Homework on Factorization of $x^n - 1$

1. Consider the polynomial $x^{15} - 1$ over $\mathbb{Z}_2$. What is the smallest extension $GF(2^r)$ of $\mathbb{Z}_2$ that contains a primitive 15-th root of 1 (hence all the roots of $x^{15} - 1$)?

2. Construct the field $GF(2^r)$ using a primitive polynomial of degree r over $\mathbb{Z}_2$. Use Magma to verify (or generate) that your polynomial is primitive. Call a root of that polynomial a.

3. Use Magma to find minimal polynomials of all non-zero elements of $GF(2^r)$ (express all the elements of $GF^*(2^r)$ as powers of a). Recall that if $f(\alpha) = 0$ for a polynomial f over $\mathbb{Z}_2$, then $f(\alpha^2) = 0, f(\alpha^4) = 0, ...$

4. Verify that the product of all minimal polynomials is equal to $x^{15} - 1$.

5. Compute cyclotomic cosets of 2 mod 15 and exhibit the correspondence between cyclotomic cosets and factors of $x^{15} - 1$.