1. As \( d' \) divides \( a \) and \( b \), by the universal property of \( d \), \( d'|d \). By symmetry \( d \) divides \( d' \). But then \( d \) and \( d' \) are associates.

2. (a) As \( R \) is a UFD, we may factor \( a \) and \( b \) as

\[
a = u p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \quad \text{and} \quad b = v p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k},
\]

where \( p_1, p_2, \ldots, p_k \) are primes, \( m_1, m_2, \ldots, m_k \) and \( n_1, n_2, \ldots, n_k \) are natural numbers, possibly zero, and \( u \) and \( v \) are units. Define

\[
m = p_1^{o_1} p_2^{o_2} \cdots p_k^{o_k}
\]

where \( o_i \) is the maximum of \( m_i \) and \( n_i \). It follows easily that \( a|m \) and \( b|m \).

Now suppose that \( a|m' \) and \( b|m' \). Then, possibly enlarging our list of primes, we may assume that

\[
m' = w p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},
\]

where \( w \) is a unit and \( r_1, r_2, \ldots, r_k \) are positive integers. As \( a|m' \), \( r_i \geq m_i \). Similarly as \( b|m' \), \( r_i \geq n_i \). It follows that \( r_i \geq o_i = \max(m_i, n_i) \).

Thus \( m \) is indeed an lcm of \( a \) and \( b \). Uniqueness of lcms’ up to associates, follows as in the proof of uniqueness of gcd’s.

(b) It suffices to prove this result for one choice of gcd \( d \) and one choice of lcm \( m \). Pick \( d \) as in class (that is, take the minimum exponent) and take \( m \) as above (that is, the maximum exponent). In this case I claim that \( dm \) and \( ab \) are associates. It suffices to check this prime by prime, in which case this becomes the simple rule,

\[
m + n = \max(m, n) + \min(m, n)
\]

where \( m \) and \( n \) are integers.

3. (a) Clearly \( I + J \) is non-empty. For example it contains \( 0 = 0 + 0 \in I + J \). Suppose that \( a \) and \( b \) are in \( I + J \). Then \( a = i + j \) and \( b = k + l \), where \( i \) and \( k \) are in \( I \) and \( j \) and \( l \) are in \( J \). In this case

\[
a + b = (i + j) + (k + l) = (i + k) + (j + l).
\]

As \( i + k \in I \) and \( j + l \in J \), it follows that \( a + b \in I + J \). Thus \( I + J \) is closed under addition. Now suppose \( r \in R \). Then

\[
ra = r(i + j) = ri + rj.
\]
As $I$ and $J$ are ideals, $ri \in I$ and $rj \in J$. Thus $ra \in I + J$. Taking $r = -1$, we see that $I + J$ is closed under inverses. Thus $I + J$ is an ideal.

(b) Note that $\langle 1 \rangle = R$. Indeed given $r \in R$, $r = r \cdot 1 \in \langle 1 \rangle$. Thus an ideal $K$ is the whole of $R$ if and only if it contains 1. The result follows.

(c) We want to prove

$$IJ = I \cap J.$$

One inclusion is clear. If $a \in IJ$, then $a$ is a sum of terms of the form $ij$. Each term is clearly in $i$, as $i \in I$ and $j \in R$ and $I$ is an ideal. Thus $a \in I$. By symmetry $a \in J$. It follows that $a \in I \cap J$.

Now suppose that $a \in I \cap J$. Now $1 = i + j$. In this case,

$$a = a \cdot 1 = a(i + j) = ai + aj.$$

Now $a \in J$ and so $ai \in IJ$. Similarly $a \in I$ and so $aj \in IJ$. Thus $a \in IJ$.

4. By 3. (c) and an obvious induction, it suffices to prove that $I = I_1$ and

$$J_k = \prod_{a=2}^{k} I_a$$

are coprime. We proceed by induction on $k$. The case $k = 2$ is part of our assumption. By induction then, we can write

$$1 = i + j,$$

where $j \in J_{k-1}$. On the other hand, as $I$ and $I_k$ are coprime, we may write

$$1 = a + b,$$

where $a \in I$ and $b \in I_k$. Now multiply these two equations,

$$1 = 1 \cdot 1 = (i + j)(a + b) = ia + ib + ja + jb.$$

Now the first two terms are elements of $I$ and the last two are elements of $J_k$. The result follows.

5. (a) Let

$$\phi_i : R \rightarrow R_i$$
be the natural map. Then $\phi_i$ is a ring homomorphism. $\phi$ is the map derived from the universal property of the direct sum; as such it is automatically a ring homomorphism.

(b) I claim first that $\phi$ is surjective if and only if there are elements $s_1, s_2, \ldots, s_k$ of $R$ such that

$$\phi_b(s_a) = \delta_{ab},$$

where $\delta_{ab}$ is defined in the standard way as

$$\delta_{ab} = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{otherwise.} \end{cases}$$

One direction is clear. Otherwise suppose we can find such $s_1, s_2, \ldots, s_k$. Pick $(x_1, x_2, \ldots, x_k) \in \oplus_{i=1}^k R_i$. Then each $x_a = t_a + I_a$. Set

$$s = \sum_a t_a s_a.$$

It suffices to prove that $\phi_a(s) = t_a + I_a$, that is, to prove this result coordinate by coordinate. But

$$\phi_a(s) = \phi_a\left(\sum_b t_b s_b\right)$$

$$= \sum_b \phi_a(t_b) \phi_a(s_b)$$

$$= \sum_b \delta_{ab}(t_b + I_b)$$

$$= t_a + I_a,$$

as required.

So it suffices to prove that $I_1, I_2, \ldots, I_k$ are pairwise coprime if and only if we can find $s_1, s_2, \ldots, s_k$ as above.

First suppose that we can find such elements $s_1, s_2, \ldots, s_k$. Pick two indices $a$ and $b$ and let $I = I_a$, $J = I_b$ and $s = s_a$. Then $s + I = 1 + I$ and $s + J = 0 + J = J$. It follows that there are elements $i$ and $j$ of $I$ and $J$ such that $s + i = 1$ and $s = j$. In this case $1 - i = j$, so that $1 = i + j$. Hence $I$ and $J$ are coprime. As $a$ and $b$ are arbitrary, it follows that if $\phi$ is surjective then $I_1, I_2, \ldots, I_k$ are pairwise coprime.

It remains to prove that if $I_1, I_2, \ldots, I_k$ are pairwise coprime, we may find $s_1, s_2, \ldots, s_k$ with the given properties. By symmetry we may assume that $a = 1$. Set $I = I_1$ and $J = \cap_{a=2}^k I_a$. Then we have already seen that $I$ and $J$ are coprime. Thus there are $i$ and $j$ in $I$ and $J$ such that $1 = i + j$. Let $s = j$. As $j \in J$, $\phi_b(s_a) = 0$, if $b > 1$. As $s = 1 - i$, $\phi(s) = 1$. The result follows.
(c) The kernel is clearly equal to the intersection of the ideals. By 2, this is the same as the product.

5. Follows immediately from the Isomorphism Theorem and what we proved. There are two places that the book asks the reader to prove versions of the Chinese Remainder Theorem. The first is on page 147. The relevant questions are 20, 21, 22, 23 and 24. 20 follows from our version (GCRT). 21 is a special case of 23. 22 is a special case of the GCRT. 23 follows from the our version, by taking $R = \mathbb{Z}$, $I = \langle m \rangle$ and $J = \langle n \rangle$. 24 is equivalent to saying $\phi$ is surjective.

The second is on page 165. The relevant question is 17. As $R = F[x]$ is a UFD, if $p(x)$ is prime it is certainly irreducible. As $R$ is also a Euclidean domain, if $p(x)$ and $q(x)$ have no common factor (for example if $p(x)$ is prime and $p(x)$ does not divide $q(x)$) then we may find $r$ and $s$ such that

$$1 = r(x)p(x) + s(x)q(x).$$

Thus the ideals $\langle p_a(x) \rangle$ are pairwise coprime and the result follows by the GCRT.