Algebra II. Exercise 1.
Solutions.

1. The implication $f \circ g = f \circ h \Rightarrow g = h$ does not hold for example, if $f: Y \to Z$ is a constant function and $g, h: X \to Y$ are any two different functions. Then $g \neq h$, but $f \circ g = f \circ h$.
The implication $g \circ f = h \circ f \Rightarrow g = h$ does not hold for example, if $f: X \to Y$ is a constant function y_0 and $g, h: Y \to Z$ are any two different functions which obtain the same value at y_0. Then $g \neq h$, but $g \circ f = h \circ f$. For example $f: \mathbb{R} \to \mathbb{R}, f(x) \equiv 1$; $g, h: \mathbb{R} \to \mathbb{R},\ g(x) = x,\ h(x) = x^2$.
Suppose that $f: Y \to Z$ on injective, $g, h: X \to Y$ and $f \circ g = f \circ h$. We prove that $g = h$: Let $x \in X$. By assumption we have $f(g(x)) = f(h(x))$, from which (by using injectivity of f) we obtain $g(x) = h(x)$. Thus $g(x) = h(x)$ for every $x \in X$, that is, $g = h$.
Suppose then that $f: X \to Y$ is surjective, $g, h: Y \to Z$ and $g \circ f = h \circ f$. We prove that $g = h$: Let $y \in Y$. Since f is surjective, we can choose $x \in X$, for which $f(x) = y$. By assumption $g(f(x)) = h(f(x))$, that is $g(y) = h(y)$. Thus $g(y) = h(y)$ for every $y \in Y$, that is, $g = h$.

2. Each coset gH is non-empty, since always $g = ge \in gH$. Furthermore every element belongs to some coset: if $g \in G$, then $g = ge \in gH$. Suppose the contrary that the cosets don't form a partition, that is there exists an element $x \in G$, which belongs to two different cosets $gH, \bar{g}H$. Since $gH \neq \bar{g}H$, there exists an element in one of the sets which doesn't belong to the other set, say $g' \in gH \setminus \bar{g}H$; thus $g' = gh_1$ for some $h_1 \in H$. Since $x \in gH \cap \bar{g}H$, we have that $x = gh_2 = \bar{g}h_3$ for some $h_2, h_3 \in H$. Now $g = \bar{g}h_3h_2^{-1}$, from which it follows that

$$g' = gh_1 = \bar{g}h_3h_2^{-1}h_1 \in \bar{g}H,$$

which is a contradiction. Thus the cosets form a partition.

Then we prove that the given conditions are equivalent:

1) $\Rightarrow$ 2): Since $y = ye \in yH$ and $yH = xH$, we have that $y \in xH$, that is $y = xh$ for some $h \in H$. Then $x^{-1}y = h \in H$.
2) $\Rightarrow$ 3): Since $x^{-1}y \in H$, we have that $y^{-1}x = (x^{-1}y)^{-1} \in H$. Thus $y^{-1}x = h$ for some $h \in H$ and hence $x = yh \in yH$.

3) $\Rightarrow$ 4): Suppose that $x \in yH$. We may choose $z = y$, since $x \in yH$ and $y \in yH$.
4) $\Rightarrow$ 1): Follows from the fact that the cosets form a partition: if $x \in zH$ and $x \in xH$, then necessarily $xH = zH$. Similarly $yH = zH$, from which it follows that $xH = yH$.

3. a) We assume known that $\mathbb{Z} \leq \mathbb{Q}$, from which it follows that the relation is an equivalence relation [Häsä-Rämö, Lemma 11.4, p. 149]. Compatibility: Let $x, x', y, y' \in \mathbb{Q}$, $x \sim x'$ and $y \sim y'$. Thus $x - x' = k \in \mathbb{Z}$ and $y - y' = l \in \mathbb{Z}$. Now

$$(x + y) - (x' + y') = (x - x') + (y - y') = k + l \in \mathbb{Z},$$

and thus $x + y \sim x' + y'$, which proves compatibility.
b) The set $\mathbb{Q}/\mathbb{Z}$ is infinite: If $n, m \in \mathbb{N}_+$ and $n \neq m$, then $\frac{1}{n} - \frac{1}{m}$ is not an integer, and thus all the numbers $1, \frac{1}{2}, \frac{1}{3}, ...$ belong to different equivalence classes. Thus there are infinitely many equivalence classes, that is, elements of the set $\mathbb{Q}/\mathbb{Z}$.
By the compatibility and Proposition 1.3 we have that $\mathbb{Q}/\mathbb{Z}$ is a group. It is an Abelian group, because $\mathbb{Q}$ is:

$$[x] + [y] = [x + y] = [y + x] = [y] + [x]$$

for every $[x], [y] \in \mathbb{Q}/\mathbb{Z}$.
The orders of the elements: An arbitrary element of the group $\mathbb{Q}/\mathbb{Z}$ can be written in the form $x = \frac{m}{n} + \mathbb{Z}$, where $m \in \mathbb{Z}$, $n \in \mathbb{N}_+$. Now for $x + x + ... + x$ (n times) we have $(\frac{m}{n} + \cdots + \frac{m}{n}) + \mathbb{Z} = m + \mathbb{Z} = \mathbb{Z}$, which is the neutral element of the group $\mathbb{Q}/\mathbb{Z}$. Thus the order of x is finite.

4. a) The group $\mathbb{Z}_5 \times \mathbb{Z}_3$ is cyclic, for example the element $([1]_5, [1]_3)$ generates the group. Thus $\mathbb{Z}_5 \times \mathbb{Z}_3 \cong \mathbb{Z}_{15}$, by [Häsä-Rämö, Proposition 9.6, p. 126].
b) Suppose that G is a group of order 4. We know [Häsä-Rämö, Proposition 11.14, p. 155] that the possible orders of elements of G are factors of 4. The neutral element is the only with order 1, so the other elements have order 2 or 4.
That leaves two possibilities:
1) There exists an element in G whose order is 4. Then this element generates the whole group, that is, G is cyclic. Thus it is isomorphic with $\mathbb{Z}_4$ [Häsä-Rämö, Proposition 9.6, p. 126].

2) Every element (except the neutral element) has order two. When we write the multiplication table for G, we have the neutral element at each place in the diagonal (from the top left corner to the bottom right corner). After this we can fill the whole table using the fact that "every element appears in each row and each column exactly once", and we notice that G is isomorphic with $\mathbb{Z}_2 \times \mathbb{Z}_2$.
Remark. The groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic with each other, since $\mathbb{Z}_4$ is cyclic and $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not.

5. Let $x \in R$. Now

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$$

(in the second step we used the distributive law), from which we get $0 = x \cdot 0$ by using the cancellation law for the addition. Similarly we obtain $0 \cdot x = 0$.
Assume the contrary that $0 = 1$ and there exists $x \in R$, $x \neq 0$. Then $0 \cdot x = 1 \cdot x$, but using the above fact we have $0 \cdot x = 0$ and from the definition of the unit element 1 it follows that $1 \cdot x = x \neq 0$. This is a contradiction, and hence $0 \neq 1$.

6. First we prove compatibility: Suppose that $x, x', y, y' \in \mathbb{N}$ are elements such that xRx' and yRy'. We have four possibilities:
1) $x = x'$ and $y = y'$
2) $x = x'$ and $y \geq n$ and $y' \geq n$ and $m|y - y'$
3) $y = y'$ and $x \geq n$ and $x' \geq n$ and $m|x - x'$
4) $x, x', y, y' \geq n$ and $m|x - x'$ and $m|y - y'$.
In case 1) clearly $x + y = x' + y'$, and thus $(x + y)R(x' + y')$. In case 2) we observe that then $x + y \geq n$ and $x' + y' \geq n$ and $(x + y) - (x' + y') = (x - x') + (y - y') = y - y'$, which m divides; thus case 2) is ok. Case 3) can be treated similarly as 2). In case 4) we have $x + y \geq n$ and $x' + y' \geq n$ and $(x+y) - (x'+y') = (x - x') + (y - y')$, which m divides, since it divides both $x - x'$ and $y - y'$.
Thus in every case we have $(x + y)R(x' + y')$, which proves compatibility.
Next we list the equivalence classes, that is, the elements of the set $\mathbb{N}/R_{m,n}$: If $x \leq n - 1$, then $[x] = \{x\}$. If $x \geq n$, then

$$[x] = \{x + my \mid y \in \mathbb{Z} \text{ ja } x + my \geq n\}.$$

Thus $[n] = \{n, n+m, n+2m, ...\}$, $[n+1] = \{n+1, n+m+1, n+2m+1, ...\}$, ..., $[n+m-1] = \{n+m-1, n+2m-1, ...\}$ and $[n+m] = [n]$, ...
A binary operation can be defined by the formula $[x] + [x'] = [x + x']$ and $[0]$ is the neutral element of this operation.

Some additional information: If $n = 0$, we have $(\mathbb{N}/R_{m,n}, +) \cong (\mathbb{Z}_m, +)$, that is, the quotient set becomes a group. If $n > 0$, then $[0]$ is the only element which has an inverse element.