資工系 **Error Control Coding** 期末考　**100. 1. 12(open book)**

Definition: A **Primitive Polynomial** *p(x)* over *GF(q)* is a prime polynomial over *GF(q)* with the property that in the extension field constructed modulo *p(x)*, the field element represented by ***x*** is a primitive element.

**Notice that: Primitive polynomials of every degree exist over every Galois Field.**

1. (25%) Find the generator polynomials and the minimum distance for the following codes：(primitive polynomial $x^4+x+1$, $x^5+x^2+1$ over GF(2))
   (a) RS(15,7) code
   (b) RS(31,21) code

2. (25%) Consider the Galois field $GF(2^3)$. The element $\beta = \alpha^3$ is a primitive element. Let $g_0(x)$ be the lowest-degree polynomial over GF(2) which has

   $$\beta, \beta^2$$

   as its roots. This polynomial can generate a one-error-correcting primitive BCH code of length 7.
   (a) Find the parity-check matrix [each element is belong to GF(2)] for this code by the method shown in pp. 13 of lecture note BCH_Code.
   (b) Determine g(x).
   (c) Find the parity-check matrix for this code by the method shown in pp. 10 of lecture note Cyclic_Code.
   (d) Compare the result with that obtained by (a).

3. (25%) Construct GF(9) from GF(3) using an appropriate primitive polynomial.

4. (25%) Find the generator polynomial g(x) for a double error correcting *ternary* BCH code of blocklength 8. What is the code rate of this code?