Math 427  Section E  Exam 2 (SOLUTIONS)
Prof. I.Kapovich  April 11, 2005

Problem 1.
(i) Consider the ideal \( I = (3x^3 + 3x^2 + 2, x^2 + x) \) in \( \mathbb{Z}[x] \).
Find the characteristic of the ring \( \mathbb{Z}[x]/I \).
(ii) Consider the ideal \( J = (3x^3 + 3x^2 + 2, x^2 + x) \) in \( \mathbb{R}[x] \). Find a polynomial \( f \in \mathbb{R}[x] \) such that \( J = (f) \).

Solution
(i) We have \( 3x^3 + 3x^2 + 2 - 3x(x^2 + x) = 2 \) and therefore \( 2 \in I \). Thus the characteristic of \( \mathbb{Z}[x]/I \) is either 1 or 2.
We claim that \( 1 \notin I \). Indeed, suppose \( 1 \in I \) so that for some \( f(x), g(x) \in \mathbb{Z}[x] \) we have
\[
f(x)(3x^3 + 3x^2 + 2) + g(x)(x^2 + x) = 1 \text{ in } \mathbb{Z}[x].
\]
The constant term of the left hand side of the above equation is even while the constant term of the right-hand side is 1, yielding a contradiction. This \( 1 \notin I \) and therefore the characteristic of \( \mathbb{Z}[x]/I \) is equal to 2.

(ii) The calculation in part (i) shows that \( 2 \in J \) and therefore \( \frac{1}{2} \cdot 2 = 1 \in J \). Thus \( J = \mathbb{R}[x] \) and \( J = (1) \).

Problem 2.
Let \( R \) be a finite nonzero integral domain. Prove that \( R \) is a field.

Proof. First solution.
Let \( a \in R, a \neq 0 \) be arbitrary. Consider the function \( f_a : R \to R \) defined as \( f_a(x) = ax \), where \( x \in R \).
We claim that \( f_a \) is injective. Indeed, if \( f_a(x) = f_a(y) \) then \( ax = ay \) and therefore \( a(x - y) = 0 \). Since \( a \neq 0 \) and \( R \) is an integral domain, it follows that \( x - y = 0 \) so that \( x = y \).
Thus \( f_a : R \to R \) is injective. Since \( R \) is a finite set, it follows that \( f_a \) is surjective. Hence there exists \( b \in R \) such that \( f_a(b) = 1 \) that is \( ab = 1 \).

Proof. Second solution. Let \( a \in R, a \neq 0 \) be arbitrary. Consider the sequence
\[
a, a^2, a^3, \ldots
\]
Since \( R \) is finite, there exist positive integers \( m, n \) such that \( m < n \) and \( a^m = a^n \). Then
\[
a^n - a^m = a^m(a^{n-m} - 1) = 0.
\]
Since $a \neq 0$ and $R$ is an integral domain, it follows that $a^{n-m} - 1 = 0$, that is $a^{n-m} = 1$. Thus $aa^{n-m-1} = 1$ and hence $a^{n-m-1}$ is the multiplicative inverse of $a$. \hfill \Box

**Problem 3.** [10 points]
Prove that $\mathbb{F}_5[x]/(x^3 + 2x + 1)$ is a field.

**Solution.**
We claim that $x^3 + 2x + 1 \in \mathbb{F}_5[x]$ is an irreducible polynomial. Since the degree of $x^3 + 2x + 1$ is equal to 3 and since $\mathbb{F}_5$ is a field, to see this it suffices to check that $x^3 + 2x + 1$ has no roots in $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$. We verify this by substituting each of the elements of $\mathbb{F}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$ as $x$ in $x^3 + 2x + 1$:

\[
\begin{align*}
[0]_5^3 + 2[0]_5 + [1]_5 &= [1]_5 
eq [0]_5 \\
[1]_5^3 + 2[1]_5 + [1]_5 &= [4]_5 
eq [0]_5 \\
[2]_5^3 + 2[2]_5 + [1]_5 &= [2]_5 
eq [0]_5 \\
[3]_5^3 + 2[3]_5 + [1]_5 &= [-2]_5^3 + 2[-2]_5 + [1]_5 = [4]_5 
eq [0]_5 \\
[4]_5^3 + 2[4]_5 + [1]_5 &= [-1]_5^3 + 2[-1]_5 + [1]_5 = [3]_5 
eq [0]_5.
\end{align*}
\]

Thus $x^3 + 2x + 1 \in \mathbb{F}_5[x]$ is irreducible. It follows that $(x^3 + 2x + 1)$ is a maximal ideal in $\mathbb{F}_5[x]$ and therefore $\mathbb{F}_5[x]/(x^3 + 2x + 1)$ is a field.

**Problem 4.**
(i) Give an example of a finite nonzero ring $R$ and of a finitely generated nonzero $R$-module $V$ such that $V$ is not free. Explain why your example has the required properties.

(ii) Give an example of an ideal $I$ in $\mathbb{Z}[x]$ such that $I$ is not principal. Prove that your example has the required property.

**Solution.**
(i) Let $R = \mathbb{Z}/4\mathbb{Z}$. And consider the ideal $I = ([2]_4) = \{[0]_4, [2]_4\} \subseteq R$. Then $I$ is an also $R$-module.

A free $R$-module of rank 1 has $4^n$ elements. Since $I$ has two elements, it follows that $I$ is not free.

(ii) Consider the ideal $I = (2, x) \subseteq \mathbb{Z}[x]$.

Note that $1 \notin I$ since for any $a(x), b(x) \in \mathbb{Z}[x]$ the constant term of $2a(x) + xb(x)$ is even, while 1 is odd.

Suppose that $I$ is principal and $I = (f)$ for some $f \in \mathbb{Z}[x]$. Then $2 = fg$ for some $g \in \mathbb{Z}$. Since $\text{deg}(fg) = \text{deg}(f) + \text{deg}(g) = 0$ it
follows that $def(f) = \deg(g) = 0$. Thus $f = c \in \mathbb{Z}$. Hence either $f = \pm 1, g = \pm 2$ or $f = \pm 2, g = \pm 1$.

If $f = \pm 1$ then $1 \in I$, which is impossible. Thus $f = \pm 2$ and hence $I = (2)$. However, $x \not\in (2)$, while $x \in I$, yielding a contradiction.

Problem 5.

Let $R$ be a commutative ring. An element $a$ of $R$ is said to be nilpotent if there exists an integer $n \geq 1$ such that $a^n = 0$.

(i) Prove that the set $N$ of all nilpotent elements in $R$ is an ideal.

(ii) Prove that if $x \in R$ is a nilpotent element then $1 + x$ has a multiplicative inverse in $R$.

Solution.

(i) Let $a, b \in N$ and let $m, n \geq 1$ be integers such that $a^n = b^m = 0$. For any $r \in R$ we have $(ra)^n = r^n a^n = 0$ and hence $ra \in N$.

Also

$$(a + b)^{m+n} = \sum_{i=0}^{m+n} a^i b^{n+m-i} \binom{n+m}{i}$$

For every $i = 0, \ldots, n+m$ either $i \geq n$ or $n+m-i \geq m$ and so $a^i b^{n+m-i} = 0$. Therefore $(a + b)^{n+m} = 0$ so that $a + b \in I$.

Therefore $N$ is an ideal in $R$.

(ii) Let $x \in N$ and $n \geq 1$ be such that $x^n = 0$.

Then

$$(1 + x)(1 - x + x^2 - x^3 + \cdots + (-1)^{n-1}x^{n-1}) = 1$$

and therefore $1 + x$ has a multiplicative inverse in $R$. 