MATH 23a, FALL 2002
THEORETICAL LINEAR ALGEBRA
AND MULTIVARIABLE CALCULUS
Midterm Solutions (take-home portion)

**1. Prove the Second Isomorphism Theorem, which states:**

**If $V$ and $W$ are subspaces of a vector space $U$, then**

$$V/(V \cap W) \cong (V + W)/W.$$

We present two solutions:

(a) We use the First Isomorphism Theorem, which states that if $L : X \to Y$ is surjective, then $X/Ker(L) \cong Y$.

In this case, we let $X = V$ and $Y = (V + W)/W$ and define $L : X \to Y$ by $L(\mathbf{v}) = \mathbf{v} + W$. It is clear that this $L$ is linear, so we need to show that $L$ is surjective and that $Ker(L) = V \cap W$.

Given $(\mathbf{v} + \mathbf{w}) + W \in (V + W)/W$, choose $\mathbf{v} \in V$. Then $L(\mathbf{v}) = \mathbf{v} + W$, and we claim that $\mathbf{v} + W \sim \mathbf{v} + \mathbf{w} + W$. This is true because $(\mathbf{v} + \mathbf{w}) - \mathbf{v} = \mathbf{w} \in W$, and hence $L$ is surjective.

Now we show that $Ker(L) = V \cap W$. Suppose $\mathbf{v} \in Ker(L)$. Then $L(\mathbf{v}) = \mathbf{v} + W \sim \mathbf{0} + W$, and $\mathbf{v} = \mathbf{v} - \mathbf{0} \in W$. Hence $\mathbf{v} \in W$ and hence $\mathbf{v} \in V \cap W$.

On the other hand, suppose $\mathbf{v} \in V \cap W$. Then $L(\mathbf{v}) = \mathbf{v} + W$. We claim that $\mathbf{v} + W \sim \mathbf{0} + W$, but this follows since $\mathbf{v} = \mathbf{v} - \mathbf{0} \in W$, and hence $\mathbf{v} \in Ker(L)$.

(b) We prove the theorem directly by constructing a bijective linear map $L : V/(V \cap W) \to (V + W)/W$ as follows.
Let $L(\mathbf{v} + (V \cap W)) = \mathbf{v} + W$. We need to show that $L$ is well-defined, linear, and bijective, and the second of these is easy.

For well-definedness, suppose $\mathbf{v}_1+(V\cap W)\sim \mathbf{v}_2+(V\cap W)$. Then $\mathbf{v}_1-\mathbf{v}_2\in V\cap W$, and hence in particular $\mathbf{v}_1-\mathbf{v}_2\in W$. Thus, $L(\mathbf{v}_1)=\mathbf{v}_1+W\sim \mathbf{v}_2+W=L(\mathbf{v}_2)$, and $L$ is well-defined.

For injectivity, suppose $L(\mathbf{v}_1)=\mathbf{v}_1+W\sim \mathbf{v}_2+W=L(\mathbf{v}_2)$. Then by definition of the equivalence, $\mathbf{v}_1-\mathbf{v}_2\in W$, but since both $\mathbf{v}_1$ and $\mathbf{v}_2$ are in $V$, by closure we also have $\mathbf{v}_1-\mathbf{v}_2\in V$, and hence $\mathbf{v}_1-\mathbf{v}_2\in V\cap W$.

For surjectivity, given $(\mathbf{v}+\mathbf{w})+W\in (V+W)/W$, choose $\mathbf{v}+(V\cap W)\in V/(V\cap W)$, and as in the first proof, it is easy to see that $L(\mathbf{v}+(V\cap W))=\mathbf{v}+W$ is equivalent to $(\mathbf{v}+\mathbf{w})+W$.

**2. Consider the field $F=\mathbb{Z}/2\mathbb{Z}$ with its elements identified as 0 and 1. (Properly speaking, these are representatives of equivalence classes, but we will allow the simpler notation.)**

**Now define $F[x]=\{a_0+a_1x+a_2x^2+\cdots+a_nx^n|n\in\mathbb{N},a_i\in F,\forall i\}$ to be the vector space of all polynomials with coefficients in $F=\mathbb{Z}/2\mathbb{Z}$, where addition and scalar multiplication are defined as usual. Note, however, there is also already a notion of the multiplication of two polynomials, and that $F[x]$ actually satisfies the axioms for a ring.**

**Let $p(x)=x^3+x+1$ be a fixed vector (polynomial) in $F[x]$, and define $I=\{a(x)p(x)|a(x)\in F[x]\}$ to be the subspace of $F[x]$ consisting of all (polynomial, not just scalar) multiples of this single vector.**

**(a) Show that $I$ is a subspace of vector space $F[x]$. (In fact, it is a *subring*, but we are only concerned with vector space properties in this part of the question.)**

We show closure under addition and scalar multiplication. Suppose $q_1(x)$ and $q_2(x)$ are in $I$ and $c\in F$. Then, by the definition of $I$, there are polynomials $a_1(x)$ and $a_2(x)$ such that $q_1(x)=a_1(x)p(x)$ and $q_2(x)=a_2(x)p(x)$, and hence $(q_1+q_2)(x)=(a_1+a_2)(x)p(x)$, and we have written $q_1+q_2$ as a product of $p$ with some polynomial $a_1+a_2$, so $q_1+q_2\in I$.

Similarly, we write $(c\cdot q_1)(x)=c\cdot a_1(x)p(x)=(c\cdot a_1)(x)p(x)$, and we have $c\cdot q_1$ as a product of $p$ with some other polynomial.

**(b) Define the quotient space $F[x]/I$ in terms of the data above, and find a minimal complete set of coset representatives. (Note that this is not the same as finding a basis. Since $F$ is finite, it is possible to list all the elements of $F[x]/I$. Hint: You might consider long division of polynomials to help you classify the cosets.)**

Recall from the Division Algorithm for polynomials that if $a(x)$ and $b(x)$ are in $F[x]$ and $b(x) \neq 0$, then there exist unique polynomials $q(x), r(x) \in F[x]$ (the quotient and remainder, respectively) such that $a(x) = q(x) \cdot b(x) + r(x)$ and $deg(r) < deg(b)$.

With this observation in place and thinking of $b(x) = p(x)$ from the definition of $I$, we see that given the relationship

$$a(x) = q(x) \cdot p(x) + r(x),$$

we have $a(x) + I \sim r(x) + I$ since $a(x) - r(x) = q(x) \cdot p(x) \in I$. Hence any polynomial is in the same coset as its remainder when divided by $p(x)$, and hence the set of all possible remainders will be a complete set of coset representatives.

Since we are dividing by $p(x) = x^3 + x + 1$, we see that $0 \leq deg(r) < 3$, or in other words, we may write $r(x) = a_0 + a_1x + a_2x^2$, where $a_0, a_1, a_2 \in F = \mathbb{Z}/2\mathbb{Z}$. Since there are two choices each for the three coefficients, we have the following 8 cosets:

| | | | |
|---|---|---|---|
| $0 + I$ | $x + I$ | $x^2 + I$ | $(x^2 + x) + I$ |
| $1 + I$ | $(x + 1) + I$ | $(x^2 + 1) + I$ | $(x^2 + x + 1) + I$ |

**(c) We have already seen in general that the quotient space has the structure of a vector space (so that we already have addition and scalar multiplication). Show that the natural definition of multiplication is well-defined for elements of the quotient space $F[x]/I$.**

The natural definition of multiplication for two cosets follows the multiplication of polynomials:

$$(a(x) + I) \cdot (b(x) + I) = (a(x)b(x)) + I.$$

To show this is well-defined, suppose $a_1(x) + I \sim a_2(x) + I$ and $b_1(x) + I \sim b_2(x) + I$. Then by definition of the equivalence, we

have $a_1(x) - a_2(x) \in I$ and $b_1(x) - b_2(x) \in I$, and hence there are two polynomials $c_1(x)$ and $c_2(x)$ in $F[x]$ such that:

$$a_1(x) = a_2(x) + c_1(x) \cdot p(x)$$
$$b_1(x) = b_2(x) + c_2(x) \cdot p(x)$$

Multiplying the corresponding sides of the equations yields:

$a_1(x)b_1(x) = a_2(x)b_2(x)+c_1(x)b_2(x)\cdot p(x)+c_2(x)a_2(x)\cdot p(x)+c_1(x)c_2(x)\cdot p(x)^2$,

or in other words,

$$\begin{aligned} a_1(x)b_1(x) - a_2(x)b_2(x) &= c_1(x)b_2(x) \cdot p(x) + c_2(x)a_2(x) \cdot p(x) + c_1(x)c_2(x) \cdot p(x)^2 \\ &= [c_1(x)b_2(x) + c_2(x)a_2(x) + c_1(x)c_2(x) \cdot p(x)] \cdot p(x) \end{aligned}$$

and hence $a_1(x)b_1(x) - a_2(x)b_2(x) \in I$ and $a_1(x)b_1(x) + I \sim a_2(x)b_2(x) + I$, which shows that multiplication is well-defined.

**(d) With the multiplication from part (c) and the representatives from part (b), show that $F[x]/I$ satisfies Axiom M3 and M4 (multiplicative identity and inverses) for a field by explicitly naming the identity and all multiplicative inverses. (This shows that $F[x]/I$ is a field because Axioms M1, M2, and D are inherited from the stucture of $F[x]$.)**

Given the natural definition of multiplication above, the multiplicative identity is the coset $1 + I$ because $(1 + I)(a(x) + I) = a(x) + I$ for any $a(x)$.

As for any ring, the multiplicative identity is its own multiplicative inverse, and the additive identity (in this case $0 + I$) has no multiplicative inverse. The other six elements of the quotient space are all invertible and they come in the following pairs:

| $a$ | $a^{-1}$ |
|---|---|
| $x + I$ | $(x^2 + 1) + I$ |
| $(x + 1) + I$ | $(x^2 + x) + I$ |
| $x^2 + I$ | $(x^2 + x + 1) + I$ |

The justification for each is similar, and we do the first as an example:

$$(x + I)((x^2 + 1) + I) = (x^3 + x) + I \sim 1 + I$$

and hence the two elements are inverses of each other.