Decomposing a vector space as direct sums of $f$-invariant subspaces

1. Polynomials over a field.

**Def.** A polynomial $p$ is called **irreducible** a unit if there is another polynomial $q$ with $p \cdot q = 1$.

($\Rightarrow$ Units are all polynomials of degree 0 (except the zero polynomial).

A polynomial is called **irreducible**, if it cannot be written as a product of two other polynomials (that are not units).

(Example: all polynomials of degree 1 are irreducible).

A polynomial $p$ is called **prime**, if whenever $p$ divides a product $a \cdot b$ of two polynomials, it has to divide one of the factors.

**Remark:** These notions make sense for general rings (like $\mathbb{Z}$). For polynomials over a field these "prime" and "irreducible" are the same.

**Then:** A polynomial can be uniquely factored as a product of irreducible polynomials (Of course the same irreducible factors might appear more than once in this factorization).

(Uniqueness: Up to reordering them, like $6 = 2 \cdot 3 = 3 \cdot 2$).
**Goal:** Decompose $V$ as a direct sum of $f$-invariant subspaces (as (until you cannot decompose these subspaces further).

**Theorem:** Let $p(t)$ be the characteristic polynomial of $f$.

Factor it as $p(t) = p_1(t)^{n_1} \cdots p_n(t)^{n_n}$ where each $p_i(t)$ is irreducible.

Then, $V$ is a direct sum of all the $f$-invariant subspaces $N(p_i(t)^{i_i})$, $i = 1, \ldots, n$.

The proof follows from the following lemma:

**Lemma:** If $p(t)$ is the characteristic polynomial of $f$, then we write it as a product of two coprime polynomials, say $p(t) = q(t)r(t)$, then $V$ is the direct sum of $N(q(t))$ and $N(r(t))$.

**Proof:** Let $v \in V$ be an arbitrary vector.

Claim 1: $q(t)(v) \in N(r(t))$ (and analogously $r(t)(v) \in N(q(t))$).

Proof: $r(t)(q(t)) (v) = (r \cdot q)(t)(v) = p(t)(v) = 0$

Claim 2: There exist polynomials $a(t)$, $b(t)$ with

$$1 = a(t)q(t) + b(t)r(t)$$

(This follows from the Euclidean Algorithm & the assumption that $q$ and $r$ are coprime.)
Claim (3): \( N(q(f)) \) and \( N(v(f)) \) are \( f \)-invariant.

To show: \( \forall v \in N(q(f)) \implies f(v) \in N(q(f)) \)

\[ \iff \forall v \in N(q(f)) \implies f(q(f)(v)) = 0 \]

\[ = q(f) \circ f \mid v = f \left( \frac{q(f)(v)}{\|v\|} \right) = 0 \quad \forall v \]

Claim (4): The restriction of \( r(f) \) to \( N(q(f)) \) is invertible.

\[ I = a(f) \cdot q(f) + b(f) \cdot r(f) \quad \text{Plug in } f \]

\[ id = a(f) \cdot q(f) + b(f) \cdot r(f) \quad \text{Plug in } \nu \]

\[ \nu = a(f) \left( q(f)(\nu) \right) + b(f) \left( r(f)(\nu) \right) \]

\[ = 0 \quad \text{The inverse that we are looking for.} \]

Claim (5): We have \( \forall v \in V \) can be written as a sum \( v = v_q + v_r \) with \( v_q \in N(q(f)) \) and \( v_r \in N(v(f)) \).

\[ v = q(f) \left( a(f)(v) \right) + r(f) \left( b(f)(v) \right) \]

\[ \in N(v(f)) \quad \subseteq V_q \]

\[ \in N(q(f)) \quad \subseteq V_r \]

Claim (6): \( N(q(f)) \cap N(v(f)) = 0 \). Let \( v \) be in this intersection.

\[ v = a(f) \left( q(f)(v) \right) + b(f) \left( v(f)(v) \right) = 0 \]

\[ = 0 \]

\[ = 0 \]
Maps whose characteristic polynomial is a power of an irreducible polynomial.

Special case: \( f : V \to V \). Suppose the characteristic polynomial of \( f \) is irreducible (say \( a_n x^n + \ldots + a_0 \)).

Pick \( v \in V \), \( v \neq 0 \). Then we obtain a basis for the smallest \( f \)-invariant subspace containing \( v \) by as follows:

\[ v, f(v), f^2(v), \ldots, f^{n-1}(v). \]

The matrix of \( f \) w.r.t. this basis is

\[
\begin{pmatrix}
0 & \cdots & 0 & -a_0 \\
0 & \ddots & \vdots & \vdots \\
0 & \cdots & 0 & -a_{n-1} \\
0 & \cdots & 1 & -a_n
\end{pmatrix}
\]

\( \Rightarrow \) If the \( A \), suppose \( A, A' \) have the same irreducible characteristic polynomial. Then there is a \( B \) with \( BAB^{-1} = A' \).

Does this also hold for non-irreducible char. polynomials?

Example: \( A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad A' = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \)

\( A \) and \( A' \) have the same char. polynomial \( t^4 \) and the same rank. Can there be such a \( B \) as above?

No! look at \( A^2 = 0 \), \( A^2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \neq 0 \).
Prop: Let $f: V \to V$ be a linear map and suppose the characteristic polynomial of $A$ is a power of an irreducible polynomial, say $p(t)^m$. Then we can look at the numbers

$$\dim \left( N\left( p(A) \right) \right) \text{ for } i = 1, \ldots, m.$$ 

Then $A$ and $A'$ are conjugate, if those sequence of numbers again.

Example:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad p(t) = t^2 \quad \Rightarrow \quad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 4 & 4 & 4 \end{array} \quad m = 4$$

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad p(t) = t^3 \quad \Rightarrow \quad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 4 \end{array} \quad m = 4$$

$\Rightarrow$ not conjugate.

To prove this proposition, we start with a map $f: V \to V$ and we will construct a basis for $V$ such that the matrix of $f$ w.r.t. this basis only depends on those numbers.
Finding bases such that the matrix of $f$ has Jordan Normal Form

Recall: $f: V \rightarrow V$ linear, char poly of $f$ is assumed to be a product of linear factors $(t - a_1)(t - a_2)\ldots(t - a_n)$

$N(a_1(t)), \ldots, N(a_n(t))$

So if we choose bases for all those subspaces and take the union of those bases, we get a basis for $V$ s.t. the matrix of $f$ has block form

$\begin{pmatrix} A_1 & \mathbf{0} \\ \mathbf{0} & A_n \end{pmatrix}$

and each $A_i$ is a block whose characteristic polynomial is $q_i(t^a)$ (a power of an irreducible polynomial). We can improve the bases of those blocks separately.

Assume $f: V \rightarrow V$ linear, char poly $= \prod q_i(t)^{a_i}$ where $q_i$ is irreducible.

Recall: Dot Diagram: $\tilde{A}^2 = A - 2I$

Now we have to choose a basis of $V$.

(\text{Note: V is 8-dim.}) so we have to choose a basis vector for each dot.

$\text{Ker}(A), \text{Ker}(A^2), \text{Ker}(A^3)$

Here $= V$

Look at the last column first. We have $\dim(N(A^2)) = 6, \dim(V) = 8$.

Choose 2 vectors that extend a/some basis of $N(A^2)$ to a basis of $V$, say $v_1, v_2$.

If $\lambda_1 v_1 + \lambda_2 v_2 \in N(A^2)$, then $\lambda_1 = \lambda_2 = 0$.

Look at $\tilde{A}v_1, \tilde{A}v_2 \in N(A)$ and we have:

$\lambda_1 \tilde{A}v_1 + \lambda_2 \tilde{A}v_2 \in N(A) \Rightarrow \lambda_1 v_1 + \lambda_2 v_2 \in N(A^2) \Rightarrow \lambda_1 = \lambda_2 = 0$.

$\Rightarrow \tilde{A}v_1, \tilde{A}v_2$ are still lin. indep.)
Repeat this. This gives us 6 of 8 basis vectors.

\[ \tilde{A}v_1, \tilde{A}v_2, v_1, v_2 \]

\[ \tilde{A}v_2, \tilde{A}v_2, v_2 \]

\[ \tilde{A}v_2, \tilde{A}v_2, v_2 \]

Now we have to choose this one.

Find a vector \( v_3 \in \text{null}(\tilde{A}^2) \) such that if we take a basis of \( \text{null}(\tilde{A}^2) \), and we take the vectors \( \tilde{A}v_1, \tilde{A}v_2, v_3 \), we get a basis of \( \text{null}(\tilde{A}^2) \).

\[ \tilde{A}v_1, \tilde{A}v_2, v_1, v_2 \]

Repeat...

\[ \tilde{A}v_2, \tilde{A}v_2, v_2 \]

\[ \tilde{A}v_3, v_3 \]

\[ \text{Example: } A = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 3 & 1 \\ 0 & 0 & 1 \end{pmatrix} \]

\[ \text{Char Poly: } \det \begin{pmatrix} 1-t & 1 & 1 \\ -1 & 3-t & 1 \\ 0 & 0 & 1-z-t \end{pmatrix} \]

\[ = (1-z-t)^2 (1-t)(3-t)+1 (2-t) \]

\[ = (t^2 - 4t + 4)(2-t) = (2-t)^2 \]

\[ = (t^2 - 4t + 4)(2-t) = (t-2)^2 \]

\[ \tilde{A} = -2I_3 + A = \begin{pmatrix} -1 & 1 & 1 \\ -1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \]

\[ \tilde{A}^2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \]

\[ \dim \text{null}(\tilde{A}^2) = 2 \]

\[ \text{Dot - Diagonal: } \]

\[ \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \]
Pick a vector \( y \) that would complete a basis of \( U(\tilde{A}) \) to a basis of \( \mathbb{R}^3 \) (i.e. a vector that is not in \( U(\tilde{A}) \)), say \( \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \).

\[ \tilde{A} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \rightarrow \quad \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \]

Pick a vector \( z \) in \( U(\tilde{A}) \) such that \( \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \) is a basis of \( U(\tilde{A}) \).

\[ \text{e.g. } z = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \]

The basis \( \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \} \) is a basis such that \( \tilde{A} \) has JNF w.r.t. that basis is \( \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \)

\[ \text{Check: } \]
\[ \tilde{A} \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ 0 \end{pmatrix} = 2 \cdot \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} \]
\[ \tilde{A} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix} = 2 \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} + (1) \cdot \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix} \]
\[ \tilde{A} \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ -2 \end{pmatrix} = 2 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \]

The matrix w.r.t. this basis is
\[ \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \\ 2 \\ 0 \\ 0 \\ 0 \\ 2 \end{pmatrix} \text{ JNF } \]