UNIVERSITY OF ST ANDREWS
MT5826 Finite Fields
Tutorial Sheet: Chapter 4

1. Fill in the details of the proof of Theorem 8.2(i) to show that $E^{(n)}$ is cyclic.

2. In the following, assume we are working in a field over which the cyclotomic polynomial Q_n is defined.
Find $Q_n(x)$, in its simplest form, for

(i) $n = 8$;

(ii) $n = 20$.

3. Express $\mathbb{F}_8$ using

- root adjunction;
- the fact that it is the 7th cyclotomic field over $\mathbb{F}_2$.

Draw up a table showing how the two representations correspond.

4. In this question, you are given the following theorem:
As in Theorem 7.16, let $I(q, n; x)$ be the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree n. Then for $n > 1$ we have

$$I(q, n; x) = \prod_m Q_m(x),$$

where the product is extended over all positive divisors m of $q^n - 1$ for which n is the multiplicative order of q modulo m, and where $Q_m(x)$ is the mth cyclotomic polynomial over $\mathbb{F}_q$.

(i) Using the given theorem (or otherwise), calculate $I(3, 2; x)$.

(ii) Use part (i) to determine all three monic irreducible polynomials in $\mathbb{F}_3[x]$ of degree 2. (Hint: Theorems 8.8 and 8.12 of the notes will help you here).