Math 122 / Problem Set 4 Solution

By Tien Anh Nguyen - based on solutions by Corina Pătraşcu

Problem 1

We need to prove that the *hermitian* matrices form a vector subspace of the vector spaces of complex matrices with real multiplication Utilizing the notation used in the question, we have :
if A and B are *hermitian* matrices, and $A + B = C$ then $c_{ji} = a_{ji} + b_{ji} = \overline{a_{ij}} + \overline{b_{ij}} = \overline{a_{ij} + b_{ij}} = \overline{c_{ij}}$, thus C is also hermitian and the space is closed under addition
Similarly, for $\alpha \in \mathbb{R}$, if $\alpha A = B$, then $b_{ij} = \overline{b}_{ji} = \overline{\alpha a_{ji}} = \alpha \overline{a_{ji}} = \alpha a_{ij}$ (as $\alpha \in \mathbb{R}$ The zero matrix $\{a_{ij}\} = 0$ is obviously *hermitian*, and thus we have shown that they form a subspace.
Now, to formalize the symmetry across the diagonal of the elements in a *hermitian* matrix, we write down the following set of nxn matrices:
$A_{\alpha,\beta}$ with entries a_{ij} such that

$$a_{ij} = \begin{cases} 1, \text{if } \{\alpha,\beta\} = \{i,j\} \\ 0, \text{otherwise} \end{cases}$$

for every $1 \leq \alpha \leq \beta \leq n$
$B_{\alpha,\beta}$ with entries b_{ij} such that

$$b_{ij} = \begin{cases} \sqrt{-1}, \text{if } \{\alpha,\beta\} = \{i,j\} \\ -\sqrt{-1}, \text{if } \{\alpha,\beta\} = \{j,i\} \\ 0, \text{otherwise} \end{cases}$$

for every $1 \leq \alpha < \beta \leq n$ (We are not counting the matrices with $\pm i$ on the diagonal because as $a_{ii} = \overline{a_{ii}}, a_{ii} \in \mathbb{R}$)
Because these matrices form a subset of the standard basis of the vector space of complex matrices $\mathbb{M}_n(\mathbb{C})$, they are independent as well. They span our subspace and there are exactly $n(n+1)/2 + n(n-1)/2 = n^2$ such matrices, therefore the dimension of the space is n^2.

Problem 2

(a) Since W is a finite dimensional subspace of V, we can find a finite basis $\{w_1, w_2, \ldots, w_m\}$. By result in class, we can extend this basis to a basis $\{w_1, \ldots, w_n\}$ for V where V has dimension n. Now let $U = \text{span}\{w_{m+1}, \ldots, w_n\}$. Since w_i are all independent, $U \cap W = \{0\}$. At the same time, by virtue of $\{w_i\}$ being the basis of $V, U + W = V$.
(b) By proposition 3.6.9 in Artin, we have:
dim($U + W$) = dim(U) +dim(W) - dim($U \cap W$) , then it follows that if there were such a subspace U, then dim($U + W$) =dim(U) + dim(W) $>$ dim(V) which is impossible because any vector in $U + W$ is also a vector in V, and thus $U + W \subset V$.

Problem 3

Let A be a matrix with columns $\{v_1, \dots, v_n\}$, A is then the matrix of a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$

Now for any $v = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n, Av = A(x_1, x_2, \dots, x_n)^t = x_1v_1 + x_2v_2 + \cdots + x_nv_n$, thus if $\{v_i\}$ are independent, the only solution to $Av = 0$ is $v = 0$, thus ker$A = \{0\}$, and dim(img$A$) = dim(span of columns of A) = n = dim($\mathbb{R}^n$), and thus A is both onto and injective, and hence is invertible.

Now if A is invertible, it means that ker(A) = $\{0\}$ and by a similar argument, the columns $\{v_i\}$ of A have to be linearly independent.

* General comments: While most people got this problem right, the majority of the class spent a lot of time re-proving what we have done in class or failed to make use of Artin's results concerning invertibility of matrices.

Problem 4

(a) This was already done in class, and also proved in Artin. For the first vector in the basis, we have $p^2 - 1$ choices (all possible vectors except (0,0)). For the second vector, besides excluding (0,0), we need to also exclude $p - 1$ multiples of the first vector, thus we have $p^2 - p$ choices, thus we have in total $(p^2 - 1)(p^2 - p) = p^4 - p^3 - p^2 + p$ ordered bases.

(b) This is corollary **3.4.24** in Artin's. By problem 3 above, each pair of linearly independent vector forms an invertible matrix, and vice versa, thus the number of invertible matrices is the same as the number of ordered bases as we have found, which is $(p^2 - 1)(p^2 - p)$.

(c) Consider a homomorphism φ: GL$_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^*$, $\varphi(A) = detA$ (this being a homomorphism was proved in class). To check that this homomorphism is surjective, for each $a \in (\mathbb{Z}/p\mathbb{Z})^*$, just form the matrix that has columns $(a, 0), (0, 1)$, this will have determinant a and is thus invertible. The kernel of this map is all matrices with determinant 1, which is exactly SL$_2(\mathbb{Z}/p\mathbb{Z})$. Thus by the First Isomorphism Theorem, |SL$_2(\mathbb{Z}/p\mathbb{Z})$| = |GL$_2(\mathbb{Z}/p\mathbb{Z})$|/|$(\mathbb{Z}/p\mathbb{Z})^*$| = $(p^2 - 1)(p^2 - p)/(p - 1) = p^3 - p$.

(d) An easy example of an element of order p is $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.

Problem 5

The columns of the matrix for T are simply the images of the basis vectors under T: $T(1) = 0$; $T(X) = 0$; $T(X^2) = 2$, $T(X^3) = 6X$

Thus the matrix of T (with respect to this standard basis) is $\begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$

Rank(T) = 2

Some notes: Some solutions have T^t instead of T, I have given you credit only because you did the right calculation.

Problem 6

Note that every matrix $A \in M_n(\mathbb{R})$ can be written as:

$$A = \frac{A + A^t}{2} + \frac{A - A^t}{2}$$

Now $A+A^t$ is symmetric as $(A+A^t)^t = A^t+(A^t)^t = A+A^t$ and similarly, $A-A^t$ is skew-symmetric. Thus any matrix can be written as a sum of a symmetric matrix and a skew-symmetric matrix. Recall Problem 2 and Artin's proposition 3.6.5, knowing that the symmetric matrices and skew symmetric matrices form vector subspaces of $M_n(\mathbb{R})$, we just need to prove that these two subspaces only intersect at 0 to show that $M_n(\mathbb{R})$ is their direct sum.
Indeed, if A is in their intersection, then $A = A^t = -A^t$, or $A = A^t = 0$.
*General comments: Similar to problem 3, many have spent too much time proving things unnecessarily, leading to cumbersome and inelegant solutions. While writing out actual bases for the spaces is almost a sure-win strategy for this kind of problem, they also entail a lot of technicalities which you can avoid by simply using what you have proven in Problem 2 and in Artin's.

Problem 7

Over the field of scalars $\mathbb{Z}/p\mathbb{Z}$, by Artin's 3.4.15, a n-dimensional vector space is isomorphic to the space F^n of column vectors, and thus has exactly p^n elements (as for each coordinates, we have p choices). Now consider a map $T : V \to W$, we have the following formulas

$$|V| = |KerT| \cdot |ImT|$$

(when T is considered a homomorphism of groups).

$$dimV = dim(KerT) + dim(ImT)$$

(when T is considered a linear operator).
If $V, KerT, ImT$ are vector spaces of dimensions n, m, t respectively, then $|V| = p^n, |KerT| = p^m, |ImT| = p^t$, and the two formulas become:

$$p^n = p^{m+t} \text{ and } n = m + t$$

Problem 8

If $n \leq m$ the proof is trivial because the vector $\vec{v} = \vec{0}$ is always a solution.
When $n \geq m$, we consider the rank-nullity theorem on the linear operator $T : F^n \to$

F^m represented by the matrix A:

$$n = \dim(KerT) + \dim(ImT)$$

The space of solutions of $AX = 0$ is also the kernel $KerT$ of the operator T. Since $ImT \subset F^m$, $\dim(ImT) \leq m$, we have $\dim(KerT) + \dim(ImT) = n \leq \dim(KerT) + m \Rightarrow \dim(KerT) \geq n - m$.