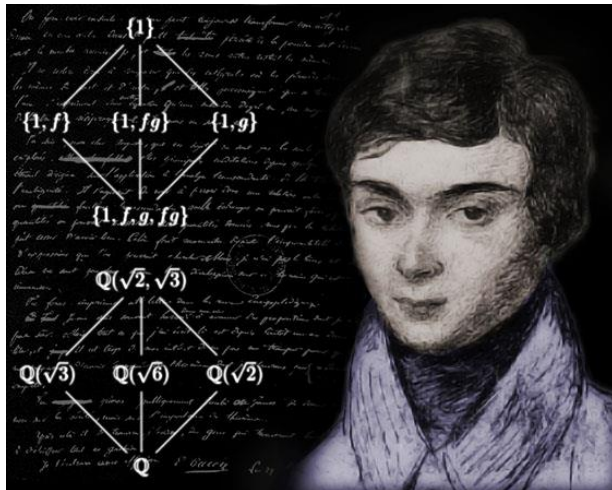


# GALOIS THEORY



by **Dr C.D.H. Cooper**  
Macquarie University

**13<sup>th</sup> Edition September 2022**

These notes were prepared for students at Macquarie University in Australia but are freely available to anyone. However if you make use of them and are not a Macquarie University student it would be nice if you could email me at [christopherdonaldcooper@gmail.com](mailto:christopherdonaldcooper@gmail.com) to let me know where you are from. And, if you are from outside of Australia perhaps you could send me a postcard of where you are from to pin up on my wall (Christopher Cooper, 31 Epping Avenue, EASTWOOD, NSW 2122, Australia).

# PREFACE

Two of the most beautiful and intellectually satisfying topics in mathematics are Galois Theory and Group Representation Theory. Interestingly both owe their existence to the French mathematician Évariste Galois (1811-1832).

And just as a first taste of Representation Theory should concentrate on representations over the complex field so one's first experience of Galois Theory should concentrate on number fields, that is, subfields of the complex numbers. Trying to be too general on a first encounter introduces unnecessary complications and detracts from the core ideas. At least that is the philosophy we have adopted here. The fact that  $\mathbb{C}$  is algebraically closed and has characteristic zero shows Galois Theory at its most elegant. So we do not get bogged down with separability and normal extensions. Instead of normal extensions we use polynomial extensions – the same thing over  $\mathbb{C}$ .

There are many excellent books on Galois Theory. One of the best is *Galois Theory* by Ian Stewart and my notes owe a lot to his treatment of the subject. What makes these notes different to other accounts, other than the focus on number fields, is the large number of examples given. One doesn't really understand a theory unless one has immersed oneself in many specific examples.

Another novelty in these notes is the emphasis on tests of primeness of polynomials, a property that is important in Galois Theory. The material on the too-many-primes test is published here for the first time. It establishes the fact that if an integer polynomial  $f(x)$  takes prime or  $\pm 1$  values for more than a certain number of integer values of  $x$  then  $f(x)$  is prime over  $\mathbb{Q}$ .

Galois Theory texts often comment on the fact that in general the quintic is not soluble by radicals with an assurance that “of course these days, with the help of computers, we can solve any polynomial equation to any desired degree of accuracy by suitable numerical methods”. This of course is true, but one needs to go beyond Newton’s Method if one wants to find non-real zeros of a real polynomial. In these notes we do this and show a simple method for finding the non-real zeros of a quintic once the real zeros have been found.

Several of the theorems have the tag ‘(COOPER)’ added. This is not to show off but rather to indicate that you probably won’t find them in other sources. If you do, I would be interested to hear.

# CONTENTS

## CHAPTER 1: OVERVIEW

1.1 Galois and Third Generation Mathematics ...	11
1.2 What Galois Did .....	15
1.3 A Baby Example of Galois Theory .....	17

## CHAPTER 2: BACKGROUND

2.1 Sets and Functions .....	21
2.2 Complex Numbers .....	22
2.3 Coordinate Geometry .....	23
2.4 Polynomials .....	24
2.5 Calculus .....	25
2.6 Groups .....	28
2.7 Permutations .....	29
2.8 Fields and Rings .....	30
2.9 Vector Spaces .....	32
2.10 Numbers of Real Zeros .....	38
Exercises for Chapter 2 .....	41
Solutions for Chapter 2 .....	46

## CHAPTER 3: PRIME POLYNOMIALS

3.1 Tests for Primeness .....	51
3.2 Prime Polynomials over $\mathbb{Z}_p$ .....	54
3.3 Integer Polynomials .....	57
3.4 Tests for Primeness over $\mathbb{Q}$ .....	60
3.5 Conjugate Polynomials .....	63
3.6 Minimum Polynomials .....	66
Exercises for Chapter 3 .....	74
Solutions for Chapter 3 .....	76

**CHAPTER 4: THE TOO MANY PRIMES TEST**

4.1 Prime or Unit Values of a Polynomial ..... 87  
4.2 Unit Values of Integer Polynomials ..... 89  
4.3 Prime or Unit Values of an Integer Cubic ... 92  
Exercises for Chapter 4 ..... 96  
Solutions for Chapter 4 ..... 97

**CHAPTER 5: FIELD EXTENSIONS**

5.1 Field Extensions as Vector Spaces ..... 101  
5.2 The Degree of a Simple Extension ..... 106  
5.3 Dimensions of Field Extensions ..... 107  
Exercises for Chapter 5 ..... 111  
Solutions for Chapter 5 ..... 113

**CHAPTER 6: RULER AND COMPASS  
CONSTRUCTIBILITY**

6.1 Ruler and Compass Constructions ..... 119  
6.2 Examples of Ruler and Compass ..... 123  
6.3 Constructible Numbers ..... 126  
Exercise for Chapter 6 ..... 132  
Solutions for Chapter 6 ..... 133

**CHAPTER 7: SOLVING POLYNOMIAL  
EQUATIONS**

7.1 Early Solutions to Polynomial Equations ..... 139  
7.2 The Quadratic Equation From An  
Advanced Standpoint ..... 140  
7.3 The Cubic Equation ..... 143  
7.4 Quartic Equations ..... 153

7.5 Solving Quintics .....	156
Exercises for Chapter 7 .....	159
Solutions for Chapter 7 .....	160

## CHAPTER 8: GALOIS GROUPS

8.1 Galois Groups of Field Extensions .....	163
8.2 The Heart of Galois Theory .....	168
8.3 Galois Groups of Radical Extensions .....	176
8.4 The Order of a Galois Group .....	181
8.5 The Galois Correspondance .....	182
8.6 Orders and Degrees .....	185
Exercises for Chapter 8 .....	188
Solutions for Chapter 8 .....	189

## 8

## CHAPTER 9: EXAMPLES OF GALOIS GROUPS

9.1 The Fundamental Theorem of Galois Theory .....	191
9.2 $f(x) = x^4 - x^2 - 2$ .....	194
9.3 $f(x) = x^3 - 2$ .....	198
9.4 $f(x) = x^4 - 2$ .....	201
9.5 $f(x) = x^{20} - 1$ .....	207
9.6 $f(x) = x^{16} - 1$ .....	210
9.7 $f(x) = x^4 - 4x^2 + 10$ .....	212
9.8 $f(x) = x^4 - 5x^2 + 5$ .....	215
9.9 $f(x) = x^3 - 3x + 1$ .....	217
9.10 A Mystery Polynomial .....	218
9.11 $f(x) = x^6 - 6x^3 + 6$ .....	220
9.12 $f(x) = x^6 + 6x^4 + 12x^2 + 6$ .....	224
9.13 $f(x) = x^8 - 5x^4 - 7x^3 + 35$ .....	228

9.14 $f(x) = x^{30} - 30x^{15} + 216$ .....	234
Exercises for Chapter 9 .....	231
Solutions for Chapter 9 .....	233

## **CHAPTER 10: SOLUBILITY BY RADICALS**

10.1 A Short History of Solubility of Polynomials .....	259
10.2 Solubility by Radicals .....	262
10.3 Soluble Groups .....	265
10.4 Soluble Polynomials and Soluble Groups .....	266
10.5 Insoluble Quintics .....	269
Exercises for Chapter 10 .....	271
Solutions for Chapter 10 .....	272

## **CHAPTER 11: FINITE FIELDS**

11.1 A Field With 4 Elements .....	277
11.2 Fields as Quotient Rings .....	279
11.3 The Characteristic of a Field .....	281
11.4 The Multiplicative Group of a Finite Field .....	289
11.5 The Number of Monic Prime Polynomials Over $\mathbb{Z}_p$ .....	293
11.6 Galois Groups of Finite Fields .....	295
Exercises for Chapter 11 .....	297
Solutions for Chapter 11 .....	299

**CHAPTER 12: THE FUNDAMENTAL THEOREM  
OF ALGEBRA**

12.1 Extensions of  $\mathbb{R}$  and  $\mathbb{C}$  ..... 307  
12.2 The Fundamental Theorem of Algebra ..... 308

**APPENDICES**

**APPENDIX A:** The Life of Galois ..... 311  
**APPENDIX B:** Overview of Galois Theory ... 317  
**APPENDIX C:** Cubic Equation Worksheet ... 323  
**APPENDIX D:** Galois Theory Project ..... 325

