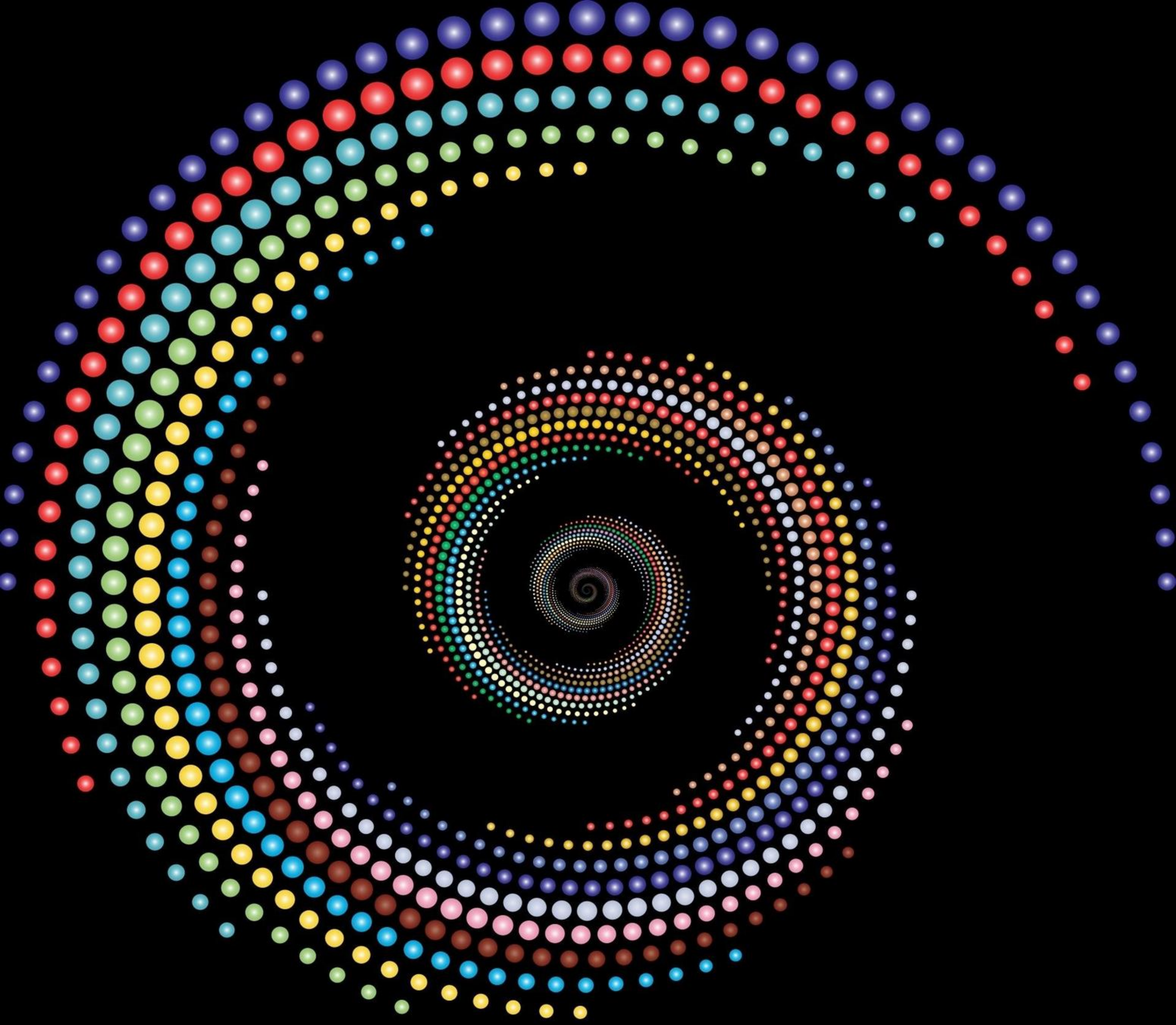

Galois Groups and Field Extensions for Solvable Quintics

Achim Plum

GALOIS GROUPS AND FIELD EXTENSIONS FOR SOLVABLE QUINTICS

GALOIS GROUPS AND FIELD EXTENSIONS FOR SOLVABLE QUINTICS

ABSTRACT

In the context of self-studies on polynomials of degree 5 (quintics), Galois groups and field extensions related to solvable quintics - irreducible and reducible ones - have been analyzed. Effort has been spent to provide comprehensive explanations and some examples of those structures; the intention is to give the reader an overview and a decent insight into the topic, which may help to understand the algebraic structures and their arithmetics better.

Quite some reference materials of relevant or related topics are listed at the end of the e-book, primarily referring to Wikipedia articles. This ebook was written according to the best knowledge of the author. To foster further learning and exchange on the topic and the mathematical content, the author is interested in feedback for improvements or extensions and can be contacted at the email address math@iquadrat-1.online.

1 INTRODUCTION

This e-book focuses on solvable irreducible and reducible quintics - polynomials of degree 5 - and how Galois groups can be determined. Galois theory laid the foundation for understanding whether polynomials can be solved by radicals or not: if the Galois group is solvable, the polynomial is as well. Nevertheless, the determination of Galois groups and corresponding field extensions is not always easy.

The following second chapter provides a compact overview of the theory of Galois groups and field extensions. See [2,3,4] for some background on group theory and finite groups, and [1] for an overview of Galois theory. It is key to understand the concept of field automorphisms and the role the field $\mathbb{Q}$ plays in this context; actually, the base field normally chosen is $\mathbb{Q}$, which implies that all irrational zeroes generate field extensions of $\mathbb{Q}$, and many polynomials are irreducible over $\mathbb{Q}$ [10]. The concepts are explained in general as well as with some examples.

When analyzing a polynomial, the splitting field [14] is of highest interest. It is constructed by a chain of field extensions created by irreducible factors of the polynomial over a given base field F. Conceptually, there is an isomorphism between the quotient ring of the commmutative ring of polynomials over the maximal ideal [8] generated by an irreducible polynomial to the field created by adjoining a zero of that polynomial (i.e. adding with closure under addition and multiplication [12]). The convention to write this down for an irreducible polynomial f(x) over a field F is F[x]/(f(x)), with F[x] being the ring of polynomials with coefficients in F and (f(x)) denoting the ideal generated by f(x). Such a quotient ring is a field that is isomorphic to F(n), with n being a zero of f(x), which is the field generated by