# Course content for MT3850/MT4850, Applications of Field Theory

**Prerequisites:**
MT2800 and MT2830

**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. MT4850: Demonstrate a breadth of understanding appropriate for an M-level course.

**Course content:**
**Extension theory**: Polynomial factorisation. Field extensions. Simple extensions. The degree of an extension. Applications to ruler and compass constructions.
**Classifying finite fields**: Existence and uniqueness of finite fields of a given size. Concrete representations of a finite field. Finite field multiplication using logarithm tables. The number of irreducible polynomials.
**The structure and applications of (finite) fields**: The Frobenius automorphism. Cyclotomic polynomials and cyclotomic fields. The Galois correspondence for finite fields. An indication of the Galois correspondence for general fields, e.g. cyclotomic fields. The normal basis theorem and applications to multiplication in finite fields. Further topics, such as: algorithms for factoring polynomials over finite fields, for example the Cantor-Zassenhaus algorithm; the norm and trace of an element; applications to m-sequences; dual and self-dual bases.