Fields and Galois Theory

J. S. Milne

December 28, 2021

Contents

1 Basic Definitions and Results **1**
1.1 The characteristic of a field 1
1.2 Factoring polynomials 2
1.3 Extensions 4
1.4 The subring generated by a subset 4
1.5 The subfield generated by a subset 5
1.6 Construction of some extensions 5
1.7 Stem fields 6
1.8 Algebraic and transcendental elements 7
1.9 Algebraically closed fields 8

1 Basic Definitions and Results

1.1 The characteristic of a field

Given a field F and consider a map

$$\mathbb{Z} \to F, \quad n \mapsto n \cdot 1_F$$

If the kernel of the map is $\neq (0)$, so that $n \cdot 1_F = 0$ for some $n \neq 0$. The smallest positive such n will be a prime p (otherwise $(m \cdot n) \cdot 1_F = (m \cdot 1_F) \cdot (n \cdot 1_F) = 0$ there will be two nonzero elements in F whose product is zero, but a field is an integral domain) and p generates the kernel. Thus the map $n \mapsto n \cdot 1_F : \mathbb{Z} \to F$ defines an isomorphism from $\mathbb{Z}/p\mathbb{Z}$ onto the subring

$$\{m \cdot 1_F \mid m \in \mathbb{Z}\}$$

of F. In this case, F contains a copy of $\mathbb{F}_p$

A field isomorphic to one of the fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \ldots, \mathbb{Q}$ is called a **prime field**. Every field contains exactly one prime field (as a subfield)

A commutative ring R is said to have **characteristic** p (resp. 0) if it contains a prime field (as a subring) of characteristic p (resp. 0). Then the prime field is unique and, by definition, contains 1_R. Thus if R has characteristic $p \neq 0$, then $1_R + \cdots + 1_R = 0$ (p terms)

Let R be a nonzero commutative ring. If R has characteristic $p \neq 0$, then

$$pa := \underbrace{a + \cdots + a}_{p \text{ terms}} = \underbrace{(1_R + \cdots + 1_R)}_{p \text{ terms}} a = 0a = 0$$

for all $a \in R$. Conversely, if $pa = 0$ for all $a \in R$, then R has characteristic p

Let R be a nonzero commutative ring. The usual proof by induction shows that the binomial theorem

$$(a+b)^m = a^m + \binom{m}{1} a^{m-1} b + \binom{m}{2} a^{m-2} b^2 + \cdots + b^m$$

holds in R. If p is prime, then it divides

$$\binom{p}{r} := \frac{p!}{r!(p-r)!}$$

for all r with $1 \leq r \leq p-1$. Therefore, when R has characteristic p

$$(a+b)^p = a^p + b^p \quad \text{for all } a, b \in R$$

and so the map $a \mapsto a^p : R \to R$ is a homomorphism of rings (even of $\mathbb{F}_p$-algebras). It is called the **Frobenius endomorphsim** of R. The map $a \mapsto a^{p^n} : R \to R$, $n \geq 1$, is hte composite of n copies of the Frobenius endomorphsim, and so it also is a homomorphism. Therefore

$$(a_1, \ldots, a_m)^{p^n} = a_1^{p^n} + \cdots + a_m^{p^n}$$

for all $a_i \in R$.

When F is a field, the Frobenius endomorphsim is injective

1.2 Factoring polynomials

Proposition 1.1. *Let $r \in \mathbb{Q}$ be a root of a polynomial*

$$a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0, \quad a_i \in \mathbb{Z}$$

and write $r = c/d$, $c, d \in \mathbb{Z}$, $\gcd(c,d) = 1$. Then $c \mid a_0$ and $d \mid a_m$

Proof.

$$a_m c^m + a_{m-1} c^{m-1} d + \cdots + a_0 d^m = 0$$

$d \mid a_m c^m$ and therefore $d \mid a_m$. Similarly $c \mid a_0$ □

Example 1.1. The polynomial $f(X) = X^3 - 3X - 1$ is irreducible in $\mathbb{Q}[X]$ because its only possible roots are ± 1 and $f(1) \neq 0 \neq f(-1)$

Proposition 1.2 (Gauss's Lemma)**.** *Let $f(X) \in \mathbb{Z}[X]$. If $f(X)$ factors nontrivially in $\mathbb{Q}[X]$, then it factors nontrivially in $\mathbb{Z}[X]$*

Proof. Let $f = gh \in \mathbb{Q}[X]$ with g, h nonconstant. For suitable integers m and n, $g_1 := mg$ and $h_1 := nh$ have coefficients in $\mathbb{Z}$, so we have a factoriztion

$$mnf = g_1 \cdot h_1$$

in $\mathbb{Z}[X]$. If a prime p divides mn, then looking modulo p, we obtain

$$0 = \overline{g_1} \cdot \overline{h_1} \in \mathbb{F}_p[X]$$

Since $\mathbb{F}_p[X]$ is an integral domain, this implies that p divides all the coefficients of at least one of the polynomials g_1, h_1, say g_1, so that $g_1 = pg_2$ for some $g_2 \in \mathbb{Z}[X]$. Thus we have a factoriztion

$$(mn/p)f = g_2 \cdot h_1 \in \mathbb{Z}[X]$$

Continuing in this fashion, we eventually remove all the prime factors of mn. □

Proposition 1.3. *If $f \in \mathbb{Z}[X]$ is monic, then every monic factor of f in $\mathbb{Q}[X]$ lies in $\mathbb{Z}[X]$*

Proof. Let g be a monic factor of f in $\mathbb{Q}[X]$, so that $f = gh$ with $h \in \mathbb{Q}[X]$ also monic. Let m, n be the positive integers with the fewest prime factors s.t. $mg, nh \in \mathbb{Z}[X]$. As in the proof of Gauss's Lemma, if a prime p divides mn, then it divides all the coefficients of at least one of the polynomials mg, nh, say mg, in which case it divides m because g is monic. Now $\frac{m}{p} g \in \mathbb{Z}[X]$ which contradicts the definition of m. □

Proposition 1.4 (Eisenstein's Criterion)**.** *Let*

$$f = a_m X^m + \cdots + a_0, \quad a_i \in \mathbb{Z}$$

suppose that there is a prime p s.t.

1. $p \nmid a_m$

2. $p \mid a_i$ *for* $i = 0, \ldots, m-1$

3. $p^2 \nmid a_0$

Then f *is irreducible in* $\mathbb{Q}[X]$

Proof. If $f(X)$ factors nontrivially in $\mathbb{Q}[X]$, then it factors nontrivially in $\mathbb{Z}[X]$, say

$$a_m X^m + \cdots + a_0 = (b_r X^r + \cdots + b_0)(c_s X^s + \cdots + c_0)$$

where $b_i, c_i \in \mathbb{Z}$. Since p, but not p^2, divides $a_0 = b_0 c_0$, p must divide exactly one of b_0, c_0, say b_0. Now from the equation

$$a_1 = b_0 c_1 + b_1 c_0$$

we see that $p \mid b_1$, and from the equation

$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$$

that $p \mid b_2$. By continuing in this way, we find that p divides $b_0, b_1, \ldots, b_r$, which contradicts the condition that p does not divide a_m □

1.3 Extensions

Let F be a field. A field containing F is called an **extension** of F. In other words, an extension is an F-algebra whose underlying ring is a field. An extension E of F is, in particular, an F-vector space, whose dimension is called the **degree** of E over F. It is denoted by $[E : F]$. An extension is **finite** if its degree is finite.

When E and E' are extensions of F, an F**-homomorphism** $E \to E'$ is a homomorphism $\varphi : E \to E'$ s.t. $\varphi(c) = c$ for all $c \in F$

Proposition 1.5 (Multiplicity of degrees)**.** *Consider fields* $L \supset E \supset F$*. Then* L/F *is of finite degree iff* L/E *and* E/F *are both of finite degree, in which case*

$$[L : F] = [L : E][E : F]$$

1.4 The subring generated by a subset

Let F be a subfield of a field E and let S be a subset of E. The intersection of all the subrings of E containing F and S is obviously the smallest subring of E containing both F and S. We call it the subring of E **generated by** F **and** S (**generated over** F **by** S), and we denote it by $F[S]$.

Lemma 1.6. *The ring $F[S]$ consists of the elements of E that can be expressed as finite sums of the form*

$$\sum a_{i_1\cdots i_n}\alpha_1^{i_1}\cdots\alpha_n^{i_n}, \quad a_{i_1\cdots i_n}\in F, \quad \alpha_i\in S, \quad i_j\in\mathbb{N}$$

Lemma 1.7. *Let R be an integral domain containing a subfield F (as a subring). If R is finite-dimensional when regarded as an F-vector space, then it is a field*

Proof. Let $\alpha\in R$ be nonzero. The map $h:x\mapsto\alpha x$ is an injective linear map of finite-dimensional F-vector spaces, and is therefore surjective. In particular, there is an element $\beta\in R$ s.t. $\alpha\beta=1$

$\alpha x=\alpha y$, we need R to be integral domain to make $x=y$

Also for $f\in R$, we need R to be a field to make $\alpha f x=f\alpha x$

Surjection is trivial □

1.5 The subfield generated by a subset

The intersection of all the subfields of E containing F and S is the smallest subfield of E containing both F and S. We call it the subfield of E **generated by** F **and** S, and we denote it by $F(S)$, it is the fraction field of $F[S]$

An extension E of F is **simple** if $E=F(\alpha)$ for some $\alpha\in E$

Let F and F' be subfields of a field E. The intersection of the subfields of E containing both F and F' is obviously the smallest subfield of E containing both $F$and F. We call it the **composite** of F and F' in E, and we denote it by $F\cdot F'$. It can also be described as the subfield of E generated over F by F', or the subfield generated over F' by F

$$F(F')=F\cdot F'=F'(F)$$

1.6 Construction of some extensions

Let $f(X)\in F(X)$ be a monic polynomial of degree m. Consider the quotient $F[X]/(f(X))$, and write x for the image of X in $F[X]/(f(X))$, i.e., $x=X+(f(X))$

1. The map
$$P(X)\mapsto P(x):F[X]\to F[x]$$
is a homomorphism sending $f(X)$ to 0, therefore $f(x)=0$. $F[x]=F[X]/(f)$ since for each $x^n=(X+(f(X))^n)=X^n+(f(X))$.

2. The division algorithm shows that every element $g \in F[X]/(f)$ is represented by a unique polynomial r of degree $< m$. Hence each element of $F[x]$ can be expressed uniquely as a sum

$$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}, \quad a_i \in F$$

3. *Now assume that $f(X)$ is irreducible*. Then every nonzero $\alpha \in F[x]$ has an inverse, which can be found as follows. Use 2 to write $\alpha = g(x)$ with $g(X)$ a polynomial of degree $\leq m-1$, and apply Euclid's algorithm in $F[X]$ to find polynomials $a(X)$ and $b(X)$ s.t.

$$a(X)f(X) + b(X)g(X) = d(X)$$

with $d(X)$ the gcd of f and g. In our case, $d(X)$ is 1 because $f(X)$ is irreducible and deg $g(X) <$ deg $f(X)$. When we replace X with x, the equality becomes

$$b(x)g(x) = 1$$

Hence $b(x)$ is the inverse of $g(x)$

We have proved the following statement

Proposition 1.8. *For a monic irreducible polynomial $f(X)$ of degree m in $F[X]$*

$$F[x] := F[X]/(f(X))$$

is a field of degree m over F. Computations in $F[x]$ come down to computations in F

Since $F[x]$ is a field, $F(x) = F[x]$

Example 1.2. Let $f(X) = X^2+1 \in \mathbb{R}[X]$. Then $\mathbb{R}[x]$ has elements $a+bx, a, b \in \mathbb{R}$

We usually write i for x and $\mathbb{C}$ for $\mathbb{R}[x]$

1.7 Stem fields

Let f be a monic irreducible polynomial in $F[X]$. A pair (E, α) consisting of an extension E of F and an $\alpha \in E$ is called a **stem field for** f if $E = F[\alpha]$ and $f(\alpha) = 0$. For example, the pair (E, α) with $E = F[X]/(f) = F[x]$ and $\alpha = x$.

Let (E, α) be a stem field, and consider the surjective homomorphism of F-algebras

$$g(X) \to g(\alpha) : F[X] \to E$$

Its kernel is generated by a nonzero monic polynomial, which divides f, and so must equal it. Therefore the homomorphism defines an F-isomorphism

$$x \mapsto \alpha : F[x] \to E, \quad F[x] = F[X]/(f)$$

In other words, the stem field (E, α) of f is F-isomorphic to the standard stem field $(F[X]/(f), x)$. It follows that every element of a stem field (E, α) for f can be written uniquely in the form

$$a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1}, \quad a_i \in F, \quad m = \deg(f)$$

and that arithmetic in $F[\alpha]$ can be performed using the same rules in $F[x]$.

1.8 Algebraic and transcendental elements

Let F be a field. An element α of an extension E of F defines a homomorphism

$$f(X) \mapsto f(\alpha) : F[X] \to E$$

There are two possibilities:

1. Kernel is (0), so that for $f \in F[X]$

   $$f(\alpha) = 0 \Rightarrow f = 0 (\text{in } F[X])$$

   In this case we say that α **transcendental over** F. The homomorphism $X \mapsto \alpha$ is an isomorphism, and it extends to an isomorphism $F(X) \to F(\alpha)$

2. The kernel $\neq (0)$, so that $g(\alpha) = 0$ for some nonzero $g \in F[X]$. In this case, we say that α is **algebraic over** F. The polynomials g s.t. $g(\alpha) = 0$ form a nonzero ideal in $F[X]$, which is generated by the monic polynomial f of least degree such $f(\alpha) = 0$. We call f the **minimal polynomial** of α over F.

   Note that $F[X]/(f) \cong F[\alpha]$, since the first is a field, so is the second

Example 1.3. Let $\alpha \in \mathbb{C}$ be s.t. $\alpha^3 - 3\alpha - 1 = 0$. Then $X^3 - 3X - 1$ is monic, irreducible in $\mathbb{Q}[X]$ and has α as a root, and so it is the minimal polynomial of α over $\mathbb{Q}$. The set $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$.

An extension E of F is **algebraic** (E is **algebraic over** F) if all elements of E are algebraic over F; otherwise it is said to be **transcendental**

Proposition 1.9. *Let $E \supset F$ be fields. If E/F is finite, then E is algebraic and finitely generated (as a field) over F; conversely if E is generated over F by a finite set of algebraic elements, then it is finite over F*

Proof. $\Rightarrow$. α of E is transcendental over F iff $1, \alpha, \alpha^2, \ldots$ are linearly independent over F iff $F(\alpha)$ is of infinite degree. Thus if E is finite over F, then every element of E is algebraic over F. If $E \neq F$, then we can pick $\alpha_1 \in E \setminus F$ and compare E and $F[\alpha_1]$ □

1.9 Algebraically closed fields

Let F be a field. A polynomial is said to **split** in $F[X]$ if it is a product of polynomials of degree at most 1 in $F[X]$

Proposition 1.10. *For a field Ω, TFAE*

1. *Every nonconstant polynomial in $\Omega[X]$ splits in $\Omega[X]$*
2. *Every nonconstant polynomial in $\Omega[X]$ has at least one root in Ω*
3. *The irreducible polynomials in $\Omega[X]$ are those of degree 1*
4. *Every field of finite degree over Ω equals Ω*

Definition 1.11.
1. A field Ω is **algebraically closed** if it satisfies the equivalent statements in Proposition 1.10
2. A field Ω is an **algebraic closure** of a subfield F if it is algebraically closed and algebraic over F

Proposition 1.12. *If Ω is algebraic over F and every polynomial $f \in F[X]$ splits in $\Omega[X]$, then Ω is algebraically closed*

Proof. Let f be a nonconstant polynomial in $\Omega[X]$. We know (1.8) that f has a root α in some finite extension Ω' of Ω. Set

$$f = a_n X^n + \cdots + a_0, \quad a_i \in \Omega$$

and consider the fields

$$F \subset F[a_0, \ldots, a_n] \subset F[a_0, \ldots, a_n, \alpha]$$

Each extension generated by a finite set of algebraic elements, and hence is finite (**??**) Therefore α lies in a finite extension of F and so is algebraic over F □