Algebra And Coding
Work Sheet 02

Exercise 1. ***Eisenstein's criterion***. *Suppose we have the following polynomial with integer coefficients :* $Q(X) = \sum_{0\leqslant k\leqslant n} a_k X^k \in \mathbb{Z}[X]$. *If there exists a prime number p such that the following three conditions all apply :* p ***divides each*** a_k *for* $k < n$, p ***does not divide*** a_n, *and* p^2 ***does not divide*** a_0. *then* Q *is irreducible over the rational numbers (over* $\mathbb{Q}[X]$.*)*

1. Determine the irreducible polynomials of degree $\leqslant 4$ in $\mathbb{F}_2[X]$.
2. Proof that $X^5 + 21X^2 - 63$ is irreducible in $\mathbb{Z}[X]$.
3. Write $X^n - 1$ as a product of irreducible polynomials in $\mathbb{Z}[X]$ and in $\mathbb{Q}[X]$ for $n = 3, 7$.

Exercise 2. Let K be a finite field of q elements, and g is a generator of K^*. Describe how to determine that an element $a \in K^*$ is a square or not in K. If yes, show how to calculate a square root of a while $q = 3[4]$.

Exercise 3. Determine which polynomials are irreducible or not in $\mathbb{Z}[X]$, in $\mathbb{Q}[X]$, and in $\mathbb{F}_p[X]$.

$$X^4 - 2x^2 + 4, \qquad X^4 + 1, \qquad X^4 + 4x^2 + 4.$$

Indication : *Let* g *be a generator of G. Set* $a = g^n, b = g^m$, $ab = g^{n+m}$. *One of 3 numbers* $n, m, m+n$ *must be even and the corresponding power of* g *is a square number.*

Exercise 4. Using $f(x) = x^2 + x - 1$ and $g(x) = x^3 - x + 1$, construct finite fields containing 4, 8, 9, 27 elements. Write down multiplication tables for the fields with 4 and 9 elements and verify that the multiplicative groups of these fields are cyclic.

Exercise 5. Let$f(X) = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in \mathbb{Z}[X]$. Suppose that $f(0)$ and $f(1)$ are odd integers. Show that $f(X)$ has no integer roots.

Exercise 6. Let $\mathbb{F}_q$ be a finite field. Evaluate the sum and product of the non-zero elements of $\mathbb{F}_q$.