Math 562 **Spring 2014**
Homework 3 **Drew Armstrong**

Let R be a ring. We say that R is a domain if for all $a, b \in R$ we have

$$ab = 0 \quad \Longrightarrow \quad a = 0 \text{ or } b = 0,$$

that is, if the ring has no zerodivisors.

1. Prime Ideals. Given an ideal $I \leq R$ in a general ring R we say that I is prime if for all $a, b \in R$ we have

$$ab \in I \quad \Longrightarrow \quad a \in I \text{ or } b \in I.$$

(a) If $I \leq R$ is a prime ideal, prove that R/I is a domain.
(b) If R/I is a domain, prove that I is a prime ideal.
(c) Prove that every maximal ideal is prime. [Hint: Every field is a domain.]

Proof. For part (a), let $I \leq R$ be a prime ideal. To show that R/I is a domain we consider $a+I$ and $b+I$ in R/I such that $(a+I)(b+I) = ab+I = 0+I$ (the zero coset). If $ab+I = I$ then we have $ab \in I$. Since I is prime this implies that $a \in I$ (i.e. $a+I = I$) or $b \in I$ (i.e. $b+I = I$). We have shown that

$$(a+I)(b+I) = I \quad \Longrightarrow \quad a+I = I \text{ or } b+I = I,$$

and hence R/I is a domain.

For part (b), let R/I be a domain and consider $a, b \in R$ such that $ab \in I$ (i.e. $ab + I = I$). Since R/I is a domain the fact that $(a+I)(b+I) = ab+I = I$ implies that $a+I = I$ (i.e. $a \in I$) or $b+I = I$ (i.e. $b \in I$). We have shown that

$$ab \in I \quad \Longrightarrow \quad a \in I \text{ or } b \in I,$$

hence $I \leq R$ is a prime ideal.

For part (c), let $I \leq R$ be a **maximal** ideal. In class we saw that this implies that the quotient ring R/I is a field. Hence R/I is a domain (every field is a domain). Then by part (b) we conclude that $I \leq R$ is a **prime** ideal. $\square$

[Maximal always implies prime but not the other way around. However, in some very special rings it may be true that prime implies maximal. See Problem 3 below.]

2. Domain = Subring of a Field. In this problem you will prove that R is a domain if and only if R is a subring of a field.

(a) If R is a subring of a field K, prove that R is a domain.
(b) Let R be a domain and define the set of fractions:

$$\text{Frac}(R) := \left\{ \left[\frac{a}{b}\right] : a, b \in R, b \neq 0 \right\}.$$

At first these are just abstract symbols. We define a relation on Frac(R) by saying that $\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right]$ if and only if $ad = bc$. Prove that this is an **equivalence relation**.

(c) Now we define "multiplication" and "addition" of fractions by:

$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] := \left[\frac{ac}{bd}\right] \quad \text{and} \quad \left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] := \left[\frac{ad+bc}{bd}\right].$$

Prove that these operations are **well-defined**.

(d) It follows that $\mathrm{Frac}(R)$ is a field (you don't need to check this) since for all nonzero $\left[\frac{a}{b}\right]$ we have $\left[\frac{a}{b}\right]^{-1} = \left[\frac{b}{a}\right]$. Prove that the map $\iota : R \to \mathrm{Frac}(R)$ defined by $\iota(a) := \left[\frac{a}{1}\right]$ is an injective ring homomorphism. Use the First Isomorphism Theorem to conclude that R is isomorphic to a subring of its field of fractions $\mathrm{Frac}(R)$.

Proof. For part (a), let R be a subring of a field K. Suppose for contradiction that we have $a, b \in R$ with $ab = 0$ and $a, b \neq 0$. Since $0 \neq a \in K$ there exists $a^{-1} \in K$ (maybe not in R) such that $a^{-1}a = 1$. But then

$$\begin{aligned} ab &= 0 \\ a^{-1}ab &= a^{-1}0 \\ b &= 0. \end{aligned}$$

Contradiction.

For part (b), consider the relation on fractions defined by $\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right]$ if and only if $ad = bc$. To see that the relation is reflexive note that for all $a, b \in R$ with $b \neq 0$ we have $ab = ba$ and hence $\left[\frac{a}{b}\right] = \left[\frac{a}{b}\right]$. To see that the relation is symmetric, consider $a, b, c, d \in R$ with $b, d \neq 0$ such that $\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right]$, i.e., $ad = bc$. Since the usual equals sign is symmetric this implies that $cb = da$ and hence $\left[\frac{c}{d}\right] = \left[\frac{a}{b}\right]$. To show that the relation is transitive, consider $a, b, c, d, e, f \in R$ with $b, d, f \neq 0$ and assume that $\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right]$ and $\left[\frac{c}{d}\right] = \left[\frac{e}{f}\right]$, i.e., $ad = bc$ and $cf = de$. It follows that

$$\begin{aligned} c(af - be) &= c(af) - c(be) \\ &= a(cf) - (bc)e \\ &= a(de) - (ad)e \\ &= 0. \end{aligned}$$

Since R is a domain and $c \neq 0$ this implies that $af - be = 0$, hence $\left[\frac{a}{b}\right] = \left[\frac{e}{f}\right]$.

For part (c) we assume that $\left[\frac{a}{b}\right] = \left[\frac{a'}{b'}\right]$ (i.e. $ab' = a'b$) and $\left[\frac{c}{d}\right] = \left[\frac{c'}{d'}\right]$ (i.e. $cd' = c'd$). To see that multiplication is well-defined note that

$$\begin{aligned} (ac)(b'd') &= (ab')(cd') \\ &= (a'b)(c'd) \\ &= (bd)(a'c'), \end{aligned}$$

hence

$$\left[\frac{a}{b}\right]\left[\frac{c}{d}\right] = \left[\frac{ac}{bd}\right] = \left[\frac{a'c'}{b'd'}\right] = \left[\frac{a'}{b'}\right]\left[\frac{c'}{d'}\right].$$

To see that addition is well-defined note that

$$\begin{aligned} (ad + bc)(b'd') &= (ad)(b'd') + (bc)(b'd') \\ &= (ab')(dd') + (bb')(cd') \\ &= (a'b)(dd') + (bb')(c'd) \\ &= (bd)(a'd') + (bd)(b'c') \\ &= (bd)(a'd' + b'c'), \end{aligned}$$

hence

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad + bc}{bd}\right] = \left[\frac{a'd' + b'c'}{b'd'}\right] = \left[\frac{a'}{b'}\right] + \left[\frac{c'}{d'}\right].$$

For part (d) consider $a, b \in R$. Then we have

$$\iota(a) + \iota(b) = \left[\frac{a}{1}\right] + \left[\frac{b}{1}\right] = \left[\frac{a \cdot 1 + 1 \cdot b}{1 \cdot 1}\right] = \left[\frac{a+b}{1}\right] = \iota(a+b),$$

and

$$\iota(a)\iota(b) = \left[\frac{a}{1}\right]\left[\frac{b}{1}\right] = \left[\frac{ab}{1 \cdot 1}\right] = \left[\frac{ab}{1}\right] = \iota(ab).$$

Since $\iota(1) = \left[\frac{1}{1}\right]$ is the unit element of $\text{Frac}(R)$ we conclude that $\iota : R \to \text{Frac}(R)$ is a ring homomorphism. To see that it is injective, suppose that $\iota(a) = \left[\frac{a}{1}\right] = \left[\frac{b}{1}\right] = \iota(b)$. By definition of equivalence of fractions this implies that $a = a \cdot 1 = 1 \cdot b = b$. Finally, recall that the image $\operatorname{im} \iota$ is a subring of $\text{Frac}(R)$. By the First Isomorphism Theorem we have

$$R = \frac{R}{(0)} = \frac{R}{\ker \iota} \approx \operatorname{im} \iota \subseteq \text{Frac}(R).$$

We conclude that R is isomorphic to a subring of the field $\text{Frac}(R)$. $\square$

3. Prime $\Longrightarrow$ Maximal in a PID. In Problem 1 we saw that every maximal ideal in a general ring is prime. Now let R be a PID. We will see that every prime ideal in R is maximal.

(a) Let $I \leq R$ be a prime ideal. Since R is a PID we have $I = (p)$ for some $p \in R$. Show that for all $a, b \in R$ we have

$$p|ab \quad \Longrightarrow \quad p|a \text{ or } p|b.$$

We say that $p \in R$ is a prime element.

(b) We say that $a \in R$ is an irreducible element if for all $b, c \in R$ we have

$$a = bc \quad \Longrightarrow \quad b \text{ or } c \text{ is a unit.}$$

Prove that every prime element in a PID is irreducible.

(c) Use this to conclude that every prime ideal in a PID is maximal. [Hint: Let $I \leq R$ be a prime ideal. Then $I = (p)$ for some prime element $p \in R$. By part (c), this p is also irreducible. Then what?]

Proof. For part (a), let $I \leq R$ be a prime ideal. Since R is a PID we have $I = (p)$ for some $p \in R$. Now let $a, b \in R$ such that $p|ab$, i.e., $ab \in (p)$. Since (p) is a prime ideal this implies that $a \in (p)$ (i.e. $p|a$) or $b \in (p)$ (i.e. $p|b$). We conclude that $p \in R$ is a prime element.

For part (b), let $p \in R$ be a prime element. We wish to show that p is irreducible. So assume for contradiction that we have $p = ab$ where a and b are both nonunits. In particular we have $p|ab$, which implies that $p|a$ or $p|b$ since p is prime. Without loss of generality suppose that $p|a$, i.e., $a = pu$ for some $u \in R$. Substituting this into $p = ab$ gives

$$\begin{aligned} p &= ab \\ p &= pub \\ p(1 - ub) &= 0. \end{aligned}$$

Since R is a domain and $p \neq 0$ this implies that $1 - ub = 0$, and hence b is a unit. Contradiction. [Note that part (b) only uses the fact that R is a domain. We will use the fact that R is a PID in part (c).]

For part (c), let $I \leq R$ be a **prime** ideal. By part (a) this implies that $I = (p)$ for some prime element $p \in R$. Now we wish to show that (p) is a **maximal** ideal. Assume for contradiction that there exists an ideal $(p) < J < (1)$. Since R is a PID we have $J = (a)$ for some $a \in R$. Then $(p) < (a)$ implies that there exists $b \in R$ with $p = ab$ where b is not a unit (if b were a unit we would have $a = pb^{-1} \in (p)$, hence $(a) \leq (p)$), and $(a) < (1)$ implies that

a is not a unit (recall HW1.6). We have expressed $p = ab$ as a product of nonunits, which contradicts the fact that p is irreducible. Hence (p) is maximal. $\square$

4. Polynomials Over a Domain. Let R be a domain and consider the ring $R[x]$. Given a polynomial $f(x) = \sum_{k\geq 0} a_k x^k \in R[x]$ we define $\deg(f)$ to be the largest k such that $a_k \neq 0$.

(a) Given $f, g \in R[x]$ prove that $\deg(fg) = \deg(f) + \deg(g)$.
(b) Prove that $R[x]$ is a domain.
(c) Prove that the group of units is $R[x]^\times = R^\times$.
(d) Give a specific example to show that (c) can fail when R is not a domain. [Hint: Let $R = \mathbb{Z}/4\mathbb{Z}$. Show that the polynomial $1 + 2x \in (\mathbb{Z}/4\mathbb{Z})[x]$ is a unit.]

Proof. For part (a), suppose that $f(x) = \sum_k a_k x^k$ has degree m and $g(x) = \sum_k b_k x^k$ has degree n. Recall that the coefficient of x^k in $f(x)g(x)$ is $\sum_{i+j=k} a_i b_j$. The coefficient of x^{m+n} is $a_m b_n$ which is nonzero because $a_m \neq 0$ and $b_n \neq 0$. Note that if $k > m + n$ then $i + j = k$ implies that either $i > m$ (hence $a_i = 0$) or $j > n$ (hence $b_j = 0$), and it follows that every term in the sum $\sum_{i+j=k} a_i b_j$ is zero, hence the coefficient of x^k in $f(x)g(x)$ is zero. We conclude that the degree of $f(x)g(x)$ is $m + n$.

For part (b), consider $f, g \in R$, both nonzero. We wish to show that fg is nonzero. If $\deg(f) = \deg(g) = 0$ then f, g are constants and the fact that $fg \neq 0$ follows from the fact that R is a domain. If either of $\deg(f), \deg(g)$ is > 0 then $\deg(fg) = \deg(f) + \deg(g) > 0$ and we conclude that fg is not zero.

For part (c), we will abuse notation and identify the ring element $a \in R$ with the polynomial $a + 0x + 0x^2 + \cdots \in R[x]$. I claim that the unit polynomials are just the polynomials $a + 0x + 0x^2 + \cdots$ where $a \in R$ is a unit. Indeed, suppose that $a \in R^\times$ so there exists $a^{-1} \in R$. Then $a \in R[x]$ is also a unit with

$$(a + 0x + 0x^2 + \cdots)^{-1} = a^{-1} + 0x + 0x^2 + \cdots,$$

hence $R^\times \subseteq R[x]^\times$. Conversely, suppose that $f(x) \in R[x]$ is a unit, i.e., there exists $g(x) \in R[x]$ such that $f(x)g(x) = 1$. Using part (a) gives

$$\deg(f) + \deg(g) = \deg(fg) = \deg(1) = 0.$$

Since $\deg(f), \deg(g) \geq 0$ this implies that $\deg(f) = \deg(g) = 0$. Hence f is a constant and we conclude that $f \in R^\times$. Hence $R[x]^\times \subseteq R^\times$.

For part (d), consider the polynomial $1 + 2x \in (\mathbb{Z}/4\mathbb{Z})[x]$. This polynomial is **not** constant because $2 \neq 0$ in $\mathbb{Z}/4\mathbb{Z}$. Nevertheless, it is a unit because

$$(1 + 2x)(1 + 2x) = 1 + 4x + 4x^2 = 1 + 0x + 0x^2 = 1 \in (\mathbb{Z}/4\mathbb{Z})[x].$$

$\square$

[The general theorem says the following: The polynomial $f(x) \in R[x]$ is a unit if and only if its constant coefficient is a unit and every other coefficient is nilpotent in R. (For example, 2 is nilpotent in $\mathbb{Z}/4\mathbb{Z}$ because $2^2 = 0$.) Try to prove it if you want.]

5. Prime $\not\Rightarrow$ Maximal in General.

(a) Let $I \leq R$ be an ideal in a general ring and consider the map

$$\varphi : R[x] \to (R/I)[x]$$

defined by $\sum_k a_k x^k \mapsto \sum_k (a_k + I)x^k$. Show that φ is a surjective ring homomorphism.

(b) Show that the kernel of φ is the set

$$I[x] := \left\{ \sum_k a_k x^k \in R[x] : a_k \in I \text{ for all } k \right\},$$

and hence $I[x] \leq R[x]$ is an ideal.

(c) Use the First Isomorphism Theorem to conclude that $(R/I)[x] \approx (R[x])/(I[x])$.

(d) Consider the prime (hence maximal) ideal $3\mathbb{Z}$ in the PID $\mathbb{Z}$. Show that $3\mathbb{Z}[x]$ is a prime ideal of $\mathbb{Z}[x]$ that is not maximal. Conclude that $\mathbb{Z}[x]$ is not a PID. [Hint: Use Problem 4 to show that $(\mathbb{Z}/3\mathbb{Z})[x]$ is a domain but not a field. Use part (c) and Problem 1 to conclude that $3\mathbb{Z}[x]$ is prime but not maximal. Use Problem 3 to conclude that $\mathbb{Z}[x]$ is not a PID.]

Proof. For part (a), consider polynomials $f(x) = \sum_k a_k x^k$ and $g(x) = \sum_k b_k x^k$ in $R[x]$. Then we have

$$\begin{aligned}
\varphi(f+g) &= \varphi\left(\sum_k (a_k + b_k) x^k\right) \\
&= \sum_k \left((a_k + b_k) + I\right) x^k \\
&= \sum_k \left((a_k + I) + (b_k + I)\right) x^k \\
&= \sum_k (a_k + I) x^k + \sum_k (b_k + I) x^k \\
&= \varphi(f) + \varphi(g),
\end{aligned}$$

and

$$\begin{aligned}
\varphi(fg) &= \varphi\left(\sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k\right) \\
&= \sum_k \left(\left(\sum_{i+j=k} a_i b_j\right) + I\right) x^k \\
&= \sum_k \left(\sum_{i+j=k} (a_i b_j + I)\right) x^k \\
&= \sum_k \left(\sum_{i+j=k} (a_i + I)(b_j + I)\right) x^k \\
&= \left(\sum_k (a_k + I) x^k\right)\left(\sum_k (b_k + I) x^k\right) \\
&= \varphi(f)\varphi(g).
\end{aligned}$$

Finally, φ sends the identify polynomial $1 + 0x + 0x^2 + \cdots$ in $R[x]$ to the identity polynomial $(1+I)+(0+I)x+(0+I)x^2+\cdots$ in $(R/I)[x]$. Thus φ is a ring homomorphism. It is surjective because the canonical map $a \mapsto a + I$ is a surjection $R \to R/I$.

For part (b), note that $f(x) = \sum_k a_k x^k \in R[x]$ is in the kernel of φ if and only if $\sum_k (a_k + I)x^k$ is the zero polynomial in $(R/I)[x]$. In other words, we have $f(x) \in \ker\varphi$ if and only if $a_k + I = I$ (i.e. $a_k \in I$) for all k. It follows that $\ker\varphi = I[x]$ and that this set is an ideal.

For part (c), the First Isomorphism Theorem says that

$$\frac{R[x]}{I[x]} = \frac{R[x]}{\ker\varphi} \approx \operatorname{im}\varphi = (R/I)[x].$$

For part (d), consider the ideal $3\mathbb{Z} \leq \mathbb{Z}$ in the ring of integers. By part (c) we have

$$\frac{\mathbb{Z}[x]}{3\mathbb{Z}[x]} \approx (\mathbb{Z}/3\mathbb{Z})[x].$$

Since $3\mathbb{Z} \leq \mathbb{Z}$ is a prime ideal (because 3 is a prime integer), Problem 1(a) says that $\mathbb{Z}/3\mathbb{Z}$ is a domain. Then Problem 4(b) says that $(\mathbb{Z}/3\mathbb{Z})[x]$ is a domain, and Problem 1(c) implies that $3\mathbb{Z}[x] \leq \mathbb{Z}[x]$ is a prime ideal. However, note that $(\mathbb{Z}/3\mathbb{Z})[x]$ is **not** a field. Indeed, the nonzero element $x \in (\mathbb{Z}/3\mathbb{Z})[x]$ has no multiplicative inverse because for all polynomials $f(x) \in (\mathbb{Z}/3\mathbb{Z})[x]$ we have $\deg(xf(x)) = \deg(x) + \deg(f) = \deg(f) + 1 > 0$ but $\deg(1) = 0$. Since $\mathbb{Z}[x]/3\mathbb{Z}[x]$ is not a field, it follows that $3\mathbb{Z}[x] \leq \mathbb{Z}[x]$ is not a maximal ideal. We have shown that $3\mathbb{Z}[x] \leq \mathbb{Z}[x]$ is a prime ideal that is not maximal. By Problem 3(c) it follows that the domain $\mathbb{Z}[x]$ is not a PID. $\square$

[We took a bit of a sneaky route to prove that $\mathbb{Z}[x]$ is not a PID. In particular, we showed that nonprincipal ideals exist, but we didn't give an example of one. Here's an example: The set of polynomials in $\mathbb{Z}[x]$ whose constant term is divisible by 3 is a nonprincipal ideal in $\mathbb{Z}[x]$ (i.e., it is not of the form $(f(x))$ for any $f(x) \in \mathbb{Z}[x]$). But it **is** generated by the two elements 3 and x. Try to prove that if you like. It turns out that every prime ideal of $\mathbb{Z}[x]$ can be generated by one or two elements. So it's not very far from a PID.]