

# Fields and Galois Theory

J. S. Milne

January 8, 2022

## Contents

<b>1</b>	<b>Basic Definitions and Results</b>	<b>1</b>
1.1	The characteristic of a field . . . . .	1
1.2	Review of polynomial rings . . . . .	2
1.3	Factoring polynomials . . . . .	3
1.4	Extensions . . . . .	4
1.5	The subring generated by a subset . . . . .	5
1.6	The subfield generated by a subset . . . . .	5
1.7	Construction of some extensions . . . . .	5
1.8	Stem fields . . . . .	7
1.9	Algebraic and transcendental elements . . . . .	7
1.10	Transcendental numbers . . . . .	9
1.11	Constructions with straight-edge and compass . . . . .	9
1.12	Algebraically closed fields . . . . .	11
1.13	Exercises . . . . .	12
<b>2</b>	<b>Splitting Fields; Multiple Roots</b>	<b>13</b>
2.1	Homomorphisms from simple extensions . . . . .	13
2.2	Splitting fields . . . . .	15
2.3	Multiple roots . . . . .	17
2.4	Exercises . . . . .	20
<b>3</b>	<b>The Fundamental Theorem of Galois Theory</b>	<b>21</b>
3.1	Groups of automorphism of fields . . . . .	21
3.2	Separable, normal, and Galois extensions . . . . .	22
<b>4</b>	<b>Problem</b>	<b>23</b>

# 1 Basic Definitions and Results

## 1.1 The characteristic of a field

Given a field  $F$  and consider a map

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

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  $n \mapsto n \cdot 1_F : \mathbb{Z} \rightarrow F$  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  $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \dots, \mathbb{Q}$  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  $1_R + \dots + 1_R = 0$  ( $p$  terms)

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

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

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

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

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

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

for all  $a_i \in R$ .

When  $F$  is a field, the Frobenius endomorphism is injective

## 1.2 Review of polynomial rings

The  $F$ -algebra  $F[X]$  has the following universal property: for any  $F$ -algebra  $R$  and element  $r \in R$ ,  $\exists!$   $F$ -homomorphism  $\alpha : F[X] \rightarrow R$  s.t.  $\alpha(X) = r$

## 1.3 Factoring polynomials

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

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

*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.*

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

$d \mid a_m c^m$  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  $\pm 1$  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 factorization

$$mnf = g_1 \cdot h_1$$

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 factorization

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

Continuing in this fashion, we eventually remove all the prime factors of  $mn$ .  $\square$

**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  $m$ .  $\square$

**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  $i = 0, \dots, m-1$
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  $b_0, b_1, \dots, b_r$ , which contradicts the condition that  $p$  does not divide  $a_m$ .  $\square$

## 1.4 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**  $E \rightarrow E'$  is a homomorphism  $\varphi : E \rightarrow E'$  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*

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

## 1.5 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*

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

**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 □

## 1.6 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  $F$

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

## 1.7 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

$$P(X) \mapsto P(x) : F[X] \rightarrow F[x]$$

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

$$a_0 + a_1x + \cdots + a_{m-1}x^{m-1}, \quad a_i \in F$$

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  $\mathbb{R}[x]$

## 1.8 Stem fields

Let  $f$  be a monic irreducible polynomial in  $F[X]$ . A pair  $(E, \alpha)$  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  $(E, \alpha)$  with  $E = F[X]/(f) = F[x]$  and  $\alpha = x$ .

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

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

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

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

In other words, the stem field  $(E, \alpha)$  of  $f$  is  $F$ -isomorphic to the standard stem field  $(F[X]/(f), x)$ . It follows that every element of a stem field  $(E, \alpha)$  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  $F[x]$ .

## 1.9 Algebraic and transcendental elements

Let  $F$  be a field. An element  $\alpha$  of an extension  $E$  of  $F$  defines a homomorphism

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

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  $\alpha$  **transcendental over**  $F$ . The homomorphism  $X \mapsto \alpha$  is an isomorphism, and it extends to an isomorphism  $F(X) \rightarrow F(\alpha)$

2. The kernel  $\neq (0)$ , so that  $g(\alpha) = 0$  for some nonzero  $g \in F[X]$ . In this case, we say that  $\alpha$  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  $\alpha$  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  $\alpha$  as a root, and so it is the minimal polynomial of  $\alpha$  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.*  $\Rightarrow$ .  $\alpha$  of  $E$  is transcendental over  $F$  iff  $1, \alpha, \alpha^2, \dots$  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  $F[\alpha_1]$ . If  $E \neq F[\alpha_1]$ , then there exists an  $\alpha_2 \in E \setminus F[\alpha_1]$ , and so on. Since

$$[F[\alpha_1] : F] < [F[\alpha_1, \alpha_2] : F] < \dots < [E : F]$$

this process terminates with  $E = F[\alpha_1, \dots, \alpha_n]$

$\Leftarrow$ : Let  $E = F(\alpha_1, \dots, \alpha_n)$  with  $\alpha_1, \dots, \alpha_n$  algebraic over  $F$ . The extension  $F(\alpha_1)/F$  is finite because  $\alpha_1$  is algebraic over  $F$ . And  $F(\alpha_1, \alpha_2)/F$  is finite because  $\alpha_2$  is algebraic over  $F$  and hence over  $F(\alpha_1)$ . Thus by 1.5  $F(\alpha_1, \alpha_2)$  is finite over  $F$   $\square$

**Corollary 1.10.** *1. If  $E$  is algebraic over  $F$ , then every subring  $R$  of  $E$  containing  $F$  is a field*



2. Consider fields  $L \supset E \supset F$ . If  $L$  is algebraic over  $E$  and  $E$  is algebraic over  $F$ , then  $L$  is algebraic over  $F$

*Proof.* 1. If  $\alpha \in R$ , then  $F[\alpha] \subset R$ . But  $F[\alpha]$  is a field because  $\alpha$  is algebraic, and so  $R$  contains  $\alpha^{-1}$

2. By assumption, every  $\alpha \in L$  is a root of a monic polynomial

$$X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in E[X]$$

Each of the extensions

$$F[a_0, \dots, a_{m-1}, \alpha] \supset F[a_0, \dots, a_{m-1}] \supset \cdots \supset F$$

is finite. Therefore  $F[a_0, \dots, a_{m-1}, \alpha]$  is finite over  $F$ , which implies that  $\alpha$  is algebraic over  $F$

□

## 1.10 Transcendental numbers

**Proposition 1.11.** *The set of algebraic numbers is countable*

**Theorem 1.12.** *The number  $\alpha = \sum \frac{1}{2^{n!}}$  is transcendental*

## 1.11 Constructions with straight-edge and compass

A real number (length) is **constructible** if it can be constructed by forming successive intersections of

- lines drawn through two points already constructed
- circles with center a point already constructed and radius a constructed length

This led them to three famous questions: is it possible to duplicate the cube, trisect an angle, or square the circle by straight-edge and compass constructions? We'll see that the answer to all three is negative.

Let  $F$  be a subfield of  $\mathbb{R}$ . For a positive  $a \in F$ , The  **$F$ -plane** is  $F \times F \subset \mathbb{R} \times \mathbb{R}$

An  **$F$ -line** is a line in  $\mathbb{R} \times \mathbb{R}$  through two points in the  $F$ -plane. These are the lines given by equations

$$ax + by + c = 0, \quad a, b, c \in F$$

An ***F*-circle** is a circle in  $\mathbb{R} \times \mathbb{R}$  with center an *F*-point and radius an element of *F*. These are the circles given by the equations

$$(x - a)^2 + (y - b)^2 = c^2, \quad a, b, c \in F$$

**Lemma 1.13.** *Let  $L \neq L'$  be *F*-lines, and let  $C \neq C'$  be *F*-circles*

1.  $L \cap L' = \emptyset$  or consists of a single *F*-point
2.  $L \cap C = \emptyset$  or consists of one or two points in the  $F[\sqrt{e}]$ -plane, some  $e \in F$ ,  $e > 0$
3.  $C \cap C' = \emptyset$  or consists of one or two points in the  $F[\sqrt{e}]$ -plane, some  $e \in F$ ,  $e > 0$

**Lemma 1.14.** 1. *If  $c$  and  $d$  are constructible, then so also are  $c + d$ ,  $-c$ ,  $cd$  and  $\frac{c}{d}$ ,  $d \neq 0$*

2. *If  $c > 0$  is constructible, then so is  $\sqrt{c}$*

*Proof.* First show that it is possible to construct a line perpendicular to a given line through a given point (link), and then a line parallel to a given line through a given point (link). Hence it is possible to construct a triangle similar to a given one on a side with given length.

$\sqrt{c}$  link

□

**Theorem 1.15.** 1. *The set of constructible numbers is a field*

2. *A number  $\alpha$  is constructible iff it is contained in a subfield of  $\mathbb{R}$  of the form*

$$\mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_r}], \quad a_i \in \mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_{i-1}}], \quad a_i > 0$$

**Corollary 1.16.** *If  $\alpha$  is constructible, then  $\alpha$  is algebraic over  $\mathbb{Q}$ , and  $[\mathbb{Q}[\alpha] : \mathbb{Q}]$  is a power of 2*

*Proof.*  $[\mathbb{Q}[\alpha] : \mathbb{Q}]$  divides  $[\mathbb{Q}[\sqrt{a_1}] \dots [\sqrt{a_r}] : \mathbb{Q}]$  and  $[\mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_r}] : \mathbb{Q}]$  is a power of 2

□

**Corollary 1.17.** *It is impossible to duplicate the cube by straight-edge and compass constructions*

*Proof.* This requires constructing the real root of the polynomial  $X^3 - 2$ . But this polynomial is irreducible and  $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$

□

**Corollary 1.18.** *In general, it is impossible to trisect an angle by straight-edge and compass constructions*

*Proof.* Knowing an angle is equivalent to knowing the cosine of the angle. Therefore, to trisect  $3\alpha$ , we have to construct a solution to

$$\cos 3\alpha = 4 \cos^3 \alpha - 3 \cos \alpha$$

For example take  $3\alpha = 60^\circ$ . As  $\cos 60^\circ = 0.5$ , we have to solve  $8x^3 - 6x - 1 = 0$ , which is irreducible, and so  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$   $\square$

**Corollary 1.19.** *It is impossible to square the circle by straight-edge and compass constructions*

*Proof.* A square with the same area as a circle of radius  $r$  has side  $\sqrt{\pi}r$ . Since  $\pi$  is transcendental, so also is  $\sqrt{\pi}$   $\square$

$$X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \dots + 1)$$

**Lemma 1.20.** *If  $p$  is prime, then  $X^{p-1} + \dots + 1$  is irreducible; hence  $\mathbb{Q}[e^{2\pi i/p}]$  has degree  $p - 1$  over  $\mathbb{Q}$*

*Proof.* Let  $f(X) = (X^p - 1)/(X - 1) = X^{p-1} + \dots + 1$ ; then

$$f(X + 1) = \frac{(X + 1)^p - 1}{X} = X^{p-1} + \dots + a_i X^i + \dots + p$$

with  $a_i = \binom{p}{i+1}$

$p \mid a_i$  for  $i = 1, \dots, p - 2$ , and so  $f(X + 1)$  is irreducible by Eisenstein's criterion 1.4. This implies that  $f(X)$  is irreducible  $\square$

## 1.12 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 1.21.** *For a field  $\Omega$ , 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  $\Omega$*
3. *The irreducible polynomials in  $\Omega[X]$  are those of degree 1*
4. *Every field of finite degree over  $\Omega$  equals  $\Omega$*

*Proof.*  $3 \rightarrow 4$ : Let  $E$  be a finite extension of  $\Omega$ , and let  $\alpha \in E$ . The minimal polynomial of  $\alpha$ , being irreducible, has degree 1, and so  $\alpha \in \Omega$

$4 \rightarrow 3$ : Let  $f$  be an irreducible polynomial of  $\Omega$ , then  $\Omega[X]/(f)$  is an extension of  $\Omega$  of degree  $\deg(f)$ , and so  $\deg(f) = 1$   $\square$

**Definition 1.22.** 1. A field  $\Omega$  is **algebraically closed** if it satisfies the equivalent statements in Proposition 1.21

2. A field  $\Omega$  is an **algebraic closure** of a subfield  $F$  if it is algebraically closed and algebraic over  $F$

**Proposition 1.23.** *If  $\Omega$  is algebraic over  $F$  and every polynomial  $f \in F[X]$  splits in  $\Omega[X]$ , then  $\Omega$  is algebraically closed*

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

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

and consider the fields

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

Each extension generated by a finite set of algebraic elements, and hence is finite (??) Therefore  $\alpha$  lies in a finite extension of  $F$  and so is algebraic over  $F$  - it is a root of a polynomial  $g$  with coefficients in  $F$ . By assumption,  $g$  splits in  $\Omega[X]$ , and so the root of  $g$  in  $\Omega'$  all lie in  $\Omega$ . In particular,  $\alpha \in \Omega$   $\square$

**Proposition 1.24.** *Let  $\Omega \supset F$ , then*

$$\{\alpha \in \Omega \mid \alpha \text{ algebraic over } F\}$$

*is a field*

*Proof.* If  $\alpha$  and  $\beta$  are algebraic over  $F$ , then  $F[\alpha, \beta]$  is a field of finite degree over  $F$ . Thus every element of  $F[\alpha, \beta]$  is algebraic over  $F$ , in particular  $\alpha \pm \beta$ ,  $\alpha/\beta$  and  $\alpha\beta$  are algebraic over  $F$   $\square$

The field constructed in the proposition is called the **algebraic closure of  $F$  in  $\Omega$**

**Corollary 1.25.**  $\Omega \models ACF$ , for any subfield  $F$  of  $\Omega$ , the algebraic closure  $E$  of  $F$  in  $\Omega$  is an algebraic closure of  $F$

*Proof.* It is algebraic over  $F$  by definition. Every polynomial in  $F[X]$  splits in  $\Omega[X]$  and has its roots in  $E$ , and so splits in  $E[X]$ . Now apply Proposition 1.23  $\square$

### 1.13 Exercises

1.  $f(x) = x^3 - \alpha^2 + \alpha + 2$ ,  $f(x)$  is irreducible in  $\mathbb{Q}[x]$ . Thus  $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/(f)$ , which is a field  
 $(\alpha - 1)^{-1} = -\frac{1}{3}(\alpha^2 + 1)$

2. 4

3.

- (a)  $f(X) - f(a) = q(X)(X - a) + r(X)$  and  $\deg r < 1$ , hence  $\deg r = 0$
- (b) obvious
- (c) obvious

5. Let  $g$  be the irreducible factor in  $E[X]$  and let  $(L, \alpha)$  be a stem field for  $g$  over  $E$ . Then  $L = E[\alpha] \cong E/(f)$ . Then  $m \mid [E[\alpha] : F]$ . Since  $f(\alpha) = 0$ .  $[F[\alpha] : F] = n$ . Now  $n \mid [L : F]$ . We deduce that  $[L : F] = mn$  and  $[L : E] = n$ . But  $[E[\alpha] : E] = \deg(g)$ . Hence  $\deg(g) = \deg(f)$

$$\begin{array}{c} E[\alpha] \xrightarrow{\leq n} E \xrightarrow{m} F \\ | \\ F[\alpha] \\ | \quad n \\ F \end{array}$$

6. The polynomials  $f(X) - 1$  and  $f(X) + 1$  have only finitely many roots, and so there is  $n \in \mathbb{Z}$  s.t.  $f(n) \neq \pm 1$ , then there is prime  $p$  s.t.  $p \mid f(n)$ . Hence  $f(x)$  is reducible in  $\mathbb{F}_p[x]$
7. Let  $f(x) = x^3 - 2$ , then  $R \cong \mathbb{Q}[x]/(f)$ .

## 2 Splitting Fields; Multiple Roots

### 2.1 Homomorphisms from simple extensions

Let  $F$  be a field and  $E, E'$  fields containing  $F$ . Recall that an  $F$ -homomorphism is a homomorphism  $\varphi : E \rightarrow E'$  s.t.  $\varphi(a) = a$  for all  $a \in F$ . Thus an  $F$ -homomorphism  $\varphi$  maps a polynomial

$$\sum a_{i_1 \dots i_m} \alpha_1^{i_1} \dots \alpha_m^{i_m}, \quad a_{i_1 \dots i_m} \in F, \quad \alpha_i \in E$$

to

$$\sum a_{i_1 \dots i_m} \varphi(\alpha_1)^{i_1} \dots \varphi(\alpha_m)^{i_m}$$

An  **$F$ -isomorphism** is a bijective  $F$ -homomorphism

An  $F$ -homomorphism  $E \rightarrow E'$  of fields is, in particular, an injective  $F$ -linear map of  $F$ -vector spaces, and so it is an  $F$ -isomorphism if  $E$  and  $E'$  have the same finite degree over  $F$

**Proposition 2.1.** *Let  $F(\alpha)$  be a simple extension of  $F$  and  $\Omega$  a second extension of  $F$*

1. *Let  $\alpha$  be transcendental over  $F$ . For every  $F$ -homomorphism  $\varphi : F(\alpha) \rightarrow \Omega$ ,  $\varphi(\alpha)$  is transcendental over  $F$ , and the map  $\varphi \mapsto \varphi(\alpha)$  defines a one-to-one correspondence*

$$\{F\text{-homomorphisms } F(\alpha) \rightarrow \Omega\} \leftrightarrow \{\text{elements of } \Omega \text{ transcendental over } F\}$$

2. *Let  $\alpha$  be algebraic over  $F$  with minimal polynomial  $f(X)$ . For every  $F$ -homomorphism  $\varphi : F[\alpha] \rightarrow \Omega$ ,  $\varphi(\alpha)$  is a root of  $f(X)$  in  $\Omega$ , and the map  $\varphi \mapsto \varphi(\alpha)$  defines a one-to-one correspondence*

$$\{F\text{-homomorphisms } \varphi : F[\alpha] \rightarrow \Omega\} \leftrightarrow \{\text{roots of } f \text{ in } \Omega\}$$

*In particular, the number of such maps is the number of distinct roots of  $f$  in  $\Omega$*

*Proof.* 1. To say that  $\alpha$  is transcendental over  $F$  means that  $F[\alpha]$  is isomorphic to the polynomial ring in the symbol  $\alpha$ . Therefore for every  $\gamma \in \Omega$ , there is a unique  $F$ -homomorphism  $\varphi : F[\alpha] \rightarrow \Omega$  s.t.  $\varphi(\alpha) = \gamma$ . This  $\varphi$  extends (uniquely) to the field of fractions  $F(\alpha)$  iff nonzero elements of  $F[\alpha]$  are sent to nonzero elements of  $\Omega$ , which is the case iff  $\gamma$  is transcendental over  $F$ . Thus there is a one-to-one correspondence between

$$(a) \ F(\alpha) \rightarrow \Omega$$

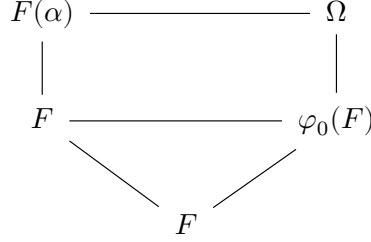
$$(b) \ \varphi : F[\alpha] \rightarrow \Omega \text{ s.t. } \varphi(\alpha) \text{ is transcendental}$$

$$(c) \ \text{the transcendental elements of } \Omega$$

2. If  $\gamma \in \Omega$  is a root of  $f(X)$ , then the map  $F[X] \rightarrow \Omega$ ,  $g(X) \mapsto g(\gamma)$ , factor through  $F[X]/(f(X))$ . When composed with the inverse of the canonical isomorphism  $F[\alpha] \rightarrow F[X]/(f(X))$ , this becomes a homomorphism  $F[\alpha] \rightarrow \Omega$  sending  $\alpha$  to  $\gamma$

□

**Proposition 2.2.** Let  $F(\alpha)$  be a simple extension of  $F$  and  $\varphi_0 : F \rightarrow \Omega$  a homomorphism from  $F$  into a second field  $\Omega$



1. if  $\alpha$  is transcendental over  $F$ , then the map  $\varphi \mapsto \varphi(\alpha)$  defines a one-to-one correspondence

$$\{\text{extensions } \varphi : F(\alpha) \rightarrow \Omega \text{ of } \varphi_0\} \leftrightarrow \{\text{elements of } \Omega \text{ transcendental over } \varphi_0(F)\}$$

2. If  $\alpha$  is algebraic over  $F$ , with minimal polynomial  $f(X)$ , then the map  $\varphi \mapsto \varphi(\alpha)$  defines a one-to-one correspondence

$$\{\text{extensions } \varphi : F[\alpha] \rightarrow \Omega \text{ of } \varphi_0\} \leftrightarrow \{\text{roots of } \varphi_0 f \text{ in } \Omega\}$$

## 2.2 Splitting fields

Let  $f$  be a polynomial with coefficients in  $F$ . A field  $E \supseteq F$  is said to **split**  $f$  if  $f$  splits in  $E[X]$ , i.e.,

$$f(X) = a \prod_{i=1}^m (X - \alpha_i), \quad \alpha_i \in E$$

If  $E$  splits  $f$  and is generated by the roots of  $f$

$$E = F[\alpha_1, \dots, \alpha_m]$$

then it is called a **splitting** or **root field** for  $f$

**Proposition 2.3.** Every polynomial  $f \in F[X]$  has a splitting field  $E_f$ , and

$$[E_f : F] \leq (\deg f)!$$

*Proof.* Let  $F_1 = F[\alpha_1]$  be a stem field for some monic irreducible factor of  $f$  in  $F[X]$ . Then  $f(\alpha_1) = 0$ , and we let  $F_2 = F_1[\alpha_2]$  be a stem field for some monic irreducible factor of  $f(X)/(X - \alpha_1)$  in  $F_1[X]$ . Continuing in this fashion, we arrive at a splitting field  $E_f$ . Let  $n = \deg f$ . Then  $[F_1 : F] = \deg g_1 \leq n$ ,  $[F_2 : F_1] \leq n - 1$ , and so  $[E_f : F] \leq n!$   $\square$

- Example 2.1.** 1. Let  $f(X) = (X^p - 1)/(X - 1) \in \mathbb{Q}[X]$ ,  $p$  prime. If  $\xi$  is one root of  $f$ , then the remaining roots are  $\xi^2, \xi^3, \dots, \xi^{p-1}$ , and so the splitting field of  $f$  is  $\mathbb{Q}[\xi]$
2. Let  $F$  have characteristic  $p \neq 0$ , and let  $f = X^p - X - a \in F[X]$ . If  $\alpha$  is one root of  $f$  in some extension of  $F$ , then the remaining roots are  $\alpha + 1, \dots, \alpha + p - 1$ , and so the splitting field of  $f$  is  $F[\alpha]$
3. If  $\alpha$  is one root of  $X^n - a$ , then the remaining roots are all of the form  $\xi\alpha$ , where  $\xi^n = 1$ . Therefore  $F[\alpha]$  is a splitting field for  $X^n - a$  iff  $F$  contains all the  $n$ th roots of 1. Note that if  $p$  is the characteristic of  $F$ , then  $X^p - 1 = (X - 1)^p$ , and so  $F$  automatically contains all the  $p$ th roots of 1

**Proposition 2.4.** *Let  $f \in F[X]$ . Let  $E$  be the extension of  $F$  generated by the roots of  $f$  in  $E$ , and let  $\Omega$  be an extension of  $F$  splitting  $f$*

1. *There exists an  $F$ -homomorphism  $\varphi : E \rightarrow \Omega$ ; the number of such homomorphisms is at most  $[E : F]$ , and equals  $[E : F]$  if  $f$  has distinct roots in  $\Omega$*
2. *If  $E$  and  $\Omega$  are both splitting fields for  $f$ , then every  $F$ -homomorphism  $E \rightarrow \Omega$  is an isomorphism. In particular, any two splitting fields for  $f$  are  $F$ -isomorphic*

*Proof.* We may assume that  $f$  is monic

Let  $F, f, \Omega$  be as in the statement of the proposition, let  $L$  be a subfield of  $\Omega$  containing  $F$ , and let  $g$  be a monic factor of  $f$  in  $L[X]$ ; as  $g$  divides  $f$  in  $\Omega[X]$ , it is a product of certain number of the factors  $X - \beta_i$  of  $f$  in  $\Omega[X]$ ; in particular, we see that  $g$  splits in  $\Omega$ , and that it has distinct roots in  $\Omega$  if  $f$  does

1.  $E = F[\alpha_1, \dots, \alpha_m]$ , each  $\alpha_i$  a root of  $f(X)$  in  $E$ . The minimal polynomial of  $\alpha_1$  is an irreducible polynomial  $f_1$  dividing  $f$ . From the initial observation with  $L = F$ , we see that  $f_1$  splits in  $\Omega$ , and that its roots are distinct if the roots of  $f$  are distinct. According to Proposition 2.1, there exists an  $F$ -homomorphism  $\varphi_1 : F[\alpha_1] \rightarrow \Omega$  and the number of such homomorphisms is at most  $[F[\alpha_1] : F]$ , with equality holding when  $f$  has distinct roots in  $\Omega$

The minimal polynomial of  $\alpha_2$  over  $F[\alpha_1]$  is an irreducible factor  $f_2$  of  $f$  in  $F[\alpha_1][X]$ . On applying the initial observation with  $L = \varphi_1 F[\alpha_1]$  and  $g = \varphi_1 f_2$  we see that  $\varphi_1 f_2$  splits in  $\Omega$ . According to Proposition



2.2, each  $\varphi_1$  extends to a homomorphism  $\varphi_2 : F[\alpha_1, \alpha_2] \rightarrow \Omega$ , and the number of extensions is at most  $[F[\alpha_1, \alpha_2] : F[\alpha_1]]$ , with equality holding when  $f$  has distinct roots in  $\Omega$

On combining these statements we conclude that there exists an  $F$ -homomorphism

$$\varphi : F[\alpha_1, \alpha_2] \rightarrow \Omega$$

and that the number of such homomorphisms is at most  $[F[\alpha_1, \alpha_2] : F]$ , with equality holding if  $f$  has distinct roots in  $\Omega$

2. Every  $F$ -homomorphism  $E \rightarrow \Omega$  is injective **if  $\alpha_1 \neq \alpha_2$ , then  $\alpha_1$  is not a root of  $f_2$ , otherwise  $f_2$  is not minimal in  $F[\alpha_1][X]$ . Thus  $f_2(\varphi_2\alpha_2) = 0 \neq f_2(\varphi_2\alpha_1)$ , and so  $\varphi_2\alpha_2 \neq \varphi_2\alpha_1$ . Thus every  $F$ -homomorphism is injective.** And so, if there exists such a homomorphism, then  $[E : F] \leq [\Omega : F]$ . If  $E$  and  $\Omega$  are both splitting fields for  $f$ , then 1 shows that there exist homomorphism  $E \hookrightarrow \Omega$ , and so  $[E : F] = [\Omega : F]$

□

**Corollary 2.5.** *Let  $E$  and  $L$  be extension of  $F$ , with  $E$  finite over  $F$*

1. *The number of  $F$ -homomorphisms  $E \rightarrow L$  is at most  $[E : F]$*
2. *There exists a finite extension  $\Omega/L$  and an  $F$ -homomorphism  $E \rightarrow \Omega$*

*Proof.* Write  $E = F[\alpha_1, \dots, \alpha_m]$ , and let  $f \in F[X]$  be the product of the minimal polynomials of the  $\alpha_i$ ; thus  $E$  is generated over  $F$  by roots of  $f$ . Let  $\Omega$  be a splitting field for  $f$  regarded as an element of  $L[X]$ . The proposition shows that there exists an  $F$ -homomorphism  $E \rightarrow \Omega$ , and the number of such homomorphisms is  $\leq [E : F]$ . This proves (2). And since an  $F$ -homomorphism  $E \rightarrow L$  can be regarded as an  $F$ -homomorphism  $E \rightarrow \Omega$ , it also proves (1) □

*Remark.* 1. Let  $E_1, \dots, E_m$  be finite extensions of  $F$ , and let  $L$  be an extension of  $F$ . From the corollary we see that there exists a finite extension  $L_1/L$  s.t.  $L_1$  contains an isomorphic image of  $E_1$ ; then there exists a finite extension  $L_2/L_1$  s.t.  $L_2$  contains an isomorphic image of  $E_2$ . Finally we can find a finite extension  $\Omega/L$  s.t.  $\Omega$  contains an isomorphic copy of each  $E_i$

2.

### 2.3 Multiple roots

Even when polynomials in  $F[X]$  have no common factor in  $F[X]$ , one might expect that they could acquire a common factor in  $\Omega[X]$  for some  $\Omega \supset F$ . In fact, this doesn't happen

**Proposition 2.6.** *Let  $f$  and  $g$  be polynomials in  $F[X]$ , and let  $\Omega$  be an extension of  $F$ . If  $r(X)$  is the gcd of  $f$  and  $g$  computed in  $F[X]$ , then it is also the gcd of  $f$  and  $g$  in  $\Omega[X]$ . In particular, distinct monic irreducible polynomials in  $F[X]$  do not acquire a common root in any extension of  $F$*

*Proof.* Let  $r_F(X)$  and  $r_\Omega(X)$  be the greatest common divisors of  $f$  and  $g$  in  $F[X]$  and  $\Omega[X]$  respectively. Certainly  $r_F(X) \mid r_\Omega(X)$  in  $\Omega[X]$ , but Euclid's algorithm shows that there are polynomials  $a$  and  $b$  in  $F[X]$  s.t.

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

and so  $r_\Omega(X)$  divides  $r_F(X)$  in  $\Omega[X]$  □

The proposition allows us to speak of the gcd of  $f$  and  $g$  without reference to a field

Let  $f \in F[X]$ , then  $f$  splits into linear factors

$$f(X) = a \prod_{i=1}^r (X - \alpha_i)^{m_i}, \alpha_i \text{ distinct}, m_i \geq 1, \sum_{i=1}^r m_i = \deg(f)$$

in  $E[X]$  for some extension  $E$  of  $F$  (2.3). We say that  $\alpha_i$  is a root of  $f$  of **multiplicity**  $m_i$  in  $E$ . If  $m_i > 1$ , then  $\alpha_i$  is said to be a **multiple root** of  $f$ , and otherwise it is a **simple root**

Let  $E$  and  $E'$  be splitting fields for  $F$ , and suppose that  $f(X) = a \prod_{i=1}^r (X - \alpha_i)^{m_i}$  in  $E[X]$  and  $f(X) = a' \prod_{i=1}^{r'} (X - \alpha'_i)^{m'_i}$  in  $E'[X]$ . Let  $\varphi : E \rightarrow E'$  be an  $F$ -isomorphism, which exists by 2.4, and extend it to an isomorphism  $E[X] \rightarrow E'[X]$  by sending  $X$  to  $X$ . Then  $\varphi$  maps the factorization of  $f$  in  $E[X]$  onto a factorization

$$f(X) = \varphi(a) \prod_{i=1}^r (X - \varphi(\alpha_i))^{m_i}$$

in  $E'[X]$ . By unique factorization, this coincides with the earlier factorization in  $E'[X]$  up to a renumbering of the  $\alpha_i$ . Therefore  $r = r'$  and

$$\{m_1, \dots, m_r\} = \{m'_1, \dots, m'_r\}$$

$f$  has a **multiple root** when at least one of the  $m_i > 1$ , and that  $f$  has **only simple roots** when all  $m_i = 1$ . Thus “ $f$  has a multiple root” means “ $f$  has a multiple root in one, hence every, extension of  $F$  splitting  $f$ ”, and similarly for “ $f$  has only simple roots”

When will an irreducible polynomial has a multiple root

**Example 2.2.** Let  $F$  be of characteristic  $p \neq 0$ , and assume that  $F$  contains an element  $a$  that is not a  $p$ th-power,  $a = T$  in the field  $\mathbb{F}_p(T)$ . Then  $X^p - a$  is irreducible, but  $X^p - a = (X - \alpha)^p$  in its splitting field. Thus an irreducible polynomial can have multiple roots

The derivative of a polynomial  $f(X) = \sum a_i X^i$  is defined to be  $f'(X) = \sum i a_i X^{i-1}$ .

**Proposition 2.7.** For a nonconstant irreducible polynomial  $f$  in  $F[X]$ , TFAE

1.  $f$  has a multiple root
2.  $\gcd(f, f') \neq 1$
3.  $F$  has nonzero characteristic  $p$  and  $f$  is a polynomial in  $X^p$
4. all the roots of  $f$  are multiple

*Proof.*  $2 \rightarrow 3$ : as  $f$  is irreducible and  $\deg(f') < \deg(f)$ ,  $f' = 0$  in  $F$ .

$3 \rightarrow 4$ .  $f(X) = g(X^p)$ . Suppose  $g(X) = \prod_i (X - a_i)^{m_i}$  in some extension field. Then  $f(X) = g(X^p) = \prod_i (X^p - a_i) = \prod_i (X - a_i)^{p m_i}$   $\square$

**Proposition 2.8.** For a nonzero polynomial  $f \in F[X]$ , TFAE

1.  $\gcd(f, f') = 1$  in  $F[X]$
2.  $f$  only has simple roots

*Proof.* Let  $\Omega$  be an extension of  $F$  splitting  $f$ . If a root  $\alpha$  of  $f$  in  $\Omega$  is multiple iff it is also a root of  $f'$   $\square$

**Definition 2.9.** A polynomial is **separable** if it is nonzero and satisfied the equivalent conditions in 2.8

**Definition 2.10.** A field  $F$  is **perfect** if it has characteristic zero or it has characteristic  $p$  and every element of  $F$  is a  $p$ th power

Thus  $F$  is perfect iff  $F = F^p$

**Proposition 2.11.** *A field  $F$  is perfect iff every irreducible polynomial in  $F[X]$  is separable*

*Proof.* If  $F$  has characteristic 0, the statement is obvious. If  $F$  has characteristic  $p \neq 0$ . If  $F$  contains an element  $a$  that is not a  $p$ th power, then  $X^p - a$  is irreducible in  $F[X]$  but not separable

If  $F$  is perfect and  $f$  is not separable, then  $f$  is a polynomial in  $X^p$ . Then  $f$  can't be irreducible

If every element of  $F$  is a  $p$ th power, then every polynomial in  $X^p$  with coefficients in  $F$  is a  $p$ th power in  $F[X]$

$$\sum a_i X^{ip} = (\sum b_i X^i)^p, \quad a_i = b_i^p$$

and so it is not irreducible □

- Example 2.3.**
1. A finite field  $F$  is perfect, because the Frobenius endomorphism  $a \mapsto a^p : F \rightarrow F$  is injective and therefore surjective
  2. A field that can be written as a union of perfect fields is perfect. Therefore, every field algebraic over  $\mathbb{F}_p$  is perfect
  3. Every algebraically closed field is perfect
  4. If  $F_0$  has characteristic  $p \neq 0$ , then  $F = F_0(X)$  is not perfect, because  $X$  is not a  $p$ th power

## 2.4 Exercises

*Exercise 2.4.1.* Let  $F$  be a field of characteristic  $\neq 2$

1. Let  $E$  be a quadratic extension of  $F$ ; show that

$$S(E) = \{a \in F^\times \mid a \text{ is a square in } E\}$$

is a subgroup of  $F^\times$  containing  $F^{\times 2}$

2. Let  $E$  and  $E'$  be quadratic extension of  $F$ ; show that there exists an  $F$ -isomorphism  $\varphi : E \rightarrow E'$  iff  $S(E) = S(E')$
3. Show that there is an infinite sequence of fields  $E_1, E_2, \dots$  with  $E_i$  a quadratic extension of  $\mathbb{Q}$  s.t.  $E_i$  is not isomorphic to  $E_j$  for  $i \neq j$
4. Let  $p$  be an odd prime. Show that, up to isomorphism, there is exactly one field with  $p^2$  elements

*Exercise 2.4.2.* Construct a splitting field for  $X^5 - 2$  over  $\mathbb{Q}$ . What is its degree over  $\mathbb{Q}$

2.4.6

*Exercise 2.4.3.* 1. Let  $F$  be a field of characteristic  $p$ . Show that if  $X^p - X - a$  is reducible in  $F[X]$ , then it splits into distinct factors in  $F[X]$

2. For every prime  $p$ , show that  $X^p - X - 1$  is irreducible in  $\mathbb{Q}[X]$

*Proof.*  $x^5 - 2$  is irreducible in  $\mathbb{Q}$

Let  $\xi^5 = 1$ , and  $\alpha = \sqrt[5]{2}$ , then the five solutions are  $\alpha, \xi\alpha, \xi^2\alpha, \xi^3\alpha, \xi^4\alpha$ . Note that  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 5$  and  $[\mathbb{Q}[\xi] : \mathbb{Q}] = 4$ . Then  $[\mathbb{Q}[\alpha, \xi] : \mathbb{Q}[\alpha]] \leq 4$ . Hence  $[\mathbb{Q}[\alpha, \xi] : \mathbb{Q}] = 20$   $\square$

*Exercise 2.4.4.* Find a splitting field of  $X^{p^m} - 1 \in \mathbb{F}_p[X]$ . What is its degree over  $\mathbb{F}_p$

*Exercise 2.4.5.* Let  $f \in F[X]$ , where  $F$  is a field of characteristic 0. Let  $d(X) = \gcd(f, f')$ . Show that  $g(X) = f(X)d(X)^{-1}$  has the same roots as  $f(X)$ , and these are all simple roots of  $g(X)$

*Exercise 2.4.6.* Let  $f(X)$  be an irreducible polynomial in  $F[X]$ , where  $F$  has characteristic  $p$ . Show that  $f(X)$  can be written  $g(X) = g(X^{p^e})$  where  $g(X)$  is irreducible and separable. Deduce that every root of  $f(X)$  has the same multiplicity  $p^e$  in any splitting field

*Proof.* If  $f$  is not separable, then  $f$  is a polynomial in  $X^p$ , say  $f(X) = g(X^p)$ . If  $g$  is not separable, then  $g(X^p) = h(X^{2p})$ . This process will end since each polynomial has finite degree.  $\square$

### 3 The Fundamental Theorem of Galois Theory

#### 3.1 Groups of automorphism of fields

Consider fields  $E \supset F$ . An  $F$ -isomorphism  $E \rightarrow E$  is called an  **$F$ -automorphism** of  $E$ . The  $F$ -automorphisms of  $E$  form a group, which we denote  $\text{Aut}(E/F)$

**Example 3.1.** Let  $E = \mathbb{C}(X)$ . A  $\mathbb{C}$ -automorphism of  $E$  sends  $X$  to another generator of  $E$  over  $\mathbb{C}$ . It follows from ?? below that these are exactly the elements  $\frac{aX+b}{cX+d}$ ,  $ad - bc \neq 0$ . Therefore  $\text{Aut}(E/\mathbb{C})$  consists of the maps  $f(X) \mapsto f\left(\frac{aX+b}{cX+d}\right)$ ,  $ad - bc \neq 0$ , and so

$$\text{Aut}(E/\mathbb{C}) \cong \text{PGL}_2(\mathbb{C})$$

the group of invertible  $2 \times 2$  matrices with complex coefficients modulo its centre.

**Proposition 3.1.** *Let  $E$  be a splitting field of a separable polynomial  $f$  in  $F[X]$ ; then  $\text{Aut}(E/F)$  has order  $[E : F]$*

*Proof.* As  $f$  is separable, it has  $\deg f$  different roots in  $E$ . Therefore Proposition 2.4 shows that the number of  $F$ -homomorphisms  $E \rightarrow E$  is  $[E : F]$ . Because  $E$  is finite over  $F$ , all such homomorphisms are isomorphisms  $\square$

When  $G$  is a group of automorphisms of a field  $E$ , we set

$$E^G = \text{Inv}(G) = \{\alpha \in E \mid \sigma\alpha = \alpha, \forall \sigma \in G\}$$

It is a subfield of  $E$ , called the subfield of  $G$ -**invariants** of  $E$  or the **fixed field** of  $G$

**Theorem 3.2** (E. Artin). *Let  $G$  be a finite group of automorphisms of a field  $E$ , then*

$$[E : E^G] \leq (G : 1)$$

*Proof.* Let  $F = E^G$ , and let  $G = \{\sigma_1, \dots, \sigma_m\}$  with  $\sigma_1$  the identity map. It suffices to show that every set  $\{\alpha_1, \dots, \alpha_n\}$  of elements of  $E$  with  $n > m$  is linearly dependent over  $F$ . For such a set, consider the system of linear equations

$$\begin{aligned} \sigma_1(\alpha_1)X_1 + \dots + \sigma_1(\alpha_n)X_n &= 0 \\ &\vdots \\ \sigma_m(\alpha_1)X_1 + \dots + \sigma_m(\alpha_n)X_n &= 0 \end{aligned}$$

with coefficients in  $E$ . There are  $m$  equations and  $n > m$  unknowns, and hence there are nontrivial solutions in  $E$ . We choose one  $(c_1, \dots, c_n)$  having the fewest possible nonzero elements. After renumbering the  $\alpha_i$ , we may choose that  $c_1 \neq 0$ , and then, after multiplying by a scalar, that  $c_1 \in F$ . **Let  $d_i = -(\sigma_i(\alpha_1^{-1}\alpha_2)c_2 + \dots + \sigma_i(\alpha_1^{-1}\alpha_n)c_n)$ . Then  $c_1 = d_i$  for  $i = 1, \dots, n$ , for any  $i \in \{1, \dots, n\}$ ,  $\sigma_i(c_1) = \sigma_i(d_1) = d_i = c_1$ . Thus  $c_1 \in F$ . With these normalizations, we'll show that all  $c_i \in F$ , and so the first equation**

$$\alpha_1 c_1 + \dots + \alpha_n c_n = 0$$

is a linear relation on the  $\alpha_i$

If not all  $c_i$  are in  $F$ , then  $\sigma_k(c_i) \neq c_i$  for some  $k \neq 1$  and  $i \neq 1$ . On applying  $\sigma_k$  to the system of linear equations

$$\begin{aligned}\sigma_1(\alpha_1)c_1 + \cdots + \sigma_1(\alpha_n)c_n &= 0 \\ &\vdots \\ \sigma_m(\alpha_1)c_1 + \cdots + \sigma_m(\alpha_n)c_n &= 0\end{aligned}$$

and using that  $\{\sigma_k\sigma_1, \dots, \sigma_k\sigma_m\} = \{\sigma_1, \dots, \sigma_m\}$ , we find that

$$(c_1, \sigma_k(c_2), \dots, \sigma_k(c_n))$$

is also a solution to the system of equations. On subtracting it from the first solution, we obtain a solution  $(0, \dots, c_i - \sigma_k(c_i), \dots)$ , which is nonzero, but has more zeros than the first solutions - contradiction **If  $c_i = 0$ , then  $\sigma_k(c_i) = 0$  since this is an automorphism**  $\square$

**Corollary 3.3.** *Let  $G$  be a finite group of automorphisms of a field  $E$ ; then*

$$G = \text{Aut}(E/E^G)$$

*Proof.* As  $G \subset \text{Aut}(E/E^G)$ , we have inequalities

$$[E : E^G] \leq (G : 1) \leq (\text{Aut}(E/E^G) : 1) \leq [E : E^G]$$

last inequality by 2.5 (1)  $\square$

### 3.2 Separable, normal, and Galois extensions

**Definition 3.4.** An algebraic extension  $E/F$  is **separable** if the minimal polynomial of every element of  $E$  is separable; otherwise it is **inseparable**

Thus, an algebraic extension  $E/F$  is separable if every irreducible polynomial in  $F[X]$  having at least one root in  $E$  is separable, and it is inseparable if

- $F$  is nonperfect, and in particular has characteristic  $p \neq 0$ , and
- there is an element  $\alpha \in E$  whose minimal polynomial is of the form  $g(X^p)$ ,  $g \in F[X]$

$\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$  is inseparable extension because  $T$  has minimal polynomial  $X^p - T^p$

**Definition 3.5.** An extension  $E/F$  is **normal** if it is algebraic and the minimal polynomial of every element of  $E$  splits in  $E[X]$

an algebraic extension  $E/F \Leftrightarrow$  every irreducible polynomial  $f \in F[X]$  having at least one root in  $E$  splits in  $E[X]$

Let  $f$  be a monic irreducible polynomial of degree  $m$  in  $F[X]$ , and let  $E$  be an algebraic extension of  $F$ . If  $f$  has a root in  $E$ , so that it is the minimal polynomial of an element of  $E$ , then

$$\left. \begin{array}{ll} E/F \text{ separable} & \Rightarrow \\ E/F \text{ normal} & \Rightarrow \end{array} \right\} \begin{array}{l} f \text{ has only simple roots} \\ f \text{ splits in } E \end{array} \Rightarrow f \text{ has } m \text{ distinct roots in } E$$

## 4 Problem

2.3