the study of algebraic elements (if you are adjoining one root of a polynomial, why not adjoin *all* the roots?) and so take a particularly important role in Galois Theory.

We end this section with a discussion of field extensions of F which contain all the roots of *all* polynomials over F.

Definition. The field $\overline{F}$ is called an *algebraic closure* of F if $\overline{F}$ is algebraic over F and if every polynomial $f(x) \in F[x]$ splits completely over $\overline{F}$ (so that $\overline{F}$ can be said to contain all the elements algebraic over F).

Definition. A field K is said to be *algebraically closed* if every polynomial with coefficients in K has a root in K.

It is not obvious that algebraically closed fields exist nor that there exists an algebraic closure of a given field F (we shall prove this shortly).

Note that if K is algebraically closed, then in fact every $f(x) \in K[x]$ has *all* its roots in K, since by definition $f(x)$ has a root $\alpha \in K$, hence has a factor $x - \alpha$ in $K[x]$. The remaining factor of $f(x)$ then is a polynomial in $K[x]$, hence has a root, so has a linear factor etc., so that $f(x)$ must split completely. Hence if K is algebraically closed, then K itself is an algebraic closure of K and the converse is obvious, so that $K = \overline{K}$ if and only if K is algebraically closed.

The next result shows that the process of "taking the algebraic closure" actually stops after one step — taking the algebraic closure of an algebraic closure does not give a larger field: the field is already algebraically closed (notationally: $\overline{\overline{F}} = \overline{F}$).

Proposition 29. Let $\overline{F}$ be an algebraic closure of F. Then $\overline{F}$ is algebraically closed.

Proof: Let $f(x)$ be a polynomial in $\overline{F}[x]$ and let α be a root of $f(x)$. Then α generates an algebraic extension $\overline{F}(\alpha)$ of $\overline{F}$, and $\overline{F}$ is algebraic over F. By Theorem 20, $\overline{F}(\alpha)$ is algebraic over F so in particular its element α is algebraic over F. But then $\alpha \in \overline{F}$, showing $\overline{F}$ is algebraically closed.

Given a field F we have already shown how to construct (finite) extensions of F containing all the roots of any given polynomial $f(x) \in F[x]$. Intuitively, an algebraic closure of F is given by the field "generated" by all of these fields. The difficulty with this is "generated" *where*?, since they are not all subfields of a given field. For a *finite* collection of polynomials $f_1(x), \dots, f_k(x)$, we can identify their splitting fields as subfields of the splitting field of the product polynomial $f_1(x) \cdots f_k(x)$, but the same idea used for an *infinite* number of polynomials requires numerous "bookkeeping" identifications and an application of Zorn's Lemma.

We shall instead construct an algebraic closure of F by first constructing an algebraically closed field containing F. The proof uses a clever idea of Artin which very neatly solves the "bookkeeping" problem of constructing a field containing the appropriate roots of polynomials (which also ultimately relies on Zorn's Lemma) by introducing a separate variable for every polynomial.

Proposition 30. For any field F there exists an algebraically closed field K containing F

Proof: For every nonconstant monic polynomial $f = f(x)$ with coefficients in F, let x_f denote an indeterminate and consider the polynomial ring $F[\dots, x_f, \dots]$ generated over F by the variables x_f. In this polynomial ring consider the ideal I generated by the polynomials $f(x_f)$. If this ideal is not proper, then 1 is an element of the ideal, hence we have a relation

$$g_1 f_1(x_{f_1}) + g_2 f_2(x_{f_2}) + \cdots + g_n f_n(x_{f_n}) = 1$$

where the g_i, $i = 1, 2, \dots, n$, are polynomials in the x_f. For $i = 1, 2, \dots, n$ let $x_{f_i} = x_i$ and let $x_{n+1}, \dots, x_m$ be the remaining variables occurring in the polynomials g_j, $j = 1, 2, \dots, n$. Then the relation above reads

$$g_1(x_1, x_2, \dots, x_m) f_1(x_1) + \cdots + g_n(x_1, x_2, \dots, x_m) f_n(x_n) = 1.$$

Let F' be a finite extension of F containing a root α_i of $f_i(x)$ for $i = 1, 2, \dots, n$. Letting $x_i = \alpha_i$, $i = 1, 2, \dots, n$ and setting $x_{n+1} = \cdots = x_m = 0$, say, in the polynomial equation above would imply that $0 = 1$ in F', clearly impossible.

Since the ideal I is a proper ideal, it is contained in a maximal ideal $\mathcal{M}$ (this is where Zorn's Lemma is used). Then the quotient

$$K_1 = F[\dots, x_f, \dots]/\mathcal{M}$$

is a field containing (an isomorphic copy of) F. Each of the polynomials f has a root in K_1 by construction, namely the image of x_f, since $f(x_f) \in I \subseteq \mathcal{M}$. We have constructed a field K_1 in which every polynomial with coefficients from F has a root. Performing the same construction with K_1 instead of F gives a field K_2 containing K_1 in which all polynomials with coefficients from K_1 have a root. Continuing in this fashion we obtain a sequence of fields

$$F = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_j \subseteq K_{j+1} \subseteq \cdots$$

where every polynomial with coefficients in K_j has a root in K_{j+1}, $j = 0, 1, \dots$. Let

$$K = \bigcup_{j \geq 0} K_j$$

be the union of these fields. Then K is clearly a field containing F. Since K is the union of the fields K_j, the coefficients of any polynomial $h(x)$ in $K[x]$ all lie in some field K_N for N sufficiently large. But then $h(x)$ has a root in K_{N+1}, so has a root in K. It follows that K is algebraically closed, completing the proof.

We now use the algebraically closed field containing F to construct an algebraic closure of F:

Proposition 31. Let K be an algebraically closed field and let F be a subfield of K. Then the collection of elements $\overline{F}$ of K that are algebraic over F is an algebraic closure of F. An algebraic closure of F is unique up to isomorphism.

Proof: By definition, $\overline{F}$ is an algebraic extension of F. Every polynomial $f(x) \in F[x]$ splits completely over K into linear factors $x - \alpha$ (the same is true for every polynomial even in $K[x]$). But each α is a root of $f(x)$, so is algebraic over F, hence is an element of $\overline{F}$. It follows that all the linear factors $x - \alpha$ have coefficients in $\overline{F}$, i.e., $f(x)$ splits completely in $\overline{F}[x]$ and $\overline{F}$ is an algebraic closure of F.

The uniqueness (up to isomorphism) of the algebraic closure is natural in light of the uniqueness (up to isomorphism) of splitting fields, and is proved along the same lines together with an application of Zorn's Lemma and will be omitted.

We shall prove later using Galois theory the following result (purely analytic proofs using complex analysis also exist).

Theorem. *(Fundamental Theorem of Algebra)* The field $\mathbb{C}$ is algebraically closed.

By Proposition 31, we immediately obtain:

Corollary 32. The field $\mathbb{C}$ contains an algebraic closure for any of its subfields. In particular, $\overline{\mathbb{Q}}$, the collection of complex numbers algebraic over $\mathbb{Q}$, is an algebraic closure of $\mathbb{Q}$.

The point of these considerations is that all the computations involving elements algebraic over a field F may be viewed as taking place in one (large) field, namely $\overline{F}$. Similarly, we can speak sensibly of the composite of any collection of algebraic extensions by viewing them all as subfields of an algebraic closure. In the case of $\mathbb{Q}$ or finite extensions of $\mathbb{Q}$ we may consider all of our computations as occurring in $\mathbb{C}$.

EXERCISES

1. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 - 2$.
2. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + 2$.
3. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^4 + x^2 + 1$.
4. Determine the splitting field and its degree over $\mathbb{Q}$ for $x^6 - 4$.
5. Let K be a finite extension of F. Prove that K is a splitting field over F if and only if every irreducible polynomial in $F[x]$ that has a root in K splits completely in $K[x]$. [Use Theorems 8 and 27.]
6. Let K_1 and K_2 be finite extensions of F contained in the field K, and assume both are splitting fields over F.
   (a) Prove that their composite K_1K_2 is a splitting field over F.
   (b) Prove that $K_1 \cap K_2$ is a splitting field over F. [Use the preceding exercise.]

13.5 SEPARABLE AND INSEPARABLE EXTENSIONS

Let F be a field and let $f(x) \in F[x]$ be a polynomial. Over a splitting field for $f(x)$ we have the factorization

$$f(x) = (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2} \cdots (x - \alpha_k)^{n_k}$$

where $\alpha_1, \alpha_2, \ldots, \alpha_k$ are distinct elements of the splitting field and $n_i \geq 1$ for all i. Recall that α_i is called a *multiple* root if $n_i > 1$ and is called a *simple* root if $n_i = 1$. The integer n_i is called the *multiplicity* of the root α_i.

Definition. A polynomial over F is called *separable* if it has no multiple roots (i.e., all its roots are distinct). A polynomial which is not separable is called *inseparable*.

Note that if a polynomial $f(x)$ has distinct roots in one splitting field then $f(x)$ has distinct roots in any splitting field (since this is equivalent to $f(x)$ factoring into distinct linear factors, and there is an isomorphism over F between any two splitting fields of $f(x)$ that is bijective on its roots), so that we need not specify the field containing all the roots of $f(x)$.

Examples

(1) The polynomial $x^2 - 2$ is separable over $\mathbb{Q}$ since its two roots $\pm\sqrt{2}$ are distinct. The polynomial $(x^2-2)^n$ for any $n \geq 2$ is inseparable since it has the multiple roots $\pm\sqrt{2}$, each with multiplicity n.

(2) The polynomial $x^2 - t$ $(= x^2 + t)$ over the field $F = \mathbb{F}_2(t)$ of rational functions in t with coefficients from $\mathbb{F}_2$ is irreducible as we've seen before, but is not separable. If $\sqrt{t}$ denotes a root in some extension field (note that $\sqrt{t} \notin F$), then

$$(x - \sqrt{t})^2 = x^2 - 2x\sqrt{t} + t = x^2 + t = x^2 - t$$

since F is a field of characteristic 2. Hence this irreducible polynomial has only one root (with multiplicity 2), so is not separable over F.

There is a simple criterion to check whether a polynomial has multiple roots.

Definition. The *derivative* of the polynomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$$

is defined to be the polynomial

$$D_x f(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1 \in F[x].$$

This formula is nothing but the usual formula for the derivative of a polynomial familiar from calculus. It is purely algebraic and so can be applied to a polynomial over an arbitrary field F, where the analytic notion of derivative (involving limits — a *continuous* operation) may not exist.

The usual (calculus) formulas for derivatives hold for derivatives in this situation as well, for example the formulas for the derivative of a sum and of a product:

$$D_x(f(x) + g(x)) = D_x f(x) + D_x g(x)$$
$$D_x(f(x)g(x)) = f(x)D_x g(x) + (D_x f(x))g(x).$$

These formulas can be proved directly from the definition for polynomials and do not require any limiting operations and are left as an exercise.

The next proposition shows that the separability of $f(x)$ can be determined by the Euclidean Algorithm in the field where the coefficients of $f(x)$ lie, without passing to a splitting field and factoring $f(x)$.