Fields
A field is a non-zero commutative ring F in which every non-zero element $a \in F$ has an inverse $a^{-1} \in F$ defined

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

- All fields are Integral Domains.
- Every finite integral domain is a field.

Vector Spaces
A vector space V over a Field F is any set where for any vector $\mathbf{v} \in \mathbf{V}$ and scalar $\lambda \in F$ we have
- An abelian group $V = (V, +)$ i.e. vector addition
- A mapping $F \times V \rightarrow$: $(\lambda, \mathbf{v} \mapsto \lambda\mathbf{v})$ i.e. scalar multiplication or the action of F on V
and which also obeys the following axioms: $\forall \quad u, v, w \in V$ and $a, b \in F$

$$\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$$
$$\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$$
$$\mathbf{v} + 0 = \mathbf{v}$$
$$\mathbf{v} + (-\mathbf{v}) = 0$$
$$a(\mathbf{v} + \mathbf{w}) = a\mathbf{v} + a\mathbf{w}$$
$$(a + b)\mathbf{v} = a\mathbf{v} + b\mathbf{v}$$
$$a(b\mathbf{v}) = (ab)\mathbf{v}$$
$$1v = v$$

Vector Subspaces
A subset U of a vector space V is called a vector subspace if U contains the zero vector and whenever $\mathbf{u}, \mathbf{v} \in \mathbf{U}$ and $\lambda \in F$ we have
- $\mathbf{u} + \mathbf{v} \in \mathbf{U}$
- $\lambda\mathbf{u} \in \mathbf{U}$
We write $U \subseteq V$.
For infinite and finite $U_1, U_2 \subseteq V$
- $U_1 \cap U_2$ is a subspace
- $U_1 + U_2$ is a subspace
- $U_1 \cup U_2$ is not a subspace
A proper vector subspace of a finite dimensional vector space has itself a smaller dimension.
- $U \subseteq V \implies \dim U \leq \dim V$
- $\dim U = \dim V \implies V = U$
QUICK CHECK: For $\mathbf{u}, \mathbf{v} \in \mathbf{U}$ and $\lambda_1 \lambda_2 \in F$ we have $\lambda_1 \mathbf{u} + \lambda_2 \mathbf{v} \in \mathbf{U}$

Generating Vector Subspaces
Let T be a subset of a vector space V over a field F. Then amongst all vector subspaces of V that include T there is a smallest vector subspace

$$\langle T \rangle = \langle T \rangle_F \subseteq V.$$

It can be described as the set of all vectors $\alpha_1 \vec{v}_1 + \cdots + \alpha_r \vec{v}_r$ with $\alpha_1, \ldots, \alpha_r \in F$ and $\vec{v}_1, \ldots, \vec{v}_r \in T$, together with the zero vector in the case $T = \emptyset$.
A subset of a vector space is called a generating or spanning set of our vector space if its span is all of the vector space.

Power Sets
If X is a set, then the set of all subsets $\mathcal{P}(X) = \{U : U \subseteq X\}$ of X is the so-called power set of X. We can refer to a subset of $\mathcal{P}(X)$ is a system of subsets of X. Given such a system $\mathcal{U} \subseteq \mathcal{P}(X)$ we can create two new subsets of X, the union and the intersection of the sets of our system $\mathcal{U}$, as follows:

$$\bigcup_{U \in \mathcal{U}} U = \{x \in X : \text{s.t. } \exists U \in \mathcal{U} \text{ with } x \in U\}$$
$$\bigcap_{U \in \mathcal{U}} U = \{x \in X : x \in U \text{ for all } U \in \mathcal{U}\}$$

In particular the intersection of the empty system of subsets of X is X, and the union of the empty system of subsets of X is the empty set.

Liinear Independence
A subset L of a vector space V is called linearly independent if for all pairwise different vectors $\vec{v}_1, \ldots, \vec{v}_r \in L$ and arbitrary scalars $\alpha_1, \ldots, \alpha_r \in F$,

$$\alpha_1 \vec{v}_1 + \cdots + \alpha_r \vec{v}_r = \overrightarrow{0} \implies \alpha_1 = \cdots = \alpha_r = 0$$

Basis
A basis of a vector space V is a linearly independent generating set in V.
A basis always exists for finite vector spaces. The following are equivalent for a subset E of a vector space V
(1) Our subset E is a basis, i.e. a linearly independent generating set;
(2) Our subset E is minimal among all generating sets, meaning that $E \backslash \{\vec{v}\}$ does not generate V, for any $\vec{v} \in E$;
(3) Our subset E is maximal among all linearly independent subsets, meaning that $E \cup \{\vec{v}\}$ is not linearly independent for any $\vec{v} \in V$.
(4) If $L \subset V$ is a linearly independent subset and E is minimal amongst all generating sets of our vector space with the property that $L \subseteq E$, then E is a basis. (5) If $E \subseteq V$ is a generating set and if L is maximal amongst all linearly independent subsets of vector space with the property $L \subseteq E$, then L is a basis.

Dimension
The dimension of a vector space V is the cardinality (size) of a basis of V.

e.g. Free Vector Space
Let X be a set and F a field. The set $\text{Maps}(X, F)$ of all mappings $f : X \rightarrow F$ is called the free vecotr space with the operations of pointwise addition and multiplication by a scalar.
The subset of all mappings which send almost all elements of X to zero is a vector subspace

Fundamental Estimate
No linearly independent subset of a given vector space has more elements than a generating set. Thus if V is a vector space, $L \subset V$ a linearly independent subset and $E \subseteq V$ a generating set, then:

$$|L| \leqslant |E|$$

Steinitz Exchange Lemma
Let V be a vector space, $L \subset V$ a finite Linear Independence—linearly independent subset and $E \subseteq V$ a generating set. Then there is an injection $\phi : L \hookrightarrow E$ such that $(E \backslash \phi(L)) \cup L$ is also a generating set for V.
In other words, we can swap some elements of a generating set by the elements of our linearly independent set, and still keep a generating set.

Dimension Theorem
Let V be a vector space containing vector subspaces $U, W \subseteq V$. Then

$$\dim(U + W) + \dim(U \cap W) = \dim U + \dim W.$$

Linear Homomorphisms Let V and W be vector spaces over the same field.
A function $f : V \rightarrow W$ is said to be a linear map if for all $x, y \in V$ and some scalar $c \in K$, the operations of vector addition and scalar multiplication are preserved.

$$f(x + y) = f(x) + f(y)$$
$$f(cx) = cf(u)$$

- A linear map is injective if and only if its kernel is zero.
- All linear maps have that $f(\vec{0}) = \vec{0}$.
- All compositions of linear maps are also linear.
- Linear mappings are completely determined by the values they take on the basis of V.
Endomorphisms are Homomorphisms from a vector space to itself.
isomorphisms are bijective homomorphisms.
Automorphisms are isomorphisms from a vector space to itself.

Kernal and Image
The pre-image of the zero vector of a linear mapping $f : V \rightarrow W$ is denoted by

$$\ker(f) := f^{-1}(0) = \{v \in V : f(v) = 0\}$$

and is called the kernel of the linear mapping f.
The image of a linear mapping $f : V \rightarrow W$ is the subset $\text{im}(f) = f(V) \subseteq W$. The kernel and image are vector subspaces of V.

Fixed Points
A point that is sent to itself by a mapping is called a fixed point of the mapping.
Given a mapping $f : X \rightarrow X$, we denote the set of fixed points by

$$X^f = \{x \in X : f(x) = x\}.$$

Complemetary Subspaces
Two vector subspaces V_1, V_2 of a vector space V are called complementary if $V_1 \times V_2 \xrightarrow{\sim} V$ (addition) defines a Bijection.

Internal Direct Sum
Given Complementary Subspaces $U, U' \subseteq V$ and the Linear Mappings $f : U \rightarrow V$,

$f': U' \to V$ then we can form a new linear mapping $f: U \oplus U' \to V$ by the recipe

$$f(u, u') = f(u) + f'(u')$$

we then produce an vector space isomorphism $U \oplus U' \xrightarrow{\sim} V$.

We abuse notation a little by writing $V = U \oplus U'$ and say that the vector space V is the internal direct sum of the vector subspaces U and U'.

Direct Sum

Let V be a Vector Space with Vector Subspaces $V_1, \ldots, V_n$.

The vector subspace of V they generate is called the sum of our vector subspaces and denoted by $V_1 + \cdots + V_n$.

$$\langle V_1 \cup \cdots \cup V_n \rangle = V_1 + \cdots + V_n$$

If the natural Homomorphism given by addition $V_1 + \cdots + V_n \to V$ is an injection then we say the sum of the vector subspaces V_i is direct.

We write their sum also as $V_1 \oplus \cdots \oplus V_n$.

Linear Mapping and Basis

Let V, W be vector spaces over F and let $B \subset V$ be a basis. Then restriction of a mapping gives a bijection

$$operatornameHom_F(V, W) \xrightarrow{\sim} \mathrm{Maps}(B, W)$$
$$f \mapsto f|_B .$$

In-Bi-Surjection

$f: A \to B$

- is an injection (or one-to-one) if $f(a_1) = f(a_2)$ implies $a_1 = a_2$.
- is a surjection (or onto) if every $b \in B$ has at least one pre-image in A.
- is a bijection (or one-to-one correspondence) if it is both an injection and a surjection.

Left and Right Inverse Every injective linear mapping $f: V \hookrightarrow W$ has a left inverse, in other words a linear mapping $g: W \to V$ such that $g \circ f = \mathrm{id}_V$.

Every surjective linear mapping $f: V \to W$ has a right inverse, in other words a linear mapping $g: W \to V$ such that $f \circ g = \mathrm{id}_W$.

Rank-Nulity

Let $f: V \to W$ be a linear mapping between vector spaces.

Then:

$$\dim V = \dim(\ker f) + \dim(\operatorname{im} f).$$

This is called the "Rank-Nullity Theorem" because it is common to call the dimension of the image of f the rank of f, and the dimension of the kernel of f the nullity of f.

Applications: $f: V \to W$ is linear and V is finite-dimensional. - Then f is injective if and only if $\operatorname{dim im} f = \dim V$. - Since $\operatorname{dim im} f \leq \dim W$, a necessary condition for injectivity is $\dim V \leq \dim W$. - Then f is surjective if and only if $\dim \ker f = \dim V - \dim W$. - Since $\dim \ker f \geq 0$, a necessary condition for surjectivity is $\dim V \geq \dim W$.

Suppose $f: V \to W$ is an isomorphism and V is finite-dimensional. Then $\dim W = \dim V$. (In particular, F^m and F^n are isomorphic if and only if $m = n$.)

Suppose $f: V \to W$ is linear and that V, W are finite-dimensional with the same dimension. Then f is injective if and only if f is surjective.

Matrices as Linear Mapppings

Let F be a field and let $m, n \in \mathbb{N}$ be natural numbers.

There is a bijection between the space of linear mappings $F^m \to F^n$ and the set of matrices with n rows and m columns and entries in F :

$$\mathrm{M}: \mathrm{Hom}_F(F^m, F^n) \xrightarrow{\sim} \mathrm{Mat}(n \times m; F)$$
$$f \mapsto [f].$$

This attaches to each linear mapping f its representing matrix $\mathrm{M}(f) := [f]$.

The columns of this matrix are the images under f of the standard basis elements of F^m

$$[f] := (f(\vec{e}_1) | f(\vec{e}_2) | \cdots | f(\vec{e}_m)).$$

Mat Mul

Let $n, m, \ell \in \mathbb{N}, F$ a field, and let $A \in \mathrm{Mat}(n \times m; F)$ and $B \in \mathrm{Mat}(m \times \ell; F)$ be matrices.

The product $A \circ B = AB \in \mathrm{Mat}(n \times \ell; F)$ is the matrix defined by

$$(AB)_{ik} = \sum_{j=1}^{m} A_{ij} B_{jk}$$

Properties

$$(A + A')B = AB + A'B$$
$$A(B + B') = AB + AB'$$
$$IB = B$$
$$AI = A$$
$$(AB)C = A(BC).$$

Composition of Linear Mappings

The composition $g \circ f: U \to W$ is the matrix product of the representing matrices of f and g:

$$_{\mathcal{C}}[g \circ f]_{\mathcal{A}} = {}_{\mathcal{C}}[g]_{\mathcal{B}} \circ \mathcal{B}[f]_{\mathcal{A}}$$

Invertible Matrices

A matrix A is called invertible if and only if there exists matrices B and C such that $BA = I$ and $AC = I$.

To calculate the inverse of a matrix A:

- Write the identity matrix I next to it, thereby producing an $(n \times 2n)$-matrix $(A \mid I)$.
- Apply elementary row operations, including multiplying a row by a non-zero scalar, in order to bring A into Echelon Form, and then possibly further row operations to bring it into "reduced" echelon form: this will actually be the identity matrix.
- The inverse to A is then what is standing in the right half of the $(n \times 2n)$-matrix.

Elementary Matrix

An elementary matrix is any square matrix that differs from the identity matrix in at most one entry.

All the elementary matrices with entries in a field are, with the exception of those where you take one 1 in the identity matrix and replace it by 0 , invertible.

Rank

The column rank of a matrix $A \in \mathrm{Mat}(n \times m; F)$ is the dimension of the subspace of F^n generated by the columns of A.

Column and row rank are equal.

Rank is subadditive:

$$\operatorname{rank}(A + B) \leq \operatorname{rank} A + \operatorname{rank} B$$

Center of a Group

The centre of a group G, denoted as $Z(G)$, consists of elements that commute with every element in G.

$$Z(G) = \{g \in G \mid \forall h \in G, gh = hg\}$$

The centre is a subgroup of G and is always non-empty.

If G is an abelian group, then its centre is the entire group $(Z(G) = G)$.

Abstract Linear Mappings as Matrices

Let F be a Field, V and W Vector Spaces over F with ordered Basis $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_m)$ and $\mathcal{B} = (\vec{w}_1, \ldots, \vec{w}_n)$.

Then to each Linear Mapping $f: V \to W$ we associate a representing matrix ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ whose entries a_{ij} are defined by the identity

$$f(\vec{v}_j) = a_{1j}\vec{w}_1 + \cdots + a_{nj}\vec{w}_n \in W.$$

i.e. the image of a basis element $\vec{v}_i \in \mathcal{A}$ of V is a linear combination of the basis elements $\vec{w}_i \in \mathcal{B}$ of W.

This produces a Bijection, which is even an Isomorphism of vector spaces:

$$\mathrm{M}_{\mathcal{B}}^{\mathcal{A}}: \mathrm{Hom}_F(V, W) \xrightarrow{\sim} \mathrm{Mat}(n \times m; F)$$
$$f \mapsto {}_{\mathcal{B}}[f]_{\mathcal{A}}$$

We call $\mathrm{M}_{\mathcal{B}}^{\mathcal{A}}(f) = {}_{\mathcal{B}}[f]_{\mathcal{A}}$ the representing matrix of the mapping f with respect to the bases $\mathcal{A}$ and $\mathcal{B}$.

The columns of this matrix give the coefficients of the linear combination of vectors in $\mathcal{B}$ that make up each element of $\mathcal{A}$

i.e. The coordinates of the image of a basis vector from $\mathcal{A}$ with respect to the basis $\mathcal{B}$.

If V is m-dimensional and W is n-dimensional then $\mathrm{M}_{\mathcal{B}}^{\mathcal{A}}(f) = (a_{ij})$ is an $n \times m$ matrix, i.e. has n rows and m columns.

Change of Basis

The representing the identity mapping with respect to these bases

$${}_{\mathcal{B}}[\mathrm{id}_V]_{\mathcal{A}}$$

is called a change of basis matrix.
By definition, its entries are given by the equalities $\vec{v}_j = \sum_{i=1}^{n} a_{ij}\vec{w}_i$.

between Vector Spaces

Let V and W be finite dimensional Vector Space—vector spaces over F and let $f : V \to W$ be a Linear Mapping.
Suppose that $\mathcal{A}, \mathcal{A}'$ are Families of Elements—ordered basis of V and $\mathcal{B}, \mathcal{B}'$ are ordered bases of W. Then

$$_{\mathcal{B}'}[f]_{\mathcal{A}'} = {}_{\mathcal{B}'}[\mathrm{id}_W]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'}$$

within a Vector Space

Now let f be the Endomorphism $f : V \to V$, we have

$$_{\mathcal{A}'}[f]_{\mathcal{A}'} = {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'}^{-1} \circ {}_{\mathcal{A}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'}$$

Similar Matrices

Let $N = {}_{\mathcal{B}}[f]_{\mathcal{B}}$ and $M = {}_{\mathcal{A}}[f]_{\mathcal{A}}$ then if

$$N = T^{-1}MT$$

where $T = {}_{\mathcal{A}}[id_V]_{\mathcal{B}}$. We say that N and M are similar matrices.
Matrices that are similar are equivalent.

Mod

The set of integers modulo m is the set of integers that have the same remainder when you divide them by m and is written $\mathbb{Z}/m\mathbb{Z}$.
$\mathbb{Z}/m\mathbb{Z}$ is a ring.
As $\bar{a} = \bar{b} \in \mathbb{Z}/m\mathbb{Z}$ is the same as $a - b \in m\mathbb{Z}$, and we write

$$a \equiv b \pmod{m}.$$

The elements of $\mathbb{Z}/m\mathbb{Z}$ consist of congruence classes of integers modulo m. Each congruence class $\bar{a}$ is of the form $\bar{a} = a + m\mathbb{Z}$ with $a \in \mathbb{Z}$.
If $m \in \mathbb{N} \geqslant 1$ then there are m congruence classes modulo m, in other words $|\mathbb{Z}/m\mathbb{Z}| = m$, and can be written out as

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$

ddition and multiplication are defined

$$\bar{a} + \bar{b} = \overline{a+b} \text{ and } \bar{a} \cdot \bar{b} = \overline{ab}.$$

$\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime.

Rings

A ring is a set with two operations $(R, +, \cdot)$ that satisfy: 1) $(R, +)$ is a Abelian group; this means - there is an identity element $0 = 0_R \in R$ 2) $(R, \cdot)$ is a monoid; this means - the second operation $\cdot : R \times R \to R$ is associative - there is an identity element $1 = 1_R \in R$, often called just the identity, with the property that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$. 3) The distributive laws hold, meaning that for all $a, b, c \in R$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

The two operations are called addition and multiplication in our ring. A ring in which multiplication is commutative, that is in which $a \cdot b = b \cdot a$ for all $a, b \in R$, is a commutative ring.

Units of a Ring

Let R be a ring. An element $a \in R$ is called a unit if is invertible in R i.e. there exists $a^{-1} \in R$ such that

$$aa^{-1} = 1 = a^{-1}a.$$

The set of units in a ring forms a group under multiplication and is called the group of units of the ring R written $R^\times$.

Integral Domains

An integral domain is a non-zero commutative ring that has no zero-divisors. 1. $ab = 0 \Rightarrow a = 0$ or $b = 0$, and
2. $a \neq 0$ and $b \neq 0 \to ab \neq 0$
Let R be an integral domain and let $a, b, c \in R$. If $ab = ac$ and $a \neq 0$ then $b = c$. All Fields are integral domains since a unit cannot be a zero-divisor.
Every finite integral domain is a field.

Orbit - Stabiliser

The orbit of an element x under the action of a group G is denoted as $G.\ x$ and is the set $\{g \cdot x \mid g \in G\}$.
The stabiliser of an element x under the action of a group G, denoted as G_x, is the subgroup of elements in G that leave x fixed. $G_x = \{g \in G \mid g \cdot x = x\}$

Polynomials

Let R be a ring. A polynomial over R is an expression of the form

$$P = a_0 + a_1X + a_2X^2 + \cdots + a_mX^m$$

for some non-negative integer m and elements $a_i \in R$ for $0 \leqslant i \leqslant m$.
The set of all polynomials over R is denoted by $R[X]$.
In case a_m is non-zero, the polynomial P has degree m, written $\deg(P)$, and a_m is its leading coefficient.
When the leading coefficient is 1 the polynomial is a monic polynomial.
A polynomial of degree one is called linear, a polynomial of degree two is called quadratic, and a polynomial of degree three is called cubic.

Ring of Polynomials

Set $R[X]$ of Polynomials becomes a Ring called the ring of polynomials with coefficients in R, with the operations $+, \times$.

$$\begin{aligned}(a_0 + a_1X + \cdots a_mX^m)& \\ + (b_0 + b_1X + \cdots b_nX^n)& \\ = (a_0 + b_0) + (a_1 + b_1)X + \cdots&\end{aligned}$$

and

$$\begin{aligned}&(a_0 + a_1X + \cdots a_mX^m) \\ &\quad\times (b_0 + b_1X + \cdots b_nX^n) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)X \\ &+ (a_0b_2 + a_1b_1 + a_2b_0)X^2 + \cdots a_mb_nX^{m+n}\end{aligned}$$

where $m, n \geqslant 0, a_i, b_j \in R$ for $0 \leqslant i \leqslant m$ and $0 \leqslant j \leqslant n$.
The zero and the identity of $R[X]$ are the zero and identity of R, respectively.
The elements of R are just polynomials of degree 0. These are constant polynomials.
From the multiplication rule, if R is commutative, then so too is $R[X]$.
If R is a ring with no zero-divisors, then $R[X]$ has no zero-divisors and $\deg(PQ) = \deg(P) + \deg(Q)$ for non-zero $P, Q \in R[X]$.
If R is an integral domain then so is $R[X]$.
Let R be an integral domain and let $P, Q \in R[X]$ with Q monic.
Then there exists unique $A, B \in R[X]$ such that

$$P = AQ + B$$

and $\deg(B) < \deg(Q)$ or $B = 0$.

Polynomial Roots

Let R be a commutative ring, let $\lambda \in R$ and $P(X) \in R[X]$. Then λ is a root of $P(X)$ if and only if $(X - \lambda)$ divides $P(X)$.
Let R be a field, or more generally an integral domain. Then a non-zero polynomial $P \in R[X]\backslash\{0\}$ has at most $\deg(P)$ roots in R.

Algebraic Closure

A field F is algebraically closed if each non-constant polynomial $P \in F[X]\backslash F$ with coefficients in our field has a root in our field F.
If F is an algebraically closed field, then every non-zero polynomial $P \in F[X]\backslash\{0\}$ decomposes into linear factors

$$P = c(X - \lambda_1) \cdots (X - \lambda_n)$$

with $n \geqslant 0, c \in F^\times$ and $\lambda_1, \ldots, \lambda_n \in F$.
This decomposition is unique up to reordering the factors.

Fundamental Theorem of Algebra

The field of complex numbers $\mathbb{C}$ is algebraically closed.

Rings Homomorphisms

Let R and S be rings.
A mapping $f : R \longrightarrow S$ is a ring homomorphism if the following hold for all $x, y \in R$:

$$f(x + y) = f(x) + f(y)$$
$$f(xy) = f(x)f(y)$$

For all $x, y \in R$ and $m \in \mathbb{Z}$:
- $f(0_R) = 0_S$, where 0_R and 0_S are the zeros of R and S respectively;
- $f(-x) = -f(x)$;
- $f(x - y) = f(x) - f(y)$;
- $f(mx) = mf(x)$,
- $f(x^n) = (f(x))^n$

f is injective if and only if $\ker f = \{0\}$.

Ideals

A subset I of a ring R is an ideal, written $I \trianglelefteq R$, if the following hold:
1. $I \neq \emptyset$;
2. I is closed under subtraction;
3. for all $i \in I$ and $r \in R$ we have $ri, ir \in I$.

Condition (3) says that I is closed under multiplication by elements of R.
In any ring R, $\{0\}$ and R are ideals of R.

The intersection of any collection of ideals of a ring R is an ideal of R.
Let I and J be ideals of a ring R. Then

$$I+J=\{a+b: a \in I, b \in J\}$$

is an ideal of R.
Each ideal is a kernel of at least one Ring Homomorphism, namely $can: R \rightarrow R/I$

Generting Ideals

Let R be a commutative ring and let $T \subset R$. Then the ideal of R generated by T is the set

$$_R\langle T\rangle=\{r_1 t_1+\cdots+r_m t_m: t_1, \ldots, t_m \in T, \\ r_1, \ldots, r_m \in R\},$$

together with the zero element in the case $T=\emptyset$.
We often write $_R\left\langle t_1, \ldots, t_n\right\rangle$ instead of $_R\left\langle\left\{t_1, \ldots, t_n\right\}\right\rangle$.
Let $m \in \mathbb{Z}$. Then $_{\mathbb{Z}}\langle m\rangle=m \mathbb{Z}$.
Let $P \in \mathbb{R}[X]$. Then $\mathbb{R}_{\mathbb{R}[]}\langle P\rangle=\{A P: A \in \mathbb{R}[X]\}=\{Q: P$ divides Q in $\mathbb{R}[X]\}$.
Let R be a commutative ring and let $T \subseteq R$. Then $_R\langle T\rangle$ is the *smallest* ideal of R that contains T.

Principle Ideals

An ideal I of R is called a principal ideal if $I=\langle t\rangle$ for some $t \in R$.
i.e. it I is generated by one element of R.

Kernal of a Ring Homomorphism

Let R and S be Rings with zero elements 0_R and 0_S respectively and let $f: R \rightarrow S$ be a ring homomorphism. The kernel of f is

$$\operatorname{ker} f=\left\{r \in R: f(r)=0_S\right\}.$$

Subrings

Let R be a ring. A subset $R^{\prime}$ of R is a subring of R if $R^{\prime}$ itself is a ring under the operations of *addition* and *multiplication* defined in R.
Quick Check
Let $R^{\prime}$ be a subset of a ring R. Then $R^{\prime}$ is a subring if and only if
1) $R^{\prime}$ has a multiplicative identity, and
2) $R^{\prime}$ is closed under subtraction: $a, b \in R^{\prime} \rightarrow a-b \in R^{\prime}$, and
3) $R^{\prime}$ is closed under multiplication.
Let R and S be rings and $f: R \longrightarrow S$ a Ring Homomorphism.
1) If $R^{\prime}$ is a subring of R then $f\left(R^{\prime}\right)$ is a subring of S. In particular, $\operatorname{im} f$ is a subring of S.
2) Assume that $f\left(1_R\right)=1_S$. Then if x is a unit in $R, f(x)$ is a unit in S and $(f(x))^{-1}=f\left(x^{-1}\right)$. In this case f restricts to a group homomorphism $\left.f\right|_{R^{\times}}: R^{\times} \rightarrow S^{\times}$.
It is not true that the intersection of two subrings of R is a subring of R.

Equivalence Relation

A relation R on a set X is a subset $R \subseteq X \times X$. In this context, instead of writing $(x, y) \in R$, I will write $x R y$.
Then R is an equivalence relation on X when for all elements $x, y, z \in X$ the following hold:
1) Reflexivity: $x R x$;
2) Symmetry: $x R y \Leftrightarrow y R x$;
3) Transitivity: ($x R y$ and $y R z) \rightarrow x R z$.

Equivalence Class

Suppose that $\sim$ is an Equivalence Relation on a set X. For $x \in X$ the set $E(x):=\{z \in X: z \sim x\}$ is called the equivalence class of x.
A subset $E \subseteq X$ is called an equivalence class for our equivalence relation if there is an $x \in X$ for which $E=E(x)$.
An element of an equivalence class is called a representative of the class.
A subset $Z \subseteq X$ containing precisely one element from each equivalence class is called a system of representatives for the equivalence relation.
For $x, y \in X$ the following are equivalent:
1) $x \sim y$;
2) $E(x)=E(y)$;
3) $E(x) \cap E(y) \neq \emptyset$.

Set of Equivalence Classes

Given an Equivalence Relation $\sim$ on the set X, we denote the set of equivalence classes, which is a subset of the Power Sets—power set $\mathcal{P}(X)$, by

$$(X / \sim):=\{E(x): x \in X\}$$

There is a canonical mapping where each element of X must belong to some equivalence class

$$can: X \rightarrow(X / \sim), x \mapsto E(x)$$

It is a Surjection.

Cosets of a Ring

Let $I \unlhd R$ be an ideal in a Ring R. The set

$$x+I:=\{x+i: i \in I\} \subseteq R$$

is a coset of I in R or the coset of x with respect to I in R.
In the sense of group theory, $x+I$ is the left coset w.r.t I and is also the right coset because R is Abelian.
It follows that there is an Equivalence Relation on R defined by

$$x \sim y \iff x-y \in I$$

whose Equivalence Classes $E(x)$ are the cosets $x+I$.

Factor Rings

Then R/I, the factor ring of R by I (or the quotient of R by I), is the Set of Equivalence Classes $(R / \sim)$ for this $\sim$.
This is actually the set of cosets of I in R because each Equivalence Class can be written

$$\begin{aligned} x \sim y & \iff x-y \in I \\ & \Longrightarrow y \in I+x \\ & \Longrightarrow [x]=x+I:=\{x+r: r \in I\}\end{aligned}$$

which is clearly of coset of I wrt x.
R/I is a ring.
Addition is defined by

$$(x+I) \dot{+}(y+I)=(x+y)+I \quad \text{for all } x, y \in R$$

with $0+I$ as the additive identity.
Multiplication is defined by

$$(x+I) \cdot(y+I)=x y+I \quad \text{for all } x, y \in R$$

with $-x+I$ as the inverse of $x+I$

Universal Property of Factor Rings

Let R be a Ring and I an ideal of R.
1) The mapping $can: R \rightarrow R/I$ sending r to $r+I$ for all $r \in R$ is a Surjection—surjective Ring Homomorphism with kernel I.
2) If $f: R \rightarrow S$ is a ring homomorphism with $f(I)=\left\{0_S\right\}$, so that $I \subseteq \operatorname{ker} f$, then there is a unique ring homomorphism $\bar{f}: R/I \rightarrow S$ such that $f=\bar{f} \circ can$.
The second part of the Theorem states that f factorises uniquely through the canonical mapping to the factor whenever the ideal I is sent to zero.

First Isomorphism Theorem for Rings

Let R and S be Rings. Then every Ring Homomorphism $f: R \longrightarrow S$ induces a ring Isomorphism

$$\bar{f}: R / \operatorname{ker} f \xrightarrow{\sim} \operatorname{im} f.$$

Modules

A (left) module M over a Ring R is a pair consisting of an Abelian group $M=(M, \dot{+})$ and a mapping

$$\begin{gathered} R \times M \rightarrow M \\ (r, a) \mapsto r a \end{gathered}$$

such that for all $r, s \in R$ and $a, b \in M$ the following identities hold:

$$\begin{gathered} r(a+b)=(r a) \dot{+}(r b) \\ (r+s) a=(r a) \dot{+}(s a) \\ r(s a)=(r s) a \\ 1_R a=a \end{gathered}$$

The first two laws are the Distributive Laws; the third law is called the Associativity Law.
We call a left module M over a ring R an R-module.
Let R be a ring and M an R-module.
1) $0_R a=0_M$ for all $a \in M$.
2) $r 0_M=0_M$ for all $r \in R$.
3) $(-r) a=r(-a)=-(r a)$ for all $r \in R, a \in M$. Here the first negative is a negative in R, the last two are negatives in M.

Direct Sum of Modules

Given a Ring R and R-modules $M_1, \ldots, M_n$, the cartesian product $M_1 \times M_2 \times \cdots \times M_n$ is an R-module if we define addition and multiplication as follows:

$$\begin{aligned} & \left(a_1, \ldots, a_n\right)+\left(b_1, \ldots, b_n\right) \\ & =\left(a_1+b_1, \ldots, a_n+b_n\right)\end{aligned}$$

and

$$r\left(a_1, \ldots, a_n\right)=\left(r a_1, \ldots, r a_n\right)$$

for all $r \in R$ and $a_i, b_i \in M$.
This is denoted $M_1 \oplus \cdots \oplus M_n$ and called the direct sum.

Sub-module

A non-empty subset M' of an R-module M is a submodule if M' is an $R-$ module with respect to the operations of the R-module M restricted to M'.
- Let $T \subseteq M$. Then ${}_R\langle T\rangle$ is the smallest submodule of M that contains T.
- The intersection of any collection of submodules of M is a submodule of M.
- Let M_1 and M_2 be submodules of a. Then

$$M_1 + M_2 = \{a + b : a \in M_1, b \in M_2\}$$

is a submodule of M.
QUICK CHECK
Let R be a Ring and let M be an R-module. A subset M' of M is a submodule if and only if
1) $0_M \in M'$
2) $a, b \in M' \Rightarrow a - b \in M'$
3) $r \in R, a \in M' \Rightarrow ra \in M'$.

Cosets of a Module

Let R be a Ring, M an R-module and N a submodule of M.
For each $a \in M$ the coset of a with respect to N in M is

$$a + N = \{a + b : b \in N\}$$

It is a coset of N in the abelian group M and so is an Equivalence Class for the Equivalence Relation $a \sim b \Leftrightarrow a - b \in N$.

Factor Module

Let R be a Ring, M an R-module and N a submodule of M.
Define M/N, as the factor module of M by N (or the quotient of M by N), to be the set $(M/\sim)$ of all cosets of N in M.
This becomes an R-module by introducing the operations of addition and multiplication as follows:

$$(a + N)\dot{+}(b + N) = (a + b) + N$$
$$r(a + N) = ra + N$$

for all $a, b \in M, r \in R$.

Universal Property of Factor Modules

Let R be a Ring, let L and M be R-modules, and N a Submoduleof M.
1) The mapping $can : M \to M/N$ sending a to $a + N$ for all $a \in M$ is a surjective R-homomorphism with kernel N.
2) If $f : M \to L$ is an R-homomorphism with $f(N) = \{0_L\}$, so that $N \subseteq \ker f$, then there is a *unique homomorphism* $\bar{f} : M/N \to L$ such that $f = \bar{f} \circ can$.
The second part of the theorem states that f factorises uniquely through the canonical mapping to the factor whenever the submodule N is sent to zero.

First Isomorphism Theorem for Modules

Let R be a Ring and let M and N be R-modules. Then every R-homomorphism $f : M \longrightarrow N$ induces an R-isomorphism

$$\bar{f} : M/\ker f \xrightarrow{\sim} \operatorname{im} f.$$

Multilinear Form

Let $U_1, U_2, \ldots, U_n, W$ be vector spaces over a Field F, then a map

$$H : U_1 \times U_2 \times \cdots \times U_n \to W$$

is multilinear if it is linear in each of its entries separately.
In the case $n = 2$ this is exactly the definition of a Bilinear Form
A multilinear form is alternating if it vanishes on every n-tuple of elements of U that has at least two entries equal, in other words if:

$$(\exists i \neq j \text{ with } v_i = v_j)$$
$$\to H(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = 0$$

This is the same as writing, for any $\sigma \in \mathfrak{S}_n$

$$H\left(v_{\sigma(1)}, \ldots, v_{\sigma(n)}\right) = \operatorname{sgn}(\sigma) H(v_1, \ldots, v_n)$$

Symmetric Group

The group of all permutations of the set $\{1, 2, \ldots, n\}$, also known as *Bijections* from $\{1, 2, \ldots, n\}$ to itself, is denoted by $\mathfrak{S}_n$ and called the **n-th symmetric group**. It is a group under *composition*.
It has $n!$ elements.
A *transposition* is a permutation that swaps two elements of the set and leaves all the others unchanged.
- All transpositions are odd permutations and have length $2|i - j| - 1$
An *inversion* of a permutation $\sigma \in \mathfrak{S}_n$ is a pair (i, j) such that $1 \leqslant i < j \leqslant n$ and $\sigma(i) > \sigma(j)$.
The number of inversions of the permutation σ is called the *length* of σ and written $\ell(\sigma)$. In formulas:

$$\ell(\sigma) = | \{(i, j) : i < j \text{ but } \sigma(i) > \sigma(j)\} |$$

Length can also be counted from the number of crossings in a permutation diagram.
The *sign* of σ is defined to be the parity of the number of inversions of σ. In formulas:

$$\operatorname{sgn}(\sigma) = (-1)^{\ell(\sigma)}$$

For each $n \in \mathbb{N}$ the sign of a permutation produces a group homomorphism $sgn : \mathfrak{S}_n \to \{+1, -1\}$ from the symmetric group to the two-element group of signs.
In formulas:

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) \quad \text{ for all } \sigma, \tau \in \mathfrak{S}_n$$

A permutation whose sign is $+1$, in other words which has *even length*, is called an *even permutation*, while a permutation whose sign is -1 , in other words which has *odd length*, is called an *odd permutation.*
For $n \in \mathbb{N}$, the set of even permutations in $\mathfrak{S}_n$ forms a subgroup of $\mathfrak{S}_n$ because it is the kernel of the group homomorphism $sgn : \mathfrak{S}_n \to \{+1, -1\}$. This group is the *alternating group* and is denoted by A_n.

Determinant

Multilinear Form Characterisation
Let F be a Field. The mapping

$$\det : \operatorname{Mat}(n; F) \to F$$

is the *unique alternating* multilinear form on n-tuples of column vectors with values in F that takes the value 1_F on the identity matrix.
Or if we are to consider the matrix as an ordered list of n column vectors

$$\det : F^n \times \cdots \times F^n \to F, (v_1, \ldots, v_n) \mapsto \det (v_1$$

Leibniz Characterisation
Let R be a commutative Ring and $n \in \mathbb{N}$. The determinant is a mapping det : $\operatorname{Mat}(n; R) \to R$ from Square Matrices with coefficients in R to the ring R that is given by the following formula:

$$A \mapsto \det(A) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \ldots a_{n\sigma(n)}$$

The sum is over all permutations of n, and the coefficient $\operatorname{sgn}(\sigma)$ is the sign of the permutation σ.
The degenerate case $n = 0$ assigns the value 1 as the determinant of the "empty matrix".
Laplace's Expansion of the Determinant
Let $A = (a_{ij})$ be an $(n \times n)$-matrix with entries from a commutative ring R. For a fixed i the i-th row expansion of the determinant is

$$\det(A) = \sum_{j=1}^{n} a_{ij} C_{ij}$$

and for a fixed j the j-th column expansion of the determinant is

$$\det(A) = \sum_{i=1}^{n} a_{ij} C_{ij}$$

Multiplicativity
Let R be a commutative ring and let $A, B \in \operatorname{Mat}(n; R)$. Then

$$\det(AB) = \det(A)\det(B).$$

Determinantal Criterion for Invertibility
The determinant of a square matrix with entries in a field F is non-zero if and only if the matrix is invertible.
A square matrix with entries in a commutative ring R is invertible if and only if its determinant is a unit in R.
That is, $A \in \operatorname{Mat}(n; R)$ is invertible if and only if $\det(A) \in R^\times$. *Inverse of the Determinant*
If A is invertible then $\det\left(A^{-1}\right) = \det(A)^{-1}$. If B is a square matrix B then

$$\det\left(A^{-1}BA\right) = \det(B)$$

Determinant of an Endomorphism
The determinant of an representative matrix ${}_{\mathcal{A}}[f]_{\mathcal{A}}$ is independent of the choice of basis $\mathcal{A}$. Therefore the determinant is in

fact defined only by the endomorphism f.
Transpose

$$\det\left(A^{\top}\right)=\det(A)$$

Cramer's Rule
Let A be an $(n\times n)$-matrix with entries in a commutative ring R. *adj* is the Adjugate Matrix. Then

$$A\cdot\operatorname{adj}(A)=(\det A)I_n$$

Jacobi's Formula
Let $A=(a_{ij})$ where the coefficients $a_{ij}=a_{ij}(t)$ are functions of t. Then

$$\frac{d}{dt}\det A=\operatorname{Tr}\operatorname{Adj}A\frac{dA}{dt}.$$

Cofactor of a Matrix
Let $A\in\operatorname{Mat}(n;R)$ for some commutative Ring R and natural number n. Let i and j be integers between 1 and n.
Then the (i,j) cofactor of A is

$$C_{ij}=(-1)^{i+j}\det(A\langle i,j\rangle)$$

where $A\langle i,j\rangle$ is the matrix obtained from A be deleting the i-th row and the j-th column.
Adjugate
Let A be an $(n\times n)$-matrix with entries in a commutative Ring R. The adjugate matrix $\operatorname{adj}(A)$ is the $(n\times n)$-matrix whose entries are $\operatorname{adj}(A)_{ij}=C_{ji}$ where C_{ji} is the (j,i)-cofactor.
Real Inner Product
Let V be a Vector Space over $\mathbb{R}$. An inner product on V is a mapping

$$(-,-):V\times V\to\mathbb{R}$$

that satisfies the following for all $\vec{x},\vec{y},\vec{z}\in V$ and $\lambda,\mu\in\mathbb{R}$:
1) $(\lambda\vec{x}+\mu\vec{y},\vec{z})=\lambda(\vec{x},\vec{z})+\mu(\vec{y},\vec{z})$
2) $(\vec{x},\vec{y})=(\vec{y},\vec{x})$
3) $(\vec{x},\vec{x})\geqslant 0$, with equality if and only if $\vec{x}=\overrightarrow{0}$
A real inner product space is a real vector space endowed with an inner product.
A real inner product space is necessarily a Symmetric Bilinear Form.
A finite-dimensional real inner product space is a Euclidean Vector Space.
Every finite dimensional inner product space has an orthonormal basis.

Complex Inner Product
Let V be a Vector Space over $\mathbb{C}$. An inner product on V is a mapping

$$(-,-):V\times V\to\mathbb{C}$$

that satisfies the following for all $\vec{x},\vec{y},\vec{z}\in V$ and $\lambda,\mu\in\mathbb{C}$:
1) $(\lambda\vec{x}+\mu\vec{y},\vec{z})=\lambda(\vec{x},\vec{z})+\mu(\vec{y},\vec{z})$
2) $(\vec{x},\vec{y})=\overline{(\vec{y},\vec{x})}$
3) $(\vec{x},\vec{x})\geqslant 0$, with equality if and only if $\vec{x}=\overrightarrow{0}$
Here $\bar{z}$ denotee the *complex conjugate* of z.
A complex inner product space is a complex vector space endowed with an inner product.
Complex inner product spaces are Skew-Linear in their second variable, also known as sesquilinear.
Inner Product Norm
In a real or complex inner product space the length or inner product norm $\|\vec{v}\|\in\mathbb{R}$ of a vector $\vec{v}$ is defined as the non-negative square root

$$\|\vec{v}\|=\sqrt{(\vec{v},\vec{v})}$$

Two vectors $\vec{v},\vec{w}$ are orthogonal and we write

$$\vec{v}\perp\vec{w}$$

if and only if $(\vec{v},\vec{w})=0$. We say that $\vec{v}$ and $\vec{w}$ are at right-angles to each other.
We write $S\perp T$ as a shorthand for $\vec{v}\perp\vec{w}$ for all $\vec{v}\in S$ and $\vec{w}\in T$.
Vectors whose length is 1 are called units.

Orthogonal Complement
Let V be an Inner Product Space and let $T\subseteq V$ be an arbitrary subset. Define

$$T^{\perp}=\{\vec{v}\in V:\vec{v}\perp\vec{t}\text{ for all }\vec{t}\in T\},$$

calling this set the orthogonal to T. If T is a subspace it is the orthogonal complement to V.
Orthogonal Matrix
An orthogonal matrix is an $(n\times n)$-matrix P with real entries such that $P^{\top}P=I_n$. In other words, an orthogonal matrix is a square matrix P with real entries such that $P^{-1}=P^{\top}$.
Unitary Matrix
An unitary matrix is an $(n\times n)$-matrix P with complex entries such that $\bar{P}^{\top}P=I_n$. In other words, a unitary matrix is a square matrix P with complex entries such that $P^{-1}=\bar{P}^{\top}$.
Gram-Schmidt Process
Given nn arbitrary linearly independent ordered subset $\vec{v}_1,\vec{v}_2,\ldots$ of an inner product space V.
Our aim is to produce the elements of $(\vec{w}_i)$, an orthonormal family in V.
1. Take the first element $\vec{v}_1$ and normalize it to have length 1 . Let this be the first element $\vec{w}_1$.
2. For each subsequent vector $\vec{v}_i$ from the subset:
- Subtract the orthogonal projection of $\vec{v}_i$ onto the space $\langle\vec{w}_1,\vec{w}_2,\ldots,\vec{w}_{i-1}\rangle$.
- Normalize the resulting vector to have length 1 . Let this be the i th element $\vec{w}_i$ of the orthonormal family.
Repeat this process until you've dealt with all vectors $\vec{v}_1,\vec{v}_2,\ldots$

Adjoint Endomorphisms
Let V be an Inner Product Space. Then two Endomorphisms $T,S:V\to V$ are called adjoint to one another if the following holds for all $\vec{v},\vec{w}\in V$:

$$(T\vec{v},\vec{w})=(\vec{v},S\vec{w})$$

In this case I will write $S=T^*$ and call S the adjoint of T. Any endomorphism has at most one adjoint. Let V be a finite dimensional inner product space. Let $T:V\to V$ be an endomorphism. Then T^* exists. That is, there exists a unique linear mapping $T^*:V\to V$ such that for all $\vec{v},\vec{w}\in V$

$$(T\vec{v},\vec{w})=(\vec{v},T^*\vec{w})$$

Self-Adjoint
An Endomorphism of an Inner Product Space $T:V\to V$ is self-adjoint if it equals its own adjoint that is if $T^*=T$. Let $T:V\to V$ be a self-adjoint linear mapping on an inner product space V.
1) Every eigenvalue of T is real.
2) If λ and μ are distinct eigenvalues of T with corresponding eigenvectors $\vec{v}$ and $\vec{w}$, then $(\vec{v},\vec{w})=0$.
3) T has an eigenvalue.
Hermitian Matrices
A real $(n\times n)$-matrix A describes a self-adjoint mapping on the standard inner product space $\mathbb{R}^n$ precisely when A is symmetric, that is when $A^{\top}=A$.
A complex $(n\times n)$-matrix A describes a self-adjoint mapping on the standard inner product space $\mathbb{C}^n$ precisely when $A=\bar{A}^{\top}$ holds.
Such matrices are called hermitian.
Conjugate Transpose
The conjugate transpose $\bar{A}^T$ is the matrix obtained from A by first conjugating each entry and then transposing the resulting matrix.
Raleigh Quotient
V is a finite dimensional real Inner Product Space. The Raleigh Quotient is the real-valued function defined

$$R:V\backslash\{\overrightarrow{0}\}\to\mathbb{R}\tag{1}$$

$$\vec{v}\mapsto R(\vec{v})=\frac{(T\vec{v},\vec{v})}{(\vec{v},\vec{v})}\tag{2}$$

$$\tag{3}$$

Spectral Theorem
For Self-Adjoint Endomorphisms
Let V be a finite dimensional Inner Product Space and let $T:V\to V$ be a self-adjoint linear mapping. Then V has an Orthonormal Basis consisting of eigenvectors of T.
For Real Symmetric Matrices
Let A be a real $(n\times n)$ symmetric matrix. Then there is an $(n\times n)$-orthogonal matrix P such that

$$P^{\top}AP=P^{-1}AP=\operatorname{diag}(\lambda_1,\ldots,\lambda_n)$$

where $\lambda_1,\ldots,\lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity as roots of the characteristic polynomial of A.
For Hermitian Matrices
Let A be $a(n\times n)$-hermitian matrix. Then there is an $(n\times n)$-unitary matrix P such that

$$\bar{P}^{\top}AP=P^{-1}AP=\operatorname{diag}(\lambda_1,\ldots,\lambda_n)$$

where $\lambda_1, \ldots, \lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity as roots of the characteristic polynomial of A.

Exponential Mapping

$$\exp : \mathrm{Mat}(n; \mathbb{C}) \to \mathrm{Mat}(n; \mathbb{C})$$
$$A \mapsto \sum_{k=0}^{\infty} \frac{1}{k!} A^k$$

This mapping plays a central role in describing the solutions to linear differential equations with constant coefficients. If $A \in \mathrm{Mat}(n; \mathbb{C})$ is a square matrix and $\vec{c} \in \mathbb{C}^n$ a column vector, then there exists exactly one differentiable mapping $\gamma : \mathbb{R} \to \mathbb{C}^n$ with initial value $\gamma(0) = \vec{c}$ and which satisfies $\dot{\gamma}(t) = A\gamma(t)$ for all $t \in \mathbb{R}$: it is the mapping

$$\gamma(t) = \exp(tA)\vec{c}.$$

Cayley-Hamilton

Let $A \in \mathrm{Mat}(n; R)$ be a square matrix with entries in a commutative Ring R. Then evaluating its characteristic polynomial $\chi_A(x) \in R[x]$ at the matrix A gives zero.

JNF

Let F be an algebraically closed field. Let V be a finite dimensional vector space and let $\phi : V \to V$ be an endomorphism of V with characteristic polynomial

$$\chi_\phi(x) = (x - \lambda_1)^{a_1} (x - \lambda_2)^{a_2} \ldots (x - \lambda_s)^{a_s} \in F[x]$$
$$, a_i \geqslant 1, \sum_{i=1}^{s} a_i = n,$$

for distinct $\lambda_1, \lambda_2, \ldots, \lambda_s \in F$.
Then there exists an ordered basis $\mathcal{B}$ of V such that the matrix of ϕ with respect to the basis $\mathcal{B}$ is block diagonal with Jordan Blocks on the diagonal

$$_{\mathcal{B}}[\phi]_{\mathcal{B}} = \mathrm{diag}(J(r_{11}, \lambda_1), \ldots, J(r_{1m_1}, \lambda_1), J(r_{21}, \lambda_2), \ldots, J(r_{sm_s}, \lambda_s))$$

with $r_{11}, \ldots, r_{1m_1}, r_{21}, \ldots, r_{sm_s} \geqslant 1$ such that

$$a_i = r_{i1} + r_{i2} + \cdots + r_{im_i} (1 \leqslant i \leqslant s).$$

Kronecker Delta

The Kronecker Delta is defined:

$$\delta^i_j = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$