Contents

1. Introduction 1

2. Decomposition Laws 5
2.1 Foundations of Prime Ideal Decomposition 5
2.2 Decomposition in Abelian Extensions 11
2.3 Density Statements 22

3. Elliptic Curves 25
3.1 Defining Equations 25
3.2 Addition on Elliptic Curves 26
3.3 Division Polynomials 28
3.4 Torsion Points 30
3.5 ℓ-adic Representations 32
3.6 Reduction Modulo $\mathfrak{p}$ and L-Series 35

4. Elliptic Modular Curves 41
4.1 Modular Curves 41
4.2 Modular Forms 45
4.3 Hecke Operators 48
4.4 The Eichler-Shimura Formula 54

5. Torsion Point Fields 59
5.1 The Groups GL(2,n) 59
5.2 Subfields of $k(E_n)$ 66
5.3 Defining Polynomials of Subfields of $k(E_n)$ 73
5.4 Decomposition in 2- and 3-Torsion Point Fields 76
5.5 Decomposition in 4-Torsion Point Fields 80
5.6 Decomposition in p^m-Torsion Point Fields 85

6. Invariants and Resolvent Polynomials 87
6.1 Foundations of Galois Theory 87
6.2 Procedure for the Description of Subfields 90
6.3 Invariant Algebras 91
6.4 Application to 4-Torsion Point Fields 100

Appendices 107

A. Invariants of Elliptic Modular Curves 109

B. L-series Coefficients a_p 111

C. Fully Decomposed Prime Numbers 119

D. Resolvent Polynomials 127

E. Free Resolution of the Invariant Algebra 131

References 134

Symbols 137

Index 141