Homework on Finite Fields, Factorization of $x^n - 1$ and BCH Codes

1. Consider the field $GF(9) = \mathbb{Z}_3(\alpha)$ where α is a root of $x^2 + 1$ over $\mathbb{Z}_3$. Construct an addition and multiplication table for $GF(9)$. Is α a primitive element of $GF(9)$? If not, find a primitive element of $GF(9)$.
2. Let $g(x) = x^2 + \alpha x + 2\alpha \in \mathbb{F}_9[x]$. Determine whether $g(x)$ is irreducible over $\mathbb{F}_9$. Justify your answer.
3. 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 $x^{15} - 1$)?
4. 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.
5. 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 $x^{15} - 1$.
6. Verify that the product of all minimal polynomials is equal to $x^{15} - 1$.
7. Show how to construct a binary BCH code C of length 15 and designed distance 5. Give a generator polynomial of this code and find its dimension. What is its actual minimum distance?
8. Use Magma's database to show that the BCH code that you constructed is optimal, i.e., there does not exist a binary linear code of length 15 with the same dimension as C that has a larger minimum distance.