1. (DF8.2.6) Let R be an integral domain and suppose that every *prime* ideal in R is principal. This exercise proves that every ideal of R is principal, i.e., R is a P.I.D.

   (a) Assume that the set of ideals of R that are not principal is nonempty and prove that this set has a maximal element under inclusion (which, by hypothesis, is not prime). [Use Zorn's Lemma.]

   Proof. Suppose that the set of ideals $\mathcal{S}$ of R that are not principal is nonempty, and give this set a partial ordering by inclusion. Then let $\mathcal{C}$ be a chain in $\mathcal{S}$, and define K to be the union of all such ideals in $\mathcal{C}$:

   $$K = \bigcup_{A \in \mathcal{C}} A.$$

   We check that this upper bound K is an ideal, and show that it must be a nonprincipal ideal. Since $0 \in A$ for every $A \in \mathcal{C}$, it follows that K contains 0 and is nonempty. Then for any elements $a, b \in K$ we have that for some ideals $A, B \in \mathcal{C}$ that $a \in A$ and $b \in B$. Because $\mathcal{C}$ is a chain, we have that either $A \subseteq B$ or $B \subseteq A$ so that in either case we view a, b as lying in one ideal so that $a - b$ is contained in that ideal and hence is contained in K. Similarly, ab must be in K and ra, ar must be in K for any $r \in R$. Hence K is an ideal.

   Suppose by way of contradiction that K is a principal ideal, meaning it is generated by some element $s \in R$. With $s \in K$, it follows that $s \in A$ for some $A \in \mathcal{C}$. But s generates K, so it follows by A being an ideal that $A = K = (s)$ (as $A \subseteq K$ and $K = (s) \subseteq A$), meaning A was a principal ideal, a contradiction. Hence K is not a principal ideal. Since $\mathcal{C}$ was any chain in $\mathcal{S}$, it follows from Zorn's lemma that $\mathcal{S}$ has a maximal element. □

   (b) Let I be an ideal which is maximal with respect to being nonprincipal, and let $a, b \in R$ with $ab \in I$ but $a \notin I$ and $b \notin I$. Let $I_a = (I, a)$ be the ideal generated by I and a, let $I_b = (I, b)$ be the ideal generated by I and b, and define $J = \{r \in R \mid rI_a \subseteq I\}$. Prove that $I_a = (\alpha)$ and $J = (\beta)$ are principal ideals in R with $I \subsetneq I_b \subseteq J$ and $I_a J = (\alpha\beta) \subseteq I$.

   Proof. Observe that since $a \notin I$, we have that $I \subsetneq I_a$, since every element of I appears in I_a, but the element $a \in I_a$ does not appear in I. Similarly, $I \subsetneq I_b$ since $b \notin I$. Then since I was maximal with respect to being nonprincipal, it follows that I_a cannot be nonprincipal (otherwise our choice for I was not maximal as asserted); that is, I_a must be a principal ideal. Hence there exists some $\alpha \in R$ such that $I_a = (\alpha)$.

   We check that J is an ideal: It is clear that $0 \in J$ since $0 \in I$ and $0I_a = (0) \subseteq I$. For elements $s, t \in J$ and any element $r \in R$, we have that $s - t, st, rs \in J$. Let p be an arbitrary element of I_a, and

   $$(s - t)p = sp - tp \in I$$
   $$(st)p = s(tp) \in I$$
   $$(rs)p = r(sp) \in I,$$

   which all follow from the fact that I is an ideal and $sp, tp \in I$. Hence J is an ideal of R.

We also show that I_b is contained in J: Let $(i's + bt) \in I_b$ and $(ip + aq) \in I_a$ be arbitrary (so $i, i' \in I$ and $p, q, s, t \in R$ are arbitrary), then

$$(i's + bt)(ip + aq) = i(i'sp + btp) + abqt + i'(asq) \in I$$

since I is an ideal (so $i(i'sp + btp), i'(asq), abqt \in I$ with $ab \in I$ by assumption).

Hence we have the chain of inclusions $I \subsetneq I_b \subseteq J$ as desired, and again with the maximality of I with respect to nonprincipality, it follows that J is a principal ideal; there exists some $\beta \in R$ such that $J = (\beta)$.

We show that $I_aJ = (\alpha)(\beta)$ is equivalent to the ideal $(\alpha\beta)$. It is clear that $(\alpha\beta)$ is contained in I_aJ since it is contained in (α). Since R is a commutative ring, any element of $(\alpha)(\beta)$ takes on the form $r\alpha\beta$ for some $r \in R$, and observe that elements of this form are in $(\alpha\beta)$. Thus $I_aJ = (\alpha\beta)$. It follows from the definition of J that $(\alpha\beta)$ is contained in I, since any multiple of β multiplied with an element of I_a will be an element of I; any element in $(\alpha\beta)$ is exactly of this form. Hence $I_aJ \subseteq I$.

To collect results, we have that $I_a = (\alpha)$ and $J = (\beta)$ are principal ideals in R with $I \subsetneq I_b \subseteq J$ and $I_aJ = (\alpha\beta) \subseteq I$. □

(c) If $x \in I$ show that $x = s\alpha$ for some $s \in J$. Deduce that $I = I_aJ$ is principal, a contradiction, and conclude that R is a P.I.D.

Proof. Let $x \in I \subseteq I_a = (\alpha)$. Then $x = s\alpha$ for some $s \in R$. Because I is an ideal, we have for any $r \in R$ that $rx \in I$, and $rx = sr\alpha \in s(\alpha) = sI_a$. This implies that $sI_a \subseteq I$, which means $s \in J$. Hence $x = s\alpha$ with $s \in J$, meaning $x \in I_aJ$. But x was an arbitrary element of I, meaning $I \subseteq I_aJ$ and by the previous part it follows that $I = I_aJ = (\alpha\beta)$, meaning I is a principal ideal. This is in contradiction to our choice of I. It follows that there are no nonprincipal ideals in R (i.e., $\mathcal{S}$ is empty). □

2. (DF8.2.8) Prove that if R is a Principal Ideal Domain and D is a multiplicatively closed subset of R, then $D^{-1}R$ is also a P.I.D. (cf. Section 7.5).

Proof. Without loss of generality, take D to not include 0 since the zero ring ($D^{-1}R$ becomes the zero ring which I showed in the last homework) is trivially a P.I.D.

Let I be an ideal of $D^{-1}R$, and let $I' = \{r \in R \mid \text{there exists } d \in D \text{ such that } r/d \in I\}$; that is, let I' be the set of numerators of fractions in the ideal I. We show that I' is an ideal of R, and hence is a principal ideal.

Since I is an ideal, it contains the zero fraction $0/d$ for any $d \in D$; hence $0 \in I'$ and I' is nonempty. If we take two elements $r, s \in I'$, there are denominators $n, m \in D$ such that $r/n, s/m \in I$. But since I is an ideal,

$$\frac{r}{n} \cdot \frac{n}{m} - \frac{s}{m} = \frac{rn}{nm} - \frac{s}{m} = \frac{r - s}{m} \in I,$$

meaning $r - s \in I'$, and

$$\frac{r}{n} \cdot \frac{s}{m} = \frac{rs}{nm} \in I,$$

meaning $rs \in I'$. For any element $p \in R$, $pr \in I'$ since any fraction p/q for $q \in D$ multiplied with r/n forms $pr/nq \in I$ as I is an ideal; hence I' is closed under multiplication by elements of R. It follows that I' is an ideal of R, meaning it is a principal ideal, so there exists $\alpha \in R$ such that $I' = (\alpha)$.

We show that $I = (\alpha/d')$ for some $d' \in D$ (any choice of a denominator would have been fine). It is clear that $(\alpha/d') \subseteq I$ since I is an ideal and multiples of α generate the numerators of fractions which appear in I. Any element $r/d \in I$ may be written in the form $s\alpha/d$ for some $s \in R$, and then by changing denominators we obtain $r/d = sd'/d \cdot \alpha/d'$, so that r/d is equivalent to a multiple of α/d'. This implies that $I \subseteq (\alpha/d')$ as desired, meaning that I is a principal ideal. Since I was arbitrary, it follows that $D^{-1}R$ is a Principal Ideal Domain. □

3. Auxiliary result for (DF8.3.6c): (DF8.2.1) Prove that in a Principal Ideal Domain two ideals (a) and (b) are comaximal (cf. Section 7.6) if and only if a greatest common divisor of a and b is 1 (in which case a and b are said to be *coprime* or *relatively prime*).

Proof. We show that for $a, b \in R$ where R is a Principal Ideal Domain with 1 that $(a, b) = (a) + (b)$. These are both ideals, so we just need to show that both are equal as sets. We have since R is a commutative ring that

$$(a) + (b) = \{p + q \mid p \in (a), q \in (b)\} = \{ra + sb \mid r, s \in R\} = (a, b),$$

since $p \in (a)$ and $q \in (b)$ imply $p = ra$ for some $r \in R$ and $q = sb$ for some $s \in R$. Hence $(a) + (b) = (a, b)$, and because R is a Principal Ideal Domain, this ideal should be generated by some $c \in R$. It follows from an earlier proposition that c must be a greatest common divisor of a and b.

Suppose that a and b are coprime elements, so that 1 is a common divisor of a and b. It follows immediately that $(a) + (b) = (a, b) = (c) = (1) = R$.

Conversely, suppose that $(a) + (b) = R$. Then $(a) + (b) = (a, b) = (c)$ contains 1, so that $(c) = (1)$ and so 1 must be a common divisor of a and b. □

4. (DF8.3.6)

   (a) Prove that the quotient ring $\mathbb{Z}[i]/(1 + i)$ is a field of order 2.

   Proof. By Proposition 18, $1 + i$ is irreducible in $\mathbb{Z}[i]$ which is a unique factorization domain. Hence $(1 + i)$ is a prime ideal, meaning the quotient ring $\mathbb{Z}[i]/(1 + i)$ is an integral domain. Finite integral domains are fields, so we just have to show that there are only two elements in this ring.

   We show that there are at most two elements in $\mathbb{Z}[i]/(1+i)$. We suppress the coset notation, and write equality of elements in the quotient ring by $\equiv$ instead. Since $2 = (1+i)(1-i)$ and $2i = (1+i)(1-i)i = (1 + i)(1 + i)$, it follows that $2 \equiv 0$ and $2i \equiv 0$ (so even integers and even multiples of i are congruent to the zero element). We also have that $1 + i \equiv 0$, so it follows that $1 \equiv -i$. So for any $a + bi \in \mathbb{Z}[i]$, its image after projection to the quotient ring depends only on whether a, b were simultaneously even or not.

If a, b are simultaneously even, then by the first two congruences we have that $a + bi$ is congruent to the zero element.

If a, b are not simultaneously even, then either a, b are both odd, or without loss of generality (since $1 \equiv -i$), a is odd and b is even. In the case that a, b are both odd, then $a + bi \equiv 1 + 1i \equiv 0$. If a is odd and b is even, then $a + bi \equiv 1 + 0i$, which cannot be reduced further outside of conversion to $-i$. Hence there are at most two elements of $\mathbb{Z}[i]/(1 + i)$.

If we exhibit two distinct elements of the quotient ring, then we are done. Observe that $0+0i$ and $1+0i$ are indeed distinct elements of the quotient ring, and so it follows that there are exactly two elements in $\mathbb{Z}[i]/(1 + i)$.

Hence $\mathbb{Z}[i]/(1 + i)$ is a field of order two. □

(b) Let $q \in \mathbb{Z}$ be a prime with $q \equiv 3 \mod 4$. Prove that the quotient ring $\mathbb{Z}[i]/(q)$ is a field with q^2 elements.

Proof. By Proposition 18, we have that q is an irreducible element in the unique factorization domain $\mathbb{Z}[i]$, so (q) is a prime ideal. Again we just have to show that the quotient ring (integral domain) $\mathbb{Z}[i]/(q)$ is finite.

We prove this in a similar manner as in part (a). First we show that there are at most q^2 elements: We have that $q \equiv qi \equiv 0$, so that we reduce elements $a + bi$ "componentwise" modulo q; this gives q distinct options for a to take on modulo q and similarly q distinct options for b to take on modulo q. Hence there are at most q^2 distinct elements of $\mathbb{Z}[i]/(q)$.

We exhibit the q^2 elements by $\{a + bi \mid 0 \leq a, b \leq q - 1\}$, which yields that $\mathbb{Z}[i]/(q)$ is a field of order q^2 as desired. □

(c) Let $p \in \mathbb{Z}$ with $p \equiv 1 \mod 4$ and write $p = \pi\overline{\pi}$ as in Proposition 18. Show that the hypotheses for the Chinese Remainder Theorem (Theorem 17 in Section 7.6) are satisfied and that $\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$ as rings. Show that the quotient ring $\mathbb{Z}[i]/(p)$ has order p^2 and conclude that $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\overline{\pi})$ are both fields of order p.

Proof. Let $p \in \mathbb{Z}$ with $p \equiv 1 \mod 4$ and write $p = \pi\overline{\pi}$ as in Proposition 18. Observe that $\pi, \overline{\pi}$ are irreducible; hence $(\pi), (\overline{\pi})$ are prime ideals in the unique factorization domain $\mathbb{Z}[i]$.

We check that (π) and $(\overline{\pi})$ are comaximal in $\mathbb{Z}[i]$, and that $(\pi)(\overline{\pi}) = (p)$. Observe first that because π is irreducible, $\mathrm{Re}(\pi)$ and $\mathrm{Im}(\pi)$ must be nonzero and coprime (otherwise we could write it as the product of two nonunit elements). Therefore there exist integers x, y such that $x\,\mathrm{Re}(\pi) + y\,\mathrm{Im}(\pi) = 1$.

We show that (π) and $(\overline{\pi})$ are comaximal (that is, $(\pi) + (\overline{\pi}) = \mathbb{Z}[i]$) by showing that $(\pi) + (\overline{\pi}) = (1)$. Observe that $\pi, \overline{\pi}$ are distinct irreducibles and $\pi, \overline{\pi}$ are not associate to each other since the real and imaginary parts of π are distinct (specifically coprime) integers. It follows that $\pi, \overline{\pi}$ are relatively prime so that their greatest common factor is 1. Hence $(\pi) + (\overline{\pi}) = (\pi, \overline{\pi}) = (1) = \mathbb{Z}[i]$.

The product $(\pi)(\overline{\pi})$ is the set of finite sums of products $\pi\overline{\pi} = p$. It follows that

$$(\pi)(\overline{\pi}) = \{r\pi\overline{\pi} = rp \mid r \in \mathbb{Z}[i]\} = (p).$$

Hence the hypotheses for the Chinese Remainder Theorem are satisfied and so we have

$$\frac{\mathbb{Z}[i]}{(\pi)(\overline{\pi})} = \frac{\mathbb{Z}[i]}{(p)} \cong \frac{\mathbb{Z}[i]}{(\pi)} \times \frac{\mathbb{Z}[i]}{(\overline{\pi})}.$$

We repeat a similar argument to part (b) to see that $\mathbb{Z}[i]/(p)$ has order p^2 (but will not be a field since there are zero divisors): With $p \equiv pi \equiv 0$, the image of $a + bi$ in the quotient ring is found by reducing a, b modulo p. This gives p options each for a and b to take on modulo p, so that there are at most p^2 elements. We can exhibit the p^2 elements in $\mathbb{Z}[i]/(p)$ by the set $\{a + bi \mid 0 \leq a, b \leq p - 1\}$; it follows that $\mathbb{Z}[i]/(p)$ has order p^2. Note that $\pi, \overline{\pi}$ are found as elements in the quotient ring, and are zero divisors as a result.

The order of the finite direct product $\mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\overline{\pi})$ is given by the product of the order of the factors; that is,

$$p^2 = \left|\frac{\mathbb{Z}[i]}{(p)}\right| = \left|\frac{\mathbb{Z}[i]}{(\pi)}\right|\left|\frac{\mathbb{Z}[i]}{(\overline{\pi})}\right|.$$

Note that the orders of both factors must be finite. But because (π) and $(\overline{\pi})$ are nontrivial proper ideals of $\mathbb{Z}[i]$ (if they were not both proper, then either (π) or $(\overline{\pi})$ is equal to (1), which is not possible), it follows that the order of the factors are both not 1 each. Since p is a prime number, the only possibility is that $|\mathbb{Z}[i]/(\pi)| = |\mathbb{Z}[i]/(\overline{\pi})| = p$. And because $(\pi), (\overline{\pi})$ are prime ideals (since $\pi, \overline{\pi}$ are irreducibles), it follows that $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\overline{\pi})$ are finite integral domains; i.e. fields (of order p each). □

This exercise shows that for any irreducible Gaussian integer π, the field $\mathbb{Z}[i]/(\pi)$ has order $N(\pi)$, where N is the field norm given by $N(\pi) = \pi\overline{\pi}$.

5. (DF8.3.7) Let π be an irreducible element in $\mathbb{Z}[i]$.

   (a) For any integer $n \geq 0$, prove that $(\pi^{n+1}) = \pi^{n+1}\mathbb{Z}[i]$ is an ideal in $(\pi^n) = \pi^n\mathbb{Z}[i]$ and that multiplication by π^n induces an isomorphism $\mathbb{Z}[i]/(\pi) \cong (\pi^n)/(\pi^{n+1})$ as additive abelian groups.

   Proof. Observe that $\pi^{n+1}\mathbb{Z}[i]$ contains zero, and is a nonempty subset of $\pi^n\mathbb{Z}[i]$, as $r\pi^{n+1} = (r\pi)\pi^n$. We have for any two elements $r\pi^{n+1}, s\pi^{n+1} \in \pi^{n+1}\mathbb{Z}[i]$ that their difference $(r - s)\pi^{n+1}$ and product $(rs\pi^{n+1})\pi^{n+1}$ are elements in $\pi^{n+1}\mathbb{Z}[i]$. Any element of $\pi^n\mathbb{Z}[i]$ takes on the form $t\pi^n$ for some $t \in \mathbb{Z}[i]$; we have for any $r\pi^{n+1} \in \pi^{n+1}\mathbb{Z}[i]$ that $(t\pi^n)(r\pi^{n+1}) = (rt\pi^n)\pi^{n+1}$ is also an element of $\pi^{n+1}\mathbb{Z}[i]$. It follows that $\pi^{n+1}\mathbb{Z}[i]$ is an ideal of $\pi^n\mathbb{Z}[i]$.

   Consider the map $\varphi\colon \mathbb{Z}[i] \to (\pi^n)$ given by $r \mapsto r\pi^n$ and the projection map (which is surjective) $\pi'\colon (\pi^n) \to (\pi^n)/(\pi^{n+1})$. View these maps as group homomorphisms: We check that φ is an additive group homomorphism. For elements $r, s \in \mathbb{Z}[i]$ we have that $r + s \mapsto (r + s)\pi^n = r\pi^n + s\pi^n$, which is $\varphi(r) + \varphi(s)$ as desired. We also have that φ is surjective because (π^n) by definition is the set of all multiples of π^n. Multiplication by π^n does not preserve the ring multiplication since multiplication only distributes over addition.

   The composition $\pi' \circ \varphi\colon \mathbb{Z}[i] \to (\pi^n)/(\pi^{n+1})$ is a surjective additive group homomorphism whose kernel is exactly the Gaussian integers which when multiplied by π^n give a multiple of π^{n+1}; i.e. the multiples

of π. Specifically, a is in $\ker(\pi' \circ \varphi)$ if and only if π^{n+1} divides $a\pi^n$, which because π is an irreducible element, we cancel π^n and obtain that π divides a. Hence $\ker(\pi' \circ \varphi) = (\pi)$, so by the first isomorphism theorem

$$\frac{\mathbb{Z}[i]}{(\pi)} \cong \frac{(\pi^n)}{(\pi^{n+1})}.$$

□

(b) Prove that $|\mathbb{Z}[i]/(\pi^n)| = |\mathbb{Z}[i]/(\pi)|^n$.

Proof. We prove by induction on n. For $n = 1$, the result is automatically true by inspection. Assume that for some $k > 1$ the result holds. Then by the third isomorphism theorem and the results of part (a), we have that

$$\left(\frac{\mathbb{Z}[i]}{(\pi^{k+1})}\right) \Big/ \left(\frac{(\pi^k)}{(\pi^{k+1})}\right) \cong \frac{\mathbb{Z}[i]}{(\pi^k)}.$$

It follows that

$$\left|\frac{\mathbb{Z}[i]}{(\pi^{k+1})}\right| = \left|\frac{\mathbb{Z}[i]}{(\pi^k)}\right| \left|\frac{(\pi^k)}{(\pi^{k+1})}\right| = \left|\frac{\mathbb{Z}[i]}{(\pi)}\right|^k \left|\frac{\mathbb{Z}[i]}{(\pi)}\right| = \left|\frac{\mathbb{Z}[i]}{(\pi)}\right|^{k+1},$$

as desired.

Hence $|\mathbb{Z}[i]/(\pi^n)| = |\mathbb{Z}[i]/(\pi)|^n$. □

(c) Prove for any nonzero α in $\mathbb{Z}[i]$ that the quotient ring $\mathbb{Z}[i]/(\alpha)$ has order equal to $N(\alpha)$. [Use (b) together with the Chinese Remainder Theorem and the results of the previous exercise.]

Proof. Let α be any nonzero element in $\mathbb{Z}[i]$.

Since $\mathbb{Z}[i]$ is a Euclidean Domain, it is automatically a Unique Factorization Domain, so we can expand α into a unique (up to associates) finite product of powers of irreducibles:

$$\alpha = \prod_{i=1}^{n} p_i^{e_i}.$$

This is equivalent to saying that the ideal (α) is equal to the product of ideals $\prod_{i=1}^n (p_i^{e_i}) = (\prod_{i=1}^n p_i^{e_i})$. We have that the ideals which appear in the product are pairwise comaximal: for $i \neq j$, the irreducibles p_i and p_j are coprime (they are pairwise not associate to each other), which imply that $(p_i^{e_i})$ and $(p_j^{e_j})$ are comaximal. Then by the Chinese Remainder Theorem, we have that

$$\frac{\mathbb{Z}[i]}{(\alpha)} = \frac{\mathbb{Z}[i]}{(\prod_{i=1}^n p_i^{e_i})} \cong \prod_{i=1}^{n} \frac{\mathbb{Z}[i]}{(p_i^{e_i})}.$$

From part (b) it follows that the order of any factor $\mathbb{Z}[i]/(p_i^{e_i})$ is given by $|\mathbb{Z}[i]/(p_i)|^{e_i}$. Since p_i is irreducible, from (DF8.3.6) we have that $|\mathbb{Z}[i]/(p_i)| = N(p_i)$ (where N is the field norm). Hence

$$\left|\frac{\mathbb{Z}[i]}{(\alpha)}\right| = \prod_{i=1}^{n} \left|\frac{\mathbb{Z}[i]}{(p_i^{e_i})}\right| = \prod_{i=1}^{n} \left|\frac{\mathbb{Z}[i]}{(p_i)}\right|^{e_i} = \prod_{i=1}^{n} N(p_i)^{e_i},$$

and since the field norm N is multiplicative, we have that

$$\left|\frac{\mathbb{Z}[i]}{(\alpha)}\right| = \prod_{i=1}^{n} N(p_i)^{e_i} = N\left(\prod_{i=1}^{n} p_i^{e_i}\right) = N(\alpha).$$

□