# COURSE SPECIFICATION FORM

| **DEPARTMENT OF: Mathematics** | | | | **Academic Session: 2017-18** | |
|---|---|---|---|---|---|
| **Course Code:** | MT4850 | **Course Value:** | 0.5 | **Status:**<br>*(ie:Core, or Optional)* | Optional |
| **Course Title:** | Applications of Field Theory | | | **Availability:**<br>*(state which teaching terms)* | Term 2 |
| **Prerequisites:** | MT2800 and MT2830 | | | **Recommended:** | |
| **Co-ordinator:** | Prof S R Blackburn | | | | |
| **Aims:** | To introduce some of the basic theory of field extensions, with emphasis on applications in the context of finite fields. | | | | |
| **Learning Outcomes:** | On completion of the course, students should be able to:<br>• understand simple field extensions of finite degree;<br>• classify finite fields and determine the number of irreducible polynomials over a finite field;<br>• state and apply the fundamental theorem of Galois theory;<br>• compute in a finite field;<br>• understand some of the applications of fields.<br>• 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.<br>**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.<br>**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. | | | | |
| **Teaching & Learning Methods:** | 33 hours of lectures and examples classes.<br>117 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes. | | | | |
| **Key Bibliography:** | Introduction to Finite Fields and their Applications – R. Lidl and H. Niederreiter (Cambridge UP 1994); *Library reference 512.4 LID*.<br>Galois Theory – I. Stewart (Chapman and Hall 2003); *Library reference 512.4 STE.* | | | | |
| **Formative Assessment & Feedback:** | Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts. | | | | |
| **Summative Assessment:** | **Exam** (100%) A two-hour paper. | | | | |

Updated September 2017