



universität  
wien

# BACHELORARBEIT

Titel der Bachelorarbeit  
Infinite Galois Theory

Verfasser  
Jakob Preininger

angestrebter akademischer Grad  
Bachelor of Science

Wien, im März 2010

Studienkennzahl lt. Studienblatt: A 033 621  
Studienrichtung lt. Studienblatt: Mathematik  
Betreuer: Dr. Leonhard Summerer

## CONTENTS

Preface	2
1. Definitions and results from classical Galois theory	2
2. Finite Fields	6
3. The fundamental theorem of Galois theory	9
4. The Krull topology	12
5. The projective limit and profinite groups	14
6. The fundamental theorem for infinite Galois extensions	16
7. Examples for infinite Galois groups	17
References	21

## PREFACE

The aim of this paper is to give an introduction to infinite Galois theory and especially to understand the absolute Galois group of finite fields. To do so I will give a brief review of the definitions and results of classical Galois theory and apply them onto the case of finite fields. Then I will give a proof of the fundamental theorem of Galois theory that gives a direct link between intermediate fields of a field extension and subgroups of its Galois group. To generalize it to the infinite case however I will need the notion of the Krull topology which leads to the definition of the projective limit, a very powerful tool of category theory. Finally I will use the generalized fundamental theorem to compute the absolute Galois group of finite fields and to determine its intermediate fields.

## 1. DEFINITIONS AND RESULTS FROM CLASSICAL GALOIS THEORY

This chapter recalls the definitions and results from classical Galois theory that we will use in this paper.

At first we define the most important tool to characterize fields.

**Definition.** Let  $F$  be a field and let  $\psi : \mathbb{Z} \rightarrow F$  be the canonical ring homomorphism defined by  $\psi(1) = 1$ . Then  $\ker(\psi)$  is an ideal of  $\mathbb{Z}$  and hence isomorphic to  $n\mathbb{Z}$  for some  $n \in \mathbb{Z}_{\geq 0}$ . Now one defines the characteristic of  $F$  to be  $n$  ( $\text{char}(F) = n$ ).

Since  $F$  has no zero divisors the ring  $\text{im}(\psi) \cong \mathbb{Z}/n\mathbb{Z}$  doesn't have any either. So  $n$  has to be either 0 or a prime and  $F$  contains a field isomorphic to  $\mathbb{Q}$  or  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  respectively. This field is called the prime field of  $F$ . Clearly it is the smallest field contained in  $F$ .

In Galois theory we study homomorphisms  $F \rightarrow E$  of fields. Since every homomorphism of fields is injective we can find a subfield of  $E$  which is isomorphic to  $F$ . Hence the following definition.

**Definition.** A pair of fields  $E/F$  is called a field extension if  $F$  is a subfield of  $E$ .

For any field extension  $E/F$  we have that  $\text{char}(E) = \text{char}(F)$  because the prime field has to be the same. So for every value of the characteristic we get a distinct family of fields which contain its prime field and there are no homomorphisms between fields of different characteristic.

For a field extension  $E/F$  the field  $E$  can be seen as an  $F$  vector space.

**Definition.** An extension  $E/F$  is called finite if  $E$  is a finite dimensional vector space over  $F$ . In this case we write  $|E/F| = [E : F] = \dim_F E = n$  and say that the extension  $E/F$  is of degree  $n$ . Otherwise  $E/F$  is called an infinite extension and  $|E/F| = [E : F] = \infty$ .

In particular any finite field extension  $E$  of  $\mathbb{F}_p$  has  $p^n$  elements for some  $n \in \mathbb{N}$ . In fact we will see later that for any prime  $p$  and any natural  $n$  there is exactly one field with  $p^n$  elements.

Galois theory only covers algebraic field extensions. Hence the following definitions.

**Definition.** We call  $\alpha \in E$  algebraic over  $F$  if there is a polynomial  $p \in F[X]$  such that  $p(\alpha) = 0$ . Otherwise we call  $\alpha$  transcendental over  $F$ .

**Lemma.** (a) If  $p, q \in F[X]$  are polynomials with  $p(\alpha) = q(\alpha) = 0$  then for  $r = \text{gcd}(p, q)$  we also have  $r(\alpha) = 0$ .

(b) If  $\alpha \in E$  is algebraic over  $F$  then there is exactly one monic polynomial  $m_{\alpha, F} \in F[X]$  of minimal degree such that  $m_{\alpha, F}(\alpha) = 0$ .

*Proof.* (a) Since  $F[X]$  is a principal ideal domain  $r$  can be written as a linear combination of  $p$  and  $q$ . Hence there are  $a, b \in F[X]$  with

$$r = ap + bq.$$

As an immediate consequence we get that  $r(\alpha) = 0$ .

(b) Assume  $p, q$  are monic polynomials of minimal degree  $n$  with  $p(\alpha) = q(\alpha) = 0$ . Then for  $r = \gcd(p, q)$  we have  $r(\alpha) = 0$  and as  $r$  then also has degree  $n$  we get  $p = q = r$ .  $\square$

**Definition.** (a) For  $\alpha \in E$  algebraic over  $F$  the polynomial  $m_{\alpha, F} \in F[x]$  of minimal degree with  $m_{\alpha, F}(\alpha) = 0$  is called the minimal polynomial of  $\alpha$  over  $F$ .

(b) A field extension  $E/F$  is called algebraic if every element  $\alpha \in E$  is algebraic.

The following theorem guarantees that there is an upper boundary for algebraic field extension of a given field  $F$ .

**Theorem.** *Let  $F$  be a field. Then there is a maximal algebraic extension  $\overline{F}$  of  $F$  such that any algebraic extension  $E$  of  $F$  is isomorphic to some subfield of  $\overline{F}$ . This extension is unique up to isomorphism and is called the algebraic closure of  $F$ .<sup>1</sup>*

So for a given field  $F$  every algebraic field extension  $E$  of  $F$  is a subfield of  $\overline{F}$ . The goal of infinite Galois theory is to find and characterize all those intermediate fields  $E$ . To do this we need some further notions for field extensions.

**Definition.** (a) A polynomial  $p \in F[X]$  is called separable if it has no repeated roots in  $\overline{F}$ .

(b) We say that an algebraic extension  $E/F$  is separable if for any  $\alpha \in E$  the minimal polynomial  $m_{\alpha, F}$  is separable.

(c) An extension  $E/F$  is called normal if any polynomial  $p \in F[X]$  which has a root in  $E$  splits into linear factors over  $E$ .

(d) Finally we call a field extension Galois if it is algebraic, normal and separable.

We can now define the Galois group of an extension  $E/F$  which is what Galois theory is about.

---

<sup>1</sup>A proof can be found in [1, p.104ff].

**Definition.** Let  $E/F$  be a Galois extension. Then the group of automorphisms on  $E$  that fix  $F$  is called the Galois group  $Gal(E/F)$  of  $E$  over  $F$ .

$$Gal(E/F) = Aut_F(E) = \{\sigma \in Aut(E) : \sigma|_F = id_F\}.$$

For later use we state the following facts about finite fields and finite extensions.

**Lemma.** *Let  $F$  be a finite field. Then its multiplicative group  $F^*$  is cyclic.*

*Proof.* Since the group  $F^*$  is abelian and finite it is isomorphic to some product  $(\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z})$  with  $n_1 | n_2 | \cdots | n_k$ . So for every element in  $a \in F^*$  its order is some divisor of  $n_k$ . Hence all elements of  $F^*$  are roots of the polynomial  $X^{n_k} - 1$  and hence  $|F^*| \leq n_k$ . So  $F^* \cong \mathbb{Z}/n_k\mathbb{Z}$  is cyclic.  $\square$

**Theorem.** (*primitive element*) *Let  $E/F$  be a finite separable extension. Then there is some  $\alpha \in E$  such that  $E = F(\alpha)$ .*

*Proof.* We first assume that  $F$  is finite and hence  $E$  is finite. Then the multiplicative group  $E^*$  is cyclic and there is an element  $\alpha \in E$  that generates  $E^*$  and hence also generates  $E$  as a field extension of  $F$ .

Now we look at the case where  $F$  is infinite. Since  $E$  is finitely generated over  $F$  it suffices to show that for  $E = F(a, b)$  there is some  $\alpha$  that generates  $E$ . Let  $n = [E : F]$  be the degree and since  $E/F$  is separable there are  $n$  pairwise disjoint elements  $\sigma_1, \dots, \sigma_n$  in  $\text{Hom}_F(E, \overline{F})$ . Consider the polynomial

$$P = \prod_{i \neq j} ((\sigma_i(a) - \sigma_j(a)) + (\sigma_i(b) - \sigma_j(b))X).$$

The polynomial  $P \in \overline{F}[X]$  is nonzero because for any  $i \neq j$  there is either  $\sigma_i(a) \neq \sigma_j(a)$  or  $\sigma_i(b) \neq \sigma_j(b)$ . Since  $F$  is infinite and  $P$  has only finitely many roots there is some  $c \in F$  such that  $P(c) \neq 0$ . That implies that the elements

$$\sigma_i(a) + c\sigma_i(b) = \sigma_i(a + cb) \in \overline{F}$$

are pairwise disjoint. So the minimal polynomial  $f$  of  $a + cb$  has  $n$  different roots and is therefore of degree  $n$ . So  $\alpha = a + cb$  is a generator of  $E$  over  $F$ .  $\square$

**Lemma.** *Let  $E/F$  be a finite Galois extension. Then  $|Gal(E/F)| = [E : F]$ .*

*Proof.* We have that  $E = F(\alpha)$  for some  $\alpha \in E$ . For the minimal polynomial  $m_{\alpha,F}$  of  $\alpha$  we have that  $\deg(m_{\alpha,F}) = [E : F]$  and since  $\alpha$  is separable it has  $[E : F]$  different roots. Now any automorphism  $\sigma \in Gal(E/F)$  is uniquely determined by the value of  $\sigma(\alpha)$  which can be any of the roots of  $m_{\alpha,F}$ . So  $|Gal(E/F)| = \deg(m_{\alpha,F}) = [E : F]$ .  $\square$

The most important infinite Galois groups are the so called absolute Galois groups.

**Definition.** (a) Let  $F$  be a field. Then the field  $\tilde{F}$  of separable elements over  $F$  in  $\bar{F}$  is called the separable algebraic closure of  $F$ .

(b) The Galois group  $Gal(\tilde{F}/F)$  is called the absolute Galois group of  $F$ .

(c) If  $\tilde{F} = \bar{F}$  then  $F$  is called a perfect field.

**Lemma.** *Every field  $F$  of characteristic 0 is perfect.*

*Proof.* Let  $a$  be an arbitrary element in  $\bar{F}$  and  $m = X^n + c_{n-1}X^{n-1} + \dots + c_0 \in F[X]$  be its minimal polynomial. Since its formal derivative

$$m' = nX^{n-1} + (n-1)c_{n-1}X^{n-2} + \dots + c_1$$

is nonzero the element  $a$  cannot be a zero of  $m'$  and hence  $a$  is not a repeated root of  $m$ . So  $a$  is separable and  $F$  is perfect.  $\square$

We will see later that every finite field is also perfect. So the only case where inseparable extensions occur is the case of extensions of infinite fields with characteristic  $\neq 0$ .

## 2. FINITE FIELDS

We have seen above that any finite field  $F$  has a prime characteristic  $p$  and hence contains a subfield with  $p$  elements. Now we want to study finite fields and all their Galois extensions. At first we will define the so called Frobenius homomorphism.

**Definition.** Let  $F$  be a field with  $char(F) = p$ . Then the map

$$\begin{aligned} \varphi_p : F &\rightarrow F \\ x &\mapsto x^p \end{aligned}$$

is called the Frobenius map.

*Remark.* The Frobenius map is in fact a homomorphism because for any given  $x, y \in F$  we have

$$\varphi_p(xy) = (xy)^p = x^p y^p = \varphi_p(x)\varphi_p(y)$$

and

$$\begin{aligned} \varphi_p(x+y) &= (x+y)^p \\ &= x^p + \binom{p}{1}x^{p-1}y + \cdots + \binom{p}{p-1}xy^{p-1} + y^p \\ &= x^p + y^p = \varphi_p(x) + \varphi_p(y) \end{aligned}$$

where we used that for  $1 \leq k \leq p-1$  we have  $\binom{p}{k}$  is divisible by  $p$  and hence vanishes in  $F$ .

Now we can prove the following theorem.

**Theorem.** *For any power of a prime  $p^n$  there is a field with  $p^n$  elements and every two such fields are isomorphic to each other.*

*Proof.* Let  $\mathbb{F}_p$  be the field with  $p$  elements and  $f = X^{p^n} - X \in \mathbb{F}_p[X]$ . Then  $f' = -1$  and so  $f$  is separable. Hence  $f$  has  $p^n$  distinct roots  $\alpha_1, \dots, \alpha_{p^n}$  in  $\overline{\mathbb{F}_p}$  including all the elements in  $\mathbb{F}_p$ . Let  $\alpha$  and  $\beta$  be two of those roots. Then

$$\begin{aligned} f(\alpha - \beta) &= (\alpha - \beta)^{p^n} - (\alpha - \beta) \\ &= (\alpha^{p^n} - \beta^{p^n}) - (\alpha - \beta) \\ &= f(\alpha) - f(\beta) = 0 \end{aligned}$$

and

$$\begin{aligned} f(\alpha\beta^{-1}) &= (\alpha\beta^{-1})^{p^n} - \alpha\beta^{-1} \\ &= \alpha^{p^n}\beta^{-p^n} - \alpha\beta^{-1} \\ &= \alpha\beta^{-1} - \alpha\beta^{-1} = 0 \end{aligned}$$

So set of those roots forms a field  $\mathbb{F}_{p^n}$  with  $p^n$  elements that contains  $\mathbb{F}_p$  as a subfield.

Let  $E$  be a field with  $p^n$  elements. Then for every element  $a \in E^*$  we have  $a^{p^n-1} = 1$  and hence every element in  $E$  is a root of  $X^{p^n} - X$  in  $\overline{\mathbb{F}_p}$ . So  $E \cong \mathbb{F}_{p^n}$ .  $\square$

This explains the structure of finite fields. To fully understand these we can now determine the possible field extensions and the automorphism groups of the finite fields.

**Theorem.** *Let  $\mathbb{F}_{p^m}$  and  $\mathbb{F}_{p^n}$  be finite fields. Then  $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$  is a field extension if and only if  $m \mid n$ . In this case the extension is Galois and its Galois group  $G$  is cyclic with  $\frac{n}{m}$  elements and generated by the  $m$ -th power of the Frobenius homomorphism  $\varphi_p$ .*

*Proof.* If  $\mathbb{F}_{p^m}$  is a subfield of  $\mathbb{F}_{p^n}$  then  $\mathbb{F}_{p^n}$  is a vector field over  $\mathbb{F}_{p^m}$  and hence  $m \mid n$ . Conversely if  $m \mid n$  then the polynomial  $X^{p^m} - X$  divides  $X^{p^n} - X$  and so  $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$  is a field extension.

The extension is finite and hence algebraic. It is separable because  $\mathbb{F}_{p^n} = \mathbb{F}_{p^m}(\alpha)$  for a primitive root  $\alpha$  of  $X^{p^n-1} - 1$  and  $\alpha$  is separable. Finally it is normal because the polynomial  $X^{p^n} - X$  splits into linear factors and contains all the elements.

Clearly the Galois group  $G$  has  $[\mathbb{F}_{p^n} : \mathbb{F}_{p^m}] = \frac{n}{m}$  elements. Consider the relative Frobenius homomorphism

$$\begin{aligned} \varphi_{p^m} : \mathbb{F}_{p^n} &\rightarrow \mathbb{F}_{p^n} \\ a &\mapsto a^{p^m} \end{aligned}$$

which is an element of  $G$ . Then  $\varphi_{p^m}$  has some order  $d \leq \frac{n}{m}$ . Now  $d < \frac{n}{m}$  would imply  $a^{p^{md}} = a$  for every element  $a \in \mathbb{F}_{p^n}$  which is a contradiction. So  $d = \frac{n}{m}$  and hence  $\varphi_{p^m}$  generates the Galois group  $G$ .  $\square$

To close our discussion about finite fields we will now try to understand the algebraic closure of a finite field.

**Theorem.** *For  $\mathbb{F}_p$  the algebraic closure is given by  $\overline{\mathbb{F}_p} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$ .*

*Proof.* At first we show that  $\mathbb{F}_{p^\infty} = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{p^n}$  is a field. Let  $a$  and  $b$  be two of its elements. Then there are natural numbers  $m, n$  such that  $a \in \mathbb{F}_{p^m}$  and  $b \in \mathbb{F}_{p^n}$ . So  $a, b \in \mathbb{F}_{p^{mn}} \subset \mathbb{F}_{p^\infty}$  and hence  $a - b$  and  $ab^{-1}$  are in  $\mathbb{F}_{p^\infty}$ .

Now we have to show that  $\mathbb{F}_{p^\infty}$  is algebraically closed. Let  $f \in \mathbb{F}_{p^\infty}[X]$  be a polynomial. Then the coefficients of  $f$  lie in some  $\mathbb{F}_{p^k}$  and hence its roots lie in some finite extension of  $\mathbb{F}_{p^k}$ . So  $f$  splits in linear factors and hence  $\mathbb{F}_{p^\infty}$  is algebraically closed.  $\square$

As an immediate consequence we get the following

**Corollary.** *Every finite field  $\mathbb{F}_{p^n}$  is perfect.*

*Proof.* Every element  $a \in \overline{\mathbb{F}_p}$  is an element of some  $\mathbb{F}_{p^k}$  and is therefore separable. So  $\overline{\mathbb{F}_p}/\mathbb{F}_{p^n}$  is separable.  $\square$

### 3. THE FUNDAMENTAL THEOREM OF GALOIS THEORY

**Definition.** Let  $E/F$  be a Galois extension and  $G = \text{Gal}(E/F)$  be its Galois group. For any subgroup  $H$  of  $G$  denote the subfield of  $E$  that is fixed under  $H$  by

$$E^H = \{a \in E \mid \sigma(a) = a \forall \sigma \in H\}.$$

For finite Galois extensions  $E/F$  we can now characterize the intermediate fields using the following

**Theorem.** (*fundamental theorem of Galois theory*) *Let  $E/F$  be a Galois extension and  $G = \text{Gal}(E/F)$  be its Galois group. Consider the maps*

$$\begin{aligned} \alpha : \{H \leq G\} &\rightarrow \{K \mid F \leq K \leq E\} \\ H &\mapsto E^H \end{aligned}$$

and

$$\begin{aligned} \beta : \{K \mid F \leq K \leq E\} &\rightarrow \{H \leq G\} \\ K &\mapsto \text{Gal}(E/K) \end{aligned}$$

- (a) *Then  $\alpha \circ \beta = \text{id}$ . In particular  $\alpha$  is surjective and  $\beta$  is injective.*
- (b) *If  $E/F$  is finite then  $\alpha$  and  $\beta$  are bijective and  $\beta \circ \alpha = \text{id}$ .*
- (c) *Let  $K$  be an intermediate field of  $E/F$ . Then  $K/F$  is a normal extension if and only if  $H = \text{Gal}(E/K)$  is a normal subgroup of  $G$ .*

*Proof.* (a) Let  $K$  be an intermediate field of  $E/F$ . First we will prove that  $E/K$  is always Galois to see that  $H = \text{Aut}_K(E)$  is a Galois group. Since  $E/F$  is normal it is clear that  $E/K$  is also normal. To prove that  $E/K$  is separable consider an element  $a \in E$  and a maximal system of elements  $\sigma_1, \dots, \sigma_r \in H$  such that  $\sigma_1(a), \dots, \sigma_r(a)$  are pairwise different. Such a finite system always exists since  $a$  is algebraic over  $K$ .

Consider the polynomial

$$f = \prod_{i=1}^r (X - \sigma_i(a)).$$

Every  $\sigma \in H$  induces a bijective map from  $\{\sigma_1(a), \dots, \sigma_r(a)\}$  onto itself and hence the coefficients of  $f$  are all fixed under  $H$ . So  $f$  is a separable polynomial in  $K[X]$  with root  $a$ . So every  $a \in E$  is separable over  $K$  and hence  $E/K$  is Galois.

Now we have to show that  $E^H = K$ . By definition of  $E^H$  we immediately get that  $K$  is a subfield of  $E^H$ . Now assume  $K \neq E^H$ . Then there is some  $a \in E^H \setminus K$  with some minimal polynomial with degree at least 2. Since  $a \in E$  is separable over  $K$  there is some  $b \neq a$  and some  $\sigma \in H$  such that  $\sigma(a) = b$ . But that contradicts the fact that  $\alpha$  is fixed under  $H$ . So  $E^H = K$  and  $\alpha \circ \beta = id$ .

(b) Let  $H$  be a subgroup of  $G$  and  $K = E^H$  be the corresponding fixed field. Since  $E/F$  is finite so is  $G$  and hence  $H$  as a subgroup. So let  $n$  be the number of elements in  $H$ . Since  $E/K$  is finite and separable there is a primitive element  $a \in E$ . Then by the argument in (a) we have that  $[E : K] = [K(a) : K] \leq n = ord(H)$ . Since  $H$  fixes the elements in  $K$  it is a subgroup of  $Gal(E/K) = Aut_K(E)$ . But since

$$ord(Gal(E/K)) = [E : K] \leq n = ord(H)$$

we have that  $Gal(E/K) = H$  and hence  $\beta \circ \alpha = id$ .

(c) Let  $K/F = E^H/F$  be normal. Then the map

$$\begin{aligned} \varphi : G &\rightarrow Gal(E^H/F) \\ \sigma &\mapsto \sigma|_{E^H} \end{aligned}$$

is a surjective group homomorphism with  $\ker \varphi = H$ . So  $H$  is a normal subgroup of  $G$ .

Conversely let  $H$  be a normal subgroup. To show that  $K/F = E^H/F$  is normal we have to show that any  $F$ -homomorphism  $\sigma : E^H \rightarrow \bar{E}$  is mapped into  $E^H$ . Since  $E/F$  is normal we have that  $\sigma(E^H) \subseteq E$ . Now let  $b \in \sigma(E^H)$  and say  $\sigma(a) = b$ . Now let  $\tau \in H$ . Since  $H$  is normal there is some  $\tau' \in H$  such that  $\tau\sigma = \sigma\tau'$  and  $\tau(b) = \tau\sigma(a) = \sigma\tau'(a) = \sigma(a) = b$ . So  $b \in E^H$  and hence  $\sigma(E^H) \subseteq E^H$ .  $\square$

*Remark.* As an immediate consequence of (c) we get the following fact.

If  $E/F$  is a Galois extension and  $K$  be an intermediate field with  $K/F$  normal. Then the maps

$$\begin{aligned}\iota : Gal(E/K) &\rightarrow Gal(E/F) \\ \sigma &\mapsto \sigma\end{aligned}$$

and

$$\begin{aligned}\varphi : Gal(E/F) &\rightarrow Gal(K/F) \\ \sigma &\mapsto \sigma|_K\end{aligned}$$

are group homomorphisms and the sequence

$$1 \longrightarrow Gal(E/K) \xrightarrow{\iota} Gal(E/F) \xrightarrow{\varphi} Gal(K/F) \longrightarrow 1$$

is exact (i.e.  $\text{im } \iota = \ker \varphi$ ).

**Example.** For a field extension of finite fields  $\mathbb{F}_{p^n}/\mathbb{F}_{p^m}$  the fundamental theorem says that the intermediate fields  $\mathbb{F}_{p^k}$  with  $m \mid k \mid n$  correspond to the unique subgroup  $Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^k}) \cong \mathbb{Z}/\frac{n}{k}\mathbb{Z}$  of  $Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) \cong \mathbb{Z}/\frac{n}{m}\mathbb{Z}$ .

If  $E/F$  is infinite then  $\alpha$  is not injective in general. This can be seen in the following example.

**Example.** Let  $p \in \mathbb{N}$  be a prime and  $\mathbb{F}_p$  be the field with  $p$  elements. Then the extension  $\overline{\mathbb{F}_p}/\mathbb{F}_p$  is infinite. Its Galois group  $G = Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$  contains Frobenius automorphism

$$\begin{aligned}\varphi_p : \overline{\mathbb{F}_p} &\rightarrow \overline{\mathbb{F}_p} \\ x &\mapsto x^p.\end{aligned}$$

The only elements fixed by  $\varphi_p$  are those in  $\mathbb{F}_p$ . So  $\overline{\mathbb{F}_p}^{\langle \varphi_p \rangle} = \mathbb{F}_p = \overline{\mathbb{F}_p}^G$ . If  $\alpha$  was injective then we would get  $G = \langle \varphi_p \rangle$ . We will now construct an automorphism  $\psi \in G$  that is not a power of  $\varphi_p$ . Let  $(a_n)_{n \in \mathbb{N}}$  be a sequence of integers such that

$$a_n \equiv a_m \pmod{m}$$

holds if  $m \mid n$  and such that for any  $a \in \mathbb{Z}$  there is some  $n \in \mathbb{N}$  with  $a_n \not\equiv a \pmod{n}$ . For example we can write  $n = n'p^{v_p(n)}$  with  $\gcd(n', p) = 1$ . Then there are some integers  $x_n, y_n$  such that  $1 = n'x_n + p^{v_p(n)}y_n$ . Now the sequence  $a_n = n'x_n$  fulfills the above conditions. Now let

$$\psi_n = \varphi^{a_n}|_{\mathbb{F}_{p^n}} \in Gal(\mathbb{F}_{p^n}/\mathbb{F}_p).$$

If  $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$  then  $m \mid n$  and therefore

$$\psi_n|_{\mathbb{F}_{p^m}} = \varphi^{a_n}|_{\mathbb{F}_{p^m}} = \varphi^{a_m}|_{\mathbb{F}_{p^m}} = \psi_m.$$

So the sequence  $(\psi_n)_{n \in \mathbb{N}}$  defines an automorphism  $\psi$  on  $\overline{\mathbb{F}_p}$ . But  $\psi$  is not a power of  $\varphi$  since otherwise we would have that  $\psi = \varphi^a$  for some  $a \in \mathbb{Z}$  and hence

$$\varphi^{a_n}|_{\mathbb{F}_{p^n}} = \psi_n = \psi|_{\mathbb{F}_{p^n}} = \varphi^a|_{\mathbb{F}_{p^n}}$$

and so  $a_n \equiv a \pmod{n}$  for every  $n \in \mathbb{N}$  which was outruled by construction.

In order to get an infinite analogue to the fundamental theorem we will have to define a topology on our Galois group.

#### 4. THE KRULL TOPOLOGY

**Definition.** A topological group  $G$  is a group which is also a topological space such that the group operation  $\circ$  and the inverse mapping  $\cdot^{-1}$  are continuous functions on  $G$ .

**Lemma.** *Let  $G$  be a topological group.*

(a) *If  $H$  is an open subgroup of  $G$  then  $H$  is closed.*

(b) *If  $H$  is closed and of finite index (i.e.  $|G/H|$  is finite) then  $H$  is open.*

*Proof.* (a) If  $H$  is open so are all the left cosets  $gH$  for  $g \in G$ . Hence  $G \setminus H = \bigcup_{g \notin H} gH$  is open and hence  $H$  is closed.

(b) If  $H$  is closed so are all the left cosets  $gH$  for  $g \in G$ . Since  $H$  is of finite index there are only finitely many left cosets. Hence  $G \setminus H = \bigcup_{g \notin H} gH$  is closed and hence  $H$  is open.  $\square$

**Example.** (a) Any group  $G$  together with the discrete topology (i.e. every subset of  $G$  is open) is a topological group.

(b) Any group  $G$  together with the trivial topology (i.e. only  $\emptyset$  and  $G$  are open) is a topological group.

(c) Every Lie group is a topological group. For example the groups of matrices  $GL_n(\mathbb{R})$ ,  $GL_n(\mathbb{C})$ ,  $O(n)$ ,  $SO(n)$  or  $SU(n)$  are Lie groups and therefore topological groups.

**Definition.** Let  $E/F$  be a Galois extension and  $G = Gal(E/F)$ . For  $\sigma \in G$  we define a neighborhood basis of  $\sigma$  via the sets  $\sigma Gal(E/K)$

where  $K/F$  runs through all finite Galois extensions of  $F$  in  $E$ . This induces a topology on  $G$ , the so called Krull topology.

**Lemma.** *Let  $E/F$  be a Galois extension and  $G = \text{Gal}(E/F)$ . Then the Krull topology makes  $G$  a topological group.*

*Proof.* To prove continuity of the multiplication we have to show that for any elements  $\sigma, \tau \in G$  and for any neighborhood  $W$  in the neighborhood basis of  $\sigma\tau$  there are neighborhoods  $U$  and  $V$  of  $\sigma$  and  $\tau$  respectively such that

$$U \cdot V \subseteq W.$$

So let  $K/F$  be a finite Galois extension and  $W = \sigma\tau\text{Gal}(E/K)$ . Then for  $U = \sigma\text{Gal}(E/K)$  and  $V = \tau\text{Gal}(E/K)$  we have that  $U \cdot V = W$ .

Similarly to prove continuity of the inverse function we observe that for any  $\sigma \in G$  and for  $W = \sigma^{-1}\text{Gal}(E/K)$  there is  $U = \sigma\text{Gal}(E/K)$  such that  $U^{-1} = W$ . So  $G$  is a topological group.  $\square$

*Remark.* (a) If  $E/F$  is finite then for every  $\sigma \in \text{Gal}(E/F)$  the set  $\{\sigma\} = \sigma\text{Gal}(E/E)$  is open. So in this case the Krull topology is just the discrete topology on  $\text{Gal}(E/F)$ .

(b) Let  $\mathfrak{K} = (K_i)_{i \in I}$  be the set of all finite extensions  $K_i/F$  lying in  $E$ . Let  $f_i : \text{Gal}(E/F) \rightarrow \text{Gal}(K_i/F)$  be restriction mappings. Then the Krull topology on  $\text{Gal}(E/F)$  is the coarsest topology such that all  $f_i$  are continuous if we consider the discrete topology for  $\text{Gal}(K_i/F)$ .

*Proof.* (of (b)) In any topology on  $\text{Gal}(E/F)$  where all  $f_i$  are continuous, the sets  $\sigma\text{Gal}(E/K_i) = f_i^{-1}(\sigma)$  are open. Since the Krull topology is defined by these sets, it is the coarsest such topology.  $\square$

**Proposition.** *Any Galois group  $G = \text{Gal}(E/F)$  is Hausdorff, compact and totally disconnected.*

*Proof.* To prove that  $G$  is Hausdorff let  $\sigma$  and  $\tau$  be two different elements in  $G$ . Then there is some finite Galois extension  $K/F$  such that  $\sigma|_K \neq \tau|_K$ . Then  $\sigma\text{Gal}(E/K) \neq \tau\text{Gal}(E/K)$  and since these are cosets of  $\text{Gal}(E/K)$  they are disjoint.

The restriction  $f_i : \text{Gal}(E/F) \rightarrow \text{Gal}(K_i/F)$  induces an injective continuous homomorphism

$$f : \text{Gal}(E/F) \rightarrow \prod_{i \in I} \text{Gal}(K_i/F)$$

which we can understand as an inclusion. The set  $\prod_{i \in I} Gal(K_i/F)$  is a product of finite discrete and hence compact topological spaces. The theorem of Tychonoff then guarantees that the product is compact itself. So to show that  $Gal(E/F)$  is compact we only have to prove that it is closed in the product space  $\prod_{i \in I} Gal(K_i/F)$ . To do so consider a point  $(\sigma_i)_{i \in I} \in \prod_{i \in I} Gal(K_i/F)$  which is not a point in  $Gal(E/F)$ . Then there are some indices  $j, k \in I$  such that  $K_j \subseteq K_k$  but  $\sigma_k|_{K_j} \neq \sigma_j$ . Then the set  $\{(\sigma'_i)_{i \in I} \in \prod_{i \in I} Gal(K_i/F) \mid \sigma'_j = \sigma_j, \sigma'_k = \sigma_k\}$  is an open neighborhood of  $(\sigma_i)_{i \in I}$  which is disjoint to  $Gal(E/F)$ . So  $Gal(E/F)$  is closed and hence compact.

To see that  $Gal(E/F)$  is totally disconnected, let  $(\sigma_i)_{i \in I}$  and  $(\sigma'_i)_{i \in I}$  be two different elements of  $\prod_{i \in I} Gal(K_i/F)$ . Then there is an index  $j \in I$  such that  $\sigma_j \neq \sigma'_j$ . Then define open sets  $V = \prod_{i \in I} V_i$  and  $V' = \prod_{i \in I} V'_i$  in  $\prod_{i \in I} Gal(K_i/F)$  via

$$V_i = \begin{cases} Gal(K_i/F) & i \neq j \\ \{\sigma_j\} & i = j \end{cases}$$

and

$$V'_i = \begin{cases} Gal(K_i/F) & i \neq j \\ Gal(K_j/F) \setminus \{\sigma_j\} & i = j \end{cases}.$$

Then  $(\sigma_i)_{i \in I} \in V$ ,  $(\sigma'_i)_{i \in I} \in V'$  and  $\prod_{i \in I} Gal(K_i/F)$  is the disjoint union of  $V$  and  $V'$ . So  $\prod_{i \in I} Gal(K_i/F)$  is totally disconnected.  $\square$

## 5. THE PROJECTIVE LIMIT AND PROFINITE GROUPS

To understand infinite Galois groups it is of advantage to see them as a projective limits of finite Galois groups. Hence the following definition.

**Definition.** Let  $(I, \leq)$  be a partially ordered set such that for any  $i, j \in I$  there is some  $k \in I$  that satisfies  $i, j \leq k$ . Let  $(G_i)_{i \in I}$  be a family of topological groups and for any  $i \leq j$  let  $f_{ij} : G_j \rightarrow G_i$  be a continuous homomorphism satisfying

$$f_{ii} = id \quad \forall i \in I$$

and

$$f_{ik} = f_{ij} \circ f_{jk} \quad \forall i \leq j \leq k.$$

Then we define the projective limit of  $((G_i)_{i \in I}, (f_{ij})_{i, j \in I, i \leq j})$  as the subgroup

$$G = \varprojlim_{i \in I} G_i = \{(g_i)_{i \in I} \in \prod_{i \in I} G_i \mid f_{ij}(g_j) = g_i \forall i, j \in I\}$$

of the direct product of the groups  $G_i$  together with the natural projections  $f_i : G \rightarrow G_i$ . The topology on  $G$  is then defined to be the coarsest topology such that all projections  $f_i$  are continuous.

**Theorem.** *Let  $E/F$  be a Galois extension and  $(K_i)_{i \in I}$  be the set of fields  $K_i \leq E$  which are finite Galois extensions of  $F$ . Define  $G = \text{Gal}(E/F)$ ,  $G_i = \text{Gal}(K_i/F)$  and for any  $K_i \leq K_j$  define*

$$\begin{aligned} f_{ij} : G_j &\rightarrow G_i \\ \sigma &\mapsto \sigma|_{K_i}. \end{aligned}$$

*Then  $G$  is isomorphic to the projective limit of  $((G_i)_{i \in I}, (f_{ij})_{i, j \in I, i \leq j})$  with the projections  $f_i(\sigma) = \sigma|_{K_i}$ .*

*Proof.* We will show that the map

$$\begin{aligned} \varphi : G &\rightarrow \varprojlim_{i \in I} \text{Gal}(K_i/F) \\ \sigma &\mapsto (\sigma|_{K_i})_{i \in I} \end{aligned}$$

is an isomorphism of topological groups.

Let  $\sigma, \tau \in G$  with  $\sigma \neq \tau$ . Then there is some finite extension  $K_i$  such that  $\sigma|_{K_i} \neq \tau|_{K_i}$  and so  $\varphi$  is injective. The map  $\varphi$  is surjective by definition of the projective limit. It is a group homomorphism by construction and the topology is the same since the Krull topology on  $G$  is the coarsest topology such that  $\varphi$  is continuous.  $\square$

In general a topological group is called profinite if it is an inverse limit of discrete finite groups or equivalent if it is Hausdorff, compact and there is a neighborhood basis of 1 that consists of normal subgroups. So all Galois groups are profinite groups. In fact it can be proved that any profinite group is a Galois group.<sup>2</sup>

---

<sup>2</sup>For further information on profinite groups see [5, p.278ff].

6. THE FUNDAMENTAL THEOREM FOR INFINITE GALOIS  
EXTENSIONS

With the Krull topology we can now generalize Galois' theorem. For the proof we will need the following

**Lemma.** *Let  $E/F$  be a Galois extension,  $H \leq \text{Gal}(E/F)$  be a subgroup. Then  $\text{Gal}(E/E^H) = \overline{H}$ .*

*Proof.* By definition of  $E^H$  the group  $H$  is a subgroup of  $\text{Gal}(E/E^H)$ . Let  $(K_i)_{i \in I}$  be the family of intermediate fields of  $E^H/F$  such that  $K_i/F$  is finite and Galois. Since  $\text{Gal}(E/K_i)$  is an open subgroup of  $\text{Gal}(E/F)$  it is also closed and so the Galois group  $\text{Gal}(E/E^H) = \bigcap_{i \in I} \text{Gal}(E/K_i)$  is closed as well. It remains to show that  $H$  is dense in  $\text{Gal}(E/E^H)$ . To do so let  $\sigma \in \text{Gal}(E/E^H)$ . Then any neighborhood of  $\sigma$  contains some  $\sigma \text{Gal}(E/K)$  where  $K = K_i$  for some  $i \in I$ . We have to prove that there is some  $\tau \in H \cap \sigma \text{Gal}(E/K)$  which is equivalent to  $\tau|_K = \sigma|_K$ . Now let  $H_K = \{h|_K \in \text{Gal}(K/F) : h \in H\}$ . Then by the Galois theorem for finite extensions  $H_K = \text{Gal}(K/K^{H_K})$  and so  $\sigma|_K \in H_K$ . Hence the required  $\tau$  exists and  $H$  is dense in  $\text{Gal}(E/E^H)$ .  $\square$

**Theorem.** *Let  $E/F$  be a Galois extension and  $G = \text{Gal}(E/F)$ . Consider the maps*

$$\begin{aligned} \alpha : \{H \leq G : H = \overline{H}\} &\rightarrow \{K : F \leq K \leq E\} \\ H &\mapsto E^H \end{aligned}$$

and

$$\begin{aligned} \beta : \{K : F \leq K \leq E\} &\rightarrow \{H \leq G : H = \overline{H}\} \\ K &\mapsto \text{Gal}(E/K) \end{aligned}$$

Then  $\alpha$  and  $\beta$  are bijective and inverse to each other.

Additionally if  $H$  is open then  $E^H/F$  is finite and  $H$  is also closed and vice versa.

*Proof.* The first statement is an immediate consequence of the classical Galois theorem and the lemma above.

Now let  $H$  be an open subgroup of  $G$  and hence also a closed subgroup by the lemma in section 4. Furthermore  $H$  contains an open neighborhood of the identity. So there is some field  $K$  such that  $K/F$  is finite and  $\text{Gal}(E/K)$  is a subgroup of  $H$ . So  $E^H$  is some subfield of  $K$  and therefore  $E^H/F$  is finite.

Conversely if  $E^H/F$  is finite and  $H$  is closed then  $H$  is of finite index in  $G$  and hence open.  $\square$

## 7. EXAMPLES FOR INFINITE GALOIS GROUPS

The easiest example for infinite Galois groups is the absolute Galois group of a finite field  $\mathbb{F}_{p^n}$ .

Since  $\mathbb{F}_{p^n}$  is algebraic over  $\mathbb{F}_p$  and a perfect field, its separable closure is just the algebraic closure  $\overline{\mathbb{F}_p}$ . The finite field extensions of  $\mathbb{F}_{p^n}$  are the fields  $\mathbb{F}_{p^{mn}}$  for  $m \in \mathbb{N}$ .

Let  $G = \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_{p^n})$  and  $G_m = \text{Gal}(\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n}) \cong \mathbb{Z}/m\mathbb{Z}$ . So  $G = \varprojlim_{m \in \mathbb{N}} G_m \cong \varprojlim_{m \in \mathbb{N}} (\mathbb{Z}/m\mathbb{Z})$ . This projective limit then has the additive structure of the so called Prüfer ring

$$\begin{aligned} \hat{\mathbb{Z}} &= \varprojlim_{m \in \mathbb{N}} (\mathbb{Z}/m\mathbb{Z}) \\ &= \{(a_m)_{m \in \mathbb{N}} \in \prod_{m \in \mathbb{N}} (\mathbb{Z}/m\mathbb{Z}) \mid a_k \equiv a_m \pmod{k} \forall k \mid m\} \end{aligned}$$

with ordinary addition  $(a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}} = (a_n + b_n)_{n \in \mathbb{N}}$  and multiplication  $(a_n)_{n \in \mathbb{N}} \cdot (b_n)_{n \in \mathbb{N}} = (a_n b_n)_{n \in \mathbb{N}}$ . In particular  $G \cong \hat{\mathbb{Z}}$  is abelian and hence any Galois group over a finite field is abelian. Furthermore any subgroup of  $G$  is normal and hence every extension is normal.

For a better understanding of the absolute Galois group  $G$  we will state some important properties of  $\hat{\mathbb{Z}}$ .

*Remark.* The canonical ring homomorphism

$$\begin{aligned} \psi : \mathbb{Z} &\rightarrow \hat{\mathbb{Z}} \\ a &\mapsto (a)_{n \in \mathbb{N}} \end{aligned}$$

is injective and hence  $\mathbb{Z}$  can be seen as a subring of  $\hat{\mathbb{Z}}$ .

In terms of the Galois group the subgroup corresponding to  $\mathbb{Z}$  is the subgroup  $H$  of  $G$  generated by the Frobenius automorphism  $\varphi_{p^n}$  which appears as the element  $(1)_{n \in \mathbb{N}}$  in  $\hat{\mathbb{Z}}$ . However as we have seen in section

3 there are elements in  $\psi \in G$  that are not in  $H$ . But as topological groups we get  $\overline{H} = G$  (i.e.  $H$  is dense in  $G$ ).

Now we analyze the structure of  $\hat{\mathbb{Z}}$  by the following theorem.

**Theorem.** *Let  $q$  be a prime and  $\mathbb{Z}_q = \varprojlim_{k \in \mathbb{N}} (\mathbb{Z}/q^k \mathbb{Z})$  be the so called  $q$ -adic integers. Then*

$$\hat{\mathbb{Z}} \cong \prod_q \mathbb{Z}_q$$

*as topological rings.*

*Proof.* We will show that  $\prod_q \mathbb{Z}_q$ , together with some canonical homomorphisms  $f_i : \prod_q \mathbb{Z}_q \rightarrow \mathbb{Z}/i\mathbb{Z}$ , fulfills the properties of a projective limit of the system  $(\mathbb{Z}/i\mathbb{Z})_{i \in \mathbb{N}^+}$ . Let  $i \in \mathbb{N} \setminus \{0\}$  be an arbitrary positive integer with prime factorization  $i = \prod_q q^{v_q(i)}$ . By the Chinese remainder theorem there is a canonical isomorphism

$$\mathbb{Z}/i\mathbb{Z} \xrightarrow{\sim} \prod_q \mathbb{Z}/q^{v_q(i)}\mathbb{Z}.$$

So the natural projections  $p_i : \prod_q \mathbb{Z}_q \rightarrow \prod_q \mathbb{Z}/q^{v_q(i)}\mathbb{Z}$  correspond to homomorphisms

$$f_i : \prod_q \mathbb{Z}_q \rightarrow \mathbb{Z}/i\mathbb{Z}.$$

If  $i \mid j$  then those homomorphisms  $f_i$  match with the projections  $f_{ij} : \mathbb{Z}/j\mathbb{Z} \rightarrow \mathbb{Z}/i\mathbb{Z}$ . By definition of  $f_i$  the topology of  $\prod_q \mathbb{Z}_q$  is the coarsest topology such that all  $f_i$  are continuous.

To show that  $(\prod_q \mathbb{Z}_q, f_i)$  is a projective limit of  $(\mathbb{Z}/i\mathbb{Z}, f_{ij})$  as rings we choose a ring  $R$  with homomorphisms  $h_i : R \rightarrow \mathbb{Z}/i\mathbb{Z}$ , which match with the maps  $f_{ij}$ . For every prime  $q$  we then get homomorphisms  $h_{i,q} : R \rightarrow \mathbb{Z}/q^{v_q(i)}\mathbb{Z}$ . So there are homomorphisms  $h_q : R \rightarrow \varprojlim_{v \in \mathbb{N}} \mathbb{Z}/q^v \mathbb{Z}$  and altogether we get a ring homomorphisms  $h : R \rightarrow \prod_q \mathbb{Z}_q$  with  $h_i = f_i \circ h$ . So  $\prod_q \mathbb{Z}_q$  is a projective limit of  $\mathbb{Z}/i\mathbb{Z}$  and hence  $\prod_q \mathbb{Z}_q$  is isomorphic to  $\hat{\mathbb{Z}}$ .  $\square$

For the elements  $a = (\tilde{a}_k)_{k \in \mathbb{N}}$  of  $\mathbb{Z}_q$  we have  $\tilde{a}_k \equiv \tilde{a}_m \pmod{k}$  for all  $k \leq m$  and hence we can also write them as power series

$$a = \sum_{k \in \mathbb{N}} a_k q^k$$

where  $\sum_{k=0}^m a_k q^k = \tilde{a}_m$  and  $a_k \in \{0, \dots, p-1\}$ . Now we can define a norm on  $\mathbb{Z}_q$  by

$$|a|_q = \begin{cases} q^{-v_q(a)} & a \neq 0 \\ 0 & a = 0 \end{cases}$$

where  $v_q(a)$  denotes the smallest  $k$  such that  $a_k$  is nonzero. This norm then induces the same topology on  $\mathbb{Z}_q$  as the projective limit does.

With this preparation we can now find closed subgroups of  $\hat{\mathbb{Z}}$  by finding closed subgroups of  $\mathbb{Z}_q$ .

**Lemma.** *For any  $k \in \mathbb{N} \cup \{\infty\}$  the sets*

$$H_k = \{a \in \mathbb{Z}_q \mid |a|_q \leq q^{-k}\} = \{a \in \mathbb{Z}_q \mid a = \sum_{l=k}^{\infty} a_l q^l\}$$

are closed subgroups of  $\mathbb{Z}_q$  with

$$|\mathbb{Z}_q/H_k| = q^k.$$

Conversely if  $H$  is a closed subgroup of  $\mathbb{Z}_q$  then there is some  $k \in \mathbb{N} \cup \{\infty\}$  such that

$$H = H_k.$$

*Proof.* By the power series representation of the elements of  $H_k$  one can easily see that  $H_k$  is a closed subgroup in  $\mathbb{Z}_q$  with  $|\mathbb{Z}_q/H_k| = q^k$ .

Now let  $H$  be a closed subgroup of  $\mathbb{Z}_q$ . Since the values of the norm are discrete and bounded above by 1 there is some  $a \in H$  with maximal norm  $|a| = q^{-k}$ . We will now show that the closure of the group generated by  $a$  is  $H_k$ . To do so we have to show that for any element  $b \in H_k$  and every  $m \in \mathbb{N}$ ,  $m \geq k$  there is some  $n \in \mathbb{Z}$  such that  $|an - b|_q \leq q^{-m}$ . Let  $a_{m,k} = \sum_{l=k}^{m-1} a_l q^{l-k}$  and  $b_{m,k} = \sum_{l=k}^{m-1} b_l q^{l-k}$ . We have to choose  $n$  such that

$$an \equiv b \pmod{q^m},$$

which can be reduced to

$$a_{m,k}n \equiv b_{m,k} \pmod{q^{m-k}}.$$

Since  $a_{m,k} \not\equiv 0 \pmod{q}$  the number  $n$  can be chosen as required. So  $H_k$  is generated by  $a$  and hence  $H_k$  is a subgroup of  $H$ . Now we get  $H_k = H$  because  $a$  has maximal norm in  $H$ .  $\square$

Let  $k_q \in \mathbb{N} \cup \{\infty\}$  and define  $H_{q,k_q}$  as the closed subgroup of  $\mathbb{Z}_q$  of index  $q^{k_q}$ . Then the Cartesian product  $\prod_q H_{q,k_q}$  is a closed subgroup of  $\hat{\mathbb{Z}}$  and we denote it as  $\prod_q q^{k_q} \hat{\mathbb{Z}}$ .

If all  $k_q$  are finite and almost all of them are zero then  $m := \prod_q q^{k_q}$  is finite and we get that

$$|\hat{\mathbb{Z}}/m\hat{\mathbb{Z}}| = m$$

and hence  $m\hat{\mathbb{Z}}$  is an open subgroup of  $\hat{\mathbb{Z}}$ . By the fundamental theorem it correspond to the finite field  $\mathbb{F}_{p^{mn}}$ .

Otherwise  $\prod_q q^{k_q} \hat{\mathbb{Z}}$  is not open and corresponds to the infinite field given by

$$\mathbb{F}_{p^{n \prod q^{k_q}}} = \bigcup_{l_q \leq k_q, m = \prod l_q} \mathbb{F}_{p^{mn}}.$$

For example the subgroup  $2^\infty \hat{\mathbb{Z}}$  corresponds to

$$\mathbb{F}_{p^{n2^\infty}} = \bigcup_{l \in \mathbb{N}} \mathbb{F}_{p^{n2^l}}.$$

For the field  $\mathbb{Q}$  the determination of the absolute Galois group is much more complicated. The Galois group  $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$  is still not very well understood. For example there is still no proof for the following inverse Galois theorem.

**Conjecture.** (*inverse Galois problem*) *Let  $G$  be a finite group. Then there is a field extension  $F/\mathbb{Q}$  such that  $Gal(F/\mathbb{Q}) \cong G$ .*

For abelian extensions of  $\mathbb{Q}$  however (i.e.  $Gal(K/\mathbb{Q})$  is abelian) Kummer theory gives a complete description of the Galois groups. The basic result is the following

**Theorem.** (*Kronecker-Weber*) *Let  $K/\mathbb{Q}$  be a finite abelian Galois extension. Then there is some root of unity  $\zeta$  such that  $K$  is a subfield of  $\mathbb{Q}(\zeta)$ .<sup>3</sup>*

This theorem allows us to fully understand the Galois group  $Gal(\mathbb{Q}^{ab}/\mathbb{Q})$  where  $\mathbb{Q}^{ab}$  denotes the maximal abelian Galois extension of  $\mathbb{Q}$ . To do so we need an easy lemma.

**Lemma.** *Let  $\zeta$  be a primitive  $n$ -th root of unity in  $\overline{\mathbb{Q}}$ . Then the extension  $\mathbb{Q}(\zeta)/\mathbb{Q}$  is Galois and its Galois group is given by*

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$$

<sup>3</sup>A proof can be found in [4, p.253ff] or [5, p.341].

*Proof.* Any automorphism  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  is uniquely determined by the value  $\sigma(\zeta)$  which also has to be a primitive  $n$ -th root  $\zeta_n^k$  with  $\gcd(k, n) = 1$ . Furthermore for any two automorphisms  $\sigma$  and  $\tau$  we have  $(\sigma \circ \tau)(\zeta) = \sigma(\zeta)\tau(\zeta)$ . Hence  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ .  $\square$

Now the Galois group  $\text{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$  is isomorphic to the projective limit  $\hat{\mathbb{Z}}^* = \varprojlim_{n \in \mathbb{N}} (\mathbb{Z}/n\mathbb{Z})^*$ .

#### REFERENCES

- [1] BOSCH, S.: Algebra. Springer, Berlin-Heidelberg-New York, 4th Ed. 2001
- [2] JANTZEN, J.C., SCHWERMER, J.: Algebra. Springer, Berlin-Heidelberg-New York 2006
- [3] LANG, S.: Algebra. Springer, New York, 3rd Ed. 2002
- [4] LEUTBECHER, A.: Zahlentheorie. Springer, Berlin-Heidelberg-New York 1996
- [5] NEUKIRCH, J.: Algebraische Zahlentheorie. Springer, Berlin-Heidelberg-New York 1992
- [6] WEINTRAUB, S.H.: Galois Theory. Springer, New York 2006