Artin: Fields

James Pagan

March 2024

Contents

1 Fields

A **field** is a commutative division ring. If $F \subseteq K$ is a pair of fields, we say K is a **field extension** of F. This relation is denoted K / F; this is *not* a quotient! Examples of fields are as follows:

1. Subfields of $\mathbb{C}$ are called **number fields**. Any subfield of $\mathbb{C}$ contains the field $\mathbb{Q}$ of rational numbers. The most important number systems are **algebraic number fields**, whose elements are algebraic numbers.
2. A **finite field** is a field that contains finitely many elements. Finite fields are gorgeous and colorful objects that obey beautiful, tight-knit properties.
3. Extensions of the field $C(t)$ of rational functions are called **function fields**.

2 Algebraic and Transcendental Elements

Let K / F be a field extension and let α be an element of K. The element α is **algebraic over F** if is the root of a monic polynomial with coefficients in F — say, $f(\alpha) = 0$ for

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad \text{where} \quad a_{n-1}, \ldots, a_0 \in F,$$

An element is **transcendental over F** if it is not algebraic. Both of these properties depend on the field F. Every element $\alpha \in F$ is algebraic over F due to the monomial $x - \alpha$. We can elegantly describe this as a substitution homomorphism

$$\phi : F[x] \to X \quad \text{defined by} \quad x \rightsquigarrow \alpha.$$

An element ϕ is transcendental if ϕ is injective and algebraic otherwise.

Proposition 1. *Let $\alpha \in K / F$ be an element of a field extension. The following conditions on a monic polynomial $f \in F[x]$ are equivalent:*

1. *f is the unique monic polynomial of lowest degree in $F[x]$ with α as a root.*
2. *f is an irreducible element of $F[x]$ with α as a root.*
3. *$f(\alpha) = 0$ and (f) is a maximal ideal.*
4. *If $g(\alpha) = 0$, then $f \mid g$.*

Proof. Since $F[x]$ is a Euclidean domain, the kernel of $\phi : F[x] \to K$ is a principal ideal generated by some polynomial f of smallest degree. f must be irreducible, or else a polynomial of smaller degree has a root at ϕ; the other properties are easy to deduce. $\square$

This polynomial is called the **minimal polynomial** of α. Like before, the minimal polynomial depends on both F and α. The degree of the minimal polynomial of α is called the **degree** of α. The minimal polynomial is critical for studying the following natural objects:

1. The field $F(\alpha_1, \dots, \alpha_n)$ denotes the subfield of K generated by $\alpha_1, \dots, \alpha_n$.

   $$F(\alpha_1, \dots, \alpha_n) \text{ is the smallest subfield of } K \text{ that contains } F \text{ and } \alpha_1, \dots, \alpha_n.$$

2. The ring $F[\alpha_1, \dots, \alpha_n]$ denotes the subring of K generated by $\alpha_1, \dots, \alpha_n$. The ring $F[\alpha]$ is isomorphic to the image of the substitution homomorphism $\phi : F[x] \to K$ as defined above.

The field $F(\alpha)$ is isomorphic to the field of fractions of $F[\alpha]$. If α is transcendental, then $F[\alpha] \cong F[x]$ and $F(\alpha) \cong F(\alpha)$; otherwise,

Proposition 2. *Let* $\alpha \in K / F$ *be an element of a field extension which is algebraic over* F*. Let* f *be the minimal polynomial of* α*.*

1. *The canonical map* $\phi : F[x] / (f) \to F[\alpha]$ *an isomorphism.*
2. $F[\alpha]$ *is a field, hence* $F[\alpha] = F(\alpha)$*.*
3. *More generally,* $F[\alpha_1, \dots, \alpha_n] = F(\alpha_1, \dots, \alpha_n)$ *if* $\alpha_1, \dots, \alpha_n \in K / F$ *are algebraic.*

Proof. Let $\phi : F[x] \to K$ be the aforementioned substitution homomorphism. Then $F[x] / \operatorname{Ker}\phi \cong K$. By Proposition 1, the kernel of ϕ is a maximal ideal generated by the minimal polynomial f, which yields (1) and (2). As per (3), an induction argument proceeds along these lines:

$$F[\alpha_1, \dots, \alpha_n] = F[\alpha_1, \dots, \alpha_{n-1}][\alpha_n] = F(\alpha_1, \dots, \alpha_n)[a_k] = F(\alpha_1, \dots, \alpha_n).$$

The omitted details are relatively easy to verify. □

The following proposition is a special case of one I omitted from Chapter 11.

Proposition 3. *Let* $\alpha \in K / F$ *be an algebraic element of a field extension. If* $\deg \alpha = n$*, then* $\alpha_1, \dots, \alpha_n$ *is a basis for* $F(\alpha)$ *as a vector space over* F*.*

A fundamental question is: given two elements α and β — or given their minimal polynomials — when can one determine whether α and β generate equal fields? Proposition three provides a necessary non-sufficient condition: that $\deg \alpha = \deg \beta$. The following proposition answers a special case.

Proposition 4. *Let $\alpha \in K / F$ and $\beta \in L / F$ be elements of field extensions which are algebraic over F. Then α and β have the same minimal polynomial if and only if $F(\alpha) \cong F(\beta)$ — in which case, the isomorphism is the identity on F and maps $\alpha \rightsquigarrow \beta$*

Proof. Suppose that α and β share the same minimal polynomial $f \in F[x]$. By Proposition 2, $F(\beta) \cong F[x] / (f) \cong F(\alpha)$; the additional conditions imposed upon the isomorphism are easy to verify.

For the other direction, suppose $F(\alpha) \cong F(\beta)$ by the described isomorphism. Let the minimal polynomial of f be α; by Proposition 5, $f(\alpha) = 0$ implies $f(\beta) = 0$ too — hence the minimal polynomial of α divides the minimal polynomial of β. Observing that they're monic and share the same degree implies they are equal. □

Let K / F and K' / F be field extensions. An **F-isomorphism** is an isomorphism $\phi : K \to K'$ that restricts F to the identity; the fields K and K' are **isomorphic field extensions**.

Proposition 5. *Let $\phi : K \to K'$ be an isomorphism of field extensions, and suppose $f \in F[x]$. Then $f(\alpha) = 0$ if and only if $f(\alpha') = 0$.*

Proof. It suffices to prove the theorem for the minimal polynomial of α — thus redefine f as such. The canonical epimorphism $K' \to K' / (f)$ may be decomposed as

$$K' \longrightarrow K \longrightarrow K / (f) \longrightarrow K' / (f),$$

of which $\phi(\alpha)$ vanishes; thus $f(\phi(\alpha)) = 0$. Alternatively, we could let $f(x) = a_n x^n + \cdots + a_0$, and observe that

$$a_n \phi(\alpha)^n + \cdots + a_0 \;=\; \phi(a_n \alpha^n + \cdots + a_0) \;=\; \phi(0) = 0.$$

The symmetry of isomorphisms entails the desired bicondition. □

My intuition is that Proposition 5 should constrain the structure of field extensions — but hell, what do I know. The following lemma regards the **characteristic** of a field.

Lemma 1. *The characteristic of a field is either 0 or prime.*

Proof. If F has characteristic $n = ab$ for $n > a, b > 2$, we attain the following equation:

$$\left(\sum_{i=1}^{a} 1\right)\left(\sum_{i=1}^{b} 1\right) \;=\; \sum_{i=1}^{n} 1 \;=\; 0$$

Since F is an integral domain, one of these is zero — violating the minimality of n. □

3 The Degree of a Field Extension

Any field extension K / F may be regarded as an F-vector space K. The **degree** $[K : F]$ of this field extension is the dimension of this vector space. If $[K : F]$ is finite, K is a **finite extension**; if $[K : F] = 2$, it **quadratic extension**, with similar terms for $n \geqslant 3$.

Lemma 2. *Let $\alpha \in K / F$ is an element of a field extension. Then the following holds:*

1. $[K : F] = 1$ *if and only if* $K = F$.
2. $\deg \alpha = 1$ *if and only if* $\alpha \in F$.

Proof. If there was some element $\alpha \in K \setminus F$, then $1, \alpha$ would be independent in K — hence $[K : F] \geqslant 2$. The contrapositive yields (1). For (2), we have

$$\deg \alpha = 1 \iff x - \alpha \text{ is the minimal polynomial of } \alpha \iff \alpha \in F.$$

This concludes the proof. □

This classifies extensions with degree 1. Extensions of degree 2 have a simple story as well:

Proposition 6. *Suppose that the characteristic of F is not 2. Then an extension K / F is quadratic if and only if adjoining $\delta^2 = a \in F$ not in F obtains K.*

Proof. Suppose that K / F is quadratic. Then there exists $\alpha \in K \setminus F$, in which case $(1, \alpha)$ is a basis of K. Thus there exist $b, c \in F$ such that $\alpha^2 = b\alpha + c$. Deriving the quadratic formula by completing the square, we find

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Because $\alpha \notin F$, the element $b^2 - 4c$ must not be a square in F. If δ is one of these square roots, it is clear that $(1, \delta)$ spans K — hence $F(\delta) = K$. The contrary is trivial. □

The following theorem is the foundational result of this section. The remainder of the results in this section are mere corollaries:

Theorem 1 (Multiplicative Property of the Degree)**.** *Let $L / K / F$ be field extensions. Then $[L : F] = [L : K]\,[K : F]$; hence each of $[L : K]$ and $[K : F]$ divides $[L : F]$.*

Proof. Let $\ell_1, \ldots, \ell_n$ be a basis of L over K; let $k_1, \ldots, k_n$ be basis of K over F. We claim the products $\ell_i k_j$ constitute a basis of L over F — which starts with demonstrating that they span L. For all $\ell \in \mathsf{L}$, there exist $j_1, \ldots, j_n$ such that

$$\ell = j_1 \ell_1 + \cdots + j_n \ell_n.$$

Similarly, each j_i factors in K for $f_{i1}, \ldots, f_{im}$ as

$$j_i = f_{i1} k_1 + \cdots + f_{im} k_m.$$

Substituting this equation into the prior one yields a linear combination of ℓ into the terms $\ell_i k_j$. What remains to be demonstrated is their independence; suppose that

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{m} f_{ij} \ell_i k_j = \ell_1 \left(\sum_{j=1}^{m} f_{1j} k_j \right) + \cdots + \ell_n \left(\sum_{j=1}^{n} f_{mj} k_j \right).$$

Since $\ell_1, \ldots, \ell_n$ are a basis, each of these sums must be zero; since $k_1, \ldots, k_m$ are a basis, each f_{ij} must be zero. The lengths of these bases imply the desired result. □

We now example the relationship between the degree of $\mathsf{F}(\alpha)$ to those of K and F.

Lemma 3. *Let $\alpha \in \mathsf{K} \,/\, \mathsf{F}$ be an element of a field extension. Then the following holds:*

1. *If α is algebraic, then $[\mathsf{F}(\alpha) : \mathsf{F}] = \deg \alpha$.*
2. *α is algebraic if and only if $[\mathsf{F}(\alpha) : \mathsf{F}]$ is finite.*
3. *If K is finite, then α is algebraic and $\deg \alpha$ divides $[\mathsf{K} : \mathsf{F}]$.*

Proof. Since α is algebraic, no linear combinations of $1, \alpha, \ldots, \alpha^{n-1}$ yield zero; by Euclidean Division, they span $\mathsf{F}(\alpha)$. This yields (1). As per (2), α being algebraic implies $1, \alpha, \alpha^2 \ldots, \alpha^{n-1}$ spans $\mathsf{F}[\alpha]$; otherwise, $1, \alpha, \alpha^2, \ldots$ is an infinite basis of $\mathsf{F}[\alpha]$.

For (3), it is clear that α is algebraic. As per the degree, if $\deg \alpha = n$:

$$[\mathsf{K} : \mathsf{F}] = [\mathsf{K} : \mathsf{F}(\alpha)]\,[\mathsf{F}(\alpha) : \mathsf{F}] = [\mathsf{K} : \mathsf{F}(\alpha)] \deg \alpha.$$

Hence $\deg \alpha$ divides $[\mathsf{K} : \mathsf{F}]$. This completes the proof. □

There is even more we can say about these objects:

Corollary 1. *The following three facts hold:*

1. *Let* $L / K / F$ *be field extensions. If* $\alpha \in L$ *is algebraic over* F*, it is algebraic over* K *and* $\deg_K \alpha \leqslant \deg_F \alpha$*.*
2. K / F *is generated by finitely many algebraic elements if and only if it is a finite extension.*
3. *If* K / F *is a field extension, the elements of* K *that are algebraic over* F *constitute a subfield of* F*.*

Proof. If $\alpha \in L$ is algebraic over F, then there exist $f_1, \dots, f_n \in L$ such that

$$\alpha^n + f_{n-1}\alpha^{n-1} + \cdots + f_0 \,=\, 0.$$

Since $L \subseteq K$, this means α is a root of a polynomial in $K[x]$ — hence α is algebraic over K. The degree is smaller than n if the above polynomial reduces in K, and equal otherwise.

For (2): if K / F is generated by finitely many algebraic elements $\alpha_1, \dots, \alpha_n$, then

$$\begin{aligned} [F(\alpha_1, \dots, \alpha_n) : F] \,&=\, [F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] \cdots [F(\alpha_1) : F(\alpha)] \\ &\leqslant\, \deg \alpha_n \times \cdots \times \deg \alpha_0 \\ &<\, \infty, \end{aligned}$$

so K / F is a finite extension. $\square$