

Generic Polynomials

Book review by Zinovy Reichstein, University of British Columbia

Generic polynomials

Constructive aspects of Galois Theory

by Christian U. Jensen, Arne Ledet and Noriko Yui

Around 1830 Galois described a procedure for assigning a finite group G to a polynomial

$$p(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,$$

where a_1, \dots, a_n are rational numbers. This group (which is now called the Galois group of $p(x)$) “measures” the difficulty in finding the roots of this polynomial; in particular, it tells us whether or not $p(x)$ can be solved in radicals. Galois’ contemporaries did not understand the importance of his ideas. His most significant papers were rejected for publication, then lost by the French Academy of Sciences, and Galois himself was killed in a duel before reaching the age of 21.

Galois’ construction naturally leads to the following question: Can every finite group be realized as the Galois group of some polynomial with rational coefficients? While there is no direct evidence that Galois himself ever posed this question, we are free to speculate that he might well have done it in one of his lost papers. In any case, this question, under the name of Inverse Galois Problem, has become one of the most famous unsolved problems in mathematics and the focus of much research over the past 150 years. The interest in this problem has been on the rise in the past two decades, as witnessed by the publication of a number of books and conference proceedings, such as *Galois groups over \mathbb{Q}* , edited by Y. Ihara, K. Ribet and J.-P. Serre (1987); *Topics in Galois Theory*, by J.-P. Serre (1992); *Recent Developments in the Inverse Galois Problem*, edited by M. D. Fried (1993); *Groups as Galois groups, an Introduction*, by H. Völklein (1996); and *Inverse Galois Theory*, by G. Malle and B. H. Matzat (1999).

Much of the research on the inverse Galois problem has been influenced by two ideas. One, due to Hilbert, is to consider polynomials over $\mathbb{Q}(t)$; the Hilbert Irreducibility Theorem says that if a given group can be realized over $\mathbb{Q}(t)$ then it can be realized over \mathbb{Q} . This gives a geometric flavor to the subject by bringing into play the rich geometry of the affine line and its coverings. Every finite group is known to be realizable over $\mathbb{C}(t)$ (by the Riemann Existence Theorem) or $\mathbb{Q}_p(t)$ (by the Harbater Existence Theorem, 1987), and it is hoped that the same should be true over $\mathbb{Q}(t)$.

The second idea, due to Emmy Noether, is to look for a polynomial $p(x) \in \mathbb{Q}[x]$ with a given Galois group G by initially assuming that the roots x_1, \dots, x_n are independent variables, permuted by G . These roots satisfy the polynomial $P(x) = (x - x_1) \cdots (x - x_n)$ whose coefficients lie in the field $\mathbb{Q}(x_1, \dots, x_n)^G$ of G -invariant rational functions in x_1, \dots, x_n . If this field happens to be a purely transcendental extension of \mathbb{Q} , then after

specializing the coefficients of $P(x)$ to suitable rational numbers, we obtain a desired polynomial $p(x) \in \mathbb{Q}[t]$ with Galois group G .

The book under review focuses on two byproducts of Noether's idea: generic polynomials and the Noether problem. (The Noether problem asks whether or not $\mathbb{Q}(x_1, \dots, x_n)^G$ is a purely transcendental extension of \mathbb{Q} . A polynomial $P(x) \in \mathbb{Q}(s_1, \dots, s_d)[x]$ with Galois group G is called versal if every G -Galois extension L/K of characteristic zero can be obtained by suitably specializing s_1, \dots, s_d in K . If s_1, \dots, s_d can also be chosen to be algebraically independent then $P(x)$ is called generic. In particular, Noether's construction always produces a versal polynomial $P(x)$, and if the Noether problem has a positive solution for G , then this polynomial is also generic.) The authors give a concrete and accessible introduction to this area of research. The writing is very clear, and the technical prerequisites are kept to a minimum; in fact, the first three chapters may even be suitable for a topics course in algebra at the first year graduate level. The only real prerequisite is a solid course in Galois Theory; the reader is not expected to know cohomology theory or algebraic geometry. In spite of these modest technical requirements, the book takes the reader to the frontiers of research in this area of Inverse Galois Theory. Much of it is an exposition of previously published results, but the reader will also find some original material, as well as numerous insights and improvements by the authors, often in the form of remarks or exercises.

At the heart of the book is the theory of generic field extensions and generic polynomials originated by Saltman. The authors should be commended for bringing this beautiful subject to a wide mathematical audience. Most of the necessary prerequisites (the Hilbert Irreducibility theorem, an introduction to the Galois theory of commutative rings, etc.) are included in the book. The authors take a very concrete and constructive approach to the subject; one of the distinctive features of this book is a great number of explicit examples of generic polynomials for small and medium size groups. Of course, one cannot hope to obtain similarly explicit formulas for much larger groups. On the other hand, the numerous generic polynomials collected by the authors will undoubtedly be of help to anyone doing Galois-theoretic computations, especially in an arithmetic setting, where roots of unity are not available.

In the last chapter the authors discuss the notions of essential and generic dimension of a group G . The generic dimension is the minimal number d of independent parameters s_1, \dots, s_d , as $P(x) \in \mathbb{Q}(s_1, \dots, s_d)[x]$ ranges over all generic polynomials; the essential dimension is defined in a similar way by allowing $P(x)$ to range over all versal polynomials (and only counting the number of independent parameters among s_1, \dots, s_d). The study of generic and essential dimension over \mathbb{Q} is still in its infancy; in particular, it is not even known whether or not they are really different (assuming the generic dimension is finite). Also, even for cyclic groups, there are no known lower bounds on the essential dimension over \mathbb{Q} , beyond $\text{ed}_{\mathbb{Q}}(\mathbb{Z}/n\mathbb{Z}) \geq 2$ for

most n . The authors put together an excellent survey of known results and several interesting conjectures; I even learned something new by reading their account of my own work in Chapter 8. It is my hope that this book will stimulate further progress in this new and exciting area of research, at the crossroads of algebra, number theory and geometry.

I have not noticed many mistakes or misstatements in the book. One, brought to my attention by J.-P. Serre and N. Yui, is the assertion that $\mathrm{PGL}_2(\mathbb{Q})$ does not contain an element of order 4 on p. 189, which is easily seen to be false. The conclusion the authors draw, to the effect that the groups C_4 , D_4 , A_4 , S_4 , C_5 , D_5 , F_{20} , A_4 , A_5 , and S_5 have generic dimension ≥ 2 over \mathbb{Q} is correct, but in the case of C_4 , D_4 , A_4 , and S_4 , a different argument is required. I was also puzzled by the note on p. 188, where the authors say that first examples of unirational but non-rational varieties over \mathbb{Q} were constructed in a 1985 paper of Beauville, Colliot-Thélène, Sancuc and Swinnerton-Dyer. (Earlier examples were constructed by Segre [1951], Chevalley [1954], Swan [1969], Voskresenskii [1970] and Manin-Iskovskih [1971].) Personally I would also have liked to see more geometric motivation for the explicit formulas in the book, and a greater emphasis on the Multiplicative Noether Problem (which only makes a brief appearance in the last chapter), as opposed to the General Noether Problem.

These minor quibbles aside, Jensen, Ledet, and Yui have written a user-friendly book that has a lot to offer, both to a beginner and an experienced researcher. I highly recommend this book to anyone who is interested in Galois Theory.