Algebra II. Exercise 12.
Solutions.

1. a) First we embed $\mathbb{R}$ into $\mathbb{R}^2$ using the map f of exercise 2 last week. Here the unit element of $\mathbb{R}^2$ is $(1,1)$, so the map $f\colon \mathbb{R} \to \mathbb{R}^2$ is $f(x) = (x,x)$. Hence $\mathbb{R}$ is identified with the subset $B = \{(x,x) \mid x \in \mathbb{R}\}$. Choose as basis elements for example $(1,1)$ and $b = (1,-1)$. We notice that $b^2 = (1 \cdot 1, (-1)\cdot(-1)) = (1,1)$, which is an element in the subset of B corresponding to the positive real numbers. Thus we have that "$b^2 > 0$".
Notice that if we had chosen the other basis element b differently, we might not have got the result immediately, but we should have done the trick presented in exercise 6 last week. Example: Choose $b = (1,2)$. Then $b^2 = (1,4) = -2 \cdot (1,1) + 3 \cdot (1,2)$ and we choose $b' = (1,2) - \frac{1}{2} \cdot 3 \cdot (1,1) = ... = (-\frac{1}{2}, \frac{1}{2})$, then $(b')^2 = (\frac{1}{4}, \frac{1}{4}) \in B$.
b) It is not a field, since for example the element $(1,0)$ doesn't have an inverse. If $(x,y)\cdot(1,0) = (1,1)$, then we should have $y \cdot 0 = 1$, which is not possible.

2. If R is a ring then denote (as before)

$$n.x = x + ... + x,$$

where the number or terms is n (or $-n$, if $n < 0$). If $n \in \mathbb{Z}$, $x \in R$, then we have that

$$n.x = (n.1_R)x \quad \text{and} \quad (nm).1_R = n.(m.1_R) = (n.1_R)\cdot(m.1_R).$$

a) Suppose that $\mathrm{char}(K) = p > 0$. Notice that we cannot have $p = 1$, since then we would have $0 = 1.1 = 1$. If $p = ab$ for some $a, b \in \mathbb{N}$, then

$$0 = (ab).1_K = (a.1_K)\cdot(b.1_K).$$

Because the field K is an integral domain, we have $a.1_K = 0$ or $b.1_K = 0$. On the other hand, $0 < a \leq p$ and $0 < b \leq p$ and p is the characteristic of K (*smallest* number, for which $p.1_K = 0$), so we must have $a = p$ or $b = p$. Thus p is a prime number.

b) Suppose that $L \subset K$ is a subfield. Define $f\colon \mathbb{Z} \to K$ by the formula $f(n) = n.1_K$. Now $f(n+m) = (n+m).1 = n.1 + m.1 = f(n) + f(m)$, $f(nm) = (nm).1 = (n.1)(m.1) = f(n) \cdot f(m)$ and $f(1) = 1.1_K = 1_K$, thus f is a ring homomorphism. Notice that since L is a subfield, then $1_K \in L$ and $n.1_K \in L$ for every $n \in \mathbb{Z}$, that is, $\mathrm{Im}(f) \subset L$.
We now prove that $\mathrm{Ker}(f) = p\mathbb{Z}$: Because $p = \mathrm{char}(K)$, then $p\mathbb{Z} \subset \mathrm{Ker}(f)$. If $n \in \mathrm{Ker}(f)$, then $n.1 = 0$ and by the division algorithm we have $n = qp + r$, where $q, r \in \mathbb{Z},\ 0 \leq r < p$. Because

$$r.1 = (n - qp).1 = n.1 - qp.1 = 0 - 0 = 0,$$

$r < p$ and $p = \mathrm{char}(K)$, we must have $r = 0$. Thus $p|n$ and $n \in p\mathbb{Z}$. By the homomorphism theorem for rings we now have

$$\mathbb{F}_p = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \cong \mathrm{Im}(f) \subset L.$$

c) Suppose that $L \subset K$ is a subfield. Define $f\colon \mathbb{Q} \to K$ by the formula $f(a/b) = (a.1) \cdot (b.1)^{-1}$. Notice that $b.1 \neq 0_K$, because $b \in \mathbb{Z} \setminus \{0\}$ and $\mathrm{char}(K) = 0$.
We prove that f is well defined: If $a/b = c/d$, then $ad = bc$, from which it follows that $(a.1)(d.1) = (b.1)(c.1)$ and also that $(a.1)(b.1)^{-1} = (c.1)(d.1)^{-1}$, that is, $f(a/b) = f(c/d)$.
Then we prove that f is a ring homomorphism:

$$f(\frac{a}{b} + \frac{c}{d}) = f(\frac{ad+bc}{bd}) = ((ad+bc).1)((bd).1)^{-1}$$

$$= ((ad).1 + (bc).1)((bd).1)^{-1} = ((ad).1)((bd).1)^{-1} + ((bc).1)((bd).1)^{-1}$$
$$= (a.1)(d.1)(b.1)^{-1}(d.1)^{-1} + (b.1)(c.1)(d.1)^{-1}(b.1)^{-1}$$
$$= (a.1)(b.1)^{-1} + (c.1)(d.1)^{-1} = f(\frac{a}{b}) + f(\frac{c}{d}).$$

$$f(\frac{a}{b} \cdot \frac{c}{d}) = f(\frac{ac}{bd}) = (ac.1)(bd.1)^{-1} = (a.1)(c.1)(b.1)^{-1}(d.1)^{-1}$$
$$= (a.1)(b.1)^{-1}(c.1)(d.1)^{-1} = f(\frac{a}{b}) \cdot f(\frac{c}{d}).$$

$$f(1) = f(\frac{1}{1}) = (1.1) \cdot (1.1)^{-1} = 1_K.$$

Finally we consider the kernel of f, $\mathrm{Ker}(f) = \{a/b \mid (a.1)(b.1)^{-1} = 0\}$. If $(a.1)(b.1)^{-1} = 0$, then $(a.1)(b.1)^{-1}(b.1) = 0$, from which it follows that $(a.1) = 0$. Because $\mathrm{char}(K) = 0$, it follows that $a = 0$, and thus $\mathrm{Ker}(f) = \{0\}$.
Hence f is injective, and $\mathrm{Im}(f) \subset L$ is isomorphic with the field $\mathbb{Q}$.

3. a) "$\Rightarrow$": If a and b are associates, then $a|b$ and $b|a$, hence there exist $c, d \in R$, such that $a = bc, b = ad$. Thus $a = adc$, that is, $a(1 - dc) = 0$. Because R is an integral domain, we have $a = 0$ or $1 - dc = 0$. If $a = 0$, then also $b = 0$ and we can write $a = b \cdot 1$, that is, $a = b\cdot$unit. On the other hand, if $1 - dc = 0$, then $dc = 1$, that is, $d = c^{-1}$, c is a unit and thus $a = b\cdot$unit.
"$\Leftarrow$": If $a = bc$, where c is a unit, then $b = ac^{-1}$. Thus $a|b$ (because $b = ac^{-1}$) and $b|a$ (because $a = bc$), that is, a and b are associates.
b) Suppose that $a, b \in R \setminus \{0\}$ are associates and $a = bc$. By item a) we have $a = bu$, where u is a unit. Now $bc = bu$, and thus $b(c - u) = 0$. Since R is an integral domain and $b \neq 0$, we must have $c = u$ and thus also c is a unit.
c) Suppose that a, b are units. Now $a = (ab^{-1})b$, which gives $b|a$ and $b = (ba^{-1})a$, which gives $a|b$. Thus a and b are associates.

4. First we notice that 2 is not a unit, because if $2 \cdot (a + i\sqrt{5}b) = 1$, then we would have $2a = 1$, which doesn't hold for any $a \in \mathbb{Z}$.
If $2 = (a + i\sqrt{5}b)(c + i\sqrt{5}d)$, where $a, b, c, d \in \mathbb{Z}$, then (by taking squares of the moduli) we obtain

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

If $b \neq 0$ or $d \neq 0$, then the right hand side of the equation would be ≥ 5, which is a contradiction, and thus we have $b = d = 0$. Thus $a^2 \cdot c^2 = 4$, from which it follows that $ac = \pm 2$, and the factoring is trivial. Hence 2 is irreducible.
Because $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 6$, then $2|(1 + i\sqrt{5})(1 - i\sqrt{5})$. If $1 + i\sqrt{5} = 2\cdot(a+i\sqrt{5}b)$, then we would have $2a = 1$ and $2b = 1$, which is a contradiction, and thus $2 \nmid 1+i\sqrt{5}$. Analogously $2 \nmid 1-i\sqrt{5}$. Hence 2 is not a prime element.
From Lemma 11.9 (5.9) it now follows that $\mathbb{Z}[i\sqrt{5}]$ is not a unique factorization domain.

4. Suppose that R is a principal ideal domain and $0 \neq a \in R$.
"(a)$\Rightarrow$(b)": Follows from Proposition 11.4 (5.4).

"(b)⇒(c)": Let a be an irreducible element. It generates the ideal

$$I = \langle a \rangle = \{ar \mid r \in R\}.$$

If $I = R$, then especially $1 \in I$, from which it follows that there exists $r \in R$, for which $ar = 1$. This is not possible, since an irreducible element is not a unit. Thus I is a proper ideal of R. Suppose now that J is an ideal and $I \subset J$. It suffices to prove that $J = I$ or $J = R$. Because R is a principal ideal domain, we have that J can be generated by one element, that is, there exists $b \in R$, for which

$$J = \langle b \rangle = \{br \mid r \in R\}.$$

Because $I \subset J$, then there exists $r \in R$, for which $a = rb$. Especially b is a factor of a. Because a is irreducible, we have that b is a unit or an associate of a. In the first case we have $J = R$, in the second case $J = I$. Thus I is maximal.
"(c)⇒(a)": Suppose that

$$I = \langle a \rangle = \{ar \mid r \in R\}$$

is a maximal ideal. We prove that a is a prime element. Suppose that $a|bc$, we prove that $a|b$ or $a|c$. Let

$$J = \langle a, b \rangle = \{ar + bs \mid r, s \in R\},$$

the ideal generated by the elements a and b. Clearly $I \subset J$. Because I is maximal, we have $J = I$ or $J = R$. If $J = I$, then $b \in I$, and thus $a|b$. If $J = R$, then $1 \in J$, and hence there exists $r, s \in R$, for which $1 = ra + sb$. From this we obtain that

$$c = c \cdot 1 = c(ra + sb) = a(rc) + s(bc) = a(rc + sd),$$

where $d \in R$ is an element, for which $ad = bc$ (such an element exists, since $a|bc$). Thus $a|c$.
We have proved that $a|b$ or $a|c$, hence a is a prime element.

The last implication follows more directly, if we use Corollary 6.8:
Suppose that $a|bc$, then $bc \in \langle a \rangle$. The ideal $\langle a \rangle$ is maximal by assumption, so it is a prime ideal by Corollary 6.8. From the definition of a prime ideal it now follows that $b \in \langle a \rangle$ or $c \in \langle a \rangle$, that is $a|b$ or $a|c$.

6. First we notice that if $a = b$, then the polynomial has the root -1, and if $a + b = -2$, then it has the root 1; thus in these cases the polynomial is reducible.
If the polynomial is reducible, then (because the degree is ≤ 3) it has a root in $\mathbb{Q}$. By Proposition 11.10 (5.10) we see that the root is 1 or -1. If the root is 1, then by substituting we obtain that $a + b = -2$; if the root is -1, we obtain that $a = b$.