Algebra II. Exercise 11.
Solutions.

1. a) Consider the polynomial $P-Q$. If $P-Q$ were not the zero polynomial, then it would have at most $\deg(P-Q)$ roots, that is, a finite number. Using the assumption, we get that $(P-Q)(x) = P(x) - Q(x) = 0$ for every $x \in K$, that is, there are infinitely many roots. Thus the polynomial $P-Q$ must be the zero polynomial, that is, $P = Q$.
b) Consider the ring $\mathbb{Z}_4$ and the polynomials $P = 2X^3 + X^2 + 1$ and $Q = X^4 + 2X^2 + 1$ in $\mathbb{Z}_4[X]$. By direct calculation we see that $P(c) = Q(c)$ for every $c \in \mathbb{Z}_4$, but clearly P and Q are different polynomials.

2. Define $f\colon R \to A,\ f(r) = r.1$. Let $r, s \in R$. Since

$$f(r+s) = (r+s).1 = r.1 + s.1 = f(r) + s(r)$$

and

$$f(r.s) = f(rs) = (rs).1 = r.(s.1) = r.f(s),$$

we see that f is an R-module homomorphism. By bilinearity of the algebra multiplication we also get that

$$f(rs) = (rs).1 = r.(s.(1 \cdot 1)) = r.(1 \cdot (s.1)) = (r.1) \cdot (s.1) = f(r) \cdot f(s),$$

thus f is an algebra homomorphism, for which $f(1_R) = 1_R.1_A = 1_A$.
Suppose now that R is a field and A non-trivial ($A \neq \{0\}$). Then $1_A \neq 0_A$: If we had $1_A = 0_A$, then for every $x \in A$ we would have $x = 1_A \cdot x = 0_A \cdot x = 0_A$, which is a contradiction, since $A \neq \{0\}$.
We prove that f is injective, that is, $\mathrm{Ker}(f) = \{0_R\}$:
If we had $r \in R \setminus \{0\}$ and $f(r) = r.1 = 0_A$, then we would have

$$1_A = 1_R.1_A = (r^{-1}r).1_A = r^{-1}.(r.1_A) = r^{-1}.0_A = 0_A,$$

which is a contradiction with the above fact.
Thus f is injective and $R \cong f(R)$, which is a subalgebra of A.

3. a) Let $x \in \mathbb{H} \setminus \{0\}$, $x = a + bi + cj + dk$, $a, b, c, d \in \mathbb{R}$. Define $\|x\| = \sqrt{a^2 + b^2 + c^2 + d^2}$ and

$$y = \frac{1}{\|x\|^2}(a - bi - cj - dk),$$

then we have that

$$xy = \frac{1}{\|x\|^2}(a^2 - abi - acj - adk + abi + b^2 - bck + bdj$$

$$+acj + bck + c^2 - cdi + adk - bdj + cdi + d^2) = \frac{1}{\|x\|^2}(a^2 + b^2 + c^2 + d^2) = 1.$$

Similarly we can calculate that $yx = 1$, that is, $y = x^{-1}$.
b) Denote $\bar{x} = (x_1, x_2, x_3)$, $\bar{y} = (y_1, y_2, y_3)$, then

$$\bar{x} \cdot \bar{y} = x_1y_1 + x_2y_2 + x_3y_3$$

and

$$\bar{x} \times \bar{y} = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1).$$

Now

$$xy = -x_1y_1 + x_1y_2k - x_1y_3j - x_2y_1k - x_2y_2 + x_2y_3i + x_3y_1j - x_3y_2i - x_3y_3$$

$$= -(x_1y_1 + x_2y_2 + x_3y_3) + (x_2y_3 - x_3y_2)i + (x_3y_1 - x_1y_3)j + (x_1y_2 - x_2y_1)k$$

$$= -(\bar{x} \cdot \bar{y}) + (\bar{x} \times \bar{y}) \cdot (i, j, k).$$

4. Denote the unit matrix by I. The first claim follows directly by calculating the matrix products, for example

$$\mathbf{i}^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I,$$

$$\mathbf{i} \cdot \mathbf{j} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \mathbf{k}.$$

When we compare with the multiplication table of the quaternions, we notice that they are identical.

Next we prove that the sequence $\{I, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ is free in the $\mathbb{R}$-vector space $\mathbb{C}^{2\times 2}$: If $a, b, c, d \in \mathbb{R}$ and

$$a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

then we get that $a + bi = 0$ and $c + di = 0$, from which it follows that $a = b = c = d = 0$, that is, the sequence is free.

Denote now $A = \{aI + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$, the vector subspace generated by the matrices $I, \mathbf{i}, \mathbf{j}, \mathbf{k}$. Now these vectors form a basis for A, so by setting $\varphi(I) = 1$, $\varphi(\mathbf{i}) = i$, $\varphi(\mathbf{j}) = j$ and $\varphi(\mathbf{k}) = k$ we obtain a linear map $\varphi\colon A \to \mathbb{H}$. The map φ is injective, since the sequence $(1, i, j, k)$ is free in $\mathbb{H}$, and surjective, since the vectors $1, i, j, k$ span $\mathbb{H}$. Thus A and $\mathbb{H}$ are isomorphic as $\mathbb{R}$-vector spaces.

The matrix product defines multiplication for the elements $I, \mathbf{i}, \mathbf{j}, \mathbf{k}$, thus (because they form a basis) we can define (by Theorem 9.6 (3.6) in the lecture material) an $\mathbb{R}$-algebra structure in the set A.

The map φ satisfies the homomorphism condition $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ for all basis elements a, b, because (as we calculated at the beginning) the multiplication tables are identical. Now by Theorem 9.5 (3.5) φ is an $\mathbb{R}$-algebra homomorphism. Since we already proved that φ is an isomorphism of $\mathbb{R}$-vector spaces, it is thus an isomorphism of $\mathbb{R}$-algebras.

Since matrix multiplication is associative, the algebra A is associative by item (i) of Proposition 9.4 (3.4). By the isomorphism we proved above, also $\mathbb{H}$ is an associative algebra.

5. "(i)⇒(ii)": Let I be an ideal of R, $I \neq \{0\}$. Let $a \in I$, $a \neq 0$. Since R is a field, there exists an inverse element a^{-1}, and we have $1 = aa^{-1} \in I$. From this it follows that $I = R$, hence the only ideals are $\{0\}$ and R.

"(ii)⇒(iii)": Clear.

"(iii)⇒(i)": If $\{0\}$ is a maximal ideal, then by Proposition 6.7 the quotient ring $R/\{0\}$ is a field. We have $R \cong R/\{0\}$, hence R is a field.

"(ii)⇒(iv)": Let S be an arbitrary ring and $f\colon R \to S$ a ring homomorphism, which is not the zero map. Now $\mathrm{Ker}(f)$ is an ideal of the ring R, thus by condition (ii) it is $\{0\}$ or R. It cannot be R, because then f would be the zero map. Thus $\mathrm{Ker}(f) = \{0\}$, and thus f is injective.

"(iv)⇒(ii)": Antithesis: there exists an ideal I of R, such that $\{0\} \subsetneq I \subsetneq R$. Consider the quotient ring R/I and the natural homomorphism $\pi\colon R \to R/I$.

Because $I \neq R$, the map π is not the zero map. Thus by condition (iv) π is injective, from which it follows that we must have $I = \{0\}$. This is a contradiction, and the claim follows.

6. Suppose that A is a two dimensional unitary $\mathbb{R}$-algebra. By Exercise 2 we may think that $\mathbb{R} \subset A$. Then choose $b \in A$, such that $\{1, b\}$ is a basis for A. To define the multiplication in A it is sufficient to define the products for the basis elements (Proposition 9.7 (3.7)), and from those we already know that $1 \cdot 1 = 1$, $1 \cdot b = b$ and $b \cdot 1 = b$. What is left to define, is $b \cdot b$. By the following argument we may assume that $b^2 \in \mathbb{R}$:
Let $b^2 = x + yb,\ x, y \in \mathbb{R}$. Define $b' = b - \frac{1}{2}y$, then we have

$$(b')^2 = b^2 - yb + \frac{1}{4}y^2 = x + \frac{1}{4}y^2 \in \mathbb{R}.$$

Since $b' \notin \mathbb{R}$, then $\{1, b'\}$ is free, and thus we may choose $\{1, b'\}$ as a basis, or simply assume from the beginning that $b^2 \in \mathbb{R}$.
We obtain three possibilities:
(i) $b^2 > 0$: Then $b^2 = r > 0$, and we can choose $b'' = (\frac{1}{\sqrt{r}}) \cdot b$. Then $(b'')^2 = b^2/r = 1$. Since $\{1, b''\}$ is free, we may choose $\{1, b''\}$ as basis, or simply assume that $b^2 = 1$.
(ii) $b^2 < 0$: Analogously we may assume that $b^2 = -1$.
(iii) $b^2 = 0$.
Denote the algebras we obtained by A_0 (case $b^2 = 0$), A_1 ($b^2 = 1$) and A_{-1} ($b^2 = -1$). What is left to prove is that none of these are isomorphic with each other. Denote the generators b by b_0, b_1, b_{-1}, respectively.
Suppose that $f \colon A_0 \to A_{-1}$ were an isomorphism. Then $f(b_0) = x + yb_{-1},\ x, y \in \mathbb{R}$. Since $f(b_0)^2 = f(b_o^2) = f(0) = 0$ and

$$(x + yb_{-1})^2 = x^2 + 2xyb_{-1} + y^2 b_{-1}^2 = (x^2 - y^2) + 2xyb_{-1},$$

we have $(x^2 - y^2) + 2xyb_{-1} = 0$. Since $\{1, b_{-1}\}$ is a basis for A_{-1}, we obtain that $x^2 - y^2 = 0$ and $2xy = 0$, from which we can solve that $x = y = 0$, that is, $f(b_0) = 0$. From this it follows that f is not surjective, because $\mathrm{Im}(f) = \langle f(1), f(b_0) \rangle = \langle 1, 0 \rangle = \mathbb{R}$. Thus $A_0 \ncong A_{-1}$.
Similarly we obtain that $A_0 \ncong A_1$.
Suppose that $g \colon A_1 \to A_{-1}$ were an isomorphism. Then $g(b_1) = x + yb_{-1},\ x, y \in \mathbb{R}$. Since $g(b_1)^2 = g(b_1^2) = g(1) = 1$, then $(x^2 - y^2) + 2xyb_{-1} = 1$. From this we

obtain $x^2 - y^2 = 1$ and $2xy = 0$, from which we can solve that $y = 0, x = \pm 1$. Thus $g(b_1) \in \mathbb{R}$. Then g is not surjective, because $\mathrm{Im}(g) = \langle g(1), g(b_1) \rangle = \mathbb{R}$. Thus $A_1 \ncong A_{-1}$.