Math 506 HW1

Rohan Mukherjee

March 30, 2024

1. If $q(x) = x + q_0$, the companion matrix is just going to be $\begin{pmatrix} -q_0 \end{pmatrix}$ who's characteristic polynomial is just $\det\begin{pmatrix} \lambda I - \begin{pmatrix} -q_0 \end{pmatrix} \end{pmatrix} = \lambda + q_0 = q(\lambda)$ as claimed. Suppose inductively that the characteristic polynomial of the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -q_0 \\ 1 & 0 & \cdots & 0 & -q_1 \\ 0 & 1 & \cdots & 0 & -q_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -q_{n-1} \end{pmatrix}$$

is $q(x) \coloneqq \sum_{i=0}^{n} q_i x^i$. Then for any $q_0, \cdots, q_n$,

$$\det\begin{pmatrix} \lambda & 0 & \cdots & 0 & q_0 \\ -1 & \lambda & \cdots & 0 & q_1 \\ 0 & -1 & \cdots & 0 & q_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & \lambda + q_n \end{pmatrix} = \lambda \det\begin{pmatrix} -1 & \lambda & \cdots & 0 & q_1 \\ 0 & -1 & \cdots & 0 & q_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & \lambda + q_n \end{pmatrix} +$$

$$q_0(-1)^{n-1} \det\begin{pmatrix} -1 & \lambda & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{pmatrix}$$

$$= \lambda \sum_{i=1}^{n} q_i \lambda^{i-1} + q_0(-1)^{2n-2} = \sum_{i=0}^{n} q_i \lambda^i$$

As desired.

2. We first prove the following lemma: Let A, B be a 3×3 matrix over a field k. Then A, B have the same minimal polynomial and same characteristic polynomial iff they are similar. Suppose that A, B are similar, i.e. $B = PAP^{-1}$ for some non-singular matrix P. Then,

$$\det(\lambda I - B) = \det\left(\lambda PP^{-1} - PAP^{-1}\right) = \det(P)\det(\lambda I - A)\det(P)^{-1} = \det(\lambda I - A)$$

which shows they have the same characteristic polynomial. On the other hand, let R be the rational canonical form for A, as prescribed by Theorem 16 in Dummit and Foote on page 477. Then $a_m = \sum_{i=0}^{n} a_i x^i$ is the largest invariant factor of R and hence the minimal polynomial of A, since we know that $A = PRP^{-1}$ for some non-singular P, then we have

$$a_m(PRP^{-1}) = \sum a_i (PRP^{-1})^i = \sum PR^i P^{-1} = P \sum R^i P^{-1} = P \cdot 0 \cdot P^{-1} = 0$$

Thus the minimal polynomial of A divides the minimal polynomial of R. Applying this result backwards shows they are equal. Since B is similar to A, it is also similar to R, which shows it also has the same minimal polynomial, completing the backward direction.

For the forward direction, notice that we have 3 cases:

(1) A has 1 invariant factor, which will be equal to the minimal polynomial. Since the characteristic polynomial is the product of all the invariant factors, the characteristic polynomial of A is equal to the minimal polynomial. This lets us say that B also has only one invariant factor, equal to A's minimal polynomial, otherwise $\det(\lambda I - B)$/minimal polynomial(B) would have degree at least 1 since invariant factors have degree at least 1, a contradiction. Thus A and B have the same invariant factors, hence they have the same RCF hence they are similar.

(2) A has 2 invariant factors, one of degree 1, and the other (the minimal polynomial) of degree 2. In this case, we can recover the other invariant factor of A by dividing it's characteristic polynomial by the minimal polynomial. Similarly, we know that the characteristic polynomial of B, equal to the characteristic polynomial of A is degree 3, and the product of all the invariant factors of A. Dividing the characteristic polynomial of B by it's minimal polynomial will yield a degree 1 factor that is a multiple of (possibly multiple) degree 1 invariant factors. Since the degrees match up it follows that this quotient is precisely another invariant factor, which shows again that A, B have the same invariant factors and hence are similar.

(3) A has 3 invariant factors. Let a_1, a_2, a_3 be the invariant factors. By the relations $a_1 \mid a_2 \mid a_3$ and since they all have degree at least 1, with degree summing to 3, we see that they are all equal. Thus the minimal polynomial is of the form $(x - \alpha)$ for some $\alpha \in k$, and the characteristic polynomial will be equal to $(x - \alpha)^3$. Since A, B have the same minimal polynomial, we can deduce that all invariant factors have degree precisely equal to 1. So we must have 3 degree-1 divisors of $(x - \alpha)^3$ being the invariant factors. There is only one choice, which shows that A, B have the same minimal polynomial and hence are similar.

The above work lets us simplify the problem to the following: the condition of being similar for 3×3 matrices is precisely equal to the condition of having the same minimal polynomial and same characteristic polynomial. So to specify an entire equivalence class, by the previous lemma, we just need to specify the minimal polynomial. Thus the number of equivalence classes for 3×3 matrices are in bijection with the number of possible minimal polynomials.

We just need to show that this number is independent of the base field $\mathbb{Q}$. Clearly, if we have at least 2 invariant factors then the characteristic polynomial has repeat roots. Recall that irreducible polynomials over $\mathbb{Q}$ do not have repeat roots. Thus if the characteristic polynomial is degree 3-irreducible there is only one choice for the minimal polynomial (equivalently, the only invariant factor) being itself. Otherwise the characteristic polynomial has repeat roots, and hence is not irreducible, so it has a linear factor $(x - \alpha)$ (being a cubic). Since the invariant factors form a tower of divisibility, we get that the characteristic polynomial is of the form $(x - \alpha)^2(x - \beta)$ for some β possibly equal to α. In this case it is clear that the number of possible minimal polynomials over any extension field is precisely equal to the number of minimal polynomials over $\mathbb{Q}$, since all divisors of this polynomial lie in $\mathbb{Q}[x]$.

For 4×4 matrices however, we can have a problem. Let $p(x) = x^2 + ax + b$ be an irreducible quadratic over $\mathbb{Q}$, and let the characteristic polynomial be $p(x)^2$. Over $\mathbb{Q}$, we can either have the minimal polynomial be $p(x)^2$, or just $p(x)$, which will both completely specify all the other invariant factors, since $p(x)$ is irreducible. However, in an algebraically closed field such as $\mathbb{C}$, factoring $p(x) = (x - \alpha)(x - \beta)$, we could have the invariant factors be $(x - \alpha)$ and $(x - \alpha)(x - \beta)^2$, which did not exist over $\mathbb{Q}$, and would specify a new equivalence class.

3. We shall first prove the forward direction. Since similar matrices have the same minimal polynomial, we need only show that if D is a diagonal matrix then it's minimal polynomial has distinct linear factors. After possible re-ordering the basis

so that the same diagonal entries are in adjacent rows, D looks like the following:

$$\begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \cdots & 0 \\ 0 & 0 & a_1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_n \end{pmatrix}$$

By a result from class, the minimal polynomial of a matrix with diagonal blocks $A_1, \ldots, A_n$

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_n \end{pmatrix}$$

is just the lcm of the minimal polynomial of each A_i. Thus it suffices to show that the minimal polynomial of aI_n is $(x - a)$. This is obvious, hence we have shown the forward direction.

For the backward direction, let M be a matrix and $a_1, \ldots, a_m$ be the invariant factors (and thus a_m is the minimal polynomial). By the divisibility relations $a_1 \mid a_2 \mid \cdots \mid a_m$, it follows that every invariant factor is a product of distinct linear factors. Thus M has rational canonical form

$$\begin{pmatrix} C(a_1) & 0 & \cdots & 0 \\ 0 & C(a_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C(a_m) \end{pmatrix}$$

We need only show that if p is a polynomial with distinct linear factors then $C(p)$ is similar to a diagonal matrix. First, it is clear that the only invariant factor of $C(p)$ is just p itself (for a formal proof, p is equal to the characteristic polynomial as well). Factor $p = (x - \alpha_1) \cdots (x - \alpha_n)$. The obvious choice of the diagonal matrix is

$$\begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha_n \end{pmatrix}$$

By the same lcm result from class, the minimal polynomial of this matrix is the lcm of the minimal polynomial of the blocks (α_i), which is clearly $x - \alpha_i$. Thus the minimal polynomial is equal to the characteristic polynomial and hence this diagonal matrix has no other invariant factors, which shows that it and $C(p)$ have the same invariant factors and thus are similar, which completes the proof.

4. We have proved last quarter that if G is an abelian group and a is an element of largest order m, then for every element $b \in G$, $|b| \mid |a|$. Let k be a field and $G \leq k^\times$, where $|G|$ is finite. Let a be the element of largest order. Since $|b| \mid |a|$ for every other element $b \in G$, we have $|G|$ solutions to the equation

$$x^{|a|} - 1 = 0$$

Since k is a field, this equation has $\leq |a|$ solutions. Putting these two facts together shows that $|G| = |a|$ thus $|G|$ is cyclic. Since $\mathbb{F}_q$ is a finite field, $\mathbb{F}_q^\times$ is cyclic with generator x. It then follows immediately that $\mathbb{F}_p(x) = \mathbb{F}_q$, since powers of x make up all (but 0) of $\mathbb{F}_q$. Thus the minimal polynomial of x has degree n, which we shall call $f \in \mathbb{F}_p[y]$. Indeed by a result in class we have that multiplication by x on $\mathbb{F}_q \cong \mathbb{F}_p^n$ is $C(f)^t$ w.r.t. some basis by a result in class. We shall show that those vectors are well-defined in the sense that the bottom $n-1$ entries of the last column of M^i is the same as the first $n-1$ entries of the last column of M^{i+1}. Notice that this statement is implied by showing that the rows of M^i move up in M^{i+1}. This is equivalent to showing the columns move left from $C(f)^i$ to $C(f)^{i+1}$. This is true by observing how x acts: $x^{i+1}x^j = x^i x^{j+1}$ for each i and $0 \leq j \leq n-1$ (recall our basis for $C(f)$ is $1, \ldots, x^{n-1}$). First notice that $x^{q-n}x^{n-1} = x^{q-1} = 1$, so the last column of $C(f)^{q-n}$ is just $(1, 0, \ldots, 0)^t$, and in particular the last entry of the last column is 0, so we have a sequence of n 0s when we wrap around.

We shall complete the proof by showing that $(M^i v^t)^t$ is not equal to $(M^j v^t)^t$ for $0 \leq j < i < q-1$. Suppose otherwise, then we would have the last column of M^i equaling the last column of M^j. We see then that the last column of $M^i - M^j$ is the zero vector, and in particular $M^i - M^j$ is non-invertible. However, this linear transformation is equivalent to multiplication by $x^i - x^j$, and since $i \neq j$, and since $0 \leq i, j < q-1$, by order considerations we must have $x^i \neq x^j$. Then $x^i - x^j$ is a non-zero element of a field and hence it is invertible (thus the linear transformation corresponding to it is also invertible), a contradiction.

We temporarily forget about a_{q-1}. We have then produced a sequence $a_0, \ldots, a_{q-2}$ by

taking the transpose of the column vector $M^i v^t$ for $0 \leq i < q - n - 1$. The powers of the matrices take place mod $q - 1$, since the matrix M have order $q - 1$. In particular the first $n - 1$ columns of $M \cdot M^{q-2} = I$ are the last $n - 1$ columns of M^{q-2}. Thus our sequence wraps around in the correct way, and the $q - 1$ distinct subsequences that these powers give us all show up in the generated sequence (when forgetting about a_{q-1}). Since the only powers of M that wrap are for $i = q - n + 1$ to $i = q - 2$, we can see that all of those would have all of their last row entries as 0. In particular, if we add a 0 to our sequence, all of these sequences still exist and remain the same. Thus by declaring $a_{q-1} = 0$ we have preserved all $q - 1$ sequences, none of which are 0 because none of the powers M^i for $0 \leq i < q - 1$ are equivalently 0. Our final sequence, 00...0 results by taking $a_{q-1}, a_0, \ldots, a_{n-2}$, by construction, giving us all $q = p^n$ sequences, which completes the proof.