1. If $a = de$ and $b = df$ then $c = d(e + f)$. If $a = de$ and $c = df$ then $b = d(f - e)$. If $b = de$ and $c = df$ then $a = d(f - e)$.

2. Let $R$ be a finite integral domain. Let $x \in R$, $x \neq 0$. Since $x$ is not a zero divisor in $R$, the map $y \mapsto xy$ from $R$ to $R$ is injective. Since $R$ is finite, this map is also surjective: there exists $x' \in R$ with $xx' = 1$. Hence $x$ is a unit and $R$ is a field.

3. The Euclidean algorithm produces

\[ A = BQ_0 + R_0 \quad \text{with} \quad Q_0 = X, R_0 = X^3 + 2X \]
\[ B = R_0Q_1 + R_1 \quad \text{with} \quad Q_1 = X, R_1 = X^2 + 1 \]
\[ R_0 = R_1Q_2 + R_2 \quad \text{with} \quad Q_2 = X, R_2 = X \]
\[ R_1 = R_2Q_3 + R_3 \quad \text{with} \quad Q_3 = X, R_3 = 1 \]
\[ R_2 = R_3Q_4 \quad \text{with} \quad Q_4 = X. \]

Hence the answer is $D = 1$

A solution $(U_0, V_0)$ to Bézout’s relation $AU_0 + BV_0 = 1$ is

\[ U_0 = -(X^3 + 2X), \quad V_0 = B:\]
\[ -(X^3 + 2X)A + B^2 = 1. \]

All other solutions are of the form $U = U_0 + WB$, $V = V_0 - WA$ with $W \in \mathbb{Q}[X]$.

4. The roots of the quadratic polynomial $T^2 - 2T + 9$ are $1 + 2i\sqrt{2}$ and $1 - 2i\sqrt{2}$. From $(i + \sqrt{2})^2 = 1 + 2i\sqrt{2}$ we deduce

\[ X^4 - 2X^2 + 9 = (X - i - \sqrt{2})(X - i + \sqrt{2})(X + i - \sqrt{2})(X + i + \sqrt{2}). \]

This is the decomposition into irreducible factors over $\mathbb{C}$, while the decomposition into irreducible factors over $\mathbb{R}$ is

\[ X^4 - 2X^2 + 9 = (X^2 - 2\sqrt{2}X + 3)(X^2 + 2\sqrt{2}X + 3). \]

The polynomial $X^4 - 2X^2 + 9$ has no root in $\mathbb{Q}$, one checks that it is not the product of two quadratic polynomials with coefficients in $\mathbb{Q}$, hence it is irreducible over $\mathbb{Q}$.

5. (a) The image of $\psi$ is a subring of $S$ containing $R$, $\alpha_1, \ldots, \alpha_n$, and any subring of $S$ containing $R$, $\alpha_1, \ldots, \alpha_n$ should contain the image of $\psi$. See Milne Lemma 1.21.

(b) See Milne p. 15.

6. The implications

\[(ii) \Rightarrow (iii) \Rightarrow (vi) \Rightarrow (i) \Rightarrow (v) \Rightarrow (iv) \Rightarrow (i)\]

are easy. One proof of $(i) \Rightarrow (ii)$ is to remark that since the ring of polynomials $K[X]$ is Euclidean, the prime ideals are maximal, hence the quotient of $K[X]$ by the ideal generated by the irreducible polynomial of $\alpha$ over $K$ is a field. For another proof, see Milne 1.25.

7. The ring $E$ is the set of elements of the form $a + bi + c\sqrt{2} + di\sqrt{2}$ with $a, b, c, d$ in $\mathbb{Q}$. This is an integral domain and also vector space of dimension 4 over $\mathbb{Q}$. Hence it is a field (Milne Lemma 1.23). There are infinitely many choices of $\alpha$ with $E = \mathbb{Q}(\alpha)$. One of them is $\alpha = i + \sqrt{2}$ (see exercise 4 above).
8. (a) Let $\mathbb{F}_p$ be the prime field of $F$. It is a field with $p$ elements, isomorphic to $\mathbb{Z}/p\mathbb{Z}$. The multiplicative group $\mathbb{F}_p^\times$ of nonzero elements in $\mathbb{F}_p$ has order $p - 1$. Hence $x^{p-1} = 1$ for all $x \in \mathbb{F}_p^\times$, and therefore $x^p = x$ for all $x \in \mathbb{F}_p$. The polynomial $X^p - X$ has degree $p$, it cannot have more than $p$ roots in a field. Hence the $p$ roots of this polynomial are the elements of $\mathbb{F}_p$.

(b) Let $E$ be the set of roots of $X^q - X$ in $F$. Using the Frobenius endomorphism $x \mapsto x^p$ iterated $r$ times, one deduces that $E$ is an additive subgroup of $F$. Clearly the product of two elements in $E$ is in $E$. Hence $E$ is a field. Let $s$ be the dimension of $E$ as a $\mathbb{F}_p$-vector space. Then $E$ has $p^s$ elements, and $p^s \leq q$ because $X^q - X$ has not more than $q$ roots in $F$.

In the case where $F$ has 4 elements, the roots of $X^8 - X$ in $F$ are the 2 elements of the prime field $\mathbb{F}_2$, hence $s = 1$.

Remark. As a matter of fact, $s$ divides $r$. We can prove it using the fact that the multiplicative group $E^\times$ of the non zero elements in $E$ is cyclic (Milne exercise 1.3): there is an element in $E$ of order $p^s - 1$. This element satisfies $x^{q-1} = 1$, hence $p^s - 1$ divides $p^r - 1$. This implies that $s$ divides $r$ (if $t$ is the remainder of the Euclidean division of $r$ by $s$, then $p^t - 1$ is the remainder of the Euclidean division of $p^r - 1$ by $p^s - 1$).


http://www.jmilne.org/math/CourseNotes/FT.pdf