QUIZ 1 CORRECTIONS – MATH 392
February 7, 2018

ALEX THIES
athies@uoregon.edu

Problem 1

Let $T : \mathbb{Q}[x] \to \mathbb{R}$ be the ring homomorphism given by

$$T(p(x)) = p(\sqrt{2}).$$

We proved last term that every kernel is an ideal, and moreover, we know that any ideal of $\mathbb{Q}[x]$ is a principal ideal, so we know $\ker T = \langle a(x) \rangle$ for some $a(x) \in \mathbb{Q}[x]$. Determine this polynomial $a(x)$ (and of course, prove your claim is true).

Proof. We claim that $p(x) = x^2 - 2$, we will show that $\ker T = \langle x^2 - 2 \rangle$ by double-inclusion.

Notice that $T(x^2 - 2) = 0$, thus $x^2 - 2 \in \ker T$, it follows by the zero product property that any linear combination of $x^2 - 2$, i.e. any element of $\langle x^2 - 2 \rangle$ will also equal zero when evaluated at $x = \sqrt{2}$. Thus, $\langle x^2 - 2 \rangle \subseteq \ker T$. It remains to show that $\langle x^2 - 2 \rangle \supseteq \ker T$.

Let $b(x) \in \ker T$ be arbitrary, then $T(b(x)) = b(\sqrt{2}) = 0$. By the division algorithm we can write $b(x) = q(x)(x^2-2)+r(x)$ for unique polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that $\deg r(x) < \deg x^2 - 2$, or $r(x) = 0$. The remainder of the proof pertains to the nature of (x). For $\ker T$ to be a subset of $\langle x^2 - 2 \rangle$ we must have $r(x) = 0(x)$, which we will prove by cases. Since $\deg x^2 - 2 = 2$, we have either $\deg r(x) = 1$, $\deg r(x) = 0$, or $r(x) = 0(x)$.

Case 1, suppose $\deg r(x) = 1$, then $r(x) = r_0 + r_1 x$ and $r_1 \neq 0$. We can see that $r(\sqrt{2}) \neq 0$, which would contradict our hypothesis that $b(x) \notin \ker T$. Hence, $\deg r(x) \neq 1$.

Case 2, suppose $\deg r(x) = 0$, then $r(x) = r_0$ and $r_0 \neq 0$. We can see that $r(\sqrt{2}) \neq 0$, which would contradict our hypothesis that $b(x) \notin \ker T$. Hence, $\deg r(x) \neq 0$.

This leaves us with the case that $r(x) = 0(x)$, which allows us to write $b(x) = q(x)(x^2 - 2)$, and then conclude that $b(x) \in \langle x^2 - 2 \rangle$. Thus, we have shown that an arbitrary element of the kernel of T is inherently also an element of $\langle x^2 - 2\rangle$, therefore $\ker T = \langle x^2 - 2\rangle$, as we aimed to prove. $\square$

Problem 2

List all polynomials $p(x)$ over $\mathbb{Z}_2$ that have degree 3, and determine which are reducible and which are irreducible. Write all polynomials as a product of their irreducible factors. For any irreducible, whether a degree 3 polynomial or a factor of something reducible, prove that it is irreducible.

Proof. Since $\mathbb{Z}_2 = \{0, 1\}$, we have the following degree three polynomials from $\mathbb{Z}_2[x]$:

$$\begin{array}{llll} p_1(x) = & x^3 + x^2 + x + 1 & p_5(x) = & x^3 + 1 \\ p_2(x) = & x^3 + x + 1 & p_6(x) = & x^3 + x^2 \\ p_3(x) = & x^3 + x^2 + 1 & p_7(x) = & x^3 + x \\ p_4(x) = & x^3 + x^2 + x & p_8(x) = & x^3 \end{array}$$

Figure 1. Degree 3 polynomials from $\mathbb{Z}_2[x]$

We will now determine which polynomials are irreducible, and for the reducible polynomials we write them as a product of their irreducible factors. Notice that since we are working in $\mathbb{Z}_2$, we have $R = \{0, 1\}$ as the only possible roots of our polynomials. Moreover, since we cannot use any theorems about factoring in $\mathbb{Q}$, we will be leaning on Theorem 8.22 quite extensively. Theorem 8.22 states that for a field K, and $a(x) \in K[x]$ with $\deg a(x) = 2$ or $\deg a(x) = 3$. The polynomial $a(x)$ is reducible over K if and only if $a(x)$ has a root in K. Finally, recall that by the definition of irreducible and reducible, any linear factors are irreducible.

$p_1(x)$. Let $p_1(x) = x^3 + x^2 + x + 1$. We compute the following,

$$p_1(0) = 1 \neq 0,$$
$$p_1(1) = 4 \equiv 0 \pmod 2.$$

Hence, $x = 1$ is a root, thus $p_1(x) = (x-1)b(x)$ for some $b(x) \in \mathbb{Z}_2[x]$; we determine $b(x)$ by polynomial long division:

$$\begin{array}{r}
x^2 + 2x + 3 \\
x-1\overline{)\; x^3 \;+ x^2 \;+ x + 1} \\
\underline{-\, x^3 \;+ x^2 \qquad\quad} \\
2x^2 \;+ x \quad\;\; \\
\underline{-\, 2x^2 + 2x \quad\;\;} \\
3x + 1 \\
\underline{-\, 3x + 3} \\
4
\end{array}$$

Again, since we are operating in $\mathbb{Z}_2[x]$, we have $b(x) = x^2 + 1$, and we can write $p_1(x) = (x+1)(x^2+1)$. We can notice that $b(1) = 0$, thus 1 is also a root of $b(x)$, thus we can write $p_1(x) = (x-1)^2\tilde{b}(x)$ for some $\tilde{b}(x) \in \mathbb{Z}_2[x]$. Again, we use polynomial long division:

$$\begin{array}{r}
x + 3 \\
x^2 - 2x + 1\overline{)\; x^3 \;+ x^2 \;+ x + 1} \\
\underline{-\, x^3 + 2x^2 \;- x \quad\;\;} \\
3x^2 \qquad\;\; + 1 \\
\underline{-\, 3x^2 + 6x - 3} \\
6x - 2
\end{array}$$

Thus, we have $p_1(x) = (x-1)^2(x+1)$, since these factors are linear, they are irreducible over $\mathbb{Z}_2$. Notice that we can also write $p_1(x) = (x+1)^3$ because $-1 \equiv 1 \pmod 2$.

$p_2(x)$. Let $p_2(x) = x^3 + x + 1$. We compute the following

$$\begin{aligned}
p_2(0) &\equiv 1 \pmod 2, \\
p_2(1) &\equiv 1 \pmod 2.
\end{aligned}$$

Thus, $p_2(x)$ has no roots in $\mathbb{Z}_2$ and is irreducible over $\mathbb{Z}_2$.

$p_3(x)$. Let $p_3(x) = x^3 + x^2 + 1$. We compute the following

$$\begin{aligned}
p_3(0) &\equiv 1 \pmod 2, \\
p_3(1) &\equiv 1 \pmod 2.
\end{aligned}$$

Thus, $p_3(x)$ has no roots in $\mathbb{Z}_2$ and is irreducible over $\mathbb{Z}_2$.

$p_4(x)$. Let $p_4(x) = x^3 + x^2 + x$. We can easily factor this as $p_4(x) = x(x^2+x+1)$, since x is linear, it remains to show that $\tilde{p}_4(x) = x^2+x+1$ is either irreducible, or has reducible factors. We compute the following

$$\begin{aligned} \tilde{p}_4(0) &\equiv 1 \pmod 2, \\ \tilde{p}_4(1) &\equiv 1 \pmod 2. \end{aligned}$$

Thus, $\tilde{p}_4(x)$ is irreducible over $\mathbb{Z}_2$, and we have p_4 as the following product of irreducible factors: $p_4(x) = x(x^2 + x + 1)$

$p_5(x)$. Let $p_5(x) = x^3 + 1$. We compute the following

$$\begin{aligned} p_5(0) &\equiv 1 \pmod 2, \\ p_5(1) &\equiv 0 \pmod 2. \end{aligned}$$

Hence 1 is a root and we have $p_5(x) = (x-1)b(x)$ for some $b(x) \in \mathbb{Z}_2[x]$. We compute $b(x)$:

$$\begin{array}{r|l} & x^2 + x + 1 \\ \hline x - 1 & x^3 \qquad\qquad + 1 \\ & -x^3 + x^2 \\ \hline & \quad x^2 \\ & \quad -x^2 + x \\ \hline & \qquad x + 1 \\ & \qquad -x + 1 \\ \hline & \qquad\quad 2 \end{array}$$

Thus, $b(x) = x^2 + x + 1$; at this point it should be fairly clear that $b(x)$ is irreducible given its only possible roots of 0 and 1, thus we have $p_5(x) = (x-1)(x^2+x+1) \equiv (x+1)(x^2+x+1) \pmod 2$.

$p_6(x)$. Let $p_6(x) = x^3 + x^2 = x^2(x+1)$, each factor is already linear, so we're done.

$p_7(x)$. Let $p_7(x) = x^3 + x = x(x^2+1)$, since x is linear, it remains to show that x^2+1 is either irreducible or reducible. From previous work its clear that $x^2 + 1 = (x+1)^2$, thus we have $p_7(x) = x(x+1)^2$.

$p_8(x)$. Let $p_8(x) = x^3$. This is already a product of irreducible linear factors, so we're done. $\square$

Problem 3

Let A and B be commutative rings with unity, and let $f : A \to B$ be a ring homomorphism that is not identically zero. Prove that for all $b \in B$, there exists a ring homomorphism $F : A[x] \to B$ such that $F(a) = f(a)$ for all $a \in A$ and $F(x) = b$ (meaning that F maps the polynomial x to b). (Hint: use theorems; it's not necessary to prove everything from the definition). You may assume that $f(1_A) = 1_B$.

Lemma 1. *The composition of ring homomorphisms is a ring homomorphism.*

Proof. Let A, B, C be rings with ring homomorphisms $\phi : A \to B$ and $\psi : B \to C$.

Additivity:

$$\begin{aligned}(\phi \circ \psi)(a + b) &= \phi(\psi(a + b)),\\ &= \phi(\psi(a) + \psi(b)),\\ &= \phi(\psi(a)) + \phi(\psi(b)),\\ &= (\phi \circ \psi)(a) + (\phi \circ \psi)(b).\end{aligned}$$

Multiplicativity:

$$\begin{aligned}(\phi \circ \psi)(a \cdot b) &= \phi(\psi(a \cdot b)),\\ &= \phi(\psi(a) \cdot \psi(b)),\\ &= \phi(\psi(a)) \cdot \phi(\psi(b)),\\ &= (\phi \circ \psi)(a) \cdot (\phi \circ \psi)(b).\end{aligned}$$

□

Proof. Recall the evaluation map $h_c : A[x] \to A$ defined by $h_c(a(x)) = a(c)$, where $c \in A$. By Theorem 7.35 we know that h_c is a homomorphism. By our previous Lemma we know that the composition of ring homomorphisms is a ring homomorphism, so consider the ring homomorphism $(f \circ h_c)$.

Let $F = (f \circ h_c)$, and let $a(x) \in A[x]$; recall that since f is a function we know for some $a \in A$, there exists $b \in B$ such that $f(a) = b$. If $a(x) = a_0$, then for any $c \in A$ we have

$$\begin{aligned}F(a(x)) &= (f \circ h_c)(a(x)),\\ &= f(h_c(a_0)),\\ &= f(a_0),\\ &= b.\end{aligned}$$

If $\deg a(x) > 0$, then we use $c = 0_A$ and get the following:

$$\begin{aligned} F(a(x)) &= (f \circ h_0)(a(x)), \\ &= f(h_0(a(x))), \\ &= f(a(0)), \\ &= f(a_0), \\ &= b. \end{aligned}$$

□

Thus, the composition $(f \circ h_c)$ is the ring homomorphism we were looking to find.