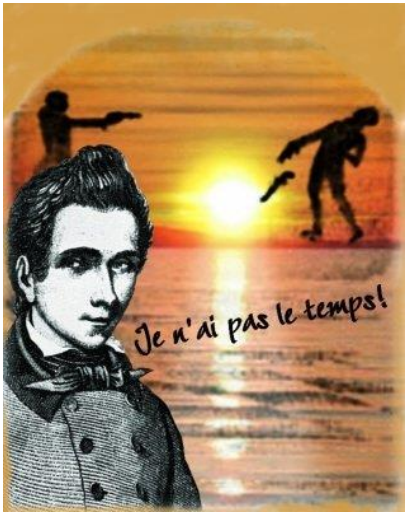
1. BACKGROUND

§1.1. Finite Groups



Before we begin let us review some of the background that is assumed knowledge. We'll be studying the theory of representations of finite groups and so we need a fairly solid background in the theory of finite groups.

Groups were invented by Évariste Galois, a young French mathematician (1811-1832) as a tool for studying the solubility of polynomials by radicals. He was also a political radical and was killed in a duel at the age of 19.

A **group** G is a set together with a binary operation such that:

(1) $ab \in G$ for all $a, b \in G$;
(2) $(ab)c = a(bc)$ for all $a, b, c \in G$;
(3) $1a = a = a1$ for some $1 \in G$;
(4) for all $a \in G$ there exists $a^{-1} \in G$ such that $aa^{-1} = 1 = a^{-1}a$.

G is **abelian** if we also have

(5) $ab = ba$ for all $a, b \in G$.

We shall mostly use ‘multiplicative notation’, as above. If n is a positive integer we define a^n to be the product of n copies of a. We then define $a^{-n} = (a^{-1})^n$ and $a^0 = 1$. The usual index laws hold, with the exception of $(ab)^n = a^n b^n$ which requires commutativity.

The **order** of a finite group G is $|\boldsymbol{G}|$, the number of elements in G. Now the order of a finite group is probably its most important property. Merely knowing how many elements there are can give us a lot of useful information about the group, especially using the prime factorisation of the group order. Elementary number theory is an important tool as many proofs hinge on whether a number associated with a group is prime or whether one such number divides another.

A subset H is a **subgroup** of G (we write $H \leq G$) if H is a group under the same operation. If $H \leq G$ and $x \in G$ then the **right coset** containing x is $\boldsymbol{x}\mathbf{H} = \{xh \mid h \in H\}$ and the **left coset** containing x is $\mathbf{H}\boldsymbol{x} = \{hx \mid h \in H\}$. Of course in abelian groups these are the same thing, and even for a non-abelian group they often are the same.

Any two different right cosets are disjoint, and similarly for left cosets. The right cosets of H are the equivalence classes under the relation $x \sim y$ if $x = yh$ for some $h \in H$. They all have the same size, namely the order of H. Yje subgroup H is itself both a left and a right coset.

So, we have Lagrange’s Theorem, that if $H \leq G$ then $|H|$ divides $|G|$. The other factor, the number of right or left cosets, is called the **index** of H and is written $|\mathbf{G:H}|$.

A subgroup H of G is a **normal subgroup** ($H \trianglelefteq G$) if every left coset is also a right coset, or equivalently, $g^{-1}Hg = H$ for all $g \in G$. Clearly for abelian groups every subgroup is normal, but there are some non-abelian groups with this property.

A group is **simple** if the only normal subgroups are 1 and G. A group of prime order is simple because, by Lagrange's Theorem, 1 and G are the only possible subgroups. Non-abelian simple groups have been extensively studied and have been classified completely.

If K is a normal subgroup of G then the left cosets and the right cosets coincide and we can make these cosets into a group, G/K, by defining $(xK)(yK) = xyK$. In other words, to multiply cosets we simply multiply representatives. This operation is *well-defined*, meaning that the product of two cosets is independent of the representatives. Note that $|G/K| = |G:K| = |G|/|K|$, being the number of cosets of K in G.

The **direct product** of the finite groups $G_1, \ldots, G_k$ is $G_1 \otimes \ldots \otimes G_k$

$= \{(g_1, \ldots, g_k) \mid \text{each } g_i \in G_i\}$ under component-wise multiplication.

§1.2. Homomorphisms and the Isomorphism Theorems

In any theory where we have sets with a certain structure, we consider functions from one set to another that preserves the structure. Depending on the type of

structure these are called linear transformations or continuous functions, or homomorphisms. For groups, rings and fields they're called homomorphisms and they preserve the operations.

At this point we'll mention a notational convention that we'll normally use in these notes when describing functions. Instead of writing $f(x)$ we'll write xf. Apart from using less ink, it makes for a very natural looking definition of the product of two functions. If f:A $\to$ B and g:B $\to$ C are functions the product fg is defined as a map from A to C by defining

$$a(fg) = (af)g \text{ for all } a \in A.$$

This looks like an associative law, but of course a is an element of A and f, g are not. You'll no doubt recognise this as essentially composition of functions, but backwards. With
$f \circ g$ we apply g first and then f while with multiplication fg means apply f first and then g.

We reserve the right to slip back to the $f(x)$ notation when it suits us. Certainly if this was a calculus text we wouldn't be writing "x sin" instead of "sin x"!

A **homomorphism** φ:G $\to$ H is a map where $(ab)\varphi = (a\varphi)(b\varphi)$ for all $a, b \in$ G. It is just as if we were re-coding the elements of G. A rather trivial example of a homomorphism from G to H (in fact it's called the **trivial homomorphism**) is the one where every element maps to the identity of H. Homomorphisms in general give scaled down versions of the original group. If we want the image

to be considered as the same group we must insist that the homomorphism be a 1-1 correspondence.

A homomorphism is an **isomorphism** if it's 1-1 and onto. If there exists an isomorphism from G to H we say that G, H are **isomorphic** and write **G ≅ H**. As I've said, isomorphic groups are considered to be essentially the same group if we are only interested in their structure.

Other special types of homomorphism are defined as follows.

The homomorphism $f : G \to H$ is an **endomorphism** if H = G, an **isomorphism** if it is 1-1 and onto and an **automorphism** if both.

The **kernel** of a homomorphism $\varphi: G \to H$ is **ker φ** = $\{g \in G \mid g\varphi = 1\}$ and

the **image** is **im φ** = $\{g\varphi \mid g \in G\}$. There are three fundamental Isomorphism Theorems. The first is proved directly and the Second and Third are proved from the First by setting up suitable homomorphisms.

First Isomorphism Theorem: If $\varphi: G \to H$ is a homomorphism then: ker φ ◁ G ; im φ ≤ H and G/ker φ ≅ im φ.

Second Isomorphism Theorem: If H ≤ G and K ◁ G and HK = {hk | h ∈ H, k ∈ K} then

HK ≤ G; H ∩ K ◁ H and HK/K ≅ H/(H ∩ K).

Third Isomorphism Theorem: If H ≤ K and H, K ◁ G then H/K ◁ G/K and

$(G/K)/(H/K) \cong G/H$.

If G is a group, a **G-set** is a set, X, together with a function $*$: $X \times G \to X$ such that:

(1) $x * 1 = x$ for all $x \in X$ and

(2) $(x * g) * h = x * (gh)$ for all $x \in X$ and g, $h \in G$.

If X is a G-set we say that G **acts** on the set X. We have here a primitive analogue of a vector space. If $Y \subseteq X$ the **stabiliser** of Y is $\boldsymbol{\sigma(Y)} = \{g \in G \mid x * g = x \text{ for all } x \in Y\}$. In general, stabilisers are not normal, but the stabiliser of the whole set is. If X is a G-set then: $\sigma(X)$ G and $G/\sigma(X)$ is isomorphic to a group of permutations on X.

A G-set X is defined to be **faithful** if $\sigma(X)$ is trivial and the group G is isomorphic to a group of permutations. Every group G is a faithful G-set if we define $x * g = xg$ for all x, g and so G is isomorphic to a group of permutations. (This is known as Cayley's Theorem).

Suppose X is a G-set and let $x \in X$. The set of all those elements of X that can be reached from x by multiplying by some element of G is called the **orbit** containing x and is denoted by $\boldsymbol{x^G}$. The relation ~ defined on X by $x \sim y$ if $x * g = y$ for some $g \in G$, is an equivalence relation and the equivalence classes are simply the orbits. If X is a G-set the size of the orbit of x is the index of the stabiliser of x in G.

§1.3. Conjugates and Commutators

Two elements g, h **commute** if $gh = hg$. In an abelian group this happens all the time and so the concepts in this section will only be of interest in a non-abelian group.

The **centraliser** of an element g in G is $\mathbf{C_G(g)} = \{x \in G \mid xg = gx\} \leq G$. It consists of all the elements of G that commute with g and is a subgroup of G.

Among the elements of $C_G(g)$ are the powers of g. We denote the set of powers of g by $\langle g \rangle$ and call it the **cyclic subgroup generated by g**. So $\langle g \rangle \leq C_G(g)$ for all $g \in G$.

The order of $\langle g \rangle$ is also the smallest positive n such that $g^n = 1$ and this is called the **order** of g, denoted by $|g|$.

We define the **centre** of a group G to be $\mathbf{Z(G)} = \{z \in G \mid zg = gz \text{ for all } g \in G\}$, a normal subgroup of G. We can produce the **ascending central series**

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \dots$$

where $Z_{n+1}(G)$ is defined by $Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G))$. If this series eventually reaches G we say that G is **nilpotent**.

If g, x are elements of G we define x^g to be $g^{-1}xg$, and say that x, y are **conjugates** if there exists $g \in G$ such that $y = g^{-1}xg$. Conjugacy is an equivalence relation, and the equivalence classes are called **conjugacy classes**. We denote the conjugacy class containing g by x^G. Conjugation makes G into a G-set in a different way to Cayley's theorem. The conjugacy classes are the orbits

and the stabilisers are the centralisers. The number of conjugates of g in G is the index of the centraliser, $C_G(g)$ in G.

We can conjugate subgroups by defining $\mathbf{H^g} = \{h^g \mid h \in H\}$ and $H^G = \{H^g \mid g \in G\}$. This makes the set of subgroups of G into a G-set. The **normalizer** of H in G is the stabiliser, $\mathbf{N_G(H)} = \{g \in G \mid H^g = H\}$. Normalisers are subgroups of G, and every subgroup of G is a normal subgroup of its normaliser. The number of conjugates of H in G is the index of the normaliser of H in G.

A **commutator** is an element $[g, h] = g^{-1}h^{-1}gh$. Whenever two elements commute, their commutator is the identity. The identity is a commutator, and the inverse of a commutator is a commutator: $[g, h]^{-1} = [h, g]$. Even a conjugate of a commutator is a commutator: $x^{-1}[g, h]x = x^{-1}g^{-1}h^{-1}ghx$. But the product of two commutators needn't be a commutator.

The **derived subgroup** G' (often called the **commutator subgroup**) of G is the set of all products of commutators. It is the smallest normal subgroup for which the quotient is abelian. We define G'' to be $(G')'$, $G''' = (G'')'$ and so on, but rather than accumulate dashes we begin to use superscripts. So we write G''' as $G^{(3)}$ and so on. Thus we define: $G^{(0)} = G$ and $G^{(n+1)} = G^{(n)\prime}$ for all n.

These are all normal subgroups of G and form a descending sequence, called the **derived series**: $G = G^{(0)} \geq G' \geq G'' \geq \ldots$ If this reaches 1, we say the group is **soluble**.

§1.4. Sylow Subgroups

Lagrange's Theorem states that the order of a subgroup divides the order of the group. The converse isn't always true. But if that number is a prime power, then there is indeed a subgroup of that order. The proofs use some clever counting techniques involving G-sets.

Sylow's First Theorem: A finite group G has a subgroup of order p^n whenever p^n divides |G|.

If $|G| = p^n m$ where p is prime and m is coprime to p, a subgroup of order p^n is called a Sylow p-subgroup of G.

Sylow's Second Theorem: All Sylow p-subgroups of G are conjugate in G.

Sylow's Third Theorem: If $|G| = p^n m$, where p is prime, coprime to m, the number of Sylow p-subgroups is congruent to 1 modulo p and divides m.

§1.5. Examples of Groups

Since this is merely a revision of basic group theory it's assumed that the reader has seen many examples of groups. But we list here some important families of groups. Most of them are described in terms of generators and relations in the form:

$$\langle A, B, \ldots \mid R_1, R_2 \ldots, R_n \rangle$$

where A, B, … are the generators and R_1, … , R_n are the relations.

Cyclic groups: $\mathbf{C_n} = \langle A \mid A^n = 1 \rangle$ is called the cyclic group of order n.

Dihedral groups: $\mathbf{D_{2n}} = \langle A, B \mid A^n = 1, B^2 = 1, BA = A^{-1}B \rangle$.

Metacyclic groups: $\mathbf{M_{m,n,r}} = \langle A, B \mid A^m = 1, B^n = 1, B^{-1}AB = A^r \rangle$.

Symmetric groups: $\mathbf{S_n}$ = {permutations on n symbols}, $\mathbf{A_n}$ = {even permutations} S_n.

General Linear groups: $\mathbf{GL(n, p)}$ = {$n \times n$ invertible matrices over the field $\mathbb{Z}_p$}.

§ 1.6. Rings and Fields

We also need to know something about rings, especially non-commutative ones. A ring R is a set with two operations + and ×. With regard to addition R is an abelian group. With regard to multiplication we only assume that it is closed under multiplication and the associative law holds for multiplication. Tying both operations together we have the distributive law.

Some books also assume that rings have a multiplicative identity, 1. We don't. The reason is that we want to be able to consider ideals of rings as subrings. The

definition of **subring** is obvious. A **left ideal** of R is a subring L with the additional property that $rx \in L$ whenever $x \in L$ and $r \in R$. This is a stronger than is required for a subring. If $x \in R$, Rx is a left ideal. If R has no 1 then Rx might not contain r. If we include it we get R$x + \mathbb{Z}r$, the set of all elements of the form $rx + nr$, where $r \in R$ and $n \in \mathbb{Z}$. This is the smallest left ideal that contains x and is called the **left ideal generated by** x. We define a **right ideal** similarly and a **2-sided ideal** is one that's both a left and a right ideal. We use the same symbol for 2-sided ideals as we do for normal subgroups.

Clearly the distinction between left and right is only of interest in non-commutative rings. (For some reason we never use the word 'abelian' for commutative rings. Perhaps this is because rings came long after Abel.)

The importance of 2-sided ideal is that they play the corresponding role for rings as normal subgroups do for groups. They are the subrings that one can factor out by to get quotient rings. The elements of R/I are cosets $x + I$, which are added and multiplied in terms of the representatives. It is easily checked that these operations are independent of the representatives used.

As with all sets with structure we have functions from one to another that preserve the structure. In the case of rings a **homomorphism** takes sums to sums and products to products. Moreover the three isomorphism theorems hold for rings. We define the **kernel** of a ring homomorphism to be the set of elements that map to zero.

Related words such as ‘isomorphism’, and ‘automorphism’ are defined in an analogous way for rings.

A **field** is a ring with the additional properties that multiplication is commutative, there is a multiplicative identity 1 (different to 0) and every non-zero element has a multiplicative inverse.

A field has **characteristic zero** if all non-zero elements have infinite order under addition. A field, F, is **algebraically closed** if every non-constant polynomial over F has a zero in F. The field, $\mathbb{C}$, of complex numbers has both properties and, as we’re doing classical representation theory, we’ll be using this field throughout.

§ 1.7. Vector Spaces

A **vector space**, over a field F, is an abelian group under addition, together with a multiplication by elements of F, written λv. We don’t adopt the convention of writing vectors in bold type because sometimes scalars are also vectors, as in the case where we consider the complex numbers to be a vector space of dimension 2 over the field of real numbers.

We insist on the following axioms related to scalar multiplication.

(1) $\lambda v \in V$ for all $\lambda \in F$ and $v \in V$;
(2) $1v = v$ for all $v \in V$;
(3) $(\lambda + \mu)v = \lambda v + \mu v$ for all $\lambda, \mu \in F$ and all $v \in V$;

(4) $\lambda(u + v) = \lambda u + \lambda v$ for all $\lambda \in F$ and all $u, v \in V$ and
(5) $(\lambda\mu)v = \lambda(\mu v)$ for all $\lambda, \mu \in F$ and all $v \in V$.

The theory of vector spaces runs a little way in parallel to the theory of groups, though the terminology is sometimes different. For a start we don't usually call it vector space theory, but rather **linear algebra**.

We define **subspaces** in the usual way, with the usual notation of $\leq$. The sum of two vector spaces is $U + V$, the set of all sums $u + v$ of vectors in U and V. The sum is a **direct sum**, written $U \oplus V$ if, in addition, $U \cap V = \{0\}$.

There's nothing special that corresponds to normal subgroups and 2-sided ideals in linear algebra. We can form **quotient spaces** U/V can be formed, in the usual way, using any subspace. (Usually these don't appear in a first course on linear algebra, but if you know about quotient groups you'll be OK with them.)

A **linear transformation** is defined to be a function θ from a vector space to a vector space, over the same field, such that:

$$\theta(\lambda x + \mu y) = \lambda\theta(x) + \mu\theta(y).$$

This corresponds to homomorphisms for groups and rings. Linear transformations from a vector space to itself are called **endomorphisms**. Those that are 1-1 and

onto are called **isomorphisms** and those that are isomorphisms from a vector space to itself are called **automorphisms**. Two vector spaces over the same field are said to be **isomorphic** if there is an isomorphism between them.

A **linear combination** of a set of elements X in a vector space V over F is a finite sum:

$$\lambda_1 v_1 + \ldots + \lambda_n v_n \text{ for some } n,$$

where each $\lambda_i \in F$ and each $v_i \in X$.

Let X be a subset of the vector space V.

- X is **spans** V if every vector in the space is a linear combination of them.
- X is **linearly independent** if the only linear combination of them that is zero is the trivial one, where all the coefficients are zero.
- X is a **basis** if it is both linearly independent and spans *V*.

The fundamental theorem of vector spaces is the fact that every finitely generated vector space has a basis and any two bases have the same number of elements, called the **dimension** of the vector space, $\dim_F V$, or just dim V if the field is understood. Any set of vectors with fewer elements does not span V and any set with more elements is automatically linearly dependent. It's also easy to see that dim V = dim U + dim (V/U) for any subspace U.

The **kernel** of a linear transformation θ is the set of vectors that map to zero, and this is a subspace, denoted by **ker** θ. The three isomorphism theorems that you have met in group theory and ring theory have their counterparts in vector space theory (usually called **linear algebra**), though they would not have had those names when you first met them. The dimension of ker θ is called the **nullity** of θ and the dimension of im θ is called the **rank** of θ.

The three isomorphism theorems that we encounter in group theory and ring theory have their counterparts in linear algebra, though they are expressed in terms of dimensions rather than isomorphisms.

First Isomorphism Theorem: If $\theta: U \to V$ is a linear transformation then $\ker \theta \leq U$ and $U/\ker \theta \cong \text{im } \theta$ (the image of θ).
Corollary: rank θ + nullity θ = dim U.

Second Isomorphism Theorem: If U, V are subspaces of a larger vector space then

$$(U + V)/V \cong U/(U \cap V).$$

Corollary: $\dim (U + V) = \dim U + \dim V - \dim (U \cap V)$.

Third Isomorphism Theorem: If $U \leq V \leq W$ then $(W/U)/(V/U) \cong W/V$.
The Corollary of this theorem, in terms of dimensions, would be

dim W – dim U – (dim V – dim U) = dim W – dim V
which is not very exciting, so that's why you've never heard of it!

The main example of a finite-dimensional vector space is $\{\lambda_1, \ldots, \lambda_n \mid \text{each } \lambda_i \in F\}$ under the usual addition and multiplication by an element of F. This is written as

$$F \oplus F \oplus \ldots \oplus F \ (n \text{ copies}).$$

and every vector space of dimension *n* over F is isomorphic to it. This is a representation theorem for vector spaces which, though useful, is not nearly as deep a theory as the theory of representations of finite groups.

An **algebra**, over a field F, is a ring with 1 that's also a vector space over F. If a ring with 1 contains a field it is automatically an algebra over that field.

§1.8. Matrices

A **matrix**, over a field F, is a rectangular array of elements from F. If there are m rows and n columns we call it an ***m* × *n* matrix**. It is a **square** matrix if $m = n$. The entry in the *i*'th row and *j*'th column is called the ***i*-*j* component**, and if it is a_{ij} we write $A = \mathbf{(a_{ij})}$.

The transpose of the $m \times n$ matrix $A = (a_{ij})$ is the $n \times m$ matrix $\mathbf{A^T} = (a_{ji})$. Clearly $(A^T)^T = A$, and if $A = A^T$, A is a **symmetric matrix**. A **diagonal matrix** is one where $a_{ij} = 0$ whenever $i \neq j$ and a **scalar matrix** is a square diagonal matrix where all the diagonal entries are the same. A

column vector, **v**, is an $n \times 1$ matrix and a **row vector** $\mathbf{v}^T$ is a $1 \times n$ matrix.

We add and, subtract and multiply two matrices with the same dimensions component-wise. That is, $(a_{ij}) \pm (b_{ij}) = (a_{ij} \pm b_{ij})$. Multiplication by a scalar (an element of F) is: $\lambda(a_{ij}) = (\lambda a_{ij})$.
The product of matrices is only defined in certain cases. If $A = (a_{ij})$ is an $m \times n$ matrix and $B = (b_{ij})$ is $n \times r$ then $AB = \left(\sum_k a_{ik} b_{kj}\right)$. Both addition and multiplication are associative and multiplication is distributive over addition.
The set of all $n \times n$ matrices over F is a ring, $M_n(F)$, with additive identity the **zero matrix**, 0, where all components are zero and multiplicative identity I, the scalar matrix where all diagonal components are 1.

If U, V are finite-dimensional vector spaces over F, with bases $\{u_1, \ldots, u_m\}$ and $\{v_1, \ldots, v_n\}$ respectively and if $\alpha: U \to V$ is a linear transformation where $\alpha(u_i) = \sum_j a_{ij} v_j$ the matrix $A = (a_{ij})$ is called the **matrix of the linear transformation** α. If $\beta: V \to W$ is a linear transformation with matrix B then the matrix of $\alpha\beta$ is AB. So matrix multiplication represents the multiplication of linear transformations.

The **determinant** of an $n \times n$ matrix A is defined inductively by (a) = a and $|A| = \sum_k a_{1j}A_{1j}$ where A_{ij} is the $(n-1)\times(n-1)$ matrix obtained from A by deleting row i and column j. Simple properties are $|A^T| = |A|$ and $|AB| = |A|.|B|$. The **adjoint** of A is $\text{adj}(A) = (|A_{ij}|)^T$ and $A.\text{adj}(A) = |A|.I = \text{adj}(A).A$. The **trace** of A is tr(A) = the sum of the diagonal elements.

The square matrix is **invertible** if A^{-1} exists and A is invertible if and only if $|A| \neq 0$. If A, B are invertible, $(AB)^{-1} = B^{-1}A^{-1}$. If $|A| = 0$ there exists a non-zero vector **v** such that $Av = 0$. If $Av = \lambda v$ for $v \neq 0$ the vector v is called an **eigenvector** of A and λ is the corresponding **eigenvalue**. The trace of a square matrix is the sum of its eigenvalues and the determinant is the product of the eigenvalues.

The polynomial $\chi_A(\lambda) = |\lambda I - A|$ is called the **characteristic polynomial** of A. Over $\mathbb{C}$ it splits into linear factors and the zeros of $\chi_A(\lambda)$ are the eigenvalues of A.

$$\chi_A(\lambda) = \lambda^n - \text{tr}(A) + \ldots + (-1)^n|A|.$$

If $f(\lambda)$ is any polynomial over F, f(A) is the matrix obtained by substituting A for λ and replacing the constant term a_0 by $a_0 I$. If f(A) = 0 then $f(\lambda) = 0$ for all eigenvalues, λ. So, if $A^n = I$, the eigenvalues of A will be

n-th roots of unity. The Cayley-Hamilton theorem states that $\chi_A(A) = 0$.

Two matrices A, B are **similar** if $B = S^{-1}AS$ for some invertible matrix S. Similarity is an equivalence relation and similar matrices have the same characteristic polynomial, eigenvalues, trace and determinant.

A matrix A is **diagonalisable** if it is similar to a diagonal matrix. Matrices with no repeated eigenvalues, symmetric matrices and matrices of finite order are among those that are diagonalisable.

§1.9. Inner Product Spaces

Finally you'll need to know a little of the theory of complex inner product spaces. A **complex inner product space** is a vector space over $\mathbb{C}$ with an inner product $\langle \mathbf{u}|\mathbf{v}\rangle$ satisfying the following axioms.

(1) $\langle u + v \mid w\rangle = \langle u|w\rangle + \langle v|w\rangle$;

(2) $\langle \lambda u \mid v\rangle = \lambda\langle u \mid v\rangle$;

(3) $\langle v \mid u\rangle$ is the complex conjugate of $\langle u \mid v\rangle$.

(4) $\langle v \mid v\rangle \geq 0$ for all v and $\langle v \mid v\rangle = 0$ if and only if $v = 0$;

By (3) $\langle v \mid v\rangle$ is real for all v and by (4) it is non-negative, so it has a real square root. This is called the **length** of a vector v. A **unit** vector is one whose length is 1. Two vectors u, v are **orthogonal** if $\langle u \mid v\rangle = 0$ and an **orthonormal basis** is a basis of mutually orthogonal unit vectors. A fundamental theorem of complex inner product

spaces is that every finite dimensional complex inner product space has an orthonormal basis.