1. Since it is a splitting field, the extension is Galois, so we can use the fundamental theorem of Galois theory for (a)–(c).
   (a) The degree of the extension is the order of the Galois group, which is 8.
   (b) This is equivalent to asking for the number of subgroups of order 2 of $\mathbb{Z}_2 \oplus \mathbb{Z}_4$. Each element of order 2 generates such a group. The elements of order 2 are $(0,2)$, $(1,0)$ and $(1,2)$. Thus the answer is 3.
   (b) This is equivalent to $[E : K] = 4$ and so we need subgroups of order 4. They are

$$\{0\} + \mathbb{Z}_4, \qquad \{(0,0),\,(1,1),\,(0,2),\,(1,3)\}, \qquad \{(0,0),\,(0,2),\,(1,0),\,(1,2)\},$$

   and so the answer is also 3.
   (c) The answer is zero since $[E : K]$ must divide $[E : \mathbb{Q}] = 8$.
   Alternatively the answer is zero since a group of order 8 cannot have a subgroup of order 3.

2. (a) Ideals are closed under multiplication by elements of R and by addition. Thus $a_i b_i \in B$ and the sum of such terms is also in B. Likewise, they are in A and hence in $A \cap B$.
   (b) One possibility is $A = B = n\mathbb{Z}$ where $n > 1$. Then $AB = n^2\mathbb{Z}$ and $A \cap B = A$.
   (c) All ideals of $\mathbb{Z}$ are principal. Hence we can write $A = k\mathbb{Z}$ and $B = n\mathbb{Z}$. Now AB consists of all multiples of kn and $A \cap B$ consists of all integers which are multiples of both k and n. Thus $AB = kn\mathbb{Z}$ and $A \cap B = \operatorname{lcm}(k,n)\mathbb{Z}$. Hence there is equality if and only if $kn = \operatorname{lcm}(k,n)$, which can be written as $\gcd(k,n) = 1$ if you prefer.

3. (a) **Closure**: For $A + B$ to be an ideal, it must be closed under subtraction and under multiplication by elements of R. Suppose $a + b \in A + B$, $a' + b' \in A + B$ and $r \in R$. Then

$$(a+b)-(a'+b') = (a-a')+(b-b') \in A+B \qquad \text{and} \qquad r(a+b) = ra+rb \in A+B$$

   and A and B are closed under subtraction and multiplication by R.
   Associative: $(A + B) + C = \{(a + b) + c \mid a \in A,\ b \in B,\ c \in C\} = \{a + (b + c) mid a \in A,\ b \in B,\ c \in C\} = A + (B + C)$.
   Identity: $\{0\} + A = \{0 + a \mid a \in A\} = \{a \mid a \in A\} = A$. Likewise $A + \{0\} = A$.
   (b) No. This can be seen in many ways. A simple one is to consider the two trivial ideals $\{0\}$ and R and note that since $\{0\} + R = R = R + R$ and so there is no cancelation.

4. An integral domain is a commutative ring with unity and no zero divisors. Every subring of a commutative ring without zero divisors will also be commutative and without zero divisors. Thus it suffices to deal with the unity issue.
   Sufficiency: If $1 \in R$, it is a unity for R and so R is an integral domain.

Necessity: Suppose R is an integral domain with unity u. Then $1u = u$ in D and $uu = u$ in R and hence D. Hence $1u = uu$ and, by cancelation in an integral domain, $1 = u$.

5. Let $F = \mathbb{Q}$ and $R = \mathbb{Z}$.

6. Call the splitting field F. Since $x^6 + x^2 + 1 \geq 1$ for all real x, it has no real zeros. Hence it has a complex zero. Hence F is larger than $\mathbb{R}$. Since $\mathbb{C}$ is algebraically closed, F is contained in $\mathbb{C}$. Since $[\mathbb{C} : \mathbb{R}] = 2$, there are no fields between $\mathbb{C}$ and $\mathbb{R}$. Thus $F = \mathbb{C}$.

7. (a) We must prove that $G \cap H$ is an additive group and that its nonzero elements are a multiplicative group. Suppose $a, b \in G \cap H$. Then $a, b \in G$ and $a, b \in H$. Hence $a - b \in G$ and $a - b \in H$ and so $a - b \in G \cap H$. Similarly, if $b \neq 0$, $ab^{-1} \in G \cap H$.

   (b) Suppose $|G| = p^n$ and $|H| = p^k$. Then $|G \cap H| = p^{\gcd(n,k)}$.
   Justification (which you need not give): Let $G = \mathrm{GF}(p^n)$ and $|H| = \mathrm{GF}(p^k)$. Since $\mathrm{GF}(p^t)$ is a subfield of both if and only if t divides both n and k, the largest possible t is $\gcd(n, k)$.

8. The linear factors of $x^{128} - x$ correspond to the elements of GF(2) of which there are 2. Hence there are two linear factors.
   The zeros of the polynomial are the elements of $\mathrm{GF}(2^7)$, which an extension of degree 7 of GF(2). If a is the zero of an irreducible factor, $[\mathrm{GF}(2)(a) : \mathrm{GF}(2)]$ equals the degree of the factor. Since 7 is prime, the only possible degrees are therefore 1 and 7. Hence all the factors of the 126-degree polynomial $\frac{x^{128}-x}{x(x-1)}$ are of degree 7.