2. The irreducible polynomials of degree 1, 2, and 4 over $\mathbb{F}_2$, are

$$X, X - 1, X^2 + X + 1, X^4 + X^3 + 1, X^4 + X^3 + X^2 + X + 1, \text{ and } X^4 + X + 1$$

One checks that their product equals $X^{16} - X$

3. If $d/n$, say $n = dn'$, then $x^n - 1 = x^{dn'} - 1 = (x^d - 1)((x^d)^{n'} - 1 + (x^d)^{n'-2} + \cdots + x^d + 1)$. Thus $x^d - 1$ divides $x^n - 1$. Conversely, keeping the notation of the hint given in the text, we see that $x^d - 1$ should divide $x^r - 1$, but this is not possible since $r < d$. Thus $r = 0$, i.e., $d/n$.

4. The proof of the first part follows from the above proof. For the second part if $d/n$, then $p^d - 1/p^n - 1$, and hence $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$. Conversely, let $a$ be a generator of $\mathbb{F}_p^\times$, then $a^{p^n - 1} = 1$ by hypothesis. Thus the order of $a$, which is $p^d - 1$, divides $p^n - 1$, and consequently $d/n$.

5. The polynomial $p(x) = x^p - x + a$ is clearly separable since its derivative is non-zero. It is also clear that if $\alpha$ is a root, then $\alpha + b$ is a root of the given polynomial for any $b \in \mathbb{F}_p$, and these are all the roots of $p(x)$. Note that $\alpha$ is not in $\mathbb{F}_p$. Suppose $f(x)$ is an irreducible factor of $p(x)$, then $f(x + 1)$ is also an irreducible factor of $p(x)$ since $p(x + 1) = p(x)$. Since degree of $f(x) > 1$, we see that $f(x + b) = f(x)$ for some non-zero $b \in \mathbb{F}_p$. This implies that $\alpha + b$ is a root of $f(x)$. We can repeat this to conclude that $\alpha + rb, 0 \leq r \leq p - 1$ are all distinct and roots of $f(x)$. Thus $f(x) = p(x)$.

6. We know that $\mathbb{F}_{p^n}$ is a splitting field for the polynomial $x^{p^n} - x$. This polynomial is separable and has $p^n$ distinct roots. Rest of the assertions are clear

7. Let $a \in K$ such that $a^p \notin K$. Let $p(x) = x^p - a \in K[x]$. Suppose $\beta$ is a root of $K$ in some algebraic closure of $K$. Then $\beta^p = a$, this implies that $p(x) = x^p - \beta^p = (x - \beta)^p$ over $K(\beta)$. Thus $\beta$ is the only root of $p(x)$ with multiplicity $p$. In particular $p(x)$ is inseparable. It remains to see that $p(x)$ is irreducible over $K$. Suppose $g(x) \in K[x]$ is an irreducible factor of $p(x)$ with degree $r < p$. Then, $g(x) = (x - \beta)^r = x^r - r\beta x^{r-1} + \cdots$; since $g(x)$ has coefficients in $K$, this implies that $r\beta \in K$. But, $r \neq 0$
since \( r < p \), therefore \( \beta \in K \) which is a contradiction. Whence \( g(x) = (x - \beta)^p = p(x) \) is irreducible. (Note that you can prove \#5 along similar lines which is a better proof than the one given above.)