

# APPLICATIONS OF FIELD THEORY

BENJAMIN KLOPSCH

ABSTRACT. I prepared these notes in parallel with designing and delivering the actual lectures at Royal Holloway, University of London, during the Autumn Term 2007. There is likely to be room for corrections and improvements. Any form of feedback is welcome.

## WHAT THE COURSE IS ABOUT

**Summary.** The course covers several aspects of field theory, with a view towards applications in the context of finite fields. As a starting point we choose the classical topic of Euclidean constructions with compasses and straight edge. Then we introduce basic notions, mainly from Linear Algebra, to study general field extensions. A key result is the Theorem of Kronecker which describes simple extensions. We provide a short review of polynomial rings over fields, with an emphasis on the notion of irreducibility. Next we turn our attention towards finite fields. The main result is the existence and uniqueness of finite fields of prescribed cardinality. We discuss the discrete logarithm problem and its applications to cryptography. We go on to study cyclotomic polynomials, which are used to give an elementary proof of a special case of Dirichlet's Theorem on primes in arithmetic progressions. Then there is a detailed study of cyclotomic fields, and we prove the central case of Gauss' characterisation of regular  $n$ -gons which are constructible by compasses and straight edge. There is an indication of Galois Theory, illustrated by the key example of cyclotomic extensions discussed earlier. We discuss in detail the implications of Galois Theory in the context of finite fields, including a description of the subfield lattice of a finite field and the Normal Basis Theorem. We end with a discussion of cyclotomic polynomials over finite fields. Additional topics, such as pseudorandom sequences, are covered in the Exercises.

**General references.** The following books cover some of the selected material in greater detail. They also address related and more advanced topics.

- Ian Stewart, Galois Theory, Chapman and Hall, London, 1973.
- Rudolf Lidl and Harald Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, Cambridge, 1986.
- Emil Artin, Galois Theory, University of Notre Dame, 1959, available at <http://projecteuclid.org/>.

ACKNOWLEDGEMENTS. In preparing the course and these notes I have made considerable use of several books. Originality I can claim, in a limited sense, with regard to the overall exposition.

---

*Date:* January 4, 2008.

## CONTENTS

What the course is about	1
Summary	1
General references	1
1. Euclidean Constructions	3
1.1. Doubling the cube	3
1.2. Regular $n$ -gons	3
1.3. Translation to Algebra	4
1.4. First consequences	4
2. Basic extension theory	5
2.1. Field extensions	5
2.2. Application to Euclidean constructions	6
3. Degree of an extension	8
4. Algebraic extensions	10
4.1. Simple transcendental extensions	10
4.2. Minimum polynomials	11
4.3. Algebraic extensions	12
5. Simple extensions	13
5.1. Kronecker's Theorem	13
5.2. Polynomial rings – ‘rebooting your memory’	15
5.3. Irreducible Polynomials	17
6. Basic theory of finite fields	18
6.1. Prime fields and characteristic	18
6.2. Existence and uniqueness of finite fields of prescribed cardinality	19
7. An application: discrete logarithms	22
7.1. Discrete logarithm	22
7.2. Diffie-Hellman key exchange and El Gamal encryption	22
7.3. Algorithms for computing discrete logarithms	24
7.4. Mersenne prime method	26
8. Cyclotomic polynomials	28
8.1. Roots of unity	28
8.2. Cyclotomic polynomials	28
8.3. Möbius Inversion	30
8.4. Primes in arithmetic progressions	31
9. Cyclotomic fields and an indication of Galois Theory	33
9.1. Cyclotomic fields and their automorphisms	33
9.2. Regular $p$ -gons	35
9.3. An indication of Galois Theory	37
10. Implications of Galois Theory in the context of finite fields	40
10.1. Subfields of finite fields	40
10.2. Automorphisms of finite fields	40
10.3. Galois Theory for finite fields	41
10.4. Cyclotomic polynomials over finite fields	44
Index	47

## 1. EUCLIDEAN CONSTRUCTIONS

1.1. **Doubling the cube.** About 100 CE, Theon of Smyrna writes in his “Exposition of mathematical things useful for the reading of Plato”:

The Delians asked for an oracle in order to be liberated from a plague. The god, Apollo, answered through the oracle that they had to construct an altar twice as large as the existing one without changing its shape.

This can be interpreted as a geometric problem, known as the *problem of doubling the cube*: given a finite length  $a$  construct the length  $\sqrt[3]{2}a$ . Other famous problems which the ancient Greeks were interested in include: *squaring the circle* and *trisecting a given angle*. The method that they allowed was construction by compasses and straight edge. Intuitively, starting from a given set of points  $S$  in the Euclidean plane one is allowed to draw (i) lines through any two distinct points in  $S$  and (ii) circles with midpoint in  $S$  and radius equal to the distance between two points in  $S$ . The intersection points of such lines and circles are added to the set  $S$  to form a larger set  $S_2$ . Iterating this process one obtains an ascending sequence of sets of points  $S = S_1 \subseteq S_2 \subseteq S_3 \subseteq \dots$ . A point is constructible from  $S$  by compasses and straight edge, if it is contained in one of the members  $S_i$  of this sequence.

To get a feeling for this kind of construction method, remember from school (or consider for the first time) the following easier problems:

- Bisect a given angle.
- Trisect a given line of finite length.
- Construct a regular triangle, a regular pentagon and a regular hexagon.

1.2. **Regular  $n$ -gons.** Another natural question which arises in this context is

*Question 1.1.* Which regular  $n$ -gons are constructible by compasses and straight edge?

Many of these classical geometric problems were resolved in the 19th century by Gauss, Lindemann, Wanzel and other mathematicians after a translation into an algebraic setting. As an example we state

**Theorem 1.2** (Gauss-Wanzel). *A regular  $n$ -gon is constructible by compasses and straight edge if and only if  $n$  is a product of a power of 2 and distinct Fermat primes.*

Recall that the  $r$ th Fermat number is defined by the equation  $F_r := 2^{2^r} + 1$ . Any Fermat number which is prime is called a Fermat prime. The first five Fermat numbers

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

are indeed prime. But Euler showed that  $F_5 = 2^{32} + 1$  is composite by finding the explicit factorisation  $F_5 = 641 \cdot 6700417$ . The following questions remain open to this day: Is  $F_r$  composite for all  $r > 4$ ? Are there infinitely many Fermat primes? Are there infinitely many composite Fermat numbers?

**1.3. Translation to Algebra.** By describing the geometric situation in terms of algebraic objects, we will give a precise meaning to Euclidean constructions based on compasses and straight edge. By introducing coordinates, one obtains a one-to-one correspondence between points in the Euclidean plane and elements of a 2-dimensional vector space  $\mathbb{R}^2$  over the real numbers  $\mathbb{R}$ . For our purposes it is convenient to go one step further and we interpret points in the Euclidean plane with real coordinates  $(x, y)$  as complex numbers  $z = x + yi$ . Here  $i$  denotes the imaginary unit satisfying the equation  $i^2 = -1$ , and  $x, y \in \mathbb{R}$  are known as the real and imaginary part of  $z = x + yi$ . In the following we speak of the *complex plane* when we want to emphasise the geometric interpretation of the complex numbers  $\mathbb{C}$ . We recall that *complex conjugation*  $z = x + yi \mapsto \bar{z} = x - yi$  constitutes an automorphism of the field  $\mathbb{C}$ . The *distance* between complex numbers  $z_1, z_2 \in \mathbb{C}$  is given by  $|z_1 - z_2| = \left( (z_1 - z_2)\overline{(z_1 - z_2)} \right)^{1/2}$

For any subset  $S \subseteq \mathbb{C}$  we define the corresponding *set of constructible numbers*

$$\triangleleft S := \{z \in \mathbb{C} \mid z \text{ constructible from } S \text{ by compasses and straightedge}\}.$$

Here we still need to make precise what we mean by the term “constructible by compasses and straight edge”. We interpret the *line in the complex plane* through two distinct points  $z_1, z_2 \in \mathbb{C}$  as the subset  $\mathfrak{l} \subseteq \mathbb{C}$  given by

$$\mathfrak{l} = \{z \in \mathbb{C} \mid \exists t \in \mathbb{R} : z = tz_1 + (1 - t)z_2\}.$$

Similarly we interpret the *circle in the complex plane* with midpoint  $z_0 \in \mathbb{C}$  and radius  $r \in \mathbb{R}_{\geq 0}$  as the subset  $\mathfrak{c} \subseteq \mathbb{C}$  given by

$$\mathfrak{c} = \{z \in \mathbb{C} \mid (z - z_0)\overline{(z - z_0)} = r^2\}.$$

For  $S \subseteq \mathbb{C}$  we write

$\mathcal{L}(S)$  to denote the set of all lines in the complex plane which contain at least two points in  $S$ .

$\mathcal{C}(S)$  to denote the set of all circles in the complex plane with midpoint in  $S$  and radius equal to the distance of two points in  $S$ .

The three *elementary construction steps using compasses and straight edge* are the following:

- (C1) intersect two distinct lines in  $\mathcal{L}(S)$ ,
- (C2) intersect a line in  $\mathcal{L}(S)$  and a circle in  $\mathcal{C}(S)$ ,
- (C3) intersect two distinct circles in  $\mathcal{C}(S)$ .

Accordingly, we define  $S_1 := S$  and recursively

$$S_{i+1} := S_i \cup \{z \in \mathbb{C} \mid \exists \mathfrak{a}, \mathfrak{b} \in \mathcal{L}(S_i) \cup \mathcal{C}(S_i) : \mathfrak{a} \neq \mathfrak{b} \text{ and } z \in \mathfrak{a} \cap \mathfrak{b}\}.$$

Then the set of constructible numbers from  $S$  is the union  $\triangleleft S = \bigcup_{i \in \mathbb{N}} S_i$ .

**1.4. First consequences.** Let  $\{0, 1\} \subseteq S \subseteq \mathbb{C}$ . The following basic result reveals the algebraic nature of the set  $\triangleleft S$ .

**Proposition 1.3.** *Let  $\{0, 1\} \subseteq S \subseteq \mathbb{C}$ . Then*

- (1)  $i \in \triangleleft S$ ,
- (2)  $z \in \triangleleft S$  implies  $\bar{z} \in \triangleleft S$ ,
- (3)  $z = x + yi \in \triangleleft S$  implies  $x, y \in \triangleleft S$ ,
- (4)  $z \in \triangleleft S$  implies  $-z \in \triangleleft S$ ,

- (5)  $z_1, z_2 \in \triangleleft S$  implies  $z_1 + z_2 \in \triangleleft S$ ,
- (6)  $z_1, z_2 \in \triangleleft S$  implies  $z_1 \cdot z_2 \in \triangleleft S$ ,
- (7)  $z \in \triangleleft S$  and  $z \neq 0$  implies  $z^{-1} \in \triangleleft S$ .

*Proof.* This is proved by a series of geometric considerations which are quite fun to figure out and which were discussed during the lectures. The Intercept Theorem plays a substantial role.  $\square$

Recall that a subset  $K \subseteq \mathbb{C}$  forms a subfield if  $K$  is a field with respect to the restrictions of the operations  $+$  and  $\cdot$ . Parts (2), (4), (5), (6), (7) of the Proposition yield

**Corollary 1.4.** *Let  $\{0, 1\} \subseteq S \subseteq \mathbb{C}$ . Then  $\triangleleft S$  is a subfield of  $\mathbb{C}$  which is closed under complex conjugation.*

The next result captures another important algebraic property of the field  $\triangleleft S$ .

**Proposition 1.5.** *Let  $\{0, 1\} \subseteq S \subseteq \mathbb{C}$ . Then the field  $K := \triangleleft S$  is quadratically closed, i.e. for all  $z \in \mathbb{C}$  the condition  $z^2 \in K$  implies  $z \in K$ .*

*Proof.* Again this is proved by geometric consideration, based on Thales' theorem, as we saw in the lectures.  $\square$

## 2. BASIC EXTENSION THEORY

**2.1. Field extensions.** A *field extension*  $L|K$  consists of a field  $L$  and a subfield  $K$  of  $L$ . The field  $L$  is called an extension field of  $K$ . Any subfield  $M$  of  $L$  containing  $K$  is called an *intermediate field* of the extension  $L|K$ . Let  $A \subseteq L$ . Then

$$K(A) := \bigcap \{M \mid M \text{ an intermediate field of } L|K \text{ with } A \subseteq M\}$$

is called the *subfield of  $L$  generated by  $A$  over  $K$* . If  $A = \{\alpha_1, \dots, \alpha_m\}$  is finite, we write  $K(\alpha_1, \dots, \alpha_m) := K(A)$ . Clearly,  $K(A)$  is the smallest subfield of  $L$  which contains  $K \cup A$ .

*Example 2.1.* Consider  $L = \mathbb{C}$ ,  $K = \mathbb{Q}$  and  $A = \{i\}$ . We claim that

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Denote the set on the right hand side by  $M$ . Clearly,  $\mathbb{Q}(i) \supseteq M$ , and  $\mathbb{Q} \cup \{i\} \subseteq M$ . It remains to prove the converse inclusion  $\mathbb{Q}(i) \subseteq M$ . For this it suffices to show that  $M$  is a field. It is easily seen that  $\{0, 1\} \subseteq M$ , that  $M$  is closed under addition as well as under multiplication and that  $M$  is closed under taking additive inverses. It remains to prove that  $M$  is closed under taking multiplicative inverses. Let  $z = a + bi \in M \setminus \{0\}$ . Then  $a^2 + b^2 = z\bar{z} \neq 0$ , and hence

$$z^{-1} = \bar{z}(z\bar{z})^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i \in M.$$

$\diamond$

Let  $L|K$  be a field extension and  $\alpha \in L$ . We offer the following general description of the field  $K(\alpha)$ . There is a natural ring homomorphism  $\eta$  from the ring of polynomials  $K[X]$  over  $K$  into  $L$  given by  $f \mapsto f(\alpha)$ . The image of  $\eta$  is

$K[\alpha] = \{f(\alpha) \mid f \in K[X]\}$ , a subring of  $L$ . Clearly,  $K[\alpha]$  is the smallest subring of  $L$  containing  $K \cup \{\alpha\}$ , and

$$K(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \mid f, g \in K[X] \text{ such that } g(\alpha) \neq 0 \right\}.$$

**2.2. Application to Euclidean constructions.** Let us link these algebraic notions to the field of constructible numbers  $\triangleleft S$  associated to a subset  $S \subseteq \mathbb{C}$  containing  $\{0, 1\}$ . As a direct consequence of Corollary 1.4 we have

$$K := \mathbb{Q}(S \cup \overline{S}) \subseteq \triangleleft S$$

Indeed, the right hand side is a subfield of  $\mathbb{C}$  containing  $S$  and closed under complex conjugation, while the left hand side is the smallest subfield of  $\mathbb{C}$  containing  $S$  and closed under complex conjugation.

**Lemma 2.2.** *Let  $K$  be a subfield of  $\mathbb{C}$  closed under complex conjugation, i.e. such that  $\overline{K} = K$ .*

- (1) *If  $z$  is in the intersection of two distinct lines  $\mathfrak{l}, \tilde{\mathfrak{l}} \in \mathcal{L}(K)$ , then  $z \in K$ .*
- (2) *If  $z$  is in the intersection of  $\mathfrak{l} \in \mathcal{L}(K)$  and  $\mathfrak{c} \in \mathcal{C}(K)$ , then there exists  $w \in \mathbb{C}$  with  $w^2 \in K$  and  $z \in K(w)$ .*
- (3) *If  $z$  is in the intersection of distinct circles  $\mathfrak{c}, \tilde{\mathfrak{c}} \in \mathcal{L}(K)$ , then there exists  $w \in \mathbb{C}$  with  $w^2 \in K$  and  $z \in K(w)$ .*

*Proof.* (1) Let two distinct lines  $\mathfrak{l}, \tilde{\mathfrak{l}} \in \mathcal{L}(K)$  be given by

$$\begin{aligned} \mathfrak{l} &= \{z \in \mathbb{C} \mid \exists s \in \mathbb{R} : z = sz_1 + (1-s)z_2\} \quad \text{with } z_1, z_2 \in K, \\ \tilde{\mathfrak{l}} &= \{z \in \mathbb{C} \mid \exists t \in \mathbb{R} : z = t\tilde{z}_1 + (1-t)\tilde{z}_2\} \quad \text{with } \tilde{z}_1, \tilde{z}_2 \in K. \end{aligned}$$

Suppose that  $z \in \mathfrak{l} \cap \tilde{\mathfrak{l}}$ . Then we find unique parameters  $s, t \in \mathbb{R}$  such that

$$sz_1 + (1-s)z_2 = z = t\tilde{z}_1 + (1-t)\tilde{z}_2.$$

Write  $z_k = x_k + y_k i$  and  $\tilde{z}_k = \tilde{x}_k + \tilde{y}_k i$  with  $x_k, y_k, \tilde{x}_k, \tilde{y}_k \in \mathbb{R}$  for  $k \in \{1, 2\}$ . Then  $(s, t)$  is the unique solution to the system of linear equations

$$(*) \begin{cases} (x_1 - x_2)s - (\tilde{x}_1 - \tilde{x}_2)t = \tilde{x}_2 - x_2, \\ (y_1 i - y_2 i)s - (\tilde{y}_1 i - \tilde{y}_2 i)t = \tilde{y}_2 i - y_2 i. \end{cases}$$

As  $K$  is closed under complex conjugation, the numbers  $x_k, \tilde{x}_k, y_k i, \tilde{y}_k i$  lie in  $K$  for  $k \in \{1, 2\}$ . Indeed,

$$x_k = (z_k + \overline{z_k})/2 \in K \quad \text{and} \quad y_k i = (z_k - \overline{z_k})/2 \in K \quad \text{for } k \in \{1, 2\};$$

similar equations hold for  $\tilde{x}_k, \tilde{y}_k i$ . This implies that the coefficients of the linear system of equations (\*) are in  $K$ . Consequently, the solution  $(s, t)$  lies in  $K^2$ , in particular  $s \in K$ . Hence,  $z = sz_1 + (1-s)z_2 \in K$ .

(2) Let  $\mathfrak{l} \in \mathcal{L}(K)$  and  $\mathfrak{c} \in \mathcal{C}(K)$  be given by

$$\begin{aligned} \mathfrak{l} &= \{z \in \mathbb{C} \mid \exists s \in \mathbb{R} : z = sz_1 + (1-s)z_2\} \quad \text{with } z_1, z_2 \in K, \\ \mathfrak{c} &= \{z \in \mathbb{C} \mid (z - z_0)\overline{(z - z_0)} = r^2\} \quad \text{with } z_0 \in K \text{ and } r \in \mathbb{R}_{\geq 0}, \end{aligned}$$

where  $r = |\tilde{z}_1 - \tilde{z}_2|$  for suitable  $\tilde{z}_1, \tilde{z}_2 \in K$ . As  $K$  is closed under complex conjugation, this implies  $r^2 = (\tilde{z}_1 - \tilde{z}_2)\overline{(\tilde{z}_1 - \tilde{z}_2)} \in K$ .

Suppose that  $z \in \mathfrak{l} \cap \mathfrak{c}$ . Then we find  $s \in \mathbb{R}$  such that  $z = sz_1 + (1-s)z_2 = s(z_1 - z_2) + z_2$ , and consequently

$$(s(z_1 - z_2) + z_2 - z_0)(\overline{s(z_1 - z_2) + (z_2 - z_0)}) = r^2.$$

Multiplying out the product on the left hand side and subsequently dividing by  $(z_1 - z_2)\overline{(z_1 - z_2)} = |z_1 - z_2|^2 \neq 0$ , we obtain a quadratic equation

$$s^2 + ps + q = 0 \quad \text{where } p, q \in K.$$

Setting  $w := s + p/2$ , we have  $w^2 = p^2/4 - q \in K$  and  $z = sz_1 + (1-s)z_2 \in K(s) = K(w)$ .

(3) The third assertion is proved very similarly and was left as an exercise.  $\square$

Let  $L|K$  be a field extension. We say that  $L$  is obtained from  $K$  by *adjoining a square root*, if there exists  $w \in L$  such that  $w^2 \in K$  and  $L = K(w)$ . In this situation we call  $w$  a square root of  $v := w^2$  and we write  $w = \sqrt{v}$ . More generally we say that  $L$  is obtained from  $K$  by *successively adjoining square roots*, if there exists a chain of intermediate fields

$$K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m = L, \quad m \in \mathbb{N},$$

such that each  $K_i$  is obtained from  $K_{i-1}$  by adjoining a square root.

*Example 2.3.* (1) Clearly, the field  $\mathbb{Q}(\sqrt{2})$  is obtained from  $\mathbb{Q}$  by adjoining a square root.

(2) The field  $\mathbb{Q}(e^{2\pi i/3})$  is obtained from  $\mathbb{Q}$  by adjoining a square root. This is not immediately obvious. But  $e^{2\pi i/3} = (-1 + \sqrt{3}i)/2$  implies  $\mathbb{Q}(e^{2\pi i/3}) = \mathbb{Q}(\sqrt{3}i)$ .

(3) The field  $\mathbb{Q}(e^{2\pi i/5})$  is not obtained from  $\mathbb{Q}$  by adjoining a square root, but by successively adjoining square roots. This is not immediately obvious.  $\diamond$

**Theorem 2.4.** *Let  $S \subseteq \mathbb{C}$  with  $\{0, 1\} \subseteq S$ . Set  $K := \mathbb{Q}(S \cup \overline{S})$ , and let  $z \in \mathbb{C}$ . Then the following assertions are equivalent:*

- (1)  $z \in \triangleleft S$ , i.e.  $z$  is constructible from  $S$  by compasses and straight edge constructions,
- (2)  $z$  is contained in an intermediate field  $L$  of  $\mathbb{C}|K$  which can be obtained from  $K$  by successively adjoining square roots.

*Proof.* Suppose that (2) holds. Then we find a chain of intermediate fields

$$K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m = L, \quad m \in \mathbb{N},$$

such that  $K_i = K_{i-1}(w_i)$  with  $w_i^2 \in K_{i-1}$  for each  $i$  and  $z \in L$ . We know that  $K_0 = K \subseteq \triangleleft S$ . Consider  $K_1 = K_0(w_1)$  with  $w_1^2 \in K_0$ . By Proposition 1.5 the field  $\triangleleft S$  is quadratically closed, hence  $K_1 \subseteq \triangleleft S$ . Continuing in this fashion, we see that  $K_2 \subseteq \triangleleft S, \dots, K_m \subseteq \triangleleft S$ . This implies  $z \in L = K_m \subseteq \triangleleft S$ , as wanted.

Now suppose that (1) holds. By induction it suffices to prove the following special case of (2): Suppose that  $z$  can be constructed from  $S$  by one of the three elementary construction steps (C1), (C2), (C3) by compasses and straight edge. Then  $z$  is contained in an intermediate field  $L$  of  $\mathbb{C}|K$  which can be obtained from  $K$  by successively adjoining square roots and which satisfies  $\overline{L} = L$ .

To prove this claim we employ Lemma 2.2. If  $z$  is constructed from  $S$  by the elementary construction (C1), then  $z \in K$  and we may take  $L = K$ . Now suppose that  $z$  arises from  $S$  by one of the elementary construction steps (C2) or (C3).

Then we find  $w \in \mathbb{C}$  such that  $z \in K(w)$  and  $w^2 \in K$ . Put  $L := K(w, \bar{w})$ . Certainly,  $z \in L$  and

$$\bar{L} = \overline{K(w, \bar{w})} = \overline{K(\bar{w}, w)} = K(w, \bar{w}) = L.$$

Moreover,  $w^2 \in K$  implies  $\bar{w}^2 \in \bar{K} = K \subseteq K(w)$ . This shows that  $L$  is obtained from  $K$  by successively adjoining square roots, namely  $w$  and then  $\bar{w}$ .  $\square$

The classical Greek problems can now be restated in a purely algebraic form.

- Doubling the cube: Is  $\sqrt[3]{2}$  contained in a subfield of  $\mathbb{C}$  which can be obtained from  $\mathbb{Q}$  by successively adjoining square roots?
- Squaring the circle: Is  $\pi$  contained in a subfield of  $\mathbb{C}$  which can be obtained from  $\mathbb{Q}$  by successively adjoining square roots?
- Trisecting a given angle: Given  $\varphi \in \mathbb{R}$ , is  $e^{\varphi i/3}$  contained in a subfield of  $\mathbb{C}$  which can be obtained from  $\mathbb{Q}(e^{\varphi i})$  by successively adjoining square roots? (Here one should observe that  $\overline{e^{\varphi i}} = (e^{\varphi i})^{-1}$  implies  $\overline{\mathbb{Q}(e^{\varphi i})} = \mathbb{Q}(e^{\varphi i})$ .)
- Constructing a regular  $n$ -gon: Is  $e^{2\pi i/n}$  contained in a subfield of  $\mathbb{C}$  which can be obtained from  $\mathbb{Q}$  by successively adjoining square roots?

### 3. DEGREE OF AN EXTENSION

Let  $L|K$  be a field extension. The following basic but extremely useful observation goes back to Dedekind:  $L$  can be regarded as a vector space over  $K$ . Indeed,  $L$  is already an abelian group with respect to addition, and scalar multiplication can be defined by restricting the multiplication map  $L \times L \rightarrow L$  to  $K \times L$ . All required properties, such as  $\lambda(\alpha + \beta) = \lambda\alpha + \lambda\beta$  for “scalars”  $\lambda \in K$  and “vectors”  $\alpha, \beta \in L$ , follow immediately from the field axioms.

Regarding  $L$  as a vector space over  $K$ , we can measure the “size” of the extension  $L|K$ : the *degree* of  $L|K$  is defined as  $[L : K] := \dim_K(L)$ , the dimension of  $L$  as a vector space over  $K$ . If  $[L : K] < \infty$ , one says that  $L$  is a *finite extension* of  $K$ .

*Example 3.1.* (1) Clearly,  $[\mathbb{C} : \mathbb{R}] = 2$ . In fact,  $(1, i)$  is a basis for  $\mathbb{C}$  as a vector space over  $\mathbb{R}$ .

(2) We have seen that  $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ . Indeed, we have shown that  $(1, \sqrt{2})$  is a basis for  $\mathbb{Q}(\sqrt{2})$  as a vector space over  $\mathbb{Q}$ .

(3) Comparing cardinalities, one obtains  $[\mathbb{R} : \mathbb{Q}] = \infty$ . In fact, the dimension of  $\mathbb{R}$  as a vector space over  $\mathbb{Q}$  has to be uncountably infinite. Otherwise  $\mathbb{R}$  would be countable.

(4) We will show that  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$  and use this fact to deduce that  $\sqrt[3]{2}$  cannot be constructed from  $\{0, 1\}$  by compasses and straight edge.  $\diamond$

**Lemma 3.2.** *Let  $L|K$  be a field extension, and suppose that  $1+1 \neq 0$  in  $K$ . Then  $[L : K] = 2$  if and only if  $L = K(w)$  with  $w^2 \in K$ , but  $w \notin K$ .*

*Proof.* First suppose that  $[L : K] = 2$ . Then we find  $\alpha \in L \setminus K$ , and  $(1, \alpha)$  constitutes a basis for  $L$  as a vector space over  $K$ . Consequently there are  $p, q \in K$  such that  $\alpha^2 = q + p\alpha$ . Put  $w := \alpha - p/2 \notin K$ . Then  $L = K(\alpha) = K(w)$  and  $w^2 = \alpha^2 - p\alpha + p^2/4 = q + p^2/4 \in K$ .

Now suppose that  $L = K(w)$  with  $w^2 \in K$ , but  $w \notin K$ . Consider  $M := \{a + bw \mid a, b \in K\} \subseteq L$ , the  $K$ -span of  $(1, w)$ . It suffices to show that  $M$  is a field, for then  $L = K(w) = M$  has basis  $(1, w)$  as a vector space over  $K$ . Clearly,  $0, 1 \in M$ ,

and one easily checks that  $M$  is closed under addition, multiplication and taking additive inverses. To locate the multiplicative inverse of  $a + bw \in M \setminus \{0\}$ , one notes that  $(a + bw)(a - bw) = a^2 - b^2w^2 \neq 0$ . Indeed,  $a^2 = b^2w^2$  would imply  $b \neq 0$  and  $(a/b)^2 = w^2$ , hence  $w = a/b \in K$  or  $w = -a/b \in K$ . Thus we find

$$(a + bw)^{-1} = \frac{a - bw}{(a + bw)(a - bw)} = \frac{a}{a^2 - b^2w^2} - \frac{b}{a^2 - b^2w^2}w \in M.$$

□

We remark that the condition  $1 + 1 \neq 0$  was only used in proving the direction “ $\Rightarrow$ ”. Based on the lemma, we can reformulate Theorem 2.4.

**Theorem 3.3.** *Let  $S \subseteq \mathbb{C}$  with  $\{0, 1\} \subseteq S$ . Set  $K := \mathbb{Q}(S \cup \overline{S})$ , and let  $z \in \mathbb{C}$ . Then  $z \in \langle S \rangle$  if and only if there exists a chain  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$ ,  $m \in \mathbb{N}_0$ , of subfields of  $\mathbb{C}$  such that  $z \in K_m$  and  $[K_i : K_{i-1}] = 2$  for each  $i \in \{1, \dots, m\}$ .*

In view of this theorem we are interested in the degrees of towers of fields.

**Proposition 3.4** (The so-called Tower Law). *Let  $M|L$  and  $L|K$  be field extensions. Then  $[M : K] = [M : L][L : K]$ .*

*Suppose that  $m := [L : K]$  and  $n := [M : L]$  are finite. Let  $(\alpha_1, \dots, \alpha_m)$  be a basis for  $L$  over  $K$ , and let  $(\beta_1, \dots, \beta_n)$  be a basis for  $M$  over  $L$ . Then  $(\alpha_i\beta_j)_{1 \leq i \leq m, 1 \leq j \leq n}$  constitutes a basis for  $M$  as a vector space over  $K$ .*

*Proof.* We leave it as an exercise to show that, if one of the degrees  $[M : L]$  or  $[L : K]$  is infinite, then so is  $[M : K]$ . Now suppose that  $m := [L : K]$  and  $n := [M : L]$  are finite. As vector spaces we have  $M \cong L^n$  and  $L \cong K^m$ . This yields  $M \cong L^n \cong (K^m)^n \cong K^{mn}$  as a vector space over  $K$ . Hence  $[M : K] = mn = [M : L][L : K]$ .

Now let  $(\alpha_1, \dots, \alpha_m)$  and  $(\beta_1, \dots, \beta_n)$  be bases for  $L$  over  $K$  and for  $M$  over  $L$ , respectively. Since the dimension of  $M$  over  $K$  is  $mn$ , it suffices to show that the elements  $\alpha_i\beta_j$ , where  $1 \leq i \leq m$  and  $1 \leq j \leq n$ , span  $M$  as a vector space over  $K$ . Let  $\gamma \in M$ . Then  $\gamma = \sum_{j=1}^n b_j\beta_j$  for suitable  $b_j \in L$ . Moreover, each  $b_j$  can be written as  $b_j = \sum_{i=1}^m a_{ij}\alpha_i$  for suitable  $a_{ij} \in K$ . This yields

$$\gamma = \sum_{j=1}^n b_j\beta_j = \sum_{j=1}^n \left( \sum_{i=1}^m a_{ij}\alpha_i \right) \beta_j = \sum_{i,j} a_{ij}(\alpha_i\beta_j),$$

so  $\gamma$  is indeed a linear combination of the  $\alpha_i\beta_j$  with coefficients  $a_{ij}$  in  $K$ . □

**Corollary 3.5.** *Let  $L|K$  be a finite field extension such that  $L$  can be obtained from  $K$  by successively adjoining square roots. Then  $[L : K]$  is a power of 2.*

One has to be cautious: in general the converse does not hold.

**Corollary 3.6.** *Let  $K$  be a subfield of  $\mathbb{C}$  with  $\overline{K} = K$ , and let  $z \in \mathbb{C}$ . If  $z \in \langle K \rangle$ , then  $[K(z) : K]$  is a power of 2.*

*Proof.* According to Theorem 3.3 and Proposition 3.4 we find a field extension  $L$  of  $K$  such that  $z \in L$  and  $[L : K] = 2^m$  for some  $m \in \mathbb{N}_0$ . Proposition 3.4 also shows that  $[L : K(z)][K(z) : K] = [L : K] = 2^m$ . Hence  $[K(z) : K]$  is a power of 2. □

For instance, once we show that  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ , it follows that  $\sqrt[3]{2}$  is not constructible from  $\{0, 1\}$ . Hence the cube cannot be doubled by compasses and straight edge.

#### 4. ALGEBRAIC EXTENSIONS

**4.1. Simple transcendental extensions.** Let  $L|K$  be a field extension. An element  $\alpha \in L$  is called *algebraic* over  $K$  if it satisfies a non-trivial polynomial equation over  $K$ , i.e. if there exists a monic polynomial  $f \in K[X]$  such that  $f(\alpha) = 0$ . If  $\alpha$  is not algebraic over  $K$ , then it is said to be *transcendental* over  $K$ .

For example,  $\sqrt[3]{2}$  is algebraic over  $\mathbb{Q}$ , because it is a root of the polynomial  $X^3 - 2$ . We remark that there are only countably many complex numbers which are algebraic over  $\mathbb{Q}$ , hence there must be uncountably complex numbers which are transcendental over  $\mathbb{Q}$ . However, it is not an easy task to prove that a given complex number is transcendental. In 1882 Lindemann succeeded in showing that  $\pi$  is transcendental over  $\mathbb{Q}$ .

*Example 4.1.* Let  $K$  be any field and consider the *field of rational functions* over  $K$  in the indeterminate  $t$ , i.e. the field

$$K(t) := \{f(t)/g(t) \mid f, g \in K[X] \text{ with } g \neq 0\}.$$

This is the field of fractions of the polynomial ring over  $K$ : indeed  $K[t] \cong K[X]$  embeds as a ring into  $K(t)$  and no proper subfield of  $K(t)$  contains  $K[t]$ .

As  $g(t) \neq 0$  for every  $g \in K[X] \setminus \{0\}$ , the indeterminate  $t \in K(t)$  is transcendental over  $K$ . We also notice that  $[K(t) : K] = \infty$ . Indeed, the infinite set  $\{t^k \mid k \in \mathbb{N}_0\}$  is linearly independent.  $\diamond$

The next proposition shows that the previous example is typical.

**Proposition 4.2.** *Let  $K(\alpha)|K$  be a field extension with  $\alpha$  transcendental over  $K$ . Then the injective ring homomorphism  $K[t] \rightarrow K(\alpha)$ ,  $f(t) \mapsto f(\alpha)$  extends uniquely to a field isomorphism  $K(t) \rightarrow K(\alpha)$  which restricts to the identity map on  $K$ . In particular,  $[K(\alpha) : K] = \infty$ .*

*Proof.* Since  $\alpha$  is transcendental over  $K$ , the kernel of the ring homomorphism  $\eta : K[t] \rightarrow K[\alpha]$ ,  $f(t) \mapsto f(\alpha)$  is trivial. So  $\eta$  is a ring isomorphism from  $K[t]$  onto  $K[\alpha]$  which restricts to the identity on  $K$ . Since every element of  $K(t)$  is of the form  $f(t)/g(t)$  where  $f(t), g(t) \in K[t]$  with  $g \neq 0$ , there is only one possible way of extending  $\eta$  to a field isomorphism  $\hat{\eta} : K(t) \rightarrow K(\alpha)$ : we have to send  $f(t)/g(t)$  to  $f(\alpha)/g(\alpha)$ .

It remains to check that two representations of the same element of  $K(t)$  lead to the same image in  $K(\alpha)$ , i.e. that  $f(t)/g(t) = \tilde{f}(t)/\tilde{g}(t)$  implies  $f(\alpha)/g(\alpha) = \tilde{f}(\alpha)/\tilde{g}(\alpha)$ . Equivalently we need to show that  $h(t) = 0$  implies  $h(\alpha) = 0$ , where  $h := f\tilde{g} - \tilde{f}g \in K[X]$ . Since both  $t$  and  $\alpha$  are transcendental over  $K$ , each of the two assertions is equivalent to  $h = 0$  in  $K[X]$ . So  $\hat{\eta}$  can be defined without any ambiguity.

The isomorphism  $\hat{\eta} : K(t) \rightarrow K(\alpha)$  restricts to the identity on  $K$ . This implies  $[K(\alpha) : K] = [K(t) : K] = \infty$ .  $\square$

Lindemann's theorem that  $\pi$  is transcendental over  $\mathbb{Q}$  implies  $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$ . According to our discussion following Theorem 2.4, this shows that the ancient problem of squaring the circle by compasses and straight edge has a negative solution.

**4.2. Minimum polynomials.** Let  $L|K$  be a field extension, and let  $\alpha \in L$  be algebraic over  $K$ . Then there exist polynomials  $f \in K[X] \setminus \{0\}$  of smallest degree such that  $f(\alpha) = 0$ . Among these there is a unique monic polynomial. This is the *minimum polynomial* of  $\alpha$  over  $K$ , denoted by  $\text{mipo}_K(\alpha) \in K[X]$ . For completeness we briefly comment on the uniqueness of the described polynomial. Suppose that  $f, g \in K[X]$  are distinct monic polynomials of equal degree  $n$  such that  $f(\alpha) = g(\alpha) = 0$ . Then  $h := f - g \in K[X]$  is a non-trivial polynomial of degree smaller than  $n$  such that  $h(\alpha) = 0$ . Consequently,  $n$  was not the smallest possible degree of a non-zero polynomial over  $K$  with root  $\alpha$ .

*Example 4.3.* Let  $L := \mathbb{C}$ ,  $K := \mathbb{Q}$  and  $\alpha := e^{2\pi i/3}$ . Then  $\alpha$  is a root of  $X^3 - 1 = (X - 1)(X^2 + X + 1)$ . Since  $\alpha - 1 \neq 0$ , the monic polynomial  $g := X^2 + X + 1$  has root  $\alpha$ . Let  $f := \text{mipo}_K(\alpha)$ , and suppose for a contradiction that  $f \neq g$ . Then  $1 \leq \deg(f) < \deg(g) = 2$ , thus  $\deg(f) = 1$  and  $X - \alpha = f \in K[X]$ . But this leads to the contradiction  $\alpha \in K$ . Hence  $\text{mipo}_{\mathbb{Q}}(\alpha) = X^2 + X + 1$ .  $\diamond$

**Proposition 4.4.** *Let  $L|K$  be a field extension, and let  $\alpha \in L$  be algebraic over  $K$ . Set  $n := \deg(\text{mipo}_K(\alpha))$ . Then  $(1, \alpha, \alpha^2, \dots, \alpha^{n-1})$  is a basis for  $K(\alpha)$  as a vector space over  $K$ . In particular,*

$$K(\alpha) = K[\alpha] = K + K\alpha + \dots + K\alpha^{n-1} \quad \text{and} \quad [K(\alpha) : K] = \deg(\text{mipo}_K(\alpha)).$$

*Proof.* Put  $f := \text{mipo}_K(\alpha)$  and write  $f = \sum_{k=0}^n f_k X^k$ . Then  $f(\alpha) = 0$  implies that  $\alpha^n = -f_0 - f_1\alpha - \dots - f_{n-1}\alpha^{n-1}$ . Induction on the degree shows that every polynomial expression in  $\alpha$  over  $K$  can be written as a polynomial expression in  $\alpha$  of degree less than  $n$ , i.e. that  $K[\alpha] = K + K\alpha + \dots + K\alpha^{n-1}$ .

Next we show that  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  are linearly independent over  $K$ . Indeed, suppose that  $g_0 + g_1\alpha + \dots + g_{n-1}\alpha^{n-1} = 0$  for suitable  $g_k \in K$ . Since the minimum polynomial of  $\alpha$  over  $K$  has degree  $n$ , this implies that  $g_0 = \dots = g_{n-1} = 0$ .

It remains to prove that  $K(\alpha) = K[\alpha]$ . Clearly,  $K(\alpha) \supseteq K[\alpha]$ . For the reverse inclusion it suffices to show that the integral domain  $K[\alpha]$  is a field, i.e. that every non-zero element of  $K[\alpha]$  already has a multiplicative inverse in  $K[\alpha]$ . Let  $\beta \in K[\alpha] \setminus \{0\}$ . Then multiplication by  $\beta$  yields an injective linear map  $m_\beta$  from the finite dimensional  $K$ -vector space  $K[\alpha]$  into itself. Then the kernel  $\ker(m_\beta) = \{0\}$  and the image  $\text{img}(m_\beta) = \beta K[\alpha]$  are vector subspaces of  $K[\alpha]$ , and the dimension formula for linear maps gives

$$\dim K[\alpha] = \dim \ker(m_\beta) + \dim \text{img}(m_\beta) = \dim \beta K[\alpha].$$

Since  $K[\alpha] \supseteq \beta K[\alpha]$ , this implies that  $K[\alpha] = \beta K[\alpha]$ . In particular, we find  $\gamma \in K[\alpha]$  such that  $1 = \beta\gamma$ . So  $\beta$  has a multiplicative inverse in  $K[\alpha]$ .  $\square$

A potential application of the proposition is the following. As soon as we show that  $X^3 - 2$  is the minimum polynomial of  $\sqrt[3]{2}$ , we obtain  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ . In view of our discussion following Theorem 2.4, this will imply that the ancient problem of doubling the cube by compasses and straight edge has a negative solution.

*Example 4.5.* We can now give an example of a subfield of  $\mathbb{C}$  which is not closed under complex conjugation; cf. Exercise 1.4. Consider  $K := \mathbb{Q}(\pi + i)$ . Suppose for a contradiction that  $K = \overline{K}$ . Then  $\pi = ((\pi + i) + (\pi - i))/2 = ((\pi + i) + \overline{(\pi + i)})/2 \in K$  and  $i = (\pi + i) - \pi \in K$ . Since  $\pi$  is transcendental over  $\mathbb{Q}$ , we have  $[K : \mathbb{Q}] = \infty$  and by the proposition  $\pi + i$  has to be transcendental over  $\mathbb{Q}$ . Consequently,  $K$  is isomorphic to the field  $\mathbb{Q}(\pi)$ . Since  $i \in K$ , this implies that  $\mathbb{Q}(\pi)$  contains a square root of  $-1$ . This contradicts  $\mathbb{Q}(\pi) \subseteq \mathbb{R}$ .

We observe that instead of  $\pi$  we could have taken any element of  $\mathbb{R}$  which is transcendental over  $\mathbb{Q}$ . Comparing cardinalities one easily sees that there have to be uncountably many such elements.  $\diamond$

**4.3. Algebraic extensions.** A field extension  $L|K$  is called *algebraic* if every  $\alpha \in L$  is algebraic over  $K$ .

**Proposition 4.6.** *Let  $L|K$  be a finite field extension. Then  $L|K$  is algebraic.*

*Proof.* Suppose that  $[L : K] \leq n < \infty$ , and let  $\alpha \in L$ . Then  $1, \alpha, \dots, \alpha^n$  are linearly dependent over  $K$ . Hence we find  $f_0, f_1, \dots, f_n \in K$ , not all zero, such that  $f_0 + f_1\alpha + \dots + f_n\alpha^n = 0$ . This shows that  $\alpha$  is algebraic over  $K$ .  $\square$

**Corollary 4.7** (Characterisation of algebraic elements). *Let  $L|K$  be a field extension, and let  $\alpha \in K$ . Then the following assertions are equivalent:*

- (1)  $\alpha$  is algebraic over  $K$ ,
- (2)  $[K(\alpha) : K] < \infty$ ,
- (3)  $K(\alpha)|K$  is algebraic.

**Proposition 4.8** (Characterisation of finite extensions). *Let  $L|K$  be a field extension. Then the following assertions are equivalent:*

- (1)  $L = K(\alpha_1, \dots, \alpha_m)$  with  $\alpha_1, \dots, \alpha_m \in L$  algebraic over  $K$ ,
- (2)  $L$  is finite over  $K$ , i.e.  $[L : K] < \infty$ .

*Proof.* If  $[L : K] < \infty$ , then every element of  $L$  is algebraic over  $K$  by Proposition 4.6, and  $L = K(\alpha_1, \dots, \alpha_m)$  for any basis  $(\alpha_1, \dots, \alpha_m)$  of the vector space  $L$  over  $K$ .

Now suppose that  $L = K(\alpha_1, \dots, \alpha_m)$  with  $\alpha_1, \dots, \alpha_m \in L$  algebraic over  $K$ . We show by induction on  $m$  that  $[L : K] < \infty$ . If  $m = 0$ , the  $L = K$  and  $[L : K] = 1 < \infty$ . Now suppose that  $m \geq 1$ . By induction  $M := K(\alpha_1, \dots, \alpha_{m-1})$  satisfies  $[M : K] < \infty$ . The element  $\alpha_m$  is algebraic over  $K$ , a fortiori it is algebraic over  $M$ . By Corollary 4.7, the extension  $M(\alpha_m)|M$  is finite. As  $L = M(\alpha_m)$ , this implies  $[L : K] = [L : M][M : K] < \infty$ .  $\square$

**Corollary 4.9.** *Let  $L|K$  be a field extension. Then the algebraic closure  $F := \{\alpha \in L \mid \alpha \text{ algebraic over } K\}$  of  $K$  in  $L$  is an intermediate field of  $L|K$ .*

*Proof.* Let  $\alpha, \beta \in L$  be algebraic over  $K$ . Then  $K(\alpha, \beta)$  is a finite extension of  $K$  and hence algebraic. This implies that  $\alpha - \beta$ ,  $\alpha\beta$  and, if  $\alpha \neq 0$ , also  $\alpha^{-1}$  are algebraic over  $K$ .  $\square$

The proof of the last corollary appears to be rather straightforward. However, one should pause and appreciate that the ease of our argumentation is really due to the powerful conceptual approach that we have taken. Starting from two elements

$\alpha, \beta \in L$  which satisfy certain polynomial equations over  $K$ , it is far from clear how to produce a polynomial equation over  $K$  satisfied by their sum  $\alpha + \beta$  or by their product  $\alpha\beta$ .

**Corollary 4.10.** *Let  $M|L$  and  $L|K$  be field extensions. Then  $M|K$  is algebraic if and only if both  $M|L$  and  $L|K$  are algebraic.*

*Proof.* If  $M|K$  is algebraic, then clearly both  $M|L$  and  $L|K$  are algebraic. Suppose now that  $M|L$  and  $L|K$  are algebraic. Let  $\alpha \in M$ . We have to show that  $\alpha$  is algebraic over  $K$ . Since  $\alpha$  is algebraic over  $L$ , it satisfies a non-trivial polynomial equation  $f_0 + f_1\alpha + \dots + f_n\alpha^n = 0$  with  $f_0, \dots, f_n \in L$ . As  $L|K$  is algebraic, all the elements  $f_0, \dots, f_n$  are algebraic over  $K$ . Put  $F := K(f_0, \dots, f_n)$ . Then Proposition 4.8 implies that  $[F : K] < \infty$ , and clearly  $[F(\alpha) : F] \leq n < \infty$ . This shows that  $[F(\alpha) : K] = [F(\alpha) : F][F : K] < \infty$ . Hence  $\alpha$  is algebraic over  $K$  by Proposition 4.6.  $\square$

## 5. SIMPLE EXTENSIONS

A field extension  $L|K$  is said to be *simple* if there exists  $\alpha \in L$  such that  $L = K(\alpha)$ . In this situation  $\alpha$  is called a *primitive element* for  $L|K$ .

We already have a clear understanding of simple extensions where the corresponding primitive element is transcendental; cf. Proposition 4.2. In this section we look more closely at simple extensions where the corresponding primitive element is algebraic. It turns out that such extensions can be completely understood based on the minimum polynomial of the primitive element. The outcome is Kronecker's Theorem which constitutes a generalisation of Proposition 4.4.

**5.1. Kronecker's Theorem.** Let  $L|K$  be a field extension, and let  $\alpha \in L$  be algebraic over  $K$ . Then there is a unique ring homomorphism  $\eta : K[X] \rightarrow L$  which restricts to the identity on  $K$  and satisfies  $\eta(X) = \alpha$ . It is given by  $g \mapsto g(\alpha)$  and its image is the subring  $K[\alpha]$  of  $L$ . The kernel  $\ker(\eta)$  of the homomorphism  $\eta$  consists of all polynomials  $g \in K[X]$  such that  $g(\alpha) = 0$  and forms an ideal of  $K[X]$ . Polynomial division with remainder shows that  $\ker(\eta)$  is a principal ideal generated by  $f := \text{mipo}_K(\alpha)$ , in symbols  $\ker(\eta) = fK[X]$ . According to Proposition 4.4, the image  $K[\alpha]$  of the homomorphism  $\eta$  is a field and coincides with  $K(\alpha)$ .

Altogether we have the following inclusions and maps:

$$fK[X] = \ker(\eta) \subseteq K[X] \longrightarrow K[\alpha] = K(\alpha) \subseteq L.$$

The Isomorphism Theorem for rings, applied to  $\eta$ , shows that the field  $K(\alpha)$  is isomorphic to the quotient ring  $K[X]/fK[X]$  where  $f = \text{mipo}_K(\alpha)$ .

Let us recall the statement of the Isomorphism Theorem in its general form. Suppose that  $\eta : R \rightarrow S$  is a homomorphism of commutative rings with identity. Then  $\text{img}(\eta) := \{\eta(r) \mid r \in R\}$  forms a subring of  $S$ . Furthermore,  $\ker(\eta) := \{r \in R \mid \eta(r) = 0\}$  is an ideal of  $R$ . This means that  $\ker(\eta)$  forms an additive subgroup of  $R$  which is closed under multiplication by elements from  $R$ . If  $I$  is any ideal of  $R$ , the quotient ring  $R/I$  is the set of all additive cosets  $\bar{r} = r + I = \{r + x \mid x \in I\}$  and the ring operations are defined via representatives: for all  $r_1, r_2 \in R$  one has (i)  $\bar{r}_1 = \bar{r}_2$  if and only if  $r_1 - r_2 \in I$ , (ii)  $\bar{r}_1 + \bar{r}_2 = \overline{r_1 + r_2}$  and (iii)  $\bar{r}_1\bar{r}_2 = \overline{r_1r_2}$ . The Isomorphism Theorem states that there is a natural isomorphism of rings

$R/\ker(\eta) \rightarrow \text{img}(\eta)$  given by  $\bar{r} \mapsto \eta(r)$ . The essential and quite striking insight is that the homomorphic images of  $R$  in arbitrary rings can be described entirely in terms of the ideals of  $R$ .

Returning to the specific ring homomorphism  $\eta : K[X] \rightarrow K[\alpha]$  with kernel  $fK[X]$ , we remark that a convenient set of representatives for the elements of  $K[X]/fK[X]$  is given by the polynomials of degree strictly less than  $\deg(f)$ . In other words, the map  $\{g \in K[X] \mid \deg(g) < \deg(f)\} \rightarrow K[X]/fK[X]$ ,  $g \mapsto g + fK[X]$  is a bijection. This follows immediately from polynomial division with remainder.

By turning this analysis around, we can now create field extensions ‘into empty space’, starting from a base field  $K$ . For this we have to characterise internally those polynomials  $f \in K[X]$  which arise as (scalar multiples of) minimum polynomials of elements  $\alpha$  in potential field extensions  $L$  of  $K$ . The central feature of minimum polynomials is that they are irreducible. Recall that  $f \in K[X]$  is *irreducible* if (i)  $\deg(f) \geq 1$  and (ii) there exists no factorisation  $f = gh$  in  $K[X]$  with  $\deg(g), \deg(h) < \deg(f)$ .

**Theorem 5.1** (Kronecker’s Theorem). *Let  $f \in K[X]$ . Then there exists a simple field extension  $L = K(\alpha)$  of  $K$  with  $f(\alpha) = 0$ . If  $f$  is irreducible over  $K$ , then the extension  $L$  is unique in sense that the natural map*

$$K[X]/fK[X] \rightarrow L, \quad g + fK[X] \mapsto g(\alpha)$$

*constitutes an isomorphism.*

The uniqueness assertion in Kronecker’s Theorem can be stated more precisely as follows. Suppose that  $\iota : K \rightarrow K_*$  is an automorphism of fields. This extends to a natural automorphism  $\tilde{\iota} : K[X] \rightarrow K_*[X]$ . Let  $f \in K[X]$  be irreducible, and denote by  $f_*$  the image of  $f$  under  $\tilde{\iota}$ . Suppose that  $L = K(\alpha)$  where  $f(\alpha) = 0$  and that  $L_* = K_*(\alpha_*)$  where  $f_*(\alpha_*) = 0$ . Then there exists a unique isomorphism  $\hat{\iota} : L \rightarrow L_*$  such that  $\hat{\iota}|_K = \iota$  and  $\hat{\iota}(\alpha) = \alpha_*$ .

$$\begin{array}{ccc} L = K(\alpha) & \xrightarrow[\cong]{\tilde{\iota}} & L_* = K_*(\alpha_*) \quad (\cong K[X]/(f)) \\ \bullet & & \bullet \\ \downarrow & & \downarrow \\ K & \xrightarrow[\cong]{\iota} & K_* \\ \\ f \in K[X] & \xrightarrow[\cong]{\tilde{\iota}} & f_* \in K_*[X] \end{array}$$

*Example 5.2.* (1) Let  $K := \mathbb{R}$  and  $f := X^2 + 1$ . Then  $f$  is irreducible over  $K$ , and hence  $L := \mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[X]/(X^2 + 1)\mathbb{R}[X]$ .

(2) Let  $K := \mathbb{Q}$  and  $f := X^2 - 5$ . Then  $f$  is irreducible over  $K$ , and hence  $L := \mathbb{Q}(\sqrt{5}) \cong \mathbb{Q}[X]/(X^2 - 5)\mathbb{Q}[X]$ .

(3) Consider  $K := \mathbb{Q}$  and  $f := X^2 - 1 = (X - 1)(X + 1)$ . Note that  $f$  is not irreducible over  $K$ . Nevertheless we can consider the quotient ring  $R := \mathbb{Q}[X]/(X^2 - 1)\mathbb{Q}[X]$ . The Chinese Remainder Theorem implies that

$$R \cong \frac{\mathbb{Q}[X]}{(X - 1)\mathbb{Q}[X]} \times \frac{\mathbb{Q}[X]}{(X + 1)\mathbb{Q}[X]} \cong \mathbb{Q} \times \mathbb{Q}.$$

Here  $\mathbb{Q} \times \mathbb{Q}$  is regarded as a ring with respect to addition and multiplication defined component-wise. In particular,  $\mathbb{Q} \times \mathbb{Q}$  has zero-divisors and is therefore not a field.

An explicit isomorphism between  $R$  and  $\mathbb{Q} \times \mathbb{Q}$  can be obtained from the ring homomorphism  $\eta : \mathbb{Q}[X] \rightarrow \mathbb{Q} \times \mathbb{Q}$ ,  $f \mapsto (f(1), f(-1))$ . Observe that  $\eta$  maps onto  $\mathbb{Q} \times \mathbb{Q}$ : given any  $(a, b) \in \mathbb{Q} \times \mathbb{Q}$  we have  $\eta(a(X+1)/2 - b(X-1)/2) = (a, b)$ . Moreover,  $f \in \ker(\eta)$  if and only if  $(f(1), f(-1)) = (0, 0)$ , i.e. if and only if  $(X-1) \mid f$  and  $(X+1) \mid f$ . As  $X-1$  and  $X+1$  are coprime, this shows that  $\ker(\eta) = (X^2 - 1)\mathbb{Q}[X]$ . The Isomorphism Theorem for rings yields  $R = \mathbb{Q}[X]/(X^2 - 1)\mathbb{Q}[X] = \mathbb{Q}[X]/\ker(\eta) \cong \text{img}(\eta) = \mathbb{Q} \times \mathbb{Q}$ .  $\diamond$

**5.2. Polynomial rings – ‘rebooting your memory’.** Tacitly we have already used a few definitions and facts from the elementary theory of polynomial rings over fields. In this subsection we recall these results in a more systematic manner. By a *ring* we always mean a commutative ring with identity. A homomorphism between rings  $R \rightarrow S$  is always supposed to map the identity of  $R$  to the identity of  $S$ .

Let  $K$  be a field. There is a close analogy between the ring  $K[X]$  of polynomials over  $K$  and the ring of integers  $\mathbb{Z}$ . (In fact, both are examples of integral domains of dimension 1. Higher dimensional rings, such as  $K[X, Y]$  or  $\mathbb{Z}[X]$  are of considerable interest, but more difficult to handle. This would lead to the subject of Algebraic Geometry.)

The ring of integers  $\mathbb{Z}$  has the universal property that for any ring  $R$  there is a unique homomorphism  $\mathbb{Z} \rightarrow R$ . The ring  $K[X]$  also has a *universal property*: for any ring  $R$ , any homomorphism  $\eta : K \rightarrow R$  and any  $r \in R$  there is a unique homomorphism  $\hat{\eta} : K[X] \rightarrow R$  such that  $\hat{\eta}|_K = \eta$  and  $\hat{\eta}(X) = r$ .

The size of an integer  $m \in \mathbb{Z}$  is measured by the familiar absolute value  $|m| := \max\{m, -m\}$ . The size of a polynomial  $f \in K[X]$  is measured by its *degree*

$$\deg(f) := \begin{cases} n & \text{if } f = \sum_{k=0}^n f_k X^k \text{ and } f_n \neq 0, \\ -\infty & \text{if } f = 0 \end{cases}$$

The fact that  $K$  has no zero-divisors implies that the following degree formula holds

$$\deg(gh) = \deg(g) + \deg(h) \quad \text{for all } g, h \in K[X].$$

In particular,  $K[X]$  has no zero-divisors and is thus an integral domain.

The *group of units* of a ring  $R$  is the multiplicative group  $R^* := \{r \in R \mid \exists s \in R : rs = 1\}$ . The group of units of  $\mathbb{Z}$  is simply  $\{1, -1\}$ . The group of units of  $K[X]$  is typically much larger:

$$K[X]^* = \{f \in K[X] \mid \deg(f) = 0\} = K \setminus \{0\} = K^*.$$

A basic operation in the ring of integers is division with remainder. The corresponding operation on polynomials is captured by the following lemma.

**Lemma 5.3** (Division with remainder). *If  $f, g \in K[X]$  with  $f \neq 0$  then there exist unique polynomials  $q, r \in K[X]$  such that  $g = qf + r$  and  $\deg(r) < \deg(f)$ .*

Let  $g = qf + r$  in  $K[X]$  with  $\deg(r) < \deg(f)$ . The polynomial  $r$  is called the *remainder* of  $g$  divided by  $f$ . One says that  $f$  *divides*  $g$  in  $K[X]$ , written as  $f \mid g$ , if  $r = 0$ . The set of non-zero polynomials  $K[X] \setminus \{0\}$  decomposes into *divisibility*

*classes* where  $f, g \in K[X] \setminus \{0\}$  belong to the same class if  $f \mid g$  and  $g \mid f$ . It is easily seen that the divisibility class of  $g \in K[X] \setminus \{0\}$  is precisely  $gK[X]^* = gK^*$ . A non-zero polynomial  $f$  is said to be *monic* if its leading coefficient is equal to 1. Clearly, each divisibility class in  $K[X] \setminus \{0\}$  contains a unique monic representative.

Again the situation can be compared with the corresponding notions in the ring of integers  $\mathbb{Z}$ : here each divisibility class is of the form  $\{m, -m\}$  for  $m \neq 0$ , and one usually takes the positive integers  $\mathbb{N}$  as a set of representatives for the divisibility classes. An important role is played by the ‘irreducible’ positive integers, better known as prime numbers.

A polynomial  $f \in K[X] \setminus \{0\}$  is called *irreducible* if

- (i)  $f$  is not a unit, i.e. if  $f \notin K^*$ ,
- (ii) if  $f$  admits only trivial factorisations, i.e.  $f = gh$  in  $K[X]$  implies  $g \in K^*$  or  $h \in K^*$ .

A polynomial  $f \in K[X] \setminus \{0\}$  is called *reducible* if (i)  $f$  is not a unit and (ii) if  $f$  does admit a non-trivial factorisation. By induction one easily shows that every non-zero polynomial  $g \in K[X]$  can be written as a product of a unit and a certain number of irreducible polynomials. The important insight that this factorisation is essentially unique requires comparatively more effort and rests on the fact that irreducible polynomials are prime; see below.

In  $K[X]$  as in  $\mathbb{Z}$  division with remainder allows one to show that every ideal is principal, i.e. generated by a single element. Given  $f, g \in K[X]$  any polynomial  $h \in K[X]$  with  $hK[X] = fK[X] + gK[X]$  is called a *highest common factor* of  $f, g$ . Unless they are both zero,  $f$  and  $g$  possess a unique monic highest common factor. This polynomial is called the *greatest common divisor* of  $f, g$  and denoted by  $\gcd(f, g)$ . Similarly as in  $\mathbb{Z}$ , an effective method for determining the greatest common divisor of two polynomials is given by the Euclidean algorithm.

The existence of highest common factors implies that every irreducible polynomial is *prime*: if  $f \in K[X]$  is irreducible and  $f \mid gh$  where  $g, h \in K[X]$ , then  $f \mid g$  or  $f \mid h$ . From this property one derives that  $K[X]$ , like  $\mathbb{Z}$ , is a *unique factorisation domain*: every  $f \in K[X] \setminus \{0\}$  admits a factorisation  $f = \alpha g_1 \cdots g_r$  where  $\alpha \in K^*$  and  $g_1, \dots, g_r \in K[X]$  are monic and irreducible; moreover,  $\alpha$  is uniquely determined and  $g_1, \dots, g_r$  are uniquely determined up to permutation.

We emphasise two important consequences of this general theory.

**Proposition 5.4.** *Let  $K$  be a field,  $f \in K[X]$  and  $\alpha \in K$ . Then  $f(\alpha) = 0$  if and only if  $(X - \alpha) \mid f$ .*

**Corollary 5.5.** *Let  $K$  be a field and  $f \in K[X]$  of degree  $n := \deg(f)$ . Then  $f$  admits at most  $n$  distinct roots in  $K$ .*

**Proposition 5.6.** *Let  $K$  be a field and  $f \in K[X]$ . Then there exists a field extension  $L|K$  such that  $f$  splits over  $L$  into a product of linear factors.*

*Proof.* This follows by induction on the degree of  $f$  from Kronecker’s Theorem.  $\square$

Let  $L|K$  be a field extension and  $f \in K[X]$ . Suppose that  $f$  decomposes over  $L$  into a product of linear factors  $f = (X - \alpha_1) \cdots (X - \alpha_n)$ . Then  $K(\alpha_1, \dots, \alpha_n)$  is the smallest intermediate field of the extension  $L|K$  over which  $f$  splits into a product of linear factors. Accordingly, this field is called a *splitting field* for  $f$

over  $K$ . It can be shown that any two splitting fields for  $f$  over  $K$  are, in fact, isomorphic over  $K$ .

**5.3. Irreducible Polynomials.** In view of Kronecker's Theorem we are particularly interested in irreducible polynomials. We recall some basic irreducibility criteria. The first proposition is very easy to prove.

**Proposition 5.7.** *Let  $K$  be a field and  $f \in K[X]$  with  $\deg(f) \in \{2, 3\}$ . Then  $f$  is irreducible over  $K$  if and only if  $f$  does not have a root in  $K$ .*

A substantially more important and useful result is

**Proposition 5.8** (Gauss' Lemma). *Let  $f \in \mathbb{Z}[X]$  be monic, and suppose that  $f = gh$  where  $g, h \in \mathbb{Q}[X]$  are also monic. Then  $g, h \in \mathbb{Z}[X]$ .*

*Proof.* Write the coefficients of  $g$  in lowest terms with positive denominators. Define  $a \in \mathbb{N}$  to be the lowest common multiple of all these 'reduced' denominators. Then  $\tilde{g} := ag \in \mathbb{Z}[X]$  and, because the original polynomial  $g$  is monic, the leading term of  $\tilde{g}$  is equal to  $a$ . From this one sees that the greatest common divisor of the coefficients of  $\tilde{g}$  is equal to 1. Do the same for  $h$  to find  $b \in \mathbb{N}$  such that  $\tilde{h} := bh \in \mathbb{Z}[X]$  also has the property that the greatest common divisor of its coefficients is equal to 1.

Put  $n := ab$  so that  $nf = \tilde{g}\tilde{h}$ . It suffices to show that  $n = 1$ , because this implies  $a = b = 1$  and hence  $g = \tilde{g}, h = \tilde{h} \in \mathbb{Z}[X]$  as wanted. Assume for a contradiction that  $n > 1$ . Let  $p$  be a prime divisor of  $n$  and consider the congruence  $0 \equiv nf = \tilde{g}\tilde{h}$  modulo  $p\mathbb{Z}[X]$ . Since  $p$  does not divide all the coefficients of  $\tilde{g}$ , we have  $\tilde{g} \not\equiv 0$  modulo  $p\mathbb{Z}[X]$ . But  $\mathbb{Z}/p\mathbb{Z}$  is a field, and so  $\mathbb{Z}[X]/p\mathbb{Z}[X] \cong (\mathbb{Z}/p\mathbb{Z})[X]$  is an integral domain. This implies that  $\tilde{h} \equiv 0$  modulo  $p\mathbb{Z}[X]$  and consequently all the coefficients of  $\tilde{h}$  are divisible by  $p$ . This is the required contradiction.  $\square$

Frequently the following corollary is also referred to as Gauss' Lemma.

**Corollary 5.9** (Gauss' Lemma). *Let  $f \in \mathbb{Z}[X]$  be irreducible over  $\mathbb{Z}$ , i.e. suppose that  $f$  is not constant and cannot be written as a product of polynomials of degree smaller than  $\deg(f)$ . Then  $f$  is irreducible over  $\mathbb{Q}$ .*

*Proof.* For a contradiction suppose that  $f = gh$  in  $\mathbb{Q}[X]$  with  $\deg(g), \deg(h) < \deg(f)$ . Clearing denominators, we obtain

$$nf = \tilde{g}\tilde{h} \quad \text{where } n \in \mathbb{N} \text{ and } \tilde{g}, \tilde{h} \in \mathbb{Z}[X].$$

We argue by induction on  $n$  that  $f$  is reducible over  $\mathbb{Z}$ . If  $n = 1$ , this is immediate. Now suppose that  $n > 1$ . Then  $n$  has a prime divisor  $p$  and, using reduction modulo  $p$  as in the second part of the proof of Proposition 5.8, we show that without loss of generality  $p$  divides all the coefficients of  $\tilde{g}$ . Replacing  $n$  by  $n/p$  and  $\tilde{g}$  by  $p^{-1}\tilde{g} \in \mathbb{Z}[X]$ , we conclude from the induction hypothesis that  $f$  is reducible over  $\mathbb{Z}$ .  $\square$

Based on Gauss' Lemma we can now prove Eisenstein's Criterion which is useful, for instance, for producing explicitly irreducible polynomials over  $\mathbb{Q}$  of arbitrarily high degree.

**Proposition 5.10** (Eisenstein's Criterion). *Let  $f = \sum_{k=0}^n f_k X^k \in \mathbb{Z}[X]$  with  $n = \deg(f) \geq 1$ , and let  $p$  be a prime. Suppose that*

$$p \nmid f_n, \quad p \mid f_k \quad \text{for } k \in \{0, \dots, n-1\}, \quad \text{and } p^2 \nmid f_0.$$

*Then  $f$  is irreducible over  $\mathbb{Q}$ .*

*Proof.* By Gauss' Lemma it suffices to show that  $f$  is irreducible over  $\mathbb{Z}$ . Suppose that  $f = gh$  with  $g, h \in \mathbb{Z}[X]$ . We have to show that  $\deg(g) = 0$  or  $\deg(h) = 0$ . Clearly,  $d := \deg(g) \leq n$  and  $\deg(h) = n - d$ . Write  $g = \sum_{k=0}^d g_k X^k$  and  $h = \sum_{k=0}^{n-d} h_k X^k$  accordingly. The equation  $f = gh$  is equivalent to the system of equations

$$f_m = \sum_{k=0}^m g_k h_{m-k} \quad \text{for all } k \in \{0, 1, \dots, n\}.$$

The condition  $p \nmid f_n = g_d h_{n-d}$  implies that  $p \nmid g_d, h_{n-d}$ . The conditions  $p \mid f_0 = g_0 h_0$  and  $p^2 \nmid f_0 = g_0 h_0$  imply that precisely one of the elements  $g_0, h_0$  is divisible by  $p$ . Without loss of generality suppose that  $p \mid g_0$  and  $p \nmid h_0$ . As  $p \nmid g_d$  this implies  $d > 0$  and we may define  $m := \min\{k \mid 1 \leq k \leq d, p \nmid k\}$ . Now consider the equation  $f_m = \sum_{k=0}^{m-1} g_k h_{m-k} + g_m h_0$ . Every term of the left hand sum is divisible by  $p$ , but  $g_m h_0$  is not divisible by  $p$ . This implies  $p \nmid f_m$  and hence  $m = n$ . We obtain  $\deg(g) = n$  and  $\deg(h) = n - \deg(g) = 0$  as wanted.  $\square$

*Example 5.11.* Let  $p$  be a prime. Then  $X^p - 1 \in \mathbb{Z}[X]$  has 1 as a root and is therefore reducible. We claim that

$$f := \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \dots + X^2 + X + 1$$

is irreducible over  $\mathbb{Q}$ . As it stands we cannot apply Eisenstein's Criterion. Therefore we perform a well-chosen change of variable. For any  $a \in \{1, -1\}$  and  $b \in \mathbb{Z}$  the map  $\mathbb{Z}[X] \rightarrow \mathbb{Z}[Y]$ ,  $g \mapsto g(aY + b)$  constitutes an isomorphism between the polynomial rings  $\mathbb{Z}[X]$  and  $\mathbb{Z}[Y]$ . (Evaluation at other polynomials in  $Y$  would still give a homomorphism  $\mathbb{Z}[X] \rightarrow \mathbb{Z}[Y]$ , but the map would fail to be surjective.) Clearly, the property of being irreducible or not is invariant under isomorphisms.

Our discussion shows that  $f$  is irreducible over  $\mathbb{Q}$  if and only if

$$\begin{aligned} g(Y) := f(Y + 1) &= \frac{(Y + 1)^p - 1}{(Y + 1) - 1} = \sum_{k=1}^p \binom{p}{k} Y^{k-1} \\ &= Y^{p-1} + \binom{p}{p-1} Y^{p-2} + \binom{p}{p-2} Y^{p-3} + \dots + \binom{p}{2} Y + \binom{p}{1} \end{aligned}$$

is irreducible over  $\mathbb{Q}$ . Expanding the coefficients

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{1 \cdot 2 \cdots p}{(1 \cdot 2 \cdots k)(1 \cdot 2 \cdots (p-k))}, \quad 1 \leq k < p$$

we see that each of the non-leading coefficients of  $g$  is divisible by  $p$  but not by  $p^2$ . By Eisenstein's Criterion  $g$  is indeed irreducible over  $\mathbb{Q}$ .  $\diamond$

## 6. BASIC THEORY OF FINITE FIELDS

**6.1. Prime fields and characteristic.** Every field  $K$  contains a unique *prime subfield*, i.e. a subfield which itself contains no proper subfields. Indeed, the prime subfield of  $K$  is given by the intersection of all subfields of  $K$  (cf. Exercise 1.3). Alternatively, the prime subfield of  $K$  can be described as the field of fractions

of the image of the canonical ring homomorphism  $\mathbb{Z} \rightarrow K$ ,  $m \mapsto m \cdot 1$ . A *prime field* is a field which is equal to its prime subfield, i.e. which does not possess any proper subfields. The prime fields are up to isomorphism precisely the fields  $\mathbb{Q}$  and  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$  where  $p$  is a prime. The *characteristic* of  $K$  is defined as

$$\text{char}(K) := \begin{cases} 0 & \text{if the prime subfield of } K \text{ is isomorphic to } \mathbb{Q}, \\ p & \text{if the prime subfield of } K \text{ is isomorphic to } \mathbb{F}_p. \end{cases}$$

If  $\text{char}(K) = p > 0$ , then  $p = \underbrace{1 + \dots + 1}_{p \text{ summands}} = 0$  in  $K$ .

If  $K$  is a finite field, then  $K$  cannot have any subfield isomorphic to  $\mathbb{Q}$  and hence  $\text{char}(K) = p > 0$ . There exist infinite fields which have positive characteristic, e.g. the field of rational functions  $\mathbb{F}_p(t)$  over a finite field  $\mathbb{F}_p$ .

### 6.2. Existence and uniqueness of finite fields of prescribed cardinality.

**Proposition 6.1.** *Let  $K$  be a finite field, and set  $p := \text{char}(K)$ . Then the cardinality of  $K$  is a power of  $p$ . Indeed,  $|K| = p^d$  where  $d$  is the degree of  $K$  over its prime subfield  $K_0 \cong \mathbb{F}_p$ .*

*Proof.* Regarding  $K$  as a vector space over its prime subfield  $K_0 \cong \mathbb{F}_p$ , we have  $|K| = |K_0^d| = |K_0|^d = p^d$ .  $\square$

**Theorem 6.2** (Existence and Uniqueness Theorem). *Let  $p$  be a prime and  $d \in \mathbb{N}$ . Then there exists a finite field of cardinality  $p^d$ . Moreover, any two such fields are isomorphic.*

Extending the notation  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ , we shall freely write  $\mathbb{F}_{p^d}$  for any field of cardinality  $p^d$ . According to the theorem all such fields are isomorphic, but one should keep in mind that for  $d \geq 2$  there is no canonical choice of any particular field of cardinality  $p^d$ .

The proof of Theorem 6.2 requires some preparation.

**Proposition 6.3.** *Let  $K$  be a field of characteristic  $p > 0$ . Then the map  $F : K \rightarrow K$ ,  $\alpha \mapsto \alpha^p$  constitutes a field endomorphism, the so-called Frobenius endomorphism of  $K$ .*

*Proof.* Let  $\alpha, \beta \in K$ . Clearly,  $F(1) = 1^p = 1$  and it suffices to prove that

$$F(\alpha + \beta) = F(\alpha) + F(\beta) \quad \text{and} \quad F(\alpha\beta) = F(\alpha)F(\beta).$$

The second assertion is immediate from  $(\alpha\beta)^p = \alpha^p\beta^p$ . For the first assertion we recall from Example 5.11 that the integer  $\binom{p}{k}$  is divisible by  $p$  for  $1 \leq k \leq p-1$ . This implies that

$$(\alpha + \beta)^p = \sum_{k=0}^p \binom{p}{k} \alpha^k \beta^{p-k} = \alpha^p + \sum_{k=1}^{p-1} \binom{p}{k} \alpha^k \beta^{p-k} + \beta^p = \alpha^p + \beta^p.$$

This shows that  $F(\alpha + \beta) = F(\alpha) + F(\beta)$  as wanted.  $\square$

Let  $K$  be a field of characteristic  $p > 0$ . Since the trivial ideal  $\{0\}$  is the only proper ideal of  $K$ , the Frobenius endomorphism  $F : K \rightarrow K$  is automatically injective. In general, the image of  $F$  is a proper subfield of  $K$ . For instance, if  $K = \mathbb{F}_p(t)$  then  $F(K) = \mathbb{F}_p(t^p)$ . But if  $K$  is a finite field, then every injective map from  $K$  into itself has to be surjective. This gives

**Corollary 6.4.** *Let  $K$  be a finite field of characteristic  $p$ . Then the Frobenius endomorphism  $K \rightarrow K$ ,  $\alpha \mapsto \alpha^p$  is an automorphism of  $K$ .*

**Corollary 6.5.** *Let  $K$  be a field of characteristic  $p > 0$  and  $d \in \mathbb{N}_0$ . Then the ‘fixed set’  $\{\alpha \in K \mid \alpha^{p^d} = \alpha\}$  is a subfield of  $K$ .*

*Proof.* The set under consideration is the set of fixed points of the map  $K \rightarrow K$ ,  $\alpha \mapsto \alpha^{p^d}$ . But this map is equal to  $F^d$ , the  $d$ -fold composition of the Frobenius endomorphism of  $K$  with itself.

It is a general principle that the fixed set of any field endomorphism  $E : K \rightarrow K$  constitutes a subfield of  $K$ . Indeed,  $E(0) = 0$  and  $E(1) = 1$ . Moreover, for  $\alpha, \beta \in K$  with  $E(\alpha) = \alpha$  and  $E(\beta) = \beta$  one has

$$\begin{aligned} E(\alpha + \beta) &= E(\alpha) + E(\beta) = \alpha + \beta, \\ E(-\alpha) &= E(0 - \alpha) = E(0) - E(\alpha) = -\alpha, \\ E(\alpha\beta) &= E(\alpha)E(\beta) = \alpha\beta, \end{aligned}$$

and finally, if  $\alpha \neq 0$ , then  $E(\alpha) \neq 0$  and

$$E(\alpha^{-1}) = E(1/\alpha) = E(1)/E(\alpha) = \alpha^{-1}.$$

This shows that the fixed set  $\{\alpha \in K \mid E(\alpha) = \alpha\}$  is a subfield of  $K$ .  $\square$

The main idea of the proof of Theorem 6.2 is to construct and characterise finite fields of prescribed cardinalities as appropriate fixed sets of suitable automorphisms of larger fields.

**Lemma 6.6.** *Let  $K$  be a finite field of characteristic  $p$  and cardinality  $p^d$ . Then  $\alpha^{p^d} = \alpha$  for all  $\alpha \in K$ .*

*Proof.* Recall that the order of a group  $G$  is its cardinality  $|G|$ . The order of an element  $g$  of  $G$  is the size of the cyclic subgroup generated by  $g$ , i.e.  $\text{ord}(g) = |\langle g \rangle|$  where  $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ . If  $g$  has finite order, then  $\text{ord}(g)$  can also be described as the smallest natural number  $n$  such that  $g^n = 1$ . If  $G$  is a finite group, then Lagrange’s Theorem states that the order of any subgroup  $H$  of  $G$  divides the order of  $G$ , in symbols  $|H|$  divides  $|G|$ . In particular,  $\text{ord}(g)$  divides  $|G|$  and hence  $g^{|G|} = 1$ .

Clearly,  $K^* = K \setminus \{0\}$  is an abelian group of order  $|K^*| = p^d - 1$ . Our discussion shows that  $\alpha^{p^d - 1} = 1$  for all  $\alpha \in K \setminus \{0\}$  and consequently  $\alpha^{p^d} = \alpha \cdot \alpha^{p^d - 1} = \alpha \cdot 1 = \alpha$  for all  $\alpha \in K$ .  $\square$

We need to recall another basic fact from the theory of finite groups. Let  $G$  be a finite group. The *exponent* of  $G$  is the invariant  $\exp(G) := \text{lcm}\{\text{ord}(g) \mid g \in G\}$ , i.e. the smallest natural number  $e$  such that  $g^e = 1$  for all  $g \in G$ . Lagrange’s Theorem implies that  $\exp(G)$  divides  $|G|$ , and it is clear that  $\exp(G) \geq \max\{\text{ord}(g) \mid g \in G\}$ .

If  $G$  is abelian, the latter inequality actually becomes an equality:  $\exp(G) = \max\{\text{ord}(g) \mid g \in G\}$ . This is a consequence of the following fact which is verified by a direct computation: if  $g, h \in G$  with  $\text{gcd}(\text{ord}(g), \text{ord}(h)) = 1$  and  $gh = hg$ , then  $\langle gh \rangle = \langle g \rangle \times \langle h \rangle$  and in particular  $\text{ord}(gh) = \text{ord}(g) \text{ord}(h)$ . Now suppose that  $G$  is an abelian group with  $\exp(G) = |G|$ . Then  $G$  has an element  $g$  of order  $|G|$ , and consequently  $G = \langle g \rangle$  is cyclic.

**Proposition 6.7.** *Let  $K$  be a field. Then every finite subgroup of  $K^*$  is cyclic.*

*Moreover, if  $G$  a subgroup of  $K^*$  of order  $n$ , then the polynomial  $X^n - 1$  has  $n$  distinct roots in  $K$  and these roots constitute the group  $G$ .*

*Proof.* Let  $K$  be a field, and let  $G$  be a finite subgroup of  $K^*$ . Put  $n := |G|$ . In view of our discussion above, it suffices to show that  $\exp(G) = n$ . Since  $\exp(G) \mid |G|$  we certainly have  $\exp(G) \leq n$ . Write  $e := \exp(G)$ . Then  $G \subseteq \{\alpha \in K \mid \alpha^e = 1\}$ . But  $\{\alpha \in K \mid \alpha^e = 1\}$  is the set of roots of the polynomial  $X^e - 1$  in  $K$  and has size at most  $e$ . This shows that  $n = |G| \leq e \leq n$ . This implies  $e = n$  and  $G = \{\alpha \in K \mid \alpha^n - 1 = 0\}$  as wanted.  $\square$

**Corollary 6.8.** *The multiplicative group of a finite field is cyclic.*

Let  $K$  be a finite field and  $\alpha \in K$ . Then  $\alpha$  is called a *primitive element* of  $K$  if  $\alpha$  generates the multiplicative group  $K^*$ . We have proved that every finite fields admits primitive elements.

Adhering to the traditional terminology, we cannot avoid a small, but unfortunate overlap with the notion of a ‘primitive element’ which we encountered in Section 5. A primitive element for a simple field extension  $L|K$  is any element  $\alpha \in L$  such that  $L = K(\alpha)$ . If  $L$  is a finite field, then any primitive element of  $L$  (in the new sense) is a fortiori a primitive element for the extension  $L|K$ , but conversely a primitive element for  $L|K$  need not be a primitive element of  $L$ .

**Corollary 6.9.** *Every extension  $L|K$  of finite fields is simple.*

We are now ready to prove the existence and uniqueness of finite fields of prescribed cardinality.

*Proof of Theorem 6.2.* Let  $p$  be a prime, let  $d \in \mathbb{N}$  and write  $q := p^d$ . First we prove the existence part. Based on Kronecker’s Theorem and an inductive argument (cf. Exercise 3.3) we obtain a splitting field  $K$  for  $X^q - X$  over the prime field  $\mathbb{F}_p$ . This means that  $X^q - X$  splits into a product of linear factors over  $K$ , but over no proper subfield of  $K$ . From Corollary 6.5 we know that the fixed set  $\{\alpha \in K \mid \alpha^q = \alpha\}$  is a subfield and hence equal to  $K$ . Since  $X^q - X$  admits at most  $q$  roots, this shows that  $|K| \leq q$  and it suffices to show that  $X^q - X$  has  $q$  distinct roots in  $K$ .

Now  $X^q - X = X(X^{q-1} - 1)$  and  $X \nmid (X^{q-1} - 1)$ . Hence 0 is not a repeated root of  $X^q - X$ . Now suppose for a contradiction that  $(X - \alpha) \mid (X^{q-1} - 1)$  for  $\alpha \in K \setminus \{0\}$ . Then we can write  $X^{q-1} - 1 = (X - \alpha) \cdot (X - \alpha)g$  for a suitable  $g \in K[X]$ . Taking formal derivatives and evaluating at  $\alpha$  yields

$$(q-1)\alpha^{q-2} = \underbrace{(1 \cdot (X - \alpha)g)|_{X=\alpha}}_{=0} + \underbrace{((X - \alpha)((X - \alpha)g)')|_{X=\alpha}}_{=0} = 0.$$

But  $q - 1 = -1 \neq 0$  in  $K$  and  $\alpha \neq 0$ . This is the required contradiction.

Now we prove the uniqueness part. Suppose that  $K_1, K_2$  are fields of cardinality  $q$ . Without loss of generality we may assume that they share the same prime subfield  $\mathbb{F}_p$ . Then the argument above shows that each of the fields  $K_1, K_2$  is a splitting field for  $X^q - X$  over  $\mathbb{F}_p$ . Factorise  $X^q - X$  over  $\mathbb{F}_p$  to find an irreducible factor  $f$  and  $\alpha_1 \in K_1$  such that  $f(\alpha_1) = 0$  and  $K_1 = \mathbb{F}_p(\alpha_1)$ , e.g. take  $f$  to be the

minimum polynomial of a primitive element  $\alpha_1 \in K_1$ . Since  $K_2$  is a splitting field for  $X^q - X$  over  $\mathbb{F}_p$ , we find  $\alpha_2 \in K_2$  with  $f(\alpha_2) = 0$ . By Kronecker's Theorem,

$$K_1 = \mathbb{F}_p(\alpha_1) \cong \frac{\mathbb{F}_p[X]}{f\mathbb{F}_p[X]} \cong \mathbb{F}_p(\alpha_2) \subseteq K_2.$$

The equality  $|K_1| = q = |K_2|$  now implies  $\mathbb{F}_p(\alpha_2) = K_2$  and hence  $K_1 \cong K_2$ .  $\square$

## 7. AN APPLICATION: DISCRETE LOGARITHMS

**7.1. Discrete logarithm.** Let  $G = \langle g \rangle$  be a finite cyclic group of order  $m$ . Then the kernel of the natural projection  $\mathbb{Z} \rightarrow G$ ,  $k \mapsto g^k$  is  $m\mathbb{Z}$ , and one obtains an induced isomorphism  $\mathbb{Z}/m\mathbb{Z} \rightarrow G$ . The inverse of this isomorphism is the *discrete logarithm map* with respect to the generator  $g$ ,

$$\log_g : G \rightarrow \mathbb{Z}/m\mathbb{Z}, \quad g^k \mapsto k + m\mathbb{Z}.$$

Notice that, since we are writing  $G$  multiplicatively and  $\mathbb{Z}/m\mathbb{Z}$  additively, the discrete logarithm map satisfies the familiar basic formulae of the ordinary logarithm function for real numbers. For instance, if  $\tilde{g}$  is another generator of  $G$ , then  $\log_g(h) = \log_g(\tilde{g}) \log_{\tilde{g}}(h)$ .

*Example 7.1.* Let  $K$  be a finite field of cardinality  $q$ . Then  $G := K^*$  is a cyclic group of order  $m := q - 1$ , and we take a primitive element  $g := \alpha$  of  $K$  as a generator for  $G$ . For instance, consider the field  $K = \mathbb{F}_{17}$  with primitive element  $\alpha = 3$ . One easily computes the powers of  $\alpha$ .

$k$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\alpha^k$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

$\diamond$

**7.2. Diffie-Hellman key exchange and El Gamal encryption.** Let  $G = \langle g \rangle$  be a finite cyclic group of order  $m$ . For instance, consider  $G = \mathbb{F}_q^*$  for a finite field  $\mathbb{F}_q$  of cardinality  $q$  so that  $m = q - 1$ , and let  $g = \alpha$  be a primitive element of  $\mathbb{F}_q$ . Suppose that  $\mathbb{F}_q$  is realised as a quotient ring  $\mathbb{F}_p[X]/f\mathbb{F}_p[X]$  where  $f \in \mathbb{F}_p[X]$  is a suitable irreducible polynomial; cf. Kronecker's Theorem. Then a natural set of representatives for the elements of  $\mathbb{F}_q$  is formed by the polynomials  $b \in \mathbb{F}_p[X]$  satisfying  $\deg(b) < \deg(f)$ . In this case one can efficiently compute powers of  $\alpha$ , using polynomial arithmetic modulo  $f$ . But taking the discrete logarithm  $\log_\alpha(\beta)$  of  $\beta \in \mathbb{F}_q$  (represented by  $b \in \mathbb{F}_p[X]$ ) with respect to  $\alpha$  (represented by  $a \in \mathbb{F}_p[X]$ ) is considered to be difficult. In this concrete realisation, the exponentiation map  $\mathbb{Z}/m\mathbb{Z} \rightarrow G$ ,  $k \mapsto g^k$  therefore constitutes a candidate for what is called a 'one-way function' and can be used for the purpose of encryption.

Suppose that Alice and Bob want to arrange a common secret key over an insecure channel. All information passed through that channel can be read (but not manipulated) by an eavesdropper Eve. Here is a well-known procedure, the *Diffie-Hellman key exchange*, which is based on the discrete logarithm problem.

- (1) Alice and Bob agree on a finite cyclic group  $G = \langle g \rangle$  of order  $m$ . For instance, they choose  $G = \mathbb{F}_q^*$  for a finite field  $\mathbb{F}_q$  of cardinality  $q$  so that  $m = q - 1$ , and they fix a primitive element  $g = \alpha$  of  $\mathbb{F}_q$ . All this information and the entire procedure under discussion are public knowledge.

- (2) Now Alice picks a secret element  $a \in \mathbb{Z}/m\mathbb{Z}$ , and Bob picks a secret element  $b \in \mathbb{Z}/m\mathbb{Z}$ . They keep this information private.
- (3) Alice computes  $g^a$  and sends the result to Bob. Bob computes  $g^b$  and sends the result to Alice. The two elements  $g^a, g^b$  are possibly picked up by the eavesdropper Eve.
- (4) Alice computes  $(g^b)^a$ , whereas Bob computes  $(g^a)^b$ . They now share the common secret key  $h := g^{ab} = (g^a)^b = (g^b)^a$ . – If Eve wanted to discover this secret key, she would have to compute  $h$  based on the information  $G = \langle g \rangle$ ,  $g^a$  and  $g^b$ . E.g. if she was able to compute discrete logarithms, she could simply work out  $a = \log_g(g^a)$  and use this to obtain  $(g^b)^a = h$ .

Alice and Bob can subsequently use their common secret key to exchange private information over an insecure channel. We give a self-contained description of the *El Gamal cryptosystem*, which is closely related to the Diffie-Hellman key exchange.

- (1) Alice and Bob agree on a finite cyclic group  $G = \langle g \rangle$  of order  $m$ . For instance, they choose  $G = \mathbb{F}_q^*$  for a finite field  $\mathbb{F}_q$  of cardinality  $q$  so that  $m = q-1$ , and they fix a primitive element  $g = \alpha$  of  $\mathbb{F}_q$ . All this information and the entire procedure under discussion are public knowledge.
- (2) Suppose Bob wants to be able to receive secret messages from Alice. He picks a secret element  $b \in \mathbb{Z}/m\mathbb{Z}$  which he keeps private. Then he computes  $g^b$  and sends the result to Alice. The element  $g^b$  is possibly picked up by the eavesdropper Eve.
- (3) Alice wants to send the secret message  $x \in G$  to Bob. She chooses a secret element  $a \in \mathbb{Z}/m\mathbb{Z}$  which she keeps private. Then she computes  $g^a$  and  $x(g^b)^a = xg^{ab}$ , and sends these elements to Bob. Again Eve may listen in and pick up  $g^a, xg^{ab}$ .
- (4) Bob recovers Alice's secret message by computing  $x = (xg^{ab})((g^a)^b)^{-1}$ . – If Eve wanted to discover the secret message, she would have to compute  $x$  based on the information  $G = \langle g \rangle$ ,  $g^a, g^b$  and  $xg^{ab}$ . Clearly, this task is equally difficult as computing the secret key  $g^{ab}$  in the Diffie-Hellman procedure.

*Example 7.2.* Realise a field of cardinality 32 as  $\mathbb{F}_{32} = \mathbb{F}_2(\alpha)$  where  $\alpha$  is a root of the irreducible polynomial  $X^5 + X^2 + 1 \in \mathbb{F}_2[X]$ . Observe that the cyclic group  $\mathbb{F}_{32}^*$  has prime order 31. This implies that every element other than 1 generates the group. In particular,  $\alpha$  is a primitive element of  $\mathbb{F}_{32}$ . Hence Alice and Bob may consider  $G = \mathbb{F}_{32}^*$  with generator  $g = \alpha$ . Suppose Bob chooses  $b = 5$ . Then he sends  $g^b = \alpha^2 + 1$  to Alice. Suppose that Alice's message for Bob is  $x = \alpha^4 + \alpha^2 + 1$  and that she picks  $a = 4$ . Then she sends  $g^a = \alpha^4$  and

$$\begin{aligned}
 x(g^b)^a &= (\alpha^4 + \alpha^2 + 1)(\alpha^2 + 1)^4 \\
 &= (\alpha^4 + \alpha^2 + 1)(\alpha^8 + 1) \\
 &= (\alpha^4 + \alpha^2 + 1)(\alpha^3 + \alpha^2) \\
 &= \alpha^2 + \alpha + 1.
 \end{aligned}$$

From this Bob computes the message

$$\begin{aligned}
 (xg^{ab})((g^a)^b)^{-1} &= (\alpha^2 + \alpha + 1)((\alpha^4)^5)^{-1} \\
 &= (\alpha^2 + \alpha + 1)\alpha^{11} \\
 &= (\alpha^2 + \alpha + 1)(\alpha^5)^2\alpha \\
 &= (\alpha^2 + \alpha + 1)(\alpha^2 + 1)^2\alpha \\
 &= (\alpha^2 + \alpha + 1)(\alpha^2 + \alpha + 1) \\
 &= \alpha^4 + \alpha^2 + 1.
 \end{aligned}$$

◇

**7.3. Algorithms for computing discrete logarithms.** We discuss three methods for computing discrete logarithms, namely complete enumeration, the Baby-step Giant-step Algorithm and the Pohlig-Hellman Algorithm.

**7.3.1. Complete enumeration.** Given  $G = \langle g \rangle \cong \mathbb{Z}/m\mathbb{Z}$  and  $h \in G$ , the task is to find the discrete logarithm  $\log_g(h)$ . This can be done by *complete enumeration*: compute successively  $1 = g^0$ ,  $g = g^1$ ,  $g^2 = g^1 \cdot g$ ,  $\dots$ ,  $g^{n+1} = g^n \cdot g$ ,  $\dots$  until  $h = g^n$ , and output  $n = \log_g(h)$  modulo  $m$ . This rather naive procedure requires roughly  $m$  operations in  $G$ . It is a fast algorithm, if  $m$  is small, but non-effective if  $m$  is large.

**7.3.2. Baby-step Giant-step Algorithm.** Given  $G = \langle g \rangle \cong \mathbb{Z}/m\mathbb{Z}$  and  $h \in G$ , the task is to find the discrete logarithm  $\log_g(h)$ . This can be done by computing two sequences of elements in  $G$ , the *baby sequence* and the *giant sequence*, as follows. Put  $M := \lceil \sqrt{m} \rceil$  and determine  $g^M$ . Then compute

- the babies  $h, hg, hg^2 = (hg)g, \dots, hg^{M-1} = (hg^{M-2})g$  with steps  $g$ ,
- the giants  $g^M, g^{2M} = g^M g^M, \dots, g^{M^2} = g^{(M-1)M} g^M$  with steps  $g^M$ .

Locate a common member of the two sequences,  $hg^i = g^{jM}$  say. Then  $h = g^{jM-i}$  and consequently  $\log_g(h)$  equals  $jM - i$  modulo  $m$ . The algorithm works because every possible exponent can be expressed as  $k = jM - i$  modulo  $m$  with  $i \in \{0, 1, \dots, M-1\}$  and  $j \in \{1, 2, \dots, M\}$ .

*Example 7.3.* Consider  $G = \mathbb{F}_{29}^*$  with generator  $g = 2$ , and  $h = 3$ . Then  $m = 28$  and  $M = \lceil \sqrt{m} \rceil = 6$ . We compute up to six babies and up to six giants:

- $h = 3, \quad hg = 3 \cdot 2 = 6, \quad hg^2 = 6 \cdot 2 = 12, \quad hg^3 = 12 \cdot 2 = -5,$   
 $hg^4 = -5 \cdot 2 = -10, \quad hg^5 = -10 \cdot 2 = 9,$
- $g^6 = 6, \quad g^{12} = 6 \cdot 6 = 7, \quad g^{18} = 7 \cdot 6 = 13, \quad g^{24} = 13 \cdot 6 = -9,$   
 $g^{30} = -9 \cdot 6 = 4, \quad g^{36} = 4 \cdot 6 = -5.$

In practise, one can stop as soon as one finds one common member. Looking at the complete lists we actually locate two common members:  $hg = 6 = g^6$  and  $hg^3 = -5 = g^{36}$ . The former gives  $h = g^5$ , the later  $h = g^{33} = g^5$ . Accordingly the discrete logarithm of  $h$  is 5 (modulo 28). ◇

Comparing to lists of length  $M$  in the naive way takes roughly  $M^2$  single comparisons. If one keeps the lists sorted, the Baby-step Giant-step Algorithm requires roughly  $M$  steps (operations or comparisons in  $G$ ) as well as a storage space of size roughly  $M$ . The algorithm is a good example of a ‘space for time’ pay off.

7.3.3. *Pohlig-Hellman Algorithm.* Given  $G = \langle g \rangle \cong \mathbb{Z}/m\mathbb{Z}$  and  $h \in G$ , the task is to find the discrete logarithm  $\log_g(h)$ . The idea behind the *Pohlig-Hellman Algorithm* is to locate a non-trivial proper subgroup  $\tilde{G}$  of  $G$  and to solve corresponding discrete logarithm problems in the smaller groups  $G/\tilde{G}$  and  $\tilde{G}$ . This leads to a recursive solution of the original problem in  $G$ .

One starts by computing a factorisation  $m = m_1 m_2 \cdots m_r$ . This corresponds to a descending sequence of subgroups  $G_i$ ,  $i \in \{0, 1, \dots, r-1\}$ , of  $G$  with  $G_i \cong \mathbb{Z}/(m_1 m_2 \cdots m_{r-i})\mathbb{Z}$  for all  $i$ . The recursion will have depth  $r$  and the running time is going to be essentially bounded by  $\max\{\sqrt{m_1}, \dots, \sqrt{m_r}\}$ . Therefore it is advantageous if the individual factors  $m_i$  of  $m$  are uniformly small.

The exact procedure is as follows.

- Compute  $\tilde{m} := m/m_r = m_1 m_2 \cdots m_{r-1}$  and set

$$\tilde{G} := G^{m_r} = \{x^{m_r} \mid x \in G\} = \langle \tilde{g} \rangle \cong \mathbb{Z}/\tilde{m}\mathbb{Z} \quad \text{where} \quad \tilde{g} := g^{m_r}.$$

- First we want to find the discrete logarithm of  $h$  with respect to  $g$  modulo  $\tilde{G}$ . We observe that the homomorphism  $G \rightarrow G^{\tilde{m}}$ ,  $x \mapsto x^{\tilde{m}}$  has kernel  $\tilde{G}$ . Hence it induces an isomorphism from  $G/\tilde{G}$  onto  $G^{\tilde{m}} = \{x^{\tilde{m}} \mid x \in G\} = \langle g^{\tilde{m}} \rangle$ . The image of the coset  $h\tilde{G}$  under this isomorphism is  $h^{\tilde{m}}$ .

Thinking of  $|G^{\tilde{m}}| = m_r$  as small compared to  $m$ , we use the Baby-step Giant-step Algorithm (or complete enumeration if appropriate) to find  $a \in \mathbb{Z}$  such that the discrete logarithm of  $h^{\tilde{m}}$  with respect to  $g^{\tilde{m}}$  is equal to  $a$  modulo  $m_r$ . Going back along the isomorphism  $G/\tilde{G} \rightarrow G^{\tilde{m}}$  we can think of  $a$  as the discrete logarithm of  $h$  with respect to  $g$  modulo  $\tilde{G}$ , i.e.  $h \equiv g^a$  modulo  $\tilde{G}$ .

- Compute  $hg^{-a}$ . If  $hg^{-a} = 1$  then  $h = g^a$ , and  $a$  modulo  $m$  is the discrete logarithm of  $h$  with respect to  $g$ . We are lucky and the algorithm stops. Otherwise continue with the next step.
- We have already solved the original problem modulo  $\tilde{G}$ . Now run the algorithm under discussion for the input:  $\tilde{G} = \langle \tilde{g} \rangle \cong \mathbb{Z}/\tilde{m}\mathbb{Z}$  where  $\tilde{g} = g^{m_r}$  and  $\tilde{h} := hg^{-a} \in \tilde{G}$ . This yields  $b \in \mathbb{Z}$  such that the discrete logarithm of  $\tilde{h}$  with respect to  $\tilde{g}$  is equal to  $b$  modulo  $\tilde{m}$ .
- The discrete logarithm of  $h$  with respect to  $g$  is  $m_r b + a$  modulo  $m$ . Indeed,

$$h = (hg^{-a})g^a = (\tilde{g})^b g^a = g^{m_r b + a}.$$

*Example 7.4.* Consider  $G = \mathbb{F}_{101}^*$  with generator  $g = 2$ , and  $h = 3$ . Let us quickly check that 2 is indeed a primitive element for  $\mathbb{F}_{101}$ . The order of  $\mathbb{F}_{101}^*$  is  $m = 100 = 2^2 5^2$ . So if the order of 2 is a proper divisor of 100, then it is a divisor of 50 or a divisor of 20. Hence we need to show that  $2^{50} \neq 1$  and  $2^{20} \neq 1$  in  $\mathbb{F}_{101}$ . We compute in  $\mathbb{F}_{101}$  successively

$$\begin{aligned} 2^{10} &= 1024 = 14, \\ 2^{20} &= 14^2 = 196 = -6, \\ 2^{40} &= (-6)^2 = 36, \\ 2^{50} &= 36 \cdot 14 = 504 = -1. \end{aligned}$$

In particular, it follows that 2 has order 100 in  $\mathbb{F}_{101}^*$  as wanted.

In order to compute the discrete logarithm of  $h = 3$  with respect to  $g = 2$  in  $G = \mathbb{F}_{101}^*$ , using the Pohlig-Hellman Algorithm, we consider the factorisation  $m = m_1 m_2$  with  $m_1 = m_2 = 10$ .

- We compute  $\tilde{m} := m/m_r = m_1 = 10$  and we set

$$\tilde{G} := \langle \tilde{g} \rangle \cong \mathbb{Z}/10\mathbb{Z} \quad \text{where} \quad \tilde{g} := 2^{10}.$$

- First we want to find the discrete logarithm of 3 with respect to 2 modulo  $\tilde{G}$ . The image of the coset  $3\tilde{G}$  under the isomorphism  $G/\tilde{G} \rightarrow \langle 2^{10} \rangle$  is  $3^{10}$ .

We use the Baby-step Giant-step Algorithm to find  $a \in \mathbb{Z}$  such that the discrete logarithm of  $3^{10}$  with respect to  $2^{10}$  is equal to  $a$  modulo 10. From our calculation above we have  $2^{10} = 14$ , and we compute  $3^{10} = (3^4 3)^2 = (81 \cdot 3)^2 = (-60)^2 = 3600 = -36$ . We need to compute up to  $M := \lceil \sqrt{10} \rceil = 4$  babies and giants. Our calculations above can be conveniently used: the babies and the giants are

$$\begin{aligned} -36, \quad (-36) \cdot 14 = 1, \quad 1 \cdot 14 = 14, \quad 14 \cdot 14 = -6; \\ 14^4 = 36, \quad 36 \cdot 36 = 1296 = -17, \quad (-17) \cdot 36 = -6, \quad \dots \end{aligned}$$

From the common element  $-6$  we gather that  $(-36) \cdot 14^3 = (14^4)^3$  and hence  $-36 = 14^9$ . We are free to take for  $a$  any representative of the coset  $9 + 10\mathbb{Z}$  and  $a := -1$  is a convenient choice.

- We compute  $hg^{-a} = 3 \cdot 2^{-(-1)} = 6 \neq 1$  and accordingly continue with the next step.
- We run the Baby-step Giant-step Algorithm for the input:  $\tilde{G} = \langle \tilde{g} \rangle \cong \mathbb{Z}/10\mathbb{Z}$  where  $\tilde{g} = 2^{10} = 14$  and  $\tilde{h} := hg^{-a} = 6$ . Again we need to compute up to  $M = \lceil \sqrt{10} \rceil = 4$  babies and giants.

Taking advantage of our earlier calculations, the babies are  $6, 6 \cdot 14 = 84 = -17$ , etc. whereas the giants remain unchanged  $36, -17$ , etc. From the common element  $-17$  in these sequences we gather that  $6 \cdot 14 = (14^4)^2$  and hence  $6 = 14^7$ . The discrete logarithm of 6 with respect to 14 is equal to 7 modulo 10, and we take  $b := 7$ .

- Finally the discrete logarithm of  $h = 3$  with respect to  $g = 2$  is  $10b + a = 69$  modulo 100. Let us check our answer:

$$2^{69} = 2^{50} 2^{20} 2^{-1} = (-1)(-6)/2 = 3.$$

◇

**7.4. Mersenne prime method.** We conclude that for  $G = \langle g \rangle$  to be secure for use in a discrete logarithm based cryptosystem it is desirable that  $m = \text{ord}(g)$  has at least one large prime factor. There are various possible approaches to achieve this requirement. One fruitful way which we shall not describe at all is to realise  $G$  as the underlying group of a suitable elliptic curve. Closer to our theme is the *Mersenne prime method*. A Mersenne prime is a prime of the form  $p = 2^l - 1$  where  $l$  is (necessarily) also prime, e.g.  $p = 7 = 2^3 - 1$ . Many Mersenne primes are known, and the largest known primes are Mersenne primes. Now suppose that  $p = 2^l - 1$  is a Mersenne prime and let  $f \in \mathbb{F}_2[X]$  be an irreducible polynomial of degree  $l$ . Then  $\mathbb{F}_{2^l} = \mathbb{F}_2[X]/f\mathbb{F}_2[X]$  is a field of order  $2^l$ . Hence  $G := \mathbb{F}_{2^l}^*$  is a cyclic group of prime order  $p$  and every non-trivial element of  $G$ , e.g.  $g = X + f\mathbb{F}_2[X]$ ,

is a generator. Since the order of  $G$  is prime, the Pohlig-Hellman Algorithm does not improve upon the Baby-step Giant-step procedure.

Even if one has a supply of Mersenne primes, it remains a problem to find irreducible polynomials of a corresponding degree. There is a curious method for producing such polynomials.

**Lemma 7.5.** *Let  $p = 2^l - 1$  be a Mersenne prime, and suppose that  $X^l + X + 1 \in \mathbb{F}_2[X]$  is irreducible. Then  $X^p + X + 1 \in \mathbb{F}_2[X]$  is irreducible.*

*Example 7.6.* It is easily seen that  $X^2 + X + 1 \in \mathbb{F}_2[X]$  is irreducible. Going along the sequence of Mersenne primes  $3 = 2^2 - 1$ ,  $7 = 2^3 - 1$ ,  $127 = 2^7 - 1$  and  $2^{127} - 1$  we conclude that  $X^{2^{127}-1} + X + 1 \in \mathbb{F}_2[X]$  is irreducible! The proof that  $2^{127} - 1$ , a number with 39 decimal digits, is prime goes back to Lucas in 1876.  $\diamond$

Lemma 7.5 is really a consequence of an elaborate and useful theory of ‘linearised polynomials’. From this theory one can extract the following direct proof.

*Proof of Lemma 7.5.* Clearly,  $X^p + X + 1$  has no roots in  $\mathbb{F}_2$ , hence no factors of degree 1. Let  $h$  be an irreducible factor of  $X^p + X + 1$  of degree  $d := \deg(h) \geq 2$ . It suffices to show that  $d = p$ . Since  $f := X^l + X + 1 \in \mathbb{F}_2[X]$  is irreducible,  $\mathbb{F}_2[X]/f\mathbb{F}_2[X]$  is a field of cardinality  $2^l$ . By construction,  $f$  has a root  $\alpha$  in this field and clearly  $\alpha^{2^l-1} - 1 = 0$ . This implies that  $f = \text{mipo}_{\mathbb{F}_2}(\alpha)$  divides  $X^{2^l-1} - 1$ . From this one deduces that  $F := X^{2^l} + X^2 + X$  divides  $X^{2^{2^l-1}} - X = X^{2^p} - X$ ; an appropriate justification is given below. It follows that

$$h \mid (X^p + X + 1) = X^{-1}F \mid F \mid (X^{2^p} - X).$$

Consequently, the field  $\mathbb{F}_{2^d} \cong \mathbb{F}_2[X]/h\mathbb{F}_2[X]$  of cardinality  $2^d$  is contained in a splitting field of  $X^{2^p} - X$ , i.e. in a field  $\mathbb{F}_{2^p}$  of cardinality  $2^p$ . Since the degree  $[\mathbb{F}_{2^p} : \mathbb{F}_2] = p$  is prime, the Tower Law shows that any intermediate field of the extension  $\mathbb{F}_{2^p}|\mathbb{F}_2$  is either equal to  $\mathbb{F}_{2^p}$  or equal to  $\mathbb{F}_2$ . Since  $d \geq 2$  this implies that  $\mathbb{F}_{2^d} = \mathbb{F}_{2^p}$  and consequently  $d = p$  as wanted.

It remains to justify that  $f \mid (X^{2^l-1} - 1)$  implies  $F \mid X^{2^{2^l-1}} - X$ . This is where we use a central idea of the theory of ‘linearised polynomials’. Suppose that  $a = \sum_i a_i X^i, b = \sum_j b_j X^{2^j}, c = \sum_k c_k X^{2^k} \in \mathbb{F}_2[X]$ . We associate to these polynomials the ‘linearisations’

$$A := \sum_i a_i X^{2^i}, \quad B := \sum_j b_j X^{2^j}, \quad C := \sum_k c_k X^{2^k} \quad \in \mathbb{F}_2[X].$$

Observe that

$$\begin{aligned}
ab = c &\iff \sum_{i,j} a_i b_j X^{i+j} = \sum_k c_k X^k \\
&\iff \sum_{i+j=k} a_i b_j = c_k \text{ for all } k \\
&\iff \sum_{2^i+j=2^k} a_i b_j = c_k \text{ for all } k \\
&\iff \sum_{i,j} a_i b_j (X^{2^j})^{2^i} = \sum_k c_k X^{2^k} \\
&\iff \sum_i a_i \left( \sum_j b_j X^{2^j} \right)^{2^i} = \sum_k c_k X^{2^k} \\
&\iff A(B) = C.
\end{aligned}$$

Moreover,  $B$  divides  $\sum_i a_i B^{2^i} = A(B)$ . Applying these general observations to the specific polynomials  $a := (X^{2^l-1} - 1)/f$ ,  $b := f = X^l + X + 1$  and  $c := X^{2^l-1} - 1$  we conclude that  $F = X^{2^l} + X^2 + X = B$  divides  $C = X^{2^{2^l-1}} - X$ .  $\square$

## 8. CYCLOTOMIC POLYNOMIALS

**8.1. Roots of unity.** For every  $m \in \mathbb{N}$  there are  $m$  distinct  $m$ th roots of unity in  $\mathbb{C}$ , namely

$$\zeta^0 = 1, \quad \zeta^1 = \zeta := e^{2\pi i/m}, \quad \zeta^2, \quad \dots, \quad \zeta^{m-1} = e^{2\pi i(m-1)/m}.$$

Under multiplication they form a cyclic group of order  $m$ :

$$\{1, \zeta, \zeta^2, \dots, \zeta^{m-1}\} = \langle \zeta \rangle \cong \mathbb{Z}/m\mathbb{Z}.$$

A *primitive  $m$ th root of unity* is an element of order  $m$  in this group, i.e. a generator of this group. The primitive  $m$ th roots of unity are precisely the elements

$$\zeta^k = e^{2\pi i k/m} \quad \text{where } \gcd(k, m) = 1.$$

The number of primitive  $m$ th roots of unity is given by the *Euler phi function*

$$\varphi(m) := \#\{k \mid 0 \leq k \leq m-1, \gcd(k, m) = 1\} = |(\mathbb{Z}/m\mathbb{Z})^*|.$$

Elementary Number Theory (essentially the Chinese Remainder Theorem) shows that

$$\varphi(m) = \prod_{i=1}^r (p_i - 1) p_i^{e_i - 1} \quad \text{where } m = \prod_{i=1}^r p_i^{e_i} \text{ is a prime factorisation.}$$

**8.2. Cyclotomic polynomials.** The  $m$ th roots of unity in  $\mathbb{C}$  are precisely the roots of the polynomial  $X^m - 1$ . We observe that this polynomial is *separable*, i.e. it does not contain any repeated roots; cf. Exercise 4.2. It is clear that a primitive  $m$ th root of unity is an  $n$ th root of unity if and only if  $m \mid n$ . The following lemma makes a slightly stronger assertion.

**Lemma 8.1.** *Let  $m, n \in \mathbb{N}$ . Then  $m \mid n$  if and only if  $(X^m - 1) \mid (X^n - 1)$  over any integral domain.*

*Proof.* Division with remainder yields  $n = qm + r$  with  $0 \leq r < m$ , and  $m \mid n$  if and only if  $r = 0$ . Observe that

$$\begin{aligned} X^n - 1 &= (X^{qm} - 1)X^r + (X^r - 1) \\ &= (X^m - 1)(X^{(q-1)m} + X^{(q-2)m} + \dots + X^m + 1) + (X^r - 1), \end{aligned}$$

hence  $(X^m - 1) \mid (X^n - 1)$  if and only if  $X^r - 1 = 0$ . The lemma now follows from the fact that  $r = 0$  if and only if  $X^r - 1 = 0$ .  $\square$

It is natural to associate a corresponding polynomial to the primitive  $m$ th roots of unity. Let  $\zeta$  be a primitive  $m$ th root of unity in  $\mathbb{C}$ . Define the  *$m$ th cyclotomic polynomial*

$$\Phi_m := \prod_{\substack{0 \leq k < m \\ \gcd(k, m) = 1}} (X - \zeta^k) \in \mathbb{C}[X]$$

so that the roots of  $\Phi_m$  are precisely the primitive  $m$ th roots of unity.

**Lemma 8.2.** *Let  $m \in \mathbb{N}$ . Then*

- (1)  $\Phi_m$  is monic of degree  $\varphi(m)$  and has no repeated roots in  $\mathbb{C}$ ,
- (2)  $X^m - 1 = \prod_{d \mid m} \Phi_d(X)$ ,
- (3)  $\Phi_m \in \mathbb{Z}[X]$ .

*Proof.* Clearly,  $\Phi_m$  is monic of degree  $\varphi(m)$  and has no repeated roots in  $\mathbb{C}$ . The order of any  $m$ th root of unity is a divisor of  $m$ . Conversely, if  $d \mid m$  then every  $d$ th root of unity is an  $m$ th root of unity. This shows that  $X^m - 1$  and  $\prod_{d \mid m} \Phi_d$  have the same set of roots. As both polynomials are monic and have no repeated roots, they must be the same.

It remains to show that  $\Phi_m \in \mathbb{Z}[X]$ . We argue by induction on  $m$ . Clearly,  $\Phi_1 = X - 1 \in \mathbb{Z}[X]$ . Now suppose that  $m > 1$ . Then (2) shows that  $X^m - 1 = \Phi_m \cdot g$  where  $g := \prod_{d \mid m, d < m} \Phi_d \in \mathbb{Z}[X]$  by induction. Therefore dividing  $X^m - 1$  by  $g$  in  $\mathbb{Z}[X]$  yields  $\Phi_m \in \mathbb{Z}[X]$ ; cf. Gauss' Lemma.  $\square$

As indicated in the proof, Lemma 8.2 provides a recursive formula for computing  $\Phi_m$ . This can be used effectively, if  $m$  has only few divisors, but otherwise becomes soon impractical.

*Example 8.3.* Using Lemma 8.2, we compute  $\Phi_m$  for  $m \leq 6$ :

$$\begin{aligned} \Phi_1 &= X - 1, \\ \Phi_2 &= (X^2 - 1)(X - 1)^{-1} = X + 1, \\ \Phi_3 &= (X^3 - 1)(X - 1)^{-1} = X^2 + X + 1, \\ \Phi_4 &= (X^4 - 1)(X - 1)^{-1}(X + 1)^{-1} = X^2 + 1, \\ \Phi_5 &= (X^5 - 1)(X - 1)^{-1} = X^4 + X^3 + X^2 + X + 1, \\ \Phi_6 &= (X^6 - 1)(X - 1)^{-1}(X + 1)^{-1}(X^2 + X + 1)^{-1} = X^2 - X + 1. \end{aligned}$$

**8.3. Möbius Inversion.** Cyclotomic polynomials can be computed fairly efficiently using Möbius Inversion. The *Möbius function* is the arithmetic function

$$\mu : \mathbb{N} \rightarrow \mathbb{N}, \quad \mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \text{ is squarefree} \\ & \text{with precisely } r \text{ distinct prime factors,} \\ 0 & \text{otherwise.} \end{cases}$$

For practical applications an essential feature of the Möbius function is that it vanishes on most natural numbers. An inclusion-exclusion argument yields the classical

**Theorem 8.4** (Möbius Inversion). *Let  $G$  be an abelian group, written multiplicatively. Let  $f, F : \mathbb{N} \rightarrow G$  such that  $F(n) = \prod_{d|n} f(d)$  for all  $n \in \mathbb{N}$ . Then  $f(n) = \prod_{d|n} F(n/d)^{\mu(d)}$  for all  $n \in \mathbb{N}$ .*

There is a corresponding additive form of this theorem which we record as a corollary.

**Corollary 8.5** (Additive form of Möbius Inversion). *Let  $G$  be an abelian group, written additively. Let  $f, F : \mathbb{N} \rightarrow G$  such that  $F(n) = \sum_{d|n} f(d)$  for all  $n \in \mathbb{N}$ . Then  $f(n) = \sum_{d|n} \mu(d)F(n/d)$  for all  $n \in \mathbb{N}$ .*

We also record the following particular applications.

**Corollary 8.6.** *Let  $n \in \mathbb{N}$ . Then*

- (1)  $n = \sum_{d|n} \varphi(d)$  and  $\varphi(n) = \sum_{d|n} \mu(d) n/d$ ,
- (2)  $X^n - 1 = \prod_{d|n} \Phi_d(X)$  and  $\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}$ .

*Example 8.7.* Consider the natural number  $n := 12$  with divisors 1, 2, 3, 4, 6, 12. Then

$$12 = 1 + 1 + 2 + 2 + 2 + 4 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12)$$

and

$$\varphi(12) = 12 - 6 - 4 + 0 + 2 + 0 = \mu(1) \cdot 12 + \mu(2) \cdot 6 + \mu(3) \cdot 4 + \mu(6) \cdot 2 + \mu(12) \cdot 1.$$

Moreover by Example 8.3 we have

$$X^{12} - 1 = (X - 1)(X + 1)(X^2 + X + 1)(X^2 + 1)(X^2 - X + 1)\Phi_{12}(X),$$

and this is in accordance with

$$\Phi_{12} = \frac{(X^{12} - 1)(X^2 - 1)}{(X^6 - 1)(X^4 - 1)} = \frac{X^6 + 1}{X^2 + 1} = X^4 - X^2 + 1.$$

We indicate another application of Möbius Inversion, in the context of finite fields. Let  $\mathbb{F}_q$  be a finite field of cardinality  $q$  and let  $n \in \mathbb{N}$ . We are interested in the number  $A_q(n)$  of monic irreducible polynomials in  $\mathbb{F}_q[X]$ .

**Proposition 8.8** (Number of irreducible polynomials). *Let  $\mathbb{F}_q$  be a finite field of cardinality  $q$ . Then the number of monic irreducible polynomials in  $\mathbb{F}_q[X]$  of degree  $n$  is*

$$A_q(n) = n^{-1} \sum_{d|n} \mu(d) q^{n/d}.$$

This proposition follows by Möbius Inversion from the observation that  $X^{q^n} - X$  is the product of all the monic irreducible polynomials over  $\mathbb{F}_q$  whose degree divides  $n$ ; cf. Exercise 8.1. A generous estimate shows that

$$A_q(n) = n^{-1} \sum_{d|n} \mu(d) q^{n/d} \geq n^{-1} \left( q^n - \frac{q^{\lfloor n/2 \rfloor + 1} - 1}{q - 1} \right) > 0.$$

For  $q = p$  prime, this estimate provides an alternative proof for the existence of finite fields of any prescribed cardinality  $p^n$ .

**8.4. Primes in arithmetic progressions.** For more than 2000 years it has been known that there are infinitely many prime numbers, but understanding the ‘precise’ distribution of primes remains to this day the aim of active research. The famous Riemann Hypothesis is still one of the greatest conjectures in Mathematics. A celebrated theorem in 19th century Number Theory is

**Theorem 8.9** (Dirichlet). *Let  $a, b \in \mathbb{Z}$  with  $\gcd(a, b) = 1$ . Then there are infinitely many primes  $p$  such that  $p \equiv_b a$ .*

Dirichlet’s beautiful idea was to define certain complex functions, called  $L$ -functions, which can be regarded as variations of the famous Riemann zeta function. By studying the analytic properties of these functions, e.g. their poles, one arrives at the stated result. Using a much more elementary argument we can prove an interesting special case.

**Theorem 8.10** (Special case of Dirichlet’s Theorem). *Let  $m \in \mathbb{N}$ . Then there are infinitely many primes  $p$  such that  $p \equiv_m 1$ .*

A key idea is to look at the cyclotomic polynomial  $\Phi_m \in \mathbb{Z}[X]$  modulo a prime  $p$ , i.e. at the polynomial in  $\mathbb{F}_p[X]$  which is obtained from  $\Phi_m$  by reducing its integer coefficients modulo  $p$ . For convenience we record some initial observations.

**Lemma 8.11.** *Let  $p$  be a prime. Let  $m \in \mathbb{N}$ , and consider the polynomials  $X^m - 1$  and  $\Phi_m$  as polynomials over  $\mathbb{F}_p$ .*

- (1) *If  $m = p\tilde{m}$ , then  $X^m - 1 = (X^{\tilde{m}} - 1)^p$ . If  $p \nmid m$ , then  $X^m - 1$  and  $\Phi_m$  are separable over  $\mathbb{F}_p$ , i.e. they have no repeated roots in any extension of  $\mathbb{F}_p$ .*
- (2) *Suppose that  $p \mid m$  and let  $K$  be a field of characteristic  $p$ . Then  $K$  contains no primitive  $m$ th roots of unity, i.e.  $K^*$  has no elements of order  $p$ .*
- (3) *Suppose that  $p \nmid m$ , and let  $K$  be a field of characteristic  $p$ . Suppose that  $\alpha \in K$  is a root of  $\Phi_m$ . Then  $\alpha$  is a primitive  $m$ th root of unity, i.e.  $\alpha \in K^*$  and the order of  $\alpha$  in  $K^*$  is  $m$ .*

*Proof.* (1) Raising a polynomial to its  $p$ th power constitutes a ring endomorphism of  $\mathbb{F}_p[X]$  which acts as the identity on  $\mathbb{F}_p$ . Indeed, this map is the restriction of the Frobenius endomorphism of the field  $\mathbb{F}_p(X)$ ; cf. Proposition 6.3. Hence  $m = p\tilde{m}$  implies  $X^m - 1 = (X^{\tilde{m}})^p - 1^p = (X^{\tilde{m}} - 1)^p$ .

Now suppose that  $p \nmid m$ , and assume for a contradiction that  $\alpha$  is a repeated root of  $X^m - 1$  in some extension of  $\mathbb{F}_p$ . Then  $\alpha^m = 1$  shows that  $\alpha \neq 0$ . Taking formal derivatives and evaluating at  $\alpha$ , as in the proof of Theorem 6.2, we obtain  $m\alpha^{m-1} = 0$ . Since  $p \nmid m$  and  $\alpha \neq 0$ , this gives the required contradiction. As  $\Phi_m$  divides  $X^m - 1$  this proves that both polynomials are separable.

(2) Let  $\alpha \in K$  with  $\alpha^m = 1$ . Writing  $m = p\tilde{m}$ , we deduce  $(\alpha^{\tilde{m}} - 1)^p = 0$  according to (1). This implies  $\alpha^{\tilde{m}} - 1 = 0$ , hence  $\alpha^{\tilde{m}} = 1$ . Therefore the order of  $\alpha$  is strictly smaller than  $m$ .

(3) Since  $\Phi_m$  divides  $X^m - 1$ , we have  $\alpha^m = 1$ . Consequently  $\alpha \in K^*$  has finite order, and in fact  $d := \text{ord}(\alpha)$  divides  $m$ . For a contradiction assume that  $d < m$ . The integer polynomials  $X^d - 1$  and  $\Phi_m$  both divide  $X^m - 1$  and are coprime, because they have no common roots in  $\mathbb{C}$ . Therefore their product  $(X^d - 1)\Phi_m$  divides  $X^m - 1$  in  $\mathbb{Z}[X]$ ; cf. Gauss' Lemma. Reducing coefficients modulo  $p$  we obtain a factorisation  $X^m - 1 = (X^d - 1)\Phi_m f$  with  $f \in \mathbb{F}_p[X]$  over the prime subfield  $\mathbb{F}_p$  of  $K$ . We observe that  $\alpha$  is a root of both  $X^d - 1$  and  $\Phi_m$ . Hence  $\alpha$  is a repeated root of  $X^m - 1$ . This contradicts (1).  $\square$

*Proof of Theorem 8.10.* Let  $\mathbb{P}$  denote the set of all primes. The proof is divided into three steps.

*Subclaim 1:* Let  $f \in \mathbb{Z}[X]$  be monic and not constant. Then the set

$$\mathcal{P}_f := \{p \in \mathbb{P} \mid \exists n \in \mathbb{N} : f(n) \equiv_p 0\}$$

is infinite. In other words,  $f$  has a root modulo  $p$  for infinitely many primes  $p$ .

*Subproof:* Essentially we argue as in Euclid's classical proof that  $\mathbb{P}$  is infinite: we show that every finite subset of  $\mathcal{P}_f$  is a proper subset. Let  $\{p_1, \dots, p_r\} \subseteq \mathcal{P}_f$ , and set  $M := p_1 \cdots p_r$ . It suffices to construct a prime  $p \in \mathcal{P}_f$  such that  $p \nmid M$ .

Since  $f$  has only finitely many roots, we find  $n_0 \in \mathbb{N}$  such that  $a := f(n_0) \neq 0$ . Put  $g := a^{-1}f(n_0 + aMX) \in \mathbb{Q}[X]$  and write  $f = \sum_{i=0}^d f_i X^i$ . Then

$$\begin{aligned} g &= a^{-1} \sum_{i=0}^d f_i (n_0 + aMX)^i \\ &= a^{-1} \left( f(n_0) + \sum_{i=0}^d f_i \sum_{j=1}^i n_0^{i-j} (aMX)^j \right) \\ &= 1 + M \sum_{i=0}^d \sum_{j=1}^i f_i n_0^{i-j} (aM)^{j-1} X^j \\ &\in \mathbb{Z}[X], \end{aligned}$$

and  $g(n) \equiv_M 1$  implies  $\gcd(g(n), M) = 1$  for all  $n \in \mathbb{N}$ . The polynomials  $g - 1$  and  $g + 1$  have only finitely many roots. Hence we find  $n_1 \in \mathbb{N}$  such that  $g(n_1) \notin \{1, -1\}$ . Let  $p$  be a prime factor of  $g(n_1)$ . Then  $f(n_0 + aMn_1) = g(n_1) \equiv_p 0$  and  $\gcd(p, M) = 1$ . This shows that  $p \in \mathcal{P}_f$  and  $p \nmid M$  as wanted.

*Subclaim 2:* Let  $p \in \mathbb{P}$  and  $a \in \mathbb{Z}$  such that  $\Phi_m(a) \equiv_p 0$ . Then  $p \mid m$  or  $p \equiv_m 1$ .

*Subproof:* Suppose that  $p \nmid m$ . Then by Lemma 8.11 the element  $\bar{a} \in \mathbb{F}_p^*$  has order  $m$ . By Lagrange's Theorem,  $m$  divides  $|\mathbb{F}_p^*| = p - 1$ , thus  $p \equiv_m 1$ .

*Subclaim 3:* There exist infinitely many primes  $p$  such that  $p \equiv_m 1$ .

*Subproof:* Applying Subclaims 1 and 2 to  $f := \Phi_m$  we conclude that the set

$$\{p \in \mathbb{P} \mid p \mid m \text{ or } p \equiv_m 1\}$$

is infinite. Since  $m$  has only finitely many prime divisors, there are infinitely many primes  $p$  such that  $p \equiv_m 1$ .  $\square$

## 9. CYCLOTOMIC FIELDS AND AN INDICATION OF GALOIS THEORY

**9.1. Cyclotomic fields and their automorphisms.** Let  $m \in \mathbb{N}$ . The splitting field  $\mathcal{K}_m$  in  $\mathbb{C}$  of the polynomial  $X^m - 1$  over  $\mathbb{Q}$  is called the  *$m$ th cyclotomic field*. A basic invariant of the extension  $\mathcal{K}_m|\mathbb{Q}$  is its degree. The key towards finding  $[\mathcal{K}_m : \mathbb{Q}]$  is to prove that the  $m$ th cyclotomic polynomial  $\Phi_m$  is irreducible over  $\mathbb{Q}$ . Note that we have already proved this in a special case: if  $p$  is prime, then Eisenstein's Criterion can be used to show that  $\Phi_p = (X^p - 1)/(X - 1) \in \mathbb{Z}[X]$  is irreducible; see Example 5.11.

**Proposition 9.1.** *Let  $m \in \mathbb{N}$ , and let  $\zeta$  be a primitive  $m$ th root of unity in  $\mathbb{C}$ . Then  $\text{mipo}_{\mathbb{Q}}(\zeta) = \Phi_m$ . In particular, the  $m$ th cyclotomic polynomial  $\Phi_m$  is irreducible over  $\mathbb{Q}$ .*

*Proof.* Put  $f := \text{mipo}_{\mathbb{Q}}(\zeta)$ . From  $\Phi_m(\zeta) = 0$  we conclude that  $f$  divides  $\Phi_m$ . Since  $\Phi_m$  is monic, it therefore suffices to prove that  $\deg(f) = \deg(\Phi_m)$ . The roots of  $\Phi_m$  in  $\mathbb{C}$  are precisely the primitive  $m$ th roots of unity and each one of them occurs with multiplicity 1. Hence it is enough to show that  $f$  is the minimum polynomial over  $\mathbb{Q}$  of every primitive  $m$ th root of unity. In other words it suffices to prove the following claim:  $f = \text{mipo}_{\mathbb{Q}}(\zeta^k)$  for every  $k \in \mathbb{Z}$  with  $\gcd(k, m) = 1$ .

Let  $k \in \mathbb{N}$  with  $\gcd(k, m) = 1$ . If  $k$  is composite, we can write  $k = ab$  with  $1 < a, b < k$ . Then  $\zeta^k = (\zeta^a)^b$  and we can prove the claim in two steps, namely  $\text{mipo}_{\mathbb{Q}}((\zeta^a)^b) = \text{mipo}_{\mathbb{Q}}(\zeta^a)$  and  $\text{mipo}_{\mathbb{Q}}(\zeta^a) = \text{mipo}_{\mathbb{Q}}(\zeta)$ . Therefore, by induction on the number of prime factors of  $k$ , we are reduced to the case where  $k = p$  is prime. In this situation the condition  $\gcd(p, m) = 1$  is equivalent to  $p \nmid m$ .

Assume for a contradiction that  $\text{mipo}_{\mathbb{Q}}(\zeta^p) \neq f$ . As  $f$  is irreducible over  $\mathbb{Q}$ , this means that  $f(\zeta^p) \neq 0$ . Observe from Gauss' Lemma that  $f \in \mathbb{Z}[X]$ , and write  $X^m - 1 = fg$  in  $\mathbb{Z}[X]$ . From  $0 = (\zeta^p)^m - 1 = f(\zeta^p)g(\zeta^p)$  we conclude that  $g(\zeta^p) = 0$ . Hence  $\zeta$  is a root of the polynomial  $g(X^p) \in \mathbb{Z}[X]$ . As  $\text{mipo}_{\mathbb{Q}}(\zeta) = f$ , we can write  $g(X^p) = fh$  in  $\mathbb{Z}[X]$ , again by Gauss' Lemma.

Now consider the images  $\bar{f}, \bar{g}, \bar{h} \in \mathbb{F}_p[X]$  of the integer polynomials  $f, g, h$  which one obtains by reducing all coefficients modulo  $p$ . Recall that raising to the  $p$ th power gives a ring endomorphism of  $\mathbb{F}_p[X]$  which acts as the identity on  $\mathbb{F}_p$ ; cf. the proof of Lemma 8.11. Over  $\mathbb{F}_p$  we have

$$\bar{g}^p = \bar{g}(X)^p = \bar{g}(X^p) = \bar{f}\bar{h}.$$

Hence  $\bar{f}$  and  $\bar{g}$  have a common root in a splitting field  $K$  of  $\bar{f}$  over  $\mathbb{F}_p$ . This implies that  $X^m - 1 = \bar{f}\bar{g}$  has a repeated root  $\alpha$  in  $K$ , in contradiction with Lemma 8.11.  $\square$

A basic theme in Mathematics is the study of structures with special algebraic, geometric or combinatorial properties. Often valuable information can be gained from looking at the automorphism groups of such structures. Galois Theory is a classical example for this procedure: it is centred around the idea that a field extension can be understood in terms of an associated group of symmetries. We illustrate the general principle by looking more carefully at cyclotomic fields and their automorphisms.

**Theorem 9.2** (Structure of cyclotomic fields). *Let  $m \in \mathbb{N}$ , and let  $\zeta$  be a primitive  $m$ th root of unity in  $\mathbb{C}$ . Then  $\text{mipo}_{\mathbb{Q}}(\zeta) = \Phi_m$  and  $\mathcal{K}_m = \mathbb{Q}(\zeta) \cong \mathbb{Q}[X]/\Phi_m\mathbb{Q}[X]$ . In particular,  $[\mathcal{K}_m : \mathbb{Q}] = \varphi(m)$ .*

*For every  $k \in \mathbb{Z}$  with  $\gcd(k, m) = 1$  there is a unique automorphism  $g_k$  of  $\mathcal{K}_m$  such that  $g_k(\zeta) = \zeta^k$ . The map  $(\mathbb{Z}/m\mathbb{Z})^* \rightarrow \text{Aut}(\mathcal{K}_m)$ ,  $k + m\mathbb{Z} \mapsto g_k$  is an isomorphism of groups.*

*Proof.* The roots of  $X^m - 1$  are the  $m$ th roots of unity and hence precisely the powers  $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$  of the primitive root  $\zeta$ . This shows that  $\mathcal{K}_m = \mathbb{Q}(\zeta)$ . Clearly,  $\Phi_m(\zeta) = 0$ . Proposition 9.1 states that  $\text{mipo}_{\mathbb{Q}}(\zeta) = \Phi_m$ . Hence by Kronecker's Theorem we have

$$\mathcal{K}_m = \mathbb{Q}(\zeta) \cong \mathbb{Q}[X]/\Phi_m\mathbb{Q}[X] \quad \text{and} \quad [\mathcal{K}_m : \mathbb{Q}] = \deg(\Phi_m) = \varphi(m).$$

Let  $k \in \mathbb{Z}$  with  $\gcd(k, m) = 1$ . Then  $\zeta^k$  is a primitive root of unity. Therefore  $\text{mipo}_{\mathbb{Q}}(\zeta^k) = \Phi_m$  by Proposition 9.1. Hence by Kronecker's Theorem there is a unique isomorphism  $g_k : \mathbb{Q}(\zeta) \rightarrow \mathbb{Q}(\zeta^k)$  (via  $\mathbb{Q}[X]/\Phi_m\mathbb{Q}[X]$ ) such that  $g_k(\zeta) = \zeta^k$  and  $g_k$  restricts to the identity on  $\mathbb{Q}$ . But every isomorphism of fields maps the prime subfield onto the prime subfield, and prime fields admit only the trivial automorphism. Observing that  $\mathcal{K}_m = \mathbb{Q}(\zeta) = \mathbb{Q}(\zeta^k)$ , this shows that  $g_k$  is the unique automorphism of  $\mathcal{K}_m$  such that  $g_k(\zeta) = \zeta^k$ .

Recall that  $(\mathbb{Z}/m\mathbb{Z})^* = \{k + m\mathbb{Z} \mid \gcd(k, m) = 1\}$ . Since  $\zeta^m = 1$ , there is a map

$$(\mathbb{Z}/m\mathbb{Z})^* \rightarrow \text{Aut}(\mathcal{K}_m), \quad \bar{k} = k + m\mathbb{Z} \mapsto g_k.$$

First we show that this map is an injective group homomorphism. Let  $\bar{k}, \bar{l} \in (\mathbb{Z}/m\mathbb{Z})^*$ . Then we have

$$(g_k g_l)(\zeta) = g_k(g_l(\zeta)) = g_k(\zeta^l) = g_k(\zeta)^l = (\zeta^k)^l = \zeta^{kl} = g_{kl}(\zeta).$$

Since  $g_{kl}$  is uniquely determined in  $\text{Aut}(\mathcal{K}_m)$  by the image  $g_{kl}(\zeta) = \zeta^{kl}$  of  $\zeta$ , it follows that  $g_k g_l = g_{kl}$ . Hence the map under consideration is a homomorphism. Now suppose that  $g_k = g_l$ . Then  $\zeta^k = g_k(\zeta) = g_l(\zeta) = \zeta^l$ , hence  $\zeta^{k-l} = 1$ . But  $\zeta$  is a primitive  $m$ th root of unity, so  $m$  divides  $k - l$  and  $\bar{k} = \bar{l}$ . This shows that the map under consideration is injective.

It remains to prove that every automorphism of  $\mathcal{K}_m$  is of the form  $g_k$ ,  $k \in \mathbb{Z}$  with  $\gcd(k, m) = 1$ . Let  $g \in \text{Aut}(\mathcal{K}_m)$ . Observe that  $g$  acts as the identity on  $\mathbb{Q}$ . Hence the equation  $\Phi_m(\zeta) = 0$ , which shows that  $\zeta$  satisfies a certain polynomial equation with coefficients in  $\mathbb{Q}$ , implies that  $g(\zeta)$  satisfies the same polynomial equation:  $\Phi(g(\zeta)) = g(\Phi(\zeta)) = g(0) = 0$ . This means that  $g(\zeta)$  is a primitive  $m$ th root of unity, hence of the form  $g(\zeta) = \zeta^k$  for suitable  $k \in \mathbb{Z}$  with  $\gcd(k, m) = 1$ . In accordance with what we proved above this implies that  $g = g_k$ .  $\square$

Cyclotomic fields are rather special fields, but they play an important role in understanding a much wider class of field extensions. As an indication we state the following celebrated result marking the starting point of Class Field Theory, a major branch of Algebraic Number Theory which was successively developed during the first half of the 20th century.

**Theorem 9.3** (Kronecker-Weber). *Let  $K$  be the splitting field in  $\mathbb{C}$  of some polynomial  $f \in \mathbb{Q}[X]$ . If  $\text{Aut}(K)$  is abelian then there exists  $m \in \mathbb{N}$  such that  $K$  is an intermediate field of the cyclotomic extension  $\mathcal{K}_m | \mathbb{Q}$ .*

Implicitly contained in this statement is the following weaker assertion concerning finite abelian groups: for every finite abelian group  $G$  there exists  $m \in \mathbb{N}$  such that  $G$  is isomorphic to a subgroup of  $(\mathbb{Z}/m\mathbb{Z})^*$ . By induction on  $|G|$ , this weaker assertion can be reduced to the special case where  $G$  is cyclic. But if  $G$  is cyclic, one can apply Theorem 8.10 to find a suitable embedding of  $G$  into  $\mathbb{Z}/m\mathbb{Z}$ .

**9.2. Regular  $p$ -gons.** The  $m$ th cyclotomic field  $\mathcal{K}_m$  is intimately linked with the geometric problem of constructing a regular  $m$ -gon by compasses and straight edge. Building upon our expertise we can now prove the central case of Theorem 1.2.

**Theorem 9.4** (Central case of the Theorem of Gauss-Wanzenel). *Let  $p$  be an odd prime. Then the regular  $p$ -gon is constructible by compasses and straight edge if and only if  $p$  is a Fermat prime, i.e.  $p = 2^{2^r} + 1$  for some  $r \in \mathbb{N}_0$ .*

According to History, Gauss as a young man was so pleased with his discovery of a construction of the regular 17-gon that he decided to pursue mathematics rather than study languages. The proof of Theorem 9.4 which we give below also serves us as a guided example towards the theorems of Galois Theory which we discuss in the next subsection. We start with an elementary lemma which clears away some of the mystery of Fermat primes.

**Lemma 9.5.** *Let  $k \in \mathbb{N}$ . If  $2^k + 1$  is prime, then  $k = 2^r$  for some  $r \in \mathbb{N}_0$ .*

*Proof.* We argue by contraposition. Suppose that  $k$  is not a power of 2. Then we write  $k = ab$  where  $a, b \in \mathbb{N}$  with  $1 \leq a < k$ ,  $1 < b \leq k$  and  $b \equiv 1 \pmod{2}$ . The equation

$$(2^a + 1)(2^{a(b-1)} - 2^{a(b-2)} + \dots + 2^{a \cdot 2} - 2^a + 1) = 2^{ab} + 1 = 2^k + 1$$

shows that  $2^a + 1$  is a factor of  $2^k + 1$ . Since  $3 \leq 2^a + 1 < 2^k + 1$ , this proves that  $2^k + 1$  is not prime.  $\square$

*Proof of Theorem 9.4.* In view of the previous lemma, it suffices to prove that the regular  $p$ -gon can be constructed by compasses and straight edge if and only if  $p = 2^k + 1$  for some  $k \in \mathbb{N}_0$ . Let  $\zeta$  be a primitive  $p$ th root of unity in  $\mathbb{C}$ . According to our discussion at the end of Section 2, the regular  $p$ -gon can be constructed by compasses and straight edge if and only if the cyclotomic field  $\mathcal{K}_p = \mathbb{Q}(\zeta)$  is contained in a subfield of  $\mathbb{C}$  which can be obtained by successively adjoining square roots.

In particular, if the regular  $p$ -gon can be constructed by compasses and straight edge, then Corollary 3.6 shows that  $p - 1 = \varphi(p) = [\mathcal{K}_p : \mathbb{Q}] = 2^k$  for some  $k \in \mathbb{N}_0$ , hence  $p = 2^k + 1$ . So it remains to show the converse. Suppose that  $p = 2^k + 1$  for some  $k \in \mathbb{N}_0$ . In view of Theorem 3.3 it suffices to construct a chain of subfields

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_k = \mathcal{K}_p \quad \text{with } [K_i : K_{i-1}] = 2 \text{ for } 1 \leq i \leq k.$$

The idea is to manufacture a similar chain of subgroups inside the automorphism group  $G := \text{Aut}(\mathcal{K}_p)$  and subsequently to associate to each subgroup a suitable intermediate field of  $\mathcal{K}_p|\mathbb{Q}$ . By Theorem 9.2 the group  $G$  is isomorphic to  $(\mathbb{Z}/p\mathbb{Z})^*$ . As  $p$  is a prime, this is a cyclic group of order  $p - 1 = 2^k$ . Let  $g$  be a generator of the group  $G$ . Then all the subgroups of  $G$  are of the form  $G_i := \langle g^{2^i} \rangle$ ,  $i \in \{0, 1, \dots, k\}$ , and they line up in a chain

$$G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_k = \{1\} \quad \text{with } |G_{i-1} : G_i| = 2 \text{ for } 1 \leq i \leq k.$$

In order to associate a suitable field  $K_i$  to the group  $G_i$  for  $i \in \{0, 1, \dots, k\}$  we consider  $\mathcal{K}_p$  as a vector space over  $\mathbb{Q}$ . Since  $\zeta$  is a primitive element for the extension  $\mathcal{K}_p|\mathbb{Q}$  and  $[\mathcal{K}_p : \mathbb{Q}] = p - 1$ , Kronecker's Theorem shows that  $1, \zeta, \zeta^2, \dots, \zeta^{p-2}$  form a basis for  $\mathcal{K}_p$  as a vector space over  $\mathbb{Q}$ . Multiplication by  $\zeta$  corresponds to a linear automorphism of the vector space  $\mathcal{K}_p$ , hence  $\zeta, \zeta^2, \dots, \zeta^{p-1}$  also form a basis for  $\mathcal{K}_p$ . According to Theorem 9.2 the group  $G$  is isomorphic to  $(\mathbb{Z}/p\mathbb{Z})^*$ : for every  $j \in \{1, 2, \dots, p-1\}$  there is precisely one  $h \in G$  such that  $h(\zeta) = \zeta^j$ . Thinking of  $G$  as  $(\mathbb{Z}/p\mathbb{Z})^*$  we write  $\zeta^h := h(\zeta)$  for  $h \in G$ . Our discussion then shows that  $\zeta^h, h \in G$ , is a basis for the vector space  $\mathcal{K}_p$  over  $\mathbb{Q}$ .

For  $i \in \{0, 1, \dots, k\}$  we define

$$K_i := \left\{ \sum_{h \in G} a_h \zeta^h \mid a_h \in \mathbb{Q}, \text{ and } a_h = a_{\tilde{h}} \text{ whenever } h \equiv_{G_i} \tilde{h} \right\} \subseteq \mathcal{K}_p,$$

where  $h, \tilde{h} \in G$  are congruent modulo  $G_i$ , in symbols  $h \equiv_{G_i} \tilde{h}$ , if and only if  $hG_i = \tilde{h}G_i$  or equivalently  $h^{-1}\tilde{h} \in G_i$ .

Let  $i \in \{0, 1, \dots, k\}$ . In order to understand the definition of  $K_i$  let us first consider the special cases  $i = 0$  and  $i = k$ . Notice that  $G_0 = G$  and that  $h \equiv_G \tilde{h}$  for all  $h, \tilde{h} \in G$ . Since  $1 + \zeta + \dots + \zeta^{p-1} = \Phi_p(\zeta) = 0$ , this implies

$$\begin{aligned} K_0 &= \left\{ \sum_{h \in G} a_h \zeta^h \mid a_h \in \mathbb{Q}, \text{ and } a_h = a_{\tilde{h}} \text{ whenever } h \equiv_G \tilde{h} \right\} \\ &= \left\{ \sum_{h \in G} a_h \zeta^h \mid a_h \in \mathbb{Q}, \text{ and } a_h = a_{\tilde{h}} \text{ for all } h, \tilde{h} \right\} \\ &= \left\{ a \underbrace{(\zeta + \zeta^2 + \dots + \zeta^{p-1})}_{=-1} \mid a \in \mathbb{Q} \right\} \\ &= \mathbb{Q}. \end{aligned}$$

This fits well into our plans.

Similarly,  $G_k = \{1\}$ , and  $h \equiv_{\{1\}} \tilde{h}$  if and only if  $h = \tilde{h}$  for all  $h, \tilde{h} \in G$ . This implies

$$\begin{aligned} K_k &= \left\{ \sum_{h \in G} a_h \zeta^h \mid a_h \in \mathbb{Q}, \text{ and } a_h = a_{\tilde{h}} \text{ whenever } h \equiv_{\{1\}} \tilde{h} \right\} \\ &= \left\{ \sum_{h \in G} a_h \zeta^h \mid a_h \in \mathbb{Q}, \text{ and } \underbrace{a_h = a_{\tilde{h}} \text{ whenever } h = \tilde{h}}_{\text{redundant}} \right\} \\ &= \left\{ \sum_{h \in G} a_h \zeta^h \mid a_h \in \mathbb{Q} \right\} \\ &= \mathcal{K}_p \end{aligned}$$

which again fits well with our plans.

In general  $K_i$  is defined by linear equations and hence a vector subspace of  $\mathcal{K}_p$ . As such it has dimension  $\dim K_i = |G : G_i| = 2^i$  over  $\mathbb{Q}$ . Indeed, a basis for  $K_i$  over  $\mathbb{Q}$  is given by the elements  $\sum_{h \in \tilde{h}G_i} \zeta^h, \tilde{h}G_i \in G/G_i$ .

We still need to prove that the vector subspace  $K_i$  is in fact a subfield of  $\mathcal{K}_p$ . In order to show this it suffices to characterise  $K_i$  as the fixed set of an appropriate set of automorphisms of  $\mathcal{K}_p$ ; cf. the proof of Corollary 6.5.

We claim that

$$K_i = \{ \alpha \in \mathcal{K}_p \mid \forall \tilde{g} \in G_i : \tilde{g}(\alpha) = \alpha \}.$$

Let  $\alpha = \sum_{h \in G} a_h \zeta^h \in \mathcal{K}_p$  with coefficients  $a_i \in \mathbb{Q}$ . For every  $\tilde{g} \in G$  we have

$$\tilde{g}(\alpha) = \tilde{g} \left( \sum_{h \in G} a_h \zeta^h \right) = \sum_{h \in G} a_h (\zeta^h)^{\tilde{g}} = \sum_{h \in G} a_h \zeta^{h\tilde{g}} = \sum_{h \in G} a_{h\tilde{g}^{-1}} \zeta^h.$$

Recall that the elements  $\zeta^h$ ,  $h \in G$ , are linearly independent over  $\mathbb{Q}$ . Hence for any individual automorphism  $\tilde{g} \in G$  we have  $\alpha = \tilde{g}(\alpha)$  if and only if  $a_h = a_{h\tilde{g}^{-1}}$  for all  $h \in G$ .

Now  $G_i$  is a group and hence closed under taking inverses. Consequently,  $\alpha = \tilde{g}(\alpha)$  for all  $\tilde{g} \in G_i$  if and only if  $a_h = a_{\tilde{h}}$  for all  $h, \tilde{h} \in G$  with  $h \equiv_{G_i} \tilde{h}$ . This shows that  $K_i$  is the fixed set of the group  $G_i$  and hence forms a subfield of  $\mathcal{K}_p$ .  $\square$

**9.3. An indication of Galois Theory.** The key idea of Galois Theory is to describe the structure of a field extension  $L|K$  by an associated group of automorphisms. Galois Theory was developed in the mid 19th century. The original motivation was to find explicit formulae for the solutions of polynomial equations. Galois realised that the solutions of a polynomial equation satisfy certain symmetries which can be captured by an associated permutation group. The structure of this permutation group determines whether the solutions to the equation can be expressed in terms of radicals. We give a brief outline of the main results of this theory; for details see, for instance, Ian Stewart's book. In the next section we will discuss and prove the implications of Galois Theory in the context of finite fields.

We begin by stating formally a basic observation which we made while establishing the existence and uniqueness of finite fields of prescribed cardinality. We used the same ideas again in the proof of Theorem 9.4.

**Lemma 9.6.** *Let  $L$  be a field and let  $G := \text{Aut}(L)$ .*

- (1) *If  $K$  is a subfield of  $L$ , then  $\{g \in G \mid \forall \alpha \in K : g(\alpha) = \alpha\}$  is a subgroup of  $G$ .*
- (2) *If  $H$  is a subgroup of  $G$ , then  $\{\alpha \in L \mid \forall g \in H : g(\alpha) = \alpha\}$  is a subfield of  $L$ .*

A *finite Galois extension* is a field extension  $L|K$  for which there exists a finite subgroup  $G$  of  $\text{Aut}(L)$  such that  $K = \{\alpha \in L \mid \forall g \in G : g(\alpha) = \alpha\}$ . Examples of Galois extensions which we have encountered so far are cyclotomic extensions  $\mathcal{K}_p|\mathbb{Q}$ , where  $p$  is prime, and quadratic extensions  $\mathbb{Q}(\sqrt{d})|\mathbb{Q}$ , where  $d \in \mathbb{Q}$ . The next theorem provides a useful criterion for testing whether a finite extension is Galois.

**Theorem 9.7.** *A finite field extension  $L|K$  is Galois if and only if  $L$  is a splitting field of a separable polynomial  $f$  over  $K$ .*

From Proposition 5.6 and Exercise 4.2 one deduces the following

**Corollary 9.8.** *In characteristic 0 every finite field extension  $L|K$  is a subextension of a finite Galois extension  $M|K$ .*

The *Galois group* of a finite Galois extension  $L|K$  is the group  $\text{Gal}(L|K) := \{g \in \text{Aut}(L) \mid \forall \alpha \in K : g(\alpha) = \alpha\}$ . We can now state the central result of Galois Theory, which is illustrated in the proof of Theorem 9.4.

**Theorem 9.9** (Main Theorem of Galois Theory). *Let  $L|K$  be a finite Galois extension with Galois group  $G := \text{Gal}(L|K)$ . Then there is an inclusion-reversing correspondence between*

$$\mathcal{M} := \{M \mid M \text{ intermediate field of } L|K\} \text{ and } \mathcal{H} := \{H \mid H \text{ subgroup of } G\}$$

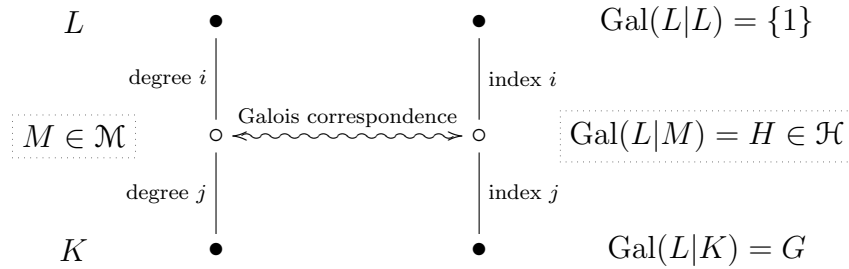
*given by the mutually inverse bijections*

$$\begin{aligned} \mathcal{M} &\rightarrow \mathcal{H}, & M &\mapsto \{h \in G \mid \forall \alpha \in M : h(\alpha) = \alpha\}, \\ \mathcal{H} &\rightarrow \mathcal{M}, & H &\mapsto \{\alpha \in L \mid \forall h \in H : h(\alpha) = \alpha\}. \end{aligned}$$

*Moreover, if the subgroup  $H$  corresponds to the intermediate field  $M$ , then*

$$|G : H| = [M : K].$$

Let  $L|K$  be a finite Galois extension, and let  $M$  be an intermediate field of  $L|K$ . From Theorem 9.7 it is clear that  $L|M$  is also a finite Galois extension. Thus the Main Theorem of Galois Theory can be depicted as follows.



There are several other important and practical aspects of Galois Theory which we do not discuss in detail. For instance, if  $M|K$  is Galois, then  $\text{Gal}(L|M)$  is a normal subgroup of  $\text{Gal}(L|K)$  and restriction gives a natural isomorphism  $\text{Gal}(M|K) \cong \text{Gal}(L|K) / \text{Gal}(L|M)$ . We illustrate the Main Theorem of Galois Theory by a concrete example.

*Example 9.10.* Consider the cyclotomic field  $\mathcal{K}_{21} = \mathbb{Q}(\zeta)$ , where  $\zeta$  is a primitive 21st root of unity in  $\mathbb{C}$ . Since  $\mathcal{K}_{21}$  is the splitting field of  $X^{21} - 1$  over  $\mathbb{Q}$ , the extension  $\mathcal{K}_{21}|\mathbb{Q}$  is Galois. Its degree is  $[\mathcal{K}_{21} : \mathbb{Q}] = \varphi(21) = \varphi(3)\varphi(7) = 12$ .

Every automorphism of  $\mathcal{K}_{21}$  restricts to the identity map on the prime subfield  $\mathbb{Q}$ . Hence Theorem 9.2 shows that

$$G := \text{Gal}(\mathcal{K}_{21}|\mathbb{Q}) = \text{Aut}(\mathcal{K}_{21}) \cong (\mathbb{Z}/21\mathbb{Z})^*.$$

Writing  $C_n$  to denote a cyclic group of order  $n$ , the Chinese Remainder Theorem provides the isomorphism

$$(\mathbb{Z}/21\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^* \cong C_2 \times C_6 \cong C_2 \times C_2 \times C_3.$$

It is not difficult to work out the subgroup lattice of  $G$ . The Main Theorem of Galois Theory then gives us the corresponding lattice of intermediate fields of the Galois extension  $\mathcal{K}_{21}|\mathbb{Q}$ . We obtain the following qualitative pictures.



particular choice of  $L$  does not affect the set of conjugates. In fact, the conjugates of  $\alpha$  over  $K$  can be characterised in terms of the minimum polynomial of  $\alpha$  over  $K$ . One can show that  $\text{mipo}_K(\alpha)$  splits into distinct linear factors over  $L$  and that its roots are precisely the conjugates of  $\alpha$  (taken without repetitions).

**Theorem 9.11** (Normal Basis Theorem). *Let  $L|K$  be a finite Galois extension. Then there exists  $\alpha \in L$  such that its conjugates  $g(\alpha)$ ,  $g \in \text{Gal}(L|K)$ , over  $K$  form a basis for  $L$  as a vector space over  $K$ .*

*Example 9.12.* Let  $p$  be a prime and  $\zeta$  a primitive  $p$ th root of unity in  $\mathbb{C}$ . Consider the cyclotomic field  $\mathcal{K}_p = \mathbb{Q}(\zeta)$ . Then  $\mathcal{K}_p|\mathbb{Q}$  is a finite Galois extension. The conjugates of  $\zeta$  over  $\mathbb{Q}$  are  $\zeta, \zeta^2, \dots, \zeta^{p-1}$ , and they are precisely the roots of  $\Phi_p$  which is the minimum polynomial of  $\zeta$  over  $\mathbb{Q}$  by Proposition 9.1. Moreover, in the proof of Theorem 9.4 we showed that the conjugates of  $\zeta$  over  $\mathbb{Q}$  form a basis for  $\mathcal{K}_p$  as a vector space over  $\mathbb{Q}$ .

## 10. IMPLICATIONS OF GALOIS THEORY IN THE CONTEXT OF FINITE FIELDS

**10.1. Subfields of finite fields.** First we give an explicit description of the subfields of any finite field.

**Proposition 10.1.** *Let  $p$  be a prime, and let  $n \in \mathbb{N}$ . Then the subfields of the finite field  $\mathbb{F}_{p^n}$  are parameterised by the divisors of  $n$ . For every  $d \in \mathbb{N}$  with  $d | n$  the polynomial  $X^{p^d} - X$  splits into distinct linear factors over  $\mathbb{F}_{p^n}$  and its roots constitute a subfield  $\mathbb{F}_{p^d}$  of cardinality  $p^d$  in  $\mathbb{F}_{p^n}$ . Moreover, these are all the subfields of  $\mathbb{F}_{p^n}$ .*

*Proof.* Let  $d \in \mathbb{N}$ . We know that, up to isomorphism, the splitting field of the separable polynomial  $X^{p^d} - X$  is the unique field of cardinality  $p^d$ ; cf. Theorem 6.2. Hence  $\mathbb{F}_{p^n}$  has at most one subfield of cardinality  $p^d$ , and it has such a subfield if and only if  $X^{p^d} - X$  splits into linear factors over  $\mathbb{F}_{p^n}$ .

The field  $\mathbb{F}_{p^n}$  itself is the splitting field of  $X^{p^n} - X$ . As both  $X^{p^d} - X$  and  $X^{p^n} - X$  have no repeated roots,  $X^{p^d} - X$  splits over  $\mathbb{F}_{p^n}$  if and only if  $(X^{p^d} - X) | (X^{p^n} - X)$ . The latter condition is equivalent to  $(p^d - 1) | (p^n - 1)$  which in turn is equivalent to  $d | n$ ; this follows from Lemma 8.1 and its proof.  $\square$

**Corollary 10.2.** *Let  $q$  be a prime power and let  $d, n \in \mathbb{N}$ . Then  $\mathbb{F}_{q^d}$  occurs as a subfield of  $\mathbb{F}_{q^n}$  if and only if  $d | n$ .*

**10.2. Automorphisms of finite fields.** Let  $K$  be a finite field of characteristic  $p > 0$ . Recall from Proposition 6.3 that the map  $F : K \rightarrow K$ ,  $\alpha \mapsto \alpha^p$  constitutes an automorphism of  $K$ , the Frobenius automorphism.

**Proposition 10.3.** *Let  $p$  be a prime, and let  $n \in \mathbb{N}$ . Then  $\text{Aut}(\mathbb{F}_{p^n})$  is a cyclic group of order  $n$ , generated by the Frobenius automorphism.*

*Proof.* Clearly, the Frobenius automorphism generates a cyclic subgroup  $\langle F \rangle$  of  $\text{Aut}(\mathbb{F}_{p^n})$ . Observe that

$$\begin{aligned} \text{ord}(F) &= \min\{d \in \mathbb{N} \mid F^d = \text{id}_{\mathbb{F}_{p^n}}\} \\ &= \min\{d \in \mathbb{N} \mid \forall \alpha \in \mathbb{F}_{p^n} : F^d(\alpha) = \alpha\} \\ &= \min\{d \in \mathbb{N} \mid \forall \alpha \in \mathbb{F}_{p^n} : \alpha^{p^d} - \alpha = 0\}. \end{aligned}$$

By Theorem 10.1 the subfields of  $\mathbb{F}_{p^n}$  are precisely the splitting fields of  $X^{p^d} - X$  for  $d \mid n$ . The field  $\mathbb{F}_{p^n}$  is the splitting field of  $X^{p^n} - X$ , and hence  $\text{ord}(F) = n$ .

It remains to show that every automorphism of  $\mathbb{F}_{p^n}$  is a power of  $F$ . For this it suffices to show that  $|\text{Aut}(\mathbb{F}_{p^n})| \leq |\langle F \rangle| = n$ . Let  $\alpha$  be a primitive element of  $\mathbb{F}_{p^n}$ . By Kronecker's Theorem every automorphism  $g$  of  $\mathbb{F}_{p^n}$  is uniquely determined by its effect on  $\alpha$ . The minimum polynomial  $f$  of  $\alpha$  over  $\mathbb{F}_p$  has degree  $n$ . Since  $g$  acts trivially on  $\mathbb{F}_p$ , the equation  $f(\alpha) = 0$  becomes  $f(g(\alpha)) = 0$  under the action of  $g$ . Since  $f$  has at most  $n$  roots, there are at most  $n$  possible values for  $g(\alpha)$ . Hence  $|\text{Aut}(\mathbb{F}_{p^n})| \leq n$  as wanted.  $\square$

**Corollary 10.4.** *Let  $q = p^r$  be a prime power, and let  $n \in \mathbb{N}$ . Then  $\mathbb{F}_{q^n} | \mathbb{F}_q$  is a Galois extension with Galois group  $\text{Gal}(\mathbb{F}_{q^n} | \mathbb{F}_q) = \langle F^r \rangle \cong \mathbb{Z}/n\mathbb{Z}$ , where  $F^r(\alpha) = \alpha^q$  for all  $\alpha \in \mathbb{F}_{q^n}$ .*

*Proof.* As  $q = p^r$  we have  $F^r(\alpha) = \alpha^q$  for all  $\alpha \in \mathbb{F}_{q^n}$ . Clearly,  $\mathbb{F}_q$  is the fixed field of  $\langle F^r \rangle$ . Hence  $\mathbb{F}_{q^n} | \mathbb{F}_q$  is a Galois extension, and  $G := \text{Gal}(\mathbb{F}_{q^n} | \mathbb{F}_q)$  satisfies

$$\langle F^r \rangle \subseteq G \subseteq \text{Aut}(\mathbb{F}_{q^n}) = \langle F \rangle.$$

Suppose that  $F^s \in G$ . Writing  $s = ur + t$  with  $u, t \in \mathbb{Z}$  and  $0 \leq t < r$ , we have  $F^t = F^s(F^r)^{-u} \in G$ . This implies  $\alpha^{p^t} - \alpha = F^t(\alpha) - \alpha = 0$  for all  $\alpha \in \mathbb{F}_q$ . Since  $p^t < p^r = q$ , this implies that  $X^{p^t} - X = 0$ , i.e.  $t = 0$ . Consequently,  $F^s = (F^r)^u$  is a power of  $F^r$ , and  $G = \langle F^r \rangle$ .  $\square$

**10.3. Galois Theory for finite fields.** Putting together the results of the previous two subsections, we obtain

**Theorem 10.5** (Main Theorem of Galois Theory for finite fields). *Let  $q = p^r$  be a prime power, and let  $n \in \mathbb{N}$ . Then  $\mathbb{F}_{q^n} | \mathbb{F}_q$  is a Galois extension of degree  $n$  with cyclic Galois group*

$$G := \text{Gal}(\mathbb{F}_{q^n} | \mathbb{F}_q) = \langle F^r \rangle \cong \mathbb{Z}/n\mathbb{Z},$$

*generated by the  $r$ th power of the Frobenius automorphism  $F : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$ ,  $\alpha \mapsto \alpha^p$ .*

*The inclusion-reversing correspondence between the intermediate fields of  $\mathbb{F}_{q^n} | \mathbb{F}_q$  and the subgroups of  $G$  takes the following special form. The set of intermediate fields of  $\mathbb{F}_{q^n} | \mathbb{F}_q$  and the set of subgroups of  $G = \langle F^r \rangle$  are*

$$\begin{aligned} \mathcal{M} &= \{M_d \mid d \mid n\}, \quad \text{where } M_d := \{\alpha \in \mathbb{F}_{q^n} \mid \alpha^{q^d} - \alpha = 0\} \cong \mathbb{F}_{q^d}, \\ \mathcal{H} &= \{H_d \mid d \mid n\}, \quad \text{where } H_d := \langle (F^r)^d \rangle \cong \mathbb{Z}/(n/d)\mathbb{Z}. \end{aligned}$$

*If  $d \in \mathbb{N}$  with  $d \mid n$ , then*

$$\begin{aligned} H_d &= \{h \in G \mid \forall \alpha \in M_d : h(\alpha) = \alpha\}, \\ M_d &= \{\alpha \in \mathbb{F}_{q^n} \mid \forall h \in H_d : h(\alpha) = \alpha\}. \end{aligned}$$

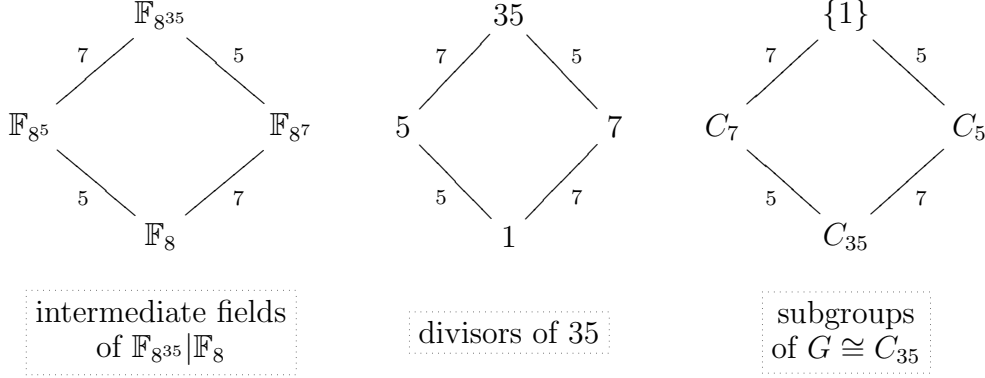
*If  $d_1, d_2 \in \mathbb{N}$  with  $d_1 \mid n$  and  $d_2 \mid n$ , then*

$$M_{d_1} \subseteq M_{d_2} \iff d_1 \mid d_2 \iff H_{d_1} \supseteq H_{d_2}.$$

*Moreover, for all  $d \in \mathbb{N}$  with  $d \mid n$  one has*

$$|G : H_d| = d = [M_d : \mathbb{F}_q].$$

*Example 10.6.* Let  $q := 8 = 2^3$  and  $n := 35 = 5 \cdot 7$ . Consider the Galois extension  $\mathbb{F}_{8^{35}}|\mathbb{F}_8$ . Writing  $C_m$  to denote a cyclic group of order  $m$ , the description of the lattice of intermediate fields provided by the theorem can be depicted as follows.



◇

Consider an extension  $\mathbb{F}_{q^n}|\mathbb{F}_q$  of finite fields where  $q = p^r$  is a prime power and  $n \in \mathbb{N}$ . Let  $\alpha \in \mathbb{F}_{q^n}$ , and put  $d := [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ . Then  $\text{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) = \langle F^r \rangle$  is cyclic of order  $n$ , but the restriction of  $F^r$  to  $\mathbb{F}_q(\alpha)$  is an automorphism of order  $d$ .

Therefore the conjugates of  $\alpha$  over  $\mathbb{F}_q$  are the elements

$$\alpha = F^0(\alpha), \quad \alpha^q = F^r(\alpha), \quad \alpha^{q^2} = F^{2r}(\alpha), \quad \dots, \quad \alpha^{q^{d-1}} = F^{(d-1)r}(\alpha).$$

Observe that any automorphism of  $\mathbb{F}_q(\alpha)$  which acts trivially on  $\mathbb{F}_q$  is uniquely determined by its effect on  $\alpha$ . Consequently, the conjugates of  $\alpha$  listed above are pairwise distinct. We now characterise the conjugates of  $\alpha$  over  $\mathbb{F}_q$  in terms of the minimum polynomial of  $\alpha$  over  $\mathbb{F}_q$ .

**Proposition 10.7.** *Let  $q$  be a prime power, and let  $n \in \mathbb{N}$ . Let  $\alpha \in \mathbb{F}_{q^n}$ , and put  $d := [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ . Then*

$$\text{mipo}_{\mathbb{F}_q}(\alpha) = (X - \alpha)(X - \alpha^q) \cdots (X - \alpha^{q^{d-1}}).$$

*In other words, the roots of  $\text{mipo}_{\mathbb{F}_q}(\alpha)$  are precisely the conjugates of  $\alpha$  over  $\mathbb{F}_q$ .*

*Proof.* Write  $f := \text{mipo}_{\mathbb{F}_q}(\alpha)$ . If  $g \in \text{Gal}(\mathbb{F}_q(\alpha)|\mathbb{F}_q)$ , then  $g$  acts as the identity on  $\mathbb{F}_q$ , and hence the equation  $f(\alpha) = 0$  implies  $f(g(\alpha)) = 0$ . Consequently, every conjugate of  $\alpha$  over  $\mathbb{F}_q$  is a root of  $f$ . As we observed  $\alpha$  has precisely  $d$  conjugates over  $\mathbb{F}_q$ , namely  $\alpha, \alpha^q, \dots, \alpha^{q^{d-1}}$ . This gives

$$f = (X - \alpha)(X - \alpha^q) \cdots (X - \alpha^{q^{d-1}}).$$

□

**Corollary 10.8.** *Let  $q$  be a prime power, and  $n \in \mathbb{N}$ . Let  $f \in \mathbb{F}_q[X]$  be irreducible. If  $f$  has a root in  $\mathbb{F}_{q^n}$ , then it splits into distinct linear factors over  $\mathbb{F}_{q^n}$ .*

Next we formulate the Normal Basis Theorem for finite fields.

**Theorem 10.9** (Normal bases for finite fields). *Let  $n \in \mathbb{N}$  and consider the extension  $\mathbb{F}_{q^n}|\mathbb{F}_q$  of finite fields. Then there exists  $\alpha \in \mathbb{F}_{q^n}$  such that its conjugates  $\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}$  over  $\mathbb{F}_q$  form a basis for  $\mathbb{F}_{q^n}$  as a vector space over  $\mathbb{F}_q$ .*

This theorem has practical applications. For instance, by representing elements of a finite field  $\mathbb{F}_{p^n}$  in terms of a normal basis  $\alpha, \alpha^p, \dots, \alpha^{p^{n-1}}$  over its prime subfield  $\mathbb{F}_p$  one can very efficiently carry out exponentiation in  $\mathbb{F}_{p^n}$ . This is because raising an element  $\beta = \sum_{k=0}^{n-1} b_k \alpha^{p^k} \in \mathbb{F}_{p^n}$  to the  $p$ th power can simply be achieved by a cyclic shift of its coordinates with respect to the chosen normal basis:

$$\beta^p = \left( \sum_{k=0}^{n-1} b_k \alpha^{p^k} \right)^p = \sum_{k=0}^{n-1} b_k \alpha^{p^{k+1}} = b_{n-1} \alpha + b_0 \alpha^p + \dots + b_{n-2} \alpha^{p^{n-1}}.$$

**Lemma 10.10 (Artin).** *Let  $G$  be a group, and let  $K$  be a field. Let  $n \in \mathbb{N}$ , and let  $\sigma_1, \dots, \sigma_n$  be pairwise distinct homomorphisms from  $G$  into  $K^*$ .*

*Then  $\sigma_1, \dots, \sigma_n$  are linearly independent over  $K$ , i.e. if  $a_1, \dots, a_n \in K$  are such that the function  $a_1 \sigma_1 + \dots + a_n \sigma_n$  is constantly zero then  $a_1 = \dots = a_n = 0$ .*

*Proof.* We argue by induction on  $n$ . If  $n = 1$ , then  $\sigma_1 : G \rightarrow K^*$  is visibly not constantly zero and hence linearly independent.

Now suppose that  $n > 1$ . Let  $a_1, \dots, a_n \in K$  such that the map  $a_1 \sigma_1 + \dots + a_n \sigma_n$  is constantly zero. This means that

$$a_1 \sigma_1(g) + \dots + a_n \sigma_n(g) = 0 \quad \text{for all } g \in G.$$

As  $\sigma_1 \neq \sigma_n$ , we find  $h \in G$  such that  $\sigma_1(h) \neq \sigma_n(h)$ . We obtain a new equation from the one above simply by multiplying through with  $\sigma_n(h)$ :

$$a_1 \sigma_n(h) \sigma_1(g) + a_2 \sigma_n(h) \sigma_2(g) + \dots + a_n \sigma_n(h) \sigma_n(g) = 0 \quad \text{for all } g \in G.$$

We obtain a second useful equation by substituting  $hg$  for  $g$ : as  $g$  runs through  $G$  so does  $hg$  and hence

$$\begin{aligned} a_1 \sigma_1(h) \sigma_1(g) + a_2 \sigma_2(h) \sigma_2(g) + \dots + a_n \sigma_n(h) \sigma_n(g) = \\ a_1 \sigma_1(hg) + a_2 \sigma_2(hg) + \dots + a_n \sigma_n(hg) = 0 \quad \text{for all } g \in G. \end{aligned}$$

Subtracting the second from the first new equation we deduce that

$$\tilde{a}_1 \sigma_1(g) + \dots + \tilde{a}_{n-1} \sigma_{n-1}(g) = 0 \quad \text{for all } g \in G,$$

where  $\tilde{a}_i := a_i(\sigma_n(h) - \sigma_i(h)) \in K$  for  $i \in \{1, \dots, n-1\}$ . By induction  $\sigma_1, \dots, \sigma_{n-1}$  are linearly independent and hence all the coefficients  $\tilde{a}_i$  are zero, in particular  $a_1(\sigma_n(h) - \sigma_1(h)) = \tilde{a}_1 = 0$ . Since  $\sigma_n(h) - \sigma_1(h) \neq 0$ , this implies  $a_1 = 0$ . But now the original dependence relation simplifies to

$$a_2 \sigma_2(g) + \dots + a_n \sigma_n(g) = 0 \quad \text{for all } g \in G,$$

and consequently  $a_2 = \dots = a_n = 0$ , by induction. □

*Proof of Theorem 10.9.* Write  $q = p^r$  so that  $\text{Gal}(\mathbb{F}_{q^n} | \mathbb{F}_q) = \langle F^r \rangle \cong \mathbb{Z}/n\mathbb{Z}$  in accordance with the Main Theorem of Galois Theory for finite fields. Consider the map  $F^r : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$  as a linear endomorphism of the vector space  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ . We show below that the minimum polynomial of this linear map is equal to  $X^n - 1$ . Since  $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ , this implies that the minimum polynomial of the linear map  $F^r$  is equal to its characteristic polynomial, and Linear Algebra supplies a cyclic vector, i.e. a vector  $\alpha \in \mathbb{F}_{q^n}$  such that

$$\alpha = F^0(\alpha), \quad \alpha^q = F^r(\alpha), \quad \alpha^{q^2} = F^{2r}(\alpha), \quad \dots, \quad \alpha^{q^{n-1}} = F^{(n-1)r}(\alpha)$$

constitute a basis for  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ . This is the sought normal basis.

It remains to prove that the minimum polynomial of the  $\mathbb{F}_q$ -linear map  $F^r : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$  is  $X^n - 1$ . Clearly,  $F^{nr} = \text{id}_{\mathbb{F}_{q^n}}$  and hence the minimum polynomial of  $F^r$  divides  $X^n - 1$ . It remains to show that  $F^r$  satisfies no non-trivial polynomial equation of degree smaller than  $n$  over  $\mathbb{F}_q$ . Since the maps

$$\text{id}_{\mathbb{F}_{q^n}} = (F^r)^0, \quad F^r = (F^r)^1, \quad \dots, \quad F^{(n-1)r} = (F^r)^{n-1}$$

restrict to pairwise distinct homomorphisms from the group  $\mathbb{F}_{q^n}^*$  into  $\mathbb{F}_{q^n}^*$ , the result follows from Lemma 10.10.  $\square$

*Example 10.11.* Consider  $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$  where  $\alpha$  is a root of the irreducible polynomial  $X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ . Then  $1, \alpha, \alpha^2$  is a basis for  $\mathbb{F}_8$  as a vector space over  $\mathbb{F}_2$ , in accordance with Kronecker's Theorem. From this one sees that

$$\alpha, \quad \alpha^2, \quad \alpha^4 = \alpha^2 + \alpha + 1$$

is a basis which consists precisely of the conjugates of  $\alpha$  over  $\mathbb{F}_2$ .

**10.4. Cyclotomic polynomials over finite fields.** Every element of a finite field is a root of unity. Consequently there is an interesting connection between finite fields and cyclotomic fields over  $\mathbb{Q}$ . In Section 8 we already took advantage of reducing cyclotomic polynomials modulo a prime  $p$ . In particular, Lemma 8.11 collects some basic observations about the cyclotomic polynomial  $\Phi_m$  regarded as a polynomial over  $\mathbb{F}_p$ .

**Proposition 10.12.** *Let  $q = p^r$  be a prime power, and let  $m \in \mathbb{N}$ . Consider  $\Phi_m$  as a polynomial over  $\mathbb{F}_p$ .*

- (1) *If  $p \nmid m$ , then  $\Phi_m$  factorises over  $\mathbb{F}_q$  into  $\varphi(m)/d$  distinct irreducible factors, each of degree  $d$ , where  $d = \text{ord}(\bar{q})$  in  $(\mathbb{Z}/m\mathbb{Z})^*$ . Equivalently,  $d$  can be described as  $d = \min\{k \mid m \mid (q^k - 1)\}$ .*
- (2) *If  $m = \tilde{m}p^s$  with  $s \geq 1$  and  $p \nmid \tilde{m}$ , then  $\Phi_m = \Phi_{\tilde{m}}^{p^s - p^{s-1}}$ .*

*Proof.* (1) Suppose that  $p \nmid m$ . By Lemma 8.11, the polynomial  $\Phi_m$  is separable over  $\mathbb{F}_p$ . Hence it decomposes into distinct irreducible factors over  $\mathbb{F}_q$ . Since  $\deg(\Phi_m) = \varphi(m)$ , it suffices to prove that each of the irreducible factors has the claimed degree. Let  $f$  be an irreducible factor of  $\Phi_m$  over  $\mathbb{F}_q$ , and put  $d := \deg(f)$ . Consider the field  $\mathbb{F}_{q^d} = \mathbb{F}_q(\alpha)$  obtained from  $\mathbb{F}_q$  by adjoining a root  $\alpha$  of  $f$ . By Lemma 8.11,  $\alpha$  is a primitive  $m$ th root of unity, i.e.  $\alpha \in \mathbb{F}_{q^d}^*$  and the order of  $\alpha$  in  $\mathbb{F}_{q^d}^*$  is  $m$ . By Lagrange's Theorem,  $m = \text{ord}(\alpha) \mid |\mathbb{F}_{q^d}^*| = q^d - 1$ , i.e.  $q^d \equiv_m 1$ .

Conversely, suppose that  $k \in \mathbb{N}$  such that  $q^k \equiv_m 1$ , or equivalently  $m \mid (q^k - 1)$ . Then the multiplicative group of the field  $\mathbb{F}_{q^k}$  is cyclic of order divisible by  $m$ . Therefore  $\mathbb{F}_{q^k}$  contains one and hence all  $\varphi(m)$  primitive  $m$ th roots of unity. This shows that  $\mathbb{F}_{q^d} = \mathbb{F}_q(\alpha)$  can be embedded into  $\mathbb{F}_{q^k}$ , and hence  $d \leq k$ .

(2) Raising a polynomial to its  $p$ th power constitutes a ring endomorphism of  $\mathbb{F}_p[X]$  which acts as the identity on  $\mathbb{F}_p$ . Indeed, this map is the restriction of the Frobenius endomorphism of the field  $\mathbb{F}_p(X)$ ; cf. Proposition 6.3. We argue by induction on  $\tilde{m}$ . If  $\tilde{m} = 1$ , then

$$\Phi_1^{p^s - p^{s-1}} = (X - 1)^{p^s - p^{s-1}} = \frac{(X - 1)^{p^s}}{(X - 1)^{p^{s-1}}} = \frac{X^{p^s} - 1}{X^{p^{s-1}} - 1} = \Phi_{p^s}$$

as wanted. Now suppose that  $\tilde{m} \geq 2$ . The formulae

$$X^{\tilde{m}} - 1 = \prod_{\tilde{d}|\tilde{m}} \Phi_{\tilde{d}} \quad \text{and} \quad X^m - 1 = \prod_{d|m} \Phi_d$$

together with the equation

$$(X^{\tilde{m}} - 1)^{p^s - p^{s-1}} (X^{\tilde{m}} - 1)^{p^{s-1}} = (X^{\tilde{m}} - 1)^{p^s} = X^m - 1$$

imply that

$$\left( \prod_{\tilde{d}|\tilde{m}} \Phi_{\tilde{d}} \right)^{p^s - p^{s-1}} (X^{\tilde{m}p^{s-1}} - 1) = \prod_{d|m} \Phi_d = \left( \prod_{d|\tilde{m}p^{s-1}} \Phi_d \right) \left( \prod_{\tilde{d}|\tilde{m}} \Phi_{\tilde{d}p^s} \right).$$

Cancelling  $X^{\tilde{m}p^{s-1}} - 1$  on the left hand side against  $\prod_{d|\tilde{m}p^{s-1}} \Phi_d$  on the right hand side, this gives

$$\prod_{\tilde{d}|\tilde{m}} \Phi_{\tilde{d}}^{p^s - p^{s-1}} = \left( \prod_{\tilde{d}|\tilde{m}} \Phi_{\tilde{d}} \right)^{p^s - p^{s-1}} = \prod_{\tilde{d}|\tilde{m}} \Phi_{\tilde{d}p^s}.$$

By induction we understand every factor on the left hand side except for  $\Phi_{\tilde{m}}^{p^s - p^{s-1}}$ . Cancelling these factors and their corresponding terms on the right hand side, we obtain  $\Phi_{\tilde{m}}^{p^s - p^{s-1}} = \Phi_{\tilde{m}p^s} = \Phi_m$  as wanted.  $\square$

Using our knowledge of the automorphism groups of finite fields we actually arrive at a clear procedure for working out a decomposition of cyclotomic polynomials over finite fields. Conceptually, it is slightly easier to work out a decomposition of the related polynomials  $X^m - 1$ ,  $m \in \mathbb{N}$ . We illustrate this by a concrete example.

*Example 10.13.* Consider the polynomial  $X^{12} - 1$  over  $\mathbb{F}_5$ . From  $5 \not\equiv_{12} 1$  and  $5^2 = 25 \equiv_{12} 1$  we gather that  $\mathbb{F}_{25}$  is the smallest finite field of characteristic 5 which contains a primitive 12-root of unity. We can realise  $\mathbb{F}_{25}$  as  $\mathbb{F}_5(\alpha)$  where  $\alpha$  is a root of the irreducible polynomial  $X^2 + 4X + 2 \in \mathbb{F}_5[X]$ . One can check that  $\alpha$  is a primitive element of  $\mathbb{F}_{25}$ . Hence  $\zeta := \alpha^2$  is a primitive 12th root of unity. Accordingly,  $X^{12} - 1$  factors over  $\mathbb{F}_{25}$  as

$$X^{12} - 1 = (X - 1)(X - \zeta)(X - \zeta^2) \cdots (X - \zeta^{11}).$$

The task is to group these linear factors appropriately so that for each individual group the product of its members yields an irreducible polynomial over  $\mathbb{F}_5$ . Some of the linear factors are already defined over  $\mathbb{F}_5$ , e.g.  $X - 1$  and  $X - \zeta^6 = X - (-1) = X + 1$ . The elements 2 and 3 have order 4 in  $\mathbb{F}_5^*$ , hence  $(X - \zeta^3)(X - \zeta^9) = (X - 2)(X - 3)$ .

There is a systematic way to find these linear and the irreducible factors of higher degree. By Proposition 10.7, it suffices to work out the conjugates of each element  $\zeta^k$ ,  $k \in \{0, 1, \dots, 11\}$  over  $\mathbb{F}_5$ . This is the same as decomposing  $\mathbb{Z}/12\mathbb{Z}$  into orbits under multiplication by 5. The orbits and the corresponding irreducible

polynomials in  $\mathbb{F}_5[X]$  are:

$$\begin{aligned}
\{0\} & X - \zeta^0 = X - 1, \\
\{1, 5\} & (X - \zeta^1)(X - \zeta^5) = X^2 - 2X - 1, \\
\{2, 10\} & (X - \zeta^2)(X - \zeta^{10}) = X^2 - X + 1, \\
\{3\} & X - \zeta^3 = X + 3 = X - 2, \\
\{4, 8\} & (X - \zeta^4)(X - \zeta^8) = X^2 + X + 1, \\
\{6\} & X - \zeta^6 = X + 1, \\
\{7, 11\} & (X - \zeta^7)(X - \zeta^{11}) = X^2 + 2X - 1, \\
\{9\} & X - \zeta^9 = X + 2.
\end{aligned}$$

Hence the decomposition of  $X^{12} - 1$  into irreducible factors over  $\mathbb{F}_5$  is

$$\begin{aligned}
X^{12} - 1 = & \underbrace{(X - 1)}_{=\Phi_1} \cdot \underbrace{(X + 1)}_{=\Phi_2} \cdot \underbrace{(X + 2)(X - 2)}_{=\Phi_4} \cdot \underbrace{(X^2 + X + 1)}_{=\Phi_3} \\
& \cdot \underbrace{(X^2 - X + 1)}_{=\Phi_6} \cdot \underbrace{(X^2 + 2X - 1)(X^2 - 2X - 1)}_{=\Phi_{12}}.
\end{aligned}$$

This is in accordance with the qualitative statement made by Proposition 10.12.

– the end –

## INDEX

- Additive form of Möbius Inversion, 30
- adjoining a square root, 7
- algebraic element, 10
- algebraic field extension, 12
- Artin's Lemma, 43
  
- baby sequence, 24
- Baby-step Giant-step Algorithm, 24
  
- Central case of the Theorem of Gauss-Wanzenel, 35
- Characterisation of algebraic elements, 12
- Characterisation of finite extensions, 12
- characteristic, 19
- circle in the complex plane, 4
- compasses and straight edge construction, 3
- complete enumeration, 24
- complex conjugation, 4
- complex plane, 4
- conjugates, 39
- constructible number, 4
- cyclotomic field, 33
- cyclotomic polynomial, 29
  
- degree of a field extension, 8
- degree of a polynomial, 15
- Diffie-Hellman key exchange, 22
- Dirichlet's Theorem, 31
- discrete logarithm, 22
- distance, 4
- divisibility class, 16
- Division with remainder, 15
  
- Eisenstein's Criterion, 18
- El Gamal cryptosystem, 23
- elementary construction steps, 4
- Euler phi function, 28
- Existence and Uniqueness Theorem for finite fields, 19
- exponent of a group, 20
  
- field extension, 5
- field of rational functions, 10
- finite extension, 8
- Frobenius automorphism, 20
- Frobenius endomorphism, 19
  
- Galois extension, 37
- Galois group, 37
- Gauss' Lemma, 17
- giant sequence, 24
- greatest common divisor, 16
- group of units, 15
  
- highest common factor, 16
- intermediate field, 5
- irreducible polynomial, 14, 16
  
- Kronecker's Theorem, 14
  
- line in the complex plane, 4
  
- Möbius function, 30
- Möbius Inversion, 30
- Main Theorem of Galois Theory, 38
- Main Theorem of Galois Theory for finite fields, 41
- Mersenne prime method, 26
- minimum polynomial, 11
- monic polynomial, 16
  
- Normal Basis Theorem, 40
- Normal Basis Theorem for finite fields, 42
- Number of irreducible polynomials, 30
  
- Pohlig-Hellman Algorithm, 25
- polynomial division, 15
- prime field, 19
- prime polynomial, 16
- prime subfield, 18
- primitive element of a finite field, 21
- primitive element of an extension, 13
- primitive root of unity, 28
  
- reducible polynomial, 16
- remainder, 15
- ring, 15
  
- separable polynomial, 28
- simple field extension, 13
- Special case of Dirichlet's Theorem, 31
- splitting field, 16
- Structure of cyclotomic fields, 33
- subfield generated by a set, 5
  
- Theorem of Gauss-Wanzenel, 3
- Theorem of Kronecker-Weber, 34
- Tower Law, 9
- transcendental element, 10
  
- unique factorisation domain, 16

DEPARTMENT OF MATHEMATICS, ROYAL HOLLOWAY, UNIVERSITY OF LONDON, EGHAM  
TW20 0EX, UNITED KINGDOM

*E-mail address:* Benjamin.Klopsch@rhul.ac.uk