## Fields

A field is a non-zero commutative division ring. - All fields are Integral Domains.

## Divsion Rings

A ring $F$ in which every non-zero element $a \in F$ has an inverse $a^{-1} \in F$ ( $\implies$ has no zero-divsors!)

## Vector Spaces

A vector space $V$ over a Field $F$ is any set equipped with vector addition and scalr multiplication. $\forall \quad u, v, w \in V$ 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
- $\dim(U) \leq \dim V$

QUICK CHECK: For $\mathbf{u}, \mathbf{v} \in \mathbf{U}$ and $\lambda_1 \lambda_2 \in F$ we have $\lambda_1 \mathbf{u} + \lambda_\mathbf{2} \mathbf{v} \in \mathbf{U}$

## 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 power set of $X$. 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.

## Linear 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 $E \subset V$:

(1) $E$ is a basis (2) $E$ is minimal among all generating sets, meaning that $E \backslash \{\vec{v}\}$ does not generate $V$, for any $\vec{v} \in E$;

(3) $E$ 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 $V$.

## 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 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 $f : V \to W$ is said to be a linear map if for all $x, y \in V$ and some scalar $c \in K$,

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

- A linear map is injective if and only if its kernel is zero.
- All linear maps have that $f(\vec{0}) = \vec{0}$.
- 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 kernel of the linear mapping $f : V \to W$ is

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

The image is the subset

$$\operatorname{im}(f) = f(V) \subseteq W$$

The kernel and image are vector subspaces of $V$.

## Fixed Points

Given a mapping $f : X \to X$, 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 $f : U \to V$, $f' : U' \to V$ we then produce an vector space isomorphism $U \oplus U' \xrightarrow{\sim} V$.

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

We write $V = U \oplus U'$ and say $V$ is the internal direct sum of $U$ 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 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

$$\operatorname{Hom}_F(V, W) \xrightarrow{\sim} \operatorname{Maps}(B, W)$$
$$f \mapsto f|_B .$$

## 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**

Injective linear mappings always have a left inverse $g: W \to V$ defined $g \circ f = \mathrm{id}_V$.
Surjective linear mapping always have a right inverse $g: W \to V$ defined $f \circ g = \mathrm{id}_W$.

**Rank-Nulity**

Let $f: V \to W$

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

$V$ is finite-dimensional:
- Then $f$ is injective if and only if $\operatorname{dimim} f = \dim V$.
- Then $f$ is surjective if and only if $\dim \ker f = \dim V - \dim W$.

$f$ 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 $m = n$.)

$V, W$ are finite-dimensional with the same dimension:
- $f$ is injective if and only if $f$ is surjective.

**Matrices as Linear Mapppings**

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 $F$ :

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

Each linear mapping $f$ has its representing matrix $\mathrm{M}(f) := [f]$.
The columns of this matrix are the images under $f$ of the standard basis elements of $F^m$

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

**Mat Mul**

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

$$\begin{gathered} \left(A + A'\right) B = AB + A'B \\ A\left(B + B'\right) = AB + AB' \\ IB = B \\ AI = A \\ (AB)C = A(BC). \end{gathered}$$

**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, producing an $(n \times 2n)$-matrix $(A \mid I)$.
- Bring $A$ into Echelon Form, (possibly further to into reduced echelon form: this is the identity matrix. )
- The inverse to $A$ is then what is standing in the right half of the $(n \times 2n)$-matrix.

**Elementary Matrix**

Any square matrix that differs from the identity matrix in at most one entry.
All the elementary matrices with non-zero diagonlas and entries in a field, are invertible.

**Rank**

The column rank of a matrix $A$ is the dimension of the subspace generated by the columns of $A$.
Column and row rank are equal.
TO CALCUALTE: Count the number of non-zero rows in the echelon form of the matrix.

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

**Center of a Group**

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

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

$Z(G)$ is never empty. If $G$ is an abelian group, then $Z(G) = G$.

**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 $\mathcal{B} = (\vec{w}_1, \ldots, \vec{w}_n)$.
U Then each linear mapping $f: V \to W$ has a representing matrix $_{\mathcal{B}}[f]_{\mathcal{A}}$ whose entries $a_{ij}$ are defined

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

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 describes the isomorphism:

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

**Change of Basis**

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

Its entries $(a_{ij})$ are given by the equalities $\vec{v}_j = \sum_{i=1}^{n} a_{ij} \vec{w}_i$.

*Changing between vector spaces:*
Let $V$ and $W$ be finite dimensional vector spaces over $F$ and let $f: V \to W$ be a linear mapping.
Suppose that $\mathcal{A}, \mathcal{A}'$ are ordered basis of $V$ and $\mathcal{B}, \mathcal{B}'$ are ordered bases of $W$. Then

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

*Changing within a vector space*
Let $f$ be the endomorphism $f: V \to V$, we have

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

**Similar Matrices**

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

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

where $T = {}_{\mathcal{A}}[id_V]_{\mathcal{B}}$. We say that $N$ and $M$ are similar matrices.
- Matrices that are similar are equivalent.
- Similar matrices have the same characteristic polynomial.

**Rings**

A ring is a set $R$ equipped with Addition satisfying:
- Commutativity: $a + b = b + a$
- Associativity: $(a + b) + c = a + (b + c)$
- Identity: $\exists 0 \in R$ such that $a + 0 = a$
- Inverse: $\exists -a \in R$ such that $a + (-a) = 0$.

Multiplication satisfying:
- Associativity: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Distributivity: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- Identity: $\exists 1 \in R$ such that $a \cdot 1 = a$

**Units of a Ring**

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

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

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

**Integral Domains**

An integral domain is a non-zero commutative ring with no zero-divisors, then:
- $ab = 0 \Rightarrow a = 0$ or $b = 0$, and
- $a \neq 0$ and $b \neq 0 \to ab \neq 0$
- $ab = ac$ and $a \neq 0 \implies b = c$.

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 $Gx$ 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

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_m X^m$$

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.

**Ring of Polynomials**

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

$$\begin{aligned} &\left(a_0 + a_1 X + \cdots a_m X^m\right) \\ &\qquad + \left(b_0 + b_1 X + \cdots b_n X^n\right) \\ &= \left(a_0 + b_0\right) + \left(a_1 + b_1\right) X + \cdots \end{aligned}$$

and

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

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.
$R$ 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 $\lambda$ is a root of $P(X)$ if and only if $(X - \lambda)$ divides $P(X)$.
Let $R$ be an integral domain. Then $P[X]$ has at most $\deg(P)$ roots in $R$.

**Algebraic Closure**
A field $F$ is algebraically closed if each non-constant polynomial with coefficients in our field has a root in our field $F$.
If $F$ is an algebraically closed field, then every non-zero polynomial 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 re-ordering 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 $x, y \in R$

$$\begin{gathered}f(x+y) = f(x) + f(y) \\ f(xy) = f(x)f(y)\end{gathered}$$

Then:
- $f(0_R) = 0_S$
- $f(-x) = -f(x)$;
- $f(x-y) = f(x) - f(y)$;
- $f(mx) = mf(x)$,
- $f(x^n) = (f(x))^n$

$f$ 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 $ri$, $ir \in I$ i.e. $I$ is closed under multiplication by elements of $R$.

In any ring $R, \{0\}$ and $R$ are ideals of $R$.
The intersection 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 $R$.

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

$$\begin{aligned}{}_R\langle T\rangle = \{r_1t_1 + \cdots + r_mt_m : t_1, \ldots, t_m \in T,& \\ r_1, \ldots, r_m \in R\},&\end{aligned}$$

together with the zero element in the case $T = \emptyset$.
${}_R\langle T\rangle$ is the *smallest* ideal of $R$ that contains $T$.
- Let $m \in \mathbb{Z}$. Then ${}_{\mathbb{Z}}\langle m\rangle = m\mathbb{Z}$.
- Let $P \in \mathbb{R}[X]$. Then ${}_{\mathbb{R}[X]}\langle P\rangle = \{AP : A \in \mathbb{R}[X]\} = \{Q : P \text{ divides } Q \text{ in } \mathbb{R}[X]\}$.

**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 $f : R \to S$ be a ring homomorphism.

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

**Subrings**
Let $R$ be a ring. A subset $R'$ of $R$ is a subring of $R$ if $R'$ itself is a ring under the operations of addition and multiplication defined in $R$.
- It is not true that the intersection of two subrings of $R$ is a subring of $R$.

QUICK CHECK
$R'$ is a subring if and only if
1) $R'$ has a multiplicative identity
2) $R'$ is closed under subtraction:
$a, b \in R' \to a - b \in R'$
3) $R'$ is closed under multiplication.

**Subrings and Homomorphisms**
Let $f : R \to S$ be a Ring Homomorphism.
1) If $R'$ is a subring of $R$ then $f(R') = \operatorname{im} f$ is a subring of $S$.
2) Assume that $f(1_R) = 1_S$. Then if $x$ is a unit in $R, f(x)$ is a unit in $S$ and $(f(x))^{-1} = f(x^{-1})$. In this case $f$ restricts to a group homomorphism $f|_{R^{\times}} : R^{\times} \to S^{\times}$.

**Equivalence Relation**
$\sim$ is an equivalence relation on $X$ when for all elements $x, y, z \in X$ we have:
1) Reflexivity: $x \sim x$;
2) Symmetry: $x \sim y \iff yRx$;
3) Transitivity: $x \sim y, y \sim z \implies x \sim z$.

**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 $x$.
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

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

Each element of $X$ must belong to some equivalence class, impliing the surjection

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

**Well-Defined Mappings**
Given $g : (X/\sim) \to Z$, and $f : X \to Z$.
$g$ is *well-defined* and only if

$$x \sim y \Rightarrow f(x) = f(y)$$

**Cosets of a Ring**
Let $I \trianglelefteq R$ be an ideal in a Ring $R$. A coset of $I$ in $R$ is the set

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

Cosets are also defined by the equivalence relation $x \sim y \Leftrightarrow x - y \in I$.

**Factor Rings**
Let $I \trianglelefteq R$ be an ideal in a ring $R$. $R/I$ is the factor ring of $R$ by $I$

$$R/I = \{r + I \mid r \in R\}$$

It describes is the set of cosets of $R$ with $I$. We have This becomes an ring with

$$\begin{aligned}(x+I) + (y+I) &= (x+y) + N \\ (x+I)\cdot(y+I) &= xy + I\end{aligned}$$

for all $x, y \in R$ with $0 + I$ as the additive identity and $-x + I$ 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 $can : R \to R/I$ sending $r$ to $r + I$ for all $r \in R$ is a surjective ring homomorphism where $I = \ker(can)$.
2) If $f : R \to S$ is has $I \subseteq \ker f$, then there is a unique ring homomorphism $\bar{f} : R/I \to S$ such that $f = \bar{f} \circ can$.

$$\begin{tikzcd} R \arrow[r, "\text{can}"] \arrow[dr, "f"'] & R/I \arrow[d, dashed, "\bar{f}"] \\ & S \end{tikzcd}$$

**First Iso Theorem for Rings**
Let $R$ and $S$ be Rings. Then every $f : R \longrightarrow S$ induces a ring Isomorphism

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

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

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

such that for all $r, s \in R$ and $a, b \in M$

$$\begin{aligned} r(a+b) &= (ra)\dot{+}(rb) \\ (r+s)a &= (ra)\dot{+}(sa) \\ r(sa) &= (rs)a \\ 1_R a &= a \\ 0_R a &= 0_M \\ r0_M &= 0_M \\ (-r)a &= r(-a) = -(ra) \end{aligned}$$

**Direct Sum of Modules**
Given a Ring $R$ and $R$-modules $M_1, \ldots, M_n, M$, the cartesian product $M_1 \times M_2 \times \cdots \times M_n \in M$ when

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

$$r(a_1, \ldots, a_n) = (ra_1, \ldots, ra_n)$$

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 $M$ 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 $M$.

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

is a submodule of $M$
QUICK CHECK
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 $M$ 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

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

**Factor Module**
Let $N$ be a sub-module of a $R$-module $M$. $M/N$ is the factor module of $M$ by $N :=$

$$M/N = \{m + N \mid m \in M\}$$

It describes the set of all cosets of $N$ in $M$.
This becomes an $R$-module with

$$\begin{aligned} (a+N)\dot{+}(b+N) &= (a+b) + N \\ r(a+N) &= ra + N \end{aligned}$$

for all $a, b \in M, r \in R$.
**Universal Property of Factor Modules**
Let $L, M$ be $R$-modules, and $N$ a Submodule of $M$.
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 $N \subseteq \ker f$, then there is a unique homomorphism $\bar{f} : M/N \to L$ such that $f = \bar{f} \circ can$.
**First Isomorphism Theorem for Modules**
Let $M$ and $N$ be $R$-modules. Then every $f : M \longrightarrow N$ 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. This is the same as writing, for any $\sigma \in \mathfrak{S}_n$

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

**Determinant**
The determinant is a mapping from $Mat(n, R) \to R$ where $n = 0 \implies \det(A) = 1$.
*Multilinear Form Characterisation*
Let $F$ be a Field. The mapping

$$\begin{aligned} \det : F^n \times \cdots \times F^n \to F(v_1, \ldots, v_n) \\ \mapsto \det(v_1 | \cdots | v_n) \end{aligned}$$

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.
*Leibniz Characterisation*

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

The sum is over all permutations of $n$.
*Laplace's Expansion of the Determinant*
Let $A = (a_{ij})$. 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

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

where 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 row $i$ and column $j$.
*Multiplicativity*

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

*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 $R$.
*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*

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

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

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

*Notes*
- $\operatorname{rk} A < n \implies \det A = 0$

**Adjugate**
For $A \in Mat(n, R)$ for a commutative ring $R$.

$$\operatorname{adj}(A)_{ij} = C_{ji}$$

where $C_{ji}$ is the $(j, i)$-cofactor.
**EigenStuff**
Let $f : V \to V$ be an endomorphism of an $F$-vector space $V$. A scalar $\lambda \in F$ is an *eigenvalue* of $f$ if and only if there exists a non-zero vector $\vec{v} \in V$ such that $f(\vec{v}) = \lambda\vec{v}$. Each such vector is called an *eigenvector* of $f$ with eigenvalue $\lambda$. For any $\lambda \in F$, the *eigenspace* of $f$ with eigenvalue $\lambda$ is

$$E(\lambda, f) = \{\vec{v} \in V : f(\vec{v}) = \lambda\vec{v}\}$$

*Properties of EigenStuff*
Each endomorphism of a non-zero finite dimensional vector space over an algebraically closed field has an eigenvalue.
Eigenvectors are linearly independent.
**Characteristic Polynomial**

$$\chi_A(x) := \det(xI_n - A)$$

The eigenvalues of the linear mapping $A : F^n \to F^n$ are exactly the roots of the characteristic polynomial $\chi_A$.
A matrix is nilpotent $\iff \chi_A(x) = x^n$
Similar matrices (including transposes !) have the same characteristic polynomial.
The constant term of the characteristic polynomial is $(-1)^n \det A$.
**Triangularisability**
Let $f : V \to V$ be an endomorphism of a finite dimensional $F$-vector space $V$. $f$ is triangularisable if either of the following statements are true

(1) The vector space $V$ has an ordered basis $\mathcal{B}=(\vec{v}_1,\vec{v}_2,\ldots,\vec{v}_n)$ such that

$$\begin{aligned} & f\left(\vec{v}_1\right)=a_{11}\vec{v}_1, \\ & f\left(\vec{v}_2\right)=a_{12}\vec{v}_1+a_{22}\vec{v}_2, \\ & \quad\vdots \\ & f\left(\vec{v}_n\right)=a_{1n}\vec{v}_1+a_{2n}\vec{v}_2+\cdots+a_{nn}\vec{v}_n\in V \end{aligned}$$

(so that the first basis vector $\vec{v}_1$ is an eigenvector, with eigenvalue $a_{11}$ ) or equivalently such that the $n\times n$ matrix ${}_{\mathcal{B}}[f]_{\mathcal{B}}=(a_{ij})$ representing $f$ with respect to $\mathcal{B}$ is upper triangular.
(2) The characteristic polynomial $\chi_f(x)$ of $f$ decomposes into linear factors in $F[x]$.
(3) $A=[f]$ is conjugate to an upper triangular matrix $B$, with $P^{-1}AP=B$ for an invertible matrix $P$.
NOTE: Any endomorphism of a $\mathbb{C}$-vector space is triangularisable.

**Diagonalisability**
An endomorphism $f:V\to V$ of an F-vector space $V$ is diagonalisable if and only if there exists a basis of $V$ consisting of eigenvectors of $f$. If $V$ is finite dimensional then this is the same as saying that there exists an ordered basis $\mathcal{B}=\{\vec{v}_1,\ldots,\vec{v}_n\}$ such that corresponding matrix representing $f$ is diagonal.

**Cayley-Hamilton**
Let $A\in\operatorname{Mat}(n;R)$ be a square matrix on a commutative ring $R$. Then evaluating its characteristic polynomial $\chi_A(x)\in R[x]$ at the matrix A gives zero.

**Inner Product**
Let $V$ be a Vector Space over $\mathbb{R}$. A real inner product on $V$ is a mapping

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

such that 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 Symmetric Bilinear Form, i.e. it is linear in both variables.
- A finite-dimensional real inner product space is a Euclidean Vector Space.
- Every finite dimensional inner product space has an orthonormal basis.
- The stander real inner product is the dot product.

Complex inner products are defined on Vector Spaces over $\mathbb{C}$ and map to $\mathbb{C}$. The differences from a real iner product are if $\lambda,\mu\in\mathbb{C}$ :
2) $(\vec{x},\vec{y})=\overline{(\vec{y},\vec{x})}$
NOTE: A complex inner product is NOT linear in the second variable.
The standard inner product for complex inner product spaces is

$$(\vec{v},\vec{w})=v_1\overline{w_1}+v_2\overline{w_2}+\cdots+v_n\overline{w_n}$$

An inner product space is any vector space endowed with an inner product.

**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

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

**Orthonormal Family and Basis**
A family $(\vec{v}_i)_{i\in I}$ for vectors from an inner product space is an orthonormal family if all the vectors $\vec{v}_i$ have length 1 and if they are pairwise orthogonal to each other

$$(\vec{v}_i,\vec{v}_j)=\delta_{ij}$$

An orthonormal family that is a basis is an orthonormal basis.

**Orthogonality**
Two vectors $\vec{v},\vec{w}$ are orthogonal

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

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 $\vec{w}\in T$.

**Orthogonal Projection**
The orthogonal projection from $V$ onto $U$ is the mapping

$$\pi_U:V\to V$$

that sends $\vec{v}=\vec{p}+\vec{r}$ to $\vec{p}$.
1) $\pi_U$ is a linear mapping with $\operatorname{im}(\pi_U)=U$ and $\ker(\pi_U)=U^{\perp}$.
2) If $\{\vec{v}_1,\ldots,\vec{v}_n\}$ is an Orthonormal Basis of $U$, then $\pi_U$ is given by the following formula for all $\vec{v}\in V$

$$\pi_U(\vec{v})=\sum_{i=1}^{n}(\vec{v},\vec{v}_i)\,\vec{v}_i$$

3) $\pi_U^2=\pi_U$, that is $\pi_U$ is an idempotent.

**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 any $P\in Mat(n,\mathbb{R}$ 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 $\bar{P}^{\top}P=I_n$. i.e. $P^{-1}=\bar{P}^{\top}$.

**Gram-Schmidt Process**
Given an 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 for all $\vec{v}_i$.

**Adjoint Endomorphisms**
Let $V$ be an Inner Product Space. Then $T,T^*:V\to V$ are adjoint if for all $\vec{v},\vec{w}\in V$

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

Any endomorphism always has an adjoint.

**Self-Adjoint**
Let $V$ be an inner product space, $T:V\to V$ is self-adjoint if $T^*=T$. 1) Every eigenvalue of $T$ is real.
2) If $\lambda$ and $\mu$ 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**
$A\in Mat(n,\mathbb{R})$ describes a self-adjoint mapping on the standard inner product space $\mathbb{R}^n$ precisely when $A^{\top}=A$.
$A\in Mat(n,\mathbb{C})$ 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

$$\begin{aligned} R: V\backslash\{\overrightarrow{0}\}\to\mathbb{R} \\ \vec{v}\mapsto R(\vec{v})=\frac{(T\vec{v},\vec{v})}{(\vec{v},\vec{v})} \end{aligned}$$

**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**

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

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

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

**Generilsed Eigenspace**

The generalized eigenspace of $\phi$ with eigenvalue $\lambda_i$, is the subspace of $V$ defined

$$E^{\text{gen}}(\lambda_i, \phi) = \ker(\phi - \lambda_i \,\mathrm{id}_V)^n$$

*Algebraic Multiplicity*

Defined $\dim(E^{\text{gen}}(\lambda_i, \phi))$. Can also be calculated from the the power of the factor of $\chi_A$ for each $\lambda_i$.

*Geometric Multiplicity*

Defined $\dim(E(\lambda_i, \phi)) = \dim(\ker(A - \lambda_i I))$

NOTE: Algebraic multiplicity $\geq$ Geometric multiplicity.

**Bezouts identity for polynomials**

For a characteristic polynomial

$$\chi_\phi(x) = \prod_{i=1}^{s} (x - \lambda_i)^{a_i} \in F[x]$$

where each $a_i$ is a positive integer, $\lambda_i \neq \lambda_j$ for $i \neq j$, and $\lambda_i$ are e.v.s of $\phi$. For each $1 \leq j \leq s$ define

$$P_j(x) = \prod_{\substack{i=1 \\ i \neq j}}^{s} (x - \lambda_i)^{a_i}$$

There exists polynomials $Q_j(x) \in F[x]$ such that

$$\sum_{j=1}^{s} P_j(x) Q_j(x) = 1$$

**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 char. polynomial

$$\chi_\phi(x) = (x - \lambda_1)^{a_1}(x - \lambda_2)^{a_2} \mathinner{..} (x - \lambda_s)^{a_s}$$
$$a_i \geq 1, \sum_{i=1} a_i = n$$

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 $\phi$ with respect to the block $\mathcal{B}$ is block diagonal with Jordan blocks on the diagonal,

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

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

$$a_i = r_{i_1} + r_{i_2} + \cdots + r_{im_i} \quad (1 \leq i \leq s)$$

**Building JNF**

Algebraic multiplicty denotes the size of Jordan Blocks. Geometric multiplicty denotes the number of boxes in each block. If $\alpha_i > 3$ then we must calculate the generilised eigenspaces to find the size of each box.

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

**Euler Identity** $e^{iz} = \cos z + i \sin z$

**Rotation Matrix**

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

**Disciminant**

$b^2 - 4ac$

$> 0$: two distinct real roots.

$= 0$: exactly one real root.

$< 0$: no real roots.

**Mod**

- $\mathbb{Z}/m\mathbb{Z}$ is a ring.
- $\bar{a} = a + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ is a congruence class.
- $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$
- $|\mathbb{Z}/m\mathbb{Z}| = m$
- $\bar{a} + \bar{b} = \overline{a+b}$
- $\bar{a} \cdot \bar{b} = \overline{ab}$
- $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if $m$ is prime.

**Symmetric Group**

$\mathfrak{S}_n$ := all permutations of the set $\{1, 2, \ldots, n\}$ under composition. It has $n!$ elements.

A *transposition* is a permutation that only swaps two elements with $l(\sigma) = 2|j - i| - 1$

An *inversion* is a pair $(i, j)$ such that $1 \leqslant i < j \leqslant n$ and $\sigma(i) > \sigma(j)$.

Lenght is the number of inversions in a permutation. (i.e. number of crossings in a diagram)

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

**Matrix Stuff**

- $(AB)^T = B^T A^T$
- $\mathrm{tr}(cA) = c\,\mathrm{tr}(A)$ for a scalar $c$.
- $\mathrm{tr}(ABC) = \mathrm{tr}(BCA) = \mathrm{tr}(CAB)$.
- Similar matrices have the same trace.
- $\overline{(\mathrm{A}+\mathrm{B})} = \overline{\mathrm{A}} + \overline{\mathrm{B}}$
- $\overline{(\mathrm{AB})} = \overline{\mathrm{B}} \cdot \overline{\mathrm{A}}$
- $\overline{(\mathrm{kA})} = \mathrm{k} \cdot \overline{\mathrm{A}}.$

**Counter Examples**

- Ring of real quaternions are a division ring
- $(\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\}$, which is not cyclic

**Trig.**

- $\sin(\theta \pm \phi) = \sin\theta\cos\phi \pm \cos\theta\sin\phi$
- $\cos(\theta \pm \phi) = \cos\theta\cos\phi \mp \sin\theta\sin\phi$
- $\tan(\theta \pm \phi) = \frac{\tan\theta \pm \tan\phi}{1 \mp \tan\theta\tan\phi}$
- $\sin(2\theta) = 2\sin\theta \cdot \cos\theta$
- $\cos(2\theta) = \cos^2\theta - \sin^2\theta$
- $\tan(2\theta) = \frac{2\tan\theta}{1 - \tan^2\theta}$
- $\sin\theta + \sin\phi = 2\sin\left(\frac{\theta+\phi}{2}\right)\cos\left(\frac{\theta-\phi}{2}\right)$
- $\sin\theta - \sin\phi = 2\cos\left(\frac{\theta+\phi}{2}\right)\sin\left(\frac{\theta-\phi}{2}\right)$
- $\cos\theta + \cos\phi = 2\cos\left(\frac{\theta+\phi}{2}\right)\cos\left(\frac{\theta-\phi}{2}\right)$
- $\cos\theta - \cos\phi = -2\sin\left(\frac{\theta+\phi}{2}\right)\sin\left(\frac{\theta-\phi}{2}\right)$
- $\sin\theta\sin\phi = \frac{[\cos(\theta-\phi) - \cos(\theta+\phi)]}{2}$
- $\cos\theta\cos\phi = \frac{[\cos(\theta-\phi) + \cos(\theta+\phi)]}{2}$
- $\sin\theta\cos\phi = \frac{[\sin(\theta+\phi) + \sin(\theta-\phi)]}{2}$
- $\cos\theta\sin\phi = \frac{[\sin(\theta+\phi) + \sin(\theta-\phi)]}{2}$