Homework Assigment 13 Solutions

1. Let R be a unique factorization domain.

   (a) Fix $r \in R$. Show that r is irreducible if and only if it is prime.

   Proof. We showed in class that in any commutative unital ring prime elements are always irreducible. To prove the converse, suppose that x is an irreducible element of R. We hope to show that (x) is a prime ideal, so suppose $ab \in (x)$, so that $ab = rx$ for some $r \in R$. Since R is a UFD we have factorizations

   $$\begin{aligned} a &= p_1 p_2 \cdots p_i \\ b &= q_1 q_2 \cdots q_j \\ r &= \ell_1 \ell_2 \cdots \ell_k \end{aligned}$$

   into irreducible elements which are unique (up to units). This gives us unique factorizations of each side of $ab = rx$ into irreducibles:

   $$p_1 \cdots p_i q_1 \cdots q_j = \ell_1 \cdots \ell_k x.$$

   Since factorizations are unique, this imlies that x has to be (up to a unit) equal to one of the factors on the left side. Without loss of generality we may assume $ux = p_1$ for some $u \in R^\times$, so that $a = uxp_2 \cdots p_i$ so that $a \in (x)$ as desired. □

   (b) Let $a, b \in R$. Show that a greatest common denominator of a and b exists, and is unique up to multiplication by a unit.

   Proof. Pick unique factorizations

   $$a = p_1^{\alpha_1} \cdots p_t^{\alpha_t} \qquad b = p_1^{\beta_1} \cdots p_t^{\beta_t}$$

   where the α_i or β_i can be potentially 0. Then let

   $$d = p_1^{\min(\alpha_1,\beta_1)} \cdots p_t^{\min(\alpha_t,\beta_t)}.$$

   Then we claim that d is a gcd up to multiplication by a unit. Indeed, suppose r divides both a and b. Suppose $rx = a$ and pick factorizations:

   $$r = q_1 \cdots q_s \qquad x = \ell_1 \cdots \ell_k.$$

   Then $rx = a$ factors as:

   $$q_1 \cdots q_s \ell_1 \cdots \ell_k = \underbrace{p_1 \cdots p_1}_{\alpha_1\text{-times}} \cdots \underbrace{p_t \cdots p_t}_{\alpha_t\text{-times}}.$$

   By unique factorization, each of the q_i must be (up to a unit) one of the p_j, and can only appear a maximum of α_j times. That is,

   $$r = up_1^{\gamma_1} \cdots p_t^{\gamma_t},$$

for some $u \in R^\times$ and $\gamma_i \leq \alpha_i$. Arguing similarly, we see that $\gamma_i \leq \beta_i$ as well so that $\gamma_i \leq \min(\alpha_i, \beta_i)$ for each i. In particular, setting

$$z = p_1^{\min(\alpha_1,\beta_1)-\gamma_1} \cdots p_t^{\min(\alpha_t,\beta_t)-\gamma_t},$$

we may conclude that $d = u^{-1}rz$ so that $r|d$. This proves that d is indeed a gcd. Uniqueness of greatest common denominators in any integral domain was proved in class. □

2. Let's turn our attention to $\mathbb{Z}[\sqrt{-5}]$.

(a) Show that 3 is an irreducible element but not a prime element of $\mathbb{Z}[\sqrt{-5}]$.

Proof. We first show that 3 is irreducible. To this end suppose

$$3 = \alpha\beta = (a + b\sqrt{-5})(c + d\sqrt{-5}) = ac - 5bd + (ad + bc)\sqrt{-5}.$$

In particular,

$$ad + bc = 0 \text{ and } ac - 5bd = 3. \tag{1}$$

If $d \neq 0$ we may solve the first equation to get $b = -ac/d$, and substitute into the second to see that $6ac = 3$. Since $a, c \in \mathbb{Z}$, this cannot be, so $d = 0$. Therefore Equation 1 becomes:

$$bc = 0 \text{ and } ac = 3.$$

If $c = 0$ the second equation cannot hold, and so we deduce that $b = 0$. Therefore the factorization becomes $3 = ac$. Therefore $\alpha = a = \pm 3$ and $\beta = c = \pm 1$ or vice versa, and so either α or β is a unit. This proves that 3 is irreducible.

Next we consider the ideal generated by 3. Notice that $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9 \in (3)$. Nevertheless, given an $\alpha = a + b\sqrt{-5}$ with $a, b \in \mathbb{Z}$, we can directly compute that $3\alpha = 3a + 3b\sqrt{-5}$. In particular, $3a \neq 2$ nd $3b \neq \pm 1$, so $2 \pm \sqrt{-5} \notin (3)$. This witnesses the fact that (3) cannot be a prime ideal. □

(b) Deduce from part (a) that $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain. Explain why this means $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain.

Proof. If $\mathbb{Z}[\sqrt{-5}]$ were a UFD, the 1(a) would imply that irreducible elements would have to be prime, but 2(a) provides an example to show that this is not the case. Therefore $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Since PIDs are automatically UFDs, $\mathbb{Z}[\sqrt{-5}]$ cannot be a PID either. □

We now know abstractly that $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain. Let's exhibit an explicit nonprincipal ideal.

(c) Let $\mathfrak{p} \subseteq \mathbb{Z}[\sqrt{-5}]$ be any prime ideal containing 3. Prove that $\mathfrak{p}$ cannot be principal.

Proof. Suppose $\mathfrak{p} = (p)$ is generated by a single element. Since $3 \in (p)$ there is some $x \in \mathbb{Z}[\sqrt{-5}]$ with $3 = px$. By part (a) we know that 3 is irreducible, so that either p or x must be a unit. Since (p) is a proper ideal, HW11 Problem 5(a) says that p is not a unit, so x must be a unit. But then HW11 Problem 5(b) says that $(3) = (p)$, so that 3 generates a prime ideal contradication part (a). □

(d) Prove that the ideal $I = (3, 2 + \sqrt{-5})$ is a maximal ideal of $\mathbb{Z}[\sqrt{-5}]$ containing 3. Conclude that it cannot be principal. (*Hint:* Show $\mathbb{Z}[\sqrt{-5}]/(3)$ has 9 elements and $I/(3)$ has 3 elements. Then leverage the third isomorphism theorem for rings to compute $\mathbb{Z}[\sqrt{-5}]/I$.)

Proof. We first compute the order of $\mathbb{Z}[\sqrt{-5}]/(3)$. Each coset of $\mathbb{Z}[\sqrt{-5}]/(3)$ can be represented by an element $a + b\sqrt{-5}$. We can add and subtract any multiple of 3 without changing the coset, so that we may assume $a, b \in \{0, 1, 2\}$. Suppose $a + b\sqrt{-5} \equiv a' + b'\sqrt{-5} \mod 3$. So $(a-a')+(b-b')\sqrt{-5}$ is a multiple of 3, so that $a =\equiv a' \mod 3$ and $b \equiv b' \mod 3$. In particular, each coset has a *unique* representative with $a, b \in \{0, 1, 2\}$, which means there are precisely 9 elements.

To compute the order of $I/(3)$ we begin by noting that the fourth isomorphism theorem (HW 11 Problem 2(a)) gives a bijection between ideals of $Z[\sqrt{-5}]$ containing (3) and ideals of $\mathbb{Z}[\sqrt{-5}]/(3)$. Since $(3) \subsetneq I \subsetneq \mathbb{Z}[\sqrt{-5}]$, this says that that $I/(3)$ is a proper and nontrivial ideal of $\mathbb{Z}[\sqrt{-5}]/(3)$. By Langranges theorem, it's order must divide 9, so it is either 1,3,9. But since it is proper, it cannot be 9, and since it is nontrivial, it cannot be 1. So $I/(3)$ has 3 elements. We now apply the third isomorphism theorem for rings to see that

$$\mathbb{Z}[\sqrt{-5}]/I \cong \frac{\mathbb{Z}[\sqrt{-5}]/(3)}{I/(3)}.$$

By Lagrange's theorem, the right side has $9/3 = 3$ elements. Therefore $\mathbb{Z}[\sqrt{-5}]/I$ has 3 elements. It is also a commutative unital ring (since the quotient of any commutative unital ring is commutative and unital), and $1 \neq 0$ since is not the 0 ring. Finally, if J is an ideal of $\mathbb{Z}[\sqrt{-5}]/I$, then by Lagrange's theorem, it has either 1 or 3 elements. In particular, it is either the 0 ideal or the entire ring. Therefore by HW 11 Problem 5(d), we may conclude that $\mathbb{Z}[\sqrt{-5}]/I$ is a field. □

3. Let R be a Euclidean domain, and $N : R \to \mathbb{Z}_{\geq 0}$ a Euclidean norm. Let's explore how the norm can help us characterize the units in R.

(a) Let $m = \min\{N(x) : x \neq 0\}$. Show that if $N(x) = m$, then $x \in R^\times$.

Proof. Apply Euclidean divison to 1 and m, so that $1 = mq + r$ for $r = 0$ or $N(r) < N(m)$¿ The minimality of $N(m)$ among nonzero elements implies that the latter case cannot hold unless $r = 0$, so in either case $r = 0$ and $1 = mq$. Thus $m \in R^\times$. □

(b) Let $\hat{N} : R \to \mathbb{Z}$ be given by the following rule.

$$\hat{N}(r) = \min_{x \in R \setminus \{0\}} N(xr).$$

Prove that $\hat{N}$ is a Euclidean norm on R, and also that it satisfies the further condition that if $a|b$ and $b \neq 0$, then $\hat{N}(a) \leq \hat{N}(b)$.

Proof. Fix $a, b \in R$. We'd like to show there is some Euclidean divison algorithm for a and b with respect to $\hat{N}$. Notice that there is some $x \in R$ so that $\hat{N}(b) = N(xb)$. Since N is a Euclidean norm, we can do Euclidean division with respect to N. Let's divide a by xb. That is, there are q, r so that $a = qxb + r$ with $r = 0$ or $N(r) < N(xb)$. We claim that $q' = qx$ is a good Euclidean quotient for $\hat{N}$ (with the same remainder r). Indeed, if $r = 0$ we're already in good shape. Otherwise, we notice that by definition:

$$\hat{N}(r) \leq N(1r) = N(r) < N(xb) = \hat{N}(b).$$

This completes the proof that $\hat{N}$ is a Euclidean norm. For the second property, suppose that $a|b$. Then $b = ca$ for some c. Let $x \in R$ so that $\hat{N}(b) = N(xb)$. Then:

$$\hat{N}(a) \leq N(xca) = N(xb) = \hat{N}(b).$$

□

(c) Prove that $x \in R^\times$ if and only if $\hat{N}(x) = \hat{N}(1)$.

Proof. We first show that $m = \hat{N}(1) = \min\{N(z) : z \neq 0\}$. Indeed, let $z \neq 0$. Then $1|z$ so that by part (b), $\hat{N}(1) \leq \hat{N}(z)$. Therefore, if $\hat{N}(x) = \hat{N}(1)$, then part (a) implies that x is a unit. Conversely, if x is a unit then $x|1$ so that by part (b) $\hat{N}(x) \leq \hat{N}(1)$. Since $\hat{N}(1)$ is minimal, we must therefore be an have $\hat{N}(x) = \hat{N}(1)$. □

4. Let R be a principal ideal domain.

(a) Show that if $\mathfrak{p}$ is a prime ideal, then $R/\mathfrak{p}$ is also a principal ideal domain.

Proof. As $\mathfrak{p}$ is prime, $R/\mathfrak{p}$ is an integral domain. Furthermore, the fourth isomorphism theorem says that any ideal of $R/\mathfrak{p}$ is the image of some ideal I of R under the projection $\pi : R \to R/\mathfrak{p}$. Therefore let $I \subseteq R$ be an ideal, it suffices to show that $\pi(I)$ is principal. Since R is a PID, we know $I = (d)$. We will show that $\pi(I) = (\pi(d))$. The right side is contained in the left since $\pi(d) \in \pi(I)$. Conversely, we notice that if $\overline{x} \in \pi(I)$ then $\overline{x} = \pi(x)$ for some $x \in I$. But $x = dr$ for some $r \in R$, so that $\overline{x} = \pi(dr) = \pi(d)\pi(r) \in (\pi(d))$ as desired. □

(b) Show that if S is a multiplicative subset not containing 0, then $S^{-1}R$ is a principal ideal domain.

Proof. Let $R \hookrightarrow Q$ with Q the field of fractions of R. Since every element of S is a unit of Q, the *universal property* of the ring of fractions (TH3 Problem 2(d)) show that $S^{-1}R \subseteq Q$. Therefore it is an integral domain (being a subring of a field). Now let $I \subseteq S^{-1}R$ be an ideal. We know that $J = I \cap R$ is an ideal of R, and since R is a PID we know that $J = dR$ for some $d \in R$. We claim that d generates I in $S^{-1}R$. Indeed, $d \in J \subseteq I$ says that $dS^{-1}R \subseteq I$. Conversely, fix $\frac{a}{b} \in I$. Then $b\frac{a}{b} = a \in I \cap R = J$, so that $a = rd$ for some $r \in R$. Therefore

$$\frac{a}{b} = \frac{rd}{b} = \frac{r}{b}d \in dS^{-1}R$$

completing the proof. □

5. Let p a prime number so that $p \equiv 3 \mod 4$.

(a) Prove that p generates a maximal ideal of $\mathbb{Z}[i]$.

Proof. It was proved on the last day of lecture that if $p \equiv 3 \mod 4$ then p is irreducible in $\mathbb{Z}[i]$. We also proved that $\mathbb{Z}[i]$ is a PID, so that irreducible elements are prime, and thus (p) is a prime ideal. But in a PID, nonzero prime ideals are maximal, completing the proof. □

(b) Show that $\mathbb{Z}[i]/(p)$ is a field with p^2 elements. Denote it by $\mathbb{F}_{p^2}$.

Proof. Since (p) is a maximal ideal, we know $\mathbb{Z}[i]/(p)$ is a field. The cosets of $\mathbb{Z}[i]/(p)$ can be reperesented by elements $a+bi$, and since we can add multiples of p without changing the coset, we may assume $a, b \in \{0, 1, \cdots, p-1\}$. Furthermore, if $a+bi \equiv a'+b'i \mod p$, then $(a-a')+(b-b')i$ is a multiple of p, so that $a \equiv a' \mod p$ and $b \equiv b' \mod p$. In particular, each coset has a *unique* representative $a+bi$ with $a, b \in \{0, 1, \cdots, p-1\}$, so there are exactly p^2 elements. □

(c) Explain why $\mathbb{F}_{p^2} \not\cong \mathbb{Z}/p^2\mathbb{Z}$.

Proof. We first observe that they cannot be isomorphic as rings. Indeed, the former element is a field, so it has no nilpotents, but p is nilpotent in $\mathbb{Z}/p^2\mathbb{Z}$.

Although it is not strictly necessary, we can also observe that they are not even isomorphic as abelian groups. Indeed, if $x = a+bi$, then $\underbrace{x + \cdots + x}_{p\text{-times}} = 0$, where as $\mathbb{Z}/p^2\mathbb{Z}$ has elements of order p^2. What we have in fact proved, is that the underlying abelian group of $\mathbb{Z}[i]/(p)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. This can also not be a ring isomorphism, as $\mathbb{F}_{p^2}$ is a field, and the latter element has zero divisors. □

(d) Prove that there is an injective homomorphism $\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^2}$.

Proof. The slick proof is to consider the composition $\mathbb{Z} \to \mathbb{Z}[i] \to \mathbb{Z}[i]/(p)$. The kernel of this composition is plainly (p), so that the first isomorphism theorem gives the desired injection.

More concretely, the viewing $\mathbb{F}_{p^2} = \{a+bi : a, b \in \mathbb{F}_p\}$, the injection could be $a \mapsto a+0i$. In this sense we can think of $\mathbb{F}_{p^2}$ as some sort of *complex numbers* over $\mathbb{F}_p$, analogous to the field extension $\mathbb{C}/\mathbb{R}$. □