant subspaces are the trivially invariant subspaces $\{0_H\}$ and H; otherwise, it is said to be **(topologically) reducible**. We generally let $\widehat{G}$ denote the set of unitary equivalence classes of irreducible representations.

Remarks: Note that the requirement that invariant subspaces must be closed ensures that they are Hilbert subspaces. This allows us to decompose arbitrary unitary representations of a discrete group into direct sums of irreducible representations, as we will detail shortly.

Definition 9.9 – Direct Sum of Unitary Representations.
Let $\{(u_i, H_i)\}_{i\in I}$ be a collection of unitary representations of a discrete group G. Their **direct sum**, $(\oplus_{i\in I}u_i, \oplus_{i\in I}H_i)$, is the unitary representation defined by $\left(\bigoplus_{i\in I} u_i\right)_g = \bigoplus_{i\in I}(u_i)_g$, for all $g \in G$.

Lemma 9.10 – Direct Sum Decomposition of Unitary Representations.
Let G be a discrete group, and $N \subset H$ an invariant subspace of the unitary representation (u, H). Then its orthogonal complement, $N^\perp$, is also invariant. Moreover, u is unitarily equivalent to the direct sum ${}_N|u \oplus {}_{N^\perp}|u$, where we define ${}_K|u : G \xrightarrow{u} \mathcal{U}(H) \xrightarrow{|_K} \mathcal{U}(K)$ for Hilbert subspaces $K \subset H$.

Proof. Suppose we let $\xi_1 \in N^\perp$. We would first like to show that $u_g(\xi_1) \in N^\perp$. We will proceed by showing that $u_g(\xi_1)$ is perpendicular to every $\xi_2 \in N$. But to see this, we simply apply the remark to definition 9.4, whence

$$\langle u_g(\xi_1), \xi_2\rangle = \langle \xi_1, u_g^*(\xi_2)\rangle = \langle \xi_1, u_g^{-1}(\xi_2)\rangle = 0$$

for all $\xi_2 \in N$ and $g \in G$, as the invariance of N ensures that $u_g^{-1}(\xi_2) \in N$. Thus $N^\perp$ is invariant under u. All that remains is to show that u is unitarily equivalent to ${}_N|u \oplus {}_{N^\perp}|u$. That is, we wish to find a unitary representation $w : H \to N \oplus N^\perp$ such that $w \circ u_g \circ w^{-1} = u_g|_N \oplus u_g|_{N^\perp}$, for all $g \in G$. But this is as simple as setting

$$w(\xi) := \mathrm{proj}_N(\xi) \oplus \mathrm{proj}_{N^\perp}(\xi),$$

$$w^{-1}(\xi_1 \oplus \xi_2) := \xi_1 + \xi_2,$$

where $\mathrm{proj}_K(\cdot)$ is the projection onto the subspace K. Note that by theorem 2.13, the closure of N ensures that $H \cong N \oplus N^\perp$, which is required in order for w to be bijective. Thus the result follows. This completes the proof. ■

Theorem 9.11 – Peter-Weyl Theorem.
Let (u, H) be a reducible unitary representation of a discrete group G. Then it is unitarily equivalent to a direct sum of irreducible representations of G.

Proof. The proof of this theorem follows from transfinite induction on the result of lemma 9.10. ■

Proposition-Definition 9.12 – Universal Representation.
Let G be a discrete group, and suppose we choose a representative u for each $[u] \in \widehat{G}$. The direct sum of all such unitarily distinct representations is called the **universal representation** of G, and denoted (U, H_U). For any unitary representation u of G, we have that $\|u(g)\| \leq \|U(g)\|$, for all $g \in G$.

Proof. By definition of the operator norm, the norm of an element $g \in G$ under U is given by

$$\|U(g)\| = \sup_{[u]\in\widehat{G}} \|u(g)\|.$$

That this holds for any arbitrary unitary representation, rather than specifically the irreducible representations, is a simple application of the Peter-Weyl theorem, as covering every irreducible representation naturally covers every reducible representation as well. This completes the proof. ■

10. Group Algebras

Definition 10.1 – Group Algebra.
The **group algebra** of a group G over a field $\mathbb{F}$, denoted $\mathbb{F}G$, is the set of all linear combinations of finitely many elements of G with coefficients in $\mathbb{F}$. That is,

$$\mathbb{F}G := \left\{ \sum_{g\in G} a_g g : a_g \in \mathbb{F}, \text{ where } a_g = 0 \text{ for all but finitely many } g \in G \right\}. \tag{10.1.1}$$

We can make $\mathbb{F}G$ into an algebra by defining

(10.1.2). scalar multiplication: $a \sum_{g\in G} a_g g := \sum_{g\in G} (a a_g) g$;

(10.1.3). vector addition: $\sum_{g\in G} a_g g + \sum_{g\in G} b_g g := \sum_{g\in G} (a_g + b_g) g$;

(10.1.4). vector multiplication: $\left(\sum_{g\in G} a_g g \right) \left(\sum_{h\in G} b_h h \right) := \sum_{g,h\in G} (a_g b_h) gh.$

Furthermore, for complex algebras with $\mathbb{F} = \mathbb{C}$, we may propose the additional definition

(10.1.5). $*$-operation: $\left(\sum_{g\in G} a_g g \right)^* := \sum_{g\in G} \overline{a}_g g^{-1}$,

whence we obtain a complex $*$-algebra.

Remarks: Note that we can rewrite vector multiplication as

$$\left(\sum_{g\in G} a_g g \right) \left(\sum_{h\in G} b_h h \right) = \sum_{h\in G} \left(\sum_{g\in G} a_g b_{g^{-1}h} \right) h.$$

In addition, using the notation $1g = g$ for all $g \in G$, we can essentially say that $G \subset \mathbb{F}G$, which is also a linear basis for $\mathbb{F}G$ by definition.

Proposition 10.2 – Abelian Group Algebras.
A group algebra on a group G is Abelian if and only if G is Abelian.

Proof. This follows trivially from the definition of vector multiplication on group algebras. ∎

Theorem 10.3 – Universal Property of Group Algebras.
Let $u : G \to \mathcal{U}(H)$ be a unitary representation of a discrete group G on the Hilbert space H. Then there exists a unique extension of u to a unital $*$-representation of $\mathbb{C}G$ on H, given by

$$\pi_u : \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g u_g. \tag{10.3.1}$$

Note, however, that this uniqueness does not necessarily guarantee that the map $u \mapsto \pi_u$ is injective. Furthermore, if $\pi : \mathbb{C}G \to \mathcal{B}(H)$ is a unital $*$-representation, then its restriction to G is a unitary representation of G. Finally, the representation u is irreducible if and only if π_u is irreducible.

Proof. To show the first result, we note that

$$\pi_u\left(\sum_{g,h\in G}(a_g b_h)gh\right) = \sum_{g,h\in G}(a_g b_h)u_{gh} = \sum_{g,h\in G}(a_g b_h)u_g u_h = \left(\sum_{g\in G} a_g u_g\right)\left(\sum_{h\in G} b_h u_h\right)$$

by the linearity and group homomorphism properties of u. Combining this with the linearity of π_u and the fact that it preserves adjoints, it is clear that it is a $*$-homomorphism; moreover, it is a unital $*$-representation, as desired.

We would now like to show that the operator $u = \pi|_G$ is a unitary representation. Well, suppose we define an operator $u_g := \pi(g)$ in the image; because π is a $*$-representation, it follows that

$$u_g^* u_g = \pi(g)^*\pi(g) = \pi(g^*)\pi(g) = \pi(g^{-1})\pi(g) = \pi(g^{-1}g) = \pi(e) = \mathrm{id}_H.$$

Similarly, $u_g u_g^* = \mathrm{id}_H$, hence u_g is unitary. To show that u is a $*$-homomorphism, we just note that π itself is a homomorphism and preserves adjoints.

Finally, if u is reducible, then by definition there exists a non-trivial invariant subspace N such that $u_g(N) \subseteq N$, for all $g \in G$. But it's clear that N must then be invariant for every operator in $\pi_u(\mathbb{C}G)$ too, as each such operator is nothing but a finite linear combination of operators u_g. Thus π_u is reducible. Conversely, if every operator in $\pi_u(\mathbb{C}G)$ has a common non-trivial invariant subspace N, then the restriction $u_g = \pi_u(g)$ must certainly also satisfy $u_g(N) = [\pi_u(g)](N) \subseteq N$ for all $g \in G$, hence u is reducible. The result follows. This completes the proof. ■

Proposition-Definition 10.4 – Left Regular Representation of Group Algebras.
Let G be a discrete group and $(\lambda, \ell^2(G))$ its left regular representation. Then the associated left regular representation of $\mathbb{C}G$ is the unitary $*$-representation $\pi_\lambda : \mathbb{C}G \to \mathcal{U}(\ell^2(G))$ mapping elements $a \in \mathbb{C}G$ to the corresponding unitary map $\pi_\lambda(a) : \ell^2(G) \to \ell^2(G)$, defined by

$$\pi_\lambda\left(\sum_{g\in G} a_g g\right) : \xi(h) \mapsto \sum_{g\in G} a_g \xi(g^{-1}h). \tag{10.4.1}$$

Proof. The proof for this is essentially the same as the proof for proposition-definition 9.6, as

$$\pi_\lambda : \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g \lambda(g).$$

■

Theorem 10.5 – Left Regular Representation is Injective.
Let G be a discrete group. The left regular representation π_λ of $\mathbb{C}G$ is injective.

Proof. Consider some $a = \sum_{g\in G} a_g g \in \ker(\pi_\lambda)$. We would like to show that $a = 0$. Well, choose any $g_0 \in G$ and let δ_h, δ_e be two delta maps, where e is the identity element of G. Then by linearity,

$$0 = \langle[\pi_\lambda(a)](\delta_{g_0}), \delta_e\rangle = \sum_{g\in G} a_g\langle[\lambda(g)](\delta_{g_0}), \delta_e\rangle = \sum_{g\in G} a_g\langle\delta_{gg_0}, \delta_e\rangle = \sum_{g\in G}\sum_{h\in G} a_g \delta_{gg_0}(h)\delta_e(h) = a_{g_0^{-1}}.$$

But g_0 was arbitrary, hence $a = 0$. The result follows by linearity. This completes the proof. ■

Theorem 10.6 – Trivial Trace on Group Algebras.
Let G be a discrete group. Then the map $\tau : \mathbb{C}G \to \mathbb{C}$, defined by

$$\tau : \sum_{g\in G} a_g g \mapsto a_e, \tag{10.6.1}$$

is a faithful trace on $\mathbb{C}G$.

Proof. Note that τ is clearly linear and unital. To see that it is positive and faithful, we observe that for any $a = \sum_{g\in G} a_g g \in \mathbb{C}G$, we have

$$a^*a = \left(\sum_{g\in G} a_g g\right)^* \left(\sum_{g\in G} a_g g\right) = \left(\sum_{g\in G} \overline{a}_g g^{-1}\right) \left(\sum_{g\in G} a_g g\right) = \sum_{g,h\in G} \overline{a}_g a_h g^{-1}h.$$

Thus we see that $\tau(a^*a)$ is the sum over $g = h$ above; that is,

$$\tau(a^*a) = \sum_{g\in G} \overline{a}_g a_g = \sum_{g\in G} |a_g|^2 \geq 0.$$

Hence τ is positive, and furthermore it is clearly faithful, as $\tau(a^*a) = 0$ only when $a_g = 0$, for all $g \in G$. This completes the proof. ■

Example 10.7 – Trivial Representation.
Consider the trace τ, as defined in theorem 10.6. Suppose we define $N_\tau := \{a \in \mathbb{C}G : \tau(a^*a) = 0\}$. Because τ is faithful, we actually have that $N_\tau = \{0\}$. Suppose we consider now the quotient group $\mathbb{C}G/N_\tau = \{a + N_\tau : a \in \mathbb{C}G\} \cong \mathbb{C}G$. Because this space is discrete, it is equal to its closure, and hence $H_\tau = \overline{\mathbb{C}G/N_\tau} \cong \mathbb{C}G$. Furthermore, this becomes a Hilbert space when endowed with the bilinear form $\langle a, b\rangle = \tau(b^*a) = \sum_{g\in G} \overline{b}_g a_g$. By the Gelfand-Naimark-Segal construction, it thus follows that $[\pi_\tau(a)](b) := ab$ defines a $*$-representation of $\mathbb{C}G$ on H_τ. It turns out that π_τ here is nothing but the map π_τ from the universal property, associated with the **trivial representation** $1_G : g \mapsto \mathrm{id}_H$.

11. Finite Group C^*-Algebras

Theorem 11.1 – C^*-Algebras of Finite Groups.
If G is a finite group, then there exists a unique norm for which the group algebra $\mathbb{C}G$ is a C^*-algebra.

Proof. Suppose we define $\|a\| := \|\pi_\lambda(a)\|$, where $\|\pi_\lambda(a)\|$ is the operator norm of the left regular representation of a. This is clearly a seminorm on $\mathbb{C}G$, from the linearity of the left regular representation and the properties of the operator norm. The fact that it is a norm – that it is positive-definite – follows from the fact that the left regular representation defines a faithful trace. Because G is a finite basis for $\mathbb{C}G$, the latter is finite-dimensional, and hence this norm is complete. Furthermore, it satisfies the C^*-condition, as π_λ is a $*$-homomorphism and the operator norm satisfies the C^*-condition. Finally, uniqueness follows from the more general properties of C^*-algebras, as C^*-norms are unique. This completes the proof. ■

Theorem 11.2 – Structure of Finite Group C^*-Algebras.
Let G be a finite group with cardinality $|G|$ and conjugacy classes $C_1, \ldots, C_K$. For each such conjugacy class, suppose we define $c_k \in \mathbb{C}G$ such that

$$c_k := \sum_{g \in C_k} g. \tag{11.2.1}$$

Then the set $\{c_1, \ldots, c_K\}$ is linearly independent, and its span is the center of $\mathbb{C}G$, where its center is given by treating it as a ring. In particular, $\mathbb{C}G$ is isomorphic to

$$\bigoplus_{k=1}^{K} M_{n_k}(\mathbb{C}), \tag{11.2.2}$$

where $M_{n_k}(\mathbb{C})$ denotes the set of complex $n_k \times n_k$ matrices, and $\{n_k\}_{k=1}^K$ is a set of positive integers. Furthermore, these integers satisfy

$$\sum_{k=1}^{K} n_k^2 = |G|. \tag{11.2.3}$$

Proof. We know that $\mathbb{C}G$ is finite-dimensional, as G forms a finite basis for it. Hence, by theorem 7.3, there exist positive integers K and $\{n_k\}_{k=1}^K$ such that conditions (11.2.2) and (11.2.3) hold.

We would now like to show that the center of $\mathbb{C}G$ is the span of $\{c_k\}_{k=1}^K$. Note that the center here is nothing but the center of the ring embedded within it. That is, it is given by the subring $\{a \in \mathbb{C}G : a = hah^{-1}, \forall h \in \mathbb{C}G\}$. Furthermore, recall that two elements $g_1, g_2 \in G$ are **conjugate** if there is an element h for which $hg_1h^{-1} = g_2$. This defines an equivalence relation, with the equivalence class $\{hgh^{-1} : h \in G\}$ referred to as the **conjugacy class** of $g \in G$. Well, suppose that $a = \sum_{g \in G} a_g g$ is in the center of $\mathbb{C}G$, and let $h \in G$. Then we have that

$$\sum_{g \in G} a_g g = a = hah^{-1} = \sum_{g \in G} a_g hgh^{-1} = \sum_{g \in G} a_{h^{-1}gh} g.$$

Comparing the coefficients of any $g \in G$, it follows that we must have $a_g = a_{h^{-1}gh}$. In other words, the coefficient corresponding to g is equal to the coefficients corresponding to the other elements of its conjugacy class. Denoting by z_k the coefficient corresponding to the conjugacy class C_k, it is clear that we may write

$$a = \sum_{g \in G} a_g g = \sum_{k \in K} z_k \sum_{g \in C_k} g = \sum_{k \in K} z_k c_k.$$

Hence $\mathbb{C}G$ is certainly spanned by $\{c_k\}_{k=1}^K$. Conversely, if we consider the entire conjugacy class, we know that each c_k must commute with every group element h. But since the set of all group elements trivially spans the entire group algebra, we know that each c_k must lie in the center of $\mathbb{C}G$. Finally, the linear independence of $\{c_k\}_{k=1}^K$ is clear from the fact that no two distinct c_i, c_j contain the same group element g. This completes the proof. ■

Example 11.3 – Structure of Symmetric Group C^*-Algebras.
Consider the group algebra $\mathbb{C}S_3$ of the symmetric group S_3. We can use the previous theorem to better understand its structure in terms of more familiar algebras. Well, S_3 has three conjugacy groups: these are the identity, two cycles of length three and the three transpositions. Furthermore, S_3 naturally has cardinality 6. Thus, we will consider three integers whose squares sum to 6. There is only one possibility for this: hence $\mathbb{C}S_3 \cong M_2(\mathbb{C}) \oplus \mathbb{C} \oplus \mathbb{C}$ by theorem 11.2.

12. Discrete Group C^*-Algebras

Definition 12.1 – ℓ^1-Norm on Discrete Group Algebras.
Let G be a discrete group. We define the **ℓ^1-norm** on $\mathbb{C}G$ by

$$\left\| \sum_{g\in G} a_g g \right\|_1 \coloneqq \sum_{g\in G} |a_g|. \tag{12.1.1}$$

Remarks: So far, we have been thinking of elements of the group algebra strictly as a linear combination of group elements. However, we typically think of the ℓ^1-norm as acting on function spaces! There is a subtle disconnect here between the implications of this notation and its actual meaning. This can be avoided by thinking of elements $a \in \mathbb{C}G$ as maps of the form $a(g) = a_g$.

Theorem-Definition 12.2 – Discrete Convolution Algebra.
Let G be a discrete group. The completion of $\mathbb{C}G$ under the ℓ^1-norm is nothing but

$$\ell^1(G) \coloneqq \left\{ a : G \to \mathbb{C} : \sum_{g\in G} |a(g)| < \infty \right\}. \tag{12.2.1}$$

We define the **(discrete) convolution algebra** of G to be $\ell^1(G)$ under the operations

(12.2.2). $[\lambda a](g) \coloneqq \lambda a(g)$, for all $\lambda \in \mathbb{C}$, $a \in \ell^1(G)$, $g \in G$ (scalar multiplication);
(12.2.3). $[a+b](g) \coloneqq a(g) + b(g)$, for all $a, b \in \ell^1(G)$, $g \in G$ (vector addition);
(12.2.4). $[ab](g) \coloneqq \sum_{h\in G} a(h)b(h^{-1}g)$, for all $a, b \in \ell^1(G)$, $g \in G$ (vector multiplication);
(12.2.5). $[a^*](g) \coloneqq \overline{a(g^{-1})}$, for all $a \in \ell^1(G)$, $g \in G$ ($*$-operation.)

In particular, these make $\ell^1(G)$ into a Banach $*$-algebra with an isometric $*$-operation.

Proof. It is a simple matter to check that the axioms of Banach $*$-algebras hold with respect to the operations provided. As a result, we shall just show that $\ell^1(G)$ is complete. Let $(a_n)_{n=0}^\infty$ be a Cauchy sequence in $\ell^1(G)$. Then for every $\varepsilon > 0$, there exists an $N(\varepsilon) \in \mathbb{N}$ such that

$$\|a_m - a_n\|_1 = \sum_{g\in G} |a_m(g) - a_n(g)| < \varepsilon,$$

whenever $m, n > N(\varepsilon)$. But for each $h \in G$, it is clear that

$$|a_m(h) - a_n(h)| \le \sum_{g\in G} |a_m(g) - a_n(g)| < \varepsilon.$$

Thus $(a_n)_{n=0}^\infty$ is Cauchy in $\mathbb{C}$, and so converges to some $z_g \in \mathbb{C}$ by the completeness of $\mathbb{C}$. Suppose we now define the map $a' : g \mapsto z_g$: we claim that $a' \in \ell^1(G)$. By definition, $\|a_n\|_1$ is a convergent sum of non-negative, real numbers. Because uncountable sums of non-negative, real numbers cannot converge, we know that $|a_n(g)| = 0$ for all but those g in some countable subset $G_n \subseteq G$. Let $G^* \coloneqq \bigcup_{n=1}^\infty G_n$. Then G^* is also countable, and in particular

$$\|a_n\|_1 = \sum_{g\in G} |a_n(g)| = \sum_{g\in G^*} |a_n(g)|,$$

for each $n \in \mathbb{N}$. Suppose we now let $(g_k)_{k=0}^\infty$ be some enumeration of G^*. Then we also have that

$$\|a_n\|_1 = \sum_{g \in G^*} |a_n(g)| = \sum_{k=0}^{\infty} a_n(g_k),$$

for any $n \in \mathbb{N}$. Because $(a_n)_{n=0}^{\infty}$ is Cauchy, it is norm bounded; thus there must exist some $M > 0$ for which $\|a_n\|_1 \leq M$, for all $n \in \mathbb{N}$. Combining these two results, we obtain

$$\sum_{k=0}^{K} |a'(g_k)| = \sum_{k=0}^{K} \lim_{n\to\infty} |a_n(g_k)| = \lim_{n\to\infty} \sum_{k=0}^{K} |a_n(g_k)| \leq \lim_{n\to\infty} \sum_{k=0}^{\infty} |a_n(g_k)| = \lim_{n\to\infty} \|a_n\|_1 \leq M,$$

for all $K \in \mathbb{N}$. Finally, taking limits,

$$\|a'\|_1 = \sum_{k=0}^{\infty} |a'(g_k)| = \lim_{k\to\infty} \sum_{k=0}^{K} |a'(g_k)| \leq M < \infty,$$

whence it follows that $a' \in \ell^1(G)$. All that remains is to show that $(a_n)_{n=0}^{\infty}$ converges to a'. Well, because $a' \in \ell^1(G)$ and $a_n \in \ell^1(G)$ for all $n \in \mathbb{N}$, we know that $a' - a_n \in \ell^1(G)$ for all $n \in \mathbb{N}$, as $\ell^1(G)$ is a linear space. Hence $\|a' - a_n\|_1 < \infty$ for all $n \in \mathbb{N}$. Similarly to before, we will denote by G_n the countable set of $g \in G$ such that $|a'(g) - a_n(g)| > 0$, and let $G^* := \bigcup_{n=1}^{\infty} G_n$. With $(g_k)_{k=0}^{\infty}$ an enumeration of G^*, we have that

$$\|a' - a_n\|_1 = \sum_{g\in G} |a'(g) - a_n(g)| = \sum_{k=0}^{\infty} |a'(g_k) - a_n(g_k)|,$$

for all $n \in \mathbb{N}$. By once again citing the fact that $(a_n)_{n=0}^{\infty}$ is Cauchy, we can say that

$$\sum_{k=0}^{K} |a_m(g_k) - a_n(g_k)| \leq \|a_m - a_n\|_1 = \sum_{g\in G} |a_m(g) - a_n(g)| = \sum_{k=0}^{\infty} |a_m(g_k) - a_n(g_k)| < \varepsilon,$$

for any $K \in \mathbb{N}$ and $m, n > N(\varepsilon)$. Furthermore, for any K and $n > N(\varepsilon)$, we see that

$$\sum_{k=0}^{K} |a'(g_k) - a_n(g_k)| = \lim_{m\to\infty} \sum_{k=0}^{K} |a_m(g_k) - a_n(g_k)| \leq \varepsilon.$$

In other words, for all $n > N(\varepsilon)$,

$$\|a' - a\|_1 = \sum_{k=0}^{\infty} |a'(g_k) - a_n(g_k)| \leq \varepsilon.$$

Hence $(a_n)_{n=0}^{\infty}$ converges to $a' \in \ell^1(G)$ under the ℓ^1-norm. This completes the proof. ■

Theorem 12.3 – Trivial Trace on Discrete Convolution Algebras.
Let G be a discrete group and $a \in \ell^1(G)$. The linear functional $\tau(a) = a(e)$, where e is the identity of G, is a bounded trace on $\ell^1(G)$.

Proof. For any $a \in \ell^1(G)$, we see that $\|a\|_1 \geq |a(e)| = |\tau(a)|$, hence τ is certainly bounded. Theorem 10.6 tells us that it is a trace on $\mathbb{C}G$, which extends to $\ell^1(G)$. This completes the proof.

■

Theorem 12.4 – Bijective Correspondences of Representations.
Let G be a discrete group. There are bijective correspondences between the unitary representations of G, the non-degenerate (that is, unital) $*$-representations of $\mathbb{C}G$ and the non-degenerate (unital) $*$-representations of $\ell^1(G)$. Furthermore, these correspondences preserve irreducibility. Finally, every non-degenerate $*$-representation of $\ell^1(G)$ is a contraction.

Proof. First, recall that the non-degenerate $*$-representations of $\mathbb{C}G$ and $\ell^1(G)$ are simply the unital $*$-representations by proposition 8.8. Furthermore, we know that $G \subset \mathbb{C}G \subset \ell^1(G)$; hence we trivially obtain bijections from the unital $*$-representations of $\ell^1(G)$ to the unital $*$-representations of $\mathbb{C}G$, and from the unital $*$-representations of $\mathbb{C}G$ to the unitary representations of G, by taking restrictions. We have already seen that the unitary representations of G extend to unital $*$-representations of $\mathbb{C}G$ by the universal property. So actually, we only need to show that there is a bijective correspondence from the unital $*$-representations of $\mathbb{C}G$ to the unital $*$-representations of $\ell^1(G)$, that every non-degenerate $*$-representation of $\ell^1(G)$ is a contraction, and that irreducibility is preserved by these correspondences.

Let π be a unital $*$-representation of $\mathbb{C}G$, and define a unital $*$-representation $\pi' : \ell^1(G) \to \mathcal{B}(H)$ by

$$\pi' : a \mapsto \sum_{g \in G} a(g)\pi(g).$$

We claim that this map is well-defined and injective. Well, we know that the coefficients $a(g)$ are absolutely summable by definition. Because π is a unital $*$-homomorphism, we also have

$$\pi(g)^*\pi(g) = \pi(g^*)\pi(g) = \pi(g^*g) = \pi(g^{-1}g) = \pi(e) = \mathrm{id}_H,$$

and similarly $\pi(g)\pi(g)^* = \mathrm{id}_H$. As a result, $\pi(g)$ is unitary and hence has unit norm, for all $g \in G$. So it follows from the triangle inequality that

$$\|\pi'(a)\| = \left\| \sum_{g \in G} a(g)\pi(g) \right\| \leq \sum_{g \in G} |a(g)| \|\pi(g)\| = \sum_{g \in G} |a(g)| = \|a\|_1.$$

Thus π' is well-defined, and furthermore it is a contraction. The map $\pi \mapsto \pi'$ is then our desired correspondence between the unital $*$-representations of $\mathbb{C}G$ and $\ell^1(G)$, which has an inverse given by taking restrictions.

Finally, we would like to show that these bijective correspondences preserve the irreducibility of the representations. If π' is a reducible $*$-representation of $\ell^1(G)$, then its restriction to $\mathbb{C}G$ must also admit the same non-trivial invariant subspaces. Similarly, the restriction of a reducible $*$-representation of $\mathbb{C}G$ to a representation of G will also be a reducible representation in this way. Conversely, if a unitary representation of G has a non-trivial invariant subspace, then its extension to $\mathbb{C}G$ will admit the same non-trivial invariant subspace. Furthermore, for any sequence $(a_n)_{n=0}^{\infty} \subseteq \mathbb{C}G$ converging to $a \in \ell^1(G)$, with $\pi'(a_n)$ leaving some subspace N invariant for $n \in \mathbb{N}$, we see that $\pi'(a)$ must also leave N invariant. This is precisely a consequence of our requirement that invariant subspaces N be closed, as $(\pi(a_n))_{n=0}^{\infty}$ is a Cauchy sequence in N, and closed subspaces of complete spaces are complete. Hence we see that the irreducibility of the representations is preserved, as desired. This completes the proof. ■

Theorem-Definition 12.5 – Universal Group C^*-Algebra.
Let G be a discrete group. We define the **universal norm** on $\mathbb{C}G$ by

$$\|a\|_U := \sup\{\|\pi_u(a)\| : u \text{ is a unitary representation of } G\}, \tag{12.5.1}$$

for each $a \in \mathbb{C}G$, is a well-defined norm on $\mathbb{C}G$. The completion of $\mathbb{C}G$ with respect to this norm is a referred to as the **universal group C^*-algebra** of G, and denoted $C^*(G)$. In particular, $C^*(G)$ is a C^*-algebra containing $\mathbb{C}G$ as a dense $*$-subalgebra.

Proof. By the universal property, π_u is a non-degenerate (unital) representation of $\mathbb{C}G$. But every non-degenerate $*$-representation π_u of $\mathbb{C}G$ corresponds to a unique, contractive $*$-representation of $\ell^1(G)$ by theorem 12.4; thus $\|\pi_u(a)\| \leq \|a\|_1$. This implies that (12.5.1) is bounded, and hence that the supremum exists for each $a \in \mathbb{C}G$. Thus (12.5.1) is well-defined. It is easy to see that the norm properties are satisfied due to being satisfied by the underlying operator norm in the definition. In fact, the Banach and C^* conditions are satisfied for this same reason. As a result, we know that the completion will be a C^*-algebra. The fact that $\mathbb{C}G$ is dense in $C^*(G)$ is essentially by definition, as $C^*(G)$ is a metric closure of $\mathbb{C}G$. This completes the proof. ■

Theorem-Definition 12.6 – Abelian Group C^*-Algebras.
Let G be a discrete group. Then the group C^*-algebra, $C^*(G)$, is a unital C^*-algebra, and it is Abelian if and only if G is Abelian.

Proof. The identity of G corresponds to the identity of $\mathbb{C}G$, and hence corresponds to the identity of any completion as well. Furthermore, by theorem 10.2, we know that $\mathbb{C}G$ is Abelian if and only if G is Abelian. Because a dense $*$-subalgebra of a C^*-algebra such as $\mathbb{C}G$ is Abelian if and only if the entire C^*-algebra is Abelian, the result follows. This completes the proof. ■

Proposition 12.7 – Universal Group C^*-Algebra Norm.
Let G be a discrete group. Then

$$\|a\|_U = \sup\{\|\pi_u(a)\| : u \text{ is an irreducible representation of } G\} = \|\pi_U(a)\|, \tag{12.7.1}$$

for each $a \in \mathbb{C}G$, where π_U is the $*$-representation of $\mathbb{C}G$ corresponding to the universal representation.

Proof. This result is a direct consequence of proposition 9.12. ■

Definition 12.8 – Reduced Group C^*-Algebra.
Let G be a discrete group. We define the **reduced norm** on $\mathbb{C}G$ by

$$\|a\|_r = \|\pi_\lambda(a)\|, \tag{12.8.1}$$

for each $a \in \mathbb{C}G$, where π_λ denotes the left regular representation. The completion of $\mathbb{C}G$ with respect to this norm is a referred to as the **reduced group C^*-algebra** of G, and denoted $C^*_r(G)$.

Remarks: It is once again easy to see that $C^*_r(G)$ is a C^*-algebra, as $\mathcal{B}(H)$ is a C^*-algebra, meaning $\|a^*a\|_r = \|\pi_\lambda(a^*a)\| = \|\pi_\lambda(a)^*\pi_\lambda(a)\| = \|\pi_\lambda(a)\|^2 = \|a\|_r^2$, for all $a \in \mathbb{C}G$. In fact, this is true for any $*$-representation π, not just π_λ; we denote by $C^*_\pi(G) := \overline{\pi(\mathbb{C}G)}$ any such associated C^*-algebra.

Theorem 12.9 – Canonical $*$-Homomorphism.
Let G be a discrete group. Then for any $*$-representation π of $\mathbb{C}G$, there exists an associated surjective $*$-homomorphism $\hat{\pi} : C^*(G) \to C^*_\pi(G)$.

Proof. Let π be a $*$-representation of $\mathbb{C}G$, with $C^*_\pi(G)$ its associated C^*-algebra (including $C^*_r(G)$, for $\pi = \pi_\lambda$). Consider the map defined by $\hat{\pi}(a) := \pi(a)$, for $a \in \mathbb{C}G \subseteq C^*(G)$. Well, due to the equivalent characterization $C^*_\pi(G) := \overline{\pi(\mathbb{C}G)}$, we know we can write $\pi(a) \in C^*_\pi(G)$, so it makes sense to think of the codomain of $\hat{\pi}$ as $C^*_\pi(G)$. To see that we may extend it to a map on $C^*(G)$, consider some $a \in C^*(G)$ corresponding to the norm limit of the Cauchy sequence $(a_n)_{n=0}^\infty$. From the definitions of the group C^*-algebras, we see that $\|\hat{\pi}(a_m) - \hat{\pi}(a_n)\|_\pi = \|\hat{\pi}(a_m - a_n)\|_\pi \leq \|a_m - a_n\|_U$ for all $m, n \in \mathbb{N}$, and hence $(\pi(a_n))_{n=0}^\infty$ defines a Cauchy sequence in $C^*_\pi(G)$. Because $C^*_\pi(G)$ is complete, it will contain the limit of this sequence. Defining $\hat{\pi}(a)$ equal to this limit for all such a, we will naturally extend $\hat{\pi}$ to a $*$-homomorphism on $C^*_\pi(G)$ as desired. This can be checked by considering two sequences $(a_m)_{m=0}^\infty, (b_n)_{n=0}^\infty$, and noting that $\hat{\pi}(ab) = \lim \hat{\pi}(a_m b_n) = \lim \hat{\pi}(a_m)\hat{\pi}(b_n)$, for instance. To prove surjectivity, we can take a Cauchy sequence in $C^*_\pi(G)$ and work backwards into $C^*(G)$, as these sequences will be of the form $(\pi(a_n))_{n=0}^\infty$. This completes the proof. ■

Theorem 12.10 – Trivial Trace on Group C^*-Algebras.
Let G be a discrete group, and define a map $\tau : \mathbb{C}G \to \mathbb{C}$ by

$$\tau(a) := \langle \pi_\lambda(a)\delta_e, \delta_e \rangle, \tag{12.10.1}$$

for each $a \in \mathbb{C}G$. This extends to continuous traces on both $C^*(G)$ and $C^*_r(G)$, with the same formula holding regardless of which of these two algebras we take the element a from.

Proof. We first observe that, from the definition of the left regular representation and its remark,

$$\tau(a) = \langle \pi_\lambda(a)\delta_e, \delta_e \rangle = \left\langle \pi_\lambda\left(\sum_{g\in G} a(g)g\right)\delta_e, \delta_e \right\rangle = \sum_{g\in G} a(g)\langle \lambda(g)\delta_e, \delta_e\rangle = \sum_{g\in G} a(g)\langle \delta_g, \delta_e\rangle = a(e).$$

It follows that $|\tau(a)| \leq \|\pi_\lambda(a)\| = \|a\|_r \leq \|a\|_U$, and hence τ extends as expected using a Cauchy sequence argument similar to those in the preceding proofs. Finally, because τ satisfies the trace properties on $\mathbb{C}G$, a dense subalgebra of both $C^*(G)$ and $C^*_r(G)$, it follows that the extensions of τ shall also satisfy these properties. This completes the proof. ■

Exercise 12.11 – Putnam Exercise 2.4.1.
The following exercise is taken from Putnam's lecture notes on C^*-algebras [4].

"Let G be a discrete group. For each group element g, we let δ_g be the function which is 1 at g and 0 elsewhere. We regard this as an element of $\ell^2(G)$. Let a be in $\mathcal{B}(\ell^2(G))$."

12.11.1. "Prove that if a is in the closure of $\pi_\lambda(\mathbb{C}G)$, then $(a\delta_e)(g) = \langle a\delta_h, \delta_{gh}\rangle$, for all g, h in G."
Proof. Let $a \in \mathcal{B}(\ell^2(G))$. First, because $\pi_\lambda(\mathbb{C}G) \subseteq \mathcal{B}(\ell^2(G))$, it makes sense to consider a also in $C_r^*(G) := \overline{\pi_\lambda(\mathbb{C}G)}$. Furthermore, by considering Cauchy sequences of elements in $\pi_\lambda(\mathbb{C}G)$, it is clear that every element in $\overline{\pi_\lambda(\mathbb{C}G)}$ can be written in a form similar to that given in definition 10.4. That is, for every $a \in \overline{\pi_\lambda(\mathbb{C}G)}$, we may write

$$a : \xi(k) \mapsto \sum_{j\in G} a_j \xi(j^{-1}k),$$

for constants $\{a_j\}_{j\in G} \subseteq \mathbb{C}$. Thus, it follows that

$$\langle a\delta_h, \delta_{gh}\rangle = \sum_{j\in G} a_j \langle \delta_{jh}, \delta_{gh}\rangle = a_g = \sum_{j\in G} a_j \delta_j(g) = [a\delta_e](g),$$

as desired. This completes the proof. ■

12.11.2. "Prove that if a is in the centre of the closure of $\pi_\lambda(\mathbb{C}G)$, then the function $a\delta_e$ is constant on conjugacy classes in G."
Proof. Note that, for $a, b \in \overline{\pi_\lambda(\mathbb{C}G)}$, we have

$$ab : \xi(k) \mapsto \sum_{g,h\in G} a_g b_h \xi(g^{-1}h^{-1}k),$$

$$ba : \xi(k) \mapsto \sum_{g,h\in G} a_g b_h \xi(h^{-1}g^{-1}k).$$

Suppose now that $a \in 中(\overline{\pi_\lambda(\mathbb{C}G)})$, where 中 denotes the center. In other words, $ab = ba$, for all $b \in \overline{\pi_\lambda(\mathbb{C}G)}$. Consider the above forms for ab and ba. Note that we require equality to hold for all $b_h \in \mathbb{C}$, $k \in G$ and $\xi \in \ell^2(G)$. Looking at the cases when $\xi = \delta_j$, for instance, we see that we at least require $g^{-1}h^{-1} = h^{-1}g^{-1}$, for all $h \in G$ and $g \in G$ such that $a_g \neq 0$. Hence $a_g = 0$ for all $g \notin 中(G)$. Because $[g] = \{g\}$ is the conjugacy class for all $g \in 中(G)$, the desired result naturally must follow. This completes the proof. ■

12.11.3. "In the last two problems, which topologies can you use when taking the closure?"
Using $C_r^*(G) := \overline{\pi_\lambda(\mathbb{C}G)}$, the obvious choice is the metric topology, induced by the reduced norm (or operator norm).

12.11.4. "Prove that if every conjugacy class in G is infinite, except that of the identity, then $C_r^*(G)$ has a trivial centre."
Proof. As we have shown previously, if an element is in the center of $C_r^*(G)$, then the only non-zero coefficients for this element are those that correspond to the elements of 中(G). But if every conjugacy class of G is infinite (except, of course, for the conjugacy class corresponding to the identity element, e), we must have 中$(G) = \{e\}$. Hence the only element that can be in the center of $C_r^*(G)$ is the element a with $a(g) = 0$ for all $g \neq e$. This completes the proof. ■

12.11.5. "Prove that the groups F_2 and S_∞ have the infinite conjugacy class property."
Proof. We will prove the statement for S_∞. Recall that two elements of S_n are conjugate if and only if they consist of the same cycle type. But for any particular cycle type in S_∞, we can obviously construct infinitely many elements with this cycle type, except of course for the cycle type corresponding to the identity element. Hence S_∞ satisfies the infinite conjugacy class property as expected. This completes the proof. ■

Exercise 12.12 – Putnam Exercise 2.4.2.
The following exercise is taken from Putnam's lecture notes on C^*-algebras [4].

"As we noted above, the identity map on $\mathbb{C}G$ extends to a $*$-homomorphism from $\ell^1(G)$ to $C^*(G)$. Prove that the composition of this map with ρ of 2.4.10 is injective."

Proof. Let $\iota : \ell^1(G) \to C^*(G)$ be the aforementioned $*$-homomorphism extending the identity map on $\mathbb{C}G$. We would like to show that it is injective by showing that the map $\iota \circ \hat{\pi}_\lambda$ is injective, where $\hat{\pi}_\lambda$ was given in theorem 12.9. But note that, for $a' \in \ell^1(G)$, we have $\pi_\lambda(\iota(a')) = \pi_\lambda(a)$, for $a = \iota(a') \in C^*(G)$. Hence the same process as in theorem 10.5 applies. This completes the proof. ■

13. Abelian Group C^*-Algebras

Definition 13.1 – Pontryagin Dual.
Let G be a group. The **Pontryagin dual** of G, denoted $\hat{G}$, is the set of all continuous group homomorphisms of the form $\chi : G \to \mathbb{T}$, where $\mathbb{T}$ denotes the typical circle group.

Remarks: Note that we will primarily be looking at discrete groups; under the discrete topology, all group homomorphisms are obviously continuous. We therefore won't need to pay much consideration to this continuity condition.

Theorem 13.2 – Discrete, Abelian Duals.
Let G be a discrete Abelian group. The corresponding dual group $\hat{G}$ is nothing but the set of irreducible representations of G over the Hilbert space $\mathbb{C}$.

Proof. Suppose we have some irreducible representation $\pi : G \to \mathcal{U}(\mathbb{C})$. Because $\mathcal{U}(\mathbb{C}) \cong \mathcal{U}(1) \cong \mathbb{T}$, this naturally corresponds to a homomorphism $\chi : G \to \mathbb{T}$. Conversely, suppose we have some group homomorphism $\chi : G \to \mathbb{T}$. As before, we note that $\mathbb{T} \cong \mathcal{U}(\mathbb{C})$. Furthermore, because $\mathbb{C}$ is one-dimensional as a complex Hilbert space, so too is $\mathcal{U}(\mathbb{C})$. Thus the representation is irreducible, as every subspace of a one-dimensional space is trivial. This completes the proof. ■

Theorem 13.3 – Pontryagin Dual is Compact and Hausdorff.
Let G be a discrete Abelian group. Its Pontryagin dual $\hat{G}$ forms a group when endowed with pointwise function multiplication. Furthermore, suppose we define

$$V(\chi, F, \varepsilon) := \left\{ \chi' \in \hat{G} : |\chi'(g) - \chi(g)| < \varepsilon, g \in F \right\}. \tag{13.3.1}$$

Then the collection of sets $S := \{V(\chi, F, \varepsilon) : \chi \in \hat{G}, F \subset G, \varepsilon > 0\}$ forms a subbase for a topology on $\hat{G}$. In particular, $\hat{G}$ is compact and Hausdorff with respect to this topology.

Proof. Verifying that $\hat{G}$ forms a group under pointwise products of functions is a straightforward process. As a result, we will focus on the second statement. Suppose we consider $\mathbb{T}^G$, the set of functions from G to $\mathbb{T}$. We can think of this as $\prod_{g \in G} \mathbb{T}_g$, where $\mathbb{T}_g$ is nothing but a copy of $\mathbb{T}$ that we associate with $g \in G$. This interpretation admits a product topology on $\mathbb{T}^G$. The topology of pointwise convergence on $\hat{G} \subset \mathbb{T}^G$, for which S is a natural subbase, is then just the subspace topology induced by this product topology on $\mathbb{T}^G$. Well, $\mathbb{T}$ is compact, thus by **Tychonoff's theorem** so too is $\mathbb{T}^G$; furthermore, it is certainly also Hausdorff. But $\hat{G}$ is a closed subset of $\mathbb{T}^G$, whence the result follows. This completes the proof. ■

Example 13.4 – Pontryagin Dual of Integers.
Consider the group of integers, $\mathbb{Z}$, one of the simplest Abelian groups. We claim that the evaluation map $\hat{\mathbb{Z}} \to \mathbb{T} : \chi \mapsto \chi(1)$ is both a group isomorphism and a homeomorphism.

Well, cyclic group homomorphisms are uniquely determined by how they map the group identity; this of course applies to all maps $\chi \in \hat{\mathbb{Z}}$, so our evaluation map is injective. Furthermore, due to the fact that $\mathbb{Z}$ is free, for any $z \in \mathbb{T}$ there exists a homomorphism χ such that $\chi(1) = z$. In particular, such a homomorphism is of course $\chi : n \mapsto z^n$. Finally, it is relatively easy to show that it is a group homomorphism, and hence a group isomorphism. To see that it is a homeomorphism, we first observe that it is continuous, with $\hat{\mathbb{Z}}$ compact by theorem 13.3 and $\mathbb{T}$ Hausdorff. But continuous bijections from compact spaces to Hausdorff spaces have continuous inverses, whence the result follows.

Theorem 13.5 – Structure of Discrete Abelian Group C^*-Algebras.
Let G be a discrete Abelian group. Then the corresponding group C^*-algebra, $C^*(G)$, is isomorphic to $\mathcal{C}(\hat{G})$, the space of continuous functionals on $\hat{G}$. Furthermore, this isomorphism takes a group element $g \in \mathbb{C}G \subset C^*(G)$ to the function $\hat{g} : \chi \mapsto \chi(g)$.

Proof. First, we know that $C^*(G)$ is unital, and by theorem 12.6 it is also Abelian. Thus by theorem 6.7, we know that $C^*(G)$ is isomorphic to $\mathcal{C}(\mathcal{M}(C^*(G)))$ by means of the function defined by $\hat{} : C^*(G) \to \mathcal{C}(\mathcal{M}(C^*(G))) : g \mapsto \hat{g}$, where $\hat{g}$ is the evaluation map $\hat{g}(\chi) = \chi(g)$. All we need to do is identify $\mathcal{M}(C^*(G))$, the set of non-zero, homomorphic functionals on $C^*(G)$, with $\hat{G}$. We will do this by showing that they are homeomorphic.

Well, consider $\chi \in \mathcal{M}(C^*(G))$; because $G \subset \mathbb{C}G \subset C^*(G)$, it makes sense to restrict it to G. In fact, since χ is a homomorphism, it follows that its restriction $\chi|_G$ is a group homomorphism. In other words, $\chi|_G \in \hat{G}$, so the restriction operation defines a map from $\mathcal{M}(C^*(G))$ to $\hat{G}$. Furthermore, two multiplicative functions that agree for each element of G must be equal, so because the elements of G span a dense subset of $C^*(G)$ by theorem 12.5, this restriction operation is injective.

To show that this restriction operation is surjective, let $\chi \in \hat{G}$. We can actually regard χ as a unitary representation on some one-dimensional Hilbert space H; thus by the universal property, we can further identify it with a unique $*$-representation of $\mathbb{C}G$ on H. Its extension to $C^*(G)$ is then a homomorphic functional whose restriction to G is χ, and hence the restriction operation is surjective.

The restriction operation is continuous, and because it is also a bijection from a compact space to a Hausdorff space, its inverse is also continuous. Thus $\mathcal{M}(C^*(G))$ is homeomorphic to $\hat{G}$, whence the result follows. This completes the proof. ■

Example 13.6 – Pontryagin Dual of Cyclic Groups.
Consider the cyclic group $\mathbb{Z}_n$, our favourite group for examples. We would like to investigate its Pontryagin dual. For positive n, the dual group will be the set of homomorphisms from $\hat{\mathbb{Z}}_n$ to the circle group $\mathbb{T}$. Let us first consider a few fixed values of n. For $n = 1$, with the only such homomorphism is the trivial homomorphism, $\chi(0) = 1$. For $n = 2$, we have two homomorphisms: the trivial homomorphism and the homomorphism mapping $\chi(0) = 1$, $\chi(1) = -1$. Finally, for $n = 3$, we have three homomorphisms: the trivial homomorphism and two homomorphisms that map the elements of $\mathbb{Z}_3$ to the third roots of unity, where these two maps differ by orientation. In fact, we can continue in this way for $n > 3$ as well; for each element $z \in \mathbb{Z}_n = \{0, 1, \dots, n-1\}$, we may associate with it a unique homomorphism $\chi \in \hat{\mathbb{Z}}_n$ such that $\chi(1) = \exp(2\pi i z/n)$, when $\mathbb{T}$ is parametrized by the complex plane. Thus we obtain the rather bizarre result that $\hat{\mathbb{Z}}_n$ is actually isomorphic to $\mathbb{Z}_n$, for all $n > 0$! Note that the binary operation here becomes pointwise function multiplication; that is, we define $(\chi_1 \cdot \chi_2)(z) \coloneqq \chi_1(z)\chi_2(z)$.

The impact of this result is that, by theorem 13.5, the group C^*-algebra $C^*(\mathbb{Z}_n)$ is isomorphic to $\mathcal{C}(\mathbb{Z}_n)$, for positive n. Moreover, because every finite Abelian group is isomorphic to a direct sum of cyclic groups of prime power order, this result generalizes to a rather nice categorization of the universal C^*-algebras for all finite Abelian groups!

14. The Free Group on Two Generators

Definition 14.1 – Free Group.
The **free group** with **free generating set** S, denoted F_S, is the group consisting of all words in S. A **word** in S is defined to be any finite product of elements of S, where the equality of two words follows strictly from the group axioms. The identity element e corresponds to the empty word with no symbols. A group G is said to be **free** if it is isomorphic to F_S, for some $S \subseteq G$.

Remarks: We will mainly be looking at the **free group on two generators**, sometimes also referred to as the **free group of rank 2**. This is simply the free group F_2, with generating set $\{a, b\}$. Elements of this group are just finite products of a, a^{-1}, b, b^{-1}: as an example, $ba^3b^{-2}a$ is one such element. Equality follows from the group axioms and nothing more, so for instance $a^2 = abb^{-1}a$. Observe that this is certainly compatible with the identity element given by the empty word.

Lemma 14.2 – Universal Property of Free Groups.
Let G be a group and F_S the group that is freely generated by S. Then for any function $\varphi : S \to G$, there exists a unique group homomorphism $\overline{\varphi} : F_S \to G$ such that $\overline{\varphi}|_S = \varphi$.

Proof. Suppose we have some function $\varphi : S \to G$, and any word $w = s_0^{k_0} \cdots s_n^{k_n}$ in F_S, where $s_i \in S$ and $k_i \in \{-1, 1\}$ for all $0 \le i \le n$. We define an extended map $\overline{\varphi} : F_S \to G$ by

$$\overline{\varphi}(w) = \overline{\varphi}(s_0^{k_0} \cdots s_n^{k_n}) \coloneqq \varphi(s_0)^{k_0} \cdots \varphi(s_n)^{k_n}.$$

This map is certainly a well-defined homomorphism by construction, and furthermore it is unique. This completes the proof. ■

Theorem 14.3 – Free Group Characterization of Unital C^*-Algebras.
Let A be a unital C^*-algebra containing the unitary elements $u, v \in A$. Then there exists a unique unital $*$-homomorphism $\rho : C^*(F_2) \to A$, with $\rho(a) = u$ and $\rho(b) = v$. Furthermore, for all $n \ge 1$, there also exists a surjective $*$-homomorphism of the form $\rho : C^*(F_2) \to M_n(\mathbb{C})$.

Proof. We will begin by finding a unique unital $*$-homomorphism $\rho : C^*(F_2) \to A$. Suppose we let $\pi : A \to \mathcal{B}(H)$ be a faithful, unital representation of A. Then it follows that the images of the unitary elements u and v under π are also unitary; that is, $\pi(u), \pi(v) \in \mathcal{U}(H)$. Hence there is a unitary representation $\alpha : F_2 \to \mathcal{U}(H)$ mapping a to $\pi(u)$ and b to $\pi(v)$. Furthermore, this extends to a unital $*$-representation of $\mathbb{C}F_2$ by the universal property, and then naturally to a unital $*$-representation of $C^*(F_2)$. Denote this extension of α to $C^*(F_2)$ by $\beta : C^*(F_2) \to \mathcal{B}(H)$. Note that $\beta[C^*(F_2)] \subseteq \pi[A]$, as $\beta[C^*(F_2)]$ lies in the closure of the *-algebra generated by $\pi(u)$ and $\pi(v)$. Thus the unique unital $*$-homomorphism proposed by the theorem is $\rho \coloneqq \pi^{-1} \circ \beta$. The second map is defined by

$$\rho(u) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & e^{2\pi i/n} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{2\pi i(n-1)/n} \end{pmatrix}, \quad \rho(v) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix};$$

the smallest C^*-algebra containing both of these is $M_n(\mathbb{C})$. This completes the proof. ■

Theorem 14.4 – Trivial Trace on Reduced Group C^*-Algebra is Faithful.
Let G be a discrete group, with $\tau : C_r^*(G) \to \mathbb{C}$ the trace from theorem 12.10. Then τ is faithful.

Proof. Suppose we identify $C_r^*(G)$ with the image of $\mathbb{C}G$ under π_λ; then we can identify c such that $\tau(c^*c)$ with some corresponding operator on $\ell^2(G)$. Thus, for any $g \in G$, we may write

$$\begin{aligned}
\|c\delta_g\|_2^2 &= \langle c\delta_g, c\delta_g \rangle, \\
&= \langle c\lambda_g\delta_e, c\lambda_g\delta_e \rangle, \\
&= \langle \lambda_g^* c^* c \lambda_g \delta_e, \delta_e \rangle, \\
&= \tau(\lambda_g^* c^* c \lambda_g), \\
&= \tau(\lambda_g^* \lambda_g c^* c), \\
&= \tau(c^* c), \\
&= 0.
\end{aligned}$$

But $\{\delta_g\}_{g\in G}$ forms a basis for $\ell^2(G)$, and so this c must map all of $\ell^2(G)$ to zero. Hence $\tau(c^*c) = 0$ implies that c is the zero operator, as desired. This completes the proof. ■

Theorem 14.5 – $C_r^*(F_2)$ is Simple.
The reduced group C^*-algebra $C_r^*(F_2)$ is simple; that is, it has no non-trivial ideals. In particular, it has no finite-dimensional representations.

Proof – omitted.

Theorem 14.6 – $C_r^*(F_2)$ Admits a Unique Trace.
The reduced group C^*-algebra $C_r^*(F_2)$ admits a unique trace.

Proof – omitted.

Theorem 14.7 – Ping-Pong Lemma.
Let G be a group generated by elements α and β, and let $(X, \cdot)$ be a G-set. Furthermore, suppose there exist non-empty, disjoint subsets $A, B \subset X$, such that

$$\alpha^n \cdot B \subset A \qquad \text{and} \qquad \beta^n \cdot A \subset B, \tag{14.7.1}$$

for all $n \in \mathbb{Z}\backslash\{0\}$. Then G is a free group on two generators; that is, $G \cong F_2$.

Proof. Let a and b be the generators of the free group F_2. We wish to find an isomorphism between F_2 and G mapping $\{a, b\}$ to $\{\alpha, \beta\}$. By the universal property of the free group, we know that a map $\varphi : F_2 \to G$ preserving the group generators exists. Furthermore, because G is generated by $\{\alpha, \beta\}$, this map is certainly surjective. We need only show that it is injective, and we will be done.

In order to show that φ is injective, we will proceed by contradiction. Assume to this end that φ is *not* injective; then there must be some non-identity word $w \in F_S \backslash \{e\}$ with $\varphi(w) = \varepsilon$, where ε is the identity element of G. Suppose we write $w = a^{n_0} b^{m_1} a^{n_1} \cdots b^{m_k} a^{n_k}$, where we allow $n_0, n_k \in \mathbb{Z}$ but require $n_1, \ldots, n_{k-1}, m_1, \ldots, m_k \in \mathbb{Z} \backslash \{0\}$. Then letting $r \in \mathbb{Z} \backslash \{0, -n_0, n_k\}$, we can write

$$\begin{aligned} B = \varepsilon \cdot B = \varphi(a^r)\varepsilon\varphi(a^{-r}) \cdot B &= \varphi(a^r w a^{-r}) \cdot B, \\ &= \alpha^{n_0+r}\beta^{m_1}\alpha^{n_1} \cdots \alpha^{n_{k-1}}\beta^{m_k}\alpha^{n_k-r} \cdot B, \\ &\subset \alpha^{n_0+r}\beta^{m_1}\alpha^{n_1} \cdots \alpha^{n_{k-1}}\beta^{m_k} \cdot A, \\ &\subset \alpha^{n_0+r}\beta^{m_1}\alpha^{n_1} \cdots \alpha^{n_{k-1}} \cdot B, \\ &\subset \cdots, \\ &\subset \alpha^{n_0+r} \cdot B, \\ &\subset A. \end{aligned}$$

This is a contradiction, as we have $B \not\subset A$ by hypothesis. The reason for choosing r as above is so that α^{n_0+r} and α^{n_k-r} do not reduce to trivial powers of α (that is, identity); the latter ensures that we can make the first jump from B to A, while the former ensures that we will eventually land in A. This is actually where the lemma gets its name, as this process of jumping between A and B mimics a game of table tennis! Thus φ is an isomorphism, and hence $G \cong F_2$. This completes the proof. ■

15. Introduction to Amenability

Definition 15.1 – Mean on a Group.
A **mean** on a group G is a **finitely additive measure** on the space $\ell^\infty(G)$ of ℓ^∞-bounded functionals on G; that is, a linear functional $m : \ell^\infty(G) \to \mathbb{C}$ satisfying the following properties:

(15.1.1). $m(\chi_G) = 1$ (normalization);

(15.1.2). $m(f) \geq 0$, for all $f \in \ell^\infty(G)$ that satisfy $f(g) \geq 0$ for all $g \in G$ (non-negativity).

Suppose we now define a group action on $\ell^\infty(G)$ by left translation; that is, $g \cdot f$ is the map taking $x \in G$ to $f(g^{-1}x)$, for all $g \in G$ and $f \in \ell^\infty(G)$. A mean is said to be **left-invariant** if it further satisfies

(15.1.3). $m(g \cdot f) = m(f)$, for all $g \in G$ and $f \in \ell^\infty(G)$ (left-invariance).

We define **right-invariance** similarly. Because left-invariance and right-invariance are equivalent conditions, we say more generally that a mean satisfying either property is ***G*-invariant**.

Remarks: Non-negativity here uses the standard definition for complex-valued functionals; that is, a complex-valed functional f is said to be non-negative at x in its domain if $f(x) \in \mathbb{R}_{\geq 0}$. Furthermore, note that we actually have $g \cdot f := \lambda_g(f)$, where λ is the left regular representation on $\ell^\infty(G)$.

Definition 15.2 – Amenable Group.
A group G is said to be **amenable** if there exists a ***G*-invariant mean**.

Theorem 15.3 – Amenability of Finite Groups.
If G is a finite group, then it is amenable.

Proof. It is easy to verify that the averaging operator defined by

$$f \mapsto \frac{1}{|G|} \sum_{g \in G} f(g),$$

for all $f \in \ell^\infty(G)$, is a G-invariant mean on $\ell^\infty(G)$. ■

Theorem-Definition 15.4 – Fixed Point Property.
A group G is said to satisfy the **fixed point property** if any continuous, affine action of G on a non-empty, compact, convex subset X of a locally convex topological vector space has a fixed point. Moreover, a group is amenable if and only if it satisfies this property.

Proof. We will only prove one direction, as the proof of the converse is quite involved and the result will not be particularly useful to us. Assume that G satisfies the fixed point property, and denote by $\mathcal{L}$ the topological dual space of $\ell^\infty(G)$ with respect to the weak*-topology. Consider the set $\mathcal{M}(G)$ of all means on $\ell^\infty(G)$; this set is certainly non-empty, as the identity evaluation $f \mapsto f(e)$ is a mean on $\ell^\infty(G)$. Furthermore, because it is a weak*-closed subset of $\mathcal{L}$, by the Banach-Alaoglu theorem it is a compact, convex subset of the unit ball in $\mathcal{L}$. Thus by hypothesis, the continuous, affine action $m \mapsto g \cdot m$ of G on $\mathcal{M}(G)$, given by $[g \cdot m](f) = m(\lambda_g(f))$ for all $g \in G$ and $f \in \ell^\infty(G)$, has a fixed point. This fixed point is precisely our left-invariant mean on G. ■

Theorem 15.5 – Markov-Kakutani Fixed Point Theorem.
Let G be an Abelian group. Then any continuous, affine action of G on a non-empty, compact, convex subset X of a locally convex topological vector space V has a fixed point. In other words, G satisfies the fixed point property, and is hence amenable.

Proof. Suppose we define a map $A_n(g) : X \to X$ by

$$[A_n(g)](x) = \frac{1}{n+1} \sum_{i=0}^{n} g^i \cdot x,$$

for $n \in \mathbb{N}$ and $g \in G$. Then $A_n(g)$ is a continuous, affine transformation of X. Let $\mathcal{A}$ denote the Abelian semigroup of continuous, affine transformations of X generated by $\{A_n(g) : n \in \mathbb{N}, g \in G\}$. Because X is compact, it follows that $\alpha(X)$ is a closed subset of X, for all $\alpha \in \mathcal{A}$. We would first like to show that the set

$$\bigcap_{\alpha \in \mathcal{A}} \alpha(X)$$

is non-empty. Because X is compact, it is covered by finitely many sets of the form $\alpha_i(X)$. It is therefore sufficient to show that $\alpha_1(X) \cap \cdots \cap \alpha_m(X)$ is non-empty for any $\alpha_1, \ldots, \alpha_m \in \mathcal{A}$. Suppose we let $\alpha = \alpha_1 \circ \cdots \circ \alpha_m \in \mathcal{A}$. Because $\mathcal{A}$ is Abelian, $\alpha(X) \subset \alpha_i(X)$ for each $1 \leq i \leq m$. Hence $\alpha(X) \subseteq \alpha_1(X) \cap \cdots \cap \alpha_m(X)$ and is this non-empty. Our final claim is that this intersection is a fixed point set for G; that is, for any

$$x_0 \in \bigcap_{\alpha \in \mathcal{A}} \alpha(X),$$

we have that $g \cdot x_0 = x_0$ under any continuous, affine group action. Well, we know that for every $n \geq 0$ and $g \in G$, there exists an $x \in X$ such that $x_0 = [A_n(g)](x)$. Thus for every $\varphi \in V^*$ and $g \in G$, we have the inequality

$$\begin{aligned} |\varphi(x_0 - g \cdot x_0)| &= |\varphi([A_n(g)](x) - g \cdot [A_n(g)](x))|, \\ &= \frac{1}{n+1} \big|\varphi(x) - \varphi(g^{n+1} \cdot x)\big|, \\ &\leq \frac{2}{n+1} \sup\{|\varphi(y)| : y \in X\}, \end{aligned}$$

where this supremum exists due to the compactness of X. Because this inequality must hold for all $n \in \mathbb{N}$, it follows that $\varphi(x_0) = \varphi(g \cdot x_0)$, for every $\varphi \in V^*$, and so $x_0 = g \cdot x_0$ for all $g \in G$ as required. This completes the proof. ∎

Theorem 15.6 – Non-Amenability of Free Groups.
The free group on two generators, F_2, is not amenable.

Proof. To show this, we will proceed by contradiction. Suppose that F_2 is amenable, with some invariant mean m. Furthermore, let $\{a, b\}$ be a generating set for F_2, and consider a set $A \subset F_2$ consisting of words that start with a non-trivial power of a. It is straightforward to observe that

$$A \cup (a^{-1}A) = F_2.$$

Writing $\chi_{F_2} = \chi_A + \chi_{a^{-1}A}$, where χ denotes the indicator function, it follows from linearity that

$$\begin{aligned} 1 = m(\chi_{F_2}) \leq m(\chi_{A \cup a^{-1}A}) &= m(\chi_A + \chi_{a^{-1}A}), \\ &= m(\chi_A) + m(\chi_{a^{-1}A}), \\ &= m(\chi_A) + m(\lambda_a(\chi_A)), \\ &= 2m(\chi_A); \end{aligned}$$

hence $m(\chi_A) \geq 1/2$. However, suppose we instead consider the disjoint sets A, bA and b^2A; then

$$\begin{aligned} 1 = m(\chi_{F_2}) \geq m(\chi_{A \cup bA \cup b^2A}) &= m(\chi_A + \chi_{bA} + \chi_{b^2A}), \\ &= m(\chi_A) + m(\chi_{bA}) + m(\chi_{b^2A}), \\ &= m(\chi_A) + m(\lambda_b(\chi_A)) + m(\lambda_{b^2}(\chi_A)), \\ &= 3m(\chi_A). \end{aligned}$$

But this contradicts the previous result; thus F_2 cannot be amenable. This completes the proof. ■

Proposition 15.7 – Inheritance Properties of Amenable Groups.

(15.7.1). Subgroups of amenable groups are amenable.
(15.7.2). Homomorphic images of amenable groups are amenable.
(15.7.3). Let G, N and Q be groups, with G an extension of Q by N. Then G is amenable if and only if both N and Q are amenable.
(15.7.4). Let $(G_i)_{i \in I}$ be a directed set of amenable subgroups of a group G, such that $G_i \subseteq G_j$ for $i \leq j$ and $G = \bigcup_{i \in I} G_i$. Then G is amenable.

Proof. (15.7.1). Let G be an amenable group with a left-invariant mean m, and let $H \subset G$ be a subgroup. Furthermore, let $R \subset G$ be a set of representatives for $H \backslash G$, the quotient group consisting of right cosets of H in G. That is, choose R such that for every element $Hg \in H \backslash G$, there is exactly one $r \in R$ such that $Hr = Hg$. Finally, let $s : G \to H$ be the map with $g \in s(g)R$, for all $g \in G$. This map certainly exists, as $\{Hr\}_{r \in R} = \{Hg\}_{g \in G}$ covers G. Then the map $\widetilde{m} : \ell^\infty(H) \to \mathbb{C}$, defined by $\widetilde{m}(f) := m(f \circ s)$, is a left-invariant mean on H.

(15.7.2). Let G be an amenable group with a left-invariant mean m, and let $\pi : G \to Q$ be a surjective group homomorphism. Then $f \mapsto m(f \circ \pi)$ is a left-invariant mean on Q.

(15.7.3). By definition, G is an extension of Q by N if there exists a short exact sequence of the form

$$\{e\} \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} Q \longrightarrow \{e\}.$$

That is, there exists a sequence of groups and group homomorphisms as above, where ι is injective and π is surjective, and where the image of each homomorphism is equal to the kernel of the next in the sequence. Suppose first that G is amenable; then it is clear from (15.7.2) that Q must also be amenable. Furthermore, by **Cayley's theorem**, N is isomorphic to a subgroup of G, and is hence amenable by both (15.7.1) and (15.7.2). Suppose conversely that both N and Q are amenable, with left-invariant means m_N and m_Q, respectively. Suppose conversely that both N and Q are amenable, with left-invariant means m_N and m_Q, respectively. Without loss of generality, we may assume $N \subset G$ and $Q = G/N$, where the latter follows from the **first isomorphism theorem**. Then $f \mapsto m_Q(g \cdot N \mapsto m_N(n \mapsto f(g \cdot n)))$ is a well-defined, left-invariant mean on G.

(15.7.4). For each $i \in I$, let m_i be a left-invariant mean on G_i. Furthermore, suppose we consider the maps $\widetilde{m}_i : \ell^\infty(G) \to \mathbb{C}$ of the form $f \mapsto m_i(f|_{G_i})$. By the Banach-Alaoglu theorem, there is a subnet of $(\widetilde{m}_i)_{i \in I}$ that converges to a functional $m : \ell^\infty(G) \to \mathbb{C}$. In fact, this limit is a left-invariant mean on G as desired. ■

Corollary 15.8 – Amenability of Locally Amenable Groups.
A group G is amenable if and only if all finitely-generated subgroups of G are amenable.

Proof. One direction is obvious from (15.7.1), so suppose that all finitely-generated subgroups of G are amenable. Because the finitely-generated subgroups of G form an ascending, directed system of subgroups that cover G, the result follows from (15.7.4). This completes the proof. ■

Corollary 15.9 – Amenability of Solvable Groups.
A group is said to be **solvable** if it can be constructed from extensions of Abelian groups. If G is a solvable group, then it is amenable.

Proof. We know from Markov-Kakutani that Abelian groups are amenable. Hence, given a series of extensions of Abelian groups, we can perform induction with respect to (15.7.3) to obtain the result. This completes the proof. ■

Corollary 15.10 – Non-Amenability of Groups with Free Subgroups.
If G is a group containing a free subgroup on two generators, then it is not amenable.

Remarks: Note that the converse to this theorem does not hold. This converse was known as the **von Neumann conjecture**; it was disproven as recently as 1980 by Olshansky, who constructed the Tarski monster groups as a counterexample.

Proof. The result follows trivially from the combination of theorem 15.6 with (15.7.1). ■

16. The Braid Groups

Definition 16.1 – Homotopy.
Let X and Y be topological spaces, and consider two continuous maps $f, g : X \to Y$. These maps are said to be **homotopic** if there exists a continuous function $H : X \times [0,1] \to Y$ such that $H(x,0) = f(x)$ and $H(x,1) = g(x)$. Such a function is referred to as a **homotopy** from f to g.

Definition 16.2 – Braid on n Strands.
Let $n \in \mathbb{Z}_+$, and fix n distinct points $p_1, \dots, p_n \in \mathbb{R}^2$. We define a **braid on n strands** to be an n-tuple $(f_1, \dots, f_n)$ of continuous maps of the form $f_i : [0,1] \to \mathbb{R}^2$, satisfying $f_i(0) = p_i$ and $f_i(1) = p_{s(i)}$ for some permutation $s : \{1, \dots, n\} \to \{1, \dots, n\}$, as well as $f_i(t) \neq f_j(t)$ for all $i \neq j$. Two such braids on n strands $(f_1, \dots, f_n)$ and $(g_1, \dots, g_n)$ are said to be **equivalent** if f_i is homotopic to g_i, for each $i \in \{1, \dots, n\}$. It is easy to see that this defines an equivalence relation on braids.

Theorem-Definition 16.3 – Braid Group on n Strands.
Let $f := (f_1, \dots, f_n)$ and $g := (g_1, \dots, g_n)$ be two n-strand braids, where f has the associated permutation s_f. Defining a concatenating product on braids by

$$(f \cdot g)_i(t) := \begin{cases} f_i(2t), & t \in [0, 1/2]; \\ g_{s_f(i)}(2t-1), & t \in [1/2, 1], \end{cases} \tag{16.3.1}$$

we can make the set of equivalence classes of braids into a group. This group is referred to as the **braid group on n strands**, and denoted B_n.

Proof. Fix n distinct points $p_1, \dots, p_n \in \mathbb{R}^2$. Consider three braids on n strands $f, g, h \in B_n$, with associated permutations s_f, s_g and s_h, respectively. We see that

$$((f \cdot g) \cdot h)_i(t) := \begin{cases} f_i(4t), & t \in [0, 1/4]; \\ g_{s_f(i)}(4t-1), & t \in [1/4, 1/2]; \\ h_{s_g(s_f(i))}(2t-1), & t \in [1/2, 1]; \end{cases}$$

$$(f \cdot (g \cdot h))_i(t) := \begin{cases} f_i(2t), & t \in [0, 1/2]; \\ g_{s_f(i)}(4t-2), & t \in [1/2, 3/4]; \\ h_{s_g(s_f(i))}(4t-3), & t \in [3/4, 1], \end{cases}$$

whence it is clear that $((f \cdot g) \cdot h)$ is equivalent to $(f \cdot (g \cdot h))$, and so associativity is satisfied. The identity braid is simply the braid $e := (e_1, \dots, e_n)$ where we define $e_i(t) := p_i$, for all $t \in [0,1]$. Finally, we can construct an inverse to each $f \in B_n$ by taking $f^{-1}(t) := f(1-t)$. This completes the proof. ■

Proposition 16.4 – Abstract Characterization of Braid Groups.
The braid group on n strands admits the presentation

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} \mid \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, \sigma_i\sigma_j = \sigma_j\sigma_i \rangle, \tag{16.4.1}$$

where the first relation must hold for all $|i-j| = 1$, while the second must hold for all $|i-j| > 1$.

Proof – omitted. The formal proofs for this result are typically rather long and involved. Rather than replicate one of many such well-documented proofs [8], we will focus on conveying an intuitive understanding. We can identify each so-called **Artin generator** $\sigma_i := (\sigma_{i,1}, \ldots, \sigma_{i,n}) \in B_n$ with the braid given by $\sigma_{i,i}(t) := p_i + t(p_{i+1} - p_i)$ and $\sigma_{i,i+1}(t) := p_{i+1} + t(p_i - p_{i+1})$, where $\sigma_{i,j}(t) := e_j$ for all remaining strands. By drawing these as typical braid diagrams, it is easy to observe that they form a generating set for B_n, and furthermore satisfy the properties of (16.4.1).

Theorem 16.5 – Non-Amenability of Braid Groups.
The braid group on n strands is amenable if $n \in \{1, 2\}$, and non-amenable otherwise.

Proof. By proposition 16.4, we know that $B_1 \cong \{e\}$ and $B_2 \cong F_1 \cong \mathbb{Z}$, which are both amenable by theorem 15.3 and theorem 15.5, respectively. Observe now that B_n is a proper subgroup of B_{n+1}, for all $n \in \mathbb{Z}_+$; thus if we are able to show that B_3 is not amenable, any higher order braid groups must also not be amenable by the first result of proposition 15.7. Well, let G be the subgroup of B_3 generated by σ_1^2 and σ_2^2, and consider the group homomorphism $\varphi : B_3 \to M_n(\mathbb{R})$ defined by

$$\varphi(\sigma_1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \varphi(\sigma_2) = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Note that $\varphi(\sigma_1)$ and $\varphi(\sigma_2)$ both, as matrices, satisfy the relation demanded by (16.4.1). We can therefore define a group action of G on $\mathbb{R}^2$ by $f \cdot v := \varphi(f)v$. Suppose we now define two subsets $A, B \subset \mathbb{R}^2$ as follows:

$$A := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 : |x| > |y| \right\}, \quad B := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 : |x| < |y| \right\}.$$

Given $v = (x, y)^T \in B$, we see that

$$\sigma_1^{2n} \cdot v = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2ny \\ y \end{pmatrix}.$$

But it follows from the definition of B that

$$|x + 2ny| \geq |2ny| - |x| > 2|y| - |y| = |y|,$$

hence $\sigma_1^{2n} \cdot B \subset A$. A similar process yields $\sigma_2^{2n} \cdot A \subset B$. Thus $G \cong F_2$ by the ping-pong lemma, whence the result follows from proposition 15.7. This completes the proof. ■

17. Reiter's Characterization of Amenability

Definition 17.1 – Reiter's Property (P_p).
Let G be a discrete group, and $\ell^p(G)_{1,+} := \{s \in \ell^p(G) : s \geq 0, \|s\|_p = 1\}$, for $p \in [1,\infty)$. Then G is said to satisfy **Reiter's property (P_p)** if, for every compact (or, equivalently, every finite) subset $Q \subset G$ and all $\varepsilon > 0$, there exists some $s \in \ell^p(G)_{1,+}$ such that

$$\|\lambda_q(s) - s\|_p < \varepsilon, \tag{17.1.1}$$

for all $q \in Q$, where λ is the left regular representation on $\ell^p(G)$.

Remarks: Recall that subsets of discrete topological spaces are compact if and only if they are finite. This is essentially why we are able to characterize this property using either compact or finite subsets.

Theorem 17.2 – Equivalence of Reiter's Properties.
Reiter's property (P_p) is equivalent to (P_1), for all $p > 1$.

Proof. We shall first show that (P_1) implies (P_p). Let $s_1 \in \ell^1(G)_{1,+}$ such that (P_1) holds, and set $s_p := s_1^{1/p}$. Then $s_p \in \ell^p(G)$; furthermore, because $|a-b|^p \leq |a^p - b^p|$ for all $a, b \geq 0$ and $p \geq 1$,

$$\begin{aligned}
\|\lambda_q(s_p) - s_p\|_p &= \left(\sum_{g\in G} |[\lambda_q(s_p)](g) - s_p(g)|^p\right)^{1/p} \leq \left(\sum_{g\in G} [|\lambda_q(s_p)](g)^p - s_p(g)^p|\right)^{1/p}, \\
&= \left(\sum_{g\in G} |[\lambda_q(s_1)](g) - s_1(g)|\right)^{1/p} = \left(\|\lambda_q(s_1) - s_1\|_1\right)^{1/p} < \varepsilon^{1/p},
\end{aligned}$$

for all compact $Q \subset G$, $q \in Q$ and $\varepsilon > 0$. Hence we have that (P_1) $\implies$ (P_p). Conversely, suppose that $s_p \in \ell^p(G)_{1,+}$ satisfies (P_p) and set $s_1 := s_p^p \in \ell^1(G)_{1,+}$. Because $|a^p - b^p| \leq p|a-b|(a^{p-1} + b^{p-1})$ for all $a, b \geq 0$ and $p \geq 1$, we have

$$\begin{aligned}
\|[\lambda_q(s_1)](g) - s_1(g)\|_1 &= \sum_{g\in G} |[\lambda_q(s_1)](g) - s_1|(g) = \sum_{g\in G} |[\lambda_q(s_p)](g)^p - s_p(g)^p|, \\
&\leq \sum_{g\in G} p|[\lambda_q(s_p)](g) - s_p(g)|([\lambda_q(s_p)](g)^{p-1} + s_p(g)^{p-1}), \\
&\leq p\left\|(\lambda_q(s_p) - s_p)(\lambda_q(s_p)^{p-1} + s_p^{p-1})\right\|_1.
\end{aligned}$$

Suppose we now choose p' such that $1/p + 1/p' = 1$; then by Hölder's inequality and the fact that $s_p^{p-1} \in \ell^{p'}(G)$ (giving it unit norm), it follows that

$$\begin{aligned}
p\left\|(\lambda_q(s_p) - s_p)(\lambda_q(s_p)^{p-1} + s_p^{p-1})\right\|_1 &\leq p\|\lambda_q(s_p) - s_p\|_p \left(\left\|\lambda_q(s_p)^{p-1}\right\|_{p'} + \left\|s_p^{p-1}\right\|_{p'}\right), \\
&\leq 2p\|\lambda_q(s_p) - s_p\|_p < 2p\varepsilon,
\end{aligned}$$

for all compact $Q \subset G$, $q \in Q$ and $\varepsilon > 0$. This completes the proof. ■

Theorem 17.3 – Amenability via Reiter's Property.
A discrete group G is amenable if and only if it satisfies Reiter's property.

Proof – omitted. A proof can be found in appendix G of *Kazhdan's Property (T)* [5].

Definition 17.4 – Weak Containment.
Let G be a group with two unitary representations $u : G \to \mathcal{U}(H)$ and $v : G \to \mathcal{U}(K)$. The representation u is said to be **weakly contained** in v, denoted $u \prec v$, if for every $\xi \in H$, every compact $Q \subset G$ and all $\varepsilon > 0$, there exists $n \in \mathbb{Z}_+$ and $\eta_1, \dots, \eta_n \in K$ such that

$$\left| \langle \xi, u_g(\xi) \rangle - \sum_{i=1}^{n} \langle \eta_i, v_g(\eta_i) \rangle \right| < \varepsilon, \tag{17.4.1}$$

for all $g \in Q$. This definition extends to the non-degenerate representations of the group C^*-algebra in the natural way.

Theorem 17.5 – Properties of Weak Containment.
Let G be a discrete group with unitary representations u and v, corresponding to the non-degenerate $*$-representations π_u and π_v of $C^*(G)$. Then the following conditions are equivalent:

(17.5.1). $u \prec v$;
(17.5.2). $\ker(\pi_u) \subset \ker(\pi_v)$;
(17.5.3). $\|\pi_u(a)\| \leq \|\pi_v(a)\|$, for all $a \in C^*(G)$.

Proof – omitted. A proof can be found in *On simplicity of reduced C^*-algebras of groups* [6].

Theorem 17.6 – Hulanicki-Reiter Theorem.
Let G be a discrete group and λ its left regular representation on $\ell^2(G)$. Then the following conditions are equivalent:

(17.6.1). G is amenable;
(17.6.2). $1_G \prec \lambda$;
(17.6.3). $u \prec \lambda$, for every unitary representation u of G.

Proof – omitted. A proof can be found in appendices F and G of *Kazhdan's Property (T)* [5].

Corollary 17.7 – Amenability and C^*-Algebras.
Let G be a discrete group. Then G is amenable if and only if $C^*(G) \cong C_r^*(G)$.

Proof. Suppose first that G is amenable. Then by Hulanicki-Reiter, every unitary representation u is weakly contained in λ. Thus every non-degenerate $*$-representation π_u is weakly contained in π_λ by theorem 12.4, and so (17.5.3) implies that $C^*(G) \cong C_r^*(G)$. Conversely, suppose $C^*(G) \cong C_r^*(G)$. Then $\|\pi_u(a)\| \leq \|\pi_\lambda(a)\|$ for every non-degenerate $*$-representation π_u of $C^*(G)$ and hence $u \prec \lambda$ for every unitary representation u by theorem 17.5, whence the result follows. This completes the proof. ■

18. Følner's Characterization of Amenability

Definition 18.1 – Uniform Discreteness.
A metric space (X, d) is said to be **uniformly discrete** if $\inf\{d(x, x') : x, x' \in X, x \neq x'\} > 0$.

Definition 18.2 – Bounded Geometry.
A metric space (X, d) is said to be of **bounded geometry** if, for all $r \in \mathbb{R}_+$, there exists some $K_r \in \mathbb{N}$ such that $|B(x, r)| \leq K_r$, for all $x \in X$. That is, every ball in (X, d) of radius r contains no more than K_r points.

Definition 18.3 – Følner Sequence.
Let (X, d) be a **UDBG space**; that is, a metric space that is uniformly discrete and of bounded geometry. If $F \subset X$ and $r \in \mathbb{N}$, we define the ***r*-boundary** of F in X by

$$\delta_r^X F := \{x \in X \backslash F : d(x, f) \leq r, \text{ for some } f \in F\}. \tag{18.3.1}$$

A **Følner sequence** for X is then a sequence $(F_n)_{n \in \mathbb{N}}$ of compact (finite) subsets of X satisfying

$$\lim_{n \to \infty} \frac{\left|\delta_r^X F_n\right|}{|F_n|} = 0, \tag{18.3.2}$$

for all $r \in \mathbb{N}$. These subsets are sometimes referred to as **Følner sets**.

Remarks: Note that the r-boundary is actually exactly what the name implies, as it gives an "outline" of width r around the space F. The existence of a Følner sequence can thus be thought of as a statement regarding the geometric "efficiency" of the space; the space admits subsets with small boundaries but relatively large volumes.

Proposition 18.4 – Følner's Property.
A UDBG space X admits a Følner sequence if and only if, for every $r \in \mathbb{N}$ and all $\varepsilon > 0$, there exists a compact (finite) subset $F \subset X$ satisfying

$$\frac{\left|\delta_r^X F\right|}{|F|} < \varepsilon. \tag{18.4.1}$$

In this case, it is said to satisfy **Følner's property**.

Proof. It is clear that if X admits a Følner sequence, then the proposed condition must hold by the definition of the limit. Conversely, the condition from our proposition implies that for all $n \in \mathbb{N}$, there exists a non-empty, finite subset $F_n \subset X$ satisfying

$$\frac{\left|\delta_n^X F_n\right|}{|F_n|} \leq \frac{1}{n}.$$

We see from this condition that $(F_n)_{n \in \mathbb{N}}$ is then a Følner sequence for X. This completes the proof. ■

Definition 18.5 – Word Metric.
Let $(G, \circ)$ be a group with finite generating set S, where we take S to be closed under inverses. We define the **word metric** on G with respect to S by

$$d_S(g,h) \coloneqq \min\{n \in \mathbb{N} : \exists x_1, \ldots, x_n \in G \text{ for which } g \circ x_1 \circ \cdots \circ x_n = h\}, \tag{18.5.1}$$

for all $g, h \in G$. That is, $d_S(g,h)$ is the smallest number of elements needed to multiply by g to get h. We refer to $d_S(e,g)$ as the **word length** of $g \in G$ with respect to the finite generating set S.

Remarks: It is not too difficult to see that the word metric is indeed a metric. Furthermore, the metric space (G, d_S) actually happens to be a UDBG space. It is obviously uniformly discrete, and because S is finite it is certainly of bounded geometry as well.

Example 18.6 – Følner Sequences on Integer Spaces.
Let $S \coloneqq \{e_1, \ldots, e_n\}$ be the standard generating set of the group $\mathbb{Z}^n$, for $n \in \mathbb{N}$. Then the set of all balls in $\mathbb{Z}^n$ centered at the origin, $(\{-k, \ldots, k\}^n)_{k\in\mathbb{N}}$, is a Følner sequence for $(\mathbb{Z}^n, d_S)$.

Theorem 18.7 – Amenability via Følner's Property.
A finitely-generated group G is amenable if and only if (G, d_S) satisfies Følner's property.

Remarks: It should be carefully observed that the Følner characterization of amenability, as it is stated here, is only viable for finitely-generated groups. In other words, amenability will only guarantee the existence of a Følner sequence if the group is finitely-generated.

Proof – omitted. A proof can be found in appendix G of *Kazhdan's Property (T)* [5], or alternatively in chapter 9 of *Geometric Group Theory: An Introduction* [7].

Definition 18.8 – Amenability on UDBG Spaces.
A UDBG space is said to be amenable if it admits a Følner sequence.

Definition 18.9 – Growth Rate.
Let X be a UDBG space, and let $x \in X$. Consider the closed ball of radius $n \in \mathbb{N}$ centered at x, $F_n \coloneqq B_X(x,n)$. We can then define a **growth function** of X by $\gamma_X : n \mapsto |B_X(x,n)|$. Moreover, because UDBG spaces have bounded geometry, the growth functions corresponding to any two elements of X will be asymptotically equivalent; hence it makes sense to define the **growth rate** of X to be the asymptotic behaviour of any such growth function γ_X.

Remarks: For a group G with a finite generating set S, the ball $B_G^S(e,n)$ of radius $n \in \mathbb{N}$ is just the set of all elements in G that can be expressed as a product of no more than n generators. We can therefore naturally define a growth function γ_G^S, that describes precisely how the group grows with respect to S. However, we should note that the word length of a particular element will not necessarily be the same with respect to every generating set. As a result, it is sensible to wonder if this growth rate is a good description of a group in general. This leads to the following proposition.

Proposition 18.10 – Bi-Lipschitz Equivalence of Word Metrics.
Let G be a group with finite generating sets S and S'. Then the word metrics d_S and $d_{S'}$ are **bi-Lipschitz equivalent**; that is, there exists some constant $C > 0$ such that

$$\frac{1}{C} d_S(g,h) \leq d_{S'}(g,h) \leq C d_S(g,h), \tag{18.10.1}$$

for any $g, h \in G$. In particular, γ_G^S and $\gamma_G^{S'}$ are asymptotically equivalent, and hence the growth rate of G is independent of the choice of generating set.

Proof. Let $S = \{s_1, \dots, s_m\}$ and $S' = \{s'_1, \dots, s'_n\}$ be finite generating sets for G. Suppose we define, for instance,

$$C_1 \coloneqq \max\{d_{S'}(e, s_i) : 1 \leq i \leq m\},$$

$$C_2 \coloneqq \max\{d_S(e, s'_i) : 1 \leq i \leq n\}.$$

In other words, every generator in S has a representation in S' composed of no more than C_1 elements. Therefore, by simply substituting generators in S with their shortest representations in S', we obtain an upper bound for $d_{S'}(g,h)$; in particular, $d_{S'}(g,h) \leq C_1 d_S(g,h)$. By symmetry, we also obtain $\frac{1}{C_2} d_S(g,h) \leq d_{S'}(g,h)$. Setting $C \coloneqq C_1 + C_2$, the result follows. This completes the proof. ■

Theorem 18.11 – Amenability via Subexponential Growth.
Let X be a UDBG space with **subexponential growth**; that is, $\gamma_X \lesssim (n \mapsto 2^n)$ with $\gamma_X \not\sim (n \mapsto 2^n)$. Furthermore, choose any $x \in X$, and define $F_n \coloneqq B_X(x, n)$. Then $(F_n)_{n \in \mathbb{N}}$ contains a Følner subsequence for X, and is hence amenable.

Proof. Let γ_X be a growth function for X with respect to the element $x \in X$, such that it exhibits subexponential growth. Then there exists, for all $j, K \in \mathbb{N}$ and $\varepsilon > 0$, some $n \geq K$ such that

$$\frac{\gamma_X(n+j)}{\gamma_X(n)} < 1 + \varepsilon.$$

Suppose we set $K = n_{j-1} + 1$ and $\varepsilon = 1/j$. Then by the previous characterization of subexponential growth, it is certainly possible to find a strictly increasing sequence $(n_j)_{j \in \mathbb{N}}$ such that

$$\frac{\gamma_X(n_j + j)}{\gamma_X(n_j)} < 1 + \frac{1}{j}$$

is satisfied for all $j \in \mathbb{N}$. We claim that $(F_{n_j})_{j \in \mathbb{N}}$ is a Følner sequence for X. Let $r \in \mathbb{N}$. Then by definition of the r-boundary, it follows that $\delta_r^X F_n \subset B_X(x, n+r) \backslash B_X(x, n)$ for all $n \in \mathbb{N}$, whence

$$\left|\delta_r^X F_n\right| \leq |B_X(x, n+r) \backslash B_X(x, n)| = \gamma_X(n+r) - \gamma_X(n).$$

Therefore, for all $j \geq r$, we obtain

$$\frac{\left|\delta_r^X F_{n_j}\right|}{\left|F_{n_j}\right|} \leq \frac{\gamma_X(n_j + r) - \gamma_X(n_j)}{\gamma_X(n_j)} = \frac{\gamma_X(n_j + r)}{\gamma_X(n_j)} - 1 \leq \frac{\gamma_X(n_j + j)}{\gamma_X(n_j)} \leq 1 + \frac{1}{j} - 1 = \frac{1}{j}.$$

This clearly tends to 0 as j tends to infinity; hence $(F_{n_j})_{j \in \mathbb{N}}$ is a Følner sequence for X as desired. This completes the proof. ■

19. The Infinite Dihedral Group

Definition 19.1 – Dihedral Group.
The **dihedral group of order n**, denoted D_n, is the group of symmetries of a regular n-gon. That is, it can be realized intuitively as the group of transformations of a regular n-gon generated by the reflection τ about the x-axis and the rotation σ about the origin by $2\pi/n$. More precisely, it is described by the presentation $\langle \sigma, \tau \mid \sigma^n = \tau^2 = (\tau\sigma)^2 = e \rangle$, where e denotes the group identity.

Definition 19.2 – Infinite Dihedral Group.
The **infinite dihedral group**, denoted D_∞, is an infinite group with behaviour analogous to that of the finite dihedral groups. It is described by the presentation $\langle \sigma, \tau \mid \tau^2 = (\tau\sigma)^2 = e \rangle$. Compare this to the finite dihedral groups; by giving σ infinite order, we lose only the condition $\sigma^n = e$.

Remarks: With the geometric intuition behind the finite dihedral groups in mind, it is easy at first to mistakenly associate the infinite dihedral group with the symmetry group of the circle. However, the symmetries on the unit circle are not "discrete" in the way that the symmetries on the dihedral groups are, and so this actually not the right lens to view the infinite dihedral group through. Instead, it is more correct to understand the infinite dihedral group as the symmetry group of the line $\mathbb{Z}$, where reflections are negations of the form $n \mapsto -n$ and rotations are shifts of the form $n \mapsto n+1$.

Proposition 19.3 – C^*-Algebra of Continuous Functions.
Let X be a compact Hausdorff space and A a C^*-algebra. Then $\mathcal{C}(X, A)$, the set of continuous functions from X to A, becomes a C^*-algebra under pointwise operations and the norm defined by
$$\|f\| = \sup\{\|f(x)\| : x \in X\}, \tag{19.3.1}$$
for each $f \in \mathcal{C}(X, A)$. Note that this norm certainly exists, as $f[X] \subseteq A$ is compact for all $f \in \mathcal{C}(X, A)$ and hence so too is $\|f[X]\| \subseteq \mathbb{R}$, whence boundedness follows by Heine-Borel.

Remarks: It turns out that we have a rather nice situation when $A = M_n(\mathbb{C})$. In this case, the space $\mathcal{C}(X, A)$ is actually isomorphic to $M_n(\mathcal{C}(X))$. This is because continuous functions that map to matrices are of course trivially equivalent to matrices of continuous functions.

Proof. Follows from the definitions. See example 4.9 for a very similar proof. ■

Theorem 19.4 – Structure of the Infinite Dihedral Group C^*-Algebra.
Suppose we define a set
$$B_1 \coloneqq \{f \in \mathcal{C}([0,1], M_2(\mathbb{C})) : f(0), f(1) \in \mathbb{D}_1\}, \tag{19.4.1}$$
where $\mathbb{D}_1$ is the subgroup of $M_2(\mathbb{C})$ consisting of linear combinations of matrices with unit diagonals and matrices with unit antidiagonals. Then there exists an isometric $*$-isomorphism of the form $\rho : C^*(D_\infty) \to B_1$, with
$$[\rho(\sigma)](t) = \begin{pmatrix} e^{i\pi t} & 0 \\ 0 & e^{-i\pi t} \end{pmatrix}, \quad [\rho(\tau)](t) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{19.4.2}$$
for $\sigma, \tau \in D_\infty \subset C^*(D_\infty)$ as described in definition 19.2.

Remarks: Surprisingly, this theorem is essentially identifying $C^*(D_\infty)$ with B_1, the set of functions interpolating between matrices in $\mathbb{D}_1$.

Proof. We first observe that $\rho(\sigma), \rho(\tau) \in B_1$, and moreover they together satisfy the same relations as $\sigma, \tau \in D_\infty$ in this new space; that is, $\rho(\tau)^2 = (\rho(\tau)\rho(\sigma))^2 = I$. Thus it follows that we can at least define a $*$-homomorphism ρ from $\mathbb{C}D_\infty$ to B_1 in the natural way, starting from (19.4.2).

Note that a linear isometry between two dense subsets preserves Cauchy sequences, and hence can be extended to a linear isometry between their completions. We shall proceed by showing that $\mathbb{C}D_\infty$, a dense subset of $C^*(D_\infty)$ by theorem 12.5, has a dense image under ρ; afterwards, we will conclude the proof by demonstrating that ρ is indeed an isometry. Well, we see that $\rho(\mathbb{C}D_\infty)$ contains both the identity and $\rho(\sigma^{-1}) = [\rho(\sigma)]^{-1}$. But this means that it contains every element $\rho(\frac{1}{2}\sigma^n + \frac{1}{2}\sigma^{-n}) = \frac{1}{2}([\rho(\sigma)]^n + [\rho(\sigma)]^{-n})$, for any $n \in \mathbb{Z}_+$; that is, all matrices with $\cos(n\pi t)$ along the diagonal. So by Fourier analysis, the closure must contain all matrices of the form

$$\begin{pmatrix} f(t) & 0 \\ 0 & f(t) \end{pmatrix},$$

for continuous $f : [0,1] \to \mathbb{C}$. A similar argument applies to $\rho(\frac{1}{2i}\sigma^n - \frac{1}{2i}\sigma^{-n})$, which gives us matrices with diagonals of the form $(\sin(n\pi t), -\sin(n\pi t))$. Hence the closure contains all matrices of the form

$$\begin{pmatrix} g(t) & 0 \\ 0 & -g(t) \end{pmatrix},$$

for continuous $g : [0,1] \to \mathbb{C}$ with $g(0) = g(1) = 0$. Combining these results, we can say that the closure of $\rho(\mathbb{C}D_\infty)$ contains all matrices of the form

$$\begin{pmatrix} f(t) & 0 \\ 0 & g(t) \end{pmatrix},$$

for continuous $f, g : [0,1] \to \mathbb{C}$ with $f(0) = g(0)$ and $f(1) = g(1)$. Finally, by taking sums with products of $\rho(\tau)$, it is clear that the closure contains all of B_1. Thus $\rho(\mathbb{C}D_\infty)$ is dense in B_1; all that remains is to show that ρ is an isometry (and hence an isomorphism).

Suppose we choose any $t \in [0,1]$. Then the map sending some element $a \in \mathbb{C}D_\infty$ to $[\rho(a)](t)$ is a $*$-homomorphism to $M_2(\mathbb{C})$. Furthermore, it follows that the we may define a $*$-representation $\pi_t : \mathbb{C}D_\infty \to \mathcal{B}(H) : a \mapsto [\rho(a)](t)$, where H is a two-dimensional Hilbert space; for instance, if $H = \mathbb{C}^2$, then we are free to identify $M_2(\mathbb{C}) \cong \mathcal{B}(\mathbb{C}^2)$. From the definition of the universal group C^*-algebra norm (12.5.1), we then have

$$\|a\|_U \geq \sup\{\|\pi_t(a)\| : t \in [0,1]\} = \|\rho(a)\|,$$

for all $a \in \mathbb{C}D_\infty$, where the rightmost norm is of course the operator norm. We would like to show that this is a strict equality. To do this, we will take into consideration the result (12.7.1), and show that every irreducible representation π of D_∞ is unitarily equivalent to the restriction of some π_t to a π_t-invariant subspace $N \subset \mathbb{C}^2$. If we accept this fact, then we can conclude that

$$\|a\|_U = \sup\{\|\pi(a)\| : \pi \text{ irreducible}\} = \sup\{\|\pi_t(a)\| : t \in [0,1]\} = \|\rho(a)\|.$$

We defer the proof of this fact to a following lemma. This completes the proof. ∎

Lemma 19.5 – Supporting Lemma for Theorem 19.4.
Let (π, H) be an irreducible representation of D_∞, and define a map $\pi_t : a \mapsto [\rho(a)](t)$, where ρ is given in theorem 19.4. Then there exists some $t \in [0,1]$ and some π_t-invariant subspace $N \subset \mathbb{C}^2$ such that π is unitarily equivalent to $\pi_t|_N$, the restriction of π_t to N.

Proof – omitted. The proof for this result can be found in Putnam's notes [4].

Lemma 19.6 – Infinite Dihedral Group Growth Rate.
The infinite dihedral group has a linear growth rate.

Proof. Consider the presentation $D_\infty = \langle x, y \mid x^2 = y^2 = e \rangle$ for the infinite dihedral group, where $x = \tau$ and $y = \tau\sigma$ in terms of the generators from the original definition. We claim that $\gamma_G^S(n) = 2n+1$. It is clear that $B_0(D_\infty, S) = \{e\}$ and $B_1(D_\infty, S) = \{x, y, e\}$. To see that this continues to work, we simply note that any x^2 or y^2 term will reduce to identity; hence all minimum-length words must have terms alternating between x and y. There are only two distinct words of length n that satisfy this condition; one beginning with x, and the other beginning with y. The result follows. This completes the proof. ■

Theorem 19.7 – Amenability of the Infinite Dihedral Group.
The infinite dihedral group is amenable.

Proof. This follows directly as a direct result of theorem 18.11, as the infinite dihedral group has a linear (and hence subexponential) growth rate by lemma 19.6. This completes the proof. ■

Remarks: Note that a more fundamental argument exists: rather than using the growth rate, we can observe that the infinite dihedral group is a semidirect product (and hence an extension) of two Abelian groups.


今回はここまで

20. References

[1] Murphy, G. J., *C^*-Algebras and Operator Theory*, Academic Press, 1990.

[2] Davidson, K. R., *C^*-Algebras by Example*, American Mathematical Society, 1996.

[3] Evans, D. E. and Kawahigashi, Y., *Quantum Symmetries on Operator Algebras*, Oxford University Press, 1998.

[4] Putnam, I. F., *Lecture Notes on C^*-algebras*, 2019.

[5] Bekka, B., de la Harpe, P., and Valette, A., *Kazhdan's Property (T)*, Cambridge University Press, 2008.

[6] de la Harpe, P., *On simplicity of reduced C^*-algebras of groups* (2005), 5–6 pp., available at `arXiv:math/0509450`.

[7] Löh, C., *Geometric Group Theory: An Introduction*, Springer, 2017.

[8] González-Meneses, J., *Basic results on braid groups* (2010), pp. 19–26.

[9] Reiter, H. J. and Stegeman, J. D., *Classical Harmonic Analysis and Locally Compact Groups*, Clarendon Press, 2000.

[10] Dixmier, J., *C^*-Algebras*, North-Holland Publishing Company, 1977.