FIELDS AND ALGEBRAIC EQUATIONS

Tadao ODA
Tohoku University, Japan

Keywords: algebraic equation, field, finite field, cyclotomic, Galois theory, solvability, ruler and compass construction

Contents

Summary

Fields are rings that allow division by nonzero elements. Algebraic equations in one variable over fields turn out to be controlled by finite groups called Galois groups. This beautiful interplay between fields and groups, known as Galois Theory, gives rise to interesting applications to the solvability of algebraic equations in terms of radicals as well as the ruler and compass constructions on the plane.

Fields will play important roles in number theory and algebraic geometry as well. Results on matrices and linear algebra in *Matrices, Vectors, Determinants, and Linear Algebra*, on groups in *Groups and Applications* and on rings and modules in *Rings and Modules* will be freely used.

1. Basic Properties and Examples of Fields

The convention in *Rings and Modules* will be followed. Namely, a *field* is a commutative and associative ring with the unity $1 \neq 0$ such that any nonzero element is invertible. Consequently, nonzero elements of a field form a group under multiplication.

Here are some of the fields that appeared so far:

- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- The field of fractions of an integral domain. For instance, $K(t)$, $K((t))$,

$K(t_1,t_2,\ldots,t_n)$, $K((t_1,t_2,\ldots,t_n))$ over a field K, and $\mathbb{Q}_p$.

- The residue ring $R/\mathfrak{m}$ of a ring R with respect to a maximal ideal $\mathfrak{m} \subset R$. For instance, $\mathbb{Z}/p\mathbb{Z}$ for a prime number p, and $K[x]/\pi(x)K[x]$ for an irreducible polynomial $\pi(x)$ in the polynomial ring $K[x]$ in one variable x over a field K.

Here is the most basic property that divides fields into two entirely different families: For a field K, a ring homomorphism

$$\chi : \mathbb{Z} \to K, \quad \text{with} \quad \chi(m) := \begin{cases} 1+1+\cdots+1 \ (m \text{ times}) & \text{if } 0 < m \in \mathbb{Z} \\ 0 & \text{if } m = 0 \\ (-1)+(-1)+\cdots+(-1) \ (-m \text{ times}) & \text{if } 0 > m \in \mathbb{Z} \end{cases}$$

is well-defined. Since the image $\chi(\mathbb{Z}) \subset K$ is an integral domain, $\ker(\chi)$ is a prime ideal of $\mathbb{Z}$. Two possibilities arise:

(characteristic 0) $\ker(\chi) = \{0\}$. In this case, K is said to be of *characteristic zero*. The injective homomorphism $\chi : \mathbb{Z} \to K$ can be extended uniquely to an injective homomorphism $\chi : \mathbb{Q} \to K$. One identifies $\mathbb{Q}$ with its image by χ so that $\mathbb{Q} \subset K$. In this way, $\mathbb{Q}$ is called the *prime field of characteristic* 0.

(characteristic p) $\ker(\chi) = p\mathbb{Z}$ for a prime number p. In this case, K is said to be of *characteristic* p. The homomorphism theorem gives rise to an isomorphism $\mathbb{Z}/p\mathbb{Z} \cong \chi(\mathbb{Z})$. The finite field $\mathbb{Z}/p\mathbb{Z}$ with p elements is often denoted by

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \bar{j}, \ldots, \overline{p-1}\}.$$

$\mathbb{F}_p$ is identified with its isomorphic image $\chi(\mathbb{Z})$ so that $\mathbb{F}_p \subset K$ and $p = 0$ in K. This $\mathbb{F}_p$ is called the *prime field of characteristic* p.

This equality $p = 0$ in a field K of characteristic p leads to a striking consequence on the binomial coefficients

$$\binom{p}{r} = \frac{p(p-1)(p-2)\cdots(p-r+1)}{r!} = 0, \qquad \text{for} \quad 0 < r < p.$$

Consequently, the binomial expansion in K becomes

$$(x+y)^p = x^p + y^p.$$

Since $(xy)^p = x^p y^p$ as well, the p-th power map

$$F : K \to K, \qquad \text{with} \quad F(x) := x^p \quad \text{for} \quad x \in K$$

is a ring homomorphism. This F is called the *Frobenius* homomorphism. One has *Fermat's little theorem*

$$x^p = x, \qquad \text{for any} \quad x \in \mathbb{F}_p.$$

Indeed, since $\mathbb{F}_p \setminus \{0\}$ is a group under multiplication with order equal to $p-1$, Cauchy's theorem implies $\xi^{p-1} = 1$ for any $0 \neq \xi \in \mathbb{F}_p$. The multiplication by ξ on both sides gives $\xi^p = \xi$, which is valid for $\xi = 0$ as well. Consequently, $0, 1, \ldots, p-1 \in \mathbb{F}_p$ are the roots of the equation $x^p - x = 0$, and hence one has a factorization

$$x^p - x = x(x-1)(x-2)\cdots(x-j)\cdots(x-p+1)$$

as polynomials in $\mathbb{F}_p[x]$. This factorization continues to hold for any field K of characteristic p, since K contains $\mathbb{F}_p$.

In connection with algebraic equations, one is mainly concerned with the relationship between fields K and L with $K \subset L$. In this situation, K is called a *subfield* of L, while L is called an *extension* of K. In such a situation, L can be regarded as a K-*vector space*. The *degree* of the extension L of K is then defined to be

$$[L : K] := \dim_K L,$$

the dimension of L as a K-vector space. It is n if L has a finite K-basis $\{e_1, e_2, \ldots, e_n\}$, but could be ∞ otherwise. L is said to be a *finite extension* if $[L : K]$ is finite.

If a "tower" of extensions $E \supset L \supset K$ is given, then the equality

$$[E : K] = [E : L][L : K].$$

holds. Indeed, without loss of generality these extensions may be assumed to be finite. Let $\{v_1, v_2, \ldots, v_m\}$ be a basis of the L-vector space E, and $\{u_1, u_2, \ldots, u_n\}$ a basis of the K-vector space L. Then

$$\begin{aligned} E &= Lv_1 + Lv_2 + \cdots + Lv_m \\ &= (Ku_1 + Ku_2 + \cdots + Ku_n)v_1 + (Ku_1 + Ku_2 + \cdots + Ku_n)v_2 + \cdots \\ &\quad \cdots + (Ku_1 + Ku_2 + \cdots + Ku_n)v_m \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} Ku_i v_j. \end{aligned}$$

The $u_i v_j$'s can be shown to form a basis of E as a K-vector space.

One may wonder why or how field extensions have anything to do with algebraic equations. The relevance of field extensions to algebraic equations is now explained.

-
-
-

Bibliography

Artin, E. (1998). Galois Theory,Edited and with a Supplemental Chapter by Arthur N. Milgram. Reprint of the 1944 Second Edition, iv+82 pp., Dover Publications, Inc., Mineola, NY, ISBN 0-486-62342-4 [A masterfully presented classic textbook originally published from University of Notre Dame Press.]

Artin, M. (1991). Algebra, xviii+618 pp. Prentice Hall, Inc., Englewood Cliffs, NJ, ISBN 0-13-004763-5 [This is one of the advanced comprehensive textbooks on algebra suitable for further study.]

Gaal, L. (1998). Classical Galois Theory. With Examples,Reprint of the Third Edition, viii+248 pp.AMS Chelsea Publishing, Providence, RI, ISBN 0-8218-1375-7.[A standard textbook for beginning graduate students with some background in abstract algebra.]

Rotman, J. (1998). Galois Theory, Second Edition, xiv+157 pp.Universitext. Springer-Verlag, New York, ISBN 0-387-98541-7 [A standard textbook.]

Stewart, I. (1989). Galois Theory, Second Edition, xxx+202 pp.,Chapman and Hall, Ltd., London, ISBN 0-412-34540-4; 0-412-34550-1 [A standard textbook.]

Biographical Sketch

Tadao ODA, born 1940 in Kyoto, Japan

Education: BS in Mathematics, Kyoto University, Japan (March, 1962). MS in Mathematics, Kyoto University, Japan (March, 1964). Ph.D. in Mathematics, Harvard University, U.S.A. (June, 1967).

Positions held: Assistant, Department of Mathematics, Nagoya University, Japan (April, 1964-July, 1968) Instructor, Department of Mathematics, Princeton University, U.S.A. (September, 1967-June, 1968) Assistant Professor, Department of Mathematics, Nagoya University, Japan (July, 1968-September, 1975) Professor, Mathematical Institute, Tohoku University, Japan (October, 1975-March, 2003) Professor Emeritus, Tohoku University (April, 2003 to date)