6.1.3 (a) Show that the set $I = \{(k, 0) \mid k \in \mathbb{Z}\}$ is an ideal in the ring $\mathbb{Z} \times \mathbb{Z}$.

We invoke Theorem 6.1 to show that I is an ideal (Note that $I \neq \varnothing$). Let $a, b \in I$ and let $r \in R$; it suffices to show that $a - b, ra \in I$ (since $\mathbb{Z} \times \mathbb{Z}$ is commutative $ar = ra$). We have $a = (k, 0)$, $b = (\ell, 0)$ and $r = (m, n)$ for some k, ℓ, m, $n \in \mathbb{Z}$ and so

$$a - b = (k, 0) - (\ell, 0) = (k - \ell, 0) \in I$$
$$ra = (m, n)(k, 0) = (mk, 0) \in I.$$

Hence, I is an ideal as required. ◆

(b) Show that the set $T = \{(k, k) \mid k \in \mathbb{Z}\}$ is not an ideal in the ring $\mathbb{Z} \times \mathbb{Z}$.

To show that T is not an ideal it suffices to find $r \in \mathbb{Z} \times \mathbb{Z}$ and $a \in T$ such that $ra \notin T$ (by the definition of ideal). Let $r = (1, 0)$ and let $a = (1, 1)$, then $r \in \mathbb{Z} \times \mathbb{Z}$ and $a \in T$, but $ra = (1, 0) \notin T$. ◆

6.1.19 If d is the greatest common divisor of a and b in $\mathbb{Z}$, show that $(a) + (b) = (d)$. (The sum of ideals is defined in Exercise 18.)

Let $a, b \in \mathbb{Z}$ (not both 0) and let d be their greatest common divisor. Recall that $(d) = \{kd \mid k \in \mathbb{Z}\}$. Note that by exercise 18, $(a) + (b)$ is an ideal and we have

$$(a) + (b) = \{\ell + m \mid \ell \in (a), m \in (b)\} = \{au + bv \mid u, v \in \mathbb{Z}\}.$$

It was proven in the solutions to Test I that

$$\{dk \mid k \in \mathbb{Z}\} = \{au + bv \mid u, v \in \mathbb{Z}\}.$$

Hence, $(d) = \{kd \mid k \in \mathbb{Z}\} = (a) + (b)$. ◆

6.1.33 Let I be an ideal in $\mathbb{Z}$ such that $(3) \subseteq I \subseteq \mathbb{Z}$. Prove that either $I = (3)$ or $I = \mathbb{Z}$.

Suppose that $I \neq (3)$. Then there is $a \in I$ such that $a \notin (3)$. Hence, a is not divisible by 3 and, since 3 is a prime, 3 and a are relatively prime. Thus by Theorem 1.3, $1 = 3u + av$ for some $u, v \in \mathbb{Z}$. But since I is an ideal containing both 3 and a we have $3u \in I$ and $av \in I$. Hence, $1 = 3u + av \in I$. For any $n \in \mathbb{Z}$, we have $n = n \cdot 1 \in I$; hence, $I = \mathbb{Z}$. ◆

6.2.13 If R is a commutative ring with identity and (x) is the principal ideal generated by x in $R[x]$, prove that $R[x]/(x) \cong R$.

Let R be a commutative ring with identity and let $\varphi : R[x] \to R$ be defined by $\varphi(f(x)) = a_0$ for $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ (equivalently, define $\varphi(f(x)) = f(0)$). It is straightforward to check that φ is a surjective homomorphism (see Exercise 4.1.16). It follows by the First Isomorphism Theorem (Theorem 6.13) that $R[x]/K_\varphi \cong R$ where $K_\varphi = \{f(x) \mid \varphi(f(x)) = 0\}$. Thus it remains to show that $K_\varphi = (x)$. So let $f(x) = a_n x^n + \cdots a_1 x + a_0 \in K_\varphi$, then $a_0 = \varphi(f(x)) = 0$; so

$$f(x) = a_n x^n + \cdots + a_1 x = (a_n x^{n-1} + \cdots + a_1)x \in (x).$$

Conversely, suppose $f(x) \in (x)$. Then, $f(x) = g(x)x$ for some $g(x) = b_m x^m + \cdots + b_1 x + b_0$ and, hence,

$$f(x) = (b_m x^m + \cdots + b_1 x + b_0)x = b_m x^{m+1} + \cdots + b_1 x^2 + b_0 x$$

and so $\varphi(f(x)) = 0$. Thus, $f(x) \in K_\varphi$ and so $K_\varphi = (x)$. Therefore, $R[x]/(x) \cong R$ as required. ◆

6.2.23 Use the First Isomorphism Theorem to show that $\mathbb{Z}_{20}/(5) \cong \mathbb{Z}_5$.

Consider the map $\varphi : \mathbb{Z}_{20} \to \mathbb{Z}_5$ defined by $\varphi([a]_{20}) = [a]_5$ for $a \in \mathbb{Z}$. It was shown in class that this map is well-defined and that it is a homomorphism. Moreover, φ is surjective, since every element in $\mathbb{Z}_5$ is of the form $[a]_5$ for some $a \in \mathbb{Z}$ ($[a]_5 = \varphi([a]_{20})$). Note that $[a]_5 = [0]_5$ iff $5 \mid a$. Hence, K_φ, the kernel of φ, consists of all $[a]_{20}$ for which $5 \mid a$, that is,

$$K_\varphi = \{0, 5, 10, 15\} = (5) \subseteq \mathbb{Z}_{20}.$$

It follows by the First Isomorphism Theorem (Theorem 6.13) that $\mathbb{Z}_{20}/(5) = \mathbb{Z}_{20}/K_\varphi \cong \mathbb{Z}_5$. ◆