01:XXX:XXX - Homework n

Pranav Tikkawar

December 25, 2024

Contents

1 Content

IN CLASS BE an expert on HW Problems:
Know little and big theorems

Look at lecture 13!
How to do RREF theory without replacement theorem
It was in 2 stages: First prove corollary 2(a)(b)(c). Then find a linear transofrmation to show that F^n is isomorsphic to V and then use the replacement theorem to show that V is finite dimensional.

This could be asked on the exam.

To prove Theorem 2.6 Do uniquemeness first:

Proof. Assume $T : V \to W$ is a lin transformation.
if $\exists T(v_i) = w_i$ for all i.
Then $\forall a_i \in F$
$T(a_1v_1 + \cdots + a_nv_n) = a_1w_1 + \cdots + a_nw_n$

$\square$

IE if T exists then it is unique.
Then do existence:

Proof. Let $x \in V$
$x = a_1v_1 + \cdots + a_nv_n$
Define $T : V \to W$ by $T(x) = a_1w_1 + \cdots + a_nw_n$
T is linear since $T(x + y) = T(x) + T(y)$ and $T(cx) = cT(x)$
$T(v_i) = w_i$ for all i

$\square$

Know all proofs in Chapter 6 Especialy gram schmidt Theorem 6.1: Let V be an inner product space. then for all $x, y, z \in V$ and $c \in F$ we have

- $< x, y + z >=< x, y > + < x, z >$
- $< x, cy >= \bar{c} < x, y >$
- $< 0, x >=< x, 0 >= 0$
- $< x, x >= 0$ if and only if $x = 0$
- if $< x, y >=< x, z >$ then $y = z$

Theorem 6.2 Theorem 6.3: $S = \{v_1...v_k\}$ and an orthogonal set of non zero vectors. For all $y \in span(S)$ we have $y = \sum_{i=1}^{k} \frac{<y,v_i>}{<v_i,v_i>} v_i$

- Sec. 2.5:
- Chapter 3:
- Chapter 4:
- Chapter 5:
- Chapter 7:

Cayley hamilton:
Replacement Theorem:
3 "brain teasers":

- Puzzle #1: Must similar matrices have the same RREF? In class I said the answer is no. Can you find a 2x2 counterexample and prove that it really is a counterexample?
- Puzzle #2 (new; a converse question): Must row-equivalent matrices be similar? Try to prove or find a 2x2 counterexample.
- Puzzle #3: Suppose that $F = \mathbb{F}_2$ instead of $\mathbb{R}$. Again, exactly as above, $e_1 + e_2$ and $e_1 - e_2$ are eigenvectors for A with eigenvalues 1 and -1, respectively, and so, again, A is similar to the diagonal matrix with diagonal entries 1 and -1. But in $\mathbb{F}_2$, $-1 = 1$, so A is similar to the identity matrix. But the only matrix similar to the identity matrix is of course the identity matrix, so A *can't* be similar to the identity matrix. That was the weird conclusion (contradiction) that we "derived" in class. Where was the fallacy in this argument? And, also, *is* A diagonalizable or not over $\mathbb{F}_2$? elements e_2 and e_1 of R^2):

Note: The following are 100% on the exam
Formulate and then prove the Replacement Theorem (for a vector space V over a field F).

Formulate and then prove the Cayley-Hamilton Theorem (for a linear operator T on an n-dimensional vector space V over a field F). When you need to invoke theorems in your proof, clearly state such theorems and give a very brief sketch of the proof of each of them. (Theorems 5.20 and 5.21)

The following are possible on the exam

Formulate and prove a theorem that asserts that the reduced row echelon form of a given mxn matrix over a field F is unique. (Do not spend time defining RREF or "row-equivalence of matrices" or "pivot columns." Use such concepts in your proof as appropriate.)
(For this, you'll need to use the Column Correspondence Principle. In your answer, state it clearly and sketch its proof. Also, formulate your proof of uniqueness very concisely, showing me that you understand the mechanism of the proof.)

Prove that in F^n, every finite linearly independent set has at most n elements, and if it has exactly n elements, then it is a basis of F^n. Do not use the Replacement Theorem in your proof.

Prove that in F^n, every finite spanning set has at least n elements, and if it has exactly n elements, then it is a basis of F^n. Do not use the Replacement Theorem in your proof. (Of course, these are the proofs on page 11 of my Lecture 13 notes.)

Helpful comments:
Needed theoresms:

- 1.9 (pg 45): If a vector space V is generated by a finite set S, then some subset of S is a basis for V. Hence V has a finite basis
- 1.10 (pg 46): Replacement Theorem
- Cayley Hamilton Theorem (5.20)
- Corolary 1 of 1.10 (pg 47): Let V be a vs with a finite basis. Then all bases for V are finite and ever vasis for V contains the same number of vectors.
- Corollary 2(a,b,c) (pg 48) Let V be a n dimensional vectorspace
  (a) Any finite generating set for V containss at least n vectors and a genering set for V with exaclty n vectors is a basis for V
  (b) Any linearly independent subset of V that contains n vectors is a basis for V
  (c) Every linearly independant subset of V can be extended to a basis for V that is if L is a LI subest of V then there is a basis β of V such that $L \subseteq \beta$
- Proofs on RREF theorey and sameresluts for the special case where $V = F^n$
- Theorem 1 and 2 near end of 13 notes:
  - 1: In F^n every finite linealey independant set has at most n elements and if it has exactly n elements then it is a basis of F^n
  - 2: In F^n every finite spanning set has at least n elements and if it has exactly n elements then it is a basis of F^n
- RREF being unique ***(11/10/2024 announcement)
- 1.11 (pg 50) Need to know proof: Let W be a subspace of finite-dimentsional vector space V. Then W is finite-dimensional and $\dim(W) \leq \dim(V)$ Moreover, if $\dim(W) = \dim(V)$ then $W = V$.
- 2.2 (pg 68) no proof neededed but need to know: Let V and W be Vector spaces and T be a linear transformation from V to W. Then the null space of T is a subspace of V and the range of T is a subspace of W.

- 2.3 (pg 70) Fundamental dimanesion thom (read proof): Let V and W be vector spaces and T be a linear transformation from V to W. If V is finite dimensional then $Rank(T) + Nullity(T) = dim(V)$

- 2.6 and corollary (pg 73) talk on minday: Let V and W be be vector spaces over F and suppose that $\{v_i\}_n$ is a basis for V. For $w_1, \ldots w_n \in W$ exists a unique linear transformation $T : V \to W$ such that $T(v_i) = w_i$ for $i = 1, \ldots n$.

- 2.11 (pg 89) super imp but read proof: Let V, W and Z be vector spaces over F and with bases α, β, γ respectively. Let $T : V \to W$ and $U : W \to Z$ be linear transformations. Then $[UT]^\gamma_\alpha = [U]^\gamma_\beta [T]^\beta_\alpha$

- 2.14 (pg 92) super imp but read proof: Let V and W be finite dimentiosnl vector spaces having ordered bases β and γ respectivly and let $T : V \to W$ be a linear transformation then $\forall x \in V$ $[T(x)]_\gamma = [T]^\gamma_\beta [x]_\beta$

Note for Corollary 1 and 2:

This can be generalized to any vector space V of dimension n by taking a unique linear transformation T from V to F^n. Then T is a linear isomorphism since it takes a basis to a basis which implies that it is onto with null space $\{0\}$. Its inverse is also a linear transformation and onto. Now, any linear isomorphism takes any spanning set to a spanning set and also takes any linearly independent set to a linearly independent set (which follows from the fact that the null space of the linear isomorphism is $\{0\}$), so these properties hold for both T and T^{-1}. We will need to use these properties of T^{-1} because we will need that T^{-1} applied to any basis of F^n is a basis of V.

To prove Theorem 1 for V, given a finite linearly independent set, its image under T is also linearly independent, so it has at most n elements by Theorem 1 above. If it has exactly n elements, then its image under T is a basis of F^n by Theorem 1 above, and so the set itself is a basis of V since T^{-1} applied to a basis is a basis.

To prove Theorem 2 for V, given a finite spanning set in V, its image under T spans F^n, so it has at least n elements by Theorem 2 above. If it has n elements, then its image under T is a basis of F^n by Theorem 2 above, and so the set itself is a basis of V (for the same reason as above). This proves both of the theorems for V.

To prove the corollary for V, combine Theorems 1 and 2 for V. (Or, one can directly invoke the corollary for F^n: Given a finite basis of V, its image under T is a finite basis of F^n and so it has n elements.)

2 Review

2.1 Proof of content (helpful info) that needs to be known

2.1.1 1.9

If a vector space V is generated by a finite set S, then some subset of S is a basis for V. Hence V has a finite basis.

Proof. If $S = \emptyset$ or $= \{0\}$ then $V = \{0\}$ and the empty set is a basis for V.
Otherwise S contains a non-zero vector u_1. This element itself is obviously LI. now choosing $u_2 ... u_k$ wuch that $u_1, \dots u_k$ is LI. Since S is a finit set we can contune this process until we have a basis for V.
This can happen untill $\beta = S$ and we have generating set of V and a LI set of V which implies this is a basis for V.
If the sey β is a proper subset of S such that $\beta\cup$ any other element of S is not LI then β is our desired subset of S
Clealry β is LI by contruction we only need to show that β generates V.
Let $v \in S$. If $v \in span(\beta)$ then we are done. If $v \notin span(\beta)$ then v is a linear combination of β and some $u_i \in S$.but we have seen that for that u_i with β is linearly dependant thus $v \in span(\beta)$

$\square$

Notes

The proof of this is kinda shakey but intuitively uses the idea of choosing the Longest LI chain of vectors in S then showing that this is a basis for V. as any vector in S is a LC of vectors of the basis and since we know S generates V we can see that the basis generates V.

2.1.2 1.10

READ THE PROBLEMS PROOFS:
Notes:
This essentially is a proof by induction on the size of the Linearly independent set. We see that we can replace any element of the generating set with an element of the linearly independent set to get a new generating set. This is done by isolating the element of the linearly independent set in the span of the generating set and then replacing it with the element of the generating set. This is done by induction on the size of the linearly independent set.

2.1.3 Cayley Hamilton Theorem

READ THE PROBLEMS PROOFS:
Notes:
This is done by using the $T-cyclic$ subspaces of V. If W is the $T-cyclic$ subspace generated by v then we can see that the characteristic polynomial of T_W divides the characteristic polynomial of T. Since T_W satisfies its characteristic polynomial we can see that T satisfies its characteristic polynomial.

2.1.4 Corollary 1 of 1.10

Let V be a VS with a finite basis. Then all bases for V are finite and every basis for V contains the same number of vectors.

Proof. Suppose a basis β of size n for V and another basis γ for V of size m. If γ has more than n vectors. There we can select a subset S of γ of size $n+1$. Since S is LI and β generates V the replacment theorem tells us this is a contratdiction as $n+1$ is not less than n
Therefore gamma is finite has at least the numbers of vectors in β.
Now if we reverse the roles of β and γ we can see that β has at least the number of vectors in γ
Thus $m = n$ and all bases for V have the same number of vectors. □

Notes:
This is a simple proof that employs the fact the size of a basis is bounded above and below by the number of longest LI chain of vectors in V.

2.1.5 Corollary 2(a,b,c)

Let V be a n dimensional vectorspace

(a) Any finite generating set for V containss at least n vectors and a genering set for V with exaclty n vectors is a basis for V

(b) Any linearly independent subset of V that contains n vectors is a basis for V

(c) Every linearly independant subset of V can be extended to a basis for V that is if L is a LI subest of V then there is a basis β of V such that $L \subseteq \beta$

Proof. Let β be a basis for V and let G be a generating set for V.

(a) We know that a subset H of G must be a basis for V and thus H must have n vectors by corollary 1 of 1.9. Thus G must have at least n vectors. Moreover if G has exactly n vectors then $H = G$ and G is a basis for V.

(b) Let L be a LI subset of V with n vectors. By the replacement theorem we can see that there is a subset of H of β containing $n - n$ vectors such that $L \cup H$ is a generating set for V. Thus $H = \emptyset$ and L generates V and is LI and thus a basis for V.

(c) IF L is a LI subset of V containing m vectors then by the replacement theorem we can see that there is a subset H of β containing $n - m$ vectors such that $L \cup H$ is a generating set for V. Thus L can be extended to a basis for V.

□

Notes:
(a) is kinda trivial as we know the dimension of V is n and thus any generating set must have at least n vectors and n vectors is a basis for V.
(b) is a direct application of the replacement theorem. with $m = n$ and thus $H = \emptyset$
(c) is a direct application of the replacement theorem.with $m < n$ and thus H is a subset of β that extends L to a basis for V

2.1.6 Proof of Theorem 1 and 2 near end of 13 notes

- 1: In F^n every finite linearly independent set has at most n elements and if it has exactly n elements then it is a basis of F^n
- 2: In F^n every finite spanning set has at least n elements and if it has exactly n elements then it is a basis of F^n

Proof. Let the VS be F^n

- 1
  Let the set $\{v_1, \dots v_k\}$ be a finite LI set in F^n.
  Let the vectors form the matrix $A = \begin{bmatrix} v_1 & \dots & v_k \end{bmatrix}$
  Let $R = rref(A)$. by CCP we can see the coumns of R are LI.
  Thus $R(x) = 0$ has no nontrivial columns and the nullity of R (and in turn A) is 0.
  Thus R must be $\begin{bmatrix} I_R \\ O \end{bmatrix}$ Thus $k \leq n$
  If $k = n$, there are no zero rows, and thus R is the identity matrix and thus A is a basis for F^n since rank of A is n and the columns of A span F^n and is LI.

- 2
  Let the set $\{v_1, \dots v_k\}$ be a finite spanning set in F^n.
  Let the vectors form the matrix $A = \begin{bmatrix} v_1 & \dots & v_k \end{bmatrix}$
  Let $R = rref(A)$. by CCP we can see the coulmns of R are LI.
  We know that $Ax = b \implies Rx = c$ for some $b \in F^n$ and $c \in F^n$
  Since R cannot have any 0 rows, it must be that $rank(A) = rank(R) = n$ an thus $k \geq n$
  If $k = n$, $R = I_n$ and thus the rank is n and the columns are LI by ccp and thus A is a basis for F^n

□

Notes:

2.1.7 RREF being unique

Prove that for any mxn matrix over a field F, the reduced row echelon form is unique.

Proof. We can suppose that A has 2 RREFs R and S.
We need to show that $R = S$
In other words for each of the n columns of R and S we need to show that the columns are equal $r_i = s_i$
We can do this by induction on the number of columns.

For the base case of $n = 1$.
$r_1 = 0 \iff s_1 = 0$ since $\{0\}$ is a linearly dependant set and a nonzero column vector is linearly independant.

Then if $r_1 \neq 0$ then it must be $\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ since R is in RREF.

similar for s_1
Thus clealry $r_1 = s_1$
Now for the inductive hypothesis we can assume that

$$r_1 = s_1, \dots r_{j-1} = s_{j-1}$$

We need to show that $r_j = s_j$
We can denote the the k piviot columns of R and S up to j as $r_{p_1}, \dots r_{p_k}$ and $s_{p_1}, \dots s_{p_k}$
r_j is either a LC of prior pivot columns or is a pivot column itself.

If r_j is a pivot column then it is the j^{th} pivot column and thus $r_j = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}$ and similar for s_j

since it is row equivalent to R
If r_j is a LC of prior pivot columns then it is a linear combination of the pivot columns of R given by $\sum_{i=1}^{k} c_i r_{p_i}$ for some $c_i \in F$
Since $r_{p_1}, \dots r_{p_k}$ are the pivot columns of S we can see that r_j is a linear combination of the pivot columns of S and thus $r_j = s_j$
Thus $R = S$

□

Notes:
This is a fun and important proof of the uniqueness of the RREF of a matrix using CCP. This is done by induction on the number of columns of the matrix. The base case is trivial and the inductive step is done by showing that the j^{th} column of R is equal to the j^{th} column of S by showing that it is a pivot column or a linear combination of pivot columns.

2.1.8 Column Correspondence Principle

Proof. *** □

Notes:

2.1.9 1.11 (pg 50)

Let W be a subspace of finite-dimentsional vector space V. Then W is finite-dimensional and $\dim(W) \leq \dim(V)$ Moreover, if $\dim(W) = \dim(V)$ then $W = V$.

Proof. Let $n = \dim(V)$ and let $\beta = \{v_1, \dots v_n\}$ be a basis for V.
Then β generates V and thus β generates W.
If $W = \{0\}$ then $\dim(W) = 0$ and we are done.
If $W \neq \{0\}$ then there exists a non-zero vector $w_1 \in W$.
We can write w_1 as a linear combination of the vectors in β.
If we take the longest LI chain in W we can see that this chain has at most n vectors and the length of this chain is the dimension of W.
Thus $\dim(W) \leq n = \dim(V)$
If $\dim(W) = \dim(V)$ then the longest LI chain in W has n vectors and thus is a basis for W by the replacement theorem. $\square$

Notes:
This is actually such a cute little proof that is super trivial. This essentially takes the Longest LI chain in W and shows it is bouned above by the dimension of V. If the dimension of W is equal to the dimension of V then the longest LI chain in W is a basis for W by coronry 2 of 1.10.

2.1.10 2.2 (pg 68)

Let V and W be Vector spaces and T be a linear transformation from V to W. Then the null space of T is a subspace of V and the range of T is a subspace of W.

Proof. We can let 0_V be the zero vector in V and 0_W be the zero vector in W.
Since $T(0_V) = 0_W$ we can see that $0_V \in N(T)$.
let $u, v \in N(T)$ and $c \in F$.
Then $T(u) = 0_W$ and $T(v) = 0_W$
Thus $T(u + v) = T(u) + T(v) = 0_W + 0_W = 0_W$
$T(cu) = cT(u) = c0_W = 0_W$
Thus $N(T)$ is a subspace of V.
Since $T(0_V) = 0_W$ we can see that $0_W \in R(T)$.
Let $w_1, w_2 \in R(T)$ and $c \in F$.
Then $\exists u_1, u_2 \in V$ such that $T(u_1) = w_1$ and $T(u_2) = w_2$
Thus $T(u_1 + u_2) = T(u_1) + T(u_2) = w_1 + w_2$
$T(cu_1) = cT(u_1) = cw_1$
Thus $R(T)$ is a subspace of W. $\square$

Notes:
This is a super trivial proof applying the definition of a subspace.
1) 0 is in subspace

2) Closed under addition
3) Closed under scalar multiplication

2.1.11 2.3 (pg 70)

Fundamental Dimension Theorem
Let V and W be vector spaces and T be a linear transformation from V to W.
If V is finite dimensional then $Rank(T) + Nullity(T) = dim(V)$

Proof. Suppose $dim(V) = n$. We can consider $dim(N(t)) = k < n$ with a basis $\gamma = \{u_1, \dots u_k\}$ for $N(T)$
We can see that γ extends to a basis β for V by the replacement theorem.
We will deonote the extension of γ by $\{u_1, \dots u_k, v_{k+1}, \dots v_n\}$
We can see that $\alpha = \{T(v_{k+1}), \dots T(v_n)\}$ is a basis for $R(T)$
Now to prove that α is a basis for $R(T)$ we need to show that it is LI and generates $R(T)$.
It is clearly LI by contruction since it is a subset of another LI set.
We known by theorem 2.2 that $R(T)$ is a subspace of W and thus α generates $R(T)$.
Thus $dim(R(T)) = n - k$
Thus $Rank(T) = n - k$ and $Nullity(T) = k$
Thus $Rank(T) + Nullity(T) = n$

□

Notes:
This is a pretty simple proof that uses the replacement theorem to extend a basis of the null space to a basis of the vector space. Then we can see that the basis of the range is the image of the basis of the vector space under T. This is a basis for the range and thus we can see that the rank of T is the dimension of the range and the nullity of T is the dimension of the null space.

2.1.12 2.6 and corollary (pg 73)

Let V and W be be vector spaces over F and suppose that $\{v_i\}_n$ is a basis for V. For $w_1, \dots w_n \in W$ exists a unique linear transformation $T : V \to W$ such that $T(v_i) = w_i$ for $i = 1, \dots n$.

Proof. Let $x \in V$. then

$$x = a_1 v_1 + \cdots + a_n v_n$$

Let $T : V \to W$ be $T(x) = a_1 w_1 + \cdots + a_n w_n$
T is linear since for $x, y \in V$ and $c \in F$ we have

$$T(x + y) = T(a_1 v_1 + \cdots + a_n v_n + b_1 v_1 + \cdots + b_n v_n) = T((a_1 + b_1)v_1 + \cdots + (a_n + b_n)v_n)$$

$= (a_1 + b_1)w_1 + \cdots + (a_n + b_n)w_n = a_1w_1 + \cdots + a_nw_n + b_1w_1 + \cdots + b_nw_n = T(x) + T(y)$

$T(cx) = T(c(a_1v_1+\cdots+a_nv_n)) = T(ca_1v_1+\cdots+ca_nv_n) = ca_1w_1+\cdots+ca_nw_n = c(a_1w_1+\cdots+a_nw_n) = cT(x)$

Thus T is linear and $T(v_i) = w_i$ for $i = 1, \dots n$
To show uniqueness suppose there exists another linear transformation $S : V \to W$ such that $S(v_i) = w_i$ for $i = 1, \dots n$
Then $S(x) = S(a_1v_1 + \cdots + a_nv_n) = a_1S(v_1) + \cdots + a_nS(v_n) = a_1w_1 + \cdots + a_nw_n = T(x)$
Thus $S = T$ and T is unique.

$\square$

Notes:
This is a super simple proof that shows that we can define a linear transformation by its action on a basis. This is done by defining the linear transformation on the basis and then extending it linearly to the entire vector space. This is a unique linear transformation.

2.1.13 2.11 (pg 89)

Let V, W and Z be vector spaces over F and with bases α, β, γ respectively. Let $T : V \to W$ and $U : W \to Z$ be linear transformations. Then

$$[UT]_\alpha^\gamma = [U]_\beta^\gamma [T]_\alpha^\beta$$

Proof. $\square$

Notes:
This is essentially asking us to see that taking the transformation from alpha to beta to gamma is the same as the one from alpha to gamma. This is done by taking the matrix of the transformation from alpha to beta and the transformation from beta to gamma and multiplying them to get the transformation from alpha to gamma.

2.1.14 2.14 (pg 92)

Let V and W be finite dimentiosnl vector spaces having ordered bases β and γ respectivly and let $T : V \to W$ be a linear transformation then $\forall x \in V$

$$[T(x)]_\gamma = [T]_\beta^\gamma [x]_\beta$$

Proof. $\square$

Notes:
This is essentially asking us to see that the matrix of the transformation applied to a vector is the same as the transformation applied to the matrix of the vector. This is done by taking the matrix of the transformation and multiplying it by the matrix of the vector.

2.1.15 Brain Teaser 1

Must similar matrices have the same RREF? In class I said the answer is no. Can you find a 2x2 counterexample and prove that it really is a counterexample?

Proof. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$

We can see that A and B are similar as $B = PAP^{-1}$ where $P = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

We can see that the RREF of A is A and the RREF of B is B and thus similar matrices do not have the same RREF.

□

2.1.16 Brain Teaser 2

Must row-equivalent matrices be similar? Try to prove or find a 2x2 counterexample.

Proof. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$

We can see that A and B are row equivalent as $B = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

We can see that A and B are not similar as A is diagonalizable and B is not.

□

2.1.17 Brain Teaser 3

Suppose that $F = \mathbb{F}_2$ instead of $\mathbb{R}$. Again, exactly as above, $e_1 + e_2$ and $e_1 - e_2$ are eigenvectors for A with eigenvalues 1 and -1, respectively, and so, again, A is similar to the diagonal matrix with diagonal entries 1 and -1. But in $\mathbb{F}_2$, $-1 = 1$, so A is similar to the identity matrix. But the only matrix similar to the identity matrix is of course the identity matrix, so A *can't* be similar to the identity matrix. That was the weird conclusion (contradiction) that we "derived" in class. Where was the fallacy in this argument? And, also, *is* A diagonalizable or not over $\mathbb{F}_2$?

Proof. We can see that the reason why that A is not diagonalizable is that the eigenvalues of A are remepated with multiplitiy two, but the eigenspace is of dimension one since the only eigenvector of A is

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} - \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

and the only eigenvector of A is $e_1 + e_2$

Thus A is not diagonalizable over $\mathbb{F}_2$

and thus it is not similar to the identity matrix.

□

3 Problems

1. Formulate then prove the Replacement Theoroem for a vector space V over a field F.

Solution: The Replacement Theorem (1.10) states the following:

Theorem 1. *Let V be a vector space over a field F by generated by a generating set G containing n vectors and let L be a linearly independent subset of V containing $m < n$ vectors. Then there exists a subset H of G containing $n - m$ vectors such that $L \cup H$ is a generating set for V.*

In other words this is saying that if we have a linearly independent set of vectors in a vector space, we can replace some of the vectors in the generating set with vectors from the linearly independent set to get a new generating set.

Proof. Let V be a vector space over a fiel F. Let G be a generating set for V of size n and let L be a linearly independent subset of V of size $m < n$.
Proof by induction on m.
Base Case: If $m = 0$ then $L = \emptyset$ and if we take $H = G$ then $L \cup H = G$ is a generating set for V.
Inductive Hypothesis: Assume that the theorem holds for all linearly independent sets of size m.
Inductive Step: Let L be a linearly independent set of size $m + 1$. Let $L = \{v_1, \ldots v_{m+1}\}$. Then $L' = \{v_1, \ldots v_m\}$ is a linearly independent set of size m.
By the inductive hypothesis, there exists a subset H' of G containing $n - m$ vectors such that $L' \cup H'$ is a generating set for V. Let $H' = \{u_1, \ldots u_{n-m}\}$.
Since $L' \cup H'$ is a generating set for V, there exists a linear combination of the vectors in $L' \cup H'$ that equals v_{m+1}. Let $v_{m+1} = a_1v_1 + \cdots + a_mv_m + b_1u_1 + \cdots + b_{n-m}u_{n-m}$.
We must have $n > m$ and there exists a non-zero b_i otherwise the set L' would not be linearly independent.
TThen we can isolate a u_i with a non zero coefficient b_i (WLOG let it be u_1) to see that $u_1 = b_1^{-1}(v_{m+1} - a_1v_1 - \cdots - a_mv_m - b_2u_2 - \cdots - b_{n-m}u_{n-m})$.
We can see that if we take $H = H' \setminus \{u_1\}$ we satisfy $L \cup H$ being a generating set for V.
This is clear as $u_1 \in span(L \cup H)$, $span(L' \cup H') \subseteq span(L \cup H)$ and $v_{m+1} \in span(L \cup H)$.
Thus by induction, the theorem holds for all m and we can replace vectors in the generating set with vectors from the linearly independent set to get a new generating set. $\square$

Think of the mechanics of this proof literally being a replacment in an induciton. We know that the one element $v_{m+1} \in L$ can be replaced by an element of H to get a LI set of vectors for V.

2. Formulate then prove the Cayley-Hamilton Theorem for a linear operator T on an n-dimensional vector space V over a field F.

Solution: Let T be a linear operator on an n-dimensional vector space V over a field F. Let $f(t)$ be the characteristic polynomial of T
Then $f(T) = T_0$ where T_0 is the zero operator.
In other words T satisfies its characteristic polynomial.

Proof. We need to prove that $f(T) = T_0$ where T_0 is the zero operator.
IE $f(T)(v) = 0$ for all $v \in V$.
if $v = 0$ then $f(T)(0) = 0$ trivially
If $v \neq 0$
Let W be a $T - cyclic$ subspace of V generated by v of dimension k.
Let $\gamma = \{v, Tv, T^2v, \dots, T^{k-1}v\}$ be a basis for W.
We can see that $a_0 + a_1T + \cdots + a_{k-1}T^{k-1} + T^k = 0$ for all $v \in W$ Let $g(t)$ be the characteristic polynomial of T_W.
Then $g(t) = a_0 + a_1t + \cdots + a_{k-1}t^{k-1} + t^k$
We see that $g(T)(v) = 0$ for all $v \in W$
We know that $g(t)$ divides $f(t)$ and thus $\exists q(t)$ such that $f(t) = q(t)g(t)$
Then $f(T)(v) = q(T)g(T)(v) = 0$ for all $v \in W$

□

This uses the idea of T-cyclic subspaces. Since the t-cyclic subspace is generated by v and T acts on v to get Tv and so on, we can get a final T^k to be a Linear combination of the prior terms. This mirrors the characteristic polynomial of T_W and since it is a restriction of T we can see that the CP of T_W divides the CP of T. Since cp of T_W is satisfied by T we can see that the CP of T is satisfied by T.