The theory of a single linear transformation.

1 Invariant subspaces.

Many problems in mathematics and applied mathematics naturally lead to a consideration of a finite dimensional vector space V and a linear transformation $T : V \longrightarrow V$. It is then of considerable importance to understand such T as well as possible. For example, we would like to know a behavior of a given vector v under iterations of T, i.e. we would like to understand the sequence $v, T(v), T(T(v)) = T^2(v), T(T^2(v)) = T^3(v), ...$ We would like to know for which v this sequence is bounded, tends to 0 or tends to infinity, what is the rate of growth of this sequence, etc..

As an illustration, let us consider the following simple example. Suppose that we have a particle which can be at two different states 1 and 2. Every second the particle in state i can change to the other state j with probability $p_{i,j}$ or it can stay at the state i with probability $p_{i,i} = 1 - p_{i,j}$. We would like to know the probability that a particle originally in state i is in state j after n seconds. It is a nice exercise to see that the answer is given in terms of the 2×2 matrix $P = (p_{i,j})$. Namely the desired probability is simply the (i, j) entry of the matrix P^n. We will show how linear algebra can be employed to get a good understanding of powers of P.

To make things more concrete, suppose that $p_{1,1} = 1/3$ and $p_{2,2} = 1/2$ so that the matrix P is $\left(\begin{smallmatrix} 1/3 & 2/3 \\ 1/2 & 1/2 \end{smallmatrix}\right)$. We consider P as the matrix representation of a linear transformation T from $\mathbb{R}^2$ to itself in the standard basis $\mathbf{e} = \{e_1, e_2\}$. Thus $T(x, y) = ((x + 2y)/3, (x + y)/2)$. Consider now another basis $\mathbf{v} = \{v_1, v_2\}$ for $\mathbb{R}^2$, where $v_1 = (1, 1)$ and $v_2 = (-4, 3)$. It is easy to see that $T(v_1) = v_1$ and $T(v_2) = (-1/6)v_2$. Thus the matrix representation B of T in the basis $\mathbf{v}$ is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1/6 \end{smallmatrix}\right)$. Let C be the transition matrix from the basis $\mathbf{e}$ to the basis $\mathbf{v}$. Then $A = C^{-1}BC$. The matrix C^{-1} is easy to find: it is the transition matrix from $\mathbf{v}$ to $\mathbf{e}$ so it equals $\left(\begin{smallmatrix} 1 & -4 \\ 1 & 3 \end{smallmatrix}\right)$. Now C is the inverse of C^{-1}, so it equals $\left(\begin{smallmatrix} 3/7 & 4/7 \\ -1/7 & 1/7 \end{smallmatrix}\right)$. The final observation is that $A^n = (C^{-1}BC)^n = C^{-1}B^nC$. But it is very easy to compute B^n, namely B^n equals $\left(\begin{smallmatrix} 1 & 0 \\ 0 & (-1/6)^n \end{smallmatrix}\right)$. This leads to a formula for A^n:

$$A^n = \left(\begin{smallmatrix} 3/7+4/7(-1/6)^n & 4/7-4/7(-1/6)^n \\ 3/7-3/7(-1/6)^n & 4/7+3/7(-1/6)^n \end{smallmatrix}\right).$$

Note that for n very large the probability that the particle ends up in state

1 practically does not depend on where it started and is about 3/7. The probability that the particle ends up in state 2 is about 4/7.

Exercise. Solve the above problem in general.
Hint. The cases when both $p_{1,1}$ and $p_{2,2}$ are 0 or both are 1 requires separate treatment, but is easy. All other cases are handled by the same method as in our example. Consider the basis $\mathbf{v} = v_1, v_2$ where $v_1 = (1, 1)$ and $v_2 = (-p_{1,2}, p_{2,1})$.

It is clear that the heart of the method used in the above example is the existence of a basis in which the transformation T has particularly simple matrix representation. It is our goal in this chapter to investigate the possibility of finding such convenient basis for arbitrary operators. Thus we need to find out what a convenient basis should be and how to find such a basis.

In order to achieve our goal we start with a short discussion of the notion of direct sum of vector spaces. Recall that given two vector spaces U, W we can construct a new vector space, $V = U \oplus W$, called the direct sum of U and W, which consists of all pairs (u, w) of vectors $u \in U$ and $w \in W$. So the direct sum is a way of building a large vector space from smaller. But in practice we would like to proceed in the opposite direction: we have a vector space which we would like to investigate and one way to do so is to try to decompose it into a direct sum of smaller subspaces.

It is easy to see that if V is a vector space and U is its subspace then there is always a subspace W such that $U \oplus W = V$ (but it is by no means unique). In fact, it is enough to choose a basis for U and complete it to a basis of V by adding $w_1, w_2, ...$ The span W of the vectors $w_1, ...$ has the required property.

So we see that it is not a big deal to decompose a vector space into a direct sum of smaller vector spaces. But recall that our goal is not the vector space itself, but the vector space together with a linear transformation on it. Note first that given linear transformation $T_U : U \longrightarrow U$ and $T_W : W \longrightarrow W$ we can define a linear transformation $T : U \oplus W \longrightarrow U \oplus W$ by $T(u, w) = (T_U(u), T_W(w))$. So again, our idea is to proceed in the opposite direction: given a vector space V and a liner transformation T on it, can we decompose V into a direct sum $V = U \oplus W$ such that T maps U into U and W into W? Note that if this is possible, then the study of T reduces to a study of the restrictions T_U of T to U and T_W of T to W. In particular, if we choose a basis $\mathbf{u}$ of U and a basis $\mathbf{w}$ of W then the sequence $\mathbf{v}$ consisting of

vectors in $\mathbf{u}$ followed by the vectors in $\mathbf{w}$ is an ordered basis of V and in this basis the matrix representation of T looks like $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$, where A is the matrix representation of T_U in the basis $\mathbf{u}$, and B is the matrix representation of T_W in the basis $\mathbf{w}$.

In order to answer our question it seems natural to investigate first subspaces U of V which are preserved by T, i.e. such that T maps U into U, and then try to decide which of them can be completed by another such subspace W to a direct sum decomposition of V. This leads to the following

Definition 1. *Let V be a vector space and $T \in L(V,V)$ a linear transformation. A subspace U of V is called* $T-$**invariant** *(or just invariant, if it is clear what transformation it refers to), if $T(U) \subseteq U$, i.e. if T maps U into itself.*

From now on we assume that our vector spaces are finite dimensional. Suppose that U is a $T-$invariant subspace of V. If $v \in U$, then also $T(v) \in U$, so also $T(T(v)) \in U$ and $T(T(T(v))) \in U$, ... In what follows we will often consider compositions of T with itself (called **iterations** of T). We will write T^n for the composition of T with itself $n-$times. Note that the operation $T \mapsto T^n$ has all formal properties of raising to $n-$th power, and if we recall that $L(V,V)$ with addition and composition is a ring, then it should become clear that this is exactly the operation of raising to $n-$th power in the ring $L(V,V)$. For convenience we define T^0 to be the identity operator.

Thus, U contains the vectors $v = T^0(v), T(v), T^2(v), T^3(v), ...$, so it contains the subspaces spanned by this vectors. We denote this subspace by $< v >$ and we call it the **cyclic subspace generated by** v. It is easy to see that $< v >$ itself is a $T-$invariant subspace, i.e. we have

Lemma 1. *Let $T \in L(V,V)$ be a linear transformation and $v \in V$. The cyclic subspace $< v >$ generated by v is $T-$invariant and it is the smallest $T-$invariant subspace which contains the vector v.*

Proof: The proof is nearly obvious. Any element u of $< v >$ looks like $u = a_0 v + a_1 T(v) + a_2 T^2(v) + ... + a_k T^k(v)$ for some k and some scalars a_i. Now $T(u) = a_0 T(v) + a_1 T^2(v) + ... + a_k T^{k+1}(v)$ so $T(u)$ clearly belongs to $< v >$. Thus $< v >$ is $T-$invariant. Since we have seen that any $T-$invariant subspace which contains v contains also $< v >$, we see that $< v >$ is the smallest $T-$invariant subspace containing v. $\square$

The next step is to get some idea about the dimension of $< v >$. Since the case when $v = 0$ is trivial, we assume from now on that $v \neq 0$. Since $< v >$ is finite dimensional, the vectors $v, T(v), T^2(v), ...$ can not be linearly independent. Let k be largest such that $v, T(v), ..., T^{k-1}(v)$ are linearly independent. Thus there are scalars $b_0, ..., b_k$ such that $b_0 T^0(v) + ... + b_k T^k(v) = 0$. Note that $b_k \neq 0$, otherwise the vectors $v, T(v), ..., T^{k-1}(v)$ would be dependent. Thus, setting $a_i = -b_i/b_k$ we see that

$$T^k(v) = a_0 T^0(v) + ... + a_{k-1} T^{k-1}(v) \qquad (*)$$

We claim that $v, T(v), ..., T^{k-1}(v)$ is a basis of $< v >$. Since these vectors are linearly independent, we just need to show that they span $< v >$. Let U be the subspace of $< v >$ spanned by $v, T(v), ..., T^{k-1}(v)$. It is enough to show that $T^n(v) \in U$ for all n, since $< v >$ is spanned by such vectors. Suppose that n is smallest such that $T^n(v) \notin U$. Clearly $n > k$, so we may apply T^{n-k} to both sides of $(*)$ to get

$$T^n(v) = a_0 T^{n-k}(v) + ... + a_{k-1} T^{n-1}(v).$$

But the right hand side is clearly contained in U by minimality of n, which contradicts our assumption that $T^n(v)$ is not in U. This shows that all the vectors $T^m(v)$ are in U so $U =< v >$. Thus we showed the following:

Theorem 1. *Let $T \in L(V, V)$ and let $v \in V$. There exists largest integer k such that the vectors $v, T(v), ..., T^{k-1}(v)$ are linearly independent. Then $k = dim(< v >)$ and the vectors $v, T(v), ..., T^{k-1}(v)$ form a basis of $< v >$. Moreover, there exist unique scalars $a_0, ..., a_{k-1}$ such that*

$$T^k(v) = a_0 T^0(v) + ... + a_{k-1} T^{k-1}(v) \qquad (*).$$

Before we proceed note that, given T and v, it is not hard to compute k and the scalars $a_0, ..., a_{k-1}$. In fact, if V has dimension n then clearly $k \leq n$ so that k is the dimension of the subspace spanned by $v, T(v), ..., T^{n-1}(v)$. Knowing k, the problem of finding the scalars a_i translates into a system of n linear equations with k unknowns, and we know how to solve such systems.

Algorithm In order to describe an explicit algorithm, we choose a basis of V and represent each vector $T^i(v)$, $i = 0, 1, ..., n$, as an $n-$tuple of its coordinates in this basis. Let A be the matrix whose $i-$th column is the vector of coordinates of $T^i(v)$. Using elementary row operations transform

this matrix into a reduced row-echelon form B. It is now easy to read the rank k of B, which is the dimension of $< v >$. The scalars $a_0, ..., a_{k-1}$ form $k+1$st column of B.

Example. Let $V = \mathbb{P}_3(\mathbb{R})$ be the space of polynomials of degree ≤ 3 and let T be given by $T(f) = xf'$. We want to find the dimension of $< v >$ and the a_i's for $v = 1 + x + x^2 + x^3$. We perform computations in the standard basis $1, x, x^2, x^3$. First note that $T(v) = x + 2x^2 + 3x^3$, $T^2(v) = x + 4x^2 + 9x^3$, $T^3(v) = x + 8x^2 + 27x^3$ and $T^4(x) = x + 16x^2 + 81x^3$. Thus the matrix A equals

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 3 & 9 & 27 & 81 \end{pmatrix}$$

The reduced row-echelon form B of A is the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & -11 \\ 0 & 0 & 0 & 1 & 6 \end{pmatrix}$$

We see that the rank k of B is 4. From the fifth column of B we get that $a_0 = 0$, $a_1 = 6$, $a_2 = -11$, $a_3 = 6$.

Let us return to our investigation. The equality $T^k(v) = a_0T^0(v) + ... + a_{k-1}T^{k-1}(v)$ can be interpreted as follows: v is in the kernel of the linear transformation $T^k - a_{k-1}T^{k-1} - ... - a_1T - a_0T^0$. This operator looks like a "polynomial in T". Since such operators will be crucial in our investigation, we have to find a convenient way of handling them, and it turns out that it may be achieved by making our analogy with polynomials more precise. First we recall basic facts about polynomials over fields, which will provide us with necessary tools to make further progress in an efficient and clear way.

2 Review of polynomials

Let us recall some basic properties of polynomials. We denote the set of polynomials with coefficients in a field F by $F[x]$. This set is equipped with addition and multiplication. Recall that in order to multiply $p(x) =$

$a_0 + a_1 x + ... + a_m x^m$ by $q(x) = b_0 + b_1 x + ... + b_n x^n$ we multiply each term of p by each term of q and combine all resulting terms with the same power of x. Explicitly, the polynomial $p(x)q(x)$ equals $c_0 + c_1 x + ... + c_{m+n} x^{m+n}$ where

$$c_i = a_0 b_i + a_1 b_{i-1} + ... + a_i b_0$$

(in this formula we set $a_j = 0$ for $j > m$ and $b_j = 0$ for $j > n$). It is well known and easy that the addition and multiplication of polynomials satisfy all basic properties required of addition and multiplication in a commutative ring: both are associative, commutative and have neutral elements (i.e. 0 for addition and 1 for multiplication), every polynomial p has an additive inverse (namely $-p$), and addition is distributive with respect to multiplication.

To each polynomial p we associate its **degree** defined as the largest integer n such that x^n occurs in p with a non-zero coefficient. The degree of p is usually denoted by $deg(p)$. The reader should note that our definition of degree does not apply to the zero polynomial (all powers of x have coefficient 0). It is customary to define the degree of 0 to be $-\infty$. With this convention we see that for any two polynomials p, q the formula $deg(pq) = deg(p) + deg(q)$ holds, provided we agree that $-\infty + a = -\infty$ for any a (without this convention we would always have to distinguish cases when some polynomials are 0, which is very inconvenient).

We define **the leading coefficient** of p as the coefficient at the highest power of x which occurs in p with non-zero coefficient if $p \neq 0$ and the leading coefficient of 0 is defined to be 0 . It is easy to see that the leading coefficient of the product of two polynomials is the product of leading coefficients.

Definition 2. *We say that a polynomial p is* **monic**, *if its leading coefficient equals 1.*

Since we can multiply polynomials, it makes sense to speak about divisibility of polynomials. More precisely, we have the following

Definition 3. *We say that a non-zero polynomial p divides a polynomial q and write $p|q$ if there is a polynomial h such that $q = ph$.*

The divisibility theory of polynomials is very interesting and is quite similar to the divisibility theory of integers. The analog of a prime number is the notion of an **irreducible polynomial**, defined as follows:

Definition 4. *A polynomial p is called* **irreducible** *if it is not constant and it can not be expressed as a product of two polynomials of positive degrees (or, equivalently, of degrees smaller than $deg(p)$).*

For example, $x+1$ is irreducible over any field. The polynomial x^2+1 is irreducible in $\mathbb{R}[x]$, but it becomes reducible in $\mathbb{C}[x]$, since $x^2+1=(x+i)(x-i)$.

It is a trivial consequence of Definition 4 that p is irreducible iff for any q such that $q|p$ we have that either q is constant or it is a constant multiple of p. In particular, if p,q are both monic then either $q=1$ or $q=p$.

It is easy to see that every non-constant polynomial g can be written as a product of irreducible polynomials. In fact, this follows from the simple fact that any non-constant divisor of g of lowest possible degree is irreducible (if not, we would get divisors of lower degree), so we can successively extract irreducible factors and after a finite number of steps we get factorization of g into irreducible factors. In such factorization we can always assume that all irreducible polynomials are monic by simply extracting the leading coefficient first. It can be proved that such decomposition into monic irreducible polynomials (and a constant) is unique up to order of factors. It should be mentioned that even though we know that each polynomial can be written as a product of irreducible elements, there is in general no algorithm which would allow to find such decomposition. Such algorithms exist if the field of coefficients is finite or is the field of rational numbers. But for two very important fields, namely $\mathbb{R}$ and $\mathbb{C}$, no such algorithm exists.

Now we describe the main fact about polynomials which will be used in our investigation and which also implies rather easily all the basic properties of divisibility theory of polynomials, for example the above mentioned uniqueness of decomposition into irreducible factors.

First we introduce the following

Definition 5. *A non-empty subset of $F[x]$ is called* **ideal**, *provided it has the following properties:*

— for any f,g in I also $f+g\in I$, i.e. I is closed under addition;

— for any f in I and any polynomial p also $pf\in I$, i.e. I is closed under multiplication by <u>any</u> polynomial from $F[x]$.

If I contains <u>non</u>-zero elements then by $d(I)$ we denote the smallest possible degree of a non-zero polynomial in I.

The main example of ideals is given by the following

Example. Fix a non-zero polynomial p. The set I of all polynomials divisible by p is an ideal. In fact, it is obvious that if $p|f$ and $p|g$ then $p|(f+g)$ and

$p|fh$ for any polynomial h. We denote this ideal by (p). It is clear that $d((p)) = deg(p)$.

The main result about polynomials says that every ideal is of the form described in the Example. More precisely, we have the following

Theorem 2. *Let I be an ideal and assume that I contains non-zero polynomials. Then there is unique monic polynomial p in I of degree $d(I)$ and I consists exactly of all multiples of p, i.e. $I = (p)$.*

Proof: By definition, there is a polynomial in I of degree $d = d(I)$. By dividing it by its leading coefficient we can assume that it is monic. Call it p. If p_1 is another monic polynomial of degree d in I then the difference $p - p_1$ is in I and has degree smaller than d. By the definition of $d = d(I)$ we see that $p - p_1 = 0$, i.e. $p = p_1$. This shows the uniqueness of p. To see that $I = (p)$ note that the inclusion $(p) \subseteq I$ is clear since $p \in I$ and I is closed under multiplication by arbitrary polynomials. Suppose that there are polynomials in I which do not belong to (p) (i.e are not divisible by p), and let f be such polynomial of lowest possible degree. Set $n = deg(f)$ so $n \geq d$ and $f(x) = c_n x^n + ... + c_0$. Now the polynomial $h(x) = f(x) - a_n x^{n-d} p(x)$ is clearly in I and it has degree smaller than n (the terms of degree n cancel out). Thus $h(x) \in (p)$ by the definition of n. But $f(x) = h(x) + a_n x^{n-d} p(x)$ and both $h(x)$, $a_n x^{n-d} p(x)$ are in (p), so also f is in (p), which contradicts our assumption that $f \notin (p)$. The contradiction shows that no such f exists, i.e. that $I = (p)$. $\square$

The last theorem gives us a very powerful tool, but we need to learn how to use it. As a first illustration let us prove the following fundamental result

Theorem 3. *Let p ba an irreducible polynomial and suppose that $p|fg$. Then either $p|f$ or $p|g$.*

Proof: Let $I = \{h : p|fh\}$ be the set of all polynomials h such that p divides fh. Clearly both p and g belong to I, so I contains non-zero polynomials. It is clear that I is an ideal (verify it). Thus there is a monic polynomial q in I such that $I = (q)$. In particular, $q|g$ and $q|p$. Since p is irreducible and both p, q are monic, we see that either $q = 1$ or $q = p$. In the former case we have $p|f \cdot 1 = f$ and in the latter case $q = p|g$. $\square$

Let us note the following useful fact

Lemma 2. *Let f be a non-zero polynomial and p an irreducible polynomial. Then there are unique integer $n \geq 0$ and polynomial g not divisible by p such that $f = p^n g$.*

Proof: If p does not divide f then we have no choice: we need to take $n = 0$ and $g = f$. Suppose that p divides f and let n be the largest integer such that p^n divides f. Thus $f = p^n g$ for some polynomial g which then can not be divisible by p. This proves the existence of g and n. To see uniqueness let $f = p^m g_1$ for some m and polynomial g_1 not divisible by p. Clearly $m \leq n$ and we have $p^m(g_1 - p^{n-m}g) = 0$, so $g_1 = p^{n-m}g$. Since g_1 is not divisible by p, we have $m = n$ and $g_1 = g$. $\square$

3 Back to linear transformations

Let us return to the main theme of this section. We want to make more precise our observation that $T^k - a_{k-1}T^{k-1} - ... - a_0$ looks like a polynomial in T.

Let $T \in L(V, V)$ be a linear operator. For any polynomial $p = b_0 + b_1 x + ...b_m x^m \in F[x]$ we define the operator $p(T)$ by $p(T) = b_0 I + b_1 T + ... + b_m T^m$, i.e. we substitute T for x in p. It is clear that for any 2 polynomials p, q we have $(p + q)(T) = p(T) + q(T)$. Almost as obvious is the fact that $(pq)(T) = p(T)q(T)$. Let us justify the last property. We have $pq = b_0 q + b_1 xq + ... + b_m x^m q$, so $(pq)(T) = (b_0 q)(T) + (b_1 xq)(T) + ... + (b_m x^m q)(T)$ and also $p(T)q(T) = b_0 q(T) + b_1 Tq(T) + ... + b_m T^m q(T)$. Thus, it is enough to show that for every j we have $(b_j x^j q)(T) = b_j T^j q(T)$. Now write $q(x) = c_0 + c_1 x + ... + c_l x^l$. Then $(b_j x^j q)(T) = b_j c_0 T^j + b_j c_1 T^{j+1} + ... + b_j c_l T^{j+l}$ and $b_j T^j q(T) = b_j T^j (c_0 T^0 + c_1 T + ... + c_l T^l) = b_j c_0 T^j + b_j c_1 T^{j+1} + ... + b_j c_l T^{j+l}$. Thus our property is established. Since multiplication of polynomials is commutative, we conclude that for any polynomials p, q the linear transformations $p(T)$ and $q(T)$ commute, i.e. $p(T)q(T) = q(T)p(T)$.

Similarly, if A is an $n \times n$ matrix then we define the matrix $p(A)$ by $p(A) = b_0 I + b_1 A + ... + b_m A^m$. It is clear that the above discussion applies also to this situation. Moreover, if $\mathbf{v}$ is an ordered basis of V and A is the matrix representation of T in the basis $\mathbf{v}$, then the matrix representation of $p(T)$ in the same basis equals $p(A)$.

Now we can characterize the scalars $a_0, ..., a_{k-1}$ in Theorem 1 in terms of polynomials. First we introduce the following

Definition 6. *Let $T \in L(V, V)$ and $v \in V$. The* **annihilator** *of the vector v with respect to T is the polynomial $p_v(x) = x^k - a_{k-1}x^{k-1} - ... - a_0$, where $a_0, ..., a_{k-1}$ are defined in Theorem 1.*

We have seen that $p_v(T)(v) = 0$ (i.e. $p_v(T)$ annihilates v). We will see in a moment that any other polynomial q such that $q(T)(v) = 0$ is divisible by p_v. This follows from the following more general fact:

Proposition 1. *Let U be a proper $T-$invariant subspace of V (proper means that $U \neq V$) and let $v \notin U$. The set I of all polynomials f such that $f(T)(v) \in U$ is an ideal. In particular, there exists unique monic polynomial p with the property that for any polynomial f, we have $f(T)(v) \in U$ iff $p|f$.*

Proof: The fact that I is an ideal is clear: if $f, g \in I$ then $(f+g)(T)(v) = f(T)(v) + g(T)(v) \in U$ (since both $f(T)(v)$ and $g(T)(v)$ are in U and U is a subspace) and for any polynomial h we have $(hf)(T)(v) = (h(T)f(T))(v) = h(T)(f(T)(v)) \in U$, since $f(T)(v) \in U$ and U is $h(T)$-invariant. By Theorem 2, the ideal I consists of all polynomials divisible by a uniquely determined monic polynomial p, which implies the last statement of the proposition. $\square$

Corollary 1. *The annihilator $p_v(x) = x^k - a_{k-1}x^{k-1} - ... - a_0$ of v is the unique monic polynomial with the following property: for any polynomial q we have $q(T)(v) = 0$ iff q is divisible by p_v.*

Proof: We apply the last proposition to v and $U = 0$. Thus there is unique monic polynomial p such that $f(T)(v) = 0$ iff $p|f$. In particular $p|p_v$. It remains to show that $p = p_v$. Since $p|p_v$ and both polynomials are monic, it is enough to show that $deg(p) = deg(p_v)$. It is clear that $deg(p) \leq deg(p_v)$. On the other hand, if $p = x^s - b_{s-1}x^{s-1} - ... - b_0$ then $T^s(v) = b_0 v + b_1 T(v) + ... + b_{s-1}T^{s-1}(v)$. It follows that the vectors $v, T(v), ..., T^{s-1}(v)$ are linearly dependent, so $s = deg(p) \geq k = deg(p_v)$. $\square$

Exercise. Let U be a $T-$invariant subspace of V and let S be a subset of V. Show that the set I of all polynomials f such that $f(T)(v) \in U$ for every $v \in S$ (i.e. $I = \{f : f(T)(v) \in U \text{ for all } v \in S\}$) is an ideal. Show that this ideal contains non-zero polynomials. Consider the case when $U = \{0\}$ and $S = V$ and conclude that there exists a monic polynomial q_T such that for any polynomial f, we have $f(T) = 0$ iff $q_T|f$. The polynomial q_T is called the **minimal polynomial** of T. We will discuss it later in more details.

Recall that our goal is to decompose V into a direct sum of several $T-$invariant subspaces which can not be decomposed any further. We will search for such subspaces among the cyclic subspaces of V (as we have seen, every invariant subspace contains a cyclic subspace generated by any of its

vectors). It is then a natural question to ask when a cyclic subspace $< v >$ can not be decomposed into a direct sum of its proper $T-$invariant subspaces. The answer is given by the following

Proposition 2. *A cyclic subspace $< v >$ cannot be decomposed into a direct sum of its proper $T-$invariant subspaces iff p_v is a power of an irreducible monic polynomial.*

A proof of this result is not difficult and is left as an exercise. We state it here only as a reason why we focus our attention on vectors whose annihilators are powers of irreducible polynomials. The following observation may be helpful in proving Proposition 2 and it will be helpful later on.

Lemma 3. *Suppose that $f|p_v$ and let $w = f(T)(v)$. Then $p_w = p_v/f$.*

Proof: Let $h = p_v/f$. It is clear that h is monic. Note that $h(T)(w) = h(T)(f(T)(v)) = (hf)(T)(v) = p_v(T)(v) = 0$, so $p_w|h$. On the other hand, $0 = p_w(T)(w) = p_w(T)(f(T)(v)) = (p_w f)(T)(v)$ so $p_v|p_w f$, so $h = \frac{p_v}{f}|p_w$. Thus $h|p_w$ and $p_w|h$ and since both h and p_w are monic, we conclude that $h = p_w$. $\square$

Exercise. Let $T : V \longrightarrow V$ be a linear transformation and let $v \in V$ be a non-zero vector.

a) Show that a vector w belongs to $< v >$ iff there is a polynomial f such that $f(T)(v) = w$.

b) Prove that any $T-$invariant subspace of a cyclic subspace is cyclic.
Hint. Let U be a T-invariant subspace of $< v >$. Consider the unique monic polynomial q with the property that for any polynomial f, we have $f(T)(v) \in U$ iff $q|f$ (which exists by Proposition 1). Show that $U =< w >$, where $w = q(T)(v)$. Show also that $q|p_v$.

c) Prove that if p_v is a power of an irreducible polynomial and U, W are T-invariant subspaces of $< v >$ then either $U \subseteq W$ or $W \subseteq U$. Conclude that $< v >$ cannot be decomposed into a direct sum of proper T-invariant subspaces.

d) Prove Proposition 2.
Hint. If p_v is not a power of an irreducible polynomial, then there are an irreducible polynomial q, a positive integer l and a polynomial f not divisible

by q such that $p_v = q^l f$ (see Lemma 2). Set $u = g^l(T)(v)$ and $w = f(T)(v)$ and show that $< v >=< u > \oplus < w >$.

e) Show that $< w >=< v >$ iff $w = f(T)(v)$ for some polynomial f relatively prime to p_v.

f) Let f be a polynomial. Describe p_w for $w = f(T)(v)$.
Hint. Show that $p_w = p_v/h$, where h is the greatest common divisor of p_v and f.

Since every polynomial has irreducible divisors, it follows from Lemma 3 that every $T-$invariant subspace contains vectors whose annihilators are irreducible. Let p be an irreducible monic polynomial which is the annihilator of some vector in V (we just observed that such polynomial exists). Let t be the largest integer such that p^t is the annihilator of some vector in V (such t exists, since the annihilator of any vector has degree bounded by the dimension n of V), and let v be such that $p^t = p_v$. Set k for the dimension of $< v >$, so $k = t \cdot \deg(p)$.

Under these assumptions we have the following key result:

Proposition 3. *Let $v \in V$ be a non-zero vector such that its annihilator $p_v = p^t$ is a power of a monic irreducible polynomial p. Suppose furthermore, that t is the largest integer such that p^t is the annihilator of some vector in V. There exists a $T-$invariant subspace W of V such that $V =< v > \oplus W$.*

The proof of this proposition is based on the following lemma:

Lemma 4. *Let U be a proper $T-$invariant subspace of V. There is a vector u not in U such that:*
— $p_u = q^r$ for some irreducible monic polynomial q;
— for any polynomial f, we have $f(T)(u) \in U$ iff $q|f$.

Proof: Let a be the smallest positive integer such that there is a vector u in V but not in U such that p_u has degree a. Let q be the monic polynomial with the property that for any polynomial f we have $f(T)(u) \in U$ iff $q|f$ (it exists by Proposition 1). Since $u \notin U$, the polynomial q is not constant. Let d be an irreducible monic divisor of p_u and $w = d(T)(u)$. The annihilator $p_w = p_u/d$ has degree smaller than a, so $w \in U$. Thus $q|d$, and therefore $q = d$ (since d is irreducible, both q, d are monic and q is not constant). It follows that q is irreducible and it is the only irreducible divisor of p_u. This implies that $p_u = q^r$ is a power of q. $\square$

Proof of Proposition 4: Let W be a $T-$invariant subspace of maximal possible dimension such that $< v > \cap W = 0$. We will prove that $V =< v > +W$. Suppose not, so that $U =< v > +W$ is a proper $T-$invariant subspace of V. By Lemma 4, there is a vector u not in U such that $p_u = q^r$ is a power of an irreducible polynomial q and $q(T)(u) \in U$. Note that $U =< v > \oplus W$, since $< v > \cap W = 0$. Thus there are unique vectors $w \in W$ and $y \in < v >$ such that $q(T)(u) = y + w$. We will show that u can be chosen so that $y = 0$.

Observe that

$$q^{r-1}(T)(y + w) = q^{r-1}(T)(q(T)(u)) = q^r(T)(u) = p_u(T)(u) = 0,$$

i.e. $q^{r-1}(T)(y) = -q^{r-1}(T)(w)$. But the left hand side of the last equality is in $< v >$ and the right hand side belongs to W. Since $W \cap < v >= 0$, we conclude that both sides are 0, i.e. $q^{r-1}(T)(y) = 0$ and $q^{r-1}(T)(w) = 0$.

We will use often the following useful observation: every vector in a cyclic space $< \omega >$ is of the form $h(T)(\omega)$ for some polynomial h. In fact, for $\mu \in < \omega >$ there exist scalars $c_0, ..., c_{k-1}$ such that $\mu = c_0\omega + c_1T(\omega) + ... + c_{k-1}T^{k-1}(\omega)$ so we may take $h(x) = c_0 + ... + c_{k-1}x^{k-1}$.

Since $y \in < v >$, we may write $y = h(T)(v)$ for some polynomial h. Thus

$$0 = q^{r-1}(T)(y) = q^{r-1}(T)(h(T)(v)) = (q^{r-1}h)(T)(y)$$

so the annihilator p_v of v divides $q^{r-1}h$, i.e. $p^t | q^{r-1}h$. We consider 2 cases:

Case 1. Suppose that $q \neq p$. Since p and q are distinct monic irreducible polynomials and $p^t | q^{r-1}h$, we must have $p^t | h$. But this implies that $0 = h(T)(v) = y$.

Case 2. Suppose that $p = q$. Since $p^r = p_u$ is the annihilator of u, we see that $r \leq t$ by our choice of t. From $p^t | p^{r-1}h$ and $t > r - 1$ we deduce that $p | h$, so we may write $h = ph_1$ for some polynomial h_1. Let $y_1 = h_1(T)(v)$ and $u_1 = u - y_1$. We have $y = p(T)(y_1)$ and therefore

$$p(T)(u_1) = p(T)(u - y_1) = p(T)(u) - p(T)(y_1) = (y + w) - y = w.$$

Note that $u_1 \notin U$, since $u \notin U$ and $y_1 \in < v > \subseteq U$. Furthermore, $p^r(T)(y_1) = p^{r-1}(T)(y) = 0$ and $p^r(T)(u) = 0$. It follows that $p^r(T)(u_1) = 0$, so $p_{u_1} | p^r$. Since p is irreducible, p_{u_1} must be a power of p. This shows that we may replace u by u_1 and then have $y = 0$.

Thus we showed that indeed u can be chosen so that $y = 0$, i.e. $q(T)(u) = w \in W$. We claim that this implies that $< v > \cap (W + < u >) = 0$, which

contradicts our choice of W. In fact, suppose that $x \in < v > \cap (W + < u >)$. Since $x \in W + < u >$, we may write $x = w' + g(T)(u)$ for some $w' \in W$ and some polynomial g. In particular, $g(T)(u) = x - w' \in U$. It follows that $q|g$. Thus $g = qd$ for some polynomial d and $g(T)(u) = d(T)(q(T)(u)) = d(T)(w) \in W$ (since W is invariant). This implies that $x = w' + g(T)(u) \in W$. Recall that also $x \in < v >$, so $x \in < v > \cap W = \{0\}$, i.e. $x = 0$. This proves that $< v > \cap (W + < u >) = 0$, which contradicts our definition of W. $\square$

Now we are able to state the main theorem:

Theorem 4. *Let $T \in L(V, V)$. Then V can de decomposed into a direct sum of cyclic subspaces:*

$$V = < v_1 > \oplus < v_2 > \oplus ... \oplus < v_l >$$

such that p_{v_i} is a power of an irreducible polynomial for each i.

Proof: The proof is an immediate application of Proposition 4. This proposition allows us to write $V = < v_1 > \oplus W_1$ with W_1 a $T-$invariant subspace. Now the same argument applied to W_1 allows us to write $W_1 = < v_2 > \oplus W_2$ for some $T-$invariant subspace W_2 of W_1. So after a finite number of steps we get the required decomposition (another way to spell out this proof is to use induction on the dimension of V). $\square$

Definition 7. *Any decomposition of V of the form described in Theorem 4 is called* **rational canonical decomposition** *of V with respect to T.*

Now the following questions naturally come to mind:

— is there any uniqueness statement about rational canonical decomposition?

— how to compute explicitly such a decomposition?

It is easy to see that a rational canonical decomposition is not unique. For example, let $V = \mathbb{R}^2$ and let $T = I$ be the identity operator. Each non-zero vector $v \in V$ has annihilator $p_v = x - 1$. Thus any two linearly independent vectors v_1 and v_2 give a rational canonical decomposition $V = < v_1 > \oplus < v_2 >$. But in a sense all these decompositions look the same. And in fact something similar is true in general. In order to spell it out we introduce the following definition:

Definition 8. *Consider a rational canonical decomposition*

$$V =< v_1 > \oplus ... \oplus < v_l > .$$

Let the annihilator of v_i be $q_i^{d_i}$, where q_i is a monic irreducible polynomial. For each irreducible polynomial p and each integer $m > 0$ define $M(p, m)$ to be the number of i such that $p_{v_i} = p^m$, i.e. it is the number of direct summands in the decomposition which have annihilator p^m (so for all but a finite number of pairs (p, m) the number $M(p, m) = 0$). For convenience, we also define $M(p, 0) = 0$.

Example. Suppose that $l = 5$, $p_{v_1} = x - 1$, $p_{v_2} = (x-1)^2$, $p_{v_3} = (x-1)^4$, $p_{v_4} = (x^2+1)^2$, $p_{v_5} = (x^2+1)^2$. Then $M(x-1, 1) = 1$, $M(x-1, 2) = 1$, $M(x-1, 3) = 0$, $M(x-1, 4) = 1$, $M(x^2+1, 1) = 0$, $M(x^2+1, 2) = 2$ and $M(p, m) = 0$ in all other cases.

We will show that the numbers $M(p, m)$ are the same for every rational canonical decomposition. This is the same as to say that the sequence of annihilators $p_{v_1}, p_{v_2}, ..., p_{v_l}$ is, up to order of elements, the same for any two rational canonical decompositions. Since two cyclic spaces with the same annihilator "look the same" (see the next exercise for more precise meaning of this claim), this justifies our claim that any two rational canonical decompositions "look the same".

Exercise. Let $< v >$, $< w >$ be two subspaces of V such that $p_v = p_w$. Prove that there is an isomorphism $S :< v > \longrightarrow < w >$ such that $ST = TS$.

Our proof of the independence of $M(p, m)$ on the particular decomposition is based on the following useful observation.

Lemma 5. *Let v be a vector whose annihilator $p_v = q^m$ is a power of an irreducible polynomial q. For any irreducible polynomial p and any integer $i > 0$ the kernel of the linear transformation $p^i(T) :< v > \longrightarrow < v >$ equals*

$$\ker p^i(T) = \begin{cases} \{0\} & \text{if } p \neq q; \\ < v > & \text{if } p = q \text{ and } i \geq m; \\ < q^{m-i}(T)(v) > & \text{if } p = q \text{ and } i < m. \end{cases}$$

In particular, if $p = q$, then the dimension of the kernel of $p^i(T)$ equals $\min(i, m) \deg q$, where $\min(i, m)$ denotes the smaller of the integers i, m.

Proof: Let $w \in < v >$, so there is a polynomial h such that $w = h(T)(v)$. Now $p^i(T)(w) = 0$ iff $(p^i h)(T)(v) = 0$ iff $p_v | p^i h$.

If $p \neq q$ then the last divisibility is equivalent to $p_v | h$ and therefore $w = h(T)(v) = 0$. Thus $\ker p^i(T) = \{0\}$ in this case.

If $p = q$ and $i \geq m$ then $p_v | p^i h$ for any h so any w in $< v >$ satisfies $p^i(T)(w) = 0$. Thus $\ker p^i(T) =< v >$ in this case and its dimension equals $\deg p_v = m \deg q = \min(i, m) \deg q$.

Finally, if $p = q$ and $i < m$ then $p_v | p^i h$ iff $q^{m-i} | h$. Thus if $p^i(T)(w) = 0$ then $h = q^{m-i} h_1$ and $w = h_1(T)(q^{m-i}(T)(v)) \in < q^{m-i}(T)(v) >$. Conversely, it is clear that any vector w in $< q^{m-i}(T)(v) >$ satisfies $p^i(T)(w) = 0$ (why?). Thus $\ker p^i(T) =< q^{m-i}(T)(v) >$ in this case. Since the annihilator of $q^{m-i}(T)(v)$ equals q^i (by Lemma 3), we see that the dimension of $< q^{m-i}(T)(v) >$ equals $\deg q^i = i \deg q = \min(i, m) \deg q$. $\square$

Exercise. For any polynomial f and any vector v describe the kernel and range of the linear transformation $f(T)$ on the cyclic space $< v >$.
Hint. Show that the range of $f(T)$ is $< f(T)(v) >$ and the kernel equals $< h(T)(v) >$, where h is such that p_v/h is the greatest common divisor of f and p_v.

Now we can prove the following

Theorem 5. *Let $T : V \longrightarrow V$ be a linear transformation. For an irreducible polynomial p and an integer $i > 0$ define $V_i(p)$ to be the kernel of the liner transformation $p^i(T) : V \longrightarrow V$ and set $d(p, i)$ to be the dimension of $V_i(p)$ for $i > 0$ and $d(p, 0) = 0$. Then*

$$M(p, i) = \frac{2d(p, i) - d(p, i-1) - d(p, i+1)}{\deg p}$$

for all $i > 0$.

Proof: Let

$$V =< v_1 > \oplus < v_2 > \oplus ... \oplus < v_l >,$$

where $p_{v_i} = p_i^{t_i}$ is a power of a monic irreducible polynomial p_i for each i. Any $w \in V$ can be uniquely written as $w = w_1 + ... + w_l$ with $w_i \in < v_i >$. We have $p^m(T)(w) = p^m(T)(w_1) + ... + p^m(T)(w_l)$. Since $p^m(T)(w_i) \in < v_i >$, we see that $p^m(T)(w) = 0$ iff $p^m(T)(w_i) = 0$ for all i. This means that $V_m(p)$

is the direct sum of the spaces $K_j = \{u \in < v_j >: p^m(T)(u) = 0\}$. Thus, $d(p,m) = \dim V_m(p) = \sum_{j=1}^{l} \dim K_j$. By Lemma 5, we have

$$\dim K_j = \begin{cases} 0 & \text{if } p \neq p_j; \\ \min(t_j, m) \deg p & \text{if } p = p_j. \end{cases}$$

Directly from the definition of the numbers $M(p,m)$ we see that

$$d(p,m) = \sum_{i=1}^{\infty} M(p,i) \min(i,m) \deg p$$

for every $m \geq 0$ (since $M(p,i)$ is the number of summands with annihilator equal to p^i and each such summand contributes to $V_m(p)$ a direct summand of dimension $\min(i,m)\deg p$). From these formulas one can now compute the numbers $M(p,i)$ in terms of the numbers $d(p,m)$ to get the expressions claimed in the theorem. But once we know what the expressions should be, the verification that they are indeed correct is quite simple:

$$2d(p,m) - d(p,m-1) - d(p,m+1) =$$

$$= \sum_{i=1}^{\infty} M(p,i)(2\min(i,m) - \min(i,m-1) - \min(i,m+1)) \deg p. \qquad (*)$$

Note that

$$2\min(i,m) - \min(i,m-1) - \min(i,m+1) = \begin{cases} 2i - i - i = 0 & \text{for } i < m \\ 2m - (m-1) - (m+1) = 0 & \text{for } i > m \\ 2m - (m-1) - m = 1 & \text{for } i = m. \end{cases}$$

Thus $(*)$ simply says that

$$2d(p,m) - d(p,m-1) - d(p,m+1) = M(p,m) \deg p$$

which is exactly what the theorem claims. $\square$

The last theorem proves in particular that the numbers $M(p,m)$ are independent on the rational canonical decomposition. Indeed, we expressed these numbers in terms of the dimensions $d(p,i)$ and these dimensions are defined without reference to any decomposition of V.

Theorem 5 suggests a simple algorithm to determine the numbers $M(p,m)$ for a given irreducible polynomial p. All we need to do is to compute the dimension $d(p,i)$ of the kernel of the linear transformation $p(T)^i$ for $i = 1, 2, ...$

Example. Consider a linear transformation $T : \mathbf{R}^5 \longrightarrow \mathbf{R}^5$ given by the matrix

$$A = \begin{pmatrix} 1 & 0 & 2 & -1 & -2 \\ -1 & 2 & 0 & 1 & -2 \\ 1 & 0 & 0 & 1 & 2 \\ 2 & 0 & -1 & 3 & 2 \\ 1 & 2 & 0 & 1 & 0 \end{pmatrix}.$$

Let $p(x) = x - 2$. Thus

$$p(A) = A - 2I = \begin{pmatrix} -1 & 0 & 2 & -1 & -2 \\ -1 & 0 & 0 & 1 & -2 \\ 1 & 0 & -2 & 1 & 2 \\ 2 & 0 & -1 & 1 & 2 \\ 1 & 2 & 0 & 1 & -2 \end{pmatrix}$$

has rank 4 (this follows from a row-echelon form of p(A) which has 4 pivot columns, but we skip the computations of row echelon forms here), hence the kernel of $p(A)$ has dimension $5 - 4 = 1$, i.e. $d(x-2,1) = 1$. Now

$$p(A)^2 = \begin{pmatrix} -1 & -4 & -5 & 0 & 8 \\ 1 & -8 & 1 & 0 & 8 \\ 1 & 4 & 5 & 0 & -8 \\ 1 & 4 & 5 & 0 & -8 \\ 3 & -4 & 1 & 0 & 0 \end{pmatrix}$$

has rank 3, so the kernel of $p(A)^2$ has dimension $5-3 = 2$, i.e. $d(x-2,2) = 2$. Next

$$p(A)^3 = \begin{pmatrix} 8 & 16 & 8 & 0 & -16 \\ 8 & 16 & 8 & 0 & -16 \\ -8 & -16 & -8 & 0 & 16 \\ -8 & -16 & -8 & 0 & 16 \\ 8 & -8 & 0 & 0 & 16 \end{pmatrix}$$

has rank 2, so the kernel of $p(A)^3$ has dimension $5-2 = 3$, i.e. $d(x-2,3) = 3$.

We continue:

$$p(A)^4 = \begin{pmatrix} -32 & -64 & -16 & 0 & 64 \\ -32 & -64 & -16 & 0 & 64 \\ 32 & 64 & 16 & 0 & -64 \\ 32 & 64 & 16 & 0 & -64 \\ 0 & 0 & 18 & 0 & 0 \end{pmatrix}$$

has again rank 2, so the kernel of $p(A)^4$ has dimension $5-2=3$, i.e. $d(x-2,4)=3$. At this point we can stop our process and conclude that $d(x-2,m)=3$ for all $m \geq 3$ (see exercise below for an explanation). From the formulas of Theorem 5 we see that $M(x-2,3)=1$ and $M(x-2,m)=0$ for all $m \neq 3$.

Now we do the same for the polynomial $p(x)=x^2+4$. Thus

$$p(A) = A^2 + 4I = \begin{pmatrix} 3 & -4 & 3 & -4 & 0 \\ -3 & 4 & -3 & 4 & 0 \\ 5 & 4 & 5 & 4 & 0 \\ 9 & 4 & 1 & 12 & 0 \\ 1 & 4 & 1 & 4 & 0 \end{pmatrix}$$

has rank 3, hence the kernel of $p(A)$ has dimension $5-3=2$, i.e. $d(x^2+4,1)=2$. Next

$$p(A)^2 = \begin{pmatrix} 0 & -32 & 32 & -64 & 0 \\ 0 & 32 & -32 & 64 & 0 \\ 64 & 32 & 32 & 64 & 0 \\ 128 & 32 & 32 & 128 & 0 \\ 32 & 32 & 0 & 64 & 0 \end{pmatrix}$$

has again rank 3, hence the kernel of $p(A)^2$ has dimension $5-3=2$, i.e. $d(x^2+4,2)=2$. As before, at this point we can stop our process and conclude that $d(x^2+4,m)=2$ for all $m \geq 1$. The formulas of Theorem 5 yield $M(x^2+4,1)=1$ and $M(x^2+4,m)=0$ for all $m \neq 1$.

Our computations so far show that any rational canonical decomposition of $\mathbf{R}^5$ with respect to T will contain a cyclic space $< v >$ with $p_v = (x-2)^3$ and a cyclic space $< w >$ with $p_w = x^2+4$. Since $\dim < v >= 3$ and $\dim < w >= 2$, we must have $\mathbf{R}^5 =< v > \oplus < w >$. Note that at this point we do not have any explicit candidates for the vectors v, w, we only know that such vectors must exist. Finding such vectors requires in general substantially more work and we will get back to this problem later. In our

particular case however we may find such v, w rather easily: for w we may take any non-zero vector in the kernel of T^2+4I and for v any vector which is in the kernel of $(T-2I)^3$ but is not in the kernel of $(T-2I)^2$ will work.

Exercise. Explain why the above choices for v and w work.

Exercise. a) Let $T : V \longrightarrow V$ be a linear transformation. Prove that $\ker T^i \subseteq \ker T^{i+1}$ and $\mathrm{Im}T^{i+1} \subseteq \mathrm{Im}T^i$ for every non-negative integer i. Prove furthermore that if $\ker T^k$ and $\ker T^{k+1}$ have the same dimension for some integer k then all the kernels $\ker T^i$ have the same dimension for $i \geq k$.

b) Use a) to show that if the matrices A^k and A^{k+1} have the same rank, then all the matrices A^i with $i \geq k$ have the same rank.

Exercise. Follow the Example above to find the numbers $M(x-2,m)$, $M(x^2+4,m)$ for the linear transformation $T : \mathbf{R}^5 \longrightarrow \mathbf{R}^5$ given by the matrix

$$B = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 \\ -3 & 2 & 2 & 0 & -2 \\ 1 & 0 & 0 & 0 & 2 \\ 3 & 0 & -2 & 2 & 2 \\ 1 & 2 & 0 & 0 & 0 \end{pmatrix}.$$

(You should get that $M(x-2,1) = 1 = M(x-2,2)$ and $M(x^2+4,1) = 1$).

The computations in the Example are rather straightforward (but tedious). There is however one question which a curious reader must have asked by now: how did we know that $x-2$ and x^2+4 are the polynomials to look at? In other words, how to find the irreducible polynomials which can be annihilators of some vector of V? In order to answer this question we introduce the following two polynomials. Consider a rational canonical decomposition $V = < v_1 > \oplus ... \oplus < v_l >$ and let the annihilator of v_i be $p_{v_i} = q_i^{d_i}$, where q_i is a monic irreducible polynomial for $i = 1, 2..., l$. We have proved that the sequence $p_{v_1}, p_{v_2}, ..., p_{v_l}$ is, up to order, the same for all rational canonical decomposition. We define two polynomials p_T, q_T as follows:

- p_T is the product of all the polynomials p_{v_i}, i.e. $p_T = q_1^{d_1} q_2^{d_2} ... q_l^{d_l}$. We call it the **characteristic** polynomial of T.
- q_T is the least common multiple of the polynomials p_{v_i}. We call it the **minimal** polynomial of T.

It is clear from the definition and our previous results that

- the polynomials p_T and q_T do not depend on the rational canonical decomposition.
- $q_T|p_T$ and p_T and q_T have the same irreducible divisors.
- $\deg p_T = \dim V$ (since $\deg p_{v_i} = \dim < v_i >$).
- an irreducible monic polynomial p is the annihilator of some vector in V (which is the same as to say that $M(p,m) \neq 0$ for some m) iff $p|q_T$ or equivalently $p|p_T$.

Example. Suppose that $l = 5$, $p_{v_1} = x - 1$, $p_{v_2} = (x-1)^2$, $p_{v_3} = (x-1)^4$, $p_{v_4} = (x^2+1)^2$, $p_{v_5} = (x^2+1)^2$. Then $p_T = (x-1)^7(x^2+1)^4$ and $q_T = (x-1)^4(x^2+1)^2$.

The main feature of the polynomials p_T and q_T is that they can be explicitly computed. It turns out that p_T is the usual characteristic polynomial defined in terms of determinants and there is a very nice algorithm to compute it. At this point however we do not have at our disposition the machinery of determinants so we focus on the polynomial q_T. We have the following simple, but crucial observation.

Proposition 4. *The polynomial q_T is the unique monic polynomial with the property that for any polynomial f we have $f(T) = 0$ iff $q_T|f$. Equivalently, q_T is the monic polynomial of lowest possible degree such that $q_T(T) = 0$.*

Proof: Since $p_{v_i}|q_T$ for every i, we see that $q_T(T)(v_i) = 0$. This means that all the spaces $< v_i >$ are contained in the kernel of $q_T(T)$, so V is in its kernel, i.e. $q_T(T) = 0$.

Now if $f(T) = 0$ for some polynomial f, then $f(T)(v_i) = 0$ so $p_{v_i}|f$ for all i. Thus $q_T|f$. $\square$

In order to find the minimal polynomial q_T we may proceed as in the proof of Theorem 1. Note that the linear operators $I, T, T^2, ...$ are elements of a finite dimensional vector space $L(V,V)$. Thus they are linearly dependent. So there are scalars $b_0, ..., b_m$ not all 0 such that $b_0T^0 + ... + b_mT^m = 0$. Taking m smallest possible we may assume that $b_m = 1$ and then the minimal polynomial q_T equals $x^m + b_{m-1}x^{m-1} + ... + b_0$. It is clear that m is bounded above by the dimension of $L(V,V)$, i.e. by n^2. But we proved above that in fact it is bounded by n, a fact not obvious at all.

The observation we just made suggests a simple algorithm for finding q_T. We simply consider $I, T, T^2, ...$ as vectors in the vector space $L(V,V)$ and we have to find largest m such that $I, T, T^2, ..., T^{m-1}$ are linearly independent and then express T^m as a linear combination of $I, T, T^2, ..., T^{m-1}$.

Example. Let us see how our algorithm works for T from the previous example. We compute the powers of A:

$$A^2 = \begin{pmatrix} -1 & -4 & 3 & -4 & 0 \\ -3 & 0 & -3 & 4 & 0 \\ 5 & 4 & 1 & 4 & 0 \\ 9 & 4 & 1 & 8 & 0 \\ 1 & 4 & 1 & 4 & -4 \end{pmatrix}, \quad A^3 = \begin{pmatrix} -2 & -8 & 2 & -6 & 8 \\ 2 & 0 & -10 & 12 & 8 \\ 10 & 8 & 6 & 12 & -8 \\ 22 & 8 & 10 & 20 & -8 \\ 2 & 0 & -2 & 12 & 0 \end{pmatrix},$$

$$A^4 = \begin{pmatrix} -8 & 0 & 8 & -32 & 0 \\ 24 & 16 & -8 & 32 & 0 \\ 24 & 0 & 8 & 32 & 0 \\ 56 & 0 & 24 & 48 & 0 \\ 24 & 0 & -8 & 32 & 16 \end{pmatrix}, \quad A^5 = \begin{pmatrix} -64 & 0 & 16 & -86 & -32 \\ 64 & 32 & 24 & 80 & -32 \\ 96 & 0 & 16 & 80 & 32 \\ 176 & 0 & 64 & 110 & 32 \\ 96 & 32 & 16 & 80 & 0 \end{pmatrix}$$

The vector space of all $n \times n$ matrices over a field K can be identified with K^{n^2} by identifying a matrix $(a_{i,j})$ with the vector

$$(a_{1,1}, a_{1,2}, ..., a_{1,n}, a_{2,1}, a_{2,2}, ..., a_{2,n}, a_{3,1}, ..., a_{n,n}).$$

For example, the matrix A is identified with

$$(1, 0, 2, -1, -2, -1, 2, 0, 1, -2, 1, 0, 0, 1, 2, 2, 0, -1, 3, 2, 1, 2, 0, 1, 0)$$

Thus in order to find the minimal polynomial of T we row reduce the matrix M below to get N.

$$M = \begin{pmatrix} 1 & 1 & -1 & -2 & -8 & -64 \\ 0 & 0 & -4 & -8 & 0 & 0 \\ 0 & 2 & 3 & 2 & 8 & 16 \\ 0 & -1 & -4 & -6 & -32 & -86 \\ 0 & -2 & 0 & 8 & 0 & -32 \\ 0 & -1 & -3 & 2 & 24 & 64 \\ 1 & 2 & 0 & 0 & 16 & 32 \\ 0 & 0 & -3 & -10 & -8 & 24 \\ 0 & 1 & 4 & 12 & 32 & 80 \\ 0 & -2 & 0 & 8 & 0 & -32 \\ 0 & 1 & 5 & 10 & 24 & 96 \\ 0 & 0 & 4 & 8 & 0 & 0 \\ 1 & 0 & 1 & 6 & 8 & 16 \\ 0 & 1 & 4 & 12 & 32 & 80 \\ 0 & 2 & 0 & -8 & 0 & 32 \\ 0 & 2 & 9 & 22 & 56 & 176 \\ 0 & 0 & 4 & 8 & 0 & 0 \\ 0 & -1 & 1 & 10 & 24 & 64 \\ 1 & 3 & 8 & 20 & 48 & 110 \\ 0 & 2 & 0 & -8 & 0 & 32 \\ 0 & 1 & 1 & 2 & 24 & 96 \\ 0 & 2 & 4 & 0 & 0 & 32 \\ 0 & 0 & 1 & -2 & -8 & 16 \\ 0 & 1 & 4 & 12 & 32 & 80 \\ 1 & 0 & -4 & 0 & 16 & 0 \end{pmatrix} \qquad N = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 32 \\ 0 & 1 & 0 & 0 & 0 & -48 \\ 0 & 0 & 1 & 0 & 0 & 32 \\ 0 & 0 & 0 & 1 & 0 & -16 \\ 0 & 0 & 0 & 0 & 1 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

It follows that $A^5 = 32I - 48A + 32A^2 - 16A^3 + 6A^4$ and the minimal polynomial $q_T = x^5 - 6x^4 + 16x^3 - 32x^2 + 48x - 32$. Once we have the minimal polynomial, we need to factor it into a product of irreducible polynomials. In our case, we get that $q_T = (x-2)^3(x^2+4)$. This explains why we considered the irreducible polynomials $x - 2$ and $x^2 + 4$ in the previous example.

Example. Let us find the minimal polynomial of the matrix $B = \begin{pmatrix} 2 & -1 & 2 \\ 4 & -2 & 2 \\ -3 & 2 & 1 \end{pmatrix}$.

First we compute B^2 and B^3:

$$B^2 = \begin{pmatrix} -6 & 4 & 4 \\ -6 & 4 & 6 \\ -1 & 1 & -1 \end{pmatrix} \quad \text{and} \quad B^3 = \begin{pmatrix} -8 & 6 & 0 \\ -14 & 10 & 2 \\ 5 & -3 & -1 \end{pmatrix}.$$

Then we find the reduced row-echelon form N of the matrix M:

$$M = \begin{pmatrix} 1 & 2 & -6 & -8 \\ 0 & -1 & 4 & 6 \\ 0 & 2 & 4 & 0 \\ 0 & 4 & -6 & -14 \\ 1 & -2 & 4 & 10 \\ 0 & 2 & 6 & 2 \\ 0 & -3 & -1 & 5 \\ 0 & 2 & 1 & -3 \\ 1 & 1 & -1 & -1 \end{pmatrix} \qquad N = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & -2 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

From N we see that $B^3 = 2I - 2B + B^2$, so the minimal polynomial $q_B = x^3 - x^2 + 2x - 2$. Note that 1 is a root of the polynomial q_B, so $q_(x-1)(x^2+2)$. If we work over the field $\mathbb{R}$ of real numbers, then x^2+2 is irreducible. Thus a rational canonical decomposition for B has one cyclic summand $< v_1 >$ with annihilator $x - 1$ (so it has dimension 1) and one cyclic summand $< v_2 >$ with annihilator $x^2 + 2$ (so it has dimension 2). Note that v_1 is a non-zero vector in the kernel of $B - I$. Since this kernel is of dimension 1, the vector v_1 is unique up to a scalar multiple and simple computation of the kernel yields $v_1 = (4, 6, 1)$ (or any multiple of this vector). For v_2 we may take any non-zero vector in the kernel of $B^2 + 2I$ (why?). This kernel is of dimension 2 (hence must be equal to $< v_2 >$; this answers the question; how?) and we may take, for example, $v_2 = (1, 2, 1)$.

Suppose now that we consider B over the field $\mathbb{C}$ of complex numbers. Then x^2+2 is no longer irreducible and we have $q_b = (x-1)(x-i\sqrt{2})(x+i\sqrt{2})$. Thus a rational canonical decomposition for B (over $\mathbb{C}$) has three cyclic factors, each of dimension 1: $< w_1 > \oplus < w_2 > \oplus < w_3 >$. As before, w_1 is a non-zero vector in the kernel of $B - I$, so we may take $w_1 = (4, 6, 1)$. Similarly, w_2 is a non-zero vector in the kernel of $B - i\sqrt{2}$ and a simple computation yields $w_2 = (1 + i\sqrt{2}, 2 + i\sqrt{2}, -1)$. Finally w_3 is a non-zero vector in the kernel of $B + i\sqrt{2}I$ so we may take $w_3 = (1 - i\sqrt{2}, 2 - i\sqrt{2}, -1)$.

The moral of the above consideration is that the form of a rational canonical decomposition depends on the field of scalars. Most convenient field for

many purposes is a field over which all the irreducible factors of the minimal polynomial are of degree 1. Over the field of complex numbers every irreducible polynomial has degree 1 (this is a very important fact often called **the Fundamental Theorem of Algebra**).

Exercise. Let $T : V \longrightarrow V$ be a linear transformation and let $v_1, ..., v_n$ be a basis of V. Prove that the minimal polynomial q_T is equal to the least common multiple of the annihilators $p_{v_1}, ..., p_{v_n}$ of $v_1, ..., v_n$.

The last exercise gives an alternative method of computing the minimal polynomial. It has the advantage that one does not have to work with matrices of big size but instead one needs to compute n annihilators. The real advantage of this method though is that with some luck the annihilators will be of lower degree than q_T so it will be easier to find the decomposition of them into irreducible factors.

Exercise. Apply this method to find the minimal polynomial of the matrices A, B in the previous examples.

Now we introduce a new, very useful basis of the cyclic space $< v >$ when the annihilator $p_v = p^r$ is a power of an irreducible monic polynomial p. Suppose that $p = x^k + a_{k-1}x^{k-1} + ... + a_0$. We have the following

Definition 9. *Let v be a vector with annihilator $p_v = p^r$, where $p = x^k + a_{k-1}x^{k-1} + ... + a_0$ is irreducible. The* **canonical basis** *corresponding to v is the ordered basis*

$$v, T(v), ..., T^{k-1}(v), p(T)(v), (Tp(T))(v), ..., (T^{k-1}p(T))(v), p^2(T)(v), ..., p^{r-1}(T)(v),$$

$$(Tp^{r-1}(T))(v), ..., (T^{k-1}p^{r-1}(T))(v).$$

The nice thing about the canonical basis is that the matrix representation of T on $< v >$ in this basis is very simple and expressed only in terms of the

coefficients of p (and not of p^r). It looks like:

$$\begin{pmatrix}
0 & 0 & \cdots & 0 & 0 & -a_0 & & & & & & & & & & & & \\
1 & 0 & \cdots & 0 & 0 & -a_1 & & & & & & & & & & & & \\
0 & 1 & \cdots & 0 & 0 & -a_2 & & & & & & & & & & & & \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & & & & & & & \\
0 & 0 & \cdots & 1 & 0 & -a_{k-2} & & & & & & & & & & & & \\
0 & 0 & \cdots & 0 & 1 & -a_{k-1} & & & & & & & & & & & & \\
 & & & & & 1 & 0 & 0 & \cdots & 0 & 0 & -a_0 & & & & & & \\
 & & & & & & 1 & 0 & \cdots & 0 & 0 & -a_1 & & & & & & \\
 & & & & & & 0 & 1 & \cdots & 0 & 0 & -a_2 & & & & & & \\
 & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & & & & & & \\
 & & & & & & 0 & 0 & \cdots & 1 & 0 & -a_{k-2} & & & & & & \\
 & & & & & & 0 & 0 & \cdots & 0 & 1 & -a_{k-1} & & & & & & \\
 & & & & & & & & & & & 1 & \ddots & & & & & \\
 & & & & & & & & & & & & \ddots & & & & & \\
 & & & & & & & & & & & & & \ddots & & & & \\
 & & & & & & & & & & & & & 1 & 0 & 0 & \cdots & 0 & 0 & -a_0 \\
 & & & & & & & & & & & & & & 1 & 0 & \cdots & 0 & 0 & -a_1 \\
 & & & & & & & & & & & & & & 0 & 1 & \cdots & 0 & 0 & -a_2 \\
 & & & & & & & & & & & & & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
 & & & & & & & & & & & & & & 0 & 0 & \cdots & 1 & 0 & -a_{k-2} \\
 & & & & & & & & & & & & & & 0 & 0 & \cdots & 0 & 1 & -a_{k-1}
\end{pmatrix}$$

where the empty space consists of zeros.

Combining all the canonical bases of the cyclic summands of a canonical decomposition produces a basis of V which is usually called a **rational canonical basis** of V with respect to T. Often we will just call it a rational canonical basis of T. A more precise definition is given by:

Definition 10. *Let $V =< v_1 > \oplus ... \oplus < v_l >$ be a rational canonical decomposition of V with respect to T. The* **rational canonical basis** *associated to $v_1, ..., v_l$ is the ordered basis obtained by taking the canonical basis corresponding to v_1 followed by the canonical basis corresponding to v_2 ... followed by the canonical basis corresponding to v_l. A an ordered basis of V is called a* **rational canonical basis** *of T if it is associated to some rational canonical decomposition.*

The matrix representation of T in a rational canonical basis is block-diagonal, with blocks on the diagonal corresponding to the cyclic factors of the underlying rational canonical decomposition (so they are of the form described above). Any such matrix representation is called a **rational canonical form** of T. So we have

Definition 11. *A* **rational canonical form** *of T is a matrix representation of T in a rational canonical basis.*

Note that by Theorem 5 a rational canonical form of T is unique up to order of the diagonal blocks.

Remark. Given an $n \times n$ matrix A we may apply the above discussion to the linear transformation $T_A : F^n \longrightarrow F^n$ whose matrix representation in the canonical basis is A. Thus we can speak about a rational canonical form of the matrix A, rational canonical basis for A, etc.

In practice, the most important case of the theory of rational canonical forms is when the irreducible divisors of the minimal polynomial are all linear. This is always the case if the field F is algebraically closed, for example $F = \mathbb{C}$. But even if F is not algebraically closed, one of the basic results in the theory of fields says that F is a subfield of an algebraically closed field $\overline{F}$. Thus we can often extend our scalars to $\overline{F}$ and study the rational canonical decomposition in this situation and then derive consequences for the original problem over F.

Example. Suppose we want to understand the operator $T(x, y) = (-2y, x + 2y)$ on $V = \mathbb{R}^2$. It is easy to see that its minimal polynomial is $x^2 - 2x + 2$, which is irreducible over $\mathbb{R}$, so the space V can not be decomposed into a direct sum of proper $T-$invariant subspaces. We have $V =< (1, 0) >$ and the corresponding rational canonical form is $A = \left(\begin{smallmatrix} 0 & -2 \\ 1 & 2 \end{smallmatrix}\right)$. Now extending our field to $\mathbb{C}$ we see that $x^2 - 2x + 2 = (x - (1 + i))(x - (1 - i))$ is a product of 2 linear polynomials. Thus there is a decomposition $\mathbb{C}^2 =< v_1 > \oplus < v_2 >$, where the vector v_1 has annihilator $x-(1+i)$ and the vector v_2 has annihilator $x-(1-i)$. It is easy to see that we may take $v_1 = (1-i, 1)$ and $v_2 = (1+i, 1)$. The rational canonical form in this basis is $B = \left(\begin{smallmatrix} 1+i & 0 \\ 0 & 1-i \end{smallmatrix}\right)$. The transition matrix from the basis v_1, v_2 to the basis $(1, 0), (0, 1)$ is $C = \left(\begin{smallmatrix} 1-i & 1+i \\ 1 & 1 \end{smallmatrix}\right)$ and its inverse is $C^{-1} = \left(\begin{smallmatrix} i/2 & (1-i)/2 \\ -i/2 & (1+i)/2 \end{smallmatrix}\right)$. All this allows us to get simple formulas for T^n. In fact, the powers of B are very easy to compute: $B^n = \left(\begin{smallmatrix} (1+i)^n & 0 \\ 0 & (1-i)^n \end{smallmatrix}\right)$.

If we want to return to the field $\mathbb{R}$, we see that $A = CBC^{-1}$ so $A^n = CB^nC^{-1}$.

So let us discuss more carefully the situation when all irreducible divisors of the minimal polynomial of T are linear. We introduce the following definition:

Definition 12. *A scalar λ is called an* **eigenvalue** *of T if $x - \lambda$ divides the minimal polynomial q_T of T. Equivalently, λ is a root of q_T.*

If λ is an eigenvalue of T then there exist vectors v such that $p_v = x - \lambda$. Any such vector is called an **eigenvector** of T for the eigenvalue λ. Note that the equality $p_v = x - \lambda$ simply means that $T(v) = \lambda v$, i.e. that v is in the kernel of $T - \lambda I$.

Definition 13. *An* **eigenvector** *of T for the eigenvalue λ is any non-zero vector v such that $T(v) = \lambda v$, i.e. such that $p_v = x - \lambda$. A* **generalized eigenvector** *of length k of T for the eigenvalue λ is any vector v such that $p_v = (x - \lambda)^k$.*

We see that an eigenvector is the same as a generalized eigenvector of length 1. Note that if v is a generalized eigenvector of length k, then $< v >$ has dimension k and the canonical basis associated to v is $v_0, v_1, ..., v_{k-1}$ with $v_i = (T-\lambda)^i(v)$ (so $v_0 = v$). The matrix representation of $T :< v > \longrightarrow < v >$ in this basis is very simple: it has λ's on the diagonal, 1's right below the main diagonal and zeros everywhere else, so it looks like

$$\begin{pmatrix} \lambda & 0 & 0 & ... & 0 & 0 \\ 1 & \lambda & 0 & ... & 0 & 0 \\ 0 & 1 & \lambda & ... & 0 & 0 \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & \lambda & 0 \\ 0 & 0 & 0 & ... & 1 & \lambda \end{pmatrix}$$

Any matrix of this form is called a **Jordan block**. A rational canonical decomposition in the case when all irreducible divisors of q_T are linear is called **Jordan decomposition**, a rational canonical basis is called **Jordan basis**, etc.

One of our motivations for the theory of rational canonical forms was the desire to compute powers of a given matrix A. We have seen that this is particularly easy when A is similar to a diagonal matrix. We introduce the following definition:

Definition 14. *A linear transformation $T : V \longrightarrow V$ is called* **diagonalizable** *if V has a basis which consists of eigenvectors. In other words, T is diagonalizable if all direct summands in a rational canonical decomposition for T have dimension 1. Another equivalent formulation is that the minimal polynomial q_T is a product of pairwise distinct linear polynomials.*

A matrix A is called **diagonalizable** *if the linear transformation T_A associated to A is diagonalizable. Equivalently, A is diagonalizable iff it is similar to a diagonal matrix.*

Exercise. Explain why the above characterization of diagonalizability are equivalent.

Exercise. Show that over algebraically closed field a linear transformation T is diagonalizable iff the minimal polynomial q_T and its derivative q_T' are relatively prime (i.e. do not have any common divisors).

It is time to discuss methods which allow to find an actual rational canonical decomposition for a given linear transformation T. The first step is to separate direct summands which are annihilated by powers of different irreducible polynomials. Let $< v_1 > \oplus < v_2 > \oplus ... \oplus < v_l >$ be a rational canonical decomposition for T. For an irreducible monic polynomial p define $V(p)$ as the sum of all those cyclic spaces $< v_i >$ in the decomposition whose annihilator is a power of p. Note that $V(p)$ is non-zero iff p divides q_T.

Theorem 6. *The subspace $V(p)$ is the same for every rational canonical decomposition. It can be characterized as the subspace of all vectors whose annihilator is a power of p. Equivalently, it is the kernel of $p(T)^m$ for any m sufficiently large (to be more precise, any m larger or equal than $M(p)$, where $M(p)$ is the largest positive integer k for which $M(p,k) \neq 0$). The vector space V is a direct sum of the spaces $V(p)$.*

Proof: It is clear that the annihilator of each vector in $V(p)$ is a power of p. Let $w \in V$ so w can be uniquely written as $w = w_1 + ... + w_l$ with $w_i \in < v_i >$. Then $p^m(T)(w) = p^m(T)(w_1) + ... + p^m(T)(w_l)$. Thus $p^m(T)(w) = 0$ iff $p^m(T)(w_i) = 0$ for all i. Now p_{v_i} is a power of an irreducible monic polynomial q_i. By Lemma 5 we have $w_i = 0$ if p_{v_i} is not a power of p and therefore $w \in V(p)$. So indeed $V(p)$ is the set of all vectors whose annihilator is a power of p. This shows that $V(p)$ is the same for every decomposition. That V is the direct sum of the subspaces $V(p)$ is clear from their definition. $\square$

In practice, it is easy to find a basis of $V(p)$, since it is the kernel of $p(T)^{M(p)}$. Once we have a basis of $V(p)$ we can find the matrix of $T : V(p) \longrightarrow V(p)$ in this basis and then try to find a rational canonical decomposition of $V(p)$. Thus it is enough to know how to find a rational canonical decomposition in the case when the minimal polynomial is a power of a single irreducible polynomial.

Algorithm Let us now describe an algorithm which produces a rational canonical decomposition for a linear transformation $T : V \longrightarrow V$.

Step 1. Find the minimal polynomial q_T or the characteristic polynomial p_T for T. Find all irreducible divisors of q_T or p_T.

For each irreducible divisor p of q_T do the following. Let d be the degree of p.

Step 2. Find a basis of $V(p)$. In other words, find a basis of the kernel of $p(T)^{M(p)}$ or any larger power of $p(T)$ (note that $M(p)$ is simply the power of p in the minimal polynomial q_T). If you know the characteristic polynomial but not the minimal, find a basis of the kernel of $p(T)^k$ where k is the exponent of p in p_T. Equivalently, find a basis of the kernel of $p(T)^{\dim V}$. We will work with the space $V(p)$ in coordinates with respect to this basis.

Step 3. Find the matrix A of $T : V(p) \longrightarrow V(p)$ in the basis constructed in Step 2. Compute the matrix $B = p(A)$. Note that to find A one needs to express the image $T(v)$ of every vector in the basis from Step 2 as linear combination of vectors in this basis. Compute the powers B^2, B^3,..., $B^{M(p)} = 0$. (Note that $M(p)$ is the smallest exponent such that $B^{M(p)} = 0$ so you compute here $M(p)$ if you do not know it from steps 1-2). Compute a basis of solutions to the system $B^k x = 0$ for $k = 1, ..., M(p)$.

For each i let $V^i(p)$ be the image of $p(T)^i : V(p) \longrightarrow V(p)$ (we set $V^0(p) = V(p)$). Thus $V^i(p)$ is spanned by the columns of B^i. Note that $i = M(p)$ is the smallest integer for which $V^i(p) = \{0\}$, i.e. $B^i = 0$. The next steps of the algorithm will construct a rational canonical decomposition of $V^{M(p)-1}(p)$, then of $V^{M(p)-2}(p)$,..., and at the end we get a rational canonical decomposition of $V(p) = V^0(p)$.

Suppose that we have already found a rational canonical decomposition

$$V^k(p) =< w_1 > \oplus ... \oplus < w_t >$$

of $V^k(p)$ for some k. Let p^{d_i} be the annihilator of w_i. We are going to find a rational canonical decomposition of $V^{k-1}(p)$.

Step 4 $(M(p)-k)$**.** For each i find a vector $v_i \in V^{k-1}(p)$ such that $p(T)v_i = w_i$. You do this as follows: find a solution to the system $B^k x = w_i$ and take $v_i = B^{k-1}x$. (You may wonder why we can't simply take for v_i a solution to $Bx = w_i$; the reason is that we would not know if it belongs to $V^{k-1}(p)$.). The annihilator of v_i is p^{d_i+1}. Note that if $Bw_i \neq 0$ then in the previous step 4 $(M(p)-k-1)$ you found a vector x such that $B^{k+1}x = Bw_i$ and you can use the same x here.

It turns out that the cyclic spaces $< v_1 >$,...,$< v_t >$ form a part of a rational canonical decomposition of V^{k-1}. The missing cyclic summands are all of the form $< v >$, where the annihilator of v is p, i.e. $Bv = 0$. To find them use the basis $b_1, ..., b_r$ of $\ker p(T)^k$, i.e. a basis of solutions to the homogeneous system $B^k x = 0$ found in step 3. Compute $u_i = B^{k-1}b_i$ (these vectors span the space $V^{k-1} \cap \ker p(T)$).

b) Consider the matrix M whose columns are

$$B^{d_1-1}w_1, AB^{d_1-1}w_1, A^2B^{d_1-1}w_1, ..., A^{d-1}B^{d_1-1}w_1,$$

$$B^{d_2-1}w_2, AB^{d_2-1}w_2, A^2B^{d_2-1}w_2, ..., A^{d-1}B^{d_2-1}w_2, ...,$$

$$B^{d_t-1}w_t, AB^{d_t-1}w_t, A^2B^{d_t-1}w_t, ..., A^{d-1}B^{d_t-1}w_t,$$

$$u_1, Au_1, A^2u_1, ..., A^{d-1}u_1, u_2, Au_2, A^2u_2, ..., A^{d-1}u_2, ..., u_r, Au_r, A^2u_r, ..., A^{d-1}u_r$$

Recall that d here is the degree of p. For $d = 1$ this list of columns is particularly simple:

$$B^{d_1-1}w_1, B^{d_2-1}w_2, ..., B^{d_t-1}w_t, u_1, u_2, ..., u_r.$$

Find the row-echelon form N of this matrix. Let u_{i_1},..., u_{i_m} be those among the vectors $u_1, ..., u_r$ which correspond to pivot columns of N. Set $v_{t+j} = u_{i_m}$, $j = 1, ..., m$. Then

$$< v_1 > \oplus ... \oplus < v_t > \oplus < v_{t+1} > \oplus ... \oplus < v_{t+m} >$$

is a rational canonical decomposition of V^{k-1}.

Starting with $k = M(p)$ we repeat the Step 4 $M(p)$ times and as a result we get a rational canonical decomposition of $V(p)$.

Very important Remark. The vectors constructed by our algorithm for $V(p)$ are expressed in terms of the basis of $V(p)$ found in Step 2. This means that what we get is coordinates of the vectors in this basis. So at the end one has to express this vectors back in terms of the original basis of V.

Remark. This is not the most efficient algorithm. But it is relatively simple to describe.

Example. Let us see how the algorithm works for a linear transformation $T : \mathbb{R}^7 \longrightarrow \mathbb{R}^7$ given by the matrix

$$C = \begin{pmatrix} 1 & 1 & 5 & -2 & 2 & -3 & 1 \\ -1 & 3 & 4 & -2 & 1 & -2 & 1 \\ -2 & 2 & 9 & -3 & 3 & -4 & 1 \\ -2 & 2 & 6 & -1 & 2 & -3 & 1 \\ 0 & 0 & 1 & 0 & 3 & -1 & 1 \\ -2 & 2 & 8 & -3 & 4 & -3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Step 1. We skip the details since we discussed them earlier. We find that $q_T = (x-2)^2(x-1)$.

Step 2. We deal first with $p(x) = x - 2$. We have $M(x-2) = 2$. We compute

$$p(C)^{M(p)} = (C - 2I)^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A basis of the kernel of $p(C)^2$ is $h_1 = (1,0,0,0,0,0,0)$, $h_2 = (1,1,0,0,0,0,0)$, $h_3 = (0,0,1,0,0,0,0)$, $h_4 = (0,0,1,1,0,0,0)$, $h_5 = (0,0,0,0,1,0,0)$, $h_6 = (0,0,0,0,1,1,0)$. (We could choose a simpler basis, but to have a better illustration of the algorithm we chose note to).

Step 3. The matrix of $T : V(x-2) \longrightarrow V(x-2)$ in this basis is

$$A = \begin{pmatrix} 2 & 0 & 1 & 1 & 1 & 0 \\ -1 & 2 & 4 & 2 & 1 & -1 \\ 0 & 0 & 3 & 1 & 1 & 0 \\ -2 & 0 & 6 & 5 & 2 & -1 \\ 2 & 0 & -7 & -4 & -1 & 1 \\ -2 & 0 & 8 & 5 & 4 & 1 \end{pmatrix}$$

Thus

$$B = A - 2I = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ -1 & 0 & 4 & 2 & 1 & -1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ -2 & 0 & 6 & 3 & 2 & -1 \\ 2 & 0 & -7 & -4 & -3 & 1 \\ -2 & 0 & 8 & 5 & 4 & -1 \end{pmatrix}$$

We have $B^2 = 0$.

Step 4. We start with $V^2(x-2) = \{0\}$. We need to find a basis of solutions to $B^2 x = 0$. Since $B^2 = 0$, we see that $b_1 = (1,0,0,0,0,0)$, $b_2 = (0,1,0,0,0,0)$, $b_3 = (0,0,1,0,0,0)$, $b_4 = (0,0,0,1,0,0)$, $b_5 = (0,0,0,0,1,0)$, $b_6 = (0,0,0,0,0,1)$ is a basis of solutions. Now $u_1 = Bb_1 = (0,-1,0,-2,2,-2)$, $u_2 = Bb_2 = (0,0,0,0,0,0)$ $u_3 = Bb_3 = (1,4,1,6,-7,8)$, $u_4 = Bb_4 = (1,2,1,3,-4,5)$, $u_5 = Bb_5 = (1,1,1,2,-3,4)$, $u_6 = Bb_6 = (0,-1,0,-1,1,-1)$. Thus

$$M = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ -1 & 0 & 4 & 2 & 1 & -1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ -2 & 0 & 6 & 3 & 2 & -1 \\ 2 & 0 & -7 & -4 & -3 & 1 \\ -2 & 0 & 8 & 5 & 4 & -1 \end{pmatrix}$$

(Note that $B = M$. This is not a coincidence. Why?). The reduced row-echelon form is

$$N = \begin{pmatrix} 1 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Thus we take $v_1 = u_1 = (0, -1, 0, -2, 2, -2)$, $v_2 = u_3 = (1, 4, 1, 6, -7, 8)$ and $v_3 = u_4 = (1, 2, 1, 3, -4, 5)$ and we have a rational canonical decomposition

$$V^1(x-2) = < v_1 > \oplus < v_2 > \oplus < v_3 > .$$

Now we repeat step 4 to get a rational canonical decomposition for $V^0(x-2) = V(x-2)$. First we have to find vectors $z_1, z_2, z_3 \in V^0(x-2)$ such that $Bz_i = v_i$. Since $k = 1$ in our case, we just solve the systems $Bz_i = v_i$. For example, for $i = 1$ the system has augmented matrix

$$\begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ -1 & 0 & 4 & 2 & 1 & -1 & -1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ -2 & 0 & 6 & 3 & 2 & -1 & -2 \\ 2 & 0 & -7 & -4 & -3 & 1 & 2 \\ -2 & 0 & 8 & 5 & 4 & -1 & -2 \end{pmatrix}$$

so its reduced row echelon form is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and we may take $z_1 = (1, 0, 0, 0, 0, 0)$. Similarly, $z_2 = (0, 0, 1, 0, 0, 0)$ and $z_3 = (0, 0, 0, 1, 0, 0)$ work. According to our algorithm, $< z_1 > \oplus < z_2 > \oplus < z_3 >$ is a part of a rational canonical decomposition for $V^0(x-2)$. To find the other part (it is easy to see that in this case there is no other part, since $V^0(x-2)$ has dimension 6, but we will pretend that we do not know this to illustrate the step in the algorithm) we need to find a basis of the solutions to $B^k x = Bx = 0$. The reduced row echelon form of B is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

so $b_1 = (0,1,0,0,0,0)$, $b_2 = (1,0,1,-2,1,0)$, $b_3 = (1,0,1,-1,0,1)$ is a basis of solutions. Since $B^{k-1} = B^0 = I$, we have $u_i = b_i$ for all i so we need to row reduce the matrix with columns $B^0v_1, B^0v_2, B^0v_3, b_1, b_2, b_3$, i.e. the matrix

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 \\ -1 & 4 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ -2 & 6 & 3 & 0 & -2 & -1 \\ 2 & -7 & -4 & 0 & 1 & 0 \\ -2 & 8 & 5 & 0 & 0 & 1 \end{pmatrix}$$

The reduced row echelon form is

$$\begin{pmatrix} 1 & 0 & 0 & 3 & 4 & 2 \\ 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 1 & -2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Thus indeed there is no pivot in the columns corresponding to b_1, b_2, b_3, i.e. we do not have anything to add and $< z_1 > \oplus < z_2 > \oplus < z_3 >$ is a rational canonical decomposition of $V^0(x-2) = V(x-2)$. Now $z_1 = (1,0,0,0,0,0)$ in the basis $h_1, ..., h_6$ of $V(x-2)$. This means that $z_1 = h_1 = (1,0,0,0,0,0,0)$. Similarly $z_2 = h_3 = (0,0,1,0,0,0,0)$ and $z_3 = h_4 = (0,0,1,1,0,0,0)$ (this step is what the "very important remark" was about).

It remains to find a rational canonical decomposition of $V(x-1)$. We could repeat the whole algorithm, but instead let us observe that $V(x-1)$ is one dimensional so it must be $< v >$, where v is any non-zero vector in the kernel of $T - I$. This kernel has dimension 1 and a simple computation yields $v = (1,0,2,1,0,3,1)$. Thus we found that

$$V = < z_1 > \oplus < z_2 > \oplus < z_3 > \oplus < v >$$

is a rational canonical decomposition of V, where $z_1 = (1,0,0,0,0,0,0)$, $z_2 = (0,0,1,0,0,0,0)$, $z_3 = (0,0,1,1,0,0,0)$ and $v = (1,0,2,1,0,3,1)$.