Math 146, Winter 2008

Homework #5

Due on Wednesday, March 12.

Problem 1. Let $\mathfrak{B} = \{(1,2,4),(0,-1,1),(2,3,8)\}$ be a basis of $\mathbb{R}^3$, and consider the linear transformation $T\colon \mathbb{R}^3 \to \mathbb{R}^3$ whose standard matrix is:

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

Find the matrix $[T]_{\mathfrak{B}}$. (Recall that $[T]_{\mathfrak{B}} = [T]_{\mathfrak{B}}^{\mathfrak{B}}$.)

Let V be a dimensional vector space V over F, and $T \in \mathcal{L}(\mathbf{V})$, a linear transformation from V to V. We say that T is **triangularizable** if there exists an ordered basis $\mathfrak{B}$ of V such that $[T]_{\mathfrak{B}}$ is an upper triangular matrix, i.e,

$$[[T]_{\mathfrak{B}}]_{ij} = 0, \text{ for all } i > j.$$

The following sequence of problems is to prove the statements below. For $F = \mathbb{C}$, or more generally, any **algebraically closed field**, T is triangularizable. Moreover, under the same condition, for any two commutative linear transformation $T, U \in \mathcal{L}(V)$, i.e., $TU = UT$, they are **simultaneously triangularizable**, which means that there exists an ordered basis $\mathfrak{B}$ of V such that $[T]_{\mathfrak{B}}$ and $[U]_{\mathfrak{B}}$ are upper triangular.

In particular, for any $n \times n$ matrix $\mathbf{A} \in M_{nn}(\mathbb{C})$, there exists an invertible $n \times n$ matrix $\mathbf{Q} \in M_{nn}(\mathbb{C})$ such that $\mathbf{Q}^{-1}\mathbf{A}\mathbf{Q}$ is an upper triangular matrix. Moreover, for any two matrices $\mathbf{A}, \mathbf{B} \in M_{nn}(\mathbb{C})$, $\mathbf{AB} = \mathbf{BA}$, then there exists an invertible $n \times n$ matrix $\mathbf{Q} \in M_{nn}(\mathbb{C})$ such that both $\mathbf{Q}^{-1}\mathbf{A}\mathbf{Q}$ and $\mathbf{Q}^{-1}\mathbf{B}\mathbf{Q}$ are upper triangular matrices.

Problem 2. Let V be a vector space over F, $W \subset V$ a subspace. As we have introduced in tutorials, we can define the set V/W of equivalence classes, under the equivalence relation $\sim_W$, or $\bmod W$

$$\mathbf{x} \sim_W \mathbf{y} \iff \mathbf{x} - \mathbf{y} \in W.$$

More precisely, let $\mathbf{x} + W$ be the subset of V consisting of all vectors of the form $\mathbf{x} + \mathbf{w}$ for some $\mathbf{w} \in W$; i.e.,

$$\mathbf{x} + W = \{\mathbf{x} + \mathbf{w} | \mathbf{w} \in W\}.$$

Then V/W is the set consisting of all distinct subsets of V of the form $\mathbf{x} + W$; i.e.,

$$V/W = \big\{\mathbf{x} + W | \mathbf{x} \in V\big\}.$$

We also denote $\mathbf{x} + W = [\mathbf{x}] \bmod W$, or simply just $[\mathbf{x}]_W$ or $[\mathbf{x}]$. Define an addition and a scalar multiplication on V/W as follows: for all $\mathbf{x}, \mathbf{y} \in V$, $c \in F$,

$$(\mathbf{x} + W) + (\mathbf{y} + W) := [(\mathbf{x} + \mathbf{y}) + W], \quad c \cdot (\mathbf{x} + W) := (c\mathbf{x} + W).$$

(a) Show that V/W is a vector space under the addition and scalar multiplication defined above. This vector space is called the **quotient space** of V by W.

(b) Let V be an n-dimensional vector space over F and W an m-dimensional subspace of V. Prove that V/W is an $n - m$-dimensional vector space.

(c) Let W a subspace of V, and T a linear transformation from V to itself. We say that W is an **invariant subspace** of T, or T**-invariant** if $T(W) = \{T(\mathbf{w}) | \mathbf{w} \in W\}$ is contained in W. Let W be an invariant space of T. Show that a mapping $\tilde{T}$ from V/W to V/W defined by

$$\tilde{T}([\mathbf{v}]_W) = [T(\mathbf{v})]_W$$

is a well-defined linear transformation. This linear transformation is called the **restriction** of T on W.

Problem 3.
Let V be a vector space, $W \subset V$ a subspace, and let $q\colon V \to V/W$ be the natural linear transformation:

$$q(\mathbf{v}) = [\mathbf{v}] \bmod W$$

where $[\mathbf{v}]$ denotes the equivalence class of $\mathbf{v}$ modulo W. Let Z be a vector space, and let $T\colon V \to Z$ be a linear transformation.

(a) If $W \not\subset \ker T$, prove that there is no linear transformation $\tilde{T}\colon V/W \to Z$ such that $T = \tilde{T} \circ q$.
(b) If $W \subset \ker T$, prove that there is a linear transformation $\tilde{T}\colon V/W \to Z$ such that $T = \tilde{T} \circ q$.

Problem 4. Let V be am n-dimensional vector space over F, and $T \in \mathcal{L}(V)$, a linear transformation from V to itself. Given a polynomial $f = \sum_{i=0}^{m} a_i t^i \in P(F)$, we define

$$f(T) := \sum_{i=0}^{m} a_i T^i,$$

where $T^i = T \circ (T^{i-1})$ and $T^0 = \mathrm{id}_V$, the identity transformation on V.

(a) Show that there is a polynomial f such that $f(T)$=0. Given a bound of the degree of f. (Hint: consider the subspace H of $\mathcal{L}(V)$, generated by $\{T^i\}_{i=0,1,...}$. Warning: you are **not** allowed to use the theorem of determinant to do this and the following problems.)
(b) Let $f, g \in P(F)$. Show that

$$f(T) \circ g(T) = (f \cdot g)(T),$$

where $f \cdot g$ is the product in $P(F)$.
(c) Let $A(T)$ be a subset of $P(F)$ consisting of all polynomials f such that $f(T) = 0$. Show that $A(T)$ is a subspace of $P(F)$ with an extra property that for any $g \in P(F)$, $f \in A(T)$, $g \cdot f \in A(T)$.
(c) Let $c(T)$ be a non-zero polynomial $A(T)$ with a minimal degree. Show that for any $f \in A(T)$, $c(T)|f$; i.e., there exists $g \in P(F)$ such that $f = g \cdot c(T)$.

Problem 5. A field F is called **algebraically closed** if any non-constant polynomial $f \in P(F)$, there exists $\alpha \in F$ such that $f(\alpha) = 0$. For instance, $\mathbb{C}$ is algebraically closed, by the fundamental theorem of algebra. Let V be a vector space over a field F, and $T \in \mathcal{L}(V)$. We say that a *non-zero* vector $\mathbf{v}$ of V is an **eigenvector** of T with the **eigenvalue** $\lambda \in F$ if

$$T(\mathbf{v}) = \lambda \mathbf{v}.$$

(a) Let V be a finite dimensional vector space over an algebraically closed field F, and $T \in \mathcal{L}(V)$. Show that there exists an eigenvector $\mathbf{v}$ with an eigenvalue λ for some $\lambda \in F$. (Hint: using the previous problem. Consider the factorization of $c(T) = (t - \lambda) \cdot g(t)$, and using the minimality of degree of $c(T)$ to prove the existence of eigenvectors. Warning: again, you are **not** allowed to use the theory of determinant.)
(b) Give an example to show that the statement of (a) is not true if we drop the condition of algebraically closed on F.

Problem 6. Let V be a finite dimensional vector space over an algebraically closed field F, and $T \in \mathcal{L}(V)$. Show that T is triangularizable. (Hint: we prove it by induction on the dimension of V. Let $\mathbf{v}$ be an eigenvector of T, and $W = \mathrm{Span}\{\mathbf{v}\}$. The $\tilde{T}$ is a linear transformation from V/W to V/W. Then we apply the induction hypothesis on V/W.)

Problem 7. Let V be a vector space over F, and $T, U \in \mathcal{L}(V)$ which commutes; i.e., $TU = UT$.

(a) Let W be a T-invariant subspace. Show that $U(W)$ is also T-invariant.
(b) Let λ be an eigenvalue of T. A subspace $V_\lambda = \{\mathbf{v} \in V | T(\mathbf{v}) = \lambda \mathbf{v}\}$ of V is called the **eigenspace of V associated to λ** or simply **λ-eigenspace**. Show that V_λ is U-invariant.
(c) Assume that F is algebraically closed. Show that T and U have an common eigenvector $\mathbf{v}$.
(d) Assume that F is algebraically closed. Show that T and U can be simultaneously triangularizable.

Problem 8. Let V be a vector space over F of dimension n, and let V^* be the vector space of linear functionals on V. That is, let:

$$V^* = \text{Hom}(V, F) = \{T\colon V \to F \mid T \text{ is linear}\}$$

(This V^* is called the dual space of V.) Prove that $\dim V^* = \dim V$.

Problem 9. Let V and W be vector spaces over F, and let $T\colon V \to W$ be a linear transformation. Let V^* and W^* be the dual vector spaces, defined on the previous problem (or in section 2.6).

Prove that $T^*\colon W^* \to V^*$ is a linear transformation:

$$T^*(f) = f \circ T$$

(T^* is called the dual transformation to T.)

Problem 10. Let V be a vector space over F with basis $\mathfrak{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. For each i, define an element $\mathbf{v}_i^* \in V^*$ by:

$$\mathbf{v}_i^*(a_1\mathbf{v}_1 + \ldots + a_n\mathbf{v}_n) = a_i$$

Show that the set $\mathfrak{B}^* = \{\mathbf{v}_1^*, \ldots, \mathbf{v}_n^*\}$ is a basis of V^*. $\mathfrak{B}^*$ is called the **dual basis** of $\mathfrak{B}$.

Problem 11. Let V be a vector space with basis $\mathfrak{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, and let W be a vector space with basis $\mathfrak{B}' = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$. Let $T\colon V \to W$ be a linear transformation. Prove the following relation:

$$[T]_{\mathfrak{B}}^{\mathfrak{B}'} = ([T^*]_{\mathfrak{B}'^*}^{\mathfrak{B}^*})^t$$

Conclude that the rank of T equals the rank of T^*.

Problem 12. Let V and W be finite dimensional vector spaces over F. Define a mapping $g : V^* \times W \to \text{Hom}_F(V, W)$ by for all $l \in V^*$, $\mathbf{w} \in W$, $\mathbf{v} \in V$,

$$g(l, \mathbf{w})(\mathbf{v}) = l(\mathbf{v})\mathbf{w}.$$

(a) Show that g is bilinear.
(b) By the universal property of the tensor product, we have a module homomorphism (linear transformation) h from $V^* \otimes W$ to $\text{Hom}_F(V, W)$. Prove that h is an isomorphism.

Problem 13. (**Bonus**) Let A be a ring, and M, N, and G be modules over A. Define the **direct sum** $M \oplus N$ of M and N to be the set of $M \times N = \{(m, n) | m \in M, n \in N\}$ with the addition and the scalar multiplication as follows: for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $a \in A$,

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2), \quad a(m, n) = (am, an).$$

It can be proved that $M \oplus N$ is a module over A. Let $M_1, M_2, \ldots, M_n$ be A-modules. We can define $\oplus M_i$ in the same way. Usually, we write the elements in $\oplus M_i$ as $\sum_i m_i$, where $m_i \in M_i$ and the zero element of $\oplus M_i$ is $\sum_i \mathbf{0}_{M_i}$.

We have learned from the last homework that linear independence is not very useful for general modules. However, there are objects in modules which are similar to vector spaces. Let M be a module over a ring A and S be a subset of M. We say that S is a **basis** of M if S is not empty, if S generates M, and if S is linearly independent; in particular, if S is a basis of M, then $M \neq \{\mathbf{0}\}$ and every elements of M has a unique expression as a linear combination of elements of M. We say M is a **free** module if M has a basis. We also define the zero module to be a free module generated by an empty set. For example, A itself is a free module over A. If M has a finite basis $\mathfrak{B} = \{m_1, \ldots, m_n\}$, then

$$M \simeq \oplus_i Am_i \simeq A^n$$

As we shown before, not every module has a basis. We say a ring A is a **domain** if for all $a, b \in A$, $a \neq 0$, $b \neq 0$, then $ab \neq 0$. A commutative domain A is called a **a principal ideal domain** if every ideal of A is principal. In this problem, we would like to show that free modules over principal ideal domains have similar properties of vector spaces.

To avoid the complication, from now on, we assume that $A = P(F)$, the polynomial ring over a field F. We have proved that A is principal. It is an integral domain since the product of any two non-zero polynomials are still a non-zero polynomial.

(a) Let M be a module over A, and $\mathfrak{a}$ be an ideal of A. Let $\mathfrak{a}M$ be a subset of M defined as

$$\mathfrak{a}M = \text{Span}\{am\}_{a\in\mathfrak{a}, m\in M} = \{a_1m_1 + \cdots + a_nm_n | a_i \in \mathfrak{a}, m_i \in M, n \in \mathbb{N}\}.$$

Show that $\mathfrak{a}M$ is a submodule. (Hint: the same as vector spaces, to prove a subset S is a submodule, we only need to show that S contains the zero element, and closed under addition and scalar multiplication.)

(b) Consider the quotient module $M/\mathfrak{a}M$. It is again an A-module (you do not need to show this). We define a scalar multiplication of $A/\mathfrak{a}$ on $M/\mathfrak{a}M$ as follows:

$$(a + \mathfrak{a}) \cdot (m + \mathfrak{a}M) = am + \mathfrak{a}M.$$

Show that this scalar multiplication is well-defined. Indeed, $M/\mathfrak{a}M$ is an $A/\mathfrak{a}$-module under this scalar multiplication (you do not need to prove this).

(c) Let M be a free module over A with a finite basis $\mathfrak{B} = \{m_1, \ldots, m_n\}$, and $\mathfrak{a}$ an ideal of A. We know that $M \simeq \oplus_i Am_i$. Show that

$$M/\mathfrak{a}M \simeq \oplus_i Am_i/\mathfrak{a}m_i$$

as A-modules and $A/\mathfrak{a}$-modules.

(Hint: consider a mapping ϕ defined by for $m = \sum a_im_i$,

$$\phi : m + \mathfrak{a}M \mapsto \sum_i (a_im_i + \mathfrak{a}m_i).$$

Show that ϕ is an isomorphism.)

(d) Let M be a free module with a basis $\{m\}$ and $\mathfrak{a}$ an ideal of A. Show that $M/\mathfrak{a}M$ is isomorphic to $A/\mathfrak{a}$ as A-modules and $A/\mathfrak{a}$-modules.

(e) Let M be a free module with a finite basis. Show that every basis has the same cardinality. This number is called the **dimension** of M. (Hint: consider an irreducible polynomial f in A (is there one?). Let $\mathfrak{a} = Af$, the principal ideal generated by f. Then $A/\mathfrak{a}$ is a field. Now the module $M/\mathfrak{a}M$ is a module over a field $A/\mathfrak{a}$, and therefore it is a vector space over $A/\mathfrak{a}$. Use this information to show that every basis of M has the same cardinality.)

(f) Let M be a finitely generated free module over A, and N a submodule. Then M is free and its dimension is less than for equal to the dimension of M. (Hint: let $\mathfrak{B} = \{m_1, \ldots, m_n\}$ be a basis of M, M_r the submodules of M generated by $\{m_1, \ldots, m_r$ for $r = 1, \ldots, n$, and $N_r = N \cap M_r$. We prove by induction on r. For $r = 1$, $N_1 = \{am_1 | am_1 \in N\}$. First of all, show that the subset $\{a \in A | am_1 \in N_1\}$ of A is an ideal and therefore $\{a \in A | am_1 \in N_1\} = Aa_1$ for some $a_1 \in A$. If $a_1 = 0$, then $N_1 = \{0\}$ and we are done. If not, it implies $N_1 = \text{Span}\{a_1m_1\}$, which is a free module of dimension 1. Assume inductively that N_r is free of dimension less than or equal to r. Let $\mathfrak{a}$ be the set of all elements $a \in A$ such that there exist an element $n \in N$ which can be written

$$n = b_1m_1 + \cdots + b_rm_r + am_{r+1},$$

for $b_i \in A$. Show that $\mathfrak{a}$ is an ideal and use this information to show that N_{r+1} is free.)