Algebra Formula Sheet

William Bevington

Chapter One - Vector spaces

Definition. A **field** F is a set with functions $+$ and $\times$ such that $G_+ := (F,+)$ and $G_\times := (F \setminus \{0_F\}, \times)$ are abelian groups with $\mathrm{id}_{G_\times} = 1_F$, $\mathrm{id}_{G_+} := 0_F$ and for $\lambda, \mu, \nu \in F$ we have that $\lambda(\mu+\nu) = \lambda\mu + \lambda\nu$.

Definition. A **vector space** V over a field F is a pair $(V, \dot{+})$ where V is a set and $\dot{+} : F \times V \to V : (\lambda, \vec{v}) \mapsto \lambda\vec{v}$ is a map where for $\lambda, \mu \in F$ and $\vec{u}, \vec{v} \in V$:

- $\lambda(\vec{u}+\vec{v}) = \lambda\vec{u} + \lambda\vec{v}$,
- $\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$,
- $(\lambda+\mu)\vec{v} = \lambda\vec{v} + \mu\vec{v}$,
- $1_F\vec{v} = \vec{v}$.

Theorem (1.2.2)**.** *If V is a vector space and $\vec{v} \in V$, then $0\vec{v} = \vec{0}$.*

Proof. $0\vec{v} = (0+0)\vec{v} = 0\vec{v} + 0\vec{v} \Rightarrow \vec{0} = 0\vec{v}$. □

Definition. A subset $U \subseteq V$ of a vector space V is a **vector subspace** if U contains $\vec{0}$ and $\vec{u}, \vec{v} \in U, \lambda \in F \Rightarrow \vec{u}+\vec{v} \in U$ and $\lambda\vec{u} \in U$.

Theorem. *Let $T \subseteq V$, then $\langle T \rangle := \{\sum_{\alpha_i \in F} \alpha_i \vec{v}_i : \vec{v}_i \in T\}$ is a subspace of V. If $V = \langle T \rangle$ then T is a* ***generating set*** *of V.*

Definition. A subset L of a vector space V is **linearly independent** if for all pairwise different vectors $\vec{v}_1, \dots, \vec{v}_r \in L$ and arbitrary scalars $\alpha_1, \dots, \alpha_r \in F$, we have that $\alpha_1\vec{v}_1 + \cdots + \alpha_r\vec{v}_r = \vec{0} \implies \forall i : \alpha_i = 0$.

Definition. A **basis** of a vector space V is a linearly independent generating set of V.

Theorem (1.5.11)**.** *Let V be a vector space over a field F and $\vec{v}_1, \dots, \vec{v}_r \in V$ vectors. The family $(\vec{v}_i)_{1 \le i \le r}$ is a basis of V if and only if $\phi : F^r \to V : (\alpha_1, \dots, \alpha_r) \mapsto \sum_{i=1}^r \alpha_i \vec{v}_i$ is a bijection.*

Proof. $(\vec{v}_i)_{1 \le i \le r}$ is a generating set $\Leftrightarrow \phi$ is a surjection $F^r \to V$. $(\vec{v}_i)_{1 \le i \le r}$ is linearly independent $\Leftrightarrow \phi$ is a injection $F^r \to V$. $(\vec{v}_i)_{1 \le i \le r}$ is a basis $\Leftrightarrow \phi$ is a bijection $F^r \to V$. □

Theorem (1.5.13)**.** *Let V be a finitely generated vector space over a field F, then V has a basis.*

Theorem. *If V is a vector space, $L \subset V$ a linearly independent subset and $E \subseteq V$ a generating set, then $|L| \le |E|$.*

Theorem (1.6.1)**.** *The* ***Fundamental estimate of linear algebra*** *gives that if L is a linearly-independent set of vectors in V and E is a generating set $V = \langle E \rangle$ then $|L| \le |E|$.*

Theorem (Exchange Lemma)**.** *Let $M \subseteq E \subseteq V$ be such that M is linearly independent and $V = \langle E \rangle$. If $\vec{w} \in V \setminus M$ is such that $M \cup \{\vec{w}\}$ is linearly independent, then $\exists \vec{e} \in E \setminus M$ such that $V = \langle (E \setminus \{\vec{e}\}) \cup \{\vec{w}\} \rangle$. Thus* ***any two bases for V must have the same cardinality****.*

Definition. The **dimension** of a vector space V is the cardinality of any basis of V (by the exchange-lemma this is independent of choice of basis).

Theorem (The Dimension Theorem)**.** *Let V be a vector space with subspaces $U, W \subseteq V$. Then $\dim(U+V) + \dim(U \cap V) = \dim(U) + \dim(V)$.*

Proof. Choose a basis $\vec{s}_1, \dots, \vec{s}_d$ of $U \cap W$ and extend it by the elements $\vec{u}_1, \dots, \vec{u}_r \in U$ to a basis of U and then by the elements $\vec{w}_1, \dots, \vec{w}_t \in W$ to a basis of $U+W$. Then show that $\{\vec{s}_1, \dots, \vec{s}_d, zvecw_1, \dots, \vec{w}_t\}$ is a basis of W. It's linearly independent by construction, so show that it's generating. □

Definition. A mapping $f : V \to W$ between vector spaces V, W is **linear** iff $\forall \vec{u}, \vec{v} \in V : f(\vec{u}+\vec{v}) = f(\vec{u}) + f(\vec{v})$ and $\forall \lambda \in F : f(\lambda\vec{v}) = \lambda f(\vec{v})$. If f is bijective then it's an **isomorphism**, if $V = W$ then f is an **endomorphism** and if both of these hold then f is an **automorphism**.

Theorem. *Let $n \in \mathbb{N}$ and V be vector space over a field F, then V is isomorphic to F^n iff $\dim(V) = n$.*

Theorem (1.7.8)**.** *Let V, W be vector spaces over F and let $B \subset V$ be a basis. Then $\mathrm{Hom}(V,W) \xrightarrow{\sim} \mathrm{Maps}(B,W) : f \mapsto f|_B$.*

Theorem (1.7.9)**.** *Let $f : V \to W$ be a linear map. If f is injective then it has a left inverse, if f is surjective then it has a right inverse.*

Definition. Let $f : U \to V$ be linear. The **image** of f is $\mathrm{im}(f) := f(U) = \{\vec{v} \in V : \exists \vec{u} \in U, \vec{v} = f(\vec{u})\}$. The **kernel** of f is the pre-image $\ker(f) := f^{-1}(\vec{0})$. We have $\mathrm{im}(f) \subseteq V$ and $\ker(f) \subseteq U$ are subspaces.

Theorem (1.8.2)**.** *A linear mapping $f : V \to W$ is injective if and only if its kernel is zero.*

Theorem (Rank-Nullity)**.** *Let $f : V \to W$ be a linear mapping between vector spaces. Then $\dim(V) = \dim(\ker(f)) + \dim(\mathrm{im}(f))$.*

Chapter Two - Linear mappings

Theorem (2.1.1)**.** *Let F be a field and $m, n \in \mathbb{N}$ then there is a bijection $\mathrm{Hom}_F(F^m, F^n) \to \mathrm{Mat}(m \times n; F) : f \to [f]$ associating a matrix to every linear mapping.*

Definition. The **matrix product** is defined for $A \in \mathrm{Mat}(m \times l; F)$, $B \in \mathrm{Mat}(l \times n)$ as

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

Theorem. *The composition of linear maps is the product of their matricies; $[f \circ g] = [f][g]$.*

Definition. A matrix $M \in \mathrm{Mat}(n \times n; F)$ is **invertible** if there exist matricies $A, B \in \mathrm{Mat}(n \times n; F)$ with $AM = MB = \mathbb{I}$.

Theorem. *The set of invertible matricies form a* ***group*** *$GL(n;F) := \mathrm{Mat}(n;F)^\times$.*

Definition. A square matrix $M \in \mathrm{Mat}(n;F)$ is **elementary** if it differs from the identity by at most one entry.

Theorem (2.2.3)**.** *Every square matrix can be written as a product of elementary matricies.*

Definition. A matrix is in **Smith-normal form** if it has either a one or zero on the diagonal entries and zeros everywhere else. (2.2.5) every matrix M has invertible P, Q such that PMQ is in Smith-normal form.

Definition. The **column rank** (resp. **row rank**) of a matrix M is the dimension of the span of the coloumns (resp rows) of A.

Theorem (2.2.7)**.** *For any matrix, the column and row ranks are equal.*

Definition. Let F be a field with V, W vector-spaces over F with ordered bases $\mathscr{A} = (\vec{v}_1, \dots, \vec{v}_m)$ and $\mathscr{B} = (\vec{u}_1, \dots, \vec{u}_n)$ respectively. Then the **representing matrix** ${}_{\mathscr{B}}[f]_{\mathscr{A}} = [a_{ij}]$ with

$$a_{ij} = f(\vec{v}_j) := a_{1j}\vec{u}_1 + \cdots + a_{nj}\vec{u}_n.$$

Theorem (2.3.4)**.** *Let V, W be vector-spaces over F with bases $\mathscr{A}, \mathscr{B}$ respectively and $f \in \mathrm{Hom}(V,W)$. Then ${}_{\mathscr{B}}[f(\vec{v})] = {}_{\mathscr{B}}[f]_{\mathscr{A}} \circ {}_{\mathscr{A}}[\vec{v}]$.*

Theorem (2.4.4)**.** *Let $f \in \mathrm{Hom}(V,V)$ be an endomorphism and $\mathscr{A}, \mathscr{A}'$ be bases of V. Then the* ***change of basis*** *formula is ${}_{\mathscr{A}'}[f]_{\mathscr{A}'} = {}_{\mathscr{A}}[id_V]^{-1}_{\mathscr{A}'}\, {}_{\mathscr{A}}[f]_{\mathscr{A}}\, {}_{\mathscr{A}}[id_V]_{\mathscr{A}'}$.*

Chapter Three - Rings and modules

Definition. A **ring** is a set with two operations $(R,+,\cdot)$ such that

- $(R,+)$ is an abelian group,
- $(R,\cdot)$ is a **monoid** (associative with identity),
- $\cdot$ distributes over $+$; $a\cdot(b+c)\cdot d = a\cdot b\cdot d + a\cdot c\cdot d$.

Definition. A **field** is a commutative ring with inverses.

Theorem (3.1.11)**.** *The ring $\mathbb{Z}/m\mathbb{Z}$ is a field iff m is prime.*

Definition. An element $a\in R$ for a ring R is a **unit** if it is invertible. We define $R^\times$ as the **group of units**.

Definition. An element $a\in R$ for a ring R is a **zero-divisor** if $\exists b\in R$: $b\neq 0$ and $ab=0$ or $ba=0$.

Definition. An **integral domain** is a non-zero commutative ring with no zero-divisors.

Theorem. *If I is an integral domain then $ab=0 \implies a=0$ or $b=0$. Moreover (3.2.16), if $ab=ac$ and $a\neq 0$ then $b=c$.*

Theorem (3.2.18)**.** *Every finite integral domain is a field.*

Definition. The **ring of polynomials** with coefficients in a ring R is denoted $R[X]$.

Theorem (3.3.3)**.** *If R is a ring with no zero-divisors then $R[X]$ has no zero-divisors and* $\deg(PQ)=\deg(P)+\deg(Q)$. *If R is an integral domain then so is $R[X]$.*

Theorem (3.3.4)**.** *Let R be an integral domain with $P,Q\in R[X]$ with $Q(X)$ **monic** (leading term has coefficient one). Then $\exists! A,B\in R[X]$: $P=AQ+B$ with* $\deg(B)<\deg(Q)$ *or $B=0$.*

Definition. The **evaluation** of $P\in R[X]$ at $\lambda\in R$ is $P(\lambda)$, the image of $\varepsilon : R[X]\to \mathrm{Maps}(R,R)$. Then λ is a **root** if $P(\lambda)=0$.

Theorem (3.3.9)**.** *Let R be a commutative ring, then $\lambda\in R$ is a root of $P\in R[X]$ iff $(X-\lambda)$ divides $P(X)$.*

Theorem (3.3.10)**.** *If $P\in R[X]$ then P has at most* $\deg(P)$ *roots in R.*

Definition. A field is **algebraically closed** if every non-constant polynomial has a root.

Theorem. *The **fundamental theorem of algebra** is that $\mathbb{C}$ is algebraically closed.*

Theorem (3.3.14)**.** *If F is an algebraically closed field then any non-zero polynomial $P(X)\in F[X]$ can be decomposed into linear factors; $P(X)=c(X-\lambda_1)\dots(X-\lambda_n)$.*

Definition. Let R and S be rings, then $f:R\to S$ is a **ring homomorphism** if $\forall x,y\in R : f(x+y)=f(x)+f(y)$ and $f(xy)=f(x)f(y)$.

Theorem (3.4.5)**.** *Let $f\in \mathrm{Hom}(R,S)$ be a ring-homomorphism. Then $f(0_R)=0_S$, $f(-x)=-f(x)$ and $f(x-y)=f(x)-f(y)$.*

Definition. A subset of a ring $\emptyset\neq I\subseteq R$ is an **ideal** of R if I is closed under subtraction and $\forall i\in I, r\in R : ir, ri\in I$.

Definition. The **ideal generated by a subset** $T\subseteq R$ is ${}_R\langle T\rangle := \{r_1t_1+\dots r_nt_n : \forall i\, r_i\in R$ and $t_i\in T\}$. It is the *smallest* ideal of R that contains T (prop 3.4.14).

Definition. An ideal I is a principle ideal if it's generated by one element, $I=\langle t\rangle$.

Theorem. *The **subring test** gives that $R'\subset R$ is a subring of R iff*

- *R' has a multiplicative identity*
- *R' is closed under subtraction*
- *R' is closed under scaler multiplication*

Theorem (2.4.29)**.** *If $f:R\to S$ is a ring homomorphism then $im(f)$ is a subring of S. Further, if $f(1_R)=1_S$ and x is a unit in R then $f(x^{-1})=f(x)^{-1}$, so f restricts to the group homomorphism $f^\times : R^\times\to S^\times$.*

Definition. A relation $\sim$ is an **equivalence relation** iff

- $\sim$ is Reflexive; $x\sim x$
- $\sim$ is Symmetric; $x\sim y \implies y\sim x$
- $\sim$ is transitive; $(x\sim y$ *and* $y\sim z) \implies x\sim z$.

Definition. If $\sim$ is an equivalence relation then the **equivalence class** of x is $E(x):=\{y : x\sim y\}$.

Definition. The **set of equivalence classes** is $(X/\sim)\subseteq \mathscr{P}(X)$, with **canonical map** can $: X\to (X/\sim), x\mapsto E(x)$.

$$\begin{tikzcd} X \arrow[r, "\mathrm{can}"] \arrow[dr, "f"'] & (X/\sim) \arrow[d, dashed, "\overline{f}"] \\ & Z \end{tikzcd}$$

A map $g:(X/\sim)\to Z$ is **well-defined** if $\exists f : X\to Z$ such that $x\sim y \implies f(x)=f(y)$ and f restricts to g.

Definition. Let I be an ideal of R, then the **coset of** I is $x+I:=\{x+i : i\in I\}$.

Definition. Let I be an ideal of R and $\sim$ be defined by $x\sim y\Leftrightarrow x-y\in I$ then $R/I=(R/\sim)$ is the **factor/quotient ring of** R **by** I.

Theorem. *The **first isomorphism theorem** is that for rings R,S we have $\forall f\in \mathrm{Hom}(R,S) : \overline{f} : R/\ker f\tilde{o}im(f)$.*

Definition. A **(left) module over R** is a pair $(M,\dot{+})$ and mapping $R\times M\to M, (r,a)\to ra$ such that for $a,b\in M$ and $r,s\in R$:

- $r(a\dot{+}b)=(ra)\dot{+}(rb)$,
- $(r+s)a=(ra)\dot{+}(sa)$,
- $r(sa)=(rs)a$, and
- $1_Ra=a$.

Theorem (3.7.8)**.** *If M is an R-module then $\forall a\in M : 0_Ra=0_M$, $\forall r\in R : r0_M=0_M$ and $(-r)a=r(-a)=-(ra)$.*

Theorem (3.7.21)**.** *Let M,N be R-modules with $f\in \mathrm{Hom}(M,N)$, then* $\ker f$ *is a sub-module of M and $im(f)$ is a sub-module of N. Moreover (3.7.22) f is injective iff* $\ker f=\{0_M\}$.

Theorem (3.7.29)**.** *The intersection of any collection of sub-modules of M is a sub-module of M.*

Definition. Let N be a sub-module of M. The set $a+N:=\{a+b : b\in N\}$ is the **coset of** M **by** N, which defines the **quotient** $(M/\sim)$.

Theorem. *Let R be a ring with L,M being R-modules and $N\subseteq M$ a sub-module of M. The canonical map can $: M\to M/N$ is a surjective R-homomorphism with kernel N, and if $f(N)=\{0_L\}$ (i.e. $N\subseteq\ker f$) then $\exists!\overline{f} : M/N\to L$ such that $f=\overline{f}\circ$ can.*

Theorem. *The **First Isomorphism Theorem**. Let R be a ring with modules M and N, then $\forall f\in \mathrm{Hom}(M,N)$ there is an R-isomorphism*

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

Chapter Four - Determinants and eigenvalues

Definition. The **permutation group** $\mathfrak{S}_n$ is the group of all bijections $\{1,\dots,n\} \to \{1,\dots,n\}$.

Definition. An **inversion** of a permutation $\sigma \in \mathfrak{S}_n$ is a pair (i,j) with $1 \le i < j \le n : \sigma(i) > \sigma(j)$. The **length** of σ is

$$l(\sigma) := |\{(i,j) : 1 \le i < j \le n, \sigma(i) > \sigma(j)\}|,$$

and the **sign of** σ is the group-homomorphism $\operatorname{sgn}(\sigma) = (-1)^{l(\sigma)}$ whose kernel is the **Alternating group** A_n. If $\operatorname{sgn}(\sigma) = +1$ then σ is an **even** permutation.

Definition. Let R be a commutative ring and $n \in \mathbb{N}$. The **determinant** $\det : \operatorname{Mat}(n \times n; R) \to R$ is given by

$$\det([a_{ij}]) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}.$$

Definition. Let U,V,W be F-vector spaces. A **bilinear form** on $U \times V$ is a mapping $H : U \times V \to W$ such that $\forall \vec{u}_1, \vec{u}_2 \in U,\ \vec{v}_1, \vec{v}_2 \in V,\ \lambda \in F$:

- $H(\vec{u}_1 + \vec{u}_2, \vec{v}_1) = H(\vec{u}_1, \vec{v}_1) + H(\vec{u}_2, \vec{v}_1)$,
- $H(\lambda \vec{u}_1, \vec{v}_1) = \lambda H(\vec{u}_1, \vec{v}_1)$,
- $H(\vec{u}_1, \vec{v}_1 + \vec{v}_2) = H(\vec{u}_1, \vec{v}_1) + H(\vec{u}_1, \vec{v}_2)$,
- $H(\vec{u}_1, \lambda \vec{v}_1) = \lambda H(\vec{u}_1, \vec{v}_1)$.

A bilinear form is **symmetric** if $U = V : \forall \vec{u}, \vec{v} \in U : H(\vec{u}, \vec{v}) = H(\vec{v}, \vec{u})$ and is **anti-symmetric** if $\forall \vec{u} \in U : H(\vec{u}, \vec{u}) = 0 \Leftrightarrow H(\vec{u}, \vec{v}) = -H(\vec{v}, \vec{u})$.

Definition. A mapping $H : V_1 \times \dots \times V_n \to W$ is a **multilinear form** if it's linear in each entry. It's **alternating** if $H(\dots, \vec{u}, \dots, \vec{u}, \dots) = 0$.

Theorem (4.3.6)**.** *Let F be a field. The mapping $\det : \operatorname{Mat}(n; F) \to F$ which is an alternating, multilinear form on $[a_{1i}| \dots |a_{ni}]$ with $\det(\mathbb{I}) = 1_F$ is unique.*

Theorem (4.4.1,4.4.4)**.**

$$\det(AB) = \det(A)\det(B) \quad \textit{and} \quad \det(A^T) = \det(A).$$

Definition. Let $A \in \operatorname{Mat}(n; R)$ where R is a commutative ring. 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 A with the i^{th} row and j^{th} column removed.

Theorem (4.4.7)**.**

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

Theorem (4.4.9)**.** *The **adjugate matrix** is $\operatorname{adj}(A)_{ij} = C_{ji}$ for cofactor matrix C of A. Then **Cramer's Rule** is that*

$$A \cdot \operatorname{adj}(A) = \det(A)\mathbb{I}_n.$$

Theorem (4.4.11)**.** *A matrix A is **invertible** iff $\det(A) \neq 0$.*

Definition. If V is an F-vector space then $\lambda \in V$ is an **eigenvalue** of $f \in \operatorname{End}(V)$ if $\exists \vec{v} \in V : f(\vec{v}) = \lambda \vec{v}$.

Theorem (4.5.4)**.** *If $f \in \operatorname{End}(V)$ for V over F which is algebraically closed, then f has eigenvalues.*

Definition. Let R be a commutative ring, the **characteristic polynomial** of $f \in \operatorname{End}(V)$ is

$$\chi_f(x) = \det([f] - x\mathbb{I}).$$

Theorem (4.5.1)**.** *The roots of the characteristic polynomial of $f \in \operatorname{End}(V)$ are exactly the eigenvalues of f.*

Theorem (4.6.1)**.** *Let $f \in \operatorname{End}(V)$ then V has an ordered basis $\mathscr{B} = \{\vec{v}_1, \dots \vec{v}_n\}$ with*

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

*if and only if $\chi_f(x)$ decomposes into linear factors. We say f is **triangularisable**.*

Definition. A mapping $f \in \operatorname{End}(V)$ is **diagonalisable** if there exists a basis of V consisting of eigenvectors of f.

Theorem (4.6.8)**.** *If $f \in \operatorname{End}(V)$ has $\dim(V)$ distinct eigenvalues then the corresponding eigenvectors are linearly independent.*

Theorem (Perran-Frobeneous)**.** *Let $M \in \operatorname{Mat}(n; \mathbb{R})$ be a markov matrix with positive entries, then the eigenspace $E(1, M)$ is one-dimensional with a basis vector $\vec{v}$ such that $\sum_{i=1}^{n} v_i = 1$ (which is unique).*

Chapter Five - Inner product spaces

Definition. Let V be a vector space over $\mathbb{R}$, an **iner product** of V is a mapping

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

such that $\forall \vec{u}, \vec{v}, \vec{w} \in V$:

- $(\lambda \vec{u} + \mu \vec{v}, \vec{w}) = \lambda(\vec{u}, \vec{w}) + \mu(\vec{v}, \vec{w})$,
- $(\vec{u}, \vec{v}) = (\vec{v}, \vec{u})$,
- $(\vec{u}, \vec{u}) \geq 0$ with equality iff $\vec{u} = \vec{0}$.

Definition. Let V be a vector space over $\mathbb{C}$, an **iner product** of V is a mapping

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

such that $\forall \vec{u}, \vec{v}, \vec{w} \in V$:

- $(\lambda \vec{u} + \mu \vec{v}, \vec{w}) = \lambda(\vec{u}, \vec{w}) + \mu(\vec{v}, \vec{w})$,
- $(\vec{u}, \vec{v}) = \overline{(\vec{v}, \vec{u})}$,
- $(\vec{u}, \vec{u}) \geq 0$ with equality iff $\vec{u} = \vec{0}$.

Definition. If $(\vec{u}, \vec{v}) = 0$ then we say $\vec{u}$ and $\vec{v}$ are **orthogonal** and write $\vec{u} \perp \vec{v}$.

Definition. Let V be an inner-product space, then the **length** or **norm** of a vector $\vec{v} \in V$ is

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

Definition. A family of vectors $(\vec{v}_i)_{i \in I}$ is an **orthonormal family of vectors** if $(\vec{v}_i, \vec{v}_j) = \delta_{ij}$.

Theorem (5.1.10)**.** *Every finite-dimensional inner-product space has an orthonormal basis.*

Definition. Let V be an inner-product space with subset $T \subseteq V$, the **orthogonal set to** T is $T^{\perp} = \{\vec{v} \in V : \vec{v} \perp \vec{u} \text{ for all } \vec{u} \in T\}$.

Theorem (5.2.2)**.** *Let U be a subspace of V, then U and $U^{\perp}$ are complementary; $U^{\perp} = V \setminus U$ and $V = U \otimes U^{\perp}$.*

Definition. Let U be a subspace of inner-product space V, then the **orthogonal projection from** V **onto** U is

$$\pi_U : V \to U, \vec{v} = \vec{p} + \vec{r} \mapsto \vec{p}.$$

Theorem (5.2.5)**.** *This is the **Cauchy-Schwarz inequality**:*

$$|(\vec{u}, \vec{v})| \leq ||\vec{u}|| \cdot ||\vec{v}||.$$

Theorem (5.2.6)**.** *Let V be a normed inner-product space, $\vec{v} \in V$:*

- $||\vec{v}|| \geq 0$ *with equality iff* $\vec{v} = \vec{0}$,
- $||\lambda \vec{v}|| = |\lambda| \cdot ||\vec{v}||$,
- $||\vec{u} + \vec{v}|| \leq ||\vec{u}|| + ||\vec{v}||$.

Definition. Let V be an inner-product space, then $T, S \in \mathrm{End}(V)$ are **adjoint** if for all $\vec{u}, \vec{v} \in V$:

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

We write $S = T^*$ and say that S **is the adjoint of** T.

Theorem (5.3.4)**.** *Let $T \in \mathrm{End}(V)$, then T has an adjoint.*

Definition. Let $T \in \mathrm{End}(V)$, then T is **self-adjoint** if $T^* = T$.

Theorem (5.3.7)**.** *Let $T\mathrm{End}(V)$ be self-adjoint, then*

- *Every eigenvalue of T is real,*
- *T has at least one eigenvalue,*
- *if the eigenvalues are distinct then the eigenvectors are orthogonal.*

Theorem (Spectral)**.** *Let V be a finite-dimensional inner-product space and $T \in \mathrm{End}(V)$ be self-adjoint, then V has an orthonormal basis consisting of eigenvectors of T.*

Definition. A matrix P is **orthogonal** if $P^{-1} = P^T$.

Theorem (Spectral II)**.** *Let $A \in \mathrm{Mat}(n; \mathbb{R})$ be symmetric. Then there is an orthogonal matrix $P \in \mathrm{Mat}(n; \mathbb{R})$ such that $P^T AP$ is diagonal with entries being eigenvalues of A.*

Definition. A matrix $A \in \mathrm{Mat}(n; \mathbb{C})$ is **unitary** if $P^{-1} = \overline{P}^T$.

Theorem (Spectral III)**.** *Let $A \in \mathrm{Mat}(n; \mathbb{C})$ be hermitian ($A = \overline{A}^T$). Then there is a unitary matrix $P \in \mathrm{Mat}(n; \mathbb{C})$ such that $\overline{P}^T AP$ is diagonal with entries being eigenvalues of A.*

Chapter Six - Jordan normal form

1. Calculate the eigenvalues $\lambda_1, \ldots, \lambda_s$ along with geometric $\mu_1, \ldots, \mu_s$ and algebraic $m_1, \ldots, m_s$ multiplicities,
2. Compute corresponding eigenspaces
$$E_\lambda^k = \{\vec{v} \in V : (A - \mathbb{I}\lambda)^k \vec{v} = 0\}.$$
3. Compute the following, and draw the chart on the right:
$$d_1 = \dim(E_\lambda^1) \qquad \underbrace{\square\square\square\square\square}_{d_1 \text{ boxes}}$$
$$d_2 = \dim(E_\lambda^2) - \dim(E_\lambda^1) \qquad \underbrace{\square\square\square\square}_{d_2 \text{ boxes}}$$
$$\vdots \qquad\qquad \vdots$$
$$d_k = \dim(E_\lambda^k) - \dim(E_\lambda^{k-1}) \qquad \underbrace{\square\square\square}_{d_k \text{ boxes}}$$
4. Start at the bottom of the diagram, filling row k with the linearly independent eigenvectors in E_λ^k which **are not in** E_λ^{k-1}. Each time you fill in a box with a vector $\vec{v}_k$, fill in every box above with the vectors $\vec{v}_{k+1} = (A - \mathbb{I}\lambda)^k \vec{v}$ until you reach the top.
5. Repeat steps two to four with different eigenvalues until the diagram is full. Then Q is the matrix whose columns are the top-left vector followed by the vectors below it so the Jordan-normal form is $J = Q^{-1}AQ$.
6. In fact you **needn't calculate** Q. Each column of the diagram is a Jordan block - easy!

Examples

- **Integral domain that isn't a field:** $\mathbb{Z}$.
- **Commutative ring that isn't an integral domain:** $\mathbb{Z}_4$.
- **A ring with infinitely many units:** $\mathrm{Mat}(2;\mathbb{Z})$.
- **A non-diagonalizable complex matrix:** $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
- **A non-zero linear map defined for any vector space** $\vec{v} \mapsto 2\vec{v}$.
- **Symmetric billinear form, not an inner-product:** $u_1 u_2$.

Matrix representation for linear maps

Let $f \in \mathrm{Hom}(V,W)$ be a linear map and $\mathscr{A}, \mathscr{B}$ be a bases of V and W respectively. Then:

$$\begin{aligned} [\mathrm{id}]_{\mathscr{B}} &= \left[\, \vec{b}_1 \mid \dots \mid \vec{b}_n \,\right] \qquad \text{where each } \vec{b}_j \in \mathscr{B} \\ {}_{\mathscr{A}}[f] &= \left[f(\vec{a}_1) \,|\, \dots \,|\, f(\vec{a}_n) \right] \qquad \text{where each } \vec{a}_j \in \mathscr{A}. \end{aligned}$$

- **A non-symmetric bilinear form:** $u_1 v_2 - u_2 v_1$.
- **An inner product on** $\mathbb{C}$: $((z_1, w_1), (z_1, w_1) \mapsto z_1 \overline{z_2} + w_1 \overline{w_2}$. A corresponding **self-adjoint operator** is $id : \vec{v} \mapsto \vec{v}$ and a **non self-adjoint** one is $(z,w) \mapsto (iz, w)$.
- **A linear mapping defined without a matrix** is $\frac{d}{dx}$.
- **An idempotent operator** is one such that $x \cdot x = x$.
- **To check if $\mathscr{B}$ is a basis:** just check whether the matrix with the elements of $\mathscr{B}$ as its columns has non-zero determinant.
- **A non-commutative ring in which all non-zero elements are invertable:** Quarternions.

Useful definitions

Definition. Let X be a set and F be a field, then the set $\mathrm{Maps}(X,F)$ is a vector-space over F. We define the **free vector space** as the sub-space $F\langle X \rangle \subseteq \mathrm{Maps}(X,F)$ which sends all but finitely many elements of X to zero.

Definition. The **direct sum** of vector spaces $V_1, \dots, V_n, W$ and linear maps $f_i : V_i \to W$ is the set $V_1 \oplus V_2 \oplus \cdots \oplus V_n$ giving the linear map

$$f : V_1 \oplus \cdots \oplus V_n \to W,\ f(a_1 \vec{v}_1 + \cdots + a_n v_n) := a_1 f_1(v_1) + \cdots + a_n f_n(\vec{v}_n).$$