Math 333 Problem Set 11
Due: 05/18/16

Be sure to list EVERYONE in the that you talk to about the homework!

1. Let $I = \langle [5]_{20} \rangle \subset \mathbb{Z}/20\mathbb{Z}$. Prove that $(\mathbb{Z}/20\mathbb{Z})/I \cong \mathbb{Z}/5\mathbb{Z}$.

   Proof. Define $\varphi : \mathbb{Z}/20\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ by $\varphi([a]_{20}) = [a]_5$. Since $5 \mid 20$ we have shown before this is a well-defined surjective ring homomorphism. We claim $I = \ker\varphi$. Let $a \in I$, i.e., we can write $a = 5b$ for some $b \in \mathbb{Z}$. We have $\varphi([a]_{20}) = [a]_5 = [5]_5[b]_5 = [0]_5$, so $I \subset \ker\varphi$. Let $[a]_{20} \in \ker\varphi$ so $[a]_5 = [0]_5$, i.e., $5 \mid a$. Thus, $[a]_2 0 \in I$ and so $\ker\varphi = I$. Now we apply the first isomorphism theorem to conclude the result. $\square$

2. (a) Let $p \in \mathbb{Z}$ be a prime number. Let T be the set of rational numbers in lowest terms whose denominators are not divisible by p. Prove that T is a ring.

   Proof. Note that $T \subset \mathbb{Q}$ so it is enough so show T is a subring. We have $0 = 0/1 \in T$ so T contains the identity element. Let $a/b, c/d \in T$. We have $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd} \in T$ since $p \nmid b$ and $p \nmid d$ implies $p \nmid bd$ as p is prime. Similarly $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \in T$. Thus, T is a subring of $\mathbb{Q}$. $\square$

   (b) Let I be the subset of T consisting of elements whose numerators are divisible by p. Prove I is an ideal in T.

   Proof. First, observe it is clear $I \subset T$. We have $0 = 0/1 \in I$ as $p \mid 0$. Let $a/b, c/d \in I$ and $r/s \in T$. We have $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd} \in T$ since $p \mid a$ and $p \mid c$ implies $p \nmid ad - bc$. Similarly $\frac{r}{s}\frac{a}{b} = \frac{ra}{sb} \in I$ as $p \mid a$ implies $p \mid ra$. Thus, I is an ideal in T. $\square$

   (c) Prove that $T/I \cong \mathbb{Z}/p\mathbb{Z}$.

   Proof. Let $a/b \in T$ and consider the coset $\frac{a}{b} + I$. Note that $\gcd(p, b) = 1$ so there exists $x, y \in \mathbb{Z}$ so that $bx + py = 1$. Multiplying this by a we obtain $a = bx + py$, i.e., $p \mid a - bx$. We claim that $\frac{a}{b} + I = \frac{x}{1} + I$. We have $\frac{a}{b} - \frac{x}{1} = \frac{a-bx}{b}$. Since $p \mid a - bx$, we have $\frac{a-bx}{b} \in I$ so $\frac{a}{b} + I = \frac{x}{1} + I$, i.e., we can represent each coset by an integer. Moreover, we have this x is unique modulo p. If $by \equiv by \pmod{p}$, then $p \mid b(x-y)$. Since $p \nmid b$ we must have $p \mid (x-y)$, i.e., $x \equiv y \pmod{p}$ as claimed.

Define $\varphi : T/I \to \mathbb{Z}/p\mathbb{Z}$ by sending $\frac{a}{b} + I$ to $[x]_p$ where $x \in \mathbb{Z}$ is chosen so that $a \equiv bx \pmod{p}$. This is well-defined by the last paragraph. Let $[a]_p \in \mathbb{Z}/p\mathbb{Z}$. We have $\varphi(a/1 + I) = [a]_p$. Thus, φ is surjective. Let $\frac{a}{b} + I$ and $\frac{c}{d} + I$ be in T/I and choose $x, y \in \mathbb{Z}$ as above so that $\frac{a}{b} + I = x/1 + I$ and $\frac{c}{d} + I = y/1 + I$. Observe that $a + c \equiv bx + dy \pmod{p}$ and $ac \equiv bxdy \pmod{p}$. This gives

$$\begin{aligned}
\varphi(a/b + I + c/d + I) &= \varphi(x/1 + I + y/1 + I) \\
&= \varphi((x+y)/1 + I) \\
&= [x+y]_p \\
&= [x]_p + [y]_p \\
&= \varphi(x/1 + I) + \varphi(y/1 + I) \\
&= \varphi(a/b + I) + \varphi(c/d + I)
\end{aligned}$$

and

$$\begin{aligned}
\varphi((a/b + I)(c/d + I)) &= \varphi((x/1 + I)(y/1 + I)) \\
&= \varphi((xy)/1 + I) \\
&= [xy]_p \\
&= [x]_p[y]_p \\
&= \varphi(x/1 + I)\varphi(y/1 + I) \\
&= \varphi(a/b + I)\varphi(c/d + I).
\end{aligned}$$

Thus, φ is a homomorphism. It only remains to show that φ is injective. Let $a/b + I \in \ker\varphi$. Thus, we must have $p \mid x$. However, this shows that since $a \equiv bx \pmod{p}$ that necessarily $p \mid a$, i.e., $a/b + I = 0 + I$. Thus, $\ker\varphi = \{0 + I\}$ and the map is injective. Hence, we have shown φ is an isomorphism. $\square$

3. Let $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ where $i^2 = -1$.

   (a) Show the map $\varphi : \mathbb{Q}(i) \to \mathbb{Q}(i)$ sending $a + bi$ to $a - bi$ is an isomorphism.

Proof. Let $a + bi \in \mathbb{Q}(i)$. We have $\varphi(a - bi) = a + bi$ so φ is surjective. We have $a + bi = c + di$ if and only if $a = b$ and $c = d$. Thus, if $\varphi(a + bi) = \varphi(c + di)$ then $a - bi = c - di$ so $a = b$ and $c = d$, i.e., φ is injective.
Let $a + bi, c + di \in \mathbb{Q}(i)$. We have

$$\begin{aligned}\varphi((a+bi)+(c+di)) &= \varphi((a+c)+(b+d)i)\\ &= (a+c)-(b+d)i\\ &= (a-bi)+(c-di)\\ &= \varphi(a+bi)+\varphi(c+di)\end{aligned}$$

and

$$\begin{aligned}\varphi((a+bi)(c+di)) &= \varphi((ac-bd)+(ad+bc)i)\\ &= (ac-bd)-(ad+bc)i\\ &= (a-bi)(c-di)\\ &= \varphi(a+bi)\varphi(c+di).\end{aligned}$$

Thus, φ is an isomorphism. $\square$

(b) Show that $\mathbb{Q}[x]/\langle x^2 + 1\rangle \cong \mathbb{Q}(i)$.

Proof. Define $\psi : \mathbb{Q}[x] \to \mathbb{Q}(i)$ by sending f to $f(i)$. As has been explained in class, we can view $f \in \mathbb{Q}(i)[x]$ and so f induces a map from $\mathbb{Q}(i)$ to $\mathbb{Q}(i)$; this is what $f(i)$ means. Let $a + bi \in \mathbb{Q}(i)$. We have $\psi(a + bx) = a + bi$ so ψ is surjective. As this is an evaluation map, it is a ring homomorphism. It only remains to show that $\ker\psi = \langle x^2 + 1\rangle$. Let $f \in \langle x^2 + 1\rangle$. Then $f = (x^2 + 1)g$ for some $g \in \mathbb{Q}[x]$. Thus, $f(i) = (i^2 + 1)g(i) = 0$ so $f \in \ker\psi$. Let $f \in \ker\psi$, i.e., $f(i) = 0$. This gives that i is a root of f. We showed in class this means $\tau(i)$ is a root of $\tau(f)$ for any $\tau : \mathbb{Q}(i) \to \mathbb{Q}(i)$ an isomorphism where $\tau(f)$ is defined by applying τ to the coefficients of f. Applying this result with the map φ from part (a) gives that $-i = \varphi(i)$ is a root of $\varphi(f) = f$ where we have used f has coefficients in $\mathbb{Q}$ so $\varphi(f) = f$. Thus, $x^2 + 1 = (x - i)(x + i) \mid f$ and so $\ker\psi = \langle x^2 + 1\rangle$ as claimed. $\square$

4. Let R be a commutative ring with identity. Prove that R is a field if and only if $\langle 0_R\rangle$ is a maximal ideal.

Proof. We know from our work in class that $\langle 0_R \rangle$ is a maximal ideal if and only if $R/\langle 0_R \rangle$ is a field. However, define $\varphi : R \to R$ by $r \mapsto r$. We see this is a surjective ring homomorphism with kernel $\langle 0_R \rangle$, so the first isomorphism theorem gives $R/\langle 0_R \rangle \cong R$. This gives the result. $\square$

5. Show that the ideal $\langle x - 1 \rangle$ in $\mathbb{Z}[x]$ is a prime ideal but not a maximal ideal.

   Proof. Define the map $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ by $f \mapsto f(1)$. Let $m \in \mathbb{Z}$. Then $\varphi(m) = m$ so the map is surjective. As we have shown in class several times, an evaluation map is a ring homomorphism so this is a surjective ring homomorphism. We claim $\ker \varphi = \langle x - 1 \rangle$. Let $f \in \langle x - 1 \rangle$ so $f = (x - 1)g$ for some $g \in \mathbb{Z}[x]$. Thus, $f(1) = (1 - 1)g(1) = 0$. Thus, $\langle x - 1 \rangle \subset \ker \varphi$. Conversely, if $f(1) = 0$ then 1 is a root of f and so $(x - 1) \mid f$, i.e., $f \in \langle x - 1 \rangle$. Thus, $\ker \varphi = \langle x - 1 \rangle$. The first isomorphism theorem gives $\mathbb{Z}[x]/\langle x - 1 \rangle \cong \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, $\langle x - 1 \rangle$ is a prime ideal, but since $\mathbb{Z}$ is not a field $\langle x - 1 \rangle$ is not a maximal ideal. $\square$

6. Let p be a fixed prime number in $\mathbb{Z}$. Let J be the set of polynomials in $\mathbb{Z}[x]$ whose constant terms are divisible by p. Prove that J is a maximal ideal in $\mathbb{Z}[x]$.

   Proof. Define $\varphi : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$ by sending $f = \sum_{j=0}^{n} a_j x^j$ to $[a_0]_p$. We have seen before that the map $\mathbb{Z}[x] \to \mathbb{Z}$ given by sending a polynomial to its constant term is a surjective ring homomorphism, and the map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ given by sending a to $[a]_p$ is a surjective ring homomorphism. It is clear that φ is a composition of these two maps, and so is a surjective ring homomorphism as the composition of surjective maps is surjective and the composition of ring homomorphisms is a ring homomorphism. Observe that if $f \in J$ then $\varphi(f) = [0]_p$. Moreover, if $f \in \ker \varphi$ then the constant term of f must be divisible by p. Thus, $J = \ker \varphi$. Since the kernel of a ring homomorphism is an ideal, this shows J is an ideal. Moreover, the first isomorphism theorem gives $\mathbb{Z}[x]/J \cong \mathbb{Z}/p\mathbb{Z}$, a field. Thus J is a maximal ideal as claimed. $\square$