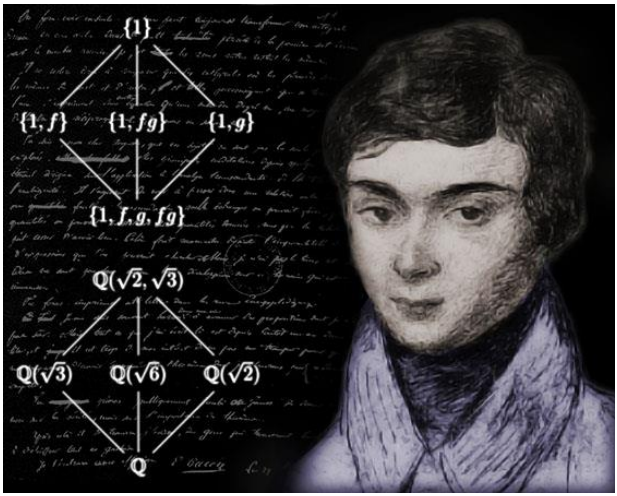
# GALOIS THEORY





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


## 13th 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 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



## CHAPTER 2: BACKGROUND



## CHAPTER 3: PRIME POLYNOMIALS

## CHAPTER 4: THE TOO MANY PRIMES TEST



## CHAPTER 5: FIELD EXTENSIONS



## CHAPTER 6: RULER AND COMPASS CONSTRUCTIBILITY



## CHAPTER 7: SOLVING POLYNOMIAL EQUATIONS

## CHAPTER 8: GALOIS GROUPS





## CHAPTER 9: EXAMPLES OF GALOIS GROUPS

## CHAPTER 10: SOLUBILITY BY RADICALS



## CHAPTER 11: FINITE FIELDS

# APPENDICES