Math 146, Winter 2008

Homework #4

Due on Wednesday, February 27.

Problem 1. Find the inverse of the following matrix:

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

Problem 2. Let $T\colon \mathbb{R}^3 \to P_2(\mathbb{Q})$ be the following linear transformation:

$$T(x,y,z) = (x+y-2z)t^2 + (x+2y+z)t + (2x+2y-3z)$$

Prove that T is an isomorphism, and find a formula for T^{-1}.

Problem 3. Find a basis for the column space of the following matrix:

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

Problem 4. Find a basis for the row space, the column space and the null space of the following matrix:

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

Problem 5. Let $V = C^2(\mathbb{R})$ be a set of all continuous functions on $\mathbb{R}$, with their values in $\mathbb{C}$, which is a vector space over $\mathbb{C}$. Without using the uniqueness theorem of ordinary differential equations, prove the following statements.

(a) Let $c \in \mathbb{C}$, and $f \in V$ which satisfies the conditions,

$$f' - cf = 0, \ \ f(0) = 0.$$

Show that $f(x) = 0$ for all $x \in \mathbb{R}$. (Hint: this is indeed a calculus problem. By the fundamental theorem of calculus, we have

$$f(x) = a \int_0^x f(t)dt.$$

Repeat this process and we will get

$$f(x) = c^n \int_0^x \cdots \int_0^{t_1} f(t_1)dt_1 \cdots dt_n.$$

for any $n \in \mathbb{N}$. Now you use the fact that $f(x)$ is bounded on $[0, x]$ (why?) to show that $f(x)$ must be zero as $n \to \infty$.)

(b) Using Part (a), show that the subspace H of V defined by

$$H = \{f \in V | f' - cf = 0\}$$

is one-dimensional and $\{e^{cx}\}$ is a basis of H.

(c) Let $c \in \mathbb{C}$, and H' be a subspace of V defined by

$$H = \{f' \in V | f' - c^2 f = 0\}.$$

Show that H finite dimensional. Find the dimension of H' and a basis of H'. (Hint: for any $d \in \mathbb{C}$, let $T_d = D - dI$ be a mapping from V to V defined as

$$D - dI(f) = f' - df.$$

Then T_d is a linear transformation. We can identify H' as the kernel of $T_c \circ T_{-c}$ or that of $T_{-c} \circ T_c$.)

Problem 6. Let T_1 (resp. to T_2) be the linear transformation of $\mathbb{R}^3$ to $\mathbb{R}^3$ which is a rotation by angle $\pi/4$ about the z-axis (resp. to x-axis).

(a) Find the matrix representation of T_1 and T_2 in the standard ordered basis of $\mathbb{R}^3$).

(b) Prove that the hyperplane $x + y + \sqrt{2}z = 0$ is mapped to xy-plane by T_2T_1.

Problem 7. Recall a **ring** A is a set, together with two laws of composition, called multiplication and addition respectively, and written as a product and as a sum respectively, satisfying the following conditions:

(i) For any $r, s \in A$, $r + s = s + r$.

(ii) There exists a zero $0 \in A$ such that For all $r \in A$, $r + 0 = r$.

(iii) For all $r \in A$, there exists $-r$ such that $r + (-r) = 0$.

(iv) For all $r, s, t \in A$, $r(st) = (rs)t$.

(v) There exists $1 \in A$ such that for all $r \in A$, $1 \cdot r = r = r \cdot 1$. Moreover, $1 \neq 0$.

(vi) For all $r, s, t \in A$, $(r + s)t = rt + st$, and $t(r + s) = tr + ts$.

It satisfies one more condition

(vii) For all $r, s \in A$, $rs = sr$,

we say A is a **commutative ring**. For examples, $P(F)$, the set of all polynomials with coefficients in a field F, is a commutative ring. However, $M_{nn}(f)$, the set of all $n \times n$ matrices with entries in a field F, is a ring but not commutative.

Let A be a ring and $\mathfrak{a}$ is a subset of A. We say that $\mathfrak{a}$ is a **(two-side) ideal** of A if $\mathfrak{a}$ satisfies (i), (ii), (iii), and

$$\forall r \in A, a \in \mathfrak{a}, \quad ra \in \mathfrak{a}, ar \in \mathfrak{a}; \tag{*}$$

or, equivalently,

$$A\mathfrak{a} \subset \mathfrak{a}, \ \mathfrak{a}A \subset \mathfrak{a}$$

For any ideal $\mathfrak{a}$ of A, we can define an equivalence relation $\equiv \bmod \mathfrak{a}$, by for all $r, s \in A$, $r \equiv s \bmod \mathfrak{a}$ if and only if $r - s \in \mathfrak{a}$. We denote $A/\mathfrak{a}$ the set of all equivalence classes associated to $\equiv \bmod \mathfrak{a}$. More precisely,

$$A/\mathfrak{a} = \{r + \mathfrak{a} | r \in A\}.$$

We define an addition and a multiplication on $A/\mathfrak{a}$ by for all $r, s \in A$

$$(r + \mathfrak{a}) + (s + \mathfrak{a}) = (r + s) + \mathfrak{a}, \quad (r + \mathfrak{a}) \cdot (s + \mathfrak{a}) = rs + \mathfrak{a}.$$

(a) Let A be a ring, and $\mathfrak{a}$ an ideal of A. Prove that the above definitions of the addition and the multiplication of $A/\mathfrak{a}$ is well-defined; i.e., if $r + \mathfrak{a} = r' + \mathfrak{a}$, $s + \mathfrak{a} = s' + \mathfrak{a}$, then

$$(r + s) + \mathfrak{a} = (r' + s') + \mathfrak{a}, \quad rs + \mathfrak{a} = r's' + \mathfrak{a}.$$

Indeed, $A/\mathfrak{a}$ is a ring under the addition and the multiplication defined above, called the **quotient ring** of A by $\mathfrak{a}$. Note that the zero element in $A/\mathfrak{a}$ is $0 + \mathfrak{a} = \mathfrak{a}$ and the identity element in $A/\mathfrak{a}$ is $1 + \mathfrak{a}$. (we will assume this fact later.)

(b) Let A be a ring, and $\mathfrak{a}$ be a subset of A satisfying the condition (i), (ii), and (iii) above. We still can define the addition on $A/\mathfrak{a}$ as the same way as above. Prove that the multiplication on $A/\mathfrak{a}$ defined in this problem is *well-defined* if and only if $\mathfrak{a}$ satisfies the condition $(*)$.

(c) Let A be a ring, and $\mathfrak{a}$ an ideal of A. We say that $\mathfrak{a}$ is a **principal ideal** if there exists $a \in A$ such that

$$\mathfrak{a} = AaA = \{ras | r \in A, s \in A\}.$$

In this case, we say that $\mathfrak{a}$ is generated by a. If all ideals of a ring A are principal and $0 \neq 1$, we call A is a **principal ring**. Show that $P(F)$ and Z are principal rings. (Hint: consider the non-zero element a in $\mathfrak{a}$ with minimal degree or absolute value. Show that $\mathfrak{a} = Aa$).

(d) Let $A = P(F)$ and f be an irreducible polynomial of A. Using the fact that for all $g \in A$, there exist $r, s \in A$ such that $rg + sf = \gcd(f, g)$, prove that every non-zero element in $A/(f)$ has an inverse, where $(f) = Af$ is the principal ideal generated by f. As a consequence, $A/(f)$ is a field. (you do not need to prove this.)

(e) Construct a field with four elements.

Problem 8. Let A be a ring. A **(left) module over** A, or a (left) A-module M is a set, together with two operations $+$ and $\cdot$, that satisfy exactly the same axioms as vector spaces except replacing F by A. For example, vector spaces over a field F are modules over F. Other example are $\mathbb{Z}_n$, viewed as $\mathbb{Z}$-modules by for all $m \in \mathbb{Z}$

$$m \cdot [a]_n = [ma]_n.$$

Let M and N be two modules over A, and T a map from M to N. We say T is a **module homomorphism**, an A**-linear map**, or A**-homomorphism**, if for all $r \in A$, $m_1, m_2 \in M$,

$$T(rm_1 + m_2) = rT(m_1) + T(m_2).$$

We use $\operatorname{Hom}_A(M, N)$ to denote the set of all A-homomorphisms from M to N. Similarly, It is exactly the same as the case in vector spaces, except replacing F by A. Similarly, we can define isomorphisms, submodules, the span, linear independence on modules as we did for vector spaces.

(a) Let $n \in \mathbb{N}$ and $M = \mathbb{Z}_n$, a $\mathbb{Z}$-module. Show that any non-empty subset S of M is linearly dependent. This example shows that the term "linear independent/dependent" is not really useful in the general module setting.

(b) A subset of S a module M over a ring A is said to be a spanning set if $M = \operatorname{Span} S = \{\sum_i a_i s_i | a_i \in A, s_i \in S\}$. A module M over a ring A is said to be **finitely generated** if there exists a finite spanning set. Show that for any $n \in \mathbb{N}$, $\mathbb{Z}_n$ is finitely generated.

(c) Let M be a finitely generated module over a ring A. A spanning set S of M is called **minimal** if any proper subset of S is not a spanning set of M. Let $M = \mathbb{Z}_{10}$. Find two minimal spanning sets of M whose sizes are different. Therefore, we can not define "dimension" on modules.

(d) Let $M = \mathbb{Z}$, and $N = \mathbb{Z}_n$ be two $\mathbb{Z}$-modules. List down all elements $\operatorname{Hom}_{\mathbb{Z}}(M, N)$ and $\operatorname{Hom}_{\mathbb{Z}}(N, M)$.

Problem 9. Let A be a commutative 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 $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $a \in A$,

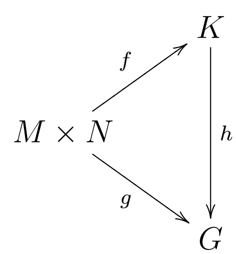
$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2), \quad a(m, n) = (am, an).$$

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.

A mapping g from the set $M \times N$ to G is called **bilinear** if it is linear respect to each component; i.e., for all $m_1, m_2 \in M$, $n_1, n_2 \in N$, $c_1, c_2 \in A$,

$$g(c_1 m_1 + m_2, c_2 n_1 + n_2) = c_1 c_2 g(m_1, n_1) + c_1 g(m_1, n_2) + c_2 g(m_2, n_1) + g(m_2, n_2).$$

Let K be a module over A with the following property, called the **universal property**: there exists a surjective bilinear mapping f from $M \times N$ to K such that for any module G over A with a bilinear mapping g from $M \times N$ to G, there exists a unique module homomorphism h from K to G such that $h \circ f = g$; i.e., the following diagram commutes



If so, we say that K is a **universal object**, and called a **tensor product** of M and N, denoted by $M \otimes_A N$. For any $m \in M$ and $n \in N$, we use $m \otimes n$ to denote $f(m, n)$. It can be showed that such a universal object exists.

(a) Prove that the tensor product is unique up to an isomorphism of modules; i.e., if K, and L are modules over A satisfying the universal property, then there exists a module homomorphism from K to L, which is bijective and its inverse is also a homomorphism of modules. (Hint: use the universal property to construct mapping from L to K and K to L, and then use it again to show the composites of them are identities.)

(b) If V and W be finite dimensional vector spaces over a field F, with bases $\mathfrak{B} = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ and $\mathfrak{C} = \{\mathbf{w}_1, \ldots, \mathbf{w}_m\}$. Define a vector space X over F whose basis is the set of pairings $\{(\mathbf{v}_i, \mathbf{w}_j) := \mathbf{v}_i \otimes \mathbf{w}_j | 1 \leq i \leq n, 1 \leq j \leq m\}$; i.e.,

$$X = \operatorname{Span}\{\mathbf{v}_i \otimes \mathbf{w}_j\}_{1 \leq i \leq n, 1 \leq j \leq m}\} = \{\sum_{i,j} a_{ij} \mathbf{v}_i \otimes \mathbf{w}_j | a_{ij} \in F\}.$$

We define a mapping f from $V \times W$ to X as follows:

$$f\left(\sum_i a_i \mathbf{v}_i, \sum_j b_j \mathbf{w}_j,\right) = \sum_{i,j} a_i b_j \mathbf{v}_i \otimes \mathbf{w}_j.$$

Show that f is bilinear and X is the tensor product $V \otimes_F W$ of V and W.

(c) Show that $\mathbb{Z}_5 \otimes_{\mathbb{Z}} \mathbb{Z}_7$ is the zero module. (Hint: consider any bilinear mapping g from $\mathbb{Z}_5 \times \mathbb{Z}_7$ to any $\mathbb{Z}$-module M. Show that g is the zero mapping; i.e., $g(a, b) = 0$ for all $a \in \mathbb{Z}_5$ and $b \in \mathbb{Z}_7$.)