Homework Assignment 13 Solutions

1. In class we proved a cancellation law for integral domains. We can actually say something a bit stronger (and quite useful). Let R be a ring and $a, b, c \in R$. Suppose that a is not zero or a zero divisor, and that $ab = ac$. Prove $b = c$.

   Proof. We can rewrite $ab = ac$ as $ab - ac = 0$, and the factor using the distributive law to show that $a(b - c) = 0$. Since a is not a zero divisor, the only thing it can be multiplied by to get 0 is 0 itself, so that $b - c = 0$. Therefore $b = c$. □

2. Let R and S be rings and $\varphi : R \to S$ a ring homomorphism.

   (a) Show that $\operatorname{im}\varphi$ is a subring of S.

   Proof. We know from HW 4 Problem 4(b) that $\operatorname{im}\varphi$ is an additive subgroup of S. It remains to show that it is closed under products. Fix $x, y \in \operatorname{im}\varphi$, and write $x = \varphi(a)$ and $y = \varphi(b)$ for $a, b \in R$. Then since φ is a ring homomorphism, we can directly verify that:

   $$xy = \varphi(a)\varphi(b) = \varphi(ab) \in \operatorname{im}\varphi.$$

   □

   (b) Show that $\ker\varphi$ is a (two-sided) ideal of R.

   Proof. We know from HW 4 Problem 4(a) that $\ker\varphi$ is an additive subgroup of R. It remains to show it is an ideal. We first point out a general fact that we will use from now on without mention: *the condition of being a (left or right) ideal is stronger than being closed under multiplication.* That is, if $I \subseteq R$ is an abelian subgroup and for all $r \in R$ and $i \in I$, $ri \in I$, then checking on $r \in I$ shows I is closed under multiplication. In particular, from now on we will only check the ideal condition, since that will also imply that I is closed under multiplication (and therefore a subring).

   We therefore now show $\ker\varphi$ satisfies the ideal condition on both sides. Let $a \in \ker\varphi$ and $r \in R$. Then for any $r \in R$ we have:

   $$\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0,$$

   $$\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0.$$

   Therefore $ra, ar \in \ker\varphi$ and so φ is a two-sided ideal. □

   (c) Suppose $J \subseteq S$ is an ideal. Show that $\varphi^{-1}(J)$ is an ideal of R.

   Proof. We must have shown at some point that the preimage of a subgroup is a subgroup, but I can't find it in my notes so I will prove it here. Nonemptyness follows because $0 \in J$ and $\varphi(0) = 0$, so that $0 \in \varphi^{-1}(J)$. Fix $a, b \in \varphi^{-1}(J)$. Then $\varphi(a - b) = \varphi(a) - \varphi(b) \in J$ so that $a - b \in \varphi^{-1}(J)$ and therefore by the subgroup criterion (HW4 2a) $\varphi^{-1}(J)$ is a subgroup. Also notice that if $\varphi(a) \in J$, the fact that J is a two-sided ideal implies that

   $$\varphi(ra) = \varphi(r)\varphi(a) \in J,$$

$$\varphi(ar) = \varphi(a)\varphi(r) \in J.$$

Therefore $ar, ra \in \varphi^{-1}(J)$ and so it is an ideal. (Observe that this proof shows the preimage of a left (resp. right) ideal is a left (resp. right) ideal). $\square$

(d) Suppose R and S are unital rings with *nonzero* identities 1_R and 1_S respectively. Prove that if $\varphi(1_R) \neq 1_S$ then $\varphi(1_R)$ is either zero, or a zero divisor in S.

Proof. We prove the contrapositive. Notice that

$$1_S \cdot \varphi(1_R) = \varphi(1_R) = \varphi(1_R \cdot 1_R) = \varphi(1_R)\varphi(1_R).$$

If $\varphi(1_R)$ is not a zero divisor or 0, then using Problem 1 we can cancel it on the right on both sides, and deduce that $1_S = \varphi(1_R)$. $\square$

(e) Deduce that if S is an integral domain and φ is nonzero then $\varphi(1_R) = 1_S$. (*Remark:* many authors require rings to be unital, and also require ring homomorphisms to take the identity to the identity.)

Proof. If $\varphi(1_R) = 0$ then $\varphi(r) = \varphi(r \cdot 1_R) = \varphi(r)\varphi(1_R) = 0$, so φ is the zero map. Therefore $\varphi(1_R)$ is nonzero. Since S has no zero divisors (it is an integral domain), we also know $\varphi(1_R)$ is not a zero divisor. By part (d) it must therefore be 1_S. $\square$

6. Let R be a commutative ring with $1 \neq 0$.

(a) Fix $a \in R$. Show that $(a) = R$ if and only if $a \in R^\times$.

Proof. We showed in class that $(a) = \{ra : r \in R\}$. Suppose $(a) = R$. Then there is some $r \in R$ such that $ra = 1$. Since R is commutative this implies that $a \in R^\times$. Conversely, if $a \in R^\times$ then there is some $r \in R$ so that $ra = 1$. Thus $1 \in (a)$. Fix $f \in R$, then $f = f \cdot 1 \in (a)$. This shows $R \subseteq (a)$. $\square$

(b) Fix $a, b \in R$, and suppose that a is not a zero divisor. Show that $(a) = (b)$ if and only if $a = ub$ for some unit $u \in R^\times$.

Proof. If $a = ub$ for some unit then $a \in (b)$ so that $(a) \subseteq (b)$. But also $b = u^{-1}a \in (a)$ so that $(b) \subseteq (a)$. Conversely, if $(a) = (b)$ then $a = xb$ and $b = ya$. We must show x is a unit. Substituting, $a = xya$. Since a is not a zero divisor we may use Problem 1 to cancel so that $xy = 1$, and therefore x and y are units, completing the proof. $\square$

(c) Let I be any ideal. Show that $I = R$ if and only if I contains a unit $u \in R^\times$.

Proof. If $I = R$ then $1 \in I$ so that I contains a unit. Conversely, suppose I contains a unit u. Then I contains $uu^{-1} = 1$, and so it contains $f = f \cdot 1$ for any $f \in R$. Thus $R \subseteq I$ as desired. $\square$

(d) Prove that R is a field if and only if the only ideals in R are (0) and R itself.

Proof. Suppose R is a field. If I is a nonzero ideal then I contains a unit (as any nonzero element of a field is a unit), so that $I = R$ by part (c). Conversely, suppose the only ideals of R are (0) and R, and consider any nonzero $a \in R$. (a) is nonzero so it must be all of R. Thus $a \in R^\times$ by part (a). Therefore every nonzero element of R is a unit, but that's what it means to be a field. □

7. Let R be a commutative ring. The *nilradical* of R is $\mathfrak{N}(R) = \{r \in R : r \text{ is nilpotent}\}$. By HW12 Problem 3 we know that $\mathfrak{N}(R)$ is an ideal of R.

   (a) Show that $R/\mathfrak{N}(R)$ is reduced. This is often called the *reduction of* R, and is denoted R_{red}.

   Proof. Let $r+\mathfrak{N}(R)$ be a nilpotent element of $R/\mathfrak{N}(R)$. Then $(r+\mathfrak{N}(R))^n = r^n+\mathfrak{N}(R) = 0$, or equivalently $r^n \in \mathfrak{N}(R)$. This means r^n is nilpotent in R, so that $0 = (r^n)^m = r^{nm}$. But this says that r was nilpotent to begin with, i.e., that $r \in \mathfrak{N}(R)$. In particular $r + \mathfrak{N}(R) = 0$ in $R/\mathfrak{N}(R)$ and so the only nilpotent element of the quotient is the zero element, but that's what it means to be reduced. □

   (b) Compute $\mathfrak{N}(R)$ and R_{red} for the following two rings.

   i. $R = \mathbb{Z}[x]/(x)^n$ for $n \geq 2$.

   Proof. We freely use that $(x)^n = (x^n)$. Indeed, every element is the n-fold product of multiples of x, but this is precisely a multiple of x^n (using commutativity).

   To simplify notation, we will think about elements of R as polynomials over $\mathbb{Z}$, but replace equality with congruence modulo x^n. We now compute $\mathfrak{N}(R)$. First notice that if $f \in (x)$, then $f = xg$ for some $g \in \mathbb{Z}[x]/(x^n)$. Therefore $f^n = x^n g^n \equiv 0 \mod x^n$, so that $f \in \mathfrak{N}(R)$. This implies that $(x) \subseteq \mathfrak{N}(R)$. On the other hand, suppose that $f \notin (x)$. Then $f = a + xg$ for some integer $a \neq 0$. Then the binomial theorem says that:

$$f^r = a^r + x(\text{stuff}).$$

   Since $a \neq 0$ we know $a^n \neq 0$ so that $f^r \notin (x^n)$. In particular, $f^r \not\equiv 0 \mod x^n$. Because R was arbitrary, we can conclude that $f \notin \mathfrak{N}(R)$. In particular, we have shown that $\mathfrak{N}(R) = (x)$.

   We will now compute $R_{red} = R/\mathfrak{N}(R)$. There are a number of ways to do this. Perhaps the slickest is to use the third isomorphism theorem, identifying $(x) \subseteq R$ as $(x)/(x^n)$. Then

$$R/\mathfrak{N}(R) = \frac{\mathbb{Z}[x]/(x^n)}{(x)/(x^n)} \cong \mathbb{Z}[x]/(x) \cong \mathbb{Z}.$$

   Another way is to consider the map $\pi : R \to \mathbb{Z}$ which takes (the class of) a polynomial f to the constant term $f(0)$. This is well defined because if $f \equiv \hat{f} \mod x^n$ then $f = \hat{f} + x^n g$ so that $f(0) = \hat{f}(0) + 0^n g(0) = \hat{f}(0)$. One easily checks it is a homomorphism, since for any polynomials $(f+g)(0) = f(0)+g(0)$ and $(fg)(0) = f(0)g(0)$ (or similarly when evaluated at any element). (One can also see this is a well defined homomorphism by noticing that (x^n) is contained in the kernel of the evaluation at

0 map from $\mathbb{Z}[x] \to \mathbb{Z}$, and then passing to the quotient: Problem 3(c)). Therefore $R/\ker\pi \cong \mathbb{Z}$. But $\ker\pi$ is the set of polynomials whose constant term is 0, which is precisely $(x) = \mathfrak{N}(R)$. □

ii. $R = \mathbb{Z}/p^n\mathbb{Z}$ for $n \geq 2$.

Proof. As before, we will think about elements of R as integers, and replace equality with congruence modulo p^n. We would first like to see that $\mathfrak{N}(R) = (p)$. Indeed, if xp is a multiple of p, then

$$(xp)^n = x^n p^n \equiv 0 \mod p^n,$$

showing that $(p) \subseteq \mathfrak{N}(R)$. Conversely, suppose $x^r \equiv 0 \mod p^n$ for some r. Then $p^n | x^r$ so that $p | x^r$, which by Euclid's lemma implies that $p | x$, i.e., that $x \in (p)$. This proves that $\mathfrak{N}(R) = (p)$. Next we use the third isomorphism theorem to observe that:

$$R/\mathfrak{N}(R) = \frac{\mathbb{Z}/p^n\mathbb{Z}}{p\mathbb{Z}/p^n\mathbb{Z}} \cong \mathbb{Z}/p\mathbb{Z}.$$

□