Algebra II. Exercise 8.
Solutions.

1. a) Because $\gcd(m,n)=1$, there exist integers b,c, such that $cm+bn=a$, see [Häsä–Rämö, Corollary 5.5, p. 80]. Now

$$\frac{a}{mn}=\frac{cm+bn}{mn}=\frac{cm}{mn}+\frac{bn}{mn}=\frac{b}{m}+\frac{c}{n}.$$

b) For example $a=1, m=n=2$. If we could have $\frac{1}{2\cdot 2}=\frac{b}{2}+\frac{c}{2}$, then $b+c=\frac{1}{2}$, which doesn't hold for any integers b,c.

c) Let $q\in\mathbb{Q}$. Write

$$q=\frac{a}{p_1^{k_1}\cdots p_n^{k_n}},$$

where the denominator is presented as a product of its' prime factors (the numbers p_i are thus different prime numbers). We prove the claim by induction with respect to n:
$n=1$: $q=\frac{a}{p_1^{k_1}}$, ok.
General case:

$$\frac{a}{p_1^{k_1}\cdots p_n^{k_n}}=\frac{a}{(p_1^{k_1}\cdots p_{n-1}^{k_{n-1}})\cdot p_n^{k_n}}=\frac{b}{p_1^{k_1}\cdots p_{n-1}^{k_{n-1}}}+\frac{m_n}{p_n^{k_n}}=\sum_{i=1}^{n-1}\frac{m_i}{p_i^{k_i}}+\frac{m_n}{p_n^{k_n}}=\sum_{i=1}^{n}\frac{m_i}{p_i^{k_i}}.$$

In the second equality we used the result of item a); we could use it, because the numbers p_i are different prime numbers, and hence $\gcd(p_1^{k_1}\cdots p_{n-1}^{k_{n-1}}, p_n^{k_n})=1$. In the third step we used the inductive assumption.

2. a) From the theory of groups, we know that $\mathrm{Ker}(f)$ is a subgroup. If $a\in A$ and $x\in\mathrm{Ker}(f)$, then $f(ax)=f(a)\cdot f(x)=f(a)\cdot 0_B=0_B$, and thus $ax\in\mathrm{Ker}(f)$. Thus the ideal condition holds.

b) From the theory of groups, we know that $\mathrm{Im}(f)$ is a subgroup. If $b_1,b_2\in\mathrm{Im}(f)$, then choose $a_1,a_2\in A$, such that $f(a_1)=b_1$, $f(a_2)=b_2$. Now $f(a_1a_2)=f(a_1)f(a_2)=b_1b_2$, and thus $b_1b_2\in\mathrm{Im}(f)$. Furthermore, by the definition of a ring homomorphism we have $f(1_A)=1_B$, hence $1_B\in\mathrm{Im}(f)$.

c) By item a) $\mathrm{Ker}(f)$ is an ideal of the ring A, so we know that $A/\mathrm{Ker}(f)$ is a ring equipped with the induced binary operations. By item b) $\mathrm{Im}(f)$ is a ring. From the theory of groups we know that the map $\bar{f}$, $\overline{a} \mapsto f(a)$ is well defined and an isomorphism between groups. Furthermore, if $\overline{a_1}, \overline{a_2} \in A/\mathrm{Ker}(f)$, then

$$\bar{f}(\overline{a_1} \cdot \overline{a_2}) = \bar{f}(\overline{a_1 a_2}) = f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2) = \bar{f}(\overline{a_1}) \cdot \bar{f}(\overline{a_2}),$$

thus $\bar{f}$ is a homomorphism also with respect to multiplication. Because $\bar{f}(\overline{1}) = f(1_A) = 1_B$, we have that $\bar{f}$ is a ring homomorphism. Thus $\bar{f}$ is a ring isomorphism.

3. First we notice that since $d|m$, we have $m \in \langle d \rangle$. Similarly $n \in \langle d \rangle$. From this it follows that $\langle m, n \rangle \subset \langle d \rangle$ (because $\langle m, n \rangle$ is the smallest ideal containing m and n; $\langle d \rangle$ is some ideal containing m and n).
By Bezout's theorem we know that d can be written as $d = xm + yn$ for some $x, y \in \mathbb{Z}$. Thus we have that $d \in \langle m, n \rangle$, from which it follows that $\langle d \rangle \subset \langle m, n \rangle$.

4. a) We present the polynomials f and g as products of irreducible polynomials in the ring $\mathbb{Z}[X]$:

$$f = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1), \; g = X(X^2 + 1).$$

We choose $h = X^2 + 1$ (=gcd(f, g)) and prove that $\langle h \rangle = \langle f, g \rangle$.
We notice that $f = (X^2 - 1) \cdot h$, and $g = X \cdot h$, thus $f \in \langle h \rangle$ and $g \in \langle h \rangle$, then also $\langle f, g \rangle \subset \langle h \rangle$ (because $\langle f, g \rangle$ is the smallest ideal containing the polynomials f and g; $\langle h \rangle$ is some ideal containing the polynomials f and g). On the other hand, h can be represented using the polynomials f and g:

$$f = (X^2 - 1)h = X^2 h - h = Xg - h,$$

thus

$$h = Xg - f \in \langle f, g \rangle,$$

and also $\langle h \rangle \subset \langle f, g \rangle$.
Hence $\langle h \rangle = \langle f, g \rangle$.
b) Let $a = [X]$, the class of the element X in the quotient ring $\mathbb{Z}[X]/\langle h \rangle$. Now $X^2 + 1 = h$, thus in the quotient ring we have

$$a^2 + 1 = [h] = 0,$$

that is, $a^2 = -1$.

5. Define $.: \mathbb{Z}_n \times M \to M$ by the formula

$$(*) \qquad [k].x = kx \quad \text{(multiple)}, \quad k \in \mathbb{Z}.$$

We prove that this is well defined: If $[k] = [k']$, then $k' = k + mn$ for some $m \in \mathbb{Z}$. Thus

$$k'x = (k + nm)x = kx + n(mx) = kx,$$

because by assumption we have $n(mx) = 0$.
The conditions (M1)–(M4) follow from properties of the multiple:

- $[1].x = 1x = x$
- $([k_1] \cdot [k_2]).x = [k_1k_2].x = (k_1k_2)x = k_1(k_2x) = [k_1].(k_2x) = [k_1].([k_2].x)$
- $([k_1] + [k_2]).x = [k_1 + k_2].x = (k_1 + k_2)x = k_1x + k_2x = [k_1].x + [k_2].x$
- $[k].(x + y) = k(x + y) = kx + ky = [k].x + [k].y.$

Uniqueness: By property (M1) we have $[1].x = x$, thus by (M3) we have $[2].x = ([1] + [1]).x = [1].x + [1].x = x + x = 2x$ etc. Also $[-1].x = -x$, $[-2].x = -2x$ etc. Thus the formula $(*)$ is the only possible linear action of $\mathbb{Z}_n$ in an Abelian group M.

6. a) If $V = \{0\}$, it has $\emptyset$ as a basis. Suppose now that the space V contains more than just the zero vector.
Let $\mathcal{A} = \{A_i \mid i \in I\}$ be a chain in the set $\mathcal{P}$. We prove that this chain has the upper bound $A = \cup_{i \in I} A_i \in \mathcal{P}$. Clearly this union is an upper bound for the chain with respect to inclusion, thus it is sufficient to prove that it belongs to the set $\mathcal{P}$, that is, the union is a linearly independent set. Suppose that $a_1, ..., a_n \in A$ are different elements and the linear combination

$$x_1a_1 + ... + x_na_n = 0, \quad x_1, ..., x_n \in K.$$

Now for every index $k = 1, ..., n$ there exists an index $i_k \in I$, for which $a_k \in A_{i_k}$. Since the sets A_i form a chain, there exists an index i, such that $a_k \in A_i$ for every $k = 1, ..., n$. Since the set A_i is linearly independent, it follows that all the coefficients $x_1, ..., x_n = 0$. Thus A is linearly independent.

Clearly the collection $\mathcal{P}$ is non-empty, since every subset containing just one vector ($\neq 0$) is linearly independent. It now follows from Zorn's lemma that the set $\mathcal{P}$ has a maximal element, denote it by X.

We now prove that the set X spans the whole space V. Antithesis 1: There exists a vector $v \in V$, $v \notin span(X)$. We prove that then the set $X \cup \{v\}$ would be linearly independent:
Antithesis 2: There exists a linear combination of the set $X \cup \{v\}$, where all the coefficients are not zero, but the linear combination is zero. The vector v has to be in this linear combination, since in the set X such linear combinations don't exist (because X is a linearly independent set). Thus there exists a linear combination

$$r_0 v + \sum_{i=1}^{n} r_i x_i = 0$$

with a non-zero coefficient r_i. The coefficient r_0 must be $\neq 0$, because otherwise some non-trivial linear combination of the set X would be 0. Now

$$(*) \qquad v = \sum_{i=1}^{n} -\frac{r_i}{r_0} x_i \in span(X),$$

which is a contradiction, since $v \notin span(X)$. From this it follows that antithesis 2 doesn't hold, and thus the set $X \cup \{v\}$ is linearly independent. However, this contradicts the maximality of X. Thus antithesis 1 is false, and we have that X spans the space V.
Thus we found a linearly independent set which spans the vector space, that is, a basis.

b) The detail $(*)$ does not work.