Homework on Factorization of $x^n - 1$

Attach/include the Magma commands you used to/in your homework

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 the cyclotomic cosets of 2 mod 15 and 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 $f(\alpha^2) = 0, f(\alpha^4) = 0, \ldots.$ Exhibit the correspondence between cyclotomic cosets and factors of $x^{15} - 1$.

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

5. Show how to construct a binary BCH code of length 15 and designed distance 4. Give the (standard) generator polynomial of this code and find its dimension. Notice that you have several choices to construct such a code. Try to find the best option and explain how you made your choice. What is the actual minimum distance of your code? (Use Magma to find the actual minimum distance, but you must answer other questions based on cyclotomic cosets and other known facts about cyclic codes.)