HOMEWORK 1 – MATH 392
January 12, 2018

ALEX THIES
athies@uoregon.edu

1. Book Problems

Problem 7.23. Let A be a commutative ring with unity and $a(x) \in A[x]$. Determine if the following statement is true or false. Either prove it or find a counterexample: If every coefficient of $a(x)$ is a zero divisor of A, then $a(x)$ is a zero divisor in $A[x]$.

Proof. This is false, we present the following counterexample: consider the polynomial ring $\mathbb{Z}_6[x]$ and polynomial $3 + 2x = a(x) \in \mathbb{Z}_6[x]$. Note that $2, 3$ are zero divisors in $\mathbb{Z}_6$, we will demonstrate that for an arbitrary nonzero $b(x) \in \mathbb{Z}_6[x]$, that $a(x)b(x) \neq 0(x)$. Furthermore, let $b(x) \in \mathbb{Z}_6[x]$ such that $b(x) \neq 0(x)$, thus $\deg(b(x)) = n$, and $b_n \neq 0$. Consider the product of these polynomials,

$$\begin{aligned} a(x)b(x) &= (2x+3)\left(\sum_{i=0}^{n} b_i x^i\right), \\ &= (2x+3)\left(b_n x^n + b_{n-1}x^{n-1} + \sum_{i=0}^{n-2} b_i x^i\right), \\ &= 2b_n x^{n+1} + (3b_n + 2b_{n-1})x^{n-1} + \cdots . \end{aligned}$$

If $a(x)$ is in fact a zero divisor in $\mathbb{Z}_6[x]$, then every coefficient would be equivalent to 0 modulo 6. Notably, it must be true that the coefficient of the new $(n+1)$th term is zero, i.e., $2b_n \equiv 0 \pmod 6 \iff b_n = 3$. If $b_n = 3$, then the coefficient for the nth term is $(9 + 2b_{n-1}) \equiv (3 + 2b_{n-1}) \pmod 6$. Again, if $a(x)$ is a zero divisor, then there exists $b_{n-1} \in \mathbb{Z}_6$ such that $3 + 2b_{n-1} \equiv 0 \pmod 6$. However, upon inspection its obvious that this congruence is not solvable, thus (in this counterexample) if the $(n+1)$th term is zero it is true that the nth term is not zero. It follows that $a(x)b(x) \neq 0(x)$, hence $a(x)$ is not a zero divisor, even though its coefficients are zero divisors in their ring. $\square$

Problem 7.24. Let A be a commutative ring with unity and $a(x) \in A[x]$. Determine if the following statement is true or false, then either prove it or find a counterexample: If $a_0 \neq 0_A$ is not a zero divisor of A, then $a(x)$ is not a zero divisor in $A[x]$.

Proof. This is true. Let A, $A[x]$, $a(x)$ be as above. Suppose $a_0 \neq 0_A$ is not a zero divisor in A. Further, consider the polynomial $b(x) \in A[x]$ such that $b(x) \neq 0(x)$, thus $\deg(b(x)) = n$ and $b_n \neq 0_A$. Since each polynomial has a least term $a_i x^i$, notice that the product $a(x)b(x)$ will contain the term $a_0 b_i x^i$, where $b_i x^i$ is the least term of $b(x)$. By our supposition $a_0 b_n \neq 0_A$, thus the degree of the product $a(x)b(x)$ will be at least n which means that $a(x)b(x)$ is not the zero polynomial and $a(x)$ is not a zero divisor of $A[x]$. ☐

Problem 7.27. Suppose A is a commutative ring with unity. Let $S = \{a(x) \in A[x] : a_0 \neq 0_A\}$. Determine if S is an ideal of $A[x]$. Either prove that it is an ideal or find a counterexample showing it fails to be an ideal.

Proof. It is immediately clear that S is not closed under subtraction and thus not an ideal.

Since A is a commutative ring with unity for each $a \in A$ there exists $-a \in A$ such that $a + (-a) = 0_A$. It follows that $a(x) = a_0$ and $a'(x) = -a_0$ are each in S, but their sum is $0(x)$ which is not in S. Hence, S is not closed under subtraction, and not an ideal. ☐

Problem 7.47. Let K be a field. Prove: The only units in $K[x]$ are the nonzero constant polynomials.

Proof. Since K is a field, each of its nonzero elements are units, i.e., for each $k \in K$ such that $k \neq 0$, there exists $k^{-1} \in K$ such that $kk^{-1} = 1_K$. Define $\varphi : K \to K[x]$ mapped by $k \mapsto k_0$ and notice that $\varphi(K) \subseteq K[x]$. The set $\varphi(K)$ is all of the nonzero constant polynomials in $K[x]$, it is clear by their construction that each element in $\varphi(K)$ has its inverse also in $\varphi(K)$, thus every element in $\varphi(K)$ is a unit. It remains to show that these are all of the units of $K[x]$.

Consider $a(x) \in K[x]$ such that $\deg(a(x)) = n$ and $n \geq 1$, and suppose by way of contradiction that there exists $b(x) \in K[x]$ with $\deg(b(x)) = m$ such that $a(x)b(x) = 1(x)$ (where $1(x)$ denotes the unity of $K[x]$). Since K is a field, $K[x]$ is an integral domain, thus $\deg(a(x)b(x)) = n + m$. Recall that $n \geq 1$, thus $\deg(a(x)b(x)) \geq 1$, which implies that $a(x)b(x) \neq 1(x)$. Thus, $a(x)$ is not a unit if its degree exceeds that of a nonzero constant polynomial, which implies that for a field K, the only units in the polynomial ring $K[x]$ are the nonzero constant polynomials, as we aimed to show. $\square$

Problem 7.52. Let A be a commutative ring with unity. Prove that the function $f : A[x] \to A$ defined by $f(a(x)) = a_0$ is a homomorphism. What is the kernel of f?

Proof. Let A, $A[x]$, and f be as above. Since the problem refers to f as a function, we will omit showing that it is uniquely defined. That leaves us with showing that f is both additive and multiplicative. Let $a(x), b(x) \in A[x]$ such that their respective degrees are finite. We compute the following:

$$\begin{aligned}
f(a(x)+b(x)) &= f\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i\right), \\
&= f\left(\sum_{i=0}^{\max(n,m)} (a_i + b_i)x^i\right), \\
&= f\left((a_0 + b_0) + \sum_{i=1}^{\max(n,m)} (a_i + b_i)x^i\right), \\
&= a_0 + b_0, \\
&= f(a(x)) + f(b(x)).
\end{aligned}$$

Thus, f is additive. We will now show that it is also multiplicative:

$$\begin{aligned}
f(a(x)b(x)) &= f\left(\sum_{i=0}^{n} a_i x^i \sum_{j=0}^{m} b_j x^j\right), \\
&= f\left(\sum_{i+j=0}^{n+m} (a_i b_j)x^{i+j}\right), \\
&= f\left(a_0 b_0 + \sum_{i+j=1}^{n+m} (a_i b_j)x^{i+j}\right), \\
&= a_0 b_0, \\
&= f(a(x))f(b(x)).
\end{aligned}$$

Thus, f is both additive and multiplicative, hence it is a ring homomorphism. $\square$

2. Extra Problems

Let $\mathbb{C}$ denote the complex numbers, $\{a+bi : a, b \text{ are real numbers, and } i^2 = -1\}$. Let $\mathbb{R}$ denote the real numbers. Define $T : \mathbb{R}[x] \to \mathbb{C}$ by $T(f) = f(i)$ (i.e. take a polynomial with real coefficients, and evaluate it at the complex number i).

Problem 1. Prove that T is a homomorphism (*hint*: use theorems, or slight modifications of theorems, from chapter 7. Not everything needs to be proven from the definitions, although there's nothing wrong with that).

Proof. We will show that T is uniquely defined, additive, multiplicative, and therefore a ring homomorphism.

Let T be as above, further let $a(x), a'(x) \in \mathbb{R}[x]$ such that $a(x) = a'(x)$. Since $a(x) = a'(x)$ it is clear that $a(i) = a'(i)$, thus T is uniquely defined.

Let $b(x) \in \mathbb{R}[x]$, we compute:

$$\begin{aligned}
T(a(x)+b(x)) &= T\left(\sum_{j=0}^{n} a_j x^j + \sum_{j=0}^{m} b_j x^j\right), \\
&= T\left(\sum_{j=0}^{\max(n,m)} (a_j + b_j) x^j\right), \\
&= \sum_{j=0}^{\max(n,m)} (a_j + b_j) i^j \\
&= \sum_{j=0}^{n} a_j i^j + \sum_{j=0}^{m} b_j i^j, \\
&= a(i) + b(i), \\
&= T(a(x)) + T(b(x)).
\end{aligned}$$

Thus, T is additive; we will now show that T is multiplicative.

$$\begin{aligned}
T(a(x)b(x)) &= T\left(\sum_{j=0}^{n} a_j x^j \sum_{k=0}^{m} b_k x^k\right), \\
&= T\left(\sum_{j+k=0}^{n+m} a_j b_k x^{j+k}\right), \\
&= \sum_{j+k=0}^{n+m} a_j b_k i^{j+k}, \\
&= \sum_{j+k=0}^{n+m} a_j i^j b_k i^k, \\
&= \sum_{j=0}^{n} a_j i^j \sum_{k=0}^{m} b_k i^k, \\
&= a(i)b(i), \\
&= T(a(x))T(b(x)).
\end{aligned}$$

Thus, T is multiplicative, and we have shown that T satisfies all of the conditions required of a ring homomorphism, as we aimed to do. ☐

Problem 2. Prove that the kernel of T is $\langle x^2+1\rangle$, i.e. the principal ideal generated by x^2+1.

Proof. We will show by double inclusion that $\ker(T) = \langle x^2+1\rangle$. Notice that $T(x^2+1) = i^2+1 = 0$, thus by the zero product property any $a(x) \in \langle x^2+1\rangle$ is also equal to zero when evaluated at i. Thus, $\langle x^2+1\rangle \subseteq \ker(T)$; it remains to show that $\ker(T) \subseteq \langle x^2+1\rangle$.

Let $b(x) \in \ker(T)$ be arbitrary, then $T(b(x)) = b(i) = 0$. By the division algorithm we can write $b(x) = q(x)(x^2+1) + r(x)$ for unique polynomials $q, r \in \mathbb{R}[x]$ such that $\deg(r(x)) < \deg(x^2+1)$, or $r(x) = 0(x)$. The rest of the proof pertains to the nature of $r(x)$. For $\ker(T)$ to be a subset of $\langle x^2+1\rangle$ it must be true that $r(x) = 0(x)$, which we will show by cases. Since $\deg(x^2+1) = 2$ we have that the degree of $r(x)$ is either 0 or 1, or that $r(x) = 0(x)$, i.e., we have the following cases (1) $r(x) = r_0$, or (2) $r(x) = r_0 + r_1 x$, or (3) $r(x) = 0(x)$.

Case 1. If $\deg(r(x)) = 0$, then $r(x) = r_0$ and $r_0 \neq 0$. It is plain to see that $r(i) \neq 0$ and then $b(i) \neq 0$, which would move $b(x)$ out of the kernel, thus $\deg(r(x)) \neq 0$.

Case 2. If $\deg(r(x)) = 1$, then $r(x) = r_0 + r_1 x$, and $r_1 \neq 0$. Again, its fairly easy to see that $r(i) = r_0 + r_1 i \neq 0$, and for the same reason as before, $\deg(r(x)) \neq 1$.

We have shown that cases one and two fail, leaving us with case three as the remaining possibility, that being that $r(x) = 0(x)$. It is clear that if $r(x) = 0(x)$ then $b(i) = 0(x)$. Since we wrote $b(x) = q(x)(x^2 + 1) + r(x)$ we can see that $b(x) \in \langle x^2 + 1\rangle$. We have shown that an arbitrary member of the kernel can be written as a linear combination of the polynomial that generates the principal ideal in question, thus $\ker(T) \subseteq \langle x^2 + 1\rangle$.

We have shown that $\ker(T)$ and $\langle x^2 + 1\rangle$ are subsets of one another, therefore they are equal, as desired. $\square$

Problem 3. Prove that $\mathbb{R}[x]/\langle x^2 + 1\rangle$ is isomorphic to $\mathbb{C}$.

Proof. Recall the Fundamental Homomorphism Theorem (FHT), which states: let A and K be rings, and let $f : A \to K$ be a ring homomorphism, then

$$A/\ker(f) \cong f(A).$$

In Problem 1 we proved that T is a homomorphism, and in Problem 2 we proved that $\ker(T) = \langle x^2 + 1\rangle$, this tees up the FHT; it remains to show that T is surjective, which gives us $T(\mathbb{R}[x]) = \mathbb{C}$. Notice that $a+bx \in \mathbb{R}[x]$ and $T(a+bx) = a+bi$, thus $T(a+bx)$ outputs all possible complex numbers. Therefore, T is surjective, $T(\mathbb{R}[x]) = \mathbb{C}$, and by the FHT: $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$, as we aimed to prove. $\square$