

18.700 Linear Algebra - Fall 2006

Topics treated in each class

1. Thursday, 9/7

- Examples of \mathbb{R}^2 , \mathbb{R}^3 , \mathbb{R}^n
- Operations on \mathbb{R}^2 , \mathbb{R}^3 , \mathbb{R}^n
- Definition of vector space over \mathbb{R}
- Examples of $\mathbb{R}[t]$, $\mathbb{R}[t]_{\leq d}$
- Properties of \mathbb{R} and examples of \mathbb{Q} and \mathbb{C}
- *Definition of field* and example of $\mathbb{Q}(i)$
- *Definition of vector space V over a field \mathbb{F}*
- Example of $\mathbb{Q}[t]$ as \mathbb{Q} -vector space, \mathbb{C} as \mathbb{R} -vector space, \mathbb{C}^n as a \mathbb{C} -vector space and as an \mathbb{R} -vector space
- Example of $\mathbb{Z}/12$ and *definition of \mathbb{Z}/n*
- \mathbb{Z}/n IS A FIELD IF AND ONLY IF $n = p$ IS A PRIME. (“only if” part)

2. Tuesday, 9/12

- \mathbb{Z}/n IS A FIELD IF AND ONLY IF $n = p$ IS A PRIME. (“if” part)
- Elementary properties of a fields and vector spaces: uniqueness of 0 and 1 in a field and of $\vec{0}$ in a vector space, uniqueness of opposites (in a field or vector space) and of inverses in a field, nonexistence of zero divisors (i.e. $a \cdot v = \vec{0}$ if and only if $a = 0$ or $v = \vec{0}$)
- *Definition of characteristic of a field*
- THE CHARACTERISTIC OF A FIELD IS EITHER ZERO OR A PRIME.
- *Definition of subfield and vector subspace*
- Examples of $\mathbb{Q} \subset \mathbb{R}$, $\mathbb{Q} \subset \mathbb{Q}(i)$, $\mathbb{R} \subset \mathbb{C}$
- Example of \mathbb{F}^n as an \mathbb{F} -vector space and \mathbb{E} -vector space, where $\mathbb{E} \subset \mathbb{F}$ subfield
- *Definition of linear combination of a set of vectors over a field*
- *Definition of a set of generators of a vector space over a field*

- Examples in \mathbb{R}^2 over \mathbb{R} and $\mathbb{Q}(i)$ over \mathbb{Q} and over $\mathbb{Q}(i)$
- *Definition of a set \mathcal{B} of linearly independent vectors*
- *Definition of a basis*
- Examples of \mathcal{B} with one vector, examples in \mathbb{R}^2
- Example that generation and linear independence depend on the field (for $\mathbb{Q}(i)$ over \mathbb{Q} and over $\mathbb{Q}(i)$)
- Canonical basis of \mathbb{F}^n over \mathbb{F}
- Example of a basis of $\mathbb{R}[t]$ over \mathbb{R}

3. Thursday, 9/14

- IF $\mathcal{B} \subseteq V$ IS A SET OF LINEARLY INDEPENDENT VECTORS (RESPECTIVELY, A SET OF GENERATORS/A BASIS) OVER \mathbb{F} , THEN EVERY $v \in V$ CAN BE WRITTEN AS A LINEAR COMBINATION OVER \mathbb{F} OF VECTORS IN \mathcal{B} IN AT MOST ONE WAY (RESPECTIVELY, IN AT LEAST ONE WAY/EXACTLY IN ONE WAY).
- Example of linearly independence of $\mathcal{B} = \{v_1, v_2\}$ and example of bases extracted from a set of generators of \mathbb{R}^2
- Examples of vector subspaces of \mathbb{R}^2 and \mathbb{R}^3
- *Definition of span of a subset $\mathcal{B} \subseteq V$ inside V over the field \mathbb{F}*
- $\text{span}_{\mathbb{F}}(\mathcal{B})$ IS A VECTOR SUBSPACE OF V OVER \mathbb{F} .
- Examples of span in \mathbb{R}^2 over \mathbb{R} , in \mathbb{C} over \mathbb{Q} and \mathbb{R}
- IF $U, W \subseteq V$ ARE SUBSPACE OF V OVER \mathbb{F} , THEN $U \cap W$ IS A SUBSPACE OF V OVER \mathbb{F} .
- IF $\mathcal{B} \subseteq V$ IS A SET OF GENERATORS AND $\mathcal{C} \subseteq \mathcal{B}$ IS A SUBSET OF LINEARLY INDEPENDENT VECTORS, THEN \mathcal{C} IS A BASIS.
- IF $\mathcal{B} \subseteq V$ IS A MINIMAL SUBSET OF GENERATORS, THEN \mathcal{B} IS A BASIS.
- IF $\mathcal{B} \subseteq V$ IS A FINITE SUBSET OF GENERATORS OF V AND $\mathcal{C} \subseteq V$ IS A FINITE SUBSET OF LINEARLY INDEPENDENT VECTORS OF V , THEN $|\mathcal{C}| \leq |\mathcal{B}|$.
- IF $\mathcal{B}, \mathcal{B}' \subseteq V$ ARE BASES OF V OVER \mathbb{F} AND $|\mathcal{B}| = n$, $|\mathcal{B}'| = m$, THEN $n = m$.
- *Definition of dimension of a vector space over a field*
- Examples of \mathbb{R}^n over \mathbb{R} , of \mathbb{C}^n over \mathbb{C} , of \mathbb{C}^n over \mathbb{R}

- LET V BE A VECTOR SPACE OVER \mathbb{F} OF DIMENSION n AND LET $\mathcal{B} \subseteq V$ BE A SUBSET OF n VECTORS. IF \mathcal{B} GENERATES V OVER \mathbb{F} , THEN \mathcal{B} IS A BASIS. IF \mathcal{B} IS A SET OF LINEARLY INDEPENDENT VECTORS OVER \mathbb{F} , THEN \mathcal{B} IS A BASIS.

4. Tuesday, 9/19

- LET V BE A VECTOR SPACE, $\mathcal{B} \subset V$ A SET OF LINEARLY INDEPENDENT VECTORS AND $\mathcal{C} \subseteq V$ A SET OF GENERATORS. THEN \mathcal{B} CAN BE COMPLETED TO A BASIS OF V USING VECTORS IN \mathcal{C} . (*Proof only for V of finite dimension.*)
- $W \subseteq V$ VECTOR SUBSPACE. THEN $\dim W \leq \dim V$. IF $\dim W = n = \dim V$, THEN $W = V$.
- Example of $W = \{v = a_1e_1 + a_2e_2 \in \mathbb{R}^2 \mid 2a_1 + a_2 = 0\} \subset \mathbb{R}^2$
- *Definition of sum $W_1 + W_2$ for $W_1, W_2 \subseteq V$ subspaces.*
- $W_1 + W_2$ IS A VECTOR SUBSPACE OF V .
- Example: if $V = \mathbb{R}^2$, $W_1 = \text{span}\{e_1, e_2\}$, $W_2 = \text{span}\{e_2, e_3\} \subset V$, then $V = W_1 + W_2$ (but not a direct sum!)
- *Definition of direct sum $W_1 \oplus W_2$ for $W_1, W_2 \subseteq V$.*
- Example: $V = \mathbb{R}^2$, $W_1 = \text{span}\{e_1\}$, $W_2 = \text{span}\{e_2\} \subset V$, then $V = W_1 \oplus W_2$
- Example: V vector space with basis $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ and $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$. Call $W_1 = \text{span}\mathcal{B}_1$ and $W_2 = \text{span}\mathcal{B}_2$. Then $V = W_1 \oplus W_2$.
- LET $W_1, W_2 \subseteq V$ BE SUBSPACES. THEN $W_1 \oplus W_2 = V$ IF AND ONLY IF [$W_1 + W_2 = V$ AND $W_1 \cap W_2 = \{0\}$].
- LET $W_1, W_2 \subseteq V$ BE SUBSPACES AND ASSUME $\dim V = n$. THEN $\dim (W_1 + W_2) = \dim W_1 + \dim W_2 - \dim (W_1 \cap W_2)$.
- *Definition of homomorphism of vector spaces over \mathbb{F} .* (Also called: “ \mathbb{F} -linear map”, or simply “linear map” when \mathbb{F} is understood.)
- Examples: identity and zero homomorphisms, inclusion of a subspace, homotheties, evaluations, derivative, example $\mathbb{R}^2 \rightarrow \mathbb{R}^3$
- LET $L, L' : V \rightarrow W$ BE HOMOMORPHISMS OF VECTOR SPACES AND LET $\mathcal{B} \subseteq V$ BE A SET OF GENERATORS OF V . IF $L(v) = L'(v)$ FOR EVERY $v \in \mathcal{B}$, THEN $L = L'$.
- LET V, W BE VECTOR SPACES AND LET $\mathcal{B} = \{v_1, \dots, v_n\} \subset V$ BE A BASIS OF V . FOR EVERY SUBSET $\{w_1, \dots, w_n\} \subseteq W$ THERE EXISTS A UNIQUE HOMOMORPHISM $L : V \rightarrow W$ SUCH THAT $L(v_i) = w_i$ FOR $i = 1, \dots, n$.

5. Thursday, 9/21

- *Definition of image, surjectivity, injectivity and bijectivity of a map*
- *Definition of composition of maps, COMPOSITION IS ASSOCIATIVE*
- *Definition of inverse of a map, THE INVERSE (IF IT EXISTS) IS UNIQUE*
- *Definition of kernel of a linear map, KERNEL AND IMAGE OF A LINEAR MAP ARE VECTOR SUBSPACES*
- *A LINEAR MAP L IS INJECTIVE IF AND ONLY IF $\ker(L) = \{\vec{0}\}$*
- *Examples of surjective, injective and bijective homomorphisms*
- *Examples of inclusion of a subspace and restriction of a homomorphism to a subspace*
- *LET $L : V \longrightarrow W$ BE A HOMOMORPHISM OF VECTOR SPACES AND $\mathcal{B} \subset V$ A SET OF LINEARLY INDEPENDENT VECTORS. THEN $L(\mathcal{B}) \subset W$ IS A SET OF LINEARLY INDEPENDENT VECTORS.*
- *IF $L : V \longrightarrow W$ IS A HOMOMORPHISM, THEN $\dim V = \dim \ker(L) + \dim \text{Im}(L)$.*
- *Examples of $V \longrightarrow W$ when $\dim(V) > \dim(W)$ or $\dim(V) < \dim(W)$*
- *Structure of \mathbb{F} -vector space on the space $\text{Hom}_{\mathbb{F}}(V, W)$ of \mathbb{F} -linear maps from V to W*
- *COMPOSITION OF HOMOMORPHISMS IS A HOMOMORPHISM, THE INVERSE OF A HOMOMORPHISM (IF IT EXISTS) IS A HOMOMORPHISM*
- *There is a bijective correspondence between $\text{Hom}_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F}^m)$ and the space $\mathcal{M}_{m \times n}(\mathbb{F})$ of $(m \times n)$ -matrices (i.e. with m rows and n columns) with entries in \mathbb{F}*

6. Tuesday, 9/26

- *Sum of $m \times n$ matrices A, B : $(A + B)_{ij} = A_{ij} + B_{ij}$*
- *Multiplication of an $m \times n$ matrix A by a number $\lambda \in \mathbb{F}$: $(\lambda \cdot A)_{ij} = \lambda \cdot A_{ij}$*
- *Structure of vector space over \mathbb{F} on $\mathcal{M}_{m \times n}(\mathbb{F})$*
- *THE CORRESPONDENCE $\text{Hom}_{\mathbb{F}}(\mathbb{F}^n, \mathbb{F}^m) \longrightarrow \mathcal{M}_{m \times n}(\mathbb{F})$ IS AN ISOMORPHISM OF \mathbb{F} -VECTOR SPACES*
- *Composition of homomorphisms $A : \mathbb{F}^n \longrightarrow \mathbb{F}^m$, $B : \mathbb{F}^m \longrightarrow \mathbb{F}^p$ and rule for multiplication $B \cdot A : \mathbb{F}^n \longrightarrow \mathbb{F}^p$ (namely, $(B \cdot A)_{ij} = \sum_{k=1}^m B_{ik}A_{kj}$)*
- *Example of product of two matrices*
- *Example: the zero matrix, $n \times n$ identity matrix I_n , diagonal matrices*
- *Counterexample: if A, B are $n \times n$ matrices, then in general $A \cdot B \neq B \cdot A$*

- Example: if A, B are $n \times n$ diagonal matrices, then $A \cdot B = B \cdot A$; in particular, $A \cdot B = B \cdot A$ if $n = 1$

- *Passage to coordinates:* fix a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V over \mathbb{F} . Define the homomorphism $M^{\mathcal{B}} : \mathbb{F}^n \xrightarrow{\sim} V$ as $M^{\mathcal{B}}(e_i) = v_i$, and the homomorphism $M_{\mathcal{B}} : V \xrightarrow{\sim} \mathbb{F}^n$ as

$$M_{\mathcal{B}}(v) = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix} \text{ where } v = \sum_{i=1}^n a_i v_i.$$

$M^{\mathcal{B}}$ and $M_{\mathcal{B}}$ isomorphisms inverse of each other.

$M_{\mathcal{B}}(v)$ is called **vector of coordinates** of v with respect to the basis \mathcal{B} .

- Example: $M^{\mathcal{B}}$ and $M_{\mathcal{B}}$ for $V = \mathbb{R}[t]_{\leq 2}$ with basis $\mathcal{B} = \{1, t, t^2\}$ and $\mathcal{B}' = \{t+1, -1, t^2\}$

- *Representation of homomorphisms in coordinates:* fix bases $\mathcal{B} = \{v_1, \dots, v_n\}$ for V and $\mathcal{C} = \{w_1, \dots, w_m\}$ for W and let $L : V \rightarrow W$ be a homomorphism.

Definition of the matrix $M_{\mathcal{C}}^{\mathcal{B}}(L) := M_{\mathcal{C}} \circ L \circ M^{\mathcal{B}}$ **associated to** L *with respect to the bases* \mathcal{B} *and* \mathcal{C}

$$\begin{array}{ccc} V & \xrightarrow{L} & W \\ M^{\mathcal{B}} \uparrow & & \uparrow M_{\mathcal{C}} \\ \mathbb{F}^n & \xrightarrow{M_{\mathcal{C}}^{\mathcal{B}}(L)} & \mathbb{F}^m \end{array}$$

- Example: $V = \mathbb{R}[t]_{\leq 1}$, $W = \mathbb{R}[t]_{\leq 2}$, $L : V \rightarrow W$ is defined as $L(p(t)) = (t+1) \cdot p(t)$. Computation of $M_{\mathcal{C}}^{\mathcal{B}}(L)$ where $\mathcal{B} = \{1, t\}$ and $\mathcal{C} = \{1, t, t^2\}$

7. Thursday, 9/28

- *Matrix of change of coordinates* $M_{\mathcal{B}'}^{\mathcal{B}}$ *from the basis* \mathcal{B} *to the basis* \mathcal{B}' *of* V *as* $M_{\mathcal{B}'}^{\mathcal{B}} = M_{\mathcal{B}'}^{\mathcal{B}}(Id_V)$
- IF $F : V \rightarrow W$ AND $G : W \rightarrow Z$ ARE HOMOMORPHISMS OF VECTOR SPACES OF FINITE DIMENSION AND $\mathcal{B}, \mathcal{C}, \mathcal{D}$ ARE BASES OF V, W, Z , THEN $M_{\mathcal{D}}^{\mathcal{B}}(G \circ F) = M_{\mathcal{D}}^{\mathcal{C}}(G) \cdot M_{\mathcal{C}}^{\mathcal{B}}(F)$
- $M_{\mathcal{C}}^{\mathcal{B}}(F)$ is invertible if and only if F is invertible; $M_{\mathcal{B}'}^{\mathcal{B}}$ is always invertible and it is equal to the identity matrix if and only if $\mathcal{B} = \mathcal{B}'$
- If F is invertible, then $M_{\mathcal{C}}^{\mathcal{B}}(F^{-1}) = M_{\mathcal{C}}^{\mathcal{B}}(F)^{-1}$
- Example: $V = \mathbb{R}[t]_{\leq 2}$, $W = \mathbb{R}[t]_{\leq 1}$, $Z = \mathbb{R}[t]_{\leq 2}$ and $F : V \rightarrow W$ given by $F(p(t)) = p'(t)$ and $G : W \rightarrow Z$ given by $G(q(t)) = t \cdot q(t)$. Explicit computation of $M_{\mathcal{C}}^{\mathcal{B}}(F)$, $M_{\mathcal{D}}^{\mathcal{C}}(G)$ and $M_{\mathcal{D}}^{\mathcal{B}}(G \circ F)$ (the last one both as a product and directly)
- *Systems of linear equations* $A \cdot X = B$: definition and interpretations ($A : \mathbb{F}^n \rightarrow \mathbb{F}^m$)

- Homogeneous and non-homogeneous systems of linear equations
- IF $A \cdot X = 0$ IS A HOMOGENEOUS SYSTEM OF m LINEAR EQUATIONS IN n UNKNOWNNS, THEN THE SPACE OF SOLUTIONS IS $\ker(A)$ (and it is a vector subspace of \mathbb{F}^n)
- A NON-HOMOGENEOUS SYSTEM $A \cdot X = B$ OF m LINEAR EQUATIONS IN n UNKNOWNNS ADMIT SOLUTIONS IF AND ONLY IF $B \in \text{Im}(A) \subset \mathbb{F}^m$ (notice that $X = 0$ is not a solution, if $B \neq 0$)
- GIVEN A PARTICULAR SOLUTION X' OF $A \cdot X = B$, THE SPACE OF SOLUTIONS OF THE SYSTEM IS $X' + \ker(A) := \{v \in \mathbb{F}^n \mid v = X' + k \quad k \in \ker(A)\}$ (notice that, if $B \neq 0$, then $X' \neq 0$ and $X' + \ker(A)$ is a “traslate” of $\ker(A)$ that does not pass through $0 \in \mathbb{F}^n$, so in particular $X' + \ker(A)$ is not a vector subspace of \mathbb{F}^n)
- Given two vector spaces V, W over \mathbb{F} , their **product** $V \times W := \{(v, w) \mid v \in V, w \in W\}$ is a vector space over \mathbb{F} with componentwise sum and scalar multiplication
- The projection $V \times W \longrightarrow V$ and the inclusion $V \longrightarrow V \times W$ are homomorphisms
- $\mathbb{F}^n \times \mathbb{F}^m$ is canonically isomorphic to \mathbb{F}^{n+m}
- If $W_1, W_2 \subseteq V$ are subspaces of V such that $W_1 \oplus W_2 = V$, then $S : W_1 \times W_2 \longrightarrow V = W_1 \oplus W_2$ given by $S(w_1, w_2) = w_1 + w_2$ is an isomorphism
- If V is a vector space over \mathbb{F} then $\text{Hom}_{\mathbb{F}}(\mathbb{F}^n, V) \longrightarrow V^n$ given by $L \mapsto (Le_1, \dots, Le_n)$ is a canonical isomorphism
- Given a vector space V over \mathbb{F} , its **dual** is $V^* := \text{Hom}_{\mathbb{F}}(V, \mathbb{F})$
- Example: if $V = \mathbb{R}[t]$, for every $x \in \mathbb{R}$ the evaluation $\text{ev}_x : \mathbb{R}[t] \longrightarrow \mathbb{R}$ at x is a vector in V^*
- THERE IS A CANONICAL INJECTIVE HOMOMORPHISM $V \longrightarrow V^{**}$ GIVEN BY $v \mapsto \text{ev}_v$, WHERE $\text{ev}_v : V^* \longrightarrow \mathbb{F}$ IS DEFINED AS $\text{ev}_v(\varphi) := \varphi(v)$ FOR EVERY $\varphi \in V^*$
- If $\mathcal{B} = \{v_i\}$ is a basis of V , then $v_i^* : V \longrightarrow \mathbb{F}$ is defined requiring that $v_i^*(v_i) = 1$ and $v_i^*(v_j) = 0$ for all $j \neq i$
- IF $\mathcal{B} = \{v_i\}$ IS A BASIS OF V , THEN $\mathcal{B}^* = \{v_i^*\}$ IS A SET OF LINEARLY INDEPENDENT VECTORS IN V^*

8. Tuesday, 10/3

- If $W \subset V$ is a vector subspace and $W \neq \{0\}, V$, then $V \setminus W \cup \{0\}$ is *never* a vector subspace of V .
- IF $\dim V = n$ AND \mathcal{B} IS A BASIS OF V , THEN $\dim V^* = n$ AND SO \mathcal{B}^* IS A BASIS OF V^*

- If $\dim V = \infty$ AND \mathcal{B} IS A BASIS OF V , THEN \mathcal{B}^* IS NOT A SET OF GENERATORS OF V^*
- Example: lines and planes in \mathbb{R}^2 and \mathbb{R}^3 defined using span or equations
- Given a subset $S \subseteq V^*$, the **annihilator** of S is $\text{Ann}(S) := \{v \in V \mid \varphi(v) = 0 \ \forall \varphi \in S\}$
- $\text{Ann}(S) = \text{Ann}(\text{span}(S))$ is a vector subspace of V
- Example: $V = \mathbb{R}[t]$ and $\mathcal{B} = \{v_k = t^k \mid k \in \mathbb{N}\}$; $v_k^*(p(t))$ is the coefficient of $p(t)$ that multiplies t^k ; the evaluation $\text{ev}_1 : V \rightarrow \mathbb{R}$ given by $\text{ev}_1(p(t)) = p(1)$ does not belong to $\text{span}_{\mathbb{R}} \mathcal{B}^*$
- Let V be a vector space over \mathbb{F} with basis $\mathcal{B} = \{v_1, \dots, v_n\}$. We have the following diagram

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & \mathbb{F} \\ M^{\mathcal{B}} \uparrow & \nearrow M^{\mathcal{B}}(\varphi) & \\ \mathbb{F}^n & & \end{array}$$

where $M^{\mathcal{B}}(\varphi) = \varphi \circ M^{\mathcal{B}} : \mathbb{F}^n \rightarrow \mathbb{F}$. Then, the representation $M^{\mathcal{B}}(\varphi)$ of $\varphi \in V^*$ in the coordinates given by \mathcal{B} and is a $1 \times n$ matrix $(* \ * \ \dots \ *)$

- Let $L : V \rightarrow W$ be a homomorphism of vector spaces over \mathbb{F} . Then $L^* : W^* \rightarrow V^*$ is the **dual** homomorphism over \mathbb{F} defined as $L^*(\varphi) = \varphi \circ L$ for every $\varphi : W \rightarrow \mathbb{F}$.
- Representation of dual homomorphisms in coordinates: fix bases $\mathcal{B} = \{v_1, \dots, v_n\}$ for V and $\mathcal{C} = \{w_1, \dots, w_m\}$ for W and let $L : V \rightarrow W$ be a homomorphism. The matrix $M_{\mathcal{B}^*}^{\mathcal{C}^*}(L^*) := M_{\mathcal{B}^*} \circ L^* \circ M_{\mathcal{C}^*}$ associated to L^* with respect to the dual bases \mathcal{B}^* of V^* and \mathcal{C}^* of W^* is

$$\begin{array}{ccc} W^* & \xrightarrow{L^*} & V^* \\ M_{\mathcal{C}^*} \uparrow & & \uparrow M_{\mathcal{B}^*} \\ \mathbb{F}^m & \xrightarrow{M_{\mathcal{B}^*}^{\mathcal{C}^*}(L^*)} & \mathbb{F}^n \end{array} \quad \begin{array}{c} \curvearrowright \\ M_{\mathcal{B}^*} \end{array}$$

- The **transpose** of a matrix $A \in \mathcal{M}_{m \times n}(\mathbb{F})$ is the matrix $A^t \in \mathcal{M}_{n \times m}(\mathbb{F})$ defined by $(A^t)_{ij} := A_{ji}$.
- $M_{\mathcal{B}^*}^{\mathcal{C}^*}(L^*)$ IS THE TRANSPOSE OF $M_{\mathcal{C}^*}^{\mathcal{B}^*}(L)$.

9. Thursday, 10/5

- Example: $V = \mathbb{C}[t]_{\leq 2}$, $W = \mathbb{C}[t]_{\leq 1}$, $D : V \rightarrow W$ is given by $D(p(t)) = p'(t)$. Pick bases $\mathcal{B} = \{1, t, t^2\}$ of V and $\mathcal{C} = \{1, t+1\}$ of W . Computation of $M_{\mathcal{C}^*}^{\mathcal{B}^*}(D)$. Computation of \mathcal{B}^* , \mathcal{C}^* and direct computation of $M_{\mathcal{B}^*}^{\mathcal{C}^*}(D^*)$. Check that $M_{\mathcal{B}^*}^{\mathcal{C}^*}(D^*) = M_{\mathcal{C}^*}^{\mathcal{B}^*}(D)^t$.

- The dual of \mathbb{F}^n as $1 \times n$ matrices; standard identification of $(\mathbb{F}^n)^*$ with \mathbb{F}^n using the dual of the standard basis

- Linear systems of equations $A \cdot X = B$ with $A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$,

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \text{ and } B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

$$\text{The extended matrix } \tilde{A} = (A|B) = \left(\begin{array}{cccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ a_{21} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array} \right).$$

- **Elementary operations on the rows of \tilde{A} :** call R_i the i -th row of \tilde{A} .
The first operation is $R_i \mapsto c \cdot R_i$ for $c \neq 0$; the second operation is $R_j \mapsto R_j + c \cdot R_i$ for $i \neq j$; the third operation is exchanging R_i with R_j
- THE THREE ELEMENTARY OPERATIONS ON THE ROWS ARE INVERTIBLE AND THEIR INVERSES ARE ELEMENTARY OPERATIONS ON THE ROWS OF THE SAME TYPE
- Every elementary operation on the rows is implemented by a left multiplication by an $n \times n$ square matrix, called **elementary matrix**

- Examples of elementary 3×3 matrices: $\begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & 1 \end{pmatrix}$ (for $c \neq 0$) multiplies the second row by c ; $\begin{pmatrix} 1 & c & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ adds $c \cdot R_2$ to R_1 ; $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ exchanges R_2 and R_3

- ELEMENTARY MATRICES ARE INVERTIBLE AND THEIR INVERSES ARE ELEMENTARY MATRICES
- THE ELEMENTARY OPERATIONS ON THE ROWS OF \tilde{A} PRESERVE THE SET OF SOLUTIONS OF $AX = B$
- GAUSS ELIMINATION ALGORITHM AND ROW-ECHELON FORM OF A MATRIX
- A matrix A is in **row-Echelon form** if: the first nonzero entry of each row is 1, and below the first nonzero entry of each row there are only zeroes
- If $A : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ is represented by an $m \times n$ matrix, then the image of A is the span of the columns of A

- The **rank** of a matrix A is the number of nonzero rows in its row-Echelon form; equivalently, it is the dimension of the image of A
- IF $\tilde{A} = (A|B)$ IS IN ROW-ECHELON FORM, THEN THE SYSTEM $AX = B$ ADMITS SOLUTIONS IF AND ONLY IF $\text{rk}(A) = \text{rk}(\tilde{A})$, I.E. IF AND ONLY IF $b_{r+1} = b_{r+2} = \dots = b_m = 0$ WHERE $r = \text{rk}(A)$
- GAUSS-JORDAN ELIMINATION AND REDUCED ROW-ECHELON FORM OF A MATRIX
- A matrix is in **reduced row-Echelon form** if it is in row Echelon form and the first nonzero entry in each row is the only nonzero entry in its column
- From the reduced row-Echelon form of $\tilde{A} = (A|B)$ to the set of solutions of the system $AX = B$
- THE OUTPUT OF GAUSS-JORDAN ELIMINATION APPLIED TO A IS A MATRIX IN ROW-ECHELON FORM A' EQUAL TO $E_p E_{p-1} \dots E_2 E_1 A$, WHERE E_i 'S ARE ELEMENTARY $n \times n$ MATRICES (similarly, if the method is applied to \tilde{A})
- IF A IS AN INVERTIBLE $n \times n$ MATRIX, THEN IT IS A PRODUCT OF ELEMENTARY MATRICES \implies GAUSS-JORDAN ELIMINATION APPLIED TO $(A|I_n)$ GIVES $(I_n|A^{-1})$ AS OUTPUT

11. Tuesday, 10/17

- Review of solutions of Midterm Exam 1
- Elementary matrices: ELEMENTARY MATRICES ARE INVERTIBLE AND THEIR INVERSES ARE ELEMENTARY MATRICES
- Elementary operations on the rows and elementary operations on the columns
- ELEMENTARY OPERATIONS ON THE ROWS ARE IMPLEMENTED BY LEFT-MULTIPLICATION BY ELEMENTARY MATRICES
- ELEMENTARY OPERATIONS ON THE COLUMNS ARE IMPLEMENTED BY RIGHT-MULTIPLICATION BY ELEMENTARY MATRICES
- ELEMENTARY OPERATIONS ON THE ROWS OF A PRESERVE $\ker(A)$
- ELEMENTARY OPERATIONS ON THE COLUMNS OF A PRESERVE $\text{Im}(A)$
- Reduced row-Echelon form and computation of the kernel of a matrix
- Reduced column-Echelon form and computation of the image of a matrix
- Algorithm to find the inverse of an invertible square matrix A by applying Gauss-Jordan reduction to $(A|I)$
- Example of computation of kernel and image of a matrix

- Example of computation of the inverse of an invertible square matrix
- Let $L : V \rightarrow W$ be a homomorphism and let \mathcal{B} be a basis of V and $\mathcal{C} = \{w_1, \dots, w_m\}$ be a basis of W . Then, OPERATIONS ON THE ROWS OF $M_{\mathcal{C}}^{\mathcal{B}}(L)$ CORRESPOND TO CHANGING THE BASIS \mathcal{C} OF THE CODOMAIN; OPERATIONS ON THE COLUMNS OF $M_{\mathcal{C}}^{\mathcal{B}}(L)$ CORRESPOND TO CHANGING THE BASIS \mathcal{B} OF THE DOMAIN.
In particular, if we multiply the i -th row of $M_{\mathcal{C}}^{\mathcal{B}}(L)$ by $c \neq 0$, we obtain $M_{\mathcal{C}'}^{\mathcal{B}}(L)$, where \mathcal{C}' is obtained from \mathcal{C} by replacing w_i by w_i/c ; if we exchange the i -th and the j -th row of $M_{\mathcal{C}}^{\mathcal{B}}(L)$, we obtain $M_{\mathcal{C}'}^{\mathcal{B}}(L)$, where \mathcal{C}' is obtained from \mathcal{C} by exchanging w_i with w_j ; if we sum c times the j -th row of $M_{\mathcal{C}}^{\mathcal{B}}(L)$ to the i -th row, we obtain $M_{\mathcal{C}'}^{\mathcal{B}}(L)$, where \mathcal{C}' is obtained from \mathcal{C} by replacing w_i by $w_i - cw_j$.
Operations on the columns of $M_{\mathcal{C}}^{\mathcal{B}}(L)$ correspond to analogous modifications of \mathcal{B} .

12. Thursday, 10/19

- An **equivalence relation** on a nonempty set S is a binary relation \sim that is reflexive (i.e. $x \sim x$ for every $x \in S$), symmetric (i.e. $x \sim y \implies y \sim x$) and transitive (i.e. $x \sim y$ and $y \sim z \implies x \sim z$).
- An **equivalence class** in (S, \sim) is a maximal subset $C \subseteq S$ of elements that are all equivalent to one another; rephrasing, an equivalence class $C \subseteq S$ is a nonempty subset such that: if $x \in C, y \in S$ and $x \sim y$, then $y \in C$.
- The **quotient set** S/\sim of S with respect to the equivalence relation \sim is the set of equivalence classes in (S, \sim) .
- Example: take $S = \mathbb{Z}$ and declare $a, b \in \mathbb{Z}$ equivalent if $a - b$ is a multiple of n . Then the equivalence classes are $\{a + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$ for $a \in \mathbb{Z}$. Call \bar{b} the equivalence class $\{b + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$. Clearly, $\bar{b} = \bar{c}$ (i.e. they are the **same** set) if and only if $b - c$ is a multiple of n . Hence, the quotient of \mathbb{Z} by this equivalence relation is exactly \mathbb{Z}/n .
- Example: take $S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ and declare $(a, b), (c, d) \in S$ equivalent if $ad = bc$. Call $\frac{a}{b}$ the equivalence class of $(a, b) \in S$. In every equivalence class there is a **canonical element** (m, n) such that m, n are coprime (i.e. they are not divisible by the same prime number) and $n > 0$. The equivalence class that contains (m, n) is $\{(am, an) \in S \mid 0 \neq a \in \mathbb{Z}\} \subset S$. Then, S/\sim is exactly \mathbb{Q} , the set of rational numbers.
- Problem: classification of matrices, up to change of basis in the domain and in the codomain; rephrasing in terms of equivalence relation (i.e. $M, N \in \mathcal{M}_{m \times n}(\mathbb{F})$ are equivalent if $M = ANB$, with $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ invertible and $B \in \mathcal{M}_{m \times m}(\mathbb{F})$ invertible).
- THE RANK IS A COMPLETE INVARIANT FOR THE EQUIVALENCE RELATION DESCRIBED ABOVE, THAT IS: $M \sim N$ IF AND ONLY IF $\text{rk}(M) = \text{rk}(N)$.

The proof goes through finding one and only one canonical form in each equivalence class, and the canonical form in this case is given by

$$R_k = \left(\begin{array}{c|c} I_k & 0 \\ \hline 0 & 0 \end{array} \right)$$

where I_k is the $k \times k$ identity matrix and k is the rank of the matrices in the class.

- *Endomorphisms of a vector space V of finite dimension; composition*
- *Two matrices $M, N \in \mathcal{M}_{n \times n}(\mathbb{F})$ are **similar** if there exists an invertible $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ such that $M = ANA^{-1}$*
- Problem: classification of endomorphisms of a vector space V of finite dimension up to change of basis; rephrasing: classification of matrices in $\mathcal{M}_{n \times n}(\mathbb{F})$ up to similitude
- *Invariants under similitude*; for example, being invertible is invariant under similitude; the rank (and so also the dimension of the kernel) is invariant under similitude
- *The **trace** of $M \in \mathcal{M}_{n \times n}(\mathbb{F})$ is $\text{tr}(M) = \sum_{i=1}^n M_{ii}$.*
- THE TRACE $\text{tr} : \mathcal{M}_{n \times n}(\mathbb{F}) \longrightarrow \mathbb{F}$ IS A HOMOMORPHISM OF \mathbb{F} -VECTOR SPACES.
- FOR EVERY $A, B \in \mathcal{M}_{n \times n}(\mathbb{F})$, $\text{tr}(AB) = \text{tr}(BA)$.
- Example: the previous result implies that $\text{tr}(ABC) = \text{tr}(BCA) = \text{tr}(CAB)$ but, in general, $\text{tr}(ABC)$ can be different from $\text{tr}(BAC)$.
- THE TRACE IS AN INVARIANT UNDER SIMILITUDE.

13. Tuesday, 10/24

- Determinant 2×2 as a ratio of areas with sign (if $\mathcal{B} = \{v, w\}$ is a basis of \mathbb{R}^2 and $A \in \mathcal{M}_{2 \times 2}(\mathbb{R})$, then $\det_2(A) = \pm \frac{\text{Area}(Av, Aw)}{\text{Area}(v, w)}$)
- *Formal properties of $\det_2 : \mathcal{M}_{2 \times 2}(\mathbb{R}) \longrightarrow \mathbb{R}$*
 - $\det_2(I_2) = 1$
 - $\det_2(A) = 0$ if the two columns of A are equal (alternating property)
 - $\det_2(C) = a\det_2(A) + b\det_2(B)$ if $A = (av|w)$, $B = (bv'|w)$ and $C = (av + bv'|w)$ and similarly for the second column (multi-linearity property for the columns)

- Remark: in general, $\det_2(A + B)$ can be different from $\det_2(A) + \det_2(B)$
- Remark: $\det_2(\lambda A) = \lambda^2 \det_2(A)$
- THE FORMAL PROPERTIES IMPLY THAT $\det_2(B) = -\det_2(A)$ IF B IS OBTAINED FROM A BY EXCHANGING THE TWO COLUMNS
- THE FORMAL PROPERTIES IMPLY THAT $\det_2(A) = 0$ IF A IS NOT INVERTIBLE
- THE FORMAL PROPERTIES DETERMINE $\det_2(E)$ WHEN E IS AN ELEMENTARY MATRIX
- THE FORMAL PROPERTIES IMPLY THAT $\det_2(BE) = \det_2(B)\det_2(E)$, WHEN E IS AN ELEMENTARY MATRIX
- AS INVERTIBLE MATRICES ARE PRODUCTS OF ELEMENTARY MATRICES, $\det_2(BA) = \det_2(B)\det_2(A)$
- THE FORMAL PROPERTIES IMPLY THAT, IF SUCH A FUNCTION \det_2 EXISTS, THEN IT IS UNIQUE
- IF A IS INVERTIBLE, THEN $\det_2(A^{-1}) = \det_2(A)^{-1}$, SO $\det_2(A) \neq 0$
- IF A IS INVERTIBLE, $\det_2(ABA^{-1}) = \det_2(B)$, I.E. \det_2 IS INVARIANT UNDER SIMILITUDE
- AS THE TRANSPOSE OF AN ELEMENTARY MATRIX IS ELEMENTARY, WE CAN CHECK THAT $\det_2(E^t) = \det_2(E)$ WHEN E IS ELEMENTARY
- $\det_2(A^t) = \det(A)$ AND SO \det_2 IS ALTERNATING AND MULTI-LINEAR ALSO ON THE ROWS
- EXISTENCE OF \det_2 : IF $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, THEN DEFINE $\det_2(A) := ad - bc$
- Check that all the formal properties of \det_2 hold
- We look for $\det_n : \mathcal{M}_{n \times n}(\mathbb{F}) \longrightarrow \mathbb{F}$ such that
 - (a) $\det_n(I_n) = 1$
 - (b) $\det_n(A) = 0$ if two (consecutive) columns of A are equal (alternating property)
 - (c) $\det_n(C) = a\det_n(A) + b\det_n(B)$ if the columns of A, B, C except for the i -th column, the i -th column of A being v , the i -th column of B being w and the i -th column of C being $av + bw$ with $a, b \in \mathbb{F}$ (multi-linearity property for the columns)
- THE PROPERTIES ABOVE IMPLY THAT $\det_n(B) = -\det_n(A)$ IF B IS OBTAINED FROM A BY EXCHANGING TWO COLUMNS
- THE PROPERTIES ABOVE IMPLY THAT $\det_n(A) = 0$ IF A IS NOT INVERTIBLE
- THE PROPERTIES ABOVE DETERMINE $\det_n(E)$ WHEN E IS AN ELEMENTARY MATRIX

- THE PROPERTIES ABOVE IMPLY THAT $\det_n(BE) = \det_n(B)\det_n(E)$, WHEN E IS AN ELEMENTARY MATRIX
- AS INVERTIBLE MATRICES ARE PRODUCTS OF ELEMENTARY MATRICES, $\det_n(BA) = \det_n(B)\det_n(A)$
- THE PROPERTIES ABOVE IMPLY THAT, IF SUCH A FUNCTION \det_n EXISTS, THEN IT IS UNIQUE
- IF A IS INVERTIBLE, THEN $\det_n(A^{-1}) = \det_n(A)^{-1}$, SO $\det_n(A) \neq 0$
- IF A IS INVERTIBLE, $\det_n(ABA^{-1}) = \det_n(B)$, I.E. \det_n IS INVARIANT UNDER SIMILITUDE
- AS THE TRANSPOSE OF AN ELEMENTARY MATRIX IS ELEMENTARY, WE CAN CHECK THAT $\det_n(E^t) = \det_n(E)$ WHEN E IS ELEMENTARY
- $\det_n(A^t) = \det(A)$ AND SO \det_n IS ALTERNATING AND MULTI-LINEAR ALSO ON THE ROWS
- We want to define \det_n by taking a polynomial in the entries of A such that each monomial has exactly one entry for each row and one entry for each columns (to ensure multi-linearity)
- Example of such monomials in the case 2×2 and 3×3
- SUCH MONOMIALS ARE ENUMERATED BY PERMUTATIONS ON $\{1, 2, \dots, n\}$
- A **permutation** of the set $\{1, 2, \dots, n\}$ is a bijective map $\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$. The set of all permutations of $\{1, 2, \dots, n\}$ is denoted by \mathfrak{S}_n
- Permutations can be composed
- EVERY MONOMIAL IN THE ENTRIES OF A WITH ONE ENTRY IN EACH ROW AND IN EACH COLUMN OF A IS A MULTIPLE OF $A_{\sigma(1),1} \cdot A_{\sigma(2),2} \cdots A_{\sigma(n),n}$, WHERE $\sigma \in \mathfrak{S}_n$ IS A PERMUTATION
- Our $\det_n(A)$ will be $\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) A_{\sigma(1),1} \cdot A_{\sigma(2),2} \cdots A_{\sigma(n),n}$ where $\varepsilon(\sigma) = \pm 1$

14. Thursday, 10/26

- Two ways of representing permutations of n elements
- Cycles and transpositions
- Composition of permutations
- EVERY PERMUTATION CAN BE (UNIQUELY) DECOMPOSED INTO A COMPOSITION OF CYCLES

- EVERY PERMUTATION IS COMPOSITION OF TRANSPOSITIONS (and really of elementary transposition of the form $(k \ k + 1)$.)
- Example: \mathfrak{S}_2 and \mathfrak{S}_3
- The sign $\varepsilon(\sigma)$ of a permutation $\sigma \in \mathfrak{S}_n$ is $(-1)^k$, where σ is the composition of k transpositions (consider the identity as a product of zero transpositions)
- $\varepsilon(\sigma)$ IS WELL-DEFINED: IN FACT, $\varepsilon(\sigma) = (-1)^{N(\sigma)}$ WHERE $N(\sigma) := \sum_{i=2}^n \#\{j < i \mid \sigma(j) > \sigma(i)\}$
- THE SIGN $\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ IS A FUNCTION SUCH THAT $\varepsilon(id) = 1$ AND $\varepsilon(\sigma_2\sigma_1) = \varepsilon(\sigma_2)\varepsilon(\sigma_1)$
- Example: signs of permutations in \mathfrak{S}_3
- EXISTENCE OF $\det_n : \mathcal{M}_{n \times n}(\mathbb{F}) \longrightarrow \mathbb{F}$: define

$$\widetilde{\det}_n(A) := \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) A_{\sigma(1),1} A_{\sigma(2),2} \cdots A_{\sigma(n),n}$$

and check that $\widetilde{\det}_n$ satisfies the three properties of \det_n , namely $\widetilde{\det}_n$ is multi-linear and alternating on the columns and $\widetilde{\det}_n(I_n) = 1$

- LAPLACE EXPANSION OF \det_n .
For every $1 \leq i, j \leq n$, call m_{ij} the $(n-1) \times (n-1)$ matrix obtained from A by removing the i -th row and the j -th column.
The quantity $\det_{n-1}(m_{ij})$ is also called *minor* (i, j) of the matrix A .
If $n = 1$, we always set $\det'(A) = \det(A) = A_{11}$.
For $n \geq 2$ and $1 \leq k \leq n$, define $\det'_n(A)$ in the following way:

$$\det'_n = (-1)^k \sum_{j=1}^n (-1)^j A_{kj} \det'_{n-1}(m_{kj})$$

By induction on $n \geq 2$, we can prove that $\det'_n(A)$ is multi-linear and alternating on the columns of A and that $\det'_n(I_n) = 1$, so that $\det'_n = \det_n$.
As $\det(A) = \det(A^t)$, we also have that Laplace formula holds if we start fixing a column instead of a row.

- FORMULA FOR THE INVERSE OF A MATRIX A . The recipe is: define a matrix B as follows: $B_{ij} := \det(A)^{-1} (-1)^{i+j} \det(m_{ji})$, where $\det(m_{ji})$ is the (j, i) minor of A .
From Laplace formula, we obtain that $BA = AB = I_n$, so that B is the inverse of A .

15. Tuesday, 10/31

- If $q(t) \in \mathbb{F}[t]$ and $L \in \text{End}(V)$, then $q(L) \in \text{End}(V)$ is defined replacing t^k (for $k \geq 0$) by L^k , where $L^0 = I$.

- IF $M \in \text{End}(V)$ IS INVERTIBLE, THEN $q(MAM^{-1}) = Mq(A)M^{-1}$.
- IF $A, B \in \mathcal{M}_{n \times n}(\mathbb{F})$ ARE SIMILAR, THEN $q(A)$ AND $q(B)$ ARE SIMILAR FOR EVERY $q(t) \in \mathbb{F}[t]$. HENCE, $\text{tr}(q(A)) = \text{tr}(q(B))$ AND $\det(q(A)) = \det(q(B))$.
- **The characteristic polynomial $p_L(\lambda)$ of $L \in \text{End}(V)$ is $p_L(\lambda) := \det(L - \lambda I) \in \mathbb{F}[\lambda]$.** If $\dim(V) = n$, then $p_L(\lambda)$ has degree n .
- IF A IS SIMILAR TO B , THEN $p_A(\lambda) = p_B(\lambda)$.
- IF $p_L(\lambda) = a_n(-\lambda)^n + a_{n-1}(-\lambda)^{n-1} + \dots + a_1(-\lambda) + a_0$ WITH $a_i \in \mathbb{F}$, THEN $a_n = 1$, $a_{n-1} = \text{tr}(L)$ AND $a_0 = \det(L)$.
- IF $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ IS AN UPPER TRIANGULAR MATRIX, THEN $\det(A) = \prod_{i=1}^n A_{ii}$.
- Let $L \in \text{End}(V)$ and $e \in \mathbb{F}$. The **eigenspace for L corresponding to e** is $E_{e,L} := \ker(L - eI)$. If $E_{e,L} \neq \{0\}$, then e is called **eigenvalue for L** . An **eigenvector for L corresponding to the eigenvalue e** is a nonzero vector $0 \neq v \in E_{e,L}$.
- Remark: v is an eigenvector for L of eigenvalue $e \iff v \in \ker(L - eI) \iff L(v) = ev$.
- $e \in \mathbb{F}$ IS AN EIGENVALUE FOR L IF AND ONLY IF $\ker(L - eI) \neq \{0\}$, THAT IS IF AND ONLY IF $\ker(L - eI)$ IS NOT INVERTIBLE, I.E. IF AND ONLY IF $\det(L - eI) = 0$. SO THE EIGENVALUES OF L ARE THE ROOTS OF ITS CHARACTERISTIC POLYNOMIAL $p_L(\lambda)$.
- IF $L, K : V \longrightarrow V$ AND $M : V \longrightarrow V$ IS INVERTIBLE AND $K = MLM^{-1}$, THEN $\ker(K) = M(\ker(L))$ AND $\text{Im}(K) = M(\text{Im}(L))$. AS M IS INVERTIBLE, $\dim \ker(K) = \dim \ker(L)$ AND $\dim \text{Im}(K) = \dim \text{Im}(L)$.
- IF $A, B \in \mathcal{M}_{n \times n}(\mathbb{F})$ ARE SIMILAR SO THAT $B = MAM^{-1}$ FOR SOME INVERTIBLE M AND IF $q(t) \in \mathbb{F}[t]$, THEN $q(B) = Mq(A)M^{-1}$ AND SO $\ker(q(B)) = M(\ker(q(A)))$ AND $\text{Im}(q(B)) = M(\text{Im}(q(A)))$. HENCE, $\dim \ker(q(B)) = \dim \ker(q(A))$.
- Let $L : V \longrightarrow V$ and $e \in \mathbb{F}$. The **multiplicity μ of e for L** is the dimension of the eigenspace of L associated to e , that is $\mu(e, L) = \dim \ker(L - eI) = \dim E_{e,L}$.
- Remark: $e \in \mathbb{F}$ is an eigenvalue for $L : V \longrightarrow V$ if and only if $\mu(e, L) \geq 1$.
- IF A, B ARE SIMILAR MATRICES, THEN $\mu(e, A) = \mu(e, B)$ FOR ALL $e \in \mathbb{F}$.
- Example: $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$ and $B = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. By direct computation, $p_A(\lambda) = (2 - \lambda)^3 = p_B(\lambda)$, so that $\text{tr}(A) = \text{tr}(B)$ and $\det(A) = \det(B)$. Moreover $\text{tr}(A^k) = 3 \cdot 2^k = \text{tr}(B^k)$.
However, A and B are not similar. In fact, $\mu(2, A) = 1$ because $\ker(A - 2I) = \text{span}\{e_1\}$, whereas $\mu(2, B) = 2$ because $\ker(B - 2I) = \text{span}\{e_1, e_3\}$.

- If $L : V \longrightarrow V$ and $e \in \mathbb{F}$, then the subspaces $\ker[(L - eI)^k] \subseteq V$ for $k \geq 2$ are called **generalized eigenspaces**.
- If $D \in \mathcal{M}_{n \times n}(\mathbb{F})$ IS DIAGONAL, THEN $p_D(\lambda) = \prod_{i=1}^n (D_{ii} - \lambda)$, SO $p_D(\lambda)$ IS A PRODUCT OF POLYNOMIALS OF DEGREE 1 WITH COEFFICIENTS IN \mathbb{F} .
- If $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ IS SIMILAR TO A DIAGONAL MATRIX, THEN $p_A(\lambda)$ MUST BE A PRODUCT OF POLYNOMIALS OF DEGREE 1 WITH COEFFICIENTS IN \mathbb{F} .
- Example: the matrix $A = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \in \mathcal{M}_{2 \times 2}(\mathbb{Q})$ has $p_A(\lambda) = \lambda^2 - 2$, which is not factorizable over \mathbb{Q} . So A is not similar to a diagonal matrix with rational coefficients.
- An endomorphism $L : V \longrightarrow V$ is called **diagonalizable** if there exists a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V such that v_i is an eigenvector for L for every $i = 1, \dots, n$.
- $A : \mathbb{F}^n \longrightarrow \mathbb{F}^n$ IS DIAGONALIZABLE AS AN ENDOMORPHISM IF AND ONLY IF A IS SIMILAR TO A DIAGONAL MATRIX.

16. Thursday, 11/2

- Example/exercise: classifying rotations of \mathbb{R}^2 up to similarity
- EIGENSPACES OF $L : V \longrightarrow V$ CORRESPONDING TO DISTINCT EIGENVALUES INTERSECT ONLY IN $\{0\}$.
- AN ENDOMORPHISM $L : V \longrightarrow V$ OVER \mathbb{F} WITH $\dim_{\mathbb{F}} V = n$ IS DIAGONALIZABLE (OVER \mathbb{F}) IF AND ONLY IF V IS THE DIRECT SUM OF ITS EIGENSPACES, I.E. IF AND ONLY IF $\mu(e_1, L) + \dots + \mu(e_k, L) = n$ WHERE $e_1, \dots, e_k \in \mathbb{F}$ ARE THE EIGENVALUES OF L .
- IF ALL ROOTS OF THE THE CHARACTERISTIC POLYNOMIAL $p_L(\lambda)$ OF AN ENDOMORPHISM $L : V \longrightarrow V$ (V BEING A VECTOR SPACE OVER \mathbb{F}) ARE DISTINCT AND BELONG TO \mathbb{F} , THEN L IS DIAGONALIZABLE.
- Example of a matrix which is upper triangular but not diagonalizable.
- If a matrix A is similar to an upper triangular one, then it is similar to a lower triangular one.
- A matrix $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ is **triangularizable** if it is similar to an upper triangular matrix.
- A MATRIX A IS TRIANGULARIZABLE IF AND ONLY IF ALL THE ROOTS OF ITS CHARACTERISTIC POLYNOMIAL $p_A(\lambda)$ ARE IN \mathbb{F} . (The proof of the “if” part is postponed.)

- Example of a matrix A in $\mathcal{M}_{2 \times 2}(\mathbb{Q})$ with characteristic polynomial $p_A(\lambda) = \lambda^2 - 2$. Then A is not triangularizable in $\mathcal{M}_{2 \times 2}(\mathbb{Q})$. But if we interpret it as a matrix in $\mathcal{M}_{2 \times 2}(\mathbb{R})$, then it is even diagonalizable. Thus, diagonalizability and triangulability depend on the field \mathbb{F} we are working on.
- Given $p(t), q(t) \in \mathbb{F}[t]$, we say that $q(t)$ **divides** $p(t)$, or equivalently that $p(t)$ is a **multiple** of $q(t)$, if $\exists r(t) \in \mathbb{F}[t]$ such that $p(t) = q(t)r(t)$ and we will write $q(t)|p(t)$.
- A nonzero polynomial $p(t) \in \mathbb{F}[t]$ is **irreducible** if: $p(t) = q(t)r(t) \implies q(t) \in \mathbb{F}$ or $r(t) \in \mathbb{F}$.
- Two nonzero polynomials $p(t), q(t) \in \mathbb{F}[t]$ are **coprime** if no nonconstant polynomial divides both of them. In this case, we will write $GCD(p, q) = 1$.

- Similarities between the polynomials in one variable $\mathbb{F}[t]$ over a field and the integers \mathbb{Z} .

$\mathbb{F}[t]$	\mathbb{Z}
$\deg : \mathbb{F}[t] \setminus \{0\} \rightarrow \mathbb{N}$	$ \cdot : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{N}$
irreducible polynomials	prime numbers
Euclidean division	Euclidean division
$p(t)$ irred. and $p(t) q(t)r(t)$ then $p(t) q(t)$ or $p(t) r(t)$	p prime and $p qr$ then $p q$ or $p r$
unique factorization (up to constants)	unique factorization (up to signs)
if $GCD(p(t), q(t)) = 1$ then $a(t)p(t) + b(t)q(t) = 1$	if $GCD(p, q) = 1$ then $ap + bq = 1$

- *Unique factorization* means: given a nonzero polynomial $p(t) \in \mathbb{F}[t]$ then there exist irreducible polynomials $r_1(t), \dots, r_k(t) \in \mathbb{F}[t]$ and $c \in \mathbb{F}$ such that $p = cr_1r_2 \cdots r_k$. Moreover, if we ask the r_i 's to be *monic* (i.e. with the leading coefficient equal to 1), then $c \in \mathbb{F}$ and r_1, \dots, r_k are unique (up to permuting the r_i 's).
- Given $0 \neq p, q \in \mathbb{F}[t]$, their **greatest common divisor** $GCD(p, q)$ is the polynomial of largest degree that divides both p and q . It is well-defined up to multiplying by a nonzero constant.
- GIVEN $0 \neq p, q \in \mathbb{F}[t]$, THE $GCD(p, q)$ IS OBTAINED BY FACTORIZING p AND q AND MULTIPLYING TOGETHER THE COMMON IRREDUCIBLE FACTORS, TAKEN WITH THEIR SMALLER EXPONENT. (Exactly the same as for the integers.)
- Euclidean division in \mathbb{Z} : for every $q, p \in \mathbb{F}[t]$ with $p \neq 0$ there exist unique $m, r \in \mathbb{F}[t]$ such that $q = mp + r$ and r is either 0 or $|r| < |p|$.
- EUCLIDEAN DIVISION IN $\mathbb{F}[t]$: FOR EVERY $q(t), p(t) \in \mathbb{F}[t]$ WITH $p(t) \neq 0$ THERE EXIST UNIQUE $m(t), r(t) \in \mathbb{F}[t]$ SUCH THAT $q(t) = m(t)p(t) + r(t)$ AND $r(t)$ IS EITHER 0 OR $\deg(r(t)) < \deg(p(t))$. One reads: "dividing $q(t)$ by $p(t)$, I get quotient $m(t)$ and remained $r(t)$ ".

- If $0 \neq p, q \in \mathbb{F}[t]$ AND $GCD(p, q) = 1$, THEN THERE EXIST $a, b \in \mathbb{F}[t]$ SUCH THAT $ap + bq = 1$. (The same proof works in \mathbb{Z} , or wherever we have a Euclidean division.)
- If $0 \neq p(t), q(t) \in \mathbb{F}[t]$ ARE COPRIME POLYNOMIALS AND $L : V \rightarrow V$ IS AN ENDOMORPHISM OF A VECTOR SPACE V OVER \mathbb{F} , THEN $\ker(p(L)) \cap \ker(q(L)) = \{0\}$.

17. Tuesday, 11/7

- **Flags and complete flags** of a vector space V .
- If $L : V \rightarrow V$, definition of L -invariant subspace of V and L -invariant flag of V .
- Let $W \subseteq V$ be an L -invariant subspace and $Z \subseteq V$ be a complement of W so that $V = W \oplus Z$. Let $\mathcal{C} = \{w_1, \dots, w_k\}$ be a basis of W , $\mathcal{D} = \{z_1, \dots, z_{n-k}\}$ a basis of Z and $\mathcal{B} = \mathcal{C} \cup \mathcal{D}$ a basis of V .
Then $M_{\mathcal{B}}^{\mathcal{B}}(L) = \left(\begin{array}{c|c} A_{k \times k} & C_{k \times (n-k)} \\ \hline 0_{(n-k) \times k} & B_{(n-k) \times (n-k)} \end{array} \right)$.
If $L|_W^W : W \rightarrow W$ is the restriction (on the domain and the codomain) of L to W , then $A = M_{\mathcal{C}}^{\mathcal{C}}(L|_W^W)$.
Let $\pi : V = W \oplus Z \rightarrow Z$ be the surjective homomorphism defined as $\pi(w+z) = z$ and let $L|_Z : Z \rightarrow V$ be the restriction of L (in the domain). Then $B = M_{\mathcal{D}}^{\mathcal{D}}(\pi \circ L|_Z)$.
- Let $W \subseteq V$ be a vector subspace. Then V/W is the **quotient** of V by W , i.e. the quotient of V by the equivalence relation \sim that declares $v_1 \sim v_2$ if and only if $v_1 - v_2 \in W$.
- Elements in V/W are denoted by $v + W = [v] = \bar{v}$ and represent $v + W = \{v + w \in V \mid w \in W\}$.
The sum on V/W is defined as $[v_1] + [v_2] = [v_1 + v_2]$ and the scalar multiplication as $\lambda[v] = [\lambda v]$.
They are well-defined and the zero vector is $[0] = 0 + W$.
- The map $\pi : V \rightarrow V/W$ defined as $\pi(v) = [v]$ is called **canonical projection** and is a surjective homomorphism. Its kernel is W . So, $\dim(V/W) + \dim(W) = \dim(V)$.
- Example: $V = \mathbb{R}[t]$ and $W = \{\text{constant polynomials}\}$. Then V/W is the vector space of “real polynomials in t up to an additive constant”.
- LET $L : V \rightarrow Z$ BE A HOMOMORPHISM, LET $W \subseteq V$ BE A SUBSPACE OF V AND LET $\pi : V \rightarrow V/W$ BE THE CANONICAL PROJECTION. THEN: THERE EXISTS A HOMOMORPHISM $\bar{L} : V/W \rightarrow Z$ SUCH THAT $\bar{L} \circ \pi = L$ IF AND ONLY IF $W \subset \ker(L)$. MOREOVER, IF \bar{L} EXISTS, THEN IT IS UNIQUE.

$$\begin{array}{ccc}
 V & \xrightarrow{L} & Z \\
 \searrow \pi & & \nearrow \bar{L} \\
 & & V/W
 \end{array}
 \qquad
 \bar{L}([v]) = L(v)$$

- In the proposition above, $\ker(\bar{L}) = \ker(L)/W \subset V/W$.
- Example: $C^k(\mathbb{R})$ is the vector space of functions $f : \mathbb{R} \rightarrow \mathbb{R}$ that are k -times differentiable and such that $f^{(k)}$ is continuous.
Let $D = d/dx : C^1(\mathbb{R}) \rightarrow C^0(\mathbb{R})$ be the derivative; it is surjective but not injective, because $\ker(D) = \{\text{constant functions}\}$. Hence, there exists $\bar{D} : C^1(\mathbb{R})/\ker(D) \rightarrow C^0(\mathbb{R})$ and it is injective. Moreover, it is surjective, because D is. Hence, it is an isomorphism and the fundamental theorem of calculus tells us that \bar{D}^{-1} is exactly the indefinite integral.
Thus, the indefinite integral gives us “a function up to an additive constant”, that is an element of $C^1(\mathbb{R})/\ker(D)$.
- Back to $L : V \rightarrow V$ and $W \subseteq V$ an L -invariant subspace, with $W \oplus Z = V$ and $\mathcal{D} = \{z_1, \dots, z_{n-k}\}$ a basis of Z .
There is an induced map $\tilde{L} : V/W \rightarrow V/W$.
The set $\mathcal{E} = \{[z_1], \dots, [z_{n-k}]\}$ is a basis of V/W and $B = M_{\mathcal{E}}^{\mathcal{E}}(\tilde{L})$.
- An endomorphism $L : V \rightarrow V$ is **triangulable** if there exists a complete L -invariant flag for V .
- L IS TRIANGULABLE IF AND ONLY IF THERE EXISTS A BASIS \mathcal{B} OF V SUCH THAT $M_{\mathcal{B}}^{\mathcal{B}}(L)$ IS UPPER TRIANGULAR.
- Hence, a matrix $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ is similar to an upper triangular matrix if and only if the homomorphism $A : \mathbb{F}^n \rightarrow \mathbb{F}^n$ is triangulable.
- LET V BE A VECTOR SPACE OF FINITE DIMENSION OVER THE FIELD \mathbb{F} . AN ENDOMORPHISM $L : V \rightarrow V$ IS TRIANGULABLE IF AND ONLY IF THE CHARACTERISTIC POLYNOMIAL $p_L(\lambda)$ IS COMPLETELY FACTORIZABLE OVER \mathbb{F} .
- A field Ω is **algebraically closed** if every nonconstant polynomial $p(t) \in \Omega[t]$ has a root in Ω .
- An extension of fields $\mathbb{F} \subseteq \Omega$ is a couple of fields \mathbb{F}, Ω such that \mathbb{F} is a subfield of Ω .
- If Ω is algebraically closed, then every $p(t) \in \Omega[t]$ is completely factorizable (i.e. either is a constant or is a product of polynomials of degree 1 in $\Omega[t]$).
- FUNDAMENTAL THEOREM OF ALGEBRA: THE FIELD OF COMPLEX NUMBERS IS ALGEBRAICALLY CLOSED. (Without proof.)
- AS A CONSEQUENCE, ALL MATRICES IN $\mathcal{M}_{n \times n}(\mathbb{C})$ ARE SIMILAR TO AN UPPER TRIANGULAR ONE.
- FOR EVERY FIELD \mathbb{F} , THERE EXISTS AN EXTENSION OF FIELDS $\mathbb{F} \subseteq \Omega$ WITH Ω ALGEBRAICALLY CLOSED. (Without proof.)

- Examples: \mathbb{Q} and $\mathbb{Q}(i)$ are not algebraically closed, because $t^k + 2$ is irreducible over \mathbb{Q} for every $k \geq 1$; \mathbb{R} is not algebraically closed, because $t^2 + 1$ is irreducible over \mathbb{R} ; $\mathbb{Z}/5$ is not algebraically closed, because $t^2 + 2$ is irreducible in $\mathbb{Z}/5$; $\mathbb{Z}/3$ is not algebraically closed, because $t^2 + 1$ is irreducible in $\mathbb{Z}/3$.
- AN ALGEBRAICALLY CLOSED FIELD IS INFINITE. (No proof.)
- Hence, \mathbb{Z}/p is not algebraically closed for any p .

18. Thursday, 11/9

- More detailed proof of: L IS TRIANGULABLE IF AND ONLY IF THERE EXISTS A BASIS \mathcal{B} OF V SUCH THAT $M_{\mathcal{B}}^{\mathcal{B}}(L)$ IS UPPER TRIANGULAR.
- *Definition of an L -cyclic subspace $W \subseteq V$ for $L : V \rightarrow V$. Definition of $C_L(v) := \mathbb{F}[L] \cdot v \subseteq V$.*
- $C_L(v)$ IS THE SMALLEST L -INVARIANT SUBSPACE OF V THAT CONTAINS THE VECTOR $v \in V$.
- IF $\dim C_L(v) = k$, THEN $\mathcal{B} = \{v, L(v), L^2(v), \dots, L^{k-1}(v)\}$ IS A BASIS OF $C_L(v)$.
- *Definition of **companion matrix** associated to a polynomial $q(t)$.*

- Example: $M = \begin{pmatrix} 0 & 0 & 0 & \alpha_0 \\ 1 & 0 & 0 & \alpha_1 \\ 0 & 1 & 0 & \alpha_2 \\ 0 & 0 & 1 & \alpha_3 \end{pmatrix}$ is the companion matrix associated to $\lambda^4 - \alpha_3\lambda^3 - \alpha_2\lambda^2 - \alpha_1\lambda - \alpha_0 = p_M(\lambda)$.

- THE COMPANION MATRIX M ASSOCIATED TO $q(\lambda)$ HAS CHARACTERISTIC POLYNOMIAL $p_M(\lambda) = q(\lambda)$.
- IF $L : V \rightarrow V$ AND V IS L -CYCLIC (THAT IS, $\exists v \in V$ SUCH THAT $V = C_L(v)$), THEN $p_L(L) = 0 \in \text{End}(V)$.
- (CAYLEY-HAMILTON THEOREM.) IF $L : V \rightarrow V$ (V OF FINITE DIMENSION), THEN $p_L(L) = 0 \in \text{End}(V)$.
- *Definition of an **ideal** $I \subsetneq \mathbb{F}[t]$. Definition of $(q(t)) = \{q(t) \cdot r(t) \in \mathbb{F}[t] \mid r(t) \in \mathbb{F}[t]\}$.*
- A polynomial $q(t) \in \mathbb{F}[t]$ is **monic** if its leading term has coefficient 1.
- EVERY IDEAL $I \subsetneq \mathbb{F}[t]$ IS OF THE FORM $(q(t))$ FOR A UNIQUE MONIC POLYNOMIAL $q(t) \in \mathbb{F}[t]$.
- Recall: $\text{ev}_L : \mathbb{F}[t] \rightarrow \text{End}(V)$ defined as $\text{ev}_L(q(t)) = q(L)$ is a homomorphism of vector spaces. Moreover, $\text{ev}_L(q(t)r(t)) = \text{ev}_L(q(t))\text{ev}_L(r(t))$.
- Call $I_L \subset \mathbb{F}[t]$ the kernel of ev_L .

- If $A \in \mathcal{M}_{n \times n}(\mathbb{F})$, then I_A is invariant under similitude.
- Call **minimal polynomial** of L the monic polynomial $p_{min,L} \in \mathbb{F}[t]$ such that $(p_{min,L}) = I_L$.
- THE MINIMAL POLYNOMIAL $p_{min,A}$ OF A MATRIX $A \in \mathcal{M}_{n \times n}(\mathbb{F})$ IS INVARIANT UNDER SIMILITUDE.

• Examples: $L_1 = \left(\begin{array}{c|cccc} 2 & 0 & 0 & 0 & 0 \\ \hline 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{array} \right), \quad L_2 = \left(\begin{array}{cc|ccc} 2 & 1 & 0 & 0 & 0 \\ \hline 0 & 2 & 0 & 0 & 0 \\ \hline 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{array} \right).$

In both cases, $p_{L_1}(\lambda) = p_{L_2}(\lambda) = (2 - \lambda)^5$.

However, $p_{min,L_1}(\lambda) = (\lambda - 2)^4$ but $p_{min,L_2}(\lambda) = (\lambda - 2)^3$.

Hence, L_1 is not similar to L_2 .

- Cayley-Hamilton theorem $\implies p_L \in I_L \implies p_{min,L} | p_L$

19. Tuesday, 11/14

- Fix V a vector space of dimension n over \mathbb{F} and fix $f : V \rightarrow V$ an endomorphism. Let $p_f = r_1^{\alpha_1} \cdots r_k^{\alpha_k}$ be the characteristic polynomial of f (with r_i irreducible, $(r_i, r_j) = 1$ for $i \neq j$ and $\alpha_i \geq 1$), $p_{f,min}$ the minimal polynomial of f . Let $I_f = (p_{f,min})$ the ideal of polynomials $q(t)$ such that $q(f) = 0$.
- For every $e \in \mathbb{F}$, the **geometric multiplicity** of e is $\mu_{geom}(e) = \dim \ker(f - eI)$ and the **algebraic multiplicity** of e is $\mu_{alg}(e) = \max\{k \in \mathbb{N} \mid (t - e)^k \text{ divides } p_f\}$.
- We always have $\mu_{geom}(e) \leq \mu_{alg}(e)$
- LET $q_1, q_2 \in \mathbb{F}[t]$ AND $q_1 q_2 \in I_f$, THEN $V = \ker(q_1(f)) \oplus \ker(q_2(f))$.
- PRIMARY DECOMPOSITION: $V = \ker(r_1^{\alpha_1}(f)) \oplus \ker(r_2^{\alpha_2}(f)) \oplus \cdots \oplus \ker(r_k^{\alpha_k}(f))$ AND $\ker(r_i^{\alpha_i}(f))$ IS f -INVARIANT FOR $i = 1, \dots, k$
- Call $V_i = \ker(r_i^{\alpha_i}(f))$ and $f_i : V_i \rightarrow V_i$ the restriction of f to V_i
- THE MINIMAL POLYNOMIAL p_f IS THE LEAST COMMON MULTIPLE OF $p_{f_1}, p_{f_2}, \dots, p_{f_k}$.
- LET $s(t) \in \mathbb{F}[t]$ AND DEFINE $W_k = \ker[s(f)^k]$, SO THAT $W_0 = \{0\} \subseteq W_1 \subseteq W_2 \subseteq \cdots \subseteq V$. LET i BE SUCH THAT $W_i = W_{i+1}$. THEN $W_i = W_j$ FOR EVERY $j \geq i$.
- In particular, if $\ker(r_i^{\alpha_i}(f)) \neq \{0\}$, then $\ker(r_i(f)) \neq \{0\}$.
- IF $g : W \rightarrow W$ AND $p_{g,min} = r^\beta$ WITH r IRREDUCIBLE, THEN $p_g = r^\alpha$ WITH $\alpha \geq \beta$
- $p_f = p_{f_1} p_{f_2} \cdots p_{f_k}$ AND $p_{f_i} = r_i^{\alpha_i}$, SO THAT $\dim \ker(r_i^{\alpha_i}(f)) = \alpha_i \deg(r_i)$
- $p_{f_i,min} = r_i^{\beta_i}$ WITH $1 \leq \beta_i \leq \alpha_i$ AND $p_{f,min} = r_1^{\beta_1} \cdots r_k^{\beta_k}$

- Let \mathcal{B}_i is a basis of V_i so that $\mathcal{B} = \mathcal{B}_1 \cup \dots \cup \mathcal{B}_k$ is a basis of V . The matrix representing f with respect to \mathcal{B} looks like

$$M_{\mathcal{B}}^{\mathcal{B}}(f) = \left(\begin{array}{c|c|c|c} M_1 & 0 & 0 & 0 \\ \hline 0 & M_2 & 0 & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & 0 & M_k \end{array} \right)$$

where $M_i = M_{\mathcal{B}_i}^{\mathcal{B}_i}(f_i)$, so that $p_{M_i} = r_i^{\alpha_i}$ and M_i is a square matrix of size $\alpha_i \deg(r_i)$.

- Now on, assume $r_i = (e_i - t)$, so that p_f is completely factorizable and f is triangulable (this always happens if \mathbb{F} is algebraically closed, for example $\mathbb{F} = \mathbb{C}$)
- JORDAN CANONICAL FORM: THERE EXISTS A BASIS \mathcal{B}_i OF V_i SUCH THAT

$$M_i = M_{\mathcal{B}_i}^{\mathcal{B}_i}(f_i) = \left(\begin{array}{c|c|c|c} B_{e_i, l_{i,1}} & 0 & 0 & 0 \\ \hline 0 & B_{e_i, l_{i,2}} & 0 & 0 \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & 0 & B_{e_i, l_{i, i_m}} \end{array} \right)$$

WHERE $B_{e_i, l} = B_{0, l} + e_i I_l$ IS CALLED **Jordan block** AND

$$B_{0, l} = \left(\begin{array}{cccccc} 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 \end{array} \right)$$

IS AN $l \times l$ STRICTLY LOWER-TRIANGULAR MATRIX SUCH THAT $(B_{0, l})_{a+1, a} = 1$ FOR $a = 1, \dots, l-1$ AND $(B_{0, l})_{a, b} = 0$ IF $a \neq b+1$ (SO THAT $B_{0, l}^{l-1} \neq 0$). FOR INSTANCE, A JORDAN BLOCK OF SIZE l CORRESPONDING TO THE EIGENVALUE e IS

$$B_{e, l} = \left(\begin{array}{cccccc} e & 0 & 0 & 0 & \dots & 0 \\ 1 & e & 0 & 0 & \dots & 0 \\ 0 & 1 & e & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & e & 0 \\ 0 & 0 & 0 & \dots & 1 & e \end{array} \right)$$

MOREOVER:

- (A) $m_i = \mu_{geom}(e_i)$
(I.E. THE NUMBER OF JORDAN BLOCKS IN M_i IS GIVEN BY $\dim E_{e_i}$)
- (B) $l_{i,1} + l_{i,2} + \dots + l_{i, m_i} = \mu_{alg}(e_i)$
(I.E. THE TOTAL SIZE OF M_i IS $\mu_{alg}(e_i) = \alpha_i$)

- (C) $\beta_i = \max\{l_{i,h} \mid h = 1, 2, \dots, m\}$
 (I.E. THE EXPONENT OF $(t - e_i)$ IN $p_{f,min}$ IS THE SIZE OF THE BIGGEST BLOCK)
- (D) $\dim(\ker(f - e_i I)^s) - \dim(\ker(f - e_i I)^{s-1}) = \#\{h \mid l_{i,h} \geq s\}$
 (I.E. THE NUMBER OF BLOCKS OF SIZE AT LEAST s)

- THE JORDAN CANONICAL FORM OF f IS UNIQUE UP TO REORDERING THE EIGENVALUES e_1, \dots, e_k AND UP TO PERMUTING THE BLOCKS CORRESPONDING TO THE SAME EIGENVALUE. FOR INSTANCE, IF WE ORDER THE BLOCKS CORRESPONDING TO THE SAME EIGENVALUE BY DECREASING LENGTH (I.E. IN SUCH A WAY THAT $l_{i,h} \geq l_{i,h+1}$ FOR $h = 1, \dots, m_i - 1$), THEN EACH M_i IS UNIQUELY DETERMINED AND SO THE JORDAN FORM OF f IS UNIQUE UP TO REORDERING THE EIGENVALUES.
- TWO MATRICES A AND B (SUCH THAT p_A AND p_B ARE COMPLETELY FACTORIZABLE) HAVE THE “SAME” JORDAN CANONICAL FORM IF AND ONLY IF $\dim \ker(A - e_i I)^s = \dim \ker(B - e_i I)^s$ FOR EVERY $e_i \in \mathbb{F}$ AND EVERY INTEGER $s > 0$.
- Next time: analogous (more complicated) statements hold if p_f is not completely factorizable. For instance, two matrices A and B are similar if and only if $p_A = p_B = r_1^{\alpha_1} \cdots r_k^{\alpha_k}$ and $\dim \ker(r_i^s(A)) = \dim \ker(r_i^s(B))$ for every $i = 1, \dots, k$ and every integer $s > 0$. The canonical form in this case is called **rational canonical form**.

21. Tuesday, 11/21

- Examples of diagonalizable matrices
- Conditions that are equivalent to diagonalizability
- Explicit computations of $\ker(f - eI)^k$ and minimal polynomials

22. Tuesday, 11/28

- Examples of matrices in triangular form and Jordan form
- Conditions that are equivalent to triangularizability
- Explicit computations of $\ker(f - eI)^k$ and minimal polynomial
- Jordan block and Jordan forms

23. Thursday, 11/30

- Explicit construction of Jordan basis for a given matrix (sketches of proof, no general abstract proof) with a single eigenvalue: the blocks are ordered by decreasing size
- LET V BE A VECTOR SPACE OF FINITE DIMENSION OVER \mathbb{F} . FOR EVERY ENDOMORPHISM $f : V \rightarrow V$ WITH COMPLETELY FACTORIZABLE CHARACTERISTIC POLYNOMIAL $p_f(t)$, THERE EXISTS A BASIS \mathcal{B} OF V SUCH THAT $M_{\mathcal{B}}^{\mathcal{B}}(f)$ IS IN JORDAN FORM. THIS FORM IS UNIQUE UP TO PERMUTING THE EIGENVALUES.

- LET $A, B \in \mathcal{M}_{n \times n}(\mathbb{F})$ WITH $p_A(t)$ AND $p_B(t)$ COMPLETELY FACTORIZABLE. THEN A AND B ARE SIMILAR \iff THEY HAVE THE SAME JORDAN FORM $\iff \dim \ker(A - eI)^k = \dim \ker(B - eI)^k$ FOR EVERY $k > 0$ AND EVERY $e \in \mathbb{F}$.
- Lengths of vectors: example of Euclidean norm (standard norm) on \mathbb{R}^n
- *Definition of a norm* $N : V \rightarrow \mathbb{R}$ on a vector space V over \mathbb{R} (also over \mathbb{C} or any subfield of \mathbb{C})
- Example of the norms $N_1(X) = |x_1| + |x_2| + \dots + |x_n|$ and $N_\infty(X) = \max\{|x_1|, |x_2|, \dots, |x_n|\}$. Picture of vectors of unit norm in \mathbb{R}^2 for N_1 , N_∞ and the standard norm.
- Example of the standard scalar product in \mathbb{R}^n (on the book you can find the names: “scalar product” and “symmetric bilinear form”; “inner product” is sometimes used to denote a positive-definite scalar product)
- *Definition of a bilinear form* $b : V \times V \rightarrow \mathbb{F}$, of a **symmetric bilinear form** and of a **skew-symmetric bilinear form**.
- For a vector space V over \mathbb{R} , definition of a **positive-definite symmetric bilinear form** and its associated norm.
- Examples of bilinear forms using matrices: for $V = \mathbb{F}^n$, define $b(v, w) = {}^t v \cdot B \cdot w$ for $v, w \in V$, where $B \in \mathcal{M}_{n \times n}(\mathbb{F})$. Then b is a bilinear form on V .
- Representation of a bilinear form $b : V \times V \rightarrow \mathbb{F}$ in coordinates using a basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V . If we want B to be the matrix $M_{\mathcal{B}}(b)$ that represents b with respect to \mathcal{B} , then we require $b(v, w) = {}^t M_{\mathcal{B}}(w) \cdot B \cdot M_{\mathcal{B}}(v)$ for all $v, w \in V$. This implies $B_{ij} = {}^t e_j \cdot B \cdot e_i = b(v_j, v_i)$, which we take as a definition of $B = M_{\mathcal{B}}(b)$.
- Example of $V = \mathbb{R}[t]_{\leq 2}$ with $b : V \times V \rightarrow \mathbb{R}$ defined as $b(p(t), q(t)) = p(0)q(1) + p(1)q(0)$. Computation of the matrix $M_{\mathcal{C}}(b)$ with respect to the basis $\mathcal{C} = \{1, t, t^2\}$.
- A BILINEAR FORM $b : V \times V \rightarrow \mathbb{F}$ IS SYMMETRIC IF AND ONLY IF THERE EXISTS A BASIS \mathcal{B} OF V SUCH THAT $M_{\mathcal{B}}(b)$ IS A SYMMETRIC MATRIX. (Analogous statement for a skew-symmetric bilinear form.)

24.-25. Tuesday, 12/5 and Thursday, 12/7

- Notation: $\text{GL}(n, \mathbb{F}) = \{N \in \mathcal{M}_{n \times n}(\mathbb{F}) \mid \det(N) \neq 0\}$ is the **general linear group**.
 $\text{SL}(n, \mathbb{F}) = \{N \in \mathcal{M}_{n \times n}(\mathbb{F}) \mid \det(N) = 1\}$ is the **special linear group**.
 $\text{O}(n, \mathbb{F}) = \{N \in \mathcal{M}_{n \times n}(\mathbb{F}) \mid {}^t N N = I\}$ is the **orthogonal group**.
 In general, if $A \in \text{O}(n, \mathbb{F})$, then $\det(A) = \pm 1$.
 $\text{SO}(n, \mathbb{F}) = \{N \in \mathcal{M}_{n \times n}(\mathbb{F}) \mid {}^t N N = I \text{ and } \det(N) = 1\}$ is the **special orthogonal group**.
 Saying that the subsets above are **groups of matrices** means that they are closed under matrix multiplication and taking inverses. For sure, they are not vector subspaces of $\mathcal{M}_{n \times n}(\mathbb{F})$, because they do not contain the zero matrix.

Instead, $\mathcal{S}(n, \mathbb{F}) = \{N \in \mathcal{M}_{n \times n}(\mathbb{F}) \mid {}^t N = N\} \subset \mathcal{M}_{n \times n}(\mathbb{F})$ is the vector subspace of **symmetric matrices**.

$\mathcal{A}(n, \mathbb{F}) = \{N \in \mathcal{M}_{n \times n}(\mathbb{F}) \mid {}^t N = -N\} \subset \mathcal{M}_{n \times n}(\mathbb{F})$ is the vector subspace of **skew-symmetric matrices**.

- If V is a vector space of dimension n , then $\text{GL}(V) = \{f : V \rightarrow V \mid \det(f) \neq 0\}$, which is also denoted as $\text{Aut}(V)$ and is called **group of automorphisms of V** .

$\text{SL}(V) = \{f : V \rightarrow V \mid \det(f) = 1\}$.

If V is endowed with a **nondegenerate** bilinear form $b : V \times V \rightarrow \mathbb{F}$, then $\text{O}(V, b) = \{f : V \rightarrow V \mid b(f(v), f(w)) = b(v, w) \forall v, w \in V\}$ is called **group of orthogonal transformations of (V, b)** . If $\text{char}(\mathbb{F}) \neq 2$ and $q(v) = b(v, v)$ is the quadratic form associated to b , then $\text{O}(V, b) = \text{O}(V, q) = \{f : V \rightarrow V \mid q(f(v)) = q(v) \forall v \in V\}$.

In general, if $f \in \text{O}(V, b)$, then $\det(f) = \pm 1$.

$\text{SO}(V, b) = \{f : V \rightarrow V \mid b(f(v), f(w)) = b(v, w) \forall v, w \in V \text{ and } \det(f) = 1\}$.

Saying that the subsets above are **groups of automorphisms of V** means that they are closed under composition and taking inverses.

- Example: let $B \in \text{GL}(n, \mathbb{F}) \cap \mathcal{S}(n, \mathbb{F})$ represent a nondegenerate scalar product on \mathbb{F}^n . Then $\text{O}(\mathbb{F}^n, B) = \{N \in \mathcal{M}_{n \times n}(\mathbb{F}) \mid {}^t NBN = B\}$.
- Example: $V = \mathbb{R}^2$ and $b = \langle \cdot, \cdot \rangle$ is the standard scalar product. Then an orthogonal matrix $A \in \text{O}(2, \mathbb{R})$ looks like: $A = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ if $\det(A) = 1$ (it is a rotation of an angle θ centered at the origin of \mathbb{R}^2); or $A = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$ if $\det(A) = -1$ (it is a reflection with respect to a line passing through the origin of \mathbb{R}^2).
- Two matrices $A, B \in \mathcal{M}_{n \times n}(\mathbb{F})$ are **congruent** if there exists $N \in \text{GL}(n, \mathbb{F})$ such that $A = {}^t NBN$.
- If (V, b) is a vector space with a symmetric bilinear form and \mathcal{B}, \mathcal{C} are two bases of V , then $\boxed{M_{\mathcal{B}}(b) = {}^t M_{\mathcal{C}}^{\mathcal{B}} M_{\mathcal{C}}(b) M_{\mathcal{C}}^{\mathcal{B}}}$, i.e. $M_{\mathcal{B}}(b)$ and $M_{\mathcal{C}}(b)$ are congruent.
- If (V, b) is a vector space with a symmetric bilinear form and $W \subset V$ is a vector subspace, denote by $b|_W$ the **restriction of b to W** .
- A nonzero vector $v \in V$ is **isotropic** if $b(v, v) = 0$. A subspace $W \subset V$ is **isotropic** if the restriction $b|_W$ is zero. A subspace $W \subset V$ is **maximally isotropic** if it is of maximal dimension among all isotropic subspaces.
- Remark: if V is a real vector space and b is positive-definite (or negative-definite), then there are no isotropic vectors in V .
- Example: $V = \mathbb{R}^2$ and $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ representing a symmetric bilinear form. Then B is nondegenerate but e_1 and e_2 are isotropic. In fact, $W = \text{span}\{e_1\}$ is a maximal isotropic subspace of (\mathbb{R}^2, B) .

- $q : V \longrightarrow \mathbb{F}$ is a **quadratic form** if $q(\lambda v) = \lambda^2 q(v)$ for every $\lambda \in \mathbb{F}$ and $v \in V$ and moreover the form $b_q(\cdot, \cdot) : V \times V \longrightarrow \mathbb{F}$ defined as $b_q(v, w) := q(v + w) - q(v) - q(w)$ is a symmetric bilinear form.
- Example: $V = \mathbb{R}^n$ and $q(X) = x_1^2 + x_2^2 + \cdots + x_n^2$ (standard quadratic form).
- GIVEN A SYMMETRIC BILINEAR FORM $b : V \times V \longrightarrow \mathbb{F}$ WE CAN DEFINE A QUADRATIC FORM $q : V \longrightarrow \mathbb{F}$, SETTING $q(v) := b(v, v)$. CONVERSELY, IF $\text{char}(\mathbb{F}) \neq 2$, GIVEN A QUADRATIC FORM q WE CAN DEFINE A SYMMETRIC BILINEAR FORM b , SETTING $b(v, w) := \frac{q(v + w) - q(v) - q(w)}{2}$ (**polarization formula**). THESE OPERATIONS ARE INVERSES OF EACH OTHER.
- Given $b : V \times V \longrightarrow \mathbb{F}$ bilinear, we can define two homomorphisms $L_b : V \longrightarrow V^*$ as $L_b(v) = b(v, \cdot)$ and $R_b : V \longrightarrow V^*$ as $R_b(v) = b(\cdot, v)$. If b is symmetric, then $L_b = R_b$. If b is skew-symmetric, then $L_b = -R_b$. In any case, L_b is the homomorphism **dual** to R_b , so that L_b is invertible if and only if R_b is.
IF \mathcal{B} IS A BASIS OF V AND \mathcal{B}^* IS THE DUAL BASIS OF V^* , THEN $M_{\mathcal{B}}(b) = M_{\mathcal{B}^*}^{\mathcal{B}}(R_b)$.
CONSEQUENTLY, ${}^t M_{\mathcal{B}}(b) = M_{\mathcal{B}^*}^{\mathcal{B}}(L_b)$.
- A bilinear form $b : V \times V \longrightarrow \mathbb{F}$ is **nondegenerate** if $R_b : V \longrightarrow V^*$ (or equivalently L_b) is injective. Otherwise, it is said **degenerate**.
- If $b : V \times V \longrightarrow \mathbb{F}$ is a symmetric bilinear form (also called “scalar product”), then $\ker(R_b) = \ker(L_b)$ is called **radical of b** and is denoted by $\text{Rad}(b)$.
- Example: $V = \mathbb{R}[t]_{\leq 2}$ with $b : V \times V \longrightarrow \mathbb{R}$ defined as $b(p(t), q(t)) = p''(0)q(0) + p(0)q''(0)$. Computation of the matrix $M_{\mathcal{C}}(b)$ with respect to the basis $\mathcal{B} = \{1, t, t^2\}$:
$$M_{\mathcal{B}}(b) = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{pmatrix}$$
 and so b is degenerate and $\text{Rad}(b) = \text{span}\{t\}$.
- LET (V, b) BE A VECTOR SPACE WITH A DEGENERATE SCALAR PRODUCT. IF $V = \text{Rad}(b) \oplus W$, THEN THE RESTRICTION $b|_W$ IS NONDEGENERATE. MOREOVER, THERE IS AN INDUCED WELL-DEFINED SCALAR PRODUCT $\bar{b} : (V/\text{Rad}(b)) \times (V/\text{Rad}(b)) \longrightarrow \mathbb{F}$ ON $V/\text{Rad}(b)$, DEFINED AS $\bar{b}([v], [w]) = b(v, w)$, AND \bar{b} IS NONDEGENERATE.
- If (V, b) is a vector space with a scalar product, then two vectors $v, w \in V$ are **orthogonal** if $b(v, w) = 0$. Two subspaces $W_1, W_2 \subset V$ are **orthogonal** to each other if $b(w_1, w_2) = 0$ for every $w_1 \in W_1$ and $w_2 \in W_2$. Given a subspace $W \subset V$, its **orthogonal** is $W^\perp := \{v \in V \mid b(v, w) = 0 \ \forall w \in W\}$.
- A basis $\mathcal{B} = \{v_1, \dots, v_n\}$ of V is an **orthogonal basis** for the scalar product $b : V \times V \longrightarrow \mathbb{F}$ if $b(v_i, v_j) = 0$ for $i \neq j$. It is an **orthonormal basis** if moreover $b(v_i, v_i) = 0$ for every $i = 1, \dots, n$.
- Rephrasing: a vector is isotropic if it is orthogonal to itself; a vector belongs to the radical if it is orthogonal to all the other vectors; a basis \mathcal{B} is orthogonal for b if and

only if $M_{\mathcal{B}}(b)$ is a diagonal matrix; a basis \mathcal{B} is orthonormal for b if and only if $M_{\mathcal{B}}(b)$ is the identity matrix.

- $W^\perp = \text{Ann}(R_b(W))$.
- IF b IS NONDEGENERATE AND $W \subset V$ IS A SUBSPACE, THEN $\dim W + \dim W^\perp = \dim V$.
- $W^\perp \cap W = \{0\}$ IF AND ONLY IF $b|_W$ IS A NONDEGENERATE SCALAR PRODUCT ON W .
- IF (V, b) IS A VECTOR SPACE WITH NONDEGENERATE SCALAR PRODUCT AND $W \subset V$ IS A SUBSPACE SUCH THAT THE RESTRICTION $b|_W$ IS NONDEGENERATE, THEN $V = W \oplus W^\perp$.
- Example: $V = \mathbb{R}^2$, $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ representing a symmetric bilinear form and $W = \text{span}\{e_1\}$. Then $W^\perp = W$ and, in fact, the restriction $b|_W = 0$.
- FOR EVERY (V, b) VECTOR SPACE ENDOWED WITH A SCALAR PRODUCT THERE EXISTS AN ORTHOGONAL BASIS \mathcal{B} . (Idea of the proof: write $V = \text{Rad}(b) \oplus W$, so that $b|_W$ is nondegenerate. Let $\{u_1, \dots, u_k\}$ be a basis of $\text{Rad}(b)$. If we find $\{w_1, \dots, w_{n-k}\}$ orthogonal basis of $(W, b|_W)$, then $\mathcal{B} = \{u_1, \dots, u_k, w_1, \dots, w_{n-k}\}$ will be an orthogonal basis of (V, b) . So that we can assume without loss of generality that (V, b) is nondegenerate.
By induction on $n = \dim V$. For $n = 1$ there is nothing to prove. For $n > 1$, take $v_1 \in V$ nonisotropic (which exists, because b is nondegenerate). Define $V_1 = \text{span}\{v_1\}$ and let $V = V_1 \oplus V_1^{\text{perp}}$, because $b|_{V_1}$ is nondegenerate. The restriction of b to V_1^\perp is also nondegenerate, so there exists an orthogonal basis $\{v_2, \dots, v_n\}$ of $(V_1^\perp, b|_{V_1^\perp})$ by inductive hypothesis. Take $\mathcal{B} = \{v_1, \dots, v_n\}$.
- Remark: if $\mathbb{F} = \mathbb{C}$ and $\mathcal{B} = \{v_1, \dots, v_n\}$ is an orthogonal basis of (V, b) , we can set $v'_k := \frac{v_k}{\sqrt{b(v_k, v_k)}}$ (choose one complex square root) in such a way that $b(v'_k, v'_k) = 1$. Hence, $\mathcal{B}' = \{v'_1, \dots, v'_n\}$ is an orthogonal basis of (V, b) .
- EVERY COMPLEX VECTOR SPACE V ENDOWED WITH A NONDEGENERATE SCALAR PRODUCT b ADMITS AN ORTHONORMAL BASIS \mathcal{B} . EQUIVALENTLY, EVERY INVERTIBLE $n \times n$ SYMMETRIC MATRIX $S \in \text{GL}(n, \mathbb{C}) \cap \mathcal{S}(n, \mathbb{C})$ IS CONGRUENT TO THE IDENTITY MATRIX.
- Example: $V = \mathbb{R}^2$, $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ representing a symmetric bilinear form. Take $v_1 = e_1 + e_2$, which is nonisotropic because $b(v_1, v_1) = 2$. Set $V_1 = \text{span}\{v_1\}$. Then $V_1^\perp = \text{span}\{v_2\}$ where $v_2 = e_1 - e_2$ and $b(v_2, v_2) = -2$. So $\mathcal{B} = \{v_1, v_2\}$ is an orthogonal basis of (V, B) . Notice that $M_{\mathcal{B}}(B) = \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$.

- Remark: if $\mathbb{F} = \mathbb{R}$ and $\mathcal{B} = \{v_1, \dots, v_n\}$ is an orthogonal basis of (V, b) , we can set $v'_k := \frac{v_k}{\sqrt{|b(v_k, v_k)|}}$ in such a way that $b(v'_k, v'_k) = \pm 1$. Hence, up to rearranging the vectors in the basis $\mathcal{B}' = \{v'_1, \dots, v'_n\}$ we obtain $M_{\mathcal{B}'}(b) = \left(\begin{array}{c|c} I_p & 0 \\ \hline 0 & -I_{n-p} \end{array} \right)$.
- We call $(p, n - p)$ (or sometimes just $p - (n - p) = 2p - n$) the **signature** of b .
- IF V IS A REAL VECTOR SPACE AND b IS A NONDEGENERATE SCALAR PRODUCT ON V , THEN THE SIGNATURE OF b IS WELL-DEFINED: IN PARTICULAR, p IS THE MAXIMAL DIMENSION OF A SUBSPACE $W^+ \subset V$ SUCH THAT $b|_{W^+}$ IS POSITIVE-DEFINITE AND $n - p$ IS THE MAXIMAL DIMENSION OF A SUBSPACE $W^- \subset V$ SUCH THAT $b|_{W^-}$ IS NEGATIVE-DEFINITE.
- (SYLVESTER) TWO REAL INVERTIBLE $n \times n$ SYMMETRIC MATRICES $A, B \in \text{GL}(n, \mathbb{R}) \cap \mathcal{S}(n, \mathbb{R})$ ARE CONGRUENT IF AND ONLY IF THEY REPRESENT SCALAR PRODUCTS ON \mathbb{R}^n WITH THE SAME SIGNATURE.
- IF (V, b) IS A REAL VECTOR SPACE, b IS A SCALAR PRODUCT WITH SIGNATURE $(p, n - p)$ AND $U \subset V$ IS AN ISOTROPIC SUBSPACE, THEN $\dim U \leq \min\{p, n - p\}$. MOREOVER, THE EQUALITY IS ATTAINED FOR A MAXIMAL ISOTROPIC SUBSPACE. (Idea of the proof: if $W^+ \subset V$ is a subspace such that $b|_{W^+}$ is positive-definite, then $U \cap W^+ = \{0\}$, which implies that $\dim U + \dim W^+ \leq n \implies \dim U \leq n - p$. Using W^- , we find $\dim U \leq p$, so that $\dim U \leq \min\{p, n - p\}$. To produce an isotropic U that gives the equality, take an orthogonal basis $\mathcal{B} = \mathcal{B}^+ \cup \mathcal{B}^-$ with $\mathcal{B}^+ = \{v_1, \dots, v_p\}$ and $\mathcal{B}^- = \{w_1, \dots, w_{n-p}\}$ such that $b(v_i, v_i) = 1$ and $b(w_j, w_j) = -1$. Suppose that $p \leq n - p$ (otherwise reverse the roles of v 's and w 's) and notice that $v_i + w_i$ is isotropic for every $i = 1, \dots, p$. Hence, we can set $U = \text{span}\{v_1 + w_1, \dots, v_p + w_p\}$.)
- Example: on $V = \mathbb{R}^4$ there are 4 distinct nondegenerate scalar products up to congruence, namely of signature $(4, 0)$ (positive-definite; no isotropic vectors), $(3, 1)$ (Minkowski; isotropic subspaces are at most one-dimensional), $(2, 2)$ (isotropic subspaces are at most 2-dimensional), $(1, 3)$ (isotropic subspaces are at most 1-dimensional), $(0, 4)$ (negative-definite; no isotropic vectors).

26. Tuesday, 12/12

- LET (V, b) BE A VECTOR SPACE OVER \mathbb{F} AND b A NONDEGENERATE SCALAR PRODUCT AND LET $\mathcal{B} = \{z_1, \dots, z_n\}$ BE AN ORTHOGONAL BASIS OF V . THEN $b(z_i, z_i) \neq 0$ FOR $i = 1, \dots, n$ AND EVERY VECTOR $v \in V$ CAN BE WRITTEN AS

$$v = \sum_{i=1}^n \frac{b(v, z_i)}{b(z_i, z_i)} z_i .$$

The proof uses two facts: (1) as b is nondegenerate and V is finite-dimensional, the map $R_b : V \longrightarrow V^*$ is surjective and so $\{R_b(z_1), \dots, R_b(z_n)\}$ is a basis of V^* ; (2) if $v, w \in V$ and $\mathcal{B}^* = \{\varphi_1, \dots, \varphi_n\}$ is a basis of V^* , then $v = w$ if and only if $\varphi_k(v) = \varphi_k(w)$ for every $k = 1, \dots, n$.

- Let (V, b) be a vector space with a nondegenerate scalar product and let $W \subseteq V$ be a subspace such that $V = W \oplus W^\perp$. Then we call **orthogonal projection onto W** the natural homomorphism $p_W : V = W \oplus W^\perp \longrightarrow W$.
- Let (V, b) be a real vector space and b a positive-definite scalar product. Then, for every subspace W , the restriction of b to W is positive-definite and so nondegenerate, hence $V = W \oplus W^\perp$. Take an orthogonal basis $\{w_1, \dots, w_k\}$ of W and an orthogonal basis $\{u_1, \dots, u_{n-k}\}$ of W^\perp . Then $\mathcal{B} = \{w_1, \dots, w_k, u_1, \dots, u_{n-k}\}$ is an orthogonal basis of V and every $v \in V$ can be expressed as $v = w + u$, where

$$w = \sum_{i=1}^k \frac{b(v, w_i)}{b(w_i, w_i)} w_i \in W \quad \text{and} \quad u = \sum_{j=1}^{n-k} \frac{b(v, u_j)}{b(u_j, u_j)} u_j \in W^\perp$$

Hence, the orthogonal projection $p_W : V \longrightarrow W$ onto W can be expressed as

$$p_W(v) = \sum_{i=1}^k \frac{b(v, w_i)}{b(w_i, w_i)} w_i = v - \sum_{j=1}^{n-k} \frac{b(v, u_j)}{b(u_j, u_j)} u_j$$

- Let (V, b) be a vector space with a nondegenerate scalar product. Two endomorphisms $f, f^* : V \longrightarrow V$ are said **adjoint** to each other with respect to b if $b(f(v), w) = b(v, f^*(w))$ for every $v, w \in V$. An endomorphism $f : V \longrightarrow V$ is called **self-adjoint** (with respect to b) if $f = f^*$ and it is called **skew-self-adjoint** if $f = -f^*$.
- Example: $V = \mathbb{R}^n$ with the standard scalar product $\langle \cdot, \cdot \rangle$. Then $A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is self-adjoint if and only if A is symmetric; A is skew-self-adjoint if and only if A is skew-symmetric. In general, the adjoint of A is tA , the transpose of A .
- Example: $V = \mathbb{R}^n$ with the scalar product associated to a nondegenerate symmetric matrix B . Then the adjoint A^* of $A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ with respect to B satisfies ${}^tAB = BA^*$, so that $A^* = B^{-1}{}^tAB$, and so A^* is similar to tA .
- In general, the adjoint f^* of an $f : V \longrightarrow V$ makes the following diagram commute

$$\begin{array}{ccc} V & \xrightarrow{R_b} & V^* \\ f^* \uparrow & & \uparrow f^\vee \\ V & \xrightarrow{R_b} & V^* \end{array}$$

where $f^\vee : V^* \longrightarrow V^*$ is the dual of f .

We can informally say that *the adjoint f^* corresponds to the dual f^\vee under the isomorphism $R_b : V \longrightarrow V^*$ determined by the nondegenerate scalar product b* . So, the dual f^\vee has nothing to do with b , while the adjoint f^* need R_b and so b to be defined.

We can conclude that $f^* = R_b^{-1} \circ f^\vee \circ R_b$ and in coordinates $A^* = B^{-1}{}^tAB$, where $A = M_B^B(f)$, $A^* = M_B^B(f^*)$, $B = M_B(b) = M_{B^*}^B(R_b)$ (look at the example above!).

- Motivating example: $V = \{C^\infty \text{ functions } f : \mathbb{R} \rightarrow \mathbb{R} \text{ such that } f(x) = 0 \quad \forall x \notin (0, 1)\}$ is an infinite-dimensional vector space. The scalar product will be $b(f, g) = \int_0^1 f(x)g(x)dx$ (which is positive-definite) and $D : V \rightarrow V$ defined as $D(f(x)) = f'(x)$ is the derivative. The homomorphism D is skew-self-adjoint with respect to b : in fact, integrating by parts, $b(Df, g) = \int_0^1 f'g = [fg]_0^1 - \int_0^1 fg' = -b(f, Dg)$. Applying D twice, we find that the Laplacian in one variable $\Delta := D^2$ is self-adjoint.

- LET (V, b) BE A VECTOR SPACE WITH A POSITIVE-DEFINITE SCALAR PRODUCT AND LET $f : V \rightarrow V$ BE SELF-ADJOINT. IF $W \subseteq V$ IS f -INVARIANT, THEN W^\perp IS f -INVARIANT.

The proof is simple: let $u \in W^\perp$. Then for every $w \in W$ we have $b(f(u), w) = b(u, f(w)) = 0$, because $f(w) \in W$ and $u \in W^\perp$. Hence, $f(u) \in W^\perp$ and so $f(W^\perp) \subseteq W^\perp$.

Remark: the same conclusion holds if f is skew-self-adjoint.

- SPECTRAL THEOREM 1: LET (V, b) BE A REAL VECTOR SPACE OF DIMENSION n SPACE ENDOWED WITH A POSITIVE-DEFINITE SCALAR PRODUCT AND LET $f : V \rightarrow V$ BE A SELF-ADJOINT OPERATOR. THEN THERE EXISTS AN ORTHONORMAL BASIS \mathcal{B} OF EIGENVECTORS FOR f .

- We know that, choosing an orthonormal basis for (V, b) , we have that (V, b) is isometric to \mathbb{R}^n with the standard scalar product. The analogous statement in coordinates is the following.

- SPECTRAL THEOREM 2: LET $A : \mathbb{R}^n \rightarrow \mathbb{R}^n$ BE A SYMMETRIC MATRIX. THEN THERE EXISTS AN ORTHOGONAL MATRIX $N \in O(n, \mathbb{R})$ SUCH THAT $NA^tN = NAN^{-1}$ IS DIAGONAL.

- The two statements are equivalent. For concreteness, we will sketch the proof of the second statement.

First step: Interpret the real matrix A as $A : \mathbb{C}^n \rightarrow \mathbb{C}^n$. So there exists an eigenvector $0 \neq v \in \mathbb{C}^n$ with $Av = \lambda v$ and $\lambda \in \mathbb{C}$. We want to prove that $\lambda \in \mathbb{R}$, which will imply that there exists a real eigenvector $0 \neq v_1 \in \mathbb{R}^n$ with $Av_1 = \lambda v_1$.

Consider the complex number $c = \overline{v}Av$. Then $c = \overline{v}\lambda v = \lambda|v|^2$, where $|v|^2 = |a_1|^2 + \dots + |a_n|^2$ if $v = a_1e_1 + \dots + a_n e_n$. Notice that $a_i \in \mathbb{C}$ and that $|v|^2 > 0$ because $v \neq 0$.

Moreover, $\overline{c} = \overline{\overline{v}Av} = \overline{v}Av = c$, and so $c \in \mathbb{R}$. Hence, $\lambda = c/|v|^2 \in \mathbb{R}$.

Second step: proof by induction on $n \geq 1$.

For $n = 1$, there is nothing to prove.

If $n > 1$, then let $0 \neq v_1 \in \mathbb{R}^n$ an eigenvector for A . Call $V_1 = \text{span}\{v_1\}$; clearly, $A(V_1) \subseteq V_1$.

Key remark: $A(V_1^\perp) \subseteq V_1^\perp$.

The subspace V_1^\perp has smaller dimension and the restriction \tilde{b} of the standard scalar

product to V_1^\perp is still positive-definite. Moreover, if we call $\tilde{A} : V_1^\perp \rightarrow V_1^\perp$ the restriction of A , then \tilde{A} is still self-adjoint for (V_1^\perp, \tilde{b}) . Hence, by induction, there exists an orthonormal basis $\{v_2, \dots, v_n\}$ for (V_1^\perp, \tilde{b}) made of eigenvectors for \tilde{A} .

Clearly, the basis $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ of \mathbb{R}^n is orthonormal and made of eigenvectors for A , i.e. $Av_i = \lambda_i v_i$ with $\lambda_i \in \mathbb{R}$.

Define N to be the endomorphism of \mathbb{R}^n that sends v_i to e_i . As N sends an orthonormal basis to an orthonormal basis, N is an orthogonal matrix. Moreover, NAN^{-1} is a diagonal matrix with entries $\lambda_1, \dots, \lambda_n$ on the diagonal.

- **STRUCTURE THEOREM FOR ORTHOGONAL OPERATORS 1:** LET (V, b) BE A REAL VECTOR SPACE OF DIMENSION n ENDOWED WITH A POSITIVE-DEFINITE SCALAR PRODUCT. LET $f : V \rightarrow V$ AN ORTHOGONAL TRANSFORMATION OF (V, b) . THEN V DECOMPOSES AS

$$V = V_1 \oplus V_{-1} \oplus W_{\theta_1} \oplus \dots \oplus W_{\theta_k}$$

FOR SOME $k \geq 0$, WHERE THE SUMMANDS ABOVE ARE f -INVARIANT AND ORTHOGONAL TO EACH OTHER, AND f RESTRICTS TO Id ON V_1 (IN OTHER WORDS, V_1 IS THE EIGENSPACE WITH EIGENVALUE 1), f RESTRICTS TO $-Id$ ON V_{-1} ((IN OTHER WORDS, V_{-1} IS THE EIGENSPACE WITH EIGENVALUE -1), EACH W_{θ_i} HAS DIMENSION 2 AND THE RESTRICTION OF f TO W_{θ_i} IS A ROTATION OF ANGLE θ_i .

- Example: if $V = \mathbb{R}^3$ with the standard scalar product, the decomposition corresponding to a rotation $f : V \rightarrow V$ of axis $0 \neq v$ and angle θ is $\mathbb{R}^3 = V_1 \oplus W_\theta$, where $V_1 = \text{span}\{v\}$ and W_θ is the plane orthogonal to V_1 .
- **STRUCTURE THEOREM FOR ORTHOGONAL OPERATORS 2:** IF $T \in O(n, \mathbb{R})$, THEN THERE EXISTS ANOTHER $N \in O(n, \mathbb{R})$ SUCH THAT

$$NTN^{-1} = NT^tN = \left(\begin{array}{c|c|c|c|c|c} I_p & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & -I_q & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & R_{\theta_1} & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & R_{\theta_2} & 0 & 0 \\ \hline \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & 0 & 0 & 0 & R_{\theta_k} \end{array} \right)$$

WHERE $p = \dim \ker(T - I)$, $q = \dim \ker(T + I)$, $p + q + 2k = n$ AND $R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$.

- LET (V, b) BE A VECTOR SPACE WITH A POSITIVE-DEFINITE SCALAR PRODUCT AND LET $f : V \rightarrow V$ BE ORTHOGONAL. IF $W \subseteq V$ IS f -INVARIANT, THEN W^\perp IS f -INVARIANT.

The proof is again simple: observe first that f is invertible and that $f(W) = W$. Then, let $u \in W^\perp$. For every $w \in W$ we have $b(f(u), w) = b(u, f^{-1}(w)) = 0$, because $f^{-1}(w) \in W$ and $u \in W^\perp$. Hence, $f(u) \in W^\perp$ and so $f(W^\perp) \subseteq W^\perp$. As f is invertible, we can even conclude that $f(W^\perp) = W^\perp$.

- *Proof of structure theorem for orthogonal operators 2.*

If $Tv = \lambda v$ with $0 \neq v \in \mathbb{R}^n$ and $\lambda \in \mathbb{R}$, then $\lambda^2 \langle v, v \rangle = \langle Tv, Tv \rangle = \langle v, v \rangle$, and so $\lambda^2 = 1$ (because $\langle v, v \rangle \neq 0$, which implies that $\lambda = \pm 1$).

So call $V_1 = \ker(T - I)$ and $V_{-1} = \ker(T + I)$ the two possible eigenspaces. For $v \in V_1$ and $u \in V_{-1}$ we compute $\langle v, u \rangle = \langle Tv, Tu \rangle = -\langle v, u \rangle$ and so V_1 and V_{-1} are orthogonal to each other. They are also clearly f -invariant. Write $V = V_1 \oplus V_{-1} \oplus W$, where $W = (V_1 \oplus V_{-1})^\perp$ and W is also f -invariant.

Moreover, there are no eigenvectors for f in W .

The thesis will follow if we can write $W = W_{\theta_1} \oplus \cdots \oplus W_{\theta_k}$ as orthogonal sum, with $f|_{W_{\theta_i}}$ a rotation of angle θ_i .

Call $g : W \rightarrow W$ the restriction of f to W and let b be the restriction of the standard scalar product of \mathbb{R}^n to W .

We want to work by induction on $d = \dim W$.

If $d = 0$, there is nothing to prove, so we suppose $d > 0$.

As $W \subset \mathbb{R}^n \subset \mathbb{C}^n$, let $W_{\mathbb{C}}$ be the *complex* vector subspace of \mathbb{C}^n spanned by W .

Then $g : W_{\mathbb{C}} \rightarrow W_{\mathbb{C}}$ and let $0 \neq w_1 \in W_{\mathbb{C}}$ be an eigenvector of g (i.e. an eigenvector of $T : \mathbb{C}^n \rightarrow \mathbb{C}^n$ that belongs to $W_{\mathbb{C}}$). Then $Tw_1 = \lambda_1 w_1$, with $\lambda_1 = a_1 + ib_1 \in \mathbb{C}$.

Let $w_1 = x_1 + iy_1$, where $x_1, y_1 \in W \subset \mathbb{R}^n$. Then $Tw_1 = T(x_1 + iy_1) = Tx_1 + iTy_1$ and $Tw_1 = \lambda_1 w_1 = (a_1 + ib_1)(x_1 + iy_1) = (a_1x_1 - b_1y_1) + i(b_1x_1 + a_1y_1)$, which implies (because T is real!) that $Tx_1 = a_1x_1 - b_1y_1$ and $Ty_1 = b_1x_1 + a_1y_1$, so that $W_1 = \text{span}\{x_1, y_1\} \subset W$ is T -invariant and so $U_1 := W_1^\perp \cap W$ is T -invariant.

Write $W = W_1 \oplus U_1$. Then $\dim U_1 < \dim W$, the restriction of the scalar product to U_1 is positive-definite and T restricts to an orthogonal operator on U_1 .

Hence, induction applies and $U_1 = W_2 \oplus \cdots \oplus W_k$ and so $W = W_1 \oplus \cdots \oplus W_k$ and $V = V_1 \oplus V_{-1} \oplus W_1 \oplus \cdots \oplus W_k$.

If $\{v_1, \dots, v_p\}$ is an orthonormal basis of V_1 and $\{u_1, \dots, u_q\}$ is an orthonormal basis of V_{-1} and $\{\tilde{x}_i, \tilde{y}_i\}$ is an orthonormal basis of W_i , then define

$$\mathcal{B} = \{v_1, \dots, v_p, u_1, \dots, u_q, \tilde{x}_1, \tilde{y}_1, \tilde{x}_2, \tilde{y}_2, \dots, \tilde{x}_k, \tilde{y}_k\}.$$

Moreover, the restriction of T to W_i is orthogonal without real eigenvalues, so it must be a rotation of angle θ_i (and $\theta_i \neq 0, \pi$). Thus, $T\tilde{x}_i = \cos(\theta_i)\tilde{x}_i + \sin(\theta_i)\tilde{y}_i$ and $T\tilde{y}_i = -\sin(\theta_i)\tilde{x}_i + \cos(\theta_i)\tilde{y}_i$.

Hence, \mathcal{B} is an orthonormal basis of \mathbb{R}^n and we can choose N to be the orthogonal transformation that sends the i -th vector of \mathcal{B} to e_i .

- Example: there are six similitude classes of matrices in $O(3, \mathbb{R})$.

$$\left\{ \begin{array}{l} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \\ \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{pmatrix} \\ \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{pmatrix} \end{array} \right. \begin{array}{l} \text{if } p = 3, q = 0 \text{ and } k = 0 \\ \text{if } p = 2, q = 1 \text{ and } k = 0 \\ \text{if } p = 1, q = 2 \text{ and } k = 0 \\ \text{if } p = 0, q = 3 \text{ and } k = 0 \\ \text{if } p = 1, q = 0 \text{ and } k = 1 \\ \text{if } p = 0, q = 1 \text{ and } k = 1 \end{array} .$$

- The appearance of blocks of size 2 is due to the fact that real polynomials are not always completely factorizable. In fact, IF $p(t) = a_0 + a_1t + \cdots + a_d t^d$ IS A POLYNOMIAL WITH $a_i \in \mathbb{R}$, THEN IT FACTORIZES INTO A PRODUCT OF IRREDUCIBLE FACTORS OF DEGREE 1 OR 2.

By induction on $d \geq 1$. Clearly, for $d = 1$ there is nothing to prove.

Suppose $d > 1$ and let $\lambda \in \mathbb{C}$ be a root of $p(t)$ (uses the fundamental theorem of algebra). If $\lambda \in \mathbb{R}$, then $p(t)$ can be written as $p(t) = (t - \lambda)q(t)$ with $q(t) \in \mathbb{R}[t]$ and $\deg(q(t)) < d$. By induction, $q(t)$ is a product of real irreducible factors of degree 1 and 2, and so is $p(t)$.

If $\lambda \in \mathbb{C} \setminus \mathbb{R}$, then its conjugate $\bar{\lambda}$ is also a root of $p(t)$, because $0 = p(\lambda) = \overline{p(\lambda)} = \bar{a}_0 + \bar{a}_1\bar{\lambda} + \bar{a}_2\bar{\lambda}^2 + \cdots + \bar{a}_d\bar{\lambda}^d = a_0 + a_1\bar{\lambda} + \cdots + a_d\bar{\lambda}^d = p(\bar{\lambda})$ (uses that $a_i \in \mathbb{R}$!). This means that $r(t) = (t - \lambda)(t - \bar{\lambda}) = t^2 - 2\operatorname{Re}(\lambda)t + |\lambda|^2 \in \mathbb{R}[t]$ is irreducible over \mathbb{R} and divides $p(t)$, and so $p(t) = r(t)q(t)$, with $\deg(q(t)) < d$ and $q(t) \in \mathbb{R}[t]$.

By induction, $q(t)$ is a product of real irreducible factors of degree 1 and 2, and so is $p(t)$.

- A corollary of the result above is that IF V IS A REAL VECTOR SPACE OF DIMENSION $n > 0$ AND $f : V \rightarrow V$ IS AN ENDOMORPHISM, THEN THERE EXISTS AN f -INVARIANT SUBSPACE $W \subseteq V$ OF DIMENSION 1 OR 2.

Proof: if there is an eigenvector $0 \neq w \in V$ for f , then $W = \operatorname{span}\{w\}$ has dimension 1 and is f -invariant.

Otherwise, there is a monic irreducible polynomial $r(t) = a_0 + a_1t + t^2$ of degree 2 that divides the characteristic polynomial $p_f(t)$.

We know that $U = \ker(r(f)) \neq \{0\}$. Let $0 \neq w_1 \in U$ and $w_2 := f(w_1)$. As w_1 is not an eigenvector, $\{w_1, w_2\}$ are linearly independent. Call $W = \text{span}\{w_1, w_2\}$. The subspace W of dimension 2 is f -invariant, because $f(w_1) = w_2$ and $f(w_2) = f^2(w_1) = (-a_0I - a_1f)(w_1) = -a_0w_1 - a_1w_2$, because $r(f)(w_1) = 0$.