# Section 8.2

5. (Lawless) Let $R$ be the quadratic integer ring $\mathbb{Z}[\sqrt{-5}]$. Define the ideals $I_2 = (2, 1+\sqrt{-5})$, $I_3 = (3, 2+\sqrt{-5})$, and $I_3' = (3, 2-\sqrt{-5})$.

   (a) Prove that $I_2$, $I_3$, and $I_3'$ are nonprincipal ideals in $R$.

   *Proof.* Assume $I_2$ is a principal ideal. This would imply there is some $a + b\sqrt{-5}$ such that

   $$2 = \alpha(a + b\sqrt{-5}) \tag{1}$$

   $$1 + \sqrt{-5} = \beta(a + b\sqrt{-5}) \tag{2}$$

   Taking the norms on both side of equation (1) give us $4 = N(\alpha)(a^2 + 5b^2)$. So $a^2 + 5b^2 =$ 1,2, or 4.

   If the value of $a^2 + 5b^2$ is 4, then $N(\alpha) = 1$, and so $\alpha = \pm 1$. So $a + b\sqrt{-5} = \pm 4$. However, this is impossible, since 4 does not divide the coefficients of $1 + \sqrt{-5}$, as is required by (2).

   The value of $a^2 + 5b^2$ cannot be 2, since there are no integer solutions to $a^2 + 5b^2 = 2$. This leaves $a^2 + 5b^2 = 1$. Then $a + b\sqrt{-5} = \pm 1$, and so $1 \in I_2$. Thus, there exists some $\gamma, \delta \in \mathbb{Z}[\sqrt{-5}]$ such that

   $$2\gamma + (1 + \sqrt{-5})\delta = 1.$$

   Multiplying both sides by $1 - \sqrt{-5}$ gives

   $$(1 - \sqrt{-5})2\gamma + 6\delta = 1 - \sqrt{-5}.$$

   Since both terms on the left hand side are divisible by 2, this would imply $1 - \sqrt{-5}$ is a multiple of 2 in $\mathbb{Z}[\sqrt{-5}]$, a contradiction.

   Therefore, $I_2 = (2, 1 + \sqrt{-5})$ is not a principal ideal. The proof that $I_3$ is not principal is given on p.273 in the book, and the proof that $I_3'$ is nonprincipal is similar. □

   (b) Prove that the product of two nonprincipal ideals can be principal by showing $I_2^2$ is the principal ideal generated by 2.

   *Proof.* We will show $(2) = I_2^2$. We first show $I_2 \subseteq (2)$. Recall that if $I, J$ are ideals in a ring $R$, then $IJ = (\{ab \mid a \in I, b \in J\})$. So $I_2^2$ is generated by the elements $2^2 = 4$, $2(1 + \sqrt{-5})$, and $(1 + \sqrt{-5})^2 = 1 + 2\sqrt{-5} + 5 = 6 + 2\sqrt{-5} = 2(3 + \sqrt{-5})$. Thus $I_2^2$ is generated by elements of the form $2(a + b\sqrt{-5})$, for some $a, b \in \mathbb{Z}$. Therefore, $I_2^2 \subseteq (2)$.

   Since $1 + \sqrt{-5} \in I_2$, and $1 - \sqrt{-5} = 2 - (1 + \sqrt{-5}) \in I_2$, then $6 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \in I_2^2$. So we have $6, 4 \in I_2^2$, and so $2 = 6 - 4 \in I_2^2$. Thus $(2) \subseteq I_2^2$, and so $(2) = I_2^2$. □

   (c) Prove that $I_2 I_3 = (1 - \sqrt{-5})$ and $I_2 I_3' = (1 + \sqrt{-5})$ are principal. Conclude $(6) = I_2^2 I_3 I_3'$.

   First, we show $I_2 I_3 = (1 - \sqrt{-5})$. Notice $I_2 I_3$ will be generated by the elements $(2)(3) = 6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$, $2(2 + \sqrt{-5}) = 4 + 2\sqrt{-5} = (1 - \sqrt{-5})(-1 + \sqrt{-5})$, $3(1 + \sqrt{-5}) = 3 + 3\sqrt{-5} = (1 - \sqrt{-5})(-2 + \sqrt{-5})$ and $(2 + \sqrt{-5})(1 + \sqrt{-5}) = -3 + 3\sqrt{-5} = (1 - \sqrt{-5})(-3)$. So every element in $I_2 I_3$ can be written in the form $(1 - \sqrt{-5})(a + b\sqrt{-5})$ for $a, b \in \mathbb{Z}$, and so $I_2 I_3 \subseteq (1 - \sqrt{-5})$. Since $1 - \sqrt{-5} = 4 + 2\sqrt{-5} - (3 + 3\sqrt{-5}) \in I_2 I_3$, we get $(1 - \sqrt{-5}) \subseteq I_2 I_3$, and so $(1 - \sqrt{-5}) = I_2 I_3$, and so $I_2 I_3$ is principal.

   By a similar argument, we also get $I_2 I_3' = (1 + \sqrt{-5})$ is also principal. It remains to show $(6) = I_2^2 I_3 I_3'$. Since $Z$ is commutative, we have $(I_2 I_3)(I_2 I_3') = I_2^2 I_3 I_3'$. Thus, $I_2^2 I_3 I_3'$ is generated by $(1 - \sqrt{-5})(1 + \sqrt{-5}) = 6$. As such, $I_2^2 I_3 I_3' = (6)$.

## Section 8.3

3. Determine all the representations of the integer $2130797 = 17^2 \cdot 73 \cdot 101$ as a sum of two squares.

$$\begin{aligned} &(\pm 851)^2 + (\pm 1186)^2 \\ &(\pm 1069)^2 + (\pm 994)^2 \\ &(\pm 1411)^2 + (\pm 374)^2 \\ &(\pm 1309)^2 + (\pm 646)^2 \\ &(\pm 1421)^2 + (\pm 334)^2 \\ &(\pm 1459)^2 + (\pm 46)^2 \end{aligned}$$

Each of the six equations above gives us four representations. We can also swap the order of the terms to double the number of representations. This gives us a total of 48 representations.

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

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

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

   (a) *Proof.* (Bastille) By Proposition 18, $1+i$ is irreducible in $\mathbb{Z}[i]$, therefore it is prime since $\mathbb{Z}[i]$ is a PID (p.290 and Proposition 11). So $(1+i)$ is a prime ideal, and hence by Proposition 7, $(1+i)$ is a maximal ideal. Therefore $\mathbb{Z}[i]/(1+i)$ is a field. We now show that it is of order 2.

   <u>Long version</u> Consider the following map:

$$\begin{aligned} \varphi : \quad & \mathbb{Z}[i] \to Z_2 \\ & \varphi(a+bi) = (a^2+b^2) \bmod 2. \end{aligned}$$

   We verify that $\varphi$ is a surjective ring homomorphism since for all $a+bi, c+di \in \mathbb{Z}[i]$:

$$\begin{aligned} \varphi((a+bi)+(c+di)) &= \varphi(a+c+(b+d)i) = ((a+c)^2+(b+d)^2) \bmod 2 \\ &= (a^2+2ac+c^2+b^2+2bd+d^2) \bmod 2 = (a^2+b^2+c^2+d^2) \bmod 2 \\ &= (a^2+b^2) \bmod 2 + (c^2+d^2) \bmod 2 = \varphi(a+bi)+\varphi(c+di); \\ \varphi((a+bi)(c+di)) &= \varphi(ac-bd+(ad+bc)i) = ((ac-bd)^2+(ad+bc)^2) \bmod 2 \\ &= (a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2) \bmod 2 \\ &= (a^2(c^2+d^2)+b^2(c^2+d^2)) \bmod 2 = ((a^2+b^2)(c^2+d^2)) \bmod 2 \\ &= (a^2+b^2) \bmod 2 \cdot (c^2+d^2) \bmod 2 = \varphi(a+bi)\varphi(c+di); \\ \varphi(1) = 1 \quad \varphi(2) &= 0. \end{aligned}$$

   We claim that $\ker\varphi = (1+i)$. Note that because norms are multiplicative, if $a+bi = \alpha(1+i)$ for some $\alpha \in \mathbb{Z}[i]$, then $a^2+b^2 = N(a+bi) = N(\alpha)N(1+i) = 2N(\alpha)$ and therefore $a+bi \in \ker\varphi$. Thus $(1+i) \subseteq \ker\varphi$. Conversely, if $a^2+b^2 = 2k$, then either both $a, b$ are odd or both $a, b$ are even. In both cases, $a+b$, $b-a$ are even and

$$a+bi = \left(\frac{a+b}{2} + \frac{b-a}{2}i\right)(1+i),$$

   hence $a+bi \in (1+i)$ and $\ker\varphi \subseteq (1+i)$. Thus $\ker\varphi = (1+i)$. Therefore, by the First Isomorphism Theorem, $\mathbb{Z}[i]/(1+i) \cong Z_2$ so $\mathbb{Z}[i]/(1+i)$ is a field of order 2.

Short version Because $\mathbb{Z}[i]$ is a Euclidean domain, for any $c \in \mathbb{Z}[i]$, there exist $\alpha, r \in \mathbb{Z}[i]$ such that:

$$c = \alpha(1+i) + r \quad \text{where} \quad r = 0 \quad \text{or} \quad N(r) < N(1+i) = 2.$$

If $r = 0$ then $c \in (1+i)$, and if $N(r) = 1$ then $r$ is a unit, i.e. $r = \pm 1, \pm i$. We claim $1+(1+i) = i+(1+i) = -1+(1+i) = -i+(1+i)$. Indeed note that $1-i = -i(1+i) \in (1+i)$ so $1+(1+i) = i+(1+i)$, and similarly $1+i = 1-(-i) = i-(-1) \in (1+i)$ so $1+(1+i) = -i+(1+i)$ and $i+(1+i) = -1+(1+i)$. So all these cosets are equal. Hence

$$\mathbb{Z}[i]/(1+i) = \{(1+i), 1+(1+i)\},$$

and so $\mathbb{Z}[i]/(1+i)$ is a field of order 2. $\square$

(b) *Proof.* (Bastille) By Proposition 18, $q$ is irreducible in $\mathbb{Z}[i]$ so $q$ is prime since $\mathbb{Z}[i]$ is a PID. Furthermore, the prime ideal $(q)$ is maximal by Proposition 7. Therefore $\mathbb{Z}[i]/(q)$ is a field. Because $\mathbb{Z}$ is a Euclidean domain, for any $c, d \in \mathbb{Z}$, there exist $b_1, b_2, r_1, r_2 \in \mathbb{Z}$ such that:

$$\begin{aligned} c &= b_1 q + r_1 \quad \text{and} \quad 0 \le r_1 < q, \\ d &= b_2 q + r_2 \quad \text{and} \quad 0 \le r_2 < q. \end{aligned}$$

Therefore for any $c + di \in \mathbb{Z}[i]$, we have that $c + di + (q) = b_1 q + r_1 + (b_2 q + r_2)i + (q) = (b_1 + b_2 i)q + r_1 + r_2 i + (q) = r_1 + r_2 i + (q)$. So

$$\mathbb{Z}[i]/(q) = \{r_1 + r_2 i \mid r_1, r_2 \in \mathbb{Z}, \quad 0 \le r_1, r_2 < q\}.$$

So we have $q$ choices for $r_1$, and $q$ choices for $r_2$ so we need only show that all $q^2$ cosets thus formed are distinct. Assume $r_1, r_1^{'}, r_2, r_2^{'} \in \mathbb{Z}$ such that $0 \le r_1, r_1^{'}, r_2, r_2^{'} < q$. Then

$$\begin{aligned} r_1 + r_2 i + (q) = r_1^{'} + r_2^{'} i + (q) \quad &\Leftrightarrow \quad r_1 - r_1^{'} + (r_2 - r_2^{'})i \in (q) \\ &\Leftrightarrow \quad r_1 - r_1^{'} + (r_2 - r_2^{'})i = q(a+bi) = qa + qbi \text{ where } a, b \in \mathbb{Z}. \end{aligned}$$

But $0 \le r_1 - r_1^{'} < q$, and $0 \le r_2 - r_2^{'} < q$ so we must have $a = b = 0$ and hence $r_1 = r_1^{'}$ and $r_2 = r_2^{'}$. This in turns implies that all cosets described are distinct, and therefore $|\mathbb{Z}[i]/(q)| = q^2$. $\square$

(c) *Proof.* (Bastille) To verify the hypotheses of the Chinese Remainder Theorem, we need only show that $(\pi)$ and $(\bar{\pi})$ are comaximal ideals in $\mathbb{Z}[i]$ since we aready have that $\mathbb{Z}[i]$ is a commutative ring with 1. Note that, as in part (a), because $\pi = a + bi$ and $\bar{\pi} = a - bi$ are irreducible in $\mathbb{Z}[i]$, a PID, $(\pi), (\bar{\pi})$ are maximal ideals in $\mathbb{Z}[i]$ (by Proposition 18, 11, and 7). So we need only show that one is not a subset of the other to conclude that their sum is the whole ring. Suppose to the contrary that $\pi = \alpha\bar{\pi}$, then $\alpha$ would have to be a unit since $\pi$ is irreducible. But we are given that they are distinct irreducible, hence they cannot be associates. Therefore $\pi \notin (\bar{\pi})$ and hence, $(\pi) + (\bar{\pi}) = \mathbb{Z}[i]$, i.e. $(\pi)$ and $(\bar{\pi})$ are comaximal. Then it follows from the Chinese Remainder Theorem that the map $\mathbb{Z}[i] \to \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\bar{\pi})$ defined by $r \longmapsto (r + (\pi), r + (\bar{\pi}))$ is a surjective ring homomorphism with kernel: $(\pi) \cap (\bar{\pi}) = (\pi)(\bar{\pi}) = (\pi\bar{\pi}) = (p)$. So by the First Isomorphism Theorem,

$$\mathbb{Z}[i]/(p) \cong \mathbb{Z}[i]/(\pi) \times \mathbb{Z}[i]/(\bar{\pi}).$$

Using the division algorithm in $\mathbb{Z}$ – the same argument as in part (b) but for $p$ instead of $q$ – we can conclude that $\mathbb{Z}[i]/(p)$ has order $p^2$. And because $(\pi), (\bar{\pi})$ are maximal ideals in $\mathbb{Z}[i]$, we can conclude again that $\mathbb{Z}[i]/(\pi)$ and $\mathbb{Z}[i]/(\bar{\pi})$ are fields. Furthermore $|\mathbb{Z}[i]/(\pi)| \neq 1$, $|\mathbb{Z}[i]/(\bar{\pi})| \neq 1$ otherwise $(\pi)$ (respectively $(\bar{\pi})$) equals $\mathbb{Z}[i] = (1)$ but 1 and $\pi$ (resp. $\bar{\pi}$) can not be associates since $\pi$ (resp. $\bar{\pi}$) is irreducible and 1 is a unit. Therefore we must have $|\mathbb{Z}[i]/(\pi)| = |\mathbb{Z}[i]/(\bar{\pi})| = p$. $\square$

## Section 9.1

4. Prove that the ideals $(x)$ and $(x, y)$ are prime ideals in $\mathbb{Q}[x, y]$ but only the latter ideal is a maximal ideal.

*Proof.* (Mobley) Let $\varphi : \mathbb{Q}[x, y] \to \mathbb{Q}[y]$ such that $\varphi(x) = 0$, $\varphi(y) = y$ and $\varphi(q) = q$ for all $q \in \mathbb{Q}$. Then any polynomial in $\mathbb{Q}[x, y]$ with a term that has an $x$ will go to zero and the only terms that remain are those with y's and constants. We compute the $\ker \varphi = (x)$. By the First Isomorphism Theorem, $\mathbb{Q}[x, y]/(x) \cong \mathbb{Q}[y]$. Since $\mathbb{Q}[y]$ is an integral domain, it follows that $\mathbb{Q}[x, y]/(x)$ is as well. By Proposition 13 on page 255 of the text $(x)$ is a prime ideal.

Now consider $\Gamma : \mathbb{Q}[x, y] \to \mathbb{Q}$ such that $\Gamma(x) = 0$, $\Gamma(y) = 0$ and $\Gamma(1) = 1$. Thus any term in $\mathbb{Q}[x, y]$ that has an $x$ or $y$ will go to zero and only rationals are left. We can see that $\ker \Gamma = (x, y)$. Using the First Isomorphism Theorem again, we have that $\mathbb{Q}[x, y]/(x, y) \cong \mathbb{Q}$. Since $\mathbb{Q}$ is a field so is $\mathbb{Q}[x, y]/(x, y)$. Then it follows that $(x, y)$ is a maximal ideal and also a prime ideal.

□

9. Prove that a polynomial ring in infinitely many variables with coefficients in any commutatitive ring contains ideals that are not finitely generated.

*Proof.* (Mobley) Let $R[x_1, x_2, ...]$ be a commutative ring. We need to show that the ideal $I = (x_1, x_2, ..., x_n, ...) \subseteq R[x_1, x_2, ...]$ is not finitely generated. To this end, suppose to the contrary that $I$ is finitely generated. Then $I$ is generated by a finite number of polynomials, $I =< p_1, p_2, ..., p_n >$. Note that there is a finite number of variables $x_i$ appearing in any $p_i$. Assume $k = \max\{i \mid x_i$ such that $x_i$ is a variable in $p_i\}$. Then $I \subseteq< x_1, x_2, ..., x_k >$.

We claim that $x_{k+1} \notin< x_1, x_2, ..., x_k >$ and therefore $x_{k+1} \notin I$. Suppose $x_{k+1} \in I$. Then for ring elements $g_i$,

$$x_{k+1} = \Sigma_{i=1}^{n} g_i p_i.$$

First we collect all the terms on the right side of the equation that have an $x_1$ in them. After factoring out the $x_1$ term from these, we have $c_1 x_1$ such that

$$\Sigma_{i=1}^{n} g_i p_i - c_1 x_1$$

where $\Sigma_{i=1}^{n} g_i p_i - c_1 x_1$ no longer contains the variable $x_1$. We continue doing this again for the next variable $x_2$ which results in $\Sigma_{i=1}^{n} g_i p_i - c_2 x_2 - c_1 x_1$. Notice that $\Sigma_{i=1}^{n} g_i p_i - c_2 x_2 - c_1 x_1$ no longer contains the variables $x_1$ or $x_2$. We follow the same procedure for $x_3$ (which results in $\Sigma_{i=1}^{n} g_i p_i - c_3 x_3 - c_2 x_2 - c_1 x_1$) and so on until we have finished the process with $x_k$. Then we have

$$x_{k+1} = \Sigma_{i=1}^{n} g_i p_i = c_1 x_1 + c_2 x_2 + ... + c_k x_k.$$

But we realize that on the left most side of the equation there are no terms with $x_1$ and therefore $c_1 = 0$. This is true for all $x_i$ with $i = \{1, 2, ..., k\}$ and therefore $c_i = 0$ for $i = \{1, 2, ..., k\}$. But then $x_{k+1} = 0$ and we have a contradiction. Therefore a polynomial ring in infinitely many variables with coefficients in any commutatitive ring contains ideals that are not finitely generated.

□

13. Prove that the rings $F[x, y] / (y^2 - x)$ and $F[x, y] / (y^2 - x^2)$ are not isomorphic for any field $F$.

*Proof (Granade).* Note that $(y^2 - x^2) = (y - x)(y + x)$ is reducible. Thus, $F[x, y] / (y^2 - x^2)$ contains zero-divisors. Concretely, $\overline{(y - x)(y + x)} = \overline{y^2 - x^2} = \overline{0}$.

By contrast, we claim that $y^2 - x$ is not reducible, and hence $F[x, y] / (y^2 - x)$ is a field. To see this, suppose that $y^2 - x = f(x, y) g(x, y)$ is a non-trivial factorization for some $f, g \in F[x, y]$. Then, since $y^2 - x$ has multidegree $(1, 2)$, we must have that one of $f$ and $g$ has degree 0 in $x$ and that the other must have degree 1 in $x$. Without loss of generality, let $f(x, y)$ have degree 1 in $x$. Thus, $g(x, y) = g(y)$. Since this factorization is non-trivial, $\deg g(y) \geq 1$, and so $y^2 - x = f(x, y) \cdot y g_0(y)$ for some $g_0 \in F[y]$. This is a contradiction, as $y \nmid x$. We conclude that $y^2 - x$ is irreducible as claimed.

Since $F[x,y]/\left(y^2-x\right)$ is a field but $F[x,y]/\left(y^2-x^2\right)$ has zero-divisors, they cannot be isomorphic for any field $F$. ☐

## Section 9.2

1. Let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$ and let bars denote passage to the quotient $F[x]/(f(x))$. Prove that for each $\overline{g(x)}$ there is a unique polynomial $g_0(x)$ of degree $\leq n-1$ such that $\overline{g(x)} = \overline{g_0(x)}$ (equivilantly, the elements $\overline{1}, \overline{x}, \ldots, \overline{x^{n-1}}$ are a *basis* of the vectorspace $F[x]/(f(x))$ over $F$ — in particular, the dimension of this space is $n$).

   *Proof (Granade).* Let $\overline{g(x)} \in F[x]/(f(x))$. Then, by the division algorithm on $F[x]$, there exist unique polynomials $q(x)$ and $r(x)$ such that:

   $$\begin{aligned} g(x) &= q(x)f(x) + r(x) \\ \deg r(x) &< \deg f(x) \end{aligned}$$

   Thus, $\overline{g(x)} = \overline{q(x)f(x)+r(x)} = \overline{q(x)}f(x) + \overline{r(x)} = \overline{r(x)}$. Since $r(x)$ is unique, we are done. ☐

9.2.2 Let $F$ be a finite field of order $q$ and let $f(x)$ be a polynomial in $F[x]$ of degree $n \geq 1$, then $F[x]/(f(x))$ has $q^n$elements.

*Proof.* (Gillispie) Let $f(x) = a_n x^n + \cdots + a_0 \in F[x]$ and let $I = (f(x))$. By problem 9.2.1 we know that the elements $\bar{1}, \bar{x}, \cdots, \bar{x}^{n-1}$ form a basis for the vector space $F[x]/I$ over $F$. So every element of this vector space may be expressed as a linear combination of $\bar{1}, \bar{x}, \cdots, \bar{x}^{n-1}$ with coefficients from $F$. Since there are $n$ elements in the basis, and $q$ elements in $F$, there are $q^n$ elements in the vector space, and hence $q^n$ elements in $F[x]/I$.

☐

9.2.3 Let $f(x)$ be a polynomial in $F[x]$, then $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

*Proof.* (Gillispie) We may assume $f(x) \neq 0$, since $f(x) = 0$ is not irreducible element and $F[x]/(0)$ is not a field.
Since $F$ is a field, from Cor. 9.4 we know that $F[x]$ is a PID.
Since $F[x]$ is a PID by Prop. 7.12 and $f(x) \neq 0$, $F[x]/(f(x))$ is a field if and only if $(f(x))$ is a maximal ideal. By corollary 7.14 and Prop. 8.7 $(f(x))$ is maximal if and only if it is a prime ideal. We also know that $(f(x))$ is prime in $F[x]$ if and only if $f(x)$ is prime in $F[x]$.Finally from Prop. 8.11 since $F[x]$ is a PID, $f(x)$ is prime if and only if it is irreducible. ☐

6. Describe (briefly) the ring structure of the following rings:

   $$\text{a. } \mathbb{Z}[x]/(2) \quad \text{b. } \mathbb{Z}[x]/(x) \quad \text{c. } \mathbb{Z}[x]/(x^2) \quad \text{d. } \mathbb{Z}[x]/(x^2, y^2, 2)$$

   Show that $\alpha^2 = 0$ or 1 for every $\alpha$ in the last ring and determine those elements with $\alpha^2 = 0$. Determine the characteristics of each of these rings.
   (Baggett)

   a. $\mathbb{Z}[x]/(2) \cong \mathbb{Z}/2\mathbb{Z}[x]$
      Since $\mathbb{Z}/2\mathbb{Z}$ is a field, $\mathbb{Z}[x]/(2)$ is a ED, a PID, and a UFD with characteristic 2.
   b. $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$
      $\mathbb{Z}[x]/(x)$ is a ED, a PID, and a UFD with characteristic 0.
   c. $\mathbb{Z}[x]/(x^2) \cong \{a + bx \mid a, b \in \mathbb{Z} \text{ and } x^2 = 0\}$
      $\mathbb{Z}[x]/(x)$ has characteristic 0.

d. $\mathbb{Z}[x]/(x^2, y^2, 2) \cong \{a + bx + cy + dxy \mid a, b, c, d \in \mathbb{Z}/2\mathbb{Z} \text{ and } x^2 = y^2 = 0\}$.
Let $\alpha \in \mathbb{Z}[x]/(x^2, y^2, 2)$. Let $\alpha'$ be the image of $\alpha$ under the above isomorphism, i.e. $\alpha' = a + bx + cy + dxy$ with $a, b, c, d \in \mathbb{Z}/2\mathbb{Z}$. Then

$$(\alpha')^2 = (a + bx + cy + dxy)(a + bx + cy + dxy) = a^2 + 2abx + 2acy + 2(ad + bc)xy = a^2.$$

If $a = \overline{0}$, then $(\alpha')^2 = \overline{0}$. If $a = \overline{1}$, then $(\alpha')^2 = \overline{1}$. Hence, $\alpha^2 = 0$ or 1. We have that $\alpha^2 = 0$ if $\alpha = p(x) + (x^2, y^2, 2)$ with the constant term of $p(x)$ being even. Lastly, $\mathbb{Z}[x]/(x^2, y^2, 2)$ has characteristic 2.

7. Determine all the ideals of the ring $\mathbb{Z}[x]/(2, x^3 + 1)$.

(Schamel) Note $(2)(x^3 + 1)/(2) \equiv (x^3 + 1)$ so the third isomorphism theorem for rings and proposition 2 of section 9.1 give us

$$\mathbb{Z}[x]/(2)(x^3 + 1) \equiv (\mathbb{Z}[x]/(2))/((2)(x^3 + 1)/(2)) \equiv (\mathbb{Z}/2\mathbb{Z})[x]/(x^3 + 1).$$

In $(\mathbb{Z}/2\mathbb{Z})[x]$ (a U.F.D by corollary 4 of 9.2), we can factor $(x^3 + 1)$ into $(x + 1)(x^2 + x + 1)$. Since $\mathbb{Z}/2\mathbb{Z}$ is a field, factoring into irreducibles must reduce degree. Hence, $x + 1$ is irreducible since it has degree one, and $x^2 + x + 1$ must factor into two degree one polynomials. The only degree one polynomials in $(\mathbb{Z}/2\mathbb{Z})[x]$ are $x$ and $x+1$, but $x \cdot x = x^2$, $x(x+1) = x^2 + x$ and $(x+1)(x+1) = x^2 + 1$, so $x^2 + x + 1$ is also irreducible in $(\mathbb{Z}/2\mathbb{Z})[x]$. Thus $(\overline{x + 1})$ and $(\overline{x^2 + x + 1})$ will be distinct proper ideals of $\mathbb{Z}[x]/(2, x^3 + 1)$, along with $(\overline{0})$ and $(\overline{1})$. Furthermore, since $(\mathbb{Z}/2\mathbb{Z})[x]$ is a U.F.D., it is also a P.I.D, and hence the only proper ideals of $(\mathbb{Z}/2\mathbb{Z})[x]$ containing $(x^3 + 1)$ are $(x + 1)$ and $(x^2 + x + 1)$. The correspondence isomorphism theorem for rings then gives us that there are exactly two non-trivial proper ideals of $(\mathbb{Z}/2\mathbb{Z})[x]/(x^3 + 1)$, so we have completed our search.

## Chapter 9.3

1. Let $R$ be an integral domain with quotient field $F$ and let $p(x)$ be a monic polynomial in $R[x]$. Assume that $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of smaller degree than $p(x)$. Prove that if $a(x) \notin R[x]$ then $R$ is not a Unique Factorization Domain. Deduce that $\mathbb{Z}[2\sqrt{2}]$ is not a U.F.D.

*Proof.* (Schamel) By way of contradiction, suppose $R$ is a U.F.D. Then, by Gauss' Lemma, there exist non-zero $\alpha, \beta \in F$ such that $\alpha a(x) = \tilde{a}(x)$ and $\beta b(x) = \tilde{b}(x)$ for some $\tilde{a}(x), \tilde{b}(x) \in R[x]$ such that $p(x) = \tilde{a}(x)\tilde{b}(x)$. In particular, $p(x) = \alpha\beta a(x)b(x)$. Since $a(x)$ and $b(x)$ are monic, we have that $a(x)b(x)$ is also monic, and the highest degree coefficients of $p(x)$ and $a(x)b(x)$ give us that $1 = \alpha\beta \cdot 1$. Hence $\beta = \alpha^{-1}$ and both are units. But we also have that $a(x)$ and $b(x)$ are monic, so the coefficients of the largest terms of $\tilde{a}(x)$ and $\tilde{b}(x)$ are given by $\alpha$ and $\beta$ respectively, so $\alpha, \beta \in R$. Hence $\alpha$ and $\beta$ are units in $R$, so $p(x) = \beta\tilde{a}(x)\alpha\tilde{b}(x) = a(x)b(x)$ gives a factorization of $p(x)$ in $R[x]$, and thus $a(x), b(x) \in R[x]$, a contradiction.

Now let $R = \mathbb{Z}[2\sqrt{2}] = \left\{a + 2b\sqrt{2} : a, b \in \mathbb{Z}\right\}$. The field of fractions of $R$ is then $F = \mathbb{Q}[\sqrt{2}]$. Then the polynomial $p(x) = x^2 - 2$ is reducible in $F[x]$ to monic terms by $p(x) = (x + \sqrt{2})(x + \sqrt{2})$. However, $x + \sqrt{2} \notin R[x]$, so by our previous result, $\mathbb{Z}[2\sqrt{2}]$ is not a U.F.D. $\square$

3. Let $F$ be a field. Prove that the set $R$ of polynomials in $F[x]$ whose coefficient of $x$ is equal to 0 is a subring of $F[x]$ and that $R$ is not a U.F.D.

*Proof.* (Buchholz)

Let $R$ be a set of polynomials in $F[x]$ whose coefficient of $x$ is equal to 0. First note that $0 \in R$ and therefore non-empty. Now we must show that $R$ is closed under subtraction and multiplication. Let

$f(x), g(x) \in R$ where $f(x) = a_0 + a_2x^2 + a_3x^3 + \cdots$ and $g(x) = b_0 + b_2x^2 + b_3x^3 + \cdots$. Then

$$\begin{aligned} f(x) - g(x) &= (a_0 + a_2x^2 + a_3x^3 + \cdots) - (b_0 + b_2x^2 + b_3x^3 + \cdots) \\ &= (a_0 - b_0) + (a_2 - b_2)x^2 + (a_3 - b_3)x^3 + \cdots , \end{aligned}$$

which is contained in $R$. Hence $f(x) - g(x) \in R$. Now consider,

$$\begin{aligned} f(x)g(x) &= (a_0 + a_2x^2 + a_3x^3 + \cdots)(b_0 + b_2x^2 + b_3x^3 + \cdots) \\ &= (a_0b_0) + (a_2b_2)x^2 + \cdots , \end{aligned}$$

which is contained in $R$. Hence $f(x)g(x) \in R$. Therefore $R$ is a subring of $F[x]$. Now we must show that $R$ is not a U.F.D. First note that $x^2$ and $x^3$ are irreducible elements since $x \notin R$. So $x^6$ can be written as $(x^2)^3 = x^2x^2x^2$ and $(x^3)^2 = x^3x^3$. But $x^2$ and $x^3$ are not associates. Hence $R$ is not a U.F.D. $\square$