Math 251 Course Notes

(Gautier) Cole Killian

Winter 2020

This is McGill's undergraduate Math 251, instructed by Henri Darmon. The formal name for this class is "Honors Algebra 2". You can find this and other course notes here: https://colekillian.com/course-notes

Contents

§1 01-06

http://www.math.mcgill.ca/ daimon /courses /algebra /algebra.html
Assignments: due on wednesday at burnside floor 10. Handed back on Monday
office hourse mw 10:35 - 11:45
Midterm feb 19
Friday: no lecture this week
Textbook: "Linear algebra and geometry" Kostakin & makte

Definition 1.1 (Linear Algebra)**.** The study of vector spaces over a field and of the maps between them.
Homomorphism aka linear transformation. Studying linear transformations between vector spaces.

Groups are an abstraction of the notion of symmetry.
Rings are an abstraction of the notion of numbers.
Vector spaces arose as a model of physical space.

Example 1.2
Prototypical

1. $\mathbb{R}$
2. $\mathbb{R}^2$
3. $\mathbb{R}^3$

§1.1 Abstractions

1. $\mathbb{R}^n$. n-dimensional euclideon space
2. Replace $\mathbb{R}$ by a general field $F \to F^n$
   Allow you to study some interesting and practical ideas.

Definition 1.3. Fix a field F (e.g. $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \mathbb{F}_{p^n} = \mathbb{F}_p[x]/(q(x))\deg(q) = n, q$ irreducible
A vector space over $\mathbb{F}$ is a set V equipped with the following structures:

1. A binary operation.

$$+ : V \times V \to V$$
$$(v_1, v_2) \mapsto v_1 + v_2$$

2. A scalar multiplication

$$\cdot : F \times V \to V$$
$$(\lambda, v) \mapsto \lambda \cdot v$$

Subject to the following axioms.

1. $(V, +)$ is an abelian group, i.e. $\exists$ a mutual (identity) element for $+$.
   a) Identity:
   $$0_V \text{ such that } 0_V + w = w + 0_V = w \forall w \in V$$
   b) Commutative:
   $$v_1 + v_2 = v_2 + v_1 \forall v_1, v_2 \in V$$
   c) Inverses:
   $$\forall v \in V, \exists v' \text{ such that } v + v' = v' + v = 0_V$$

Note 1.4. $v' = -v$

d) Associativity

$$(v_1 + v_2) + v_3 = v_1 + (v_2 + v_3)$$

2. Multiplication rules

a) Identity

$$1 \cdot v = v$$

b) Associativity

$$\lambda_1, \lambda_2 \in F, v \in V$$
$$\lambda_1(\lambda_2 v) = (\lambda_1 \lambda_2)v$$

3. Distributive Laws

a)

$$\lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$$

b)

$$(\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$$

§1.2 Consequences of these axioms

1.

$$0 \cdot w = 0_V$$
$$(0 + 0) \cdot w = 0 \cdot w + 0 \cdot w = 0 \cdot w \Rightarrow 0_V = 0 \cdot w$$

2.

$$(-1) \cdot w = -w$$
$$(1 + (-1) \cdot w = 1 \cdot w + (-1) \cdot w$$
$$\Rightarrow 0_V = 0 \cdot w = w + (-1)w$$

Example 1.5 1. Euclidean space $\mathbb{R}^n$ is a vector space over $\mathbb{R}$.

2. Solutions of linear equations
Let $x_1, \ldots, x_n, a_1, dots, a_n \in F$

$$a_1 x_1 + \cdots + a_n x_n = 0$$

If $(x_1, \ldots x_n)$ and $(x_1', \ldots, x_n')$ are solutions to $(*)$, then so is $\lambda(x_1, \ldots, x_n)$ and $(x_1, \ldots, x_n) + (x_1' + \ldots, x_n')$
More generally you can set up a series of these equations. Let S be the set of solutions of this set of equations. It is a vector subspace of F^n. Homogeneous vs non homogeneous
Let $\sim S$ be solutions to $(**)$ where replace 0 with constants.
$\sim S$ is either empty, or it is a coset for S in F^n. If $x_1^0, \ldots, x_n^0) \in \sim S$, then $\sim S = (x_1^0, \ldots, x_n^0) + S$

§1.3 Linear Differential Equations

$a_0(x), a_1(x), \ldots, a_n(x)$ functions from $\mathbb{R} \to \mathbb{R}$

$$f : \mathbb{R} \to \mathbb{R} \text{ such that}$$
$$a_0(x)f(x) + a_1(x)f'(x) + \cdots + a_n(x)f^{(n)}(x) = 0$$
$$\frac{d}{dx}(f(x) + g(x)) = \frac{d}{dx}f + \frac{d}{dx}g$$

Note that this equation would not hold true when replacing addition with multiplication. Think of the product rule.

§2 Lecture 01-08

Definition 2.1. Vector space is a special kind of abelian group that can multiply by scalars. For a general vector space, the scalars are members of a field F, in which case V is called a vector space over F.

§2.1 Codes

Definition 2.2 (Codes)**.** A subset of the field $\mathbb{F}_2^n$

$$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$$

There are various features you would like a good code to have.

1. Capacity: Cardinality of sigma should be large relative to the cardinality of $\mathbb{F}_2^n$ which is 2^n.

2. Redundancy: Often data is transmitted over noisy channels, so single bits can occasionally be corrupted. One feature you would like to have is being able to detect these corruptions.
   Do this by defining Hamming distance. Let $v, w \in \mathbb{F}_2^n$. $d(v, w) = \#$ of j such that $v_j \neq w_j$.

   $$v = (v_1, \ldots, v_n)$$
   $$w = (w_1, \ldots, w_n)$$

   One bit is flipped you may fall out of sigma which may be detected.
   K-bit error detection. If $v \in \Sigma$, then

   $$\{w | d(v, w) \leq k\} \cap \Sigma = \{v\}$$

3. Computational Efficiency: Algorithms for converting elements of Σ into the acutal data you are trying to communicate should be efficient.

   Definition 2.3. Σ is a linear code if it is a vector subspace of $\mathbb{F}_2^n$. (Closed under addition). All you really have to check if closure under addition.
   Scalar multiplication is really no requirement at all because multiplying by 0 just means Σ must contain 0. And multiplying by 1 just gives you the element back.

§2.2 Function Spaces

Let x be a set, and F a field.
Let $\mathbb{F}(x, F)$ be the set of functions from x to F.

$$f_1, f_2 \in \mathbb{F}, \quad (f_1 + f_2)(x) = f_1(x) + f_2(x)$$
$$f \in \mathbb{F}, \quad (\lambda f)(x) = \lambda \cdot f(x)$$

§2.2.1 Linear subspaces of function spaces

1. Function with compact support
   x is a topological space.

   Definition 2.4 (Compact Support)**.** $f : x \to$ has compact support if $\exists B \subset x$, B compact, such that $(f(x) = 0)(\forall x \notin B)$

   If f_1 is supported on B_1 and f_2 on B_2, then $f_1 + f_2$ is supported on $B_1 \cup B_2$.

   Linearly supported is closed under addition. And scalar multiplication as well

   Special Case: x has discrete topology. Then compact sets are finite.

   $\mathbb{F}_0(x, F)$ is the set of compactly supported F-valued functions on x. $F_0(x, F) \leq F(x, F)$.

§2.3 Linear Transformations

Definition 2.5 (Linear Transformation)**.** A linear transformation from V to W (V, W vector spaces over F) is a function $T : V \to W$ such that $\forall v_1, v_2 \in V$

$$T(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 T(v_1) + \lambda_2 T(v_2)$$

T is group homomorphism with additional feature that it respects scalar multiplication.
$T(\lambda v) = \lambda T(v)$

Consequences:

$$T(\lambda_1 v_1 + \cdots + \lambda_n v_n) = \lambda_1 T(v_1) + \cdots + \lambda_n T(v_n)$$

Now we can consider the set of all these linear transformations.

Note 2.6.

1. $\hom_F(V, W)$ represents the set of all linear transformations from V to W (V and W are vector spaces).
2. A linear transformation from V to itself is called endomorphism of V.

   $$\mathrm{End}_F(V) = \hom_F(V, V)$$

3. $\hom(V, W)$ is a vector space! (this makes sense because if T_1 and T_2 are linear, so is $\lambda_1 T_1 + \lambda_2 T_2$)

4. $\mathrm{End}(V)$ is also endowed with an internal multiplication in addition to the addition arising from the vector space. The product $T_1T_2 = T_1 \circ T_2$ or $T_1T_2(v) = T_1(T_2(v))$. On the other hand you cannot compose elements of $\hom_F(V,W)$.

   Distributive Laws
   Composition of functions is always associative
   But not necesarily commutative.
   $\mathrm{End}(V)$ is a ring and a vector space over the field F!

   Definition 2.7. A vector space over F which is also a ring is called an F-algebra.

A ring R gives rise to two groups, namely

1. $(R,+,0)$ is an abelian group.
2. $(R^\times,\times,1)$ is a group.

$$\mathrm{End}(V)^\times = \mathrm{Aut}_F(V)$$

Note 2.8. Last value in $(R,+,0)$ indicates the identity element.

Definition 2.9 (Automorphism)**.** An invertible linear transformation from V to V is called an automortphism of V.

Definition 2.10 (Dual Space)**.** Linear transformation from V to F where F is a vector space over itself.

$\hom_F(V,F) = V^*$ is called the dual space of V. We will talk about it in more detail on Monday.

§3 Lecture 01-13

Linear transformation is an additive group homomorphism that preserves
an Algebra is a vector space and ring at the same time.

$$\mathrm{End}_F(V) = \hom_F(V,V)$$

This is both a vector space over F and a ring where multiplication is the composition of functions.

Definition 3.1 (Dual Space)**.** $V^* = \hom_F(V,F)$

§3.1 Bases

∇ = vector space

Definition 3.2 (Collection Linear Independence)**.** A collection $\Sigma \subset V$ is linearly independent if, $\forall v_1,\dots,v_n \in \Sigma$ (distinct) satisfies

$$\lambda v_1 + \cdots + \lambda_n v_n = 0 \Rightarrow \lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$$

Can only talk about finite sums

Definition 3.3 (Spanning Set)**.** A collection Σ spans V if,

$$\forall v \in V, \quad \exists v_1, \ldots, v_n \in \Sigma, \quad \lambda_1, \ldots, \lambda_n \in F st v = \lambda_1 + v_1 + \cdots + \lambda_n + v_n$$

Definition 3.4 (Basis)**.** A basis is a set $\Sigma \subset V$ that is both linearly independent and spans V.

Proposition 3.5

If Σ is a basis for V, then, for all $v \in V$, there is a unique

$$v_1, \ldots, v_n \in \Sigma, \quad \lambda_1, \ldots, \lambda_n \in F \text{ s.t. } v = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

Proof. Existence of $(v_1, \ldots, v_n, \lambda_1, \ldots, \lambda_n) \Leftarrow \Sigma$ spans V.

Uniqueness $\Leftarrow$ linear independence of Σ. □

Corollary 3.6

The vector space V is isomorphic to F^n or $F_0(\Sigma, F)$

Proof. We set up a linear transformation.

$$\begin{aligned} \phi : F_0(\Sigma, F) &\to V \\ f &\to \sum_{v \in \Sigma} f(v) \cdot v \end{aligned}$$

Need to check

1. ϕ is linear
2. ϕ is injective
3. ϕ is surjective

□

Theorem 3.7 (Every vector space over F has a basis)*Proof.* Let V be a vector space. Let L be a collection of all subsets of V that are linearly independent. Partial ordering on L is given by inclusion.

Completeness of ordering. If $\{A_\alpha\}_{\alpha\in I}$ is a chain, $A = \sum_\alpha A_\alpha$.

Claim: $A \in L$. If $v_1 \dots v_n \in A$, $v_j \in A_\alpha$. $\exists n$ such that $v_1, \dots, v_n \in A_{\alpha_N}$ and $v_1, \dots, v_n$ are linearly independent.

Zorn's Lemma $\Rightarrow \exists$ a maxmial element $\Sigma \in L$. Claim: Σ spans V. Otherwise $\exists$ v which is not in span(Σ).

$$\Sigma \cup \{v\} \supsetneq \Sigma$$

and is linearly independent. $\Sigma \cup \{v\} \in L$. □
Not as useful as you might think at first because basis is obtained in a non constructive way.

Definition 3.8. A set endowed with a partial ordering satisfies the maximal chain condition if, for all subsets of S, for which the ordering is a total ordering (chain condition), every totally ordered subset $A \subseteq S$ has an upper bound, $\exists B \in S$ such that $a \leq B$

A partially ordered set S is complete if, for all chains $A \subset S$, $\exists B \in S$ such that $a \leq B$, $\forall a \in A$. Partial ordering means a relation less than or equal. Anti symmetric, transitive. Think of it as a directed graph with no back tracking. Some elements are not ordered.

Every complete partially ordered set has a maximal element. i.e. $\exists s \in S$ s.t. $s \leq a \Rightarrow a = s$, $\forall a \in S$

Chain stands for a totally ordered subset.

Axiom of choice. If you have an infinite collection of sets $\{S_\alpha\}_{\alpha\in I}$. Then there exists S' containing one $s_\alpha \in S_\alpha (\alpha \in I)$

Example 3.9
$F[x]$ is the ring of polynomials with coefficients in F. Basis: $\Sigma = \{1, x, x^2, x^3, \dots, x^n, \dots\}$

Example 3.10
$F[[x]] = \{a_0 + a_1 x + a_2 x^2 + \dots, \quad a_i \in F$. The difference between $F[x]$ and $F[[x]$ is that elements in $F[[x]]$ are infinite.

Infinite sums don't make sense in algebra.

§4 Lecture 01-15

Assignment 1 due today. Burnside Hall 10th floor mail slot.
Basis for a vector space.

Theorem 4.1

If V is a vector space over F, then V has a basis. i.e. $\exists B \subset V$ which is linearly independent and spans V.

Proof. Let B be a maximal linearly independent subset of V. This ensures that is spans V. □

Example 4.2

$V = F[x]$. $B = \{1, x, x^2, x^3, \dots\}$. The fact that this is a basis is the statement that every polynomial can be written as a finite combination of powers of x.

Example 4.3

$V = F[[x] = \{\sum_{i=0}^{\infty} a_i x^i,\ a_i \in F$. Infinite linear combination of powers of x. No one has ever written down a basis for this vector space. Although there muts be one according to the theorem.

Example 4.4

$V = \mathbb{R}$ as a vector space over the rationals. B is called a Hanel basis. Source of counter examples in measure theory. Gives rise to non measurable set. Pathalogical set.

Example 4.5

Take $V = F^n = \{(a_1, \dots, a_n),\ a_i \in F\}$. You can take

$$B = \{(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 0, 1)\} = \{e_1, e_2, \dots, e_n\}$$

The "standard basis". Bases are typically most useful when they are finite.

Definition 4.6 (Finite-dimensional)**.** A vector space which has a finite-basis is said to be finite-dimensional.

§4.1 The Dimension

Theorem 4.7

If V is a finite dimensional vector space, and B_1, B_2 are two basesfor V, then the conclusion is that B_1 and B_2 are both finite and have the same cardinality.

Recall 4.8. If B is a basis for V, then V is isomorphic to the space of functions $F_0(B, F) = \{$Space of functions $f : B \to F$ such that $f(x) = 0\ \forall$ but finitely many $x \in B$.

$$\varphi : F_0(B, F) \to V$$
$$f \mapsto \sum_{x \in B} f(x) \cdot x$$

If $\#B < \infty$, then $F_0(B,F) = F(B,F) = F^N$, $N = \#B$. (i.e., can assume $B = \{1,\dots,N\} \to \{v_1,\dots,v_N\}$.

$$\varphi : F^n \to V$$
$$(a_1,\dots,a_n) \mapsto a_1v_1 + \cdots + a_Nv_N$$

Reformulation of theorem.
If $F^{n_1} isomorphic F^{n_2}$, then $n_1 = n_2$.

Lemma 4.9

Let $v_1,\dots,v_m$ be a collection of linearly independent vectors in F^n. Then $m \le n$.

Proof. If $v_1 = (a_{1_1}\ a_{1_2}\ \dots\ a_{1_n})\ \dots\ v_m = (a_{m_1}\ a_{m_2}\ \dots\ a_{m_n})$ are linearly independent.

$$x_1v_1 + \cdots + x_mv_m = 0 \Leftrightarrow (x_1,\dots,x_m) = 0$$

Gives rise to homogenous system of linear equations. There are n linearly equation with m unknowns.

The system must have a non-trivial solution if $n < m$. Since we are told that there is only a trivial solution, it must be that $m \le n$. □

Example 4.10

If $F^{n_1} isomorphic F^{n_2}$. Let

$$\varphi : F^{n_1} \to F^{n_2}$$
Let $e_1,\dots,e_{n_1}$ be the standard basis of F^{n_1}.
$\varphi(e_1),\dots,\varphi(e_{n_1})$ are linearly independent in $F^{n_2} \Rightarrow n_1 \le n_2$.
By symmetry $n_2 \le n_1$
$\Rightarrow n_1 = n_2$

Definition 4.11 (Dimension)**.** The dimension of V is the cardinality of a basis for V.

Convention:

$$\dim(V) \in \{0,1,2,3,\dots,\} \cup \{\infty\}.$$

$\dim(V) = \infty$ if V contains an infinite collection of linearly independent vectors.

§4.2 Completing to a basis

Proposition 4.12

If S_0 is a collection of linearly independent vectors in V, then $\exists$ a basis such that $S \supseteq S_0$.

Proof. Let L be the set of linearly independent subsets of V containing S_0. iLet B be a maximal element of L. □

Example 4.13

Let X be a set.

1. $\dim_F F_0(X, F) = \#X$
2. $\dim_F(F^n) = n$. Dimension is kind of like the logarithm base F of the cardinality.
3. $\dim(V_1 \times V_2) = \dim(V_1) + \dim(V_2)$

§4.3 Basic Constructions

1. Cartesian product (direction)
2. Subspaces
3. Notion of Quotients
4. Rank Nullity Theorem.

§5 Lecture 01-17

§5.1 Constructions of Vector Spaces

Given vector spaces V_1, V_2, we can construct new vector spaces.

1. Direct sum, or cartesian product. $V_1 \times V_2 = V_1 \oplus V_2 = \{(v_1, v_2) \ : \ v_1 \in V_1, v_2 \in V_2\}$.

$$(v_1, v_2) + (v_1', v_2') = (v_1 + v_1', v_2 + v_2')$$
$$\lambda(v_1, v_2) = (\lambda v_1, \lambda v_2)$$

   Note that $\dim(V_1 \oplus V_2) = \dim(V_1) + \dim(V_2)$

2. Subspace. If V is a vector space over F, then $W \subseteq V$ is a subspace if it is closed under addition and scalar multiplication.

$$w_1, w_2 \in W \Rightarrow w_1 + w_2 \in W$$
$$\lambda \in F, \ w \in W \Rightarrow \lambda w \in W$$

   Conclusion is that W is a vector space. Other properties are inherited from V.

3. Homs. $\hom_F(V_1, V_2)$ is a vector space. If V_1 and V_2 are finite dimensional, dimensions n_1 and n_2, then $\dim_F(\hom_F(V_1, V_2)) = n_1 n_2$.

   Let $(e_1, \ldots, e_n)$ be a basis for V_1.

   Key remark: A linear transformation $T : V_1 \to V_2$ is completely determined by $(T(e_1), \ldots, T(E_{n_1}))$.

   Why? If $v \in V_1$, then $v = \lambda_1 e_1 + \cdots + \lambda_{n_1} e_{n_1}$. So $T(v) = T(\lambda_1 e_1 + \cdots + \lambda_{n_1} e_{n_1} = \lambda_1 T(e_1) + \cdots + \lambda_{n_1} T(e_{n_1})$

$$\hom(V_1, V_2) = \underbrace{V_2 \oplus \cdots \oplus V_2}_{n_1 \text{ times}}$$

4. Dual space: $V^* = \hom_F(V, F)$. If B is a basis for V, then $V \simeq F_0(B, F)$. $V^* \simeq F(B, F)$.

   The choice of B determines an injection $V \hookrightarrow V^*$. When B is finite, i.e. $\dim(V) = n < \infty$, then $V \simeq V^*$.

   There is a canonical inclusion of $V \hookrightarrow V^{**}$.

   $$V \to V^{**}$$
   $$v \mapsto v^{**}(l) = l(v)$$
   $$l \in V^*,\ l : V \to F$$

   v^{**} is a linear functional on V^*. I.e. a linear transformation from $F^* \to F$. The rule $v \mapsto v^{**}$ is itself linear. i.e. $(v_1 + v_2)^{**} = v_1^{**} + v_2^{**}$.

5. The tensor product of V_1 and V_2. $V_1 \otimes V_2 = \hom_F(V_1^*, V_2)$

   If V_1 and V_2 are finite dimensional, then $\dim(V_1 \otimes V_2) = \dim(V_1)\dim(V_2)$.

   The dimension of the dual space.

   $$V \simeq F_0(B, F)$$
   $$V^* \simeq F(B, F)$$

   If $\#B = n < \infty$, then $\dim(V^*) = n = \dim(V)$.

6. Quotients. If $W \subseteq V$ is a subspace, then W is also a subgroup.

   $$V/W = \{v + W, v \in V\}$$

   V/w has a natural scalor multiplication.

   $$\lambda \in F,\ \lambda(v + W) = \lambda v + W$$

   Exercise 5.1. With this definition of scalar multiplication, the group V/W satisfies all the axioms of a vector space over F.

§5.2 Isomorphism Theorem

If $T : V \to V'$ is a linear transformation.

Definition 5.2 (Kernel)**.**

$$\ker(T) \coloneqq \{v \in V \text{ s.t. } T(v) = 0\}$$

Definition 5.3 (Image)**.**

$$\mathrm{Im}(T) = \{v \in V' \text{ s.t. } \exists \tilde{v} \in V \ :\ T(\tilde{v}) = v\}$$

Claim: $\ker(T)$ and $\mathrm{Im}(T)$ are vector spaces.

Proof. Show $v \in \ker(T),\ \lambda \in F,\ \lambda w \in \ker(T)$. $T(\lambda v) = \lambda T(v) = \lambda \cdot 0 = 0$. Likewise for image. □

If $T : V \to V'$ is linear, $W = \ker(T)$, then T induces an isomorphism $V/\ker(T)$ to $\mathrm{Im}(T)$.

$$\varphi : V/\ker(T) \to \mathrm{Im}(T)$$
$$v + \ker(T) \mapsto T(v)$$

Need to check:

1. That φ is well-defined. $W = \ker(T)$. If $v + w = v' + W$, then $T(v) = T(v')$.
2. Injection
3. Surjection

§6 Lecture 01-20

Textbook Correction. Zorn's Lemma. It doesn't imply "the maximal" element, but rather "a maximal" element. This translates over to its application of proving that every vector space has a basis, not "the" basis (Multiple vs. Single).

§6.1 Quotients of Vector Spaces

$W \subset V$. W a subspace.

$$V/W = \{v + w : v \in V\}$$
$$\lambda \in F, \quad \lambda(v + W) = \lambda v + W$$

If $v_1 + W = v_2 + W$, then $\lambda v_1 + W = \lambda v_2 + W \ \forall \lambda \in F$. This implies that $(v_1 - v_2) \in W \Rightarrow \lambda(v_1 - v_2) \in W \Rightarrow \lambda v_1 - \lambda v_2 \in W$.

Theorem 6.1

If V is finite dimensional and $W \subseteq V$ is a subspace, then W and V/W are both finite dimensional.

$$\dim(V) = \dim(W) + \dim(V/W)$$

This makes sense, because (V/W) reduces the dimension by W, because suddenly all elements in W are considered equal to one another. So the dimension behaves like a logarithm in a sense.

Proof: Subspace of finite dimensional vector space is finite dimensional.

Let $d = \dim(W)$. Let $(v_1, \ldots, v_d)$ be a basis for W. Therefore $(v_1, \ldots, v_d)$ is linearly independent in V. We can complete it to a basis for V, $(v_1, \ldots, v_d, v_{d+1} + \cdots + v_n$. Where $n = \dim(V)$.

Basis for V/W. There are associated cosets for $v_{d+1}, \ldots, v_n$. It would be incorrect to say that the basis is $v_{d+1}, \ldots, v_n$, because these elements don't live in the quotient. Claim: The $(n-d)$-tuple $(v_{d+1} + W, \ldots, v_n + W)$ is a basis for V/W.

Proof of linear independence. Let $(\lambda_{d+1}, \dots, \lambda_n) \in F^{n-d}$.

$$\lambda_{d+1}\overline{v_{d+1}} + \cdots + \lambda_n\overline{v_n} = 0 \text{ in } (V/W).$$
$$\Rightarrow \lambda_{d+1}v_{d+1} + \cdots + \lambda_n v_n \in W$$

$$\text{Hence } \exists(\lambda_1, \dots, \lambda_d) \in F^d \text{ s.t. } \lambda_{d+1}v_{d+1}\cdots + \lambda_n v_n = \lambda_1 v_1 + \cdots + \lambda_d v_d$$
$$\text{This works because } (v_1, \dots, v_n) \text{ span } W.$$
$$\text{Because } (v_1, \dots, v_n) \text{ are linearly independent}$$
$$\Rightarrow \lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$$
$$\Rightarrow \lambda_{d+1} = \cdots = \lambda_n = 0$$

□

□

Proof. $(\overline{v_{d+1}}, \dots, \overline{v_n})$ spans V/W.

Let $v + W \in V/W$. Because $v \in V$, $\exists(\lambda_1, \dots, \lambda_n) \in F^n$ such that $v = \lambda_1 v_1 + \cdots + \lambda_d v_d + \cdots + \lambda_n v_n$.

In V/W.

$$\overline{v} = \lambda_1\overline{v_1} + \cdots + \lambda_d\overline{v_d} + \cdots + \lambda_n\overline{v_n}$$
$$\Rightarrow \overline{v} = \lambda_{d+1}\overline{v_{d+1}} + \cdots + \lambda_n\overline{v_n}$$

because the other vectors are all in W. □

Note 6.2.

$$\overline{v} = v + W$$

$v \in V$, $\overline{v} \in V/W$.

Theorem 6.3 (Isomorphism Theorem)
If $T : V \to W$ is a linear transformation, then T induces an injective linear transformation

$$\overline{T} : V/\ker T \hookrightarrow W$$

In particular, $V/\ker(T) \simeq \mathrm{Im}(T)$.

$$\overline{T}(v + \ker(T)) = T(v)$$

$\overline{T}$ is injective.

$$\overline{T}(v + W) \Leftrightarrow T(v) = 0 \Leftrightarrow v \in \ker(T)$$
$$\Leftrightarrow v + \ker(T) = 0 \text{ in } V/\ker(T)$$

Theorem 6.4 (Rank-nullity theorem)
Let $T : V \to W$ be a linear transofmration with $\dim(V) < \infty$. Then $\dim\ker(T) + \dim\operatorname{Im}(T) = \dim(V)$.

Proof.

$$V/\ker(T) \simeq \operatorname{Im}(T)$$
$$\dim(V/\ker(T)) = \dim\operatorname{Im}(T)$$
$$\dim(V) - \dim\ker(T) = \dim\operatorname{Im}(T)$$

□

Remark 6.5. If $H \subset G$ is a group, $\#\ G < \infty$, then $\#(G/H) = \#G/\#H$

A vector space V is finite as a set $\Leftrightarrow \#F < \infty$ and $\dim_F(V) < \infty$. Let $q = \#F$ and $n = \dim_F(V)$. Then $\#V = q^n$. $\dim(V) = \log_q(\#V)$. $V \simeq F^n$.

Theorem 6.6 (Counting Principle)
If A and B are finite sets of the same cardinality, and $f : A \to B$ is an injective function, then f is surjective.

Linear algebra. Let V and W be finite dimensional vector spaces of the same dimension and let $T : V \to W$ be an injective linear transformation. Then T is surjective.

§7 Lecture 01-22

§7.1 Finite Dimensional

$B = (v_1, \ldots, v_n)$, a basis for V.

If $v \in V$, then $\exists!(x_1, \ldots, x_n) \in F^n$ such that $v = x_1v_1 + \cdots + x_nv_n$. (The exclamation points indicates uniqueness).

The n-tuple $(x_1, \ldots, x_n)$ are called the coordinates of v in B.

This sets up an isomorphism between $V \simeq_B F^n$.

Any vector space of dimension n "is" F^n (is non-canonically isomorphic to F^n). This non-canonicalness is reflected in the dependence on a basis.

Note 7.1. If $(x_1, \ldots, x_n)$ are the coordinates of v relative to B, then

$$v = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

If $T : V_1 \to V_2$ is a linear transformation, then T can be described by a matrix $M_{T,B_1,B_2} \in$

$M_{m\times n}$.

$$V_1 \to_T V_2$$
$$V_1 \simeq_{B_1} F_1^n$$
$$V_2 \simeq_{B_2} F_2^n$$
$$F_1^n \to_{M_{T,B_1,B_2}} F_2^n$$

Properties:

1. Let $B_1 = (v_1, \ldots, v_n)$. $B_2 = (w_1, \ldots, w_m)$ be bases for V_1 and V_2.

$$T(v_1) = a11w_1 + a_{21}w_2 + \cdots + a_{m1}w_m$$
$$T(v_2) = a12w_1 + a_{22}w_2 + \cdots + a_{m2}w_m$$
$$\vdots$$
$$T(v_n) = a1nw_1 + a_{2n}w_2 + \cdots + a_{mn}w_m$$
$$M_{T,B_1,B_2} = (a_{ij})_{i\le i\le m, 1\le j\le n}$$
$$(T(v_1), T(v_2), \ldots, T(v_n)) = (w_1, \ldots, w_m)M_{T,B_1,B_2}$$
$$T(B_1) = B_2 M_{T,B_1,B_2}$$

2. Effect of T on coordinates

$$v = \begin{pmatrix} v_1 & \cdots & v_n \end{pmatrix}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1v_1 + \cdots + x_nv_n$$

$$T(v) = T(x_1v_1 + \cdots + x_nv_n) = x_1T(V_1) + \cdots + x_nT(v_n) = \begin{pmatrix} T(v_1) & \ldots\ldots & T(v_n) \end{pmatrix}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$= \begin{pmatrix} (w_1, \cdots, w_m)M_{T,B_1,B_2} \end{pmatrix}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} w_1, \cdots, w_m \end{pmatrix}\begin{pmatrix} M_{T,B_1,B_2} \end{pmatrix}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

3. Conclusion:

   The column vector

$$V_{T,B_1,B_2}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

   is a column vector of size m, and represents the coordinates of $T(v)$ in the basis B_2.

§7.2 Important Special Case of Transformation to itself

$V_1 = V_2 = V$. $T : V \to V$. Choose $B = (v_1, \ldots, v_n)$.

$M_{T,B}$ is the matrix of T relative to $B \in M_{n\times n}(F)$

$$(T(v_1), \ldots, T(v_n)) = (v_1, \ldots, v_n)M_{T,B}$$

This gives an identification

$$\mathrm{Hom}_F(V,V) = \mathrm{End}_F(V) \simeq_B M_n(F)$$

Dependency of $M_{T,B}$ on B. Let B and B' be two bases. Then there eixst unique matrices, P, P' such that $B' = BP$.

$$\begin{gathered}
B = (v_1, \ldots, v_n) \\
B' = (v_1', \ldots, v_n') \\
T(B) = BM_{T,B} \\
T(B') = B'M_{T,B'} \\
B' = BP \\
T(BP) = BPM_{T,B} \\
T((v_1, \ldots, v_n)P) = (T(v_1), \ldots, T(v_n))P \\
T(B)P = BPM_{T,B'} \\
BM_{T,B}P = BPM_{T,B'} \\
M_{T,B} = PM_{T,B'}
\end{gathered}$$

Note 7.2. P is invertible

Proof.

$$\begin{gathered}
(v_1', \ldots, v_n') = (v_1, \ldots, v_n)P(v_1, \ldots, v_n) = (v_1', \ldots, v_n')P' \\
\Rightarrow (v_1', \ldots, v_n') = (v_1', \ldots, v_n')P'P \\
\Rightarrow P'P = E_{n\times n}
\end{gathered}$$

□

So

$$M_{T,B'} = P^{-1}M_{T,B}P$$

Definition 7.3. Matrices v in $M_n(F)$ which are related by $M_1 = P^{-1}M_2P$ for some $P \in M_n(F)^X$ are conjugate.

> **Theorem 7.4**
> If M_1 and M_2 in $M_n(F)$ represent the same linear transformation $T : V \to V$ in different bases, they are conjugate.
>
> Even though the matrices are not unique, they are conjugate to one another based on the basis.

Exercise 7.5. What functions $\varphi M_n(F) \to F$ are invariant under conjugation.

$$\varphi(A) = \varphi(PAP^{-1})$$

for all P invertible.

§8 Lecture 01-24

Recommend Colmez. Drawback is that it is in french.
Let V be a finite dimensional vector space. Let B be a basis for V. $B = (v_1, \dots, v_n) \in V^n$.
$v \in V$ has coordinates

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in F^n$$

if $v = Bx$

If T is a linear transformation,

$$T : V \to V$$
$$V \simeq_B F_1^n$$
$$V \simeq_{B'} F_2^n$$
$$F_1^n \to_{M_{T,B}} F_2^n$$

Fact 8.1. If B and B' are different bases for V, then the matrices $T_{T,B}$ and $T_{T,B'}$ are conjugate. i.e. $\exists P \in \mathrm{GL}_n(F)$ such that $M_{T,B'} = PM_{T,B}P^{-1}$

§8.1 Determinant

Proposition 8.2

There is a unique function $\det : M_n(F) \to F$ satisfying:

1. det is multilinear. i.e. it is a linear function in each row with all other rows being fixed.
2. det is alternating, namely, the determinant changes sign after interchanging two rows.

$$\det(M^\sigma) = \mathrm{sign}(\sigma)\det(M), \sigma \in S_n$$

§8.2 Proof of existence and uniqueness

$$\det(AB) = \det(A)\det(B)$$
$$\det(A + B) = ???$$
$$\det(PAP^{-1}) = \det(P)\det(A)\det(P)^{-1} = \det(A)$$

Definition 8.3. The determinant of $T : V \to V$ is the determinant of any matrix representing T.

Definition 8.4 (Trace)**.** Trace $(A) = a_{11} + a_{22} + a_{33} + \cdots + a_{nn}$ where $A = (a_{ij})$.

$$\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$$
$$\mathrm{Tr}(AB) = ??$$

Lemma 8.5

$$A \cdot B = \sum_{i,j} a_{ij} b_{ij}$$
$$\mathrm{Tr}(AB) = A \cdot B^T = \sum_{i,j} a_{ij} b_{ji}$$
$$\mathrm{Tr}(BA) = B \cdot A^T = \sum_{i,j} b_{ij} a_{ji}$$
$$\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$$
$$\mathrm{Tr}(PAP^{-1}) = \mathrm{Tr}(AP^{-1}P) = \mathrm{Tr}(A)$$

So trace is also invariant over conjugation.

Definition 8.6. The trace of $T : V \to V$ is the trace of any matrix representing T.

Exercise 8.7. Show that $\mathrm{End}_F(V) = \mathrm{End}_F(V)$

1. First show that $M_n(F) \simeq M_n(F)^*$ where $A \mapsto (x \mapsto \mathrm{Tr}(AX))$.
2. Then show that $\mathrm{End}_F(V) \simeq \mathrm{End}_F(V)^*$. Solution the mapping $T \mapsto (U \mapsto \mathrm{Tr}(TU))$.

If $T : V \to V$ is a linear transformation, study the structure of T acting on V (nullspace, eigenspaces, eigenvalues, characteristic polynomial, minimal polynomial.)

$$F[T] = \{a_0 + a_1 T + a_n T^n + \cdot\} \in \mathrm{End}_F(V) \subseteq \mathrm{End}_F(V)$$

$F[T]$ is a sub F-algebra of $\mathrm{End}_F(V)$.

Remark 8.8. If $\dim(V) > 1$, then $F[T] \neq \mathrm{End}_F(V)$.

$F[T]$ is a quotient ring of $F[x]$, the ring of polynomials. Ther eis a natural ring homomoprhism

$$\varphi_T : F[x] \to F[T] \subseteq \mathrm{End}(V)$$
$$p(x) \mapsto P(T)$$

But $F[X]$ is infinite dimensional. So this means that there is a nontrivial kernal because $F[T]$ is not infinite dimensional.

Definition 8.9 (Defining Ideal)**.** The kernel of φ_T is called the defining ideal of T.

$I_T = \ker(\varphi_T)$.

I_T is generated by a unique polynomial in $F[x]$ which is monic. $I_T = (P_T(X))$.

$$P_T(X) = X^+ a_{m-1} x^{m-1} + \cdots + a_0, \quad a_j \in F$$

What is $P_T(x)$?

$$\varphi_T(p_t) = 0$$
$$\varphi_T(T) = 0$$

P_T is called the minimal polynomial. $f \in F[x]$. $f(T) = 0$. $p_T(x) | f(x)$.

§9 Lecture 01-27

Definition 9.1 (Grassmannian)**.** The Grassmannian of k-dimensional subspace of V is the collection of k-dimensional supspaces of V.

Note 9.2. $\mathrm{Gr}(V,k)$. If $\dim(V) = n$, then $\mathrm{Gr}(n,k)$

If F is a finite field, then $\mathrm{Gr}(n,k)$ is a finite set. $\#F = q$.

Question: What is $\#\mathrm{Gr}(n,k)$. Strategy is to fix $V \simeq F^n$.

Each subspace could have multiple basis so you might over count. Let $W < V$ be a subspace of $\dim(k)$. Orbit.

$$G = \mathrm{Aut}_F(V).Gactstransitivelyon\,\mathrm{Gr}(V,k).$$
$$\#\,\mathrm{Gr}(V,k) = \#G/stab_G(W)$$

Definition 9.3 (Action of a group G)**.** An action of a group G.

Combinatorics is usually concerned with counting the cardinality of finite sets.

Finite sets of cardinality n seem to resonate with a vector space of dimension n.

$$S \mapsto F(S,F) = functionsS \to F$$

"How many sets of size k are there in a set of size n?" resonates with "How many spaces of dimension k are there in a space of dim n where $\#F = q$.

$$\binom{n}{k}$$
$$\binom{n}{k}_q$$

§9.1 Determinants

Definition 9.4 (Linear functional)**.** A linear form (or linear functional) is a linear transfromation

$$l : V \to F$$

Definition 9.5 (Bilinear Form)**.** A bilinear form is a function $f : V \times V \to F$ such that $f(v,w)$ is linear in v when w is fixed, and linear in w when v is fixed.

$$f(v_1\lambda_1 w_1 + \lambda_2 w_2) = \lambda_1 f(v_1 w_1) + \lambda_2 f(v_1 w_2)$$
$$f(\lambda_1 v_1 + \lambda_2 v_2, w) = \lambda_1 f(v_1, w) + \lambda_2 f(v_2, w)$$

An example of such a form is the dot product.

Definition 9.6 (k-linear form)**.** A k-linear form is a function

$$f : V \times V \times \cdots \times V \to F$$

which is linear in each argument, while others are fixed.

Definition 9.7. A k-multilinear form on V is symmetric, (resp alternating).

If $f(v_{\sigma 1}, v_{\sigma 2}, \ldots, v_{\sigma k}) = f(v_1, \ldots, v_k)$ where $\sigma \in S_k$.

Example 9.8

Dot product $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ is a symmetric bilinear form. $F^n \times F^n \to F$.

Example 9.9

Cross product $\mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$.

$$(x_1, y_1, 0) \times (x_2, y_2, 0) = (0, 0, x_1y_2 - y_1x_2)$$
$$(x_1, y_1) \times (x_2, y_2) = x_1y_2 - y_1x_2$$

The collection of all (symmetric or alternating) k-multiliear functions on V is an F vector space.

Lemma 9.10

Suppose V has basis $(e_1, \dots, e_n)$. Then a bilinear form is completely determined by $f(e_i, e_j)$

$$M_f = (f(e_i, e_j))$$

A k-multilinear form is specified by

$$(f(e_{i_1}, e_{i_2}, \dots, e_{i_k}))_{1 \le i_1, \dots, i_k \le n}$$

§9.2 Alternating forms

Easy properties of alternating forms.

$$f(v_1, \dots, v_k) = 0$$

if $v_i = v_j$ where $i \neq j$ because $f(\cdots) = -f(\cdots)$. We're using that $\lambda = -\lambda \Rightarrow \lambda = 0$.

$$f(v_1, \dots, v_{j-1}, v_j + \sum_{i \neq j} \lambda_i v_i, v_{j+1}, \dots, v_k)$$
$$= f(v_1, \dots, v_j, \cdots, v_k)$$

Proposition 9.11

A k-multilinear form is completely determined by its values

$$\{f(ei_1, e_{i_2}, \dots, e_{i_j})\}_{1 \le i_1 < i_2 < \cdots < i_k \le n}$$

§10 Lecture 01-29

§10.1 Multilinear functions or forms

Note 10.1. A form is just another way of saying function.

$$f : \underbrace{V \times \cdots \times V}_{k} \to F$$

Given a basis $e_1, \ldots, e_n$ of V, the k-multilinear form f is determined by

$$(f(e_{i1}, \ldots, e_{ik}))_{1 \le i_1, \ldots, i_k \le n}$$

Definition 10.2. f is symmetric if

$$f(v_{\sigma 1}, \ldots, v_{\sigma k}) = f(v_1, \ldots, v_k) \quad \forall \sigma \in S_k$$

Definition 10.3. f is alternating if

$$f(v_{\sigma 1}, \ldots, v_{\sigma k}) = \operatorname{sign}(\sigma) f(v_1, \ldots, v_k) \quad \forall \sigma \in S_k$$

Sign is defined as follows:

$$S_k \to \{1, -1\}$$
$$\sigma \mapsto (-1)^{\text{number of transposition needed to write } \sigma}$$

Remark 10.4. If f is symmetric, then f is determined by

$$(f(v_{i1}, \ldots, v_{ik}))_{1 \le i_1 \le i_2 \le \cdots \le i_k \le n}$$

If f is alternating, then f is determined by

$$(f(v_{i1}, \ldots, v_{ik}))_{1 < i_1 < i_2 < \cdots < i_k < n}$$

Theorem 10.5

The set of alternating n-multilinear functions on a vector space of dimension n is a one-dimensional vector space.

Example 10.6

$n = 2$. $V = Fe_1 \oplus Fe_2$.

Two different approaches.

1. $$f(ae_1 + be_2, ce_1 + de_2) = acf(e_1, e_1) + adf(e_1, e_2) + bcf(e_2, e_1) + bdf(e_2, e_2)$$
   $$\text{If alternating:} \quad = (ad - bc) f(e_1, e_2)$$

2. $$f(ae_1 + be_2, ce_1 + de_2) = f(ae_1 + be_2, (-\frac{c}{a}b + d)e_2)$$
   $$= (-\frac{bc}{a} + d) f(ae_1 + be_2, e_2)$$
   $$= (-\frac{bc}{a} + d) f(ae_1, e_2)$$
   $$= (-bc + ad) f(e_1, e_2)$$

Definition 10.7. The unique n-multilinear alternating function f satisfying $f(e_1, \dots, e_n) = 1$ is called the determinant relative to $(e_1, \dots, e_n)$.

$$\det : V^n \to F$$

Note 10.8. $\det_B(v_1, \dots, v_n)$ is the value of the determinant relative to B, at $(v_1, \dots, v_n)$.

Properties: $\det_B(v_1, \dots, v_n) = 0 \Leftrightarrow (v_1, \dots, v_n)$ are linearly dependent.

Proof. $\Leftarrow$ If $(v_1, \dots, v_n)$ are linearly dependent, then WLOF, $v_1 = \lambda_2 v_2 + \cdots + \lambda_n v_n$.

$$\det(v_1, \dots, v_n) = \det(\lambda_2 v_2 + \cdots + \lambda_n v_n, v_2 \dots, v_n)$$
$$= \lambda_2 \det(v_2, v_2, v_3, \dots, v_n) + \lambda_3 \det(v_3, v_2, v_3, \dots, v_n) + \cdots + \lambda_n \det(v_n, v_2, v_3, \dots, v_n)$$
$$= \lambda_2 0 + \cdots + \lambda_n 0 = 0$$

$\Rightarrow$ Left as an exercise

□

Proposition 10.9

For $(v_1, \dots, v_n)$ in a vector space of dim n, the following are equivalent:

1. $\det_B(v_1, \dots, v_n) \neq 0$
2. $(v_1, \dots, v_n)$ are linearly independent
3. $(v_1, \dots, v_n)$ span V
4. $(v_1, \dots, v_n)$ form a basis.

§10.2 Determinent of $T : V \to V$

Proposition 10.10

There is a unique scalar d_T such that $\det_B(T(v_1), \dots, T(v_n)) = d_T \det_B(v_1, \dots, v_n)$.

Proof. The function

$$(v_1, \dots, v_n) \mapsto \det_B(T(1), \dots, T(v_n))$$

is a function $V^n \to F$ which is also n-multilinear and alternating.

$$\det'(v_1, \dots, v_n) = \det(T(v_1), \dots, T(v_n))$$
$$\det'(\lambda_1 v_1 + \lambda_1' v_1', v_2, \dots, v_n) = \det(T(\lambda_1 v_1 + \lambda_1' v_1'), T(v_2), \dots, T(v_n))$$
$$= \det(\lambda_1 T(v_1) + \lambda_1' T(v_1'), T(v_2), \dots, T(v_n))$$
$$= \lambda_1 \det(T(v_1), T(v_2), \dots, T(v_n)) + \lambda_1' \det(T(v_1'), T(v_2), \dots, T(v_n))$$
$$= \lambda_1 \det'(v_1, \dots, v_n) + \lambda_1' \det'(v_1', v_2, \dots, v_n)$$

This proves that this function is still multi-linear. We know that it's a multiple because we showed that the set of alternating functions is one-dimensional.

Therefore $\det_B(T(-), \dots, T(-))$ is a scalar multiple of $\det_B$. □

Definition 10.11. The determinent of T is the unique scalar $\det(T)$ such that

$$\det_B(T(v_1),\dots,T(v_n)) = \det(T)\cdot\det_B(v_1,\dots,v_n)$$

Note that this defining property is independent of B.

§10.3 Next week

Let $T: V \to V$. Then T generates a subring of $\mathrm{End}_F(V)$.

$$F[T] = \{a_0 I + a_1 T + a_2 T^2 + \cdots + a_k T^k\} \quad a_0,\dots,a_k \in F$$

$F[T]$ is a quotient of $F[x]$. $F[x] \to F[T]$, $p(x) \mapsto p(T)$.

$$I_T = \{p(x) \in F[x] \text{ such that } p(T) = 0_v\}$$

I_T is an ideal in $F[x]$.

$\exists! P_T(x)$ monic such that $I_T = (p_T(x))$. $P_T(x)$ is the min poly.

Characteristic Poly: $\det(xI - T)$.

§11 Lecture 01-31

Calculate $\mathrm{Gr}(k,n)$ = collection of k-dimensional subspaces in a vector space of dim n over F.
Strategy: First count the number of k-tuples $(v_1,\dots,v_k)$ of linearly independent vectors.

Possibilities for $v_1 = q^n - 1$. Possibilities for $v_2 = q^n - q$. Possibilities for $v_3 = q^n - q^2$. Possibilities for $v_k = q^n - q^{k-1}$.

Let $\Sigma \coloneqq$ the set of ordered k-tuples of linearly independent vectors.

Σ injects into $\mathrm{Gr}(k,n)$ with the function $(v_1,\dots,v_k) \mapsto \mathrm{span}(v_1,\dots,v_k)$.

Given a $W \subset V$ of dim k, how many $(v_1,\dots,v_k)$ span W. i.e. how many bases does W have?

Choices for $v_1 = q^k - 1$. Choises for $v_2 = q^k - q$. Choices for $v_k = q^k - q^{k-1}$. Therefore $p^{-1}(W) = (q^k-1)(q^k-q)\cdots(q^k-q^{k-1})$.

$$\#\,\mathrm{Gr}(k,n) = \frac{(q^n-1)(q^n-q)(\cdots)(q^n-q^{k-1})}{(q^k-1)(q^k-q)(\cdots)(q^k-q^{k-1})}$$
$$= \#\,\mathrm{Gr}(k,n) = \frac{(q^n-1)(q^{n-1}-1)(\cdots)(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)(\cdots)(q^1)}$$
$$= \binom{n}{k}_q$$
$$\binom{n}{k} = \frac{n*(n-1)*\cdots*(n-k+1)}{k*(k-1)*\cdots*1}$$

Note 11.1.

$$\frac{q^j-1}{q-1} = [j]_q = 1+q+q^2+\cdots+q^{j-1}$$
$$[j]_q! = [1]_q[2]_q\cdots[j]_q$$
$$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![n-k]_q}$$

How many subsets of size k are there in a set of size n? This question is linked to how many subspaces of dimension k are there in a vector space of dimension n.

$$\binom{n}{k} \quad \binom{n}{k}_q$$
$$x \mapsto \mathcal{F}(x,F),\ \mathcal{F}_0(x,F)$$

$$\lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}$$
$$\binom{n}{k}_q = \frac{(q^n-1)(q^{n-1}-1)(\cdots)(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)(\cdots)(q^1)}$$
$$\lim_{q\to 1}\frac{q^j-1}{q-1} = \lim_{q\to 1} jq^{j-1} = j$$
$$\frac{q^j-1}{q-1} = 1+q+\cdots+q^{j-1}$$
$$\lim_{q\to 1}(n$$

$k)_q$. Divide all elements by (q - 1) on the bottom and top

$$\lim_{q\to 1}(n$$
$$k)_q. = \frac{n*(n-1)*\cdots*(n-k+1)}{k*(k-1)*\cdots*1}$$

§12 Lecture 02-03

Question:
Calculate

$$\#\{(V_1,V_2), \dim(V_1)=k_1, \dim(V_2)=k_2, \dim(V_1\cap V_2)=d, V_1,V_2\subseteq V\}$$

Given $k_1,k_2,d,\dim V = n, \#F = q$.

New approach to solution. Let $d = 0$. Understand the set of linearly disjoint pairs (V_1,V_2) with $\dim(V_1)=k_1, \dim(V_2)=k_2$.

Number of possibilities for V_1 is

$$\binom{n}{k_1}_q = \frac{(q^n-1)(q^{n-1}-1)(\cdots)(q^{n-k_1+1}-1)}{(q^{k_1}-1)(\cdots)(q-1)}$$

Next, the number of possibilities for V_2 once V_1 is chosen:

$$(q^n-q^{k_1})(q^n-q^{k_1+1})(\cdots)(q^n-q^{k_1+k_2-1})$$

Dividing by the possible bases for a single subspace of dim k_2.

$$\frac{(q^n - q^{k_1})(q^n - q^{k_1+1})(\cdots)(q^n - q^{k_1+k_2-1})}{(q^{k_2} - 1)(q^{k_2} - q)(\cdots)(q^{k_2} - q^{k_2-1})}$$
$$= \frac{q^{k_1+(k_1+1)+(k_1+2)+\cdots+(k_1+k_2-1)}}{q^{0+1+2+\cdots+(k_2-1)}} \binom{n-k_1}{k_2}_q$$

$$= q^{k_1 k_2} \binom{n-k_1}{k_2}_q$$

So

$$\#\{(V_1, V_2), \dim(V_1) = k_1, \dim(V_2) = k_2, \dim(V_1 \cap V_2) = 0, V_1, V_2 \subseteq V\}$$
$$= \binom{n}{k_1}_q \binom{n-k_1}{k_2}_q q^{k_1 k_2}$$

Remark 12.1.

$$\binom{n}{k_1}\binom{n-k_1}{k_2}$$

is the number of disjoint subsets of cardinality k_1 and k_2 in a set of cardinality n.

Now to solve for general d.

Lemma 12.2

The set $\{(V_1, V_2)$ of dim (k_1, k_2) with $\dim(V_1 \cap V_2) = d$ is a natural bijection with the set of triples $\{(W, \overline{V_1}, \overline{V_2})$ where $W \subseteq V$, $\dim W = d$,
$\overline{V_1} \subseteq V/W$, $\dim \overline{V_1} = k_1 - d$
$\overline{V_2} \subseteq V/W$, $\dim \overline{V_2} = k_2 - d$
$\overline{V_3} \subseteq V/W$, $\dim \overline{V_3} = k_3 - d$
$\overline{V_1}, \overline{V_2}$ are linearly disjoint.

Proof.

$$(V_1, V_2) \mapsto (V_1 \cap V_2, V_1 \setminus W, V_2 \setminus W)$$
$$(\pi^{-1}(\overline{V_1}), \pi^{-1}(\overline{V_2})) \mapsfrom (W, \overline{V_1}, \overline{V_2})$$

□

$$\#\Sigma = q^{(k_1-d)(k_2-d)} \binom{n}{d}_q \binom{n-d}{k_1-d}_q \binom{n-k_1}{k_2-d}_q$$

Number of choices for $W =$

$$\binom{n}{d}_q$$

Number of choices for $(\overline{V_1}, \overline{V_2})$ given W

$$\binom{n-d}{k_1-d}_q \binom{n-k_1}{k_2-d}_q q^{(k_1-d)(k_2-d)}$$

Number of linearly disjoint spaces of dims k_1, k_2 in $\mathbb{F}^n$ =

$$\binom{n}{k_1}_q \binom{n-k_1}{k_2}_q q^{k_1 k_2}$$

Question 3 from homework.

Show that if $T : V \to V$, $\dim V = n$, then T satisfies a polynomial of degree $\leq n$.

$$p(x) = x^m + a_{m-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$p(T) = T^n + a_{m-1}T^{m-1} + \cdots + a_1 T + a_0 I$$

This shows that the space generated by

$$\underbrace{(1, T, T^2, T^3, \dots)}_{\leq n} \subseteq \underbrace{\mathrm{End}(V)}_{\leq n^2}$$

We show by induction of n that if W is any vector space of dimension n, $T : W \to W$ any endomorphism, then $\exists p(x), \deg(p(x) \leq n$, such that $p(T) = 0$.

$n = 1$. $T : V \to V, T(v) = \lambda v, \lambda \in F$.

Case 1. $\exists v \in V$ such that $v_1, Tv, T^2v, \dots, T^{n-1}v$ span V.

$-T^n v = a_0 v + a_1 Tv + a_2 T^2 v + \cdots + a_{n-1}T^{n-1}v$.

$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

$p(T)(v) = 0$. $T(p(T)(v)) = 0$.

§13 Lecture 02-05

Minimal polynomial. If $T : V \to V$, $\dim V = n$, then there exists polynomial $p(x)$ such that

$$p(T) = 0$$
$$\deg(p(x)) \leq n$$

Clear for $n = 1$.

If $\exists v \in V$ such that $(v, Tv, T^2v, \dots, T^{n-1}v)$ are linearly independent, then it is fine.

$$\exists p(x) \text{ such that } p(T)(v) = 0$$
$$\Rightarrow p(T)(Tv) = 0$$
$$p(T)(T^2 v) = 0$$
$$\vdots$$
$$p(T)(T^{n-1}v) = 0$$
$$\Rightarrow p(T) = 0$$

Suppose that there is no cyclic vector. Let $v \neq 0$ in V. Then

$$\text{span}(v, T(v), \ldots, T^{n-1}(v)) = W \subsetneq V$$

W is preserved by T.

$$T_W : W \to W$$
$$\dim W = d < n$$

The induction hypothesis implies that there is a polynomial $p_W(x)$ such that $p_W(T_W) = 0$.

It would be nice if we could write $V = W \oplus W'$. Problem is that there need not be a T-stable complementary space W'.

Solution: Define $W' = V/W$. W' is naturally equipped with

$$\overline{T} : W' \to W'$$
$$\overline{T}(v + W) = T(v) + W$$

Checking well-defined:

$$v_1 + W = v_2 + W \Rightarrow v_1 - v_2 \in W \Rightarrow T(v_1 - v_2) \in T(W) \subseteq W$$
$$\Rightarrow T(v_1) - T(v_2) \in W$$

There is a polynomial $p_{W'}(x)$ such that $p_{W'}(\overline{T}) = 0$ where $\deg p_{W'}(x) \leq n - d$.

Claim: $p(x) \coloneqq p_W(x) \cdot p_{W'}(x)$ satisfies $p(T) = 0$.

Proof. $p_{W'}(\overline{T}) = 0$. Image $p_{W'}(T) \subseteq W$.

$$p_{W'}(\overline{T}) = 0 \Rightarrow p_{W'}(\overline{T})(v + W) = 0$$
$$\Rightarrow p_{W'}(T)(v) + W = 0 + W \ \ \forall x \in V$$
$$\Rightarrow p_{W'}(T)(v) \in W \ \ \forall v \in V$$
$$p_W(T)(W) = 0$$
$$p_W(T)p_{W'}(T) = p_W(T) \circ p_{W'}(T) = 0$$

□

Goal of linear algebra:

1. Given $T : V \to V$, classify all possible T.
2. Find bases for V which are "convenient" to study T.

Structural invariants attached to T.

1. Minimal polynomial $p_T(x)$
2. Characteristic polynomial $f_T(x) = \det(xI - T)$. $\deg(f_T(x)) = n = \dim V$.

Definition 13.1 (Eigenvalue)**.** An element $\lambda \in F$ is an eigenvalue for T if $\exists$ a non-zero $v \in V$ such that $T(v) = \lambda v$. A vector v with this property is called an eigenvector of T, with eigenvalue λ. Note that the zero vector is never considered an eigenvector.

Definition 13.2 (Eigenspace)**.** The set $V_\lambda = \{v \in V \text{ such that } T(v) = \lambda v\}$ is called the eigenspace for T.

Definition 13.3 (Spectrum)**.** The spectrum of T is the collection of eigenvalues of T. $spec(T) \subseteq F$.

Proposition 13.4
If $\lambda_1 \neq \lambda_2 \in spec(T)$, then V_{λ_1} and V_{λ_2} are linearly disjoint, i.e. $V_{\lambda_1} \cap V_{\lambda_2} = (0)$.

Proof. If $v \in V_{\lambda_1} \cap V_{\lambda_2}$, then $T(v) = \lambda_1 v, T(v) = \lambda_2 v \Rightarrow (\lambda_1 - \lambda_2)v = 0$. $\lambda_1 - \lambda_2 \neq 0 \Rightarrow v = 0$. □

Definition 13.5 (Diagonalizable)**.**

$$\text{If } \oplus_{\lambda \in spec(T)} V_\lambda = V$$

then T is diagonalizable.

Equivalently, T is diagonalizable if V has a basis of eigenvectors for T.

Example 13.6 1. $V = \mathbb{R}^2$, where T is a rotation by $\pi/2$.

§14 Lecture 02-07

$spec(T)$ = set of eigenvalues of $T = \{\lambda \in F : \exists v \neq 0 : T(v) = \lambda v\}$.

$$\oplus_{\lambda \in spec(T)} V_\lambda \subseteq V$$
$$V_\lambda = \{v | T(v) = \lambda v\}$$
$$\Rightarrow \#spec(T) \leq \dim V$$

Two polynomials attached to T.

1. $p_T(x)$ is the minimal polynomial of T. $\deg p_T(x) \leq \dim(V)$
2. $f_T(x)$ = characteristic polynomial = $\det(xI - T)$

Theorem 14.1

If $\lambda \in F$, then

$$p_T(\lambda) = 0 \Leftrightarrow \lambda \in spec(T)$$

Proof.

($\Leftarrow$) $\exists v \neq 0$ such that $T(v) = \lambda v$. Then $T^2(v) = \lambda^2 v$. Then $T^j(v) = \lambda^j v$.

Let $g \in F[x]$. Then

$$g(T)(v) = g(\lambda)(v)$$
$$\lambda \in spec(T) \Rightarrow g(\lambda) \in spec(g(T))$$

$$p_T(T)(v) = p_T(\lambda)v$$
$$0(v) = p_T(\lambda)v$$
$$0 = p_T(\lambda)v$$
$$\Rightarrow p_T(\lambda) = 0$$

($\Rightarrow$)

$$p_T(\lambda) = 0$$
$$\Rightarrow p_T(x) = (x - \lambda)g(x)$$
$$\deg g(x) < \deg p_T(x) \Rightarrow g(T) \neq 0$$
$$0 = p_T(T) = (T - \lambda I) \circ g(T)$$
$$\Rightarrow \mathrm{Im}(g(T)) \subseteq \ker(T - \lambda I) = V_\lambda$$
$$V_\lambda \neq \{0\} \Rightarrow \lambda \in spec(T)$$

□

Theorem 14.2

If $\lambda \in F$, then

$$f_T(\lambda) = 0 \Leftrightarrow \lambda \in spec(T)$$

Proof.

$$\begin{aligned} f_T(\lambda) = 0 &\Leftrightarrow \det(\lambda I - T) = 0 \\ &\Leftrightarrow T - \lambda \text{ is non-invertible} \\ &\Leftrightarrow \ker(T - \lambda) \supsetneq \{0\} \\ &\Leftrightarrow V_\lambda \neq \{0\} \\ &\Leftrightarrow \lambda \in spec(T) \end{aligned}$$

□

§14.1 Voting with vectors

A, B, C candidates.

$$\begin{aligned} A > B > C \quad & (1,1,-1) \\ A > C > B \quad & (1,-1,1) \\ B > A > C \quad & (-1,1,-1) \\ B > C > A \quad & (-1,1,1) \\ C > A > B \quad & (1,-1,1) \\ C > B > A \quad & (-1,-1,1) \end{aligned}$$

Where the vectors encode the following: $(A > B,\ B > C,\ C > A)$

If N_1 votes vote for $(-1,1,1)$, N_2 vote for $(1,-1,1)$, and N_3 vote for $(1,1,-1)$, then

$$N_1(-1,1,1) + N_2(1,-1,1) + N_3(1,1,-1) = (X,Y,Z)$$

where X represents the margin of voters who prefer A to B, Y represents the margin of voters who prefer B to C, and Z represents the margin of voters who prefer C to A.

Consider the following scenario. The population is $3N$. N people vote $(-1,1,1)$, N people vote $(1,-1,1)$, and N people vote $(1,1,-1)$. Then

$$\text{Vote} = (N,N,N)$$

So 66% prefer A to B, 66% prefer B to C, and 66% prefer C to A. So even though everyone voted rationally, a weird scenario arose.

§15 Lecture 02-10

$T : V \to V$. $T \in \text{End}_F(V)$.

Key Invariants

1. Minimal polynomial $p_T(x)$. Defining property: for all $g(x) \in F[x]$, $g(T) = 0 \Rightarrow p_T(x) | g(x)$.
2. Characteristic polynomial $f_T(x) = \det(xI_V - T)$. $f_T(x)$ is a monic polynomial of $d = n = \dim V$.

$spec(T) = \{eigenvalues\}$. $\lambda \in spec(T), 0 \neq V_\lambda \subseteq V$

Eigenvalue decomposition

$$\oplus_{\lambda \in spec(T)} V_\lambda \subseteq V$$

If $\oplus_{\lambda \in spec(T)} V_\lambda = V$, we say that T is diagonalizable.

Theorem 15.1

The spectrum of T is exactly the set of roots of the characteristic polynomial or of the minimal polynomial of T. This means that the characteristic and minimal polynomial have the same roots.

Note 15.2. Very often, polynomials need not have root in F.

Example 15.3 1. $F = \mathbb{R}$. $p(x) = x^2 + 1$

2. $F = \mathbb{Q}$. $p(x) = x^2 - 2$.

In $F[x]$, every polynomial can be written uniquely as $p(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_r(x)$, where $p_j(x)$ distinct, monic, irreducible polynomials.

Exercise 15.4. 1. Given (T, V), can $\overline{V}$ be broken into a direct sum of (proper) T-stable subspaces.

2. Give simple criteria for T to be diagonalizable.

Proposition 15.5

Suppose that $p_T(x) = p_1(x)p_2(x)$ with $\gcd(p_1(x), p_2(x)) = 1$. Then $V = V_1 \oplus V_2$ where V_1 and V_2 are preserved by T, and $T_j = T|V_j$ has minimal polynomial $p_j(x)$.

Proof. $P_T(x) = p_1(x)p_2(x)$. $0 = p_1(T) \circ p_2(T)$. Define

$$V_1 = \ker(p_1(T))$$
$$V_2 = \ker(p_2(T))$$

Now to show that $T(V_1) \subseteq V_1$. Let $w \in V_1$. We want to check if $T(w) \in ker(p_1(T)) \Rightarrow p_1(T)(T(w)) = 0$

$$p_1(T)(T(w)) = p_1(T) \circ T(w) = T \circ p_1(T)(w) = T(p_1(T)(w)) = T(0)$$

We can do this because T commutes with itself, and $p_1(T)(w) = 0$. □

$$\{a(x)p_1(x) + b(x)p_2(x),\ a, b \in F[x]\} = F[x]$$
$$\Rightarrow \exists a(x), b(x) \in F[x] \text{ such that } a(x)p_1(x) + b(x)p_2(x) = 1$$
$$\Rightarrow a(T) \circ p_1(T) + b(T)p_2(T) = 1_V \text{ the identity from } V \text{ to } V$$
$$\text{Evaluating at } w \in V \ p_1(T)(a(T)(w)) + p_2(T)(b(T)(w)) = w$$
$$w_2 + w_1 = w$$
$$w_1 \in \mathrm{Im}(p_2(T)) \subseteq \ker(p_1(T)) = V_1$$
$$w_2 \in \mathrm{Im}(p_1(T)) \subseteq \ker(p_2(T)) = V_2$$
$$\Rightarrow \mathrm{span}(V_1, V_2) = V$$

Remains to show that $V_1 \cap V_2 = \{0\}$. Suppose we have $\ker(p_1(T)) \cap \ker(p_2(T))$. Evaluating $(*)$ at w_1 we get $0 + 0 = w \Rightarrow w = 0$.

Theorem 15.6

If $p_T(v) = p_1(x)p_2(x)\cdots p_r(x)$, where $\gcd(p_1(x), p_j(x)) = 1 \ \forall i \neq j$, then $\exists\ V_1, \ldots, V_r$ such that

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

where

$$V_j = \ker(p_j(T))$$

i.e. $T|V_j$ has minimal polynomial $p_j(x)$.

Proof. Induction on r. □

So we can write $p_T(x) = p_1(x)^{e_1}\cdots p_r(x)^{e_r}$, $e_j \geq 1$, $p_1(x), \ldots, p_r(x)$ are irreducible and distinct. We get

$$V = V_1 \oplus \cdots \oplus V_r,$$

where, if $T_j = T|_{V_j}$, $p_{T_j}(x) = p_j(x)^{e_j}$.

This direct sum decomposition is called the primary decomposition attached to T.

§16 Lecture 02-14

$$T : V \to V$$

If $p_T(x)$ factors into linear factors, (for example if the field F is algebraically closed, then every irreducible polynomial is linear), then

$$V = \oplus_{\lambda \in spec(T)} V_{[\lambda]}$$

$$\text{Generalized eigenspace for } \lambda: \quad V_{[\lambda]} = \{v : (T-\lambda)^j(v) = 0\}$$

$$\text{Eigenspace for } \lambda: \quad V_\lambda = \{v : (T-\lambda)(v) = 0\}$$

$V_\lambda = V_{[\lambda]} \Leftrightarrow (x-\lambda) | p_T(x)$ but $(x-\lambda)^2 \nmid p_1(x)$

T is diagonalizable $\Leftrightarrow$ $p_T(x)$ factors into distinct linear factors.

Theorem 16.1

T diagonalizable $\Leftrightarrow$ $p_T(x)$ factors into distinct linear factors.

Example 16.2

$F = \mathbb{Z}/p\mathbb{Z}$. T satisfies $T^p = T \Rightarrow T$ satisfies $x^p - x \Rightarrow p_T(x)$ divides $x^p - x$.

This implies $p_T(x) = (x-\lambda_1)(\cdots)(x-\lambda_r)$, $\lambda_1 \neq \lambda_2 \neq \cdots \neq \lambda_r$. Therefore T is diagonalizable.

Example 16.3

$T^n = 1 \Rightarrow p_T(x)$ divides $x^n - 1$.

If $x^n - 1$ factors into distinct linear factors in F, then T is diagonalizable.

Conversely, if all T satisfying $T^n = 1$ are diagonalizable, then $x^n - 1$ factors into distinct linear factors.

In order to prove the converse, we need to show that $\exists T$ such that $p_T(x) = x^n - 1$.

$$V = F^n = Fe_1 \oplus \cdots \oplus Fe_n$$
$$T(e_j) = e_{j+1} \quad (j = 1, \ldots, n-1)$$
$$T_(e_n) = e_1$$

Proposition 16.4

If $p(x) \in F[x]$, then $\exists$ a vector space V over F, and $T : V \to V$ such that $p_T(x) = p(x)$.

Proof. Let $V = F[x]/(p(x))$. $\dim V = n$.

$$T(g(x) + (p(x)) = xg(x) + (p(x))$$
$$f(T)(g(x) + (p(x)) = f(x)g(x) + (p(x))$$

If we want $f(T) = 0$ then $f(T)(1 + (p(x)) = 0 \Rightarrow f(x) + (p(x)) \Rightarrow p(x)|f(x) \Rightarrow p(x) = p_T(x)$ □

Example 16.5

When is it possible to factor $x^n - 1$ in the following fields? $F = \mathbb{Q}$.Then $n \leq 2$. $F = \mathbb{R}$, then $n \leq 2$. $F = \mathbb{C}$, then any n. $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

§17 Lecture 02-17

§17.1 Dunford Decomposition

$$T : V \to V$$

If $p_T(x) = (x - \lambda_1)^{e_1}(\cdots)(x - \lambda_r)^{e_r}$, then $\exists$ D, N where D and N commute, D is diagonalizable, N is nilpotent, and $T = D + N$.

Definition 17.1 (Nilpotent)**.** Nilpotent if $N^d = 0$ for some $d \in \mathbb{N}$.

Application. Given $g(x) \in F[x]$, evaluate $g(T)$.

$$g(D + N) = g(D) + g'(D)N + \frac{g''(D)}{2!}N^2 + \cdots + \frac{g^j(D)}{j!}N^j + \frac{g^{e-1}(D)}{(e-1)!}N^{e-1}$$

where $N^e = 0$.

Relative to an eigenbasis, we have

$$D \sim \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_n \end{pmatrix}$$
$$g(D) \sim \begin{pmatrix} g(\lambda_1) & 0 \\ 0 & g(\lambda_n) \end{pmatrix}$$

More generally if g is defined by a convergent power series, and $\lambda_1, \ldots, \lambda_n$ belong to the domain of convergence, we have

$$g(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$
$$g(T) = a_0 I + a_1 T + a_2 T^2 + \cdots + a_n T^n + \cdots$$

If $g(x)$ is $(e-1)$ times differentiable, and $\lambda_1, \ldots, \lambda_n$ belong to the domain of convergence for $g(x)$, then

$$g(T) = g(D+N) = \sum_{j=0}^{e-1} \frac{g^j(D)}{j!} N^j$$

Example 17.2

$$g(x) = e^x = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n!}$$
$$e^D \sim \begin{pmatrix} e^{\lambda_1} & 0 \\ 0 & e^{\lambda_n} \end{pmatrix}$$

Focusing on a single generalized eigenbasis, what is the "nicest" basis for V_λ.

$T = \lambda + N$. We can choose a basis for V in such a way that

$$\text{Upper Triangular } M_{T,B} = \begin{pmatrix} \lambda & x \\ 0 & \lambda \end{pmatrix}$$

A jordon subspace W for N is a subspace of V that admins a cyclic vector. i.e. a vector $v \in W$ such that $v, Nv, \ldots, N^{e-1}v$ spans W.

Relative ot the basis $N^{e-1}v, N^{e-2}v, \ldots, Nv, v$, N is represented by

$$J_{0,e} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

T is represented by

$$J_{\lambda,e} = \begin{pmatrix} \lambda & 1 & 0 & 0 \\ 0 & \lambda & 1 & 0 \\ 0 & 0 & \lambda & 1 \\ 0 & 0 & 0 & \lambda \end{pmatrix}$$

Definition 17.3 (Jordan Matrix)**.** The vector $J_{\lambda,e}$ is called the Jordan matrix, or Jordan block of size e and eigenvalue λ.

Theorem 17.4 (Jordon Decomposition)
If $N : V \to V$ is a nilpotent endomorphism, then V can be decomposed into a direct sum of Jordon subspaces

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_j$$

Proof. Pianful. This decomposition is not unique.

Remark 17.5. Let $V_0 \subseteq V$. V_0 need not admit an N-stable complement.

□

Theorem 17.6 (Concrete Form)
If M is a matrix with char polynomial $(x-\lambda_1)^{e_1}\cdots(x-\lambda_r)^{e_r}$, then M is similar to a matrix of the form: Wait wait start over.

If $p_T(x) = (x-\lambda)^e$ and $f_T(x) = (x-\lambda)^d$, $e \leq d$, then $\exists$ basis B for V such that

$$M_{T,B} = \begin{pmatrix} J_{\lambda,e_1} & 0 & 0 \\ 0 & J_{\lambda,e_2} & 0 \\ 0 & 0 & J_{\lambda,e_r} \end{pmatrix}$$

$$e_1 + e_2 + \cdots + e_r = d$$
$$\max(e_1, \ldots, e_r) = e$$
$$T(J_{\lambda,e} - \lambda I)^e = 0$$

§18 Lecture 02-19

Vector spaces. Basis. Let V be a vector space over F. Then there exists a basis B of V such that all $v \in V$ can be written uniquely as a sum

$$\sum_{w \in B} \lambda_w w \quad \lambda_w \in F$$

$\lambda_w = 0$ for all but finitely many $w \in B$. Therefore

$$V = F_0(B, F)$$
$$v \mapsto (w \mapsto \lambda_w)$$
$$F_0(B, F) \subseteq F(B, F)$$

Exercise 18.1. Show that there are vector spaces that are not isomorphic to $F(X, F)$ for any set X.

Attempt 1:

$$\begin{aligned} V = F[[x]] &= \{a_0 + a_1 x + a_2 x^2 + \cdots\} \\ &= \{(a_0, a_1, a_2, \dots) \quad a_j \in F\} \\ &= \{a : \{0, 1, 2, \dots\} \to F\} \\ &= Func(\mathbb{N}, F) \end{aligned}$$

Attempt 2:

$$F[x] = \{a_0 + a_1 x + \cdots + a_n x^n \quad a_i \in F\}$$

So $F[x]$ has a countable basis.

1. If X is finite, then $\dim(Func(X, F))$ is also finite.
2. If X is infinite, then $Func(X, F)$ does not have a countable basis.

If $F = \mathbb{Q}$, we observe that $Func(X, \mathbb{Q})$ is uncountable.

$$\begin{array}{ll} f_1 & f_1(x_1), f_1(x_2) \dots \\ f_2 & f_2(x_1), f_2(x_2) \dots \\ f_n & f_n(x_1), f_n(x_2) \dots \end{array}$$

Define $f(x_n) = f_n(x_n) + 1$

1. TOH, $\mathbb{Q}[x]$ is countable.
2. $F = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. $Func(X, \mathbb{F}_2) = P(X) = \{A \subseteq X\}$.

   $Func(X, \mathbb{F}_2)$ is either finite, or uncountable. $\mathbb{F}_2[x]$ is countable.

Exercise 18.2. Show that, for any F, that $Func(X, F)$ does not have a countable basis.

§19 Lecture 02-21

> **Theorem 19.1**
> If M is a symmetric $n \times n$ matrix with real entries, then M is diagonalizable.

If M is symmetric, then $M = (a_{ij})_{i,j=1,\dots,n}$, $\quad a_{ij} = a_{ji}$.
Language for approaching this result: self adjoint operators on inner product spaces.

§19.1 Duality

V vector space. V^* is the space of linear functionals $V \to F$.

If $T : V_1 \to V_2$ is a linear transformation, then it induces

$$T^* : V_2^* \to V_1^*$$
$$T^*(l) = l \circ T$$

$$V_1 \to_{T_1} V_2 \to_{T_2} V_3$$
$$(T_2 \circ T_1)^* : V_3^* \to V_1^*$$
$$(T_2 \circ T_1)^* = T_1^* \circ T_2^*$$

$$l \in V_3^*$$
$$(T_2 \circ T_1)^*(l) = l \circ (T_2 \circ T_1) = (l \circ T_2) \circ T_1$$
$$= [T_2^*(l)] \circ T_1 = T_1^*(T_2^*(l)) = T_1^* \circ T_2^*(l)$$

Lemma 19.2

1. If $T : W \to V$ is injective, then $T^* : V^* \to W^*$ is surjective.
2. If $T : V \to W$ is surjective, then T^* is injective.

Proof.

1. If T is injective, then it realises co inclusion of W into V and

   $$T^*(l) = l|_{\mathrm{Im}(T)=W}$$

   Surjectivity of T^* means that given $l_0 : \mathrm{Im}(T) \to F$, $\exists$ an extension $l : V \to F$ such that $l|_W = l_0$. After choosing a complementary W' such that $W \oplus W' = V$, we let $l(w + w') = l_0(w)$.

2. If $T : V \to W$ is surjective, then $\ker(T^*) = \{l : W \to F \text{ such that } l \circ T = 0\}$

   $$\begin{aligned} l \circ T = 0 &\Leftrightarrow l \circ T(v) = 0 && \forall v \in V \\ &\Leftrightarrow l(T(v)) = 0 && \forall v \in V \\ &\Leftrightarrow l(w) = 0 && \forall w \in \mathrm{Im}(T) \\ &\Leftrightarrow l(w) = 0 && \forall w \in W \end{aligned}$$

   So $\ker(T^*) = 0 \Rightarrow T^*$ is injective.

If W is a subspace of V, then W^* is a quotient of V^*. If W is a quotient of V, then W^* is a subspace of V^*.

$$W^* = \{l : V \to F \text{ such that } l|_{\ker(V \to W)=0}\}$$

□

GIven a $W \subseteq V$, there is a canonical subspace of V^* attached to W,

$$W^\perp = \ker(V^* \to W^*)$$
$$W^\perp = \{l : V \to F \text{ such that } l(W) = 0\}$$

The assignment $W \mapsto W^\perp$ sets up an inclusion reversion bijection between subspaces of V and subspaces of V^*.

$$W \Leftrightarrow W^\perp$$
$$0 \Leftrightarrow V^*$$
$$V \Leftrightarrow 0$$

Claim: $\dim(W) + \dim(W^\perp) = \dim(V) = \dim(V^*)$.
Caveat: $W \oplus W^\perp$ does not make sense.

Proof.

$$i : V \hookrightarrow V$$
$$i^* : V^* \to W^*$$
$$W^\perp = \ker(i^* : V^* \to W^*)$$

□

§19.2 Rank-nullity Theorem

$$\dim(W^\perp) + \dim(W^*) = \dim(V^*)$$
$$\dim(W^\perp) + \dim(W) = \dim(V)$$

If $W \subseteq V^*$, then $W^\perp \subseteq V$. $W^\perp = \{v \in V \text{ such that } l(v) = 0, \quad \forall l \in W\}$.

§20 Lecture 02-24

Definition 20.1 (Bilinear Forms)**.** A bilinear form $B : V \times V \to F$ is said to be left non degenerate if $B(v, w) = 0,\ \forall w \in V \Rightarrow v = 0$.

Note 20.2.

$$B(v, w) = \langle v, w \rangle$$

Key remark: A non-degenerate bilinear form induces a linear injection

$$l : V \to V^*$$
$$v \mapsto l_v$$
$$l_v(w) = \langle v, w \rangle$$

Now to show the following:

1. l_v is indeed a linear transformation (follows from the linearity of $\langle , \rangle$ in the second variable)
2. The assignment $v \mapsto lv$ is linear (follows from the linearity of $\langle , \rangle$ in the first variable.

Lemma 20.3

If $\dim V < \infty$, then l is an isomorphism between V and V^*.

Proof. $\langle , \rangle$ is left-nondegenerate $\Rightarrow l : V \hookrightarrow V^*$ is injective.

The rank-nullity theorem implies that since $\dim V = \dim V^*$, l is also surjective. □

Exercise 20.4. Is it possible to classify all possible bilinear forms on V, up to isomorphism?

If V is finite dimensional, we can choose a basis $\sum = (e_1, \ldots, e_n)$ for V such that

$$v = \sum_{i=1}^{n} x_i e_i$$
$$w = \sum_{j=1}^{n} y_j e_j$$
$$\langle v, w \rangle = \langle \sum x_i e_i, \sum y_j e_j \rangle$$
$$= \sum_{i,j=1}^{n} x_i y_j \langle e_i, e_j \rangle$$

Definition 20.5. The pairing matrix associated to $B(v, w) = \langle v, w \rangle$, and the basis $\sum$.

$$M_{B,\sum} = (\langle e_i, e_j \rangle)_{i,j=1,\ldots,n}$$
$$\langle v, w \rangle = (x_1, \ldots, x_n) M_{B,\sum} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

The most general bilinear form on F^n is given by a matrix M, by

$$\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = (x_1, \ldots, x_n) M \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Lemma 20.6

$\langle , \rangle$ is left-nondegenerate $\Leftrightarrow M_{B,\sum}$ is invertible.

Proof. Left as exercise. □

§20.1 Change of Basis

Let $\sum = (e_1, \dots, e_n)$ and $\sum' = (e_1', \dots, e_n')$ be two bases for V. How are $M_{B,\sum}$ and $M_{B,\Sigma'}$ related?

$$\begin{pmatrix} e_1' \\ \vdots \\ v_n' \end{pmatrix} = P_i \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

$$p \in M_n(F), \text{ invertible}$$

$$m_{B,\Sigma} = \langle \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}, (e_1, \dots, e_n) \rangle$$

$$M_{B,\Sigma'} = \langle \begin{pmatrix} e_1' \\ \vdots \\ e_n' \end{pmatrix}, (e_1', \dots, e_n') \rangle$$

$$(e_1', \dots, e_n') = (e_1, \dots, e_n) P^t$$

$$P = (a_{ij}) \quad p^t = (a_{ji})$$

$$M_{B,\Sigma'} =$$

$$M_{B,\Sigma'} = P M_{B,\Sigma} P^t$$

Corollary 20.7

Two matrices M_1 and M_2 represent the same bilinear form $\Leftrightarrow$ there exists an invertible linear transformation P such that $M_1 = P M_2 P^t$

Isomorphism classes of linear transformations on $F^n = M_n(F)/\operatorname{GL}_n(F)$ where the group $\operatorname{GL}_n(F)$ acts on the set $M_n(F)$ by conjugation $M^g = gMg^{-1}$.

Isomorphism classes of bilinear forms we likewise identified with

$$M_n(F)/\operatorname{GL}_n(F)$$

, but where the action of $\operatorname{Gl}_n(F)$ on $M_n(F)$ is very different

$$g * M = gMg^t$$

Example 20.8

1. Orbit of I_n for the conjugation action $= \{I_n\}$.
2. Orbit of I_n for the second action is the set of $\{pp^t, p \in \operatorname{GL}_n(F)\}$

Exercise 20.9. There are no orbits of size 1 for the action $M \mapsto gMg^t$.

Definition 20.10. A vector space equipped with a non-degenerate bilinear form B is called a quadratic space (V, B).

An isomorphism $T : (V_1, B_2) \to (V_2, B_2)$ is the natural notion. A linear isomorphism $T : V_1 \to V_2$, $\forall v, w \in V_1$,

$$\langle v, w \rangle_{B_1} = \langle Tv, Tw \rangle_{B_2}$$

The adjoint of a linear transformation $T : V \to V$ when V is a quadratic space, endowed with a nondegerenate form.

$$T : V \to V$$
$$T^* : V^* \to V^*$$
$$T^*(l) = l \circ T$$

The adjoint of T on the quadratic space V is the linear transformation defined by

$$T^*(lv) = l_{T^*(v)}$$
$$T^*(lv)(w) = l'_{T^*v}(w)$$
$$lv \circ T(w) = \langle T^*v, w \rangle$$
$$\langle v, T(w) \rangle$$

$$\langle v, Tw \rangle = \langle T^*v, w \rangle$$

§21 Lecture 02-26

§21.1 Group Actions on Sets

Let G be a group.

Definition 21.1. An action G on X is a function

$$G \times X \to X$$
$$(g, x) \mapsto gx$$

satisfying

$$1_G x = x \quad \forall x \in X$$
$$g_2(g_1 x) = (g_2 g_1)x \quad \forall g_1 g_2 \in G$$

An action G on X gives rise to a homomorphism

$$\varphi : G \to S_x = \{ \text{ bijections } X \to X \}$$
$$\varphi(g)(x) = gx$$

§22 Lecture 02-28

An action of G on X is a function

$$G \times X \to X$$
$$(g, x) \mapsto gx$$

satisfying $1_G \cdot x = x$ and $g_1(g_2 x) = (g_1 g_2)x$.

Equivalently, an action of G on X is a homomorphism

$$\varphi : G \to S_x = perm(X)$$
$$\varphi \rightsquigarrow g \cdot x = \varphi(g)(x)$$
$$\text{Action } G \times X \to X \rightsquigarrow \varphi(g)(x) = gx$$

Terminology: A set X endowed with an action of G is called a G-set.

If X_1 and X_2 are two G-sets, a homomorphism $f : X_1 \to X_2$ is a function satisfying $f(gx_1) = g \cdot f(x_1)$

If X_1 and X_2 are G-sets, so it $X_1 \sqcup X_2$.

Definition 22.1 (Transitive G-set)**.** A G-set X is transitive if it cannot be expressed as a disjoin union of non-empty G-sets. If X is transitive, choose $x_0 \in X$.

$$Gx_0 = \{gx_0,\ g \in G\}$$

is called the orbit of x_0 under actions of G. Then $X = Gx_0,\ \forall x_0 \in X$. More generally,

$$\exists x_i,\ (i \in I)\ X = \sqcup_{i \in I} G_{x_i}$$

Example 22.2

$X = G$. $G \times X \to X$ is left multiplication. X is transitive. If $g \in G$, and $gx = x \forall x \in X \Rightarrow g = id$.

$$\varphi : G \hookrightarrow S_G$$

Cayley's theorem: Every G is a subgroup of S_n. So $G = S_n$, $\varphi : G \hookrightarrow S_{S_n} = S_{n!}$

Example 22.3

If H is a subgroup of G, then G/H is a G-set.

$$(g, aH) \rightsquigarrow gaH$$
$$\ker(G \to S_{G/H}) = \{g \in G \text{ such that } gaH = aH\}$$
$$gaH = aH,\ \forall a \in G$$
$$a^{-1}gaH = H,\ \forall a \in G$$
$$a^{-1}ga \in H,\ \forall a \in G$$
$$g \in aHa^{-1},\ \forall a \in G$$
$$g \in \cup_{a \in G} aHa^{-1}$$

$\ker(G \to S_{G/H})$ is the largest normal subgroup of G conained in H. In particular, if H contains no non-trivial normal subgroups, then $G \hookrightarrow S_{G/H}$ is injective.

Example 22.4

$$X = G,\ g * x = gxg^{-1}$$
$$1_G * x = 1x1^{-1} = x$$
$$(g_1g_2) * x = g_1g_2x(g_1g_2)^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = g_1(g_2 * x)g_1^{-1}$$
$$= g_1 * (g_2 * x)$$

$$G = S_3 = \{1, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$$
Orbits: $\{1\}, \{(1\,2\,3), (1\,3\,2)\}, \{(1\,2), (1\,3), (2\,3)\}$

Proposition 22.6

If X is a transitive G-set, then it is isomorphic to G/H for some subgroup H.

Proof. Let $x_0 \in X$. We know that $Gx_0 = X$. Consider the function

$$G \to X$$
$$g \mapsto gx_0$$

This function is a homomorphism of G-sets. It is surjective, by transitivity.

The map ζ is not injective in general. $\zeta^{-1}(x_0) =$ the preimage of x_0 is

$$Stab_G(x_0) = G_{x_0} = \{g \in G \text{ such that } gx_0 = x_0\}$$

Set $H = G_{x_0}$. We defined $\overline{\zeta} : G/H \to X$ by $\overline{\zeta}(gH) = gx_0$.

Claim: $\overline{\zeta}$ is a bijection of G-sets.

1. $\overline{\zeta}$ is well-defined.

   If $g_1H = g_2H$, then $g_2 = g_1h,\ h \in H$. $g_2x_0 = (g_1h)x_0 = g_1(hx_0) = g_1x_0$
2. $\overline{\zeta}$ is surjective $\Leftarrow$ transitivity.
3. $\overline{\zeta}$ is injective.

$$\overline{\zeta}(g_1H) = \overline{\zeta}(g_2H) \Rightarrow g_1x_0 = g_2x_0 \Rightarrow g_2^{-1}g_1x_0 = x_0$$
$$\Rightarrow g_2^{-1}g_1 \in H \Rightarrow g_1H = g_2H$$

□

Corollary 22.7

If G is finite, then any transitive G-set X is also finite, and

$$\#X = \frac{\#G}{\#Stab_G(x_0)}$$

Orbit stabiliser theorem.

Proof. $X \simeq G/Stab_G(x_0)$ as a G-set. Hence

$$\#X = \#(G/Stab_G(x_0)) = \frac{\#G}{\#Stab_G(x_0)}$$

□

§23 Lecture 03-09

A quadratic space is a pair $(V, <,>)$ where V is a vector space, and $<,>: V \times V \to F$ which is bilinear.
The pairing $(<,>)$ is non-degenerate if it induces an injection

$$V \to V^*$$
$$v \mapsto (w \mapsto < v, w >)$$
$$(\text{when dim V } < \infty, \text{ then } V \simeq V^*)$$

The adjoint of $T : V \to V$ is the map satisfying

$$T* : V \to V$$
$$< v, Tw >=< T^*(v), w >$$

Question: Where do non-degenerate bilinear forms arise "in nature"?
Answer: Geometry, distance.
From now on, $F = \mathbb{R}$ or $\mathbb{C}$.

Definition 23.1. A real inner product on V is a bilinear form satisfying:

1. $$< v, w >=< w, v >, \quad \forall v, w \in V$$

2. $$< v, v >\geq 0, \quad < v, v >= 0 \text{ iff } v = 0$$

Example 23.2 1. $V = \mathbb{R}^n$

$$< (x_1, \ldots, x_n), (y_1, \ldots, y_n) >= x_1y_1 + x_2y_2 + \cdots + x_ny_n$$
$$< (x_1, \ldots, x_n), (x_1, \ldots, x_n) >= x_1^2 + x_2^2 + \cdots + x_n^2$$

2. $V = e([0,1])$ represents continuous real-valued functions on $[0,1]$.

$$< f, g >= \int_0^1 f(t)g(t)dt, \quad < f, f >= \int_0^1 f(t)^2 dt$$

Definition 23.3 (Complex Inner Product)**.** A complex inner product on V is a hermition-bilinear form satisfying

Note 23.4. It would become problamatic to try and declare it as a standard bilinear form

1.
$$< v, \lambda w_1 + w_2 >= \overline{\lambda} < v, w_1 > + < v, w_2 >$$

2.
$$< v, w >= \overline{< w, v >}$$

3.
$$< v, v > \in \mathbb{R} \geq 0, \quad < v, v >= 0 \Leftrightarrow v = 0$$

Example 23.5

Reviewing the previous examples with the new complex inner product

1. $V = \mathbb{C}^n$

$$< (x_1, \ldots, x_n), (y_1, \ldots, y_n) >= x_1\overline{y_1} + x_2\overline{y_2} + \cdots + x_n\overline{y_n}$$
$$< (x_1, \ldots, x_n), (x_1, \ldots, x_n) >= |x_1|^2 + |x_2|^2 + \cdots + |x_n|^2$$

2. $V = e([0,1])$ represents continuous complex-valued functions on $[0,1]$.

$$< f, g >= \int_0^1 f(t)\overline{g(t)}dt, \quad < f, f >= \int_0^1 |f(t)|^2 dt$$

Note 23.6. Caveat: A complex inner product space is not (quite) a quadratic space as defined before.
We define the norm of v to be $||v|| = \sqrt{< v, v >}$. "Length of v".

Example 23.7 1. $V = \mathbb{R}^n$.

$$||(x_1, \ldots, x_n)|| = \sqrt{x_1^2 + \cdots + x_n^2}$$

2. $V = \mathbb{C}^n$.

$$|(z_1, \ldots, z_n)|| = \sqrt{|z_1|^2 + |z_2|^2 + \cdots + |z_n|^2}$$

Definition 23.8 (Properties of $||\ ||$)**.** Always easier to think about the square of the norm.

1.

$$\begin{aligned} ||v+w||^2 &= < v+w, v+w > = < v, v > + < v, w > + < w, v > + < w, w > \\ &= ||v||^2 + 2 \text{ Real part of } < v, w > + ||w||^2 \end{aligned}$$

Definition 23.9. Two vectors v, w are orthogonal if $< v, w >= 0$.

Theorem 23.10 (Pythagorean Theorem)

$$||v+w||^2 + ||v||^2 + ||w||^2$$

Theorem 23.11 (Parallelogram Law)

$$||v+w||^2 + ||v-w||^2 = 2(||v||^2 + ||w||^2)$$

$$\begin{aligned} ||v+w||^2 + ||v-w||^2 &= ||v||^2 + 2Re < v, w > + ||w||^2 + ||v||^2 - 2Re(< v, w >) + ||w||^2 \\ &= 2(||v||^2 + ||w||^2) \end{aligned}$$

□

Theorem 23.12 (Polarization Formula)

The function $v \mapsto < v, v >$ is enough to recover $(v, w) \mapsto < v, w >$.

1. If $F = \mathbb{R}$

$$< v, w >= 1/2(< v + w, v + w > - < v, v > - < w, w >)$$
$$< v, w >= \frac{1}{4}(< v + w, v + w > - < v - w, v - w >)$$

2. If $F = \mathbb{C}$

$$\begin{aligned} < v, w >=& < v + w, v + w > \\ &+ i < v + iw, v + iw > \\ &+ -1 < v - w, v - w > \\ &+ -i < v - iw, v - iw > \end{aligned}$$

Theorem 23.13 (Cauchy Schwarz Inequality)

$$| < v, w > |^2 \leq ||v||^2 ||w||^2$$

§24 Lecture 03-11

§24.1 Inner product spaces

V over $F = \mathbb{R}, \mathbb{C}$.

1. Positivity:

$$\langle v, v \rangle \in \mathbb{R} \geq 0$$
$$\langle v, v \rangle = 0 \Leftrightarrow v = 0$$

2. Rather than imposing bilinearity, we were lead to impose hermition linearity.
3. Basic symmetry assumption requiring the $\langle v, w \rangle = \overline{\langle w, v \rangle}$.
4. We defined norm of v as

$$||v|| = \sqrt{\langle, v, v \rangle}$$

Theorem 24.1 (Cauchy-Schwartz Inequality)
For all $v, w \in V$,

$$|\langle v, w \rangle| \leq \|v\| \cdot \|w\|$$

With equal if $\operatorname{span}(v, w)$ is one dimensional

Proof. We can assume without loss of generality that $v \neq 0$.

Positivity implies that for all $\lambda \in F$,

$$\langle \lambda v + w, \lambda v + w \rangle \in \mathbb{R} \geq 0$$
$$= |\lambda|^2 \langle v, v \rangle + \lambda \langle v, w \rangle + \overline{\lambda} \langle w, v \rangle + \langle w, w, \rangle \geq 0$$
$$|\lambda|^2 \langle v, v, \rangle + 2Re(\lambda \langle v, w \rangle) + \langle w, w, \rangle \geq 0, \quad \forall \lambda \in F$$

1. If $F = \mathbb{R}$.

$$f(\lambda) = \lambda^2 \langle v, v \rangle + 2 \langle v, w \rangle \lambda + \langle w, w \rangle \geq 0, \quad \forall \lambda \in \mathbb{R}$$

This is a quadratic so either it has a root or it doesn't

$$\Rightarrow (2 \langle v, w \rangle)^2 - 4 \langle v, v, \rangle \langle w, w, \rangle \leq 0$$

with equal if there is a root

$$\Rightarrow \langle v, w \rangle^2 \leq \|v\|^2 \|w\|^2$$
$$\Rightarrow |\langle v, w \rangle| \leq \|v\| \|w\|$$

with equal if $\exists \lambda_0$ such that $f(\lambda) = 0$

i.e. $\langle \lambda_0 v + w, \lambda_0 v + w \rangle = 0 \Rightarrow \lambda_0 v + w = 0 \Rightarrow \operatorname{span}(v, w) = \operatorname{span}(v)$ ✓

2. If $F = \mathbb{C}$. Assume that $\lambda \langle v, w \rangle \in \mathbb{R}$.

$$|\lambda|^2 \langle v, v \rangle \pm 2|\lambda| |\langle v, w \rangle| + \langle w, w, \rangle \geq 0$$

Doesn't matter on the sign because b term squared in discriminant

$$4|\langle v, w \rangle|^2 - 4 \langle v, v \rangle \langle w, w \rangle \leq 0$$
$$\Rightarrow |\langle v, w \rangle|^2 \leq \|v\|^2 \|w\|^2$$

The rest follows like the real case.

□

§24.2 Properties of $\|v\|$

1.
$$\|v\| \in \mathbb{R} \geq 0$$

2.
$$\|\lambda v\| = |\lambda| \cdot \|v\|$$

3.
$$\|v + w\| \leq \|v\| + \|w\| \text{ with equality if } (v, w) \text{ are colinear.}$$

Proof.

1. By definition
2. $$\|\lambda v\| = \sqrt{\langle \lambda v, \lambda v \rangle} = \sqrt{\lambda\overline{\lambda}}\sqrt{\langle v, v \rangle} = |\lambda| \cdot \|v\|$$
3. $$\begin{gathered}\|v+w\|^2 = \langle v+w, v+w \rangle = \|v\|^2 + 2Re\langle v, w \rangle + \|w\|^2 \\ \leq \|v\|^2 + 2|\langle v, w \rangle| + \|w\|^2, \qquad \text{because } Re(\lambda) \leq |\lambda| \\ \leq \|v\|^2 + 2\|v\|\|w\| + \|w\|^2 = (\|v\| + \|w\|)^2 \\ \Rightarrow \|v+w\| \leq \|v\| + \|w\|\end{gathered}$$

□

Definition 24.2 (Orthogonality)**.** Two vectors are orthogonal if $\langle v, w \rangle = 0$.

Definition 24.3 (Orthonormal Basis)**.** An orthonormal basis of V is a basis Σ of V such that for all $v, w \in \Sigma$,

$$\langle v, w \rangle = \begin{cases} 0, & \text{if } v \neq w \\ 1, & \text{if } v = w \end{cases}$$

Example 24.4

1. $V = \mathbb{R}^n$ or $\mathbb{C}^n$ with dot product.

   $$e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, \ldots, 0),\ e_n = (0, 0, \ldots, 1)$$

   is an orthonormal basis.

2. $V = P_n([0,1])$, the space of polynomials of degree $\leq n$ with

   $$\langle f, g \rangle = \int_0^1 f(t)\overline{g(t)}dt$$

   Then

   $$\Sigma = (1, x, x^2, \ldots, x^n)$$

   is not an orthonormal basis because inner product is not zero pairwise between these elements

Theorem 24.5

If V is a finite-dimensional inner product space over $\mathbb{R}$ or $\mathbb{C}$, then it has an orthonormal basis.

Proof. We will prove something more precise. Let $(v_1, \dots, v_n)$ be a basis for V, then there is $(e_1, \dots, e_n)$ orthonormal with

$$\operatorname{span}(e_1, \dots, e_j) = \operatorname{span}(v_1, \dots, v_j), \quad j = 1, \dots, n$$

We will prove the existence of $(e_1, \dots, e_n)$ by induction on j.

1. Base case $j = 1$, let $e_1 = v_1/\|v_1\|$.
2. Inductive step $j \to j+1$. Assume that we have an orthonormal collection $e_1, \dots, e_j$ with $\operatorname{span}(e_1, \dots, e_j)$, with $\operatorname{span}(e_1, \dots, e_j) = \operatorname{span}(v_1, \dots, v_j)$. We then must define e_{j+1}.

   $$\widetilde{e_{j+1}} = \lambda_1 e_1 + \lambda_2 e_2 + \cdots + \lambda_i e_i + \lambda_{j+1} v_{j+1}$$

   Want $\widetilde{e_{j+1}} \perp e_i, \quad i = 1, \dots, j$.

   $$0 = \langle \widetilde{e_{j+1}}, e_i \rangle = \lambda_i + \lambda_{j+1} \langle v_{j+1}, e_i \rangle$$
   $$\lambda_i = -\lambda_{j+1} \langle v_{j+1}, e_i \rangle$$

   Set $\lambda_{j+1} = 1$, then $\lambda_i = -\langle v_{j+1}, e_i \rangle$.

   $$\widetilde{e_{j+1}} = v_{j+1} - \langle v_{j+1}, e_1 \rangle e_1 + \cdots + \langle v_{j+1}, e_j \rangle e_j$$

   is orthogonal to $e_1, \dots, e_j$ and hence $v_1, \dots, v_j$.

   $$e_{j+1} = \widetilde{e_{j+1}} \frac{1}{\|\widetilde{e_{j+1}}}$$

□