2.10 Show that X^5+X^3+1 is irreducible over GF(2).

proof. $p(X)=X^5+X^3+1$

$p(0)=1$

$p(1)=3\equiv 1$

$\Rightarrow 0, 1$ are not roots

$$X^2)\overline{X^5+X^3+1}\quad \frac{X^3+X}{X^5\;\;\;\;+X^3+1}\quad \frac{X^5}{X^3}\quad \frac{X^3}{1}$$

$$X+1)\overline{X^5+X^3+1}\quad \frac{X^4+X^3}{X^5\;\;\;\;+X^3+1}\quad \frac{X^5}{X^3}\quad \frac{X^3}{1}$$

$$X)\overline{X^5+X^3+1}\quad \frac{X^4+X^2}{X^5\;\;\;\;+X^3+1}\quad \frac{X^5}{X^3}\quad \frac{X^3}{1}$$

$$X+1)\overline{X^5+X^3+1}\quad \frac{X^4-X^3+2X^2-2X+2}{X^5+X^4}\quad \frac{X^5+X^4}{-X^4+X^3}\quad \frac{-X^4-X^3}{2X^3+1}\quad \frac{2X^3+2X^2}{-2X^2+1}\quad \frac{-2X^2-2X}{2X+1}\quad \frac{2X+2}{-1.}$$

$$X+X)\overline{X^3+X^3+1}\quad \frac{X^3-X^2+2X-2}{X^3+X^4}\quad \frac{X^3+X^4}{-X^4+X^3}\quad \frac{-X^4-X^3}{2X^3+1}\quad \frac{2X^3+2X^2}{-2X^2+1}\quad \frac{-2X^2-2X}{2X+1}$$

Suppose $p(X)=X^5+X^3+1=g(X)\cdot h(X)$
and degree[g(X)] $\leq$ degree[h(X)]
∵ We can not find a g(X)
with degree 1 and 2
∴ p(X) is irreducible over GF(2)

2.11 Let f(X) be a polinomial of degree n over GF(2). The reciprocal of f(X) is defined as

$$f^*(X)=X^n f\left(\frac{1}{X}\right)$$

a. Prove that $f^*(X)$ is irreducible over GF(2) if and only if f(X) is irreducible over GF(2)

proof: Suppose $f^*(X)$ is reducible and f(X) is irreducible

$f^*(X)=a(X)\cdot b(X)$

From $f^*(X)=X^n f(\frac{1}{X})$, we can obtain $f(X)=X^n f^*(\frac{1}{X})$

$=X^n[a(\frac{1}{X})\cdot b(\frac{1}{X})]$

So f(X) is reducible, which contradicts to our hypothesis.

∴ $f^*(X)$ is irreducible

Similarty, f(X) is irreducible

∴ $f^*(X)$ is irreducible iff f(X) is irreducible.

b. Prove that $f^*(X)$ is primitive if and only if f(X) is primitive.

proof: Suppose f(X) is primitive and $f^*(X)$ is not primitive, and degree=m

Which means $X^k+1=f^*(X)\cdot h(X)$ where $m<k<2^m-1$

From $f^*(X)=X^k f(\frac{1}{X})$, we can obtain $X^k+1=X^n f(\frac{1}{X})\cdot h(X)$

reciprocal ⇒ $X^{-k}+1=X^n f(X)\cdot h(\frac{1}{X})$

$X^k+1=X^{k-n}f(X)\cdot h(\frac{1}{X})$

So f(X) divides X^k+1 with k, which contradicts to our hypothesis

∴ $f^*(X)$ must be primitive

Similary, f(X) is primitive

∴ $f^*(X)$ is primitive iff f(X) is primitive.