Splitting field

In abstract algebra, a **splitting field** of a polynomial with coefficients in a field is a smallest field extension of that field over which the polynomial *splits* or decomposes into linear factors.

Contents

Definition

A **splitting field** of a polynomial $p(X)$ over a field K is a field extension L of K over which p factors into linear factors

$$p(X) = c\prod_{i=1}^{\deg(p)}(X - a_i) \text{ where } c \in K \text{ and for each } i \text{ we have } (X - a_i) \in L[X]$$

where the a_i are not necessarily distinct and such that the roots a_i generate L over K. The extension L is then an extension of minimal degree over K in which p splits. It can be shown that such splitting fields exist and are unique up to isomorphism. The amount of freedom in that isomorphism is known as the Galois group of p (if we assume it is separable).

Properties

An extension L which is a splitting field for a set of polynomials $p(X)$ over K is called a normal extension of K.

Given an algebraically closed field A containing K, there is a unique splitting field L of p between K and A, generated by the roots of p. If K is a subfield of the complex numbers, the existence is immediate. On the other hand, the existence of algebraic closures in general is often proved by 'passing to the limit' from the splitting field result, which therefore requires an independent proof to avoid circular reasoning.

Given a separable extension K' of K, a **Galois closure** L of K' is a type of splitting field, and also a Galois extension of K containing K' that is minimal, in an obvious sense. Such a Galois closure should contain a splitting field for all the polynomials p over K that are minimal polynomials over K of elements a of K'.

Constructing splitting fields

Motivation

Finding roots of polynomials has been an important problem since the time of the ancient Greeks. Some polynomials, however, such as $x^2 + 1$ over $\mathbf{R}$, the real numbers, have no roots. By constructing the splitting field for such a polynomial one can find the roots of the polynomial in the new field.

The construction

Let F be a field and $p(X)$ be a polynomial in the polynomial ring $F[X]$ of degree n. The general process for constructing K, the splitting field of $p(X)$ over F, is to construct a sequence of fields $F = K_0, K_1, \ldots K_{r-1}, K_r = K$ such that K_i is an extension of K_{i-1} containing a new root of $p(X)$. Since $p(X)$ has at most n roots the construction will require at most n extensions. The steps for constructing K_i are given as follows:

- Factorize $p(X)$ over K_i into irreducible factors $f_1(X)f_2(X)\cdots f_k(X)$.
- Choose any nonlinear irreducible factor $f(X) = f_i(X)$.
- Construct the field extension K_{i+1} of K_i as the quotient ring $K_{i+1} = K_i[X]/(f(X))$ where $(f(X))$ denotes the ideal in $K_i[X]$ generated by $f(X)$
- Repeat the process for K_{i+1} until $p(X)$ completely factors.

The irreducible factor f_i used in the quotient construction may be chosen arbitrarily. Although different choices of factors may lead to different subfield sequences the resulting splitting fields will be isomorphic.

Since $f(X)$ is irreducible, $(f(X))$ is a maximal ideal and hence $K_i[X]/(f(X))$ is, in fact, a field. Moreover, if we let $\pi : K_i[X] \to K_i[X]/(f(X))$ be the natural projection of the ring onto its quotient then

$$f(\pi(X)) = \pi(f(X)) = f(X) \mod f(X) = 0$$

so $\pi(X)$ is a root of $f(X)$ and of $p(X)$.

The degree of a single extension $[K_{i+1} : K_i]$ is equal to the degree of the irreducible factor $f(X)$. The degree of the extension $[K : F]$ is given by $[K_r : K_{r-1}]\cdots[K_2 : K_1][K_1 : F]$ and is at most $n!$.

The field $K_i[X]/(f(X))$

As mentioned above, the quotient ring $K_{i+1} = K_i[X]/(f(X))$ is a field when $f(X)$ is irreducible. Its elements are of the form

$$c_{n-1}\alpha^{n-1} + c_{n-2}\alpha^{n-2} + \cdots + c_1\alpha + c_0$$

where the c_j are in K_i and $\alpha = \pi(X)$. (If one considers K_{i+1} as a vector space over K_i then the powers α^j for $0 \le j \le n-1$ form a basis.)

The elements of K_{i+1} can be considered as polynomials in α of degree less than n. Addition in K_{i+1} is given by the rules for polynomial addition and multiplication is given by polynomial multiplication modulo $f(X)$. That is, for $g(\alpha)$ and $h(\alpha)$ in K_{i+1} the product $g(\alpha)h(\alpha) = r(\alpha)$ where $r(X)$ is the remainder of $g(X)h(X)$ divided by $f(X)$ in $K_i[X]$.

The remainder $r(X)$ can be computed through long division of polynomials, however there is also a straightforward reduction rule that can be used to compute $r(\alpha) = g(\alpha)h(\alpha)$ directly. First let

$$f(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_1X + b_0.$$

The polynomial is over a field so one can take $f(X)$ to be monic without loss of generality. Now α is a root of $f(X)$, so

$$\alpha^n = -(b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0).$$

If the product $g(\alpha)h(\alpha)$ has a term α^m with $m \geq n$ it can be reduced as follows:

$$\alpha^n \alpha^{m-n} = -\left(b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0\right)\alpha^{m-n} = -\left(b_{n-1}\alpha^{m-1} + \cdots + b_1\alpha^{m-n+1} + b_0\alpha^{m-n}\right)$$

.

As an example of the reduction rule, take $K_i = \mathbf{Q}[X]$, the ring of polynomials with rational coefficients, and take $f(X) = X^7 - 2$. Let $g(\alpha) = \alpha^5 + \alpha^2$ and $h(\alpha) = \alpha^3 + 1$ be two elements of $\mathbf{Q}[X]/(X^7 - 2)$. The reduction rule given by $f(X)$ is $\alpha^7 = 2$ so

$$g(\alpha)h(\alpha) = \left(\alpha^5 + \alpha^2\right)\left(\alpha^3 + 1\right) = \alpha^8 + 2\alpha^5 + \alpha^2 = \left(\alpha^7\right)\alpha + 2\alpha^5 + \alpha^2 = 2\alpha^5 + \alpha^2 + 2\alpha.$$

Examples

The complex numbers

Consider the polynomial ring $\mathbf{R}[x]$, and the irreducible polynomial $x^2 + 1$. The quotient ring $\mathbf{R}[x] / (x^2 + 1)$ is given by the congruence $x^2 \equiv -1$. As a result, the elements (or equivalence classes) of $\mathbf{R}[x] / (x^2 + 1)$ are of the form $a + bx$ where a and b belong to $\mathbf{R}$. To see this, note that since $x^2 \equiv -1$ it follows that $x^3 \equiv -x$, $x^4 \equiv 1$, $x^5 \equiv x$, etc.; and so, for example $p + qx + rx^2 + sx^3 \equiv p + qx + r\cdot(-1) + s\cdot(-x) = (p - r) + (q - s)\cdot x$.

The addition and multiplication operations are given by firstly using ordinary polynomial addition and multiplication, but then reducing modulo $x^2 + 1$, i.e. using the fact that $x^2 \equiv -1$, $x^3 \equiv -x$, $x^4 \equiv 1$, $x^5 \equiv x$, etc. Thus:

$$\begin{aligned}(a_1 + b_1 x) + (a_2 + b_2 x) &= (a_1 + a_2) + (b_1 + b_2)x, \\ (a_1 + b_1 x)(a_2 + b_2 x) &= a_1 a_2 + (a_1 b_2 + b_1 a_2)x + (b_1 b_2)x^2 \equiv (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)x\,.\end{aligned}$$

If we identify $a + bx$ with (a,b) then we see that addition and multiplication are given by

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2), \\ (a_1, b_1) \cdot (a_2, b_2) &= (a_1 a_2 - b_1 b_2, a_1 b_2 + b_1 a_2).\end{aligned}$$

We claim that, as a field, the quotient $\mathbf{R}[x] / (x^2 + 1)$ is isomorphic to the complex numbers, $\mathbf{C}$. A general complex number is of the form $a + ib$, where a and b are real numbers and $i^2 = -1$. Addition and multiplication are given by

$$\begin{aligned}(a_1 + ib_1) + (a_2 + ib_2) &= (a_1 + a_2) + i(b_1 + b_2), \\ (a_1 + ib_1) \cdot (a_2 + ib_2) &= (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1).\end{aligned}$$

If we identify $a + ib$ with (a,b) then we see that addition and multiplication are given by

$$\begin{aligned}(a_1, b_1) + (a_2, b_2) &= (a_1 + a_2, b_1 + b_2), \\ (a_1, b_1) \cdot (a_2, b_2) &= (a_1 a_2 - b_1 b_2, a_1 b_2 + b_1 a_2)\,.\end{aligned}$$

The previous calculations show that addition and multiplication behave the same way in $\mathbf{R}[x] / (x^2 + 1)$ and $\mathbf{C}$. In fact, we see that the map between $\mathbf{R}[x]/(x^2 + 1)$ and $\mathbf{C}$ given by $a + bx \to a + ib$ is a homomorphism with respect to addition *and* multiplication. It is also obvious that the map $a + bx \to a + ib$ is both injective and surjective; meaning that $a + bx \to a + ib$ is a bijective homomorphism, i.e. an isomorphism. It follows that, as claimed: $\mathbf{R}[x] / (x^2 + 1) \cong \mathbf{C}$.

In 1847, Cauchy used this approach to *define* the complex numbers![1]

Cubic example

Let K be the rational number field $\mathbf{Q}$ and $p(x) = x^3 - 2$. Each root of p equals $\sqrt[3]{2}$ times a cube root of unity. Therefore, if we denote the cube roots of unity by

$$\omega_1 = 1\,,$$
$$\omega_2 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$
$$\omega_3 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

any field containing two distinct roots of p will contain the quotient between two distinct cube roots of unity. Such a quotient is a primitive cube root of unity—either ω_2 or $\omega_3 = 1/\omega_2$. It follows that a splitting field L of p will contain ω_2, as well as the real cube root of 2; conversely, any extension of $\mathbf{Q}$ containing these elements contains all the roots of p. Thus

$$L = \mathbf{Q}(\sqrt[3]{2}, \omega_2) = \{a + b\omega_2 + c\sqrt[3]{2} + d\sqrt[3]{2}\omega_2 + e\sqrt[3]{2^2} + f\sqrt[3]{2^2}\omega_2 \mid a, b, c, d, e, f \in \mathbf{Q}\}$$

Note that applying the construction process outlined in the previous section to this example, one begins with $K_0 = \mathbf{Q}$ and constructs the field $K_1 = \mathbf{Q}[X]/(X^3 - 2)$. This field is not the splitting field, but contains one (any) root. However, the polynomial $Y^3 - 2$ is not irreducible over K_1 and in fact, factorizes into $(Y - X)(Y^2 + XY + X^2)$. Note that X is not an indeterminate, and is in fact an element of K_1. Now, continuing the process, we obtain $K_2 = K_1[Y]/(Y^2 + XY + X^2)$ which is indeed the splitting field (and is spanned by the $\mathbf{Q}$-basis $\{1, X, X^2, Y, XY, X^2Y\}$).

Other examples

- The splitting field of $x^q - x$ over $\mathbf{F}_p$ is the unique finite field $\mathbf{F}_q$ for $q = p^n$.[2] Sometimes this field is denoted by GF(q).
- The splitting field of $x^2 + 1$ over $\mathbf{F}_7$ is $\mathbf{F}_{49}$; the polynomial has no roots in $\mathbf{F}_7$, i.e., −1 is not a square there, because 7 is not equivalent to 1 (mod 4).[3]
- The splitting field of $x^2 - 1$ over $\mathbf{F}_7$ is $\mathbf{F}_7$ since $x^2 - 1 = (x + 1)(x - 1)$ already factors into linear factors.
- We calculate the splitting field of $f(x) = x^3 + x + 1$ over $\mathbf{F}_2$. It is easy to verify that $f(x)$ has no roots in $\mathbf{F}_2$, hence $f(x)$ is irreducible in $\mathbf{F}_2[x]$. Put $r = x + (f(x))$ in $\mathbf{F}_2[x]/(f(x))$ so $\mathbf{F}_2(r)$ is a field and $x^3 + x + 1 = (x + r)(x^2 + ax + b)$ in $\mathbf{F}_2(r)[x]$. Note that we can write + for − since the characteristic is two. Comparison of coefficients shows that $a = r$ and $b = 1 + r^2$. The elements of $\mathbf{F}_2(r)$ can be listed as $c + dr + er^2$, where c, d, e are in $\mathbf{F}_2$. There are eight elements: 0, 1, r, $1 + r$, r^2, $1 + r^2$, $r + r^2$ and $1 + r + r^2$. Substituting these in $x^2 + rx + 1 + r^2$ we reach $(r^2)^2 + r(r^2) + 1 + r^2 = r^4 + r^3 + 1 + r^2 = 0$, therefore $x^3 + x + 1 = (x + r)(x + r^2)(x + (r + r^2))$ for r in $\mathbf{F}_2[x]/(f(x))$; $E = \mathbf{F}_2(r)$ is a splitting field of $x^3 + x + 1$ over $\mathbf{F}_2$.

See also

- Rupture field

Notes

1. Cauchy, Augustin-Louis (1847), "Mémoire sur la théorie des équivalences algébriques, substituée à la théorie des imaginaires", *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences* (in French), **24**: 1120–1130
2. Serre. *A Course in Arithmetic*.
3. Instead of applying this characterization of odd prime moduli for which −1 is a square, one could just check that the set of squares in $\mathbf{F}_7$ is the set of classes of 0, 1, 4, and 2, which does not include the class of −1≡6.

References

- Dummit, David S., and Foote, Richard M. (1999) *Abstract Algebra* (2nd ed.). New York: John Wiley & Sons, Inc ISBN 0-471-36857-1.
- Hazewinkel, Michiel, ed. (2001) [1994], "Splitting field of a polynomial", *Encyclopedia of Mathematics*, Springer Science+Business Media B.V / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- Weisstein, Eric W. "Splitting field". *MathWorld*.