

Linear Algebra II

Felix Chen

Contents

0.1 Semisimple transformations	3
0.2 Bonus section	5
1 Inner product spaces	6
1.1 Inner product	6

Let's look at the subspaces V_i . We know that T_{V_i} is primary and cyclic, thus $f_i = p_i = (x - c_i)^{r_i}$. Let $N_i = T_{V_i} - \text{id}_{V_i}$, $f_{N_i} = p_{N_i} = x^{r_i}$. Let $\mathcal{B}_i = \{\alpha_i, N_i \alpha_i, \dots, N_i^{r_i-1} \alpha_i\}$, then $[N_i]_{\mathcal{B}_i} = C_{x^{r_i}} = J_{r_i}(0)$.

We can compute the Jordan canonical forms by computing the invariant factors first, and apply the primary decomposition to each factor to get the elementary divisors.

Example 0.0.1

Let $A = \begin{pmatrix} 2 & & \\ a & 2 & \\ b & c & -1 \end{pmatrix} \in \mathbb{C}^{3 \times 3}$.

First note that $f_A = (x - 2)^2(x + 1)$, then $p_A = (x - 2)^2(x + 1)$ or $(x - 2)(x + 1)$.

- If $p_A = (x - 2)^2(x + 1)$, then $p_1 = (x - 2)^2(x + 1)$, $q_{11} = (x - 2)^2$, $q_{12} = (x + 1)$.

Hence $A \sim \begin{pmatrix} 2 & & \\ 1 & 2 & \\ & & -1 \end{pmatrix}$.

- $p_A = (x - 2)(x + 1)$, then $p_1 = (x - 2)(x + 1)$, $p_2 = (x - 2)$. The elementary divisors are $x - 2, x - 2$ and $x + 1$.

Hence $A \sim \begin{pmatrix} 2 & & \\ & 2 & \\ & & -1 \end{pmatrix}$.

Since $p_A = (x - 2)(x + 1) \iff (A - 2I)(A + I) = 0$, i.e. $3a = ac = 0 \iff a = 0$.

Remark 0.0.2 — For generic matrix A , the Jordan canonical form can be derived from the *Smith canonical form* of $xI_n - A$.

The diagonal of Jordan canonical forms are the eigen values of T with *algebraic multiplicity*, and f_T, p_T can be easily written down from it. The number of Jordan blocks with eigenvalue c is equal to $\dim \ker(T - c \text{id})$, i.e. the *geometric multiplicity* of c .

Example 0.0.3

We'll compute the Jordan canonical form of $J_n(0)^2$. Since its characteristic polynomial is x^n , and $\dim \ker J_n(0)^2 = 2$, so it has two Jordan block with eigenvalue 0.

But note that $(J_n(0)^2)^m = 0$ iff $m \geq \frac{n}{2}$, thus the minimal polynomial is x^m , the sizes of the Jordan blocks are $\lfloor \frac{n}{2} \rfloor, \lceil \frac{n}{2} \rceil$.

Proposition 0.0.4

Let $n = \dim V$, TFAE:

- (1) T is nilpotent;
- (2) p_T is a power of x ;
- (3) $f_T = x^n$;
- (4) $T^n = 0$.

Proof. Trivial. □

The nilpotent matrices and diagonalizable matrices are somehow “independent”: If A is both nilpotent and diagonalizable, then $A = 0$.

In light of this idea, we present the following theorem:

Theorem 0.0.5 (Jordan decomposition)

Let $T \in L(V)$, $n = \dim V$, and F is algebraically closed. There exists unique $D, N \in L(V)$ s.t. $T = D + N$, where D diagonalizable and N nilpotent, and $DN = ND$.

Moreover there exists $f, g \in F[x]$ s.t. $D = f(T), N = g(T)$.

Proof. For $A \in F^{n \times n}$, $\exists P \in \text{GL}_n(F)$ s.t. $P^{-1}AP = J$, where J is a Jordan matrix.

It's clear that we can find $J_1 + J_2 = J$ with J_1 diagonal, J_2 nilpotent (just exactly as what you think), and we can check $J_1 J_2 = J_2 J_1$.

Hence $A = PJ_1P^{-1} + PJ_2P^{-1}$ has the desired properties. But now it's hard to prove the uniqueness, so we'll use another approach.

Let $p_T = \prod_{i=1}^k (x - c_i)^{r_i}$, and the elementary divisors $q_i = (x - c_i)^{r_i}$. Let $V_i = \ker(q_i(T))$, so $V = \bigoplus_{i=1}^k V_i$ is the primary decomposition of T .

Claim. $\exists f \in F[x]$ s.t. $f \equiv c_i \pmod{q_i}, i = 1, 2, \dots, k$.

(This follows from Chinese Remainder Theorem)

Observe that $f(T)|_{V_i} = c_i \text{id}_{V_i}$ in this case, thus $f(T)$ is diagonalizable. Since $(T - f(T))|_{V_i}$ is nilpotent, so $N = T - f(T)$ is nilpotent. This proves the existence part and the polynomial part.

Now it's easy to prove the uniqueness: If $T = D + N = D' + N'$, since D, N are polynomials of T , D and D' is commutative, hence can be simultaneously diagonalized.

Note that $D - D' = N - N'$ is both diagonalizable and nilpotent, thus it must be 0. (N, N' is commutative, so $(N + N')^{m+m'} = 0$, here $N^m = N'^{m'} = 0$) □

Since this theorem requires the field to be algebraically closed, if T is in a smaller field, we wonder whether D and N is in that field.

Let $A \in \mathbb{R}^{n \times n}$, and $A = D + N$ be its Jordan decomposition. We'll prove that $D, N \in \mathbb{R}^{n \times n}$. By taking conjugates,

$$A = D + N \implies A = \overline{D} + \overline{N}.$$

It's clear that $\overline{D} + \overline{N}$ is also a Jordan decomposition of A , so we must have $D = \overline{D}$, which means $D \in \mathbb{R}^{n \times n}$.

In fact when \mathbb{R} is replaced by any perfect field F , this property still holds. To prove this we need to introduce the semisimple maps.

§0.1 Semisimple transformations

As we've already seen, the "diagonalizable" property depends on the base fields, thus next we'll generalize the concepts of "diagonalizable".

Definition 0.1.1. Let $T \in L(V)$,

- We say T is **simple** (or irreducible) if V has no nontrivial T -invariant subspaces.
- We say T is **semisimple** (or totally reducible) if each T -invariant subspace $W \subset V$ there exists T -invariant subspace Z , s.t. $V = W \oplus Z$.

Obviously simple maps are always semisimple.

Proposition 0.1.2

Let T be a simple linear operator, then $\forall \alpha \in V \setminus \{0\}$, α is a cyclic vector of T .

Lemma 0.1.3

Let $T \in L(V)$.

- If T is semisimple, $V' \subset V$ is T -invariant, then $T_{V'}$ is semisimple.
- If $V = \bigoplus_{i=1}^k V_i$ s.t. T_{V_i} semisimple, then T is semisimple as well.

Proof. Suppose $W \subset V'$ is a T -invariant subspace. Since T is semisimple, $\exists Z \subset V$ s.t. $V = W \oplus Z$, and Z is T -invariant.

Let $Z' = Z \cap V'$, we claim that $V' = Z' \oplus W$.

Clearly $W \cap Z' = \{0\}$ and $W + Z' \subset V'$. For all $v \in V'$, $\exists w \in W, z \in Z$ s.t. $v = w + z$, since $v, w \in V'$, $z = v - w \in V'$ as well, which means $z \in Z'$.

For the second part, (We can assume $k = 2$, but here we won't use it).

Let $W \subset V$ be a T -invariant subspace. Since T_{V_i} is semisimple, $\exists Z_i \subset V_i$ s.t.

$$V_i = \left(\left(W + \sum_{j=1}^{i-1} V_j \right) \cap V_i \right) \oplus Z_i.$$

Let $Z = \bigoplus_{i=1}^k Z_i$, we claim that $Z \oplus W = V$. If $w \in W \cap Z$, then $w = z_1 + \dots + z_k$,

$$z_k = w - z_1 - \dots - z_{k-1} \in Z_k \cap (W + V_1 + \dots + V_{k-1}) = \{0\}.$$

Thus $z_k = 0$, similarly $z_{k-1} = \dots = z_1 = 0 = w$.

Note that $W + \sum_{i=1}^j V_i \subset W \oplus \sum_{i=1}^j Z_i$ for all $j = 1, \dots, k$, so $V = W \oplus Z$. □

Corollary 0.1.4

Let $T \in L(V)$, T is semisimple \iff there exists a T -invariant decomposition $V = \bigoplus_{i=1}^k V_i$ s.t. each T_{V_i} is simple.

Theorem 0.1.5

Let $T \in L(V)$.

- T simple $\iff f_T$ is a prime polynomial;
- T semisimple $\iff p_T$ has no multiple factors.

Proof. T simple $\implies T$ cyclic $\implies f_T = p_T$, so we only need to prove p_T is a prime.

Otherwise $p_T = gh$,

$$0 = p_T(T) = g(T)h(T),$$

So either $g(T)$ or $h(T)$ is not invertible. Thus $\ker(g(T)) \neq \{0\} \implies \ker(g(T)) = V \implies g(T) = 0$, contradiction!

If T is not simple, $\exists W \subset V$, W is T -invariant nontrivial subspace, so $f_T = f_{T_W} \cdot f_{T_{V/W}}$ is not a prime.

T semisimple $\implies \exists V_i, V = \bigoplus_{i=1}^k V_i$, such that T_{V_i} is simple $\implies p_{T_{V_i}}$ is prime.

$$p_T = \text{lcm}(p_{T_{V_1}}, \dots, p_{T_{V_k}})$$

has no multiple factors.

Conversely if p_T has no multiple factors, consider the primary cyclic decomposition of T :

$$V = \bigoplus_i W_i, \quad f_{T_{W_i}} \text{ primary.}$$

Since p has no multiple factors, $f_{T_{W_i}} = p_{T_{W_i}}$ is prime polynomial.

Hence T_{W_i} simple $\implies T$ semisimple. □

Corollary 0.1.6

When F is an algebraically closed field:

- T simple $\iff \dim V = 1$.
- T semisimple $\iff T$ is diagonalizable.

This corollary means that “semisimple” is indeed the equivalent description of “diagonalizable” in the algebraic closure.

Note that whether p_T has multiple factors or not does not change under *perfect* field extensions. So “semisimple” is a more general property (it stays the same under more transformations).

Recall that:

Definition 0.1.7 (Perfect fields). If for all prime polynomials $p \in F[x]$, p has no multiple roots in \bar{F} , we say F is a **perfect field**.

Finite fields, fields with character 0 and algebraically closed fields are always perfect fields.

We can check that when F is perfect, $f \in F[x]$ has no multiple factors iff f has no multiple factors in $\overline{F}[x]$.

Now we can generalize the Jordan decomposition:

Theorem 0.1.8 (Jordan decomposition)

Let $T \in L(V)$, $n = \dim V$, and F is perfect. There exists unique $S, N \in L(V)$ s.t. $T = S + N$, where S semisimple and N nilpotent, and $SN = NS$.

Moreover there exists $f, g \in F[x]$ s.t. $S = f(T), N = g(T)$.

To prove this generalized version, we need the following observation:

Proposition 0.1.9

Let F be a perfect field, $A \in F^{n \times n}$ is semisimple iff A is diagonalizable in $\overline{F}^{n \times n}$.

Proof. A semisimple $\iff p_A$ has no multiple factors in $F[x]$

$\iff p_A$ has no multiple roots in $\overline{F}[x]$

$\iff p_A$ is the product of different monic polynomials of degree 1

$\iff A$ is diagonalizable in $\overline{F}^{n \times n}$. □

Proposition 0.1.10

Let F be a perfect field, $a \in \overline{F}$. Then $a \notin F \iff$ exists an automorphism σ s.t. $\sigma|_F = \text{id}_F$, i.e. $\sigma \in \text{Gal}(\overline{F}/F)$ but $\sigma(a) \neq a$.

Remark 0.1.11 — This proof is beyond the scope of this class, but the idea is similar to the conjugate operation on \mathbb{C}/\mathbb{R} .

Now we prove the Jordan decomposition:

Proof. Let $A = S + N$ is the Jordan decomposition on $\overline{F}^{n \times n}$. Then by applying σ on this equation,

$$A = \sigma(S) + \sigma(N)$$

holds for all $\sigma \in \text{Gal}(\overline{F}/F)$. Since $\sigma(S)$ is also diagonalizable, $\sigma(N)$ is nilpotent, as σ is an automorphism. So by the uniqueness of Jordan decomposition, $\sigma(S) = S, \sigma(N) = N$.

This implies $S, N \in F^{n \times n}$. □

§0.2 Bonus section

Starting from Galois groups mentioned above, let

$$\text{Aut}(E/F) := \{\sigma \in \text{Aut}(E) \mid \sigma|_F = \text{id}_F\}$$

be the automorphism group of field extension E/F .

Example 0.2.1

Let $F = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{2})$, then $\sigma : a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is in $\text{Aut}(E/F)$.

If $E = \mathbb{Q}(\sqrt[3]{2})$, if $\sigma \in \text{Aut}(E/F)$, then $\sigma(\sqrt[3]{2})$ is a root of $x^3 - 2 \implies \sigma = \text{id}$. Thus E/F is not a *Galois extension*.

When E/F is a Galois extension, we write $\text{Gal}(E/F) = \text{Aut}(E/F)$.

In the history, this concept is used to solve polynomial equations.

Let $f \in \mathbb{Q}[x]$, let x_1, \dots, x_n be all roots of f . Consider $E = \mathbb{Q}(x_1, \dots, x_n)$, and define $\text{Gal}(f) = \text{Gal}(E/\mathbb{Q})$. Back in the times of Galois, the concept of field haven't been developed yet, so what he did is to consider the bijections between the roots of f .

Galois discovered that f has radical solutions if and only if the group $\text{Gal}(f)$ has a property, and he named it “solvable”. Since all the subgroups of S_4 are solvable, thus if $\deg f \leq 4$, f always has radical solutions, but $A_5 < S_5$ is not solvable, so polynomials of degree greater than 4 may not have radical solutions.

One of the ultimate goal of modern algebra is to comprehend the group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

A tool developed for this goal is *group representation*. A representation of a group G is a homomorphism $\varphi : G \rightarrow \text{GL}(V)$. Since $\text{GL}(V)$ is something people knows very well, so when the elements of an abstract group G is viewed as linear maps, it's easier to discover more properties of G .

When $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the representation is called a *Galois representation*. Even one dimensional Galois representations are very nontrivial.

Midterm exam QAQ

§1 Inner product spaces

In this section we always assume the base field to be \mathbb{R} or \mathbb{C} .

§1.1 Inner product

Definition 1.1.1 (Inner product). Let V be a vector space, an **inner product** on V is a function $\langle \cdot, \cdot \rangle : V \times V \rightarrow F$, $(\alpha, \beta) \mapsto \langle \alpha, \beta \rangle$ such that:

- $\langle \alpha + \beta, \gamma \rangle = \langle \alpha, \gamma \rangle + \langle \beta, \gamma \rangle$, $\langle c\alpha, \beta \rangle = c \langle \alpha, \beta \rangle$, i.e. the linearity of the first entry.
- $\langle \alpha, \beta \rangle = \overline{\langle \beta, \alpha \rangle}$. This implies the *conjugate linearity* of the second entry.
- $\alpha \neq 0 \implies \langle \alpha, \alpha \rangle > 0$.

Remark 1.1.2 — The reason why we require the conjugate property is that we want to make the inner product positive definite: otherwise $\langle i\alpha, i\alpha \rangle = i^2 \langle \alpha, \alpha \rangle$.

The finite dimensional real inner product space is called **Euclid space**, and finite dimensional complex inner product space is called **unitary space**.

In fact the definition of inner space is related to the order in real numbers, so this is not a pure algebraic structure.

Example 1.1.3

Let $V = F^{n \times 1}$. Let $\alpha = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \beta = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, define $\langle \alpha, \beta \rangle = \sum_{j=1}^n x_j \overline{y_j} = \alpha^t \overline{\beta}$ to be the **standard inner product**.

Denote $\beta^* = \overline{\beta}^t$, then $\langle \alpha, \beta \rangle = \beta^* \alpha$.

Similarly when $V = F^{m \times n}$, $\langle A, B \rangle = \sum_{j,k} A_{jk} \overline{B_{jk}} = \text{tr}(B^* A) = \text{tr}(AB^*)$.

Definition 1.1.4 (Hermite matrices). Let $A \in F^{n \times n}$, we say A is **Hermite** if $A^* = A$, and **anti-Hermite** if $A^* = -A$.

When $F = \mathbb{R}$, Hermite matrices are symmetrical matrices.

If we also have $\forall X \in F^{n \times 1} \setminus \{0\}, X^* A X > 0$, then we say A is **positive definite**.

Example 1.1.5

For all $Q \in \text{GL}_n(F)$, $A = Q^* Q$ is positive definite.

Proposition 1.1.6

Let V be an n dimensional vector space, let $\mathcal{B} = \{\alpha_1, \dots, \alpha_n\}$ be a basis. For $\alpha, \beta \in V$, let $X = [\alpha]_{\mathcal{B}}, Y = [\beta]_{\mathcal{B}}$.

- If $A \in F^{n \times n}$ is positive definite, then

$$\langle \alpha, \beta \rangle = Y^* A X = \sum_{j,k=1}^n A_{kj} x_j \overline{y_k}$$

is an inner product.

- For any inner product $\langle \cdot, \cdot \rangle$, there exists a unique positive definite matrix A such that the above relations holds.

Proof. It's clear that $Y^* A X$ is an inner product. (just check the definition)

For the latter part, let $A_{kj} = \langle \alpha_j, \alpha_k \rangle$, so A must be unique. By the conjugate linearity of inner product, so A constructed above indeed satisfies desired condition:

$$\langle \alpha, \beta \rangle = \left\langle \sum_{j=1}^n x_j \alpha_j, \sum_{k=1}^n y_k \alpha_k \right\rangle = \sum_{j,k=1}^n x_j \overline{y_k} \langle \alpha_j, \alpha_k \rangle$$

□

Let $T : V \rightarrow W$ be an injective linear map, and $\langle \cdot, \cdot \rangle_0$ is an inner product on W . Then T induces an inner product on V :

$$\langle \alpha, \beta \rangle = \langle T\alpha, T\beta \rangle_0, \quad \alpha, \beta \in V.$$

Since T injective, so T actually realizes V as a subspace of W , this inner product is just the original one restricted on the subspace.

Example 1.1.7

Let $V = W = F^{n \times 1}$, $\langle \cdot, \cdot \rangle_0$ is the standard inner product, $Q \in \text{GL}_n(F)$. Then

$$\langle \alpha, \beta \rangle = \langle Q\alpha, Q\beta \rangle_0 = \beta^*(Q^*Q)\alpha.$$

With an inner product, we can assign a “length” to each vector: $\|\alpha\| = \sqrt{\langle \alpha, \alpha \rangle}$. It’s clear that:

$$\|c\alpha\| = |c|\|\alpha\|, \quad \|\alpha\| > 0, \forall \alpha \neq 0.$$

Proposition 1.1.8 (Polarization identity)

When $F = \mathbb{R}$,

$$\langle \alpha, \beta \rangle = \frac{1}{4} (\|\alpha + \beta\|^2 - \|\alpha - \beta\|^2).$$

When $F = \mathbb{C}$,

$$\langle \alpha, \beta \rangle = \frac{1}{4} \sum_{k=1}^4 i^k \|\alpha + i^k \beta\|^2.$$

Remark 1.1.9 — This means, *inner product is totally determined by length function*.

Proposition 1.1.10 (Cauchy-Schwarz inequality)

$$|\langle \alpha, \beta \rangle| \leq \|\alpha\| \|\beta\|.$$

The equality holds iff α, β linearly dependent.

Proof. WLOG $\alpha, \beta \neq 0$. Let $\gamma = \beta - \frac{\langle \beta, \alpha \rangle}{\|\alpha\|^2} \alpha$ be the orthogonal projection of β on α^\perp .

We can check that $\langle \alpha, \gamma \rangle = 0$, so

$$0 \leq \|\gamma\|^2 = \langle \gamma, \beta \rangle = \|\beta\|^2 - \frac{\langle \alpha, \beta \rangle^2}{\|\alpha\|^2},$$

which gives the desired inequality, equality iff $\gamma = 0$ iff α, β linearly dependent. \square

Proposition 1.1.11 (Triangle inequality)

$$\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|.$$

Proof. Square both sides and use Cauchy-Schwarz. \square

This means our “length” function is in fact a **norm**.

Definition 1.1.12 (Orthogonality). Let $\alpha, \beta \in V$, we say $\alpha \perp \beta$ if $\langle \alpha, \beta \rangle = 0$.