Course content for MT5485, Applications of Field Theory

Prerequisites:
An undergraduate course covering the elementary theory of groups, rings and fields.

Aims:
To introduce some of the basic theory of field extensions, with special emphasis on applications in the context of finite fields.

Learning outcomes:
1. understand simple field extensions of finite degree;
2. classify finite fields and determine the number of irreducible polynomials over a finite field;
3. state the fundamental theorem of Galois theory;
4. compute in a finite field;
5. understand some of the applications of fields.
6. Demonstrate independent learning skills

Course content:
Extension theory: Polynomial factorisation. Field extensions. Simple extensions. The degree of an extension. Applications to ruler and compass constructions.
Classifying finite fields: The number of irreducible polynomials. Existence and uniqueness
of finite fields of a given size. Concrete representations of a finite field.
The structure of finite fields: Roots of irreducible polynomials and the Frobenius automorphism. Cyclotomic polynomials. The Galois correspondence for finite fields. An
indication of Galois correspondence for general fields. The norm and trace of an element.
Applications to m-sequences. Dual and self-dual bases. Normal bases and the normal basis theorem. Applications to multiplication in finite fields.
Discrete logarithms: The discrete log problem and its applications. The Pohlig-Hellman and baby step, giant step algorithms.