

# SHORT NOTES ON GENERAL KUMMER THEORY

## 1. PRELIMINARIES

**Goal:** given a field  $K$  and a non-zero natural number  $n$ , characterize all Galois extensions of  $K$  whose Galois group is abelian with exponent  $d \mid n$ .

**Language:** by *abelian* extension we mean a Galois extension  $L/K$  with abelian Galois group; by *cyclic* extension we mean a Galois extension  $L/K$  with cyclic Galois group.

**Reference:** [Bos18, §4.10].

## 2. SETTING

- (1) Let  $K$  be a field and fix a separable closure  $K_s$ .
- (2) Let  $n \in \mathbb{N}$  be a non-zero natural number.
- (3) Let  $G := \text{Gal}(K_s/K)$  be the absolute Galois group.
- (4) Let  $A$  be an abelian group endowed with the discrete topology and a continuous action of  $G$  on  $A$  via group automorphisms, which we will denote by  $\sigma \cdot a =: \sigma(a)$ .
- (5) For each intermediate field  $K \subseteq L \subseteq K_s$  we denote

$$A_L := \{a \in A \mid \sigma(a) = a \text{ for all } \sigma \in \text{Gal}(K_s/L)\}.$$

- (6) Let  $\varphi: A \rightarrow A$  be a  $G$ -equivariant surjective homomorphism whose kernel, denoted  $\mu_n$ , is a cyclic subgroup of order  $n$  of  $A_K$ .

Continuity of the action of  $G$  on  $A$  ensures that for all  $a \in A$  we have

$$G(A/a) := \{\sigma \in G \mid \sigma(a) = a\} \hookrightarrow G.$$

Hence  $G(A/a)$  is also closed in  $G$  and corresponds to an intermediate field  $K \subseteq K_s^{G(A/a)} \subseteq K_s$  [Bos18, 4.2/3], let's denote it  $K(a)$ .

**Lemma 1.** *The intermediate field  $K(a)$  is a finite extension of  $K$ .*

*Proof.* Let  $\{L_i\}_{i \in I}$  be the directed system of all subfields of  $K_s$  which are finite field extensions of  $K$ . For each  $i \in I$ , let us denote by

$$f_i: G \rightarrow \text{Gal}(L_i/K)$$

the restriction morphism. The topology in  $G$  is the coarsest one making all the  $f_i$  continuous. Since each  $\text{Gal}(L_i/K)$  is a finite group, endowed with the discrete topology, it follows that the topology on  $G$  should be the smallest topology in which all fibres of the morphisms  $f_i$  are open. But the fibres of all the  $f_i$  already form a basis for some topology on  $G$ , so the topology on  $G$  can be explicitly described in terms of this basis.

Since  $G(A/a)$  is open and  $\text{id}_{K_s} \in G(A/a)$ , there is some  $i \in I$  such that

$$f_i^{-1}(f_i(\text{id}_{K_s})) = \text{Gal}(K_s/L_i) \subseteq G(A/a).$$

From Galois correspondence we deduce now that

$$K \subseteq K(a) \subseteq L_i,$$

hence  $K(a)$  is also finite over  $K$ . □

More generally, given a subset  $\Delta \subseteq A$  we may consider the subgroup

$$G(A/\Delta) := \{\sigma \in G \mid \sigma(a) = a \text{ for all } a \in \Delta\} = \cap_{a \in \Delta} G(A/a),$$

which is then a closed subgroup but not necessarily an open subgroup. In any case we obtain an intermediate field  $K \subseteq K_s^{G(A/\Delta)} \subseteq K_s$ , which we will denote by  $K(\Delta)$ .

If  $L/K$  is Galois, then the action of  $G$  on  $A$  restricts to an action of  $G$  on  $A_L$ . Indeed, let  $\tau \in G$ ,  $\sigma \in \text{Gal}(K_s/L)$  and  $a \in A_L$ . Since  $\text{Gal}(K_s/L) \trianglelefteq G$ , there is some  $\sigma' \in \text{Gal}(K_s/L)$  such that

$$\sigma\tau(a) = \tau\sigma'(a) = \tau(a),$$

hence  $\tau(a) \in A_L$ . And by definition  $\text{Gal}(K_s/L)$  acts trivially on  $A_L$ , so we get an induced action of  $G/\text{Gal}(K_s/L)$  on  $A_L$ . Using again that  $L/K$  is Galois, we may identify this quotient group with  $\text{Gal}(L/K)$ , obtaining an action of  $\text{Gal}(L/K)$  on  $A_L$ . We can then talk about the cohomology group  $H^1(\text{Gal}(L/K), A_L)$ . A function  $f: \text{Gal}(L/K) \rightarrow A_L$  is called a *crossed homomorphism* if for all  $\sigma, \tau \in \text{Gal}(L/K)$  we have

$$f(\sigma\tau) = f(\sigma) + \sigma(f(\tau)).$$

A function  $f: \text{Gal}(L/K) \rightarrow A_L$  is called a *principal crossed homomorphism* if there exists some  $a \in A_L$  such that for all  $\sigma \in \text{Gal}(L/K)$  we have

$$f(\sigma) = \sigma(a) - a.$$

Principal crossed homomorphisms form a subgroup of the group of crossed homomorphisms, and the quotient group is then our first cohomology group  $H^1(\text{Gal}(L/K), A_L)$ .

We are ready now to state the main assumption on which we will rely:

**Axiom 2.** *For every cyclic extension  $L/K$  whose degree divides  $n$  we have*

$$H^1(\text{Gal}(L/K), A_L) = 0.$$

### 3. THE PAIRING ASSOCIATED TO A SUBGROUP

Let  $C \subseteq A_K$  be a subgroup and consider  $\wp^{-1}(C) \subseteq A$ . By  $G$ -equivariance of  $\wp$  and our assumption that  $C \subseteq A_K$ , any  $\sigma \in G$  restricts to a homomorphism  $\sigma: \wp^{-1}(C) \rightarrow \wp^{-1}(C)$ . If  $\sigma(a) = 0$  for  $a \in \wp^{-1}(C)$ , then

$$\wp(\sigma(a)) = \sigma(\wp(a)) = \wp(a) = 0,$$

because  $\wp(a) \in C \subseteq A_K$ . Therefore  $a \in \mu_n \subseteq A_K$ , and this implies in turn that  $\sigma(a) = a = 0$ . So the restriction of  $\sigma$  is an injective homomorphism  $\wp^{-1}(C) \rightarrow \wp^{-1}(C)$ . For  $a \in \wp^{-1}(C)$  we have

$$\sigma(a) - a \in \mu_n$$

again by  $G$ -equivariance of  $\wp$  and our assumption that  $C \subseteq A_K$ . So if  $\sigma(a) \in \wp^{-1}(C)$ , then

$$\wp(\sigma(a)) = \wp(a) \in C$$

and  $a \in \wp^{-1}(C)$  as well, showing that the restriction of  $\sigma$  is also surjective. Hence  $\sigma$  restricts to a bijection  $\wp^{-1}(C) \rightarrow \wp^{-1}(C)$ . We obtain in this manner a group homomorphism

$$G \rightarrow \text{Aut}(\wp^{-1}(C)).$$

The kernel of this group homomorphism is  $G(A/\wp^{-1}(C))$  by definition. It is therefore a normal subgroup of  $G$ , which means in turn that  $K(\wp^{-1}(C))/K$  is a Galois extension with Galois group  $G_C \cong G/G(A/\wp^{-1}(C))$ . In particular, we also obtain an induced action of the Galois group  $G_C$  on  $\wp^{-1}(C)$ .

We define now a pairing

$$\begin{aligned} G_C \times C &\longrightarrow \mu_n \\ (\sigma, c) &\longmapsto \sigma(a) - a, \text{ for } a \in \wp^{-1}(c). \end{aligned}$$

To check that it is well-defined, pick some other  $a' \in \wp^{-1}(c)$ . This element will differ from the previous  $a$  by some  $b \in \mu_n$ , hence

$$\sigma(a') - a' = \sigma(a) + \sigma(b) - a - b = \sigma(a) - a.$$

All good then. Assume from now on that  $\wp(A_K) \subseteq C$ . We factor then the previous pairing into the pairing that we are interested in:

$$\begin{aligned} \langle \cdot, \cdot \rangle : G_C \times C/\wp(A_K) &\longrightarrow \mu_n \\ (\sigma, \bar{c}) &\longmapsto \sigma(a) - a, \text{ for } a \in \wp^{-1}(c). \end{aligned}$$

**Proposition 3.** *The pairing  $\langle \cdot, \cdot \rangle$  is non-degenerate.*

*Proof.* We have to show that the induced morphisms

$$\varphi_1 : G_C \rightarrow \text{Hom}(C/\wp(A_K), \mu_n) \quad \text{and} \quad \varphi_2 : C/\wp(A_K) \rightarrow \text{Hom}(G_C, \mu_n)$$

are injective.

Suppose that  $\sigma \in G_C$  is such that  $\langle \sigma, \bar{c} \rangle = 0$  for all  $\bar{c} \in C/\wp(A_K)$ . In particular, if  $\sigma' \in G$  is a preimage of  $\sigma$ , then  $\sigma(a) = a$  for all  $a \in \wp^{-1}(C)$ . This means precisely that  $\sigma' \in G(A/\wp^{-1}(C))$ , hence  $\sigma = \text{id}_{K(\wp^{-1}(C))}$ .

Suppose now that  $c \in C$  is such that  $\langle \sigma, \bar{c} \rangle = 0$  for all  $\sigma \in G_C$ . We want to show that  $c \in \wp(A_K)$ , so let  $a \in \wp^{-1}(c)$ . For all  $\sigma' \in G$  we have  $\sigma'(a) = a$ , which means that  $a \in A_K$  and therefore  $\bar{c} = 0$ .  $\square$

**Proposition 4.**  *$K(\wp^{-1}(C))/K$  is finite if and only if  $(C : \wp(A_K))$  is finite.*

*Proof.* Suppose first that  $[K(\wp^{-1}(C)) : K]$  is finite. Then its Galois group  $G_C$  would be finite as well, so  $\text{Hom}(G_C, \mu_n)$  is finite. But  $\varphi_2$  is injective by Proposition 3, so  $C/\wp(A_K)$  must be finite as well.

Conversely, suppose that  $C/\wp(A_K)$  is finite. Again, this implies that  $\text{Hom}(C/\wp(A_K), \mu_n)$  is finite, so injectivity of  $\varphi_1$  shows that  $[K(\wp^{-1}(C)) : K]$  is finite as well.  $\square$

**Lemma 5.** *Let  $n \in \mathbb{N}$  be a non-zero natural number and let  $H$  be a finite abelian group with exponent  $d \mid n$ . Then there exists an isomorphism  $H \cong \text{Hom}(H, \mathbb{Z}/n\mathbb{Z})$ .*

*Proof.* By the structure theorem for finitely generated abelian groups it suffices to show the result for  $H = \mathbb{Z}/d\mathbb{Z}$ . We first reduce the result to the case  $d = n$ . There is a unique cyclic subgroup  $H_d \subseteq \mathbb{Z}/n\mathbb{Z}$  of order  $d$ . Every homomorphism  $\mathbb{Z}/d\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  factors then through  $H_d$ , so the canonical map

$$\mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, H_d) \hookrightarrow \mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$$

is an isomorphism. Since  $H_d \cong \mathbb{Z}/d\mathbb{Z}$ , it suffices to show that there is an isomorphism

$$\mathbb{Z}/d\mathbb{Z} \rightarrow \mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z}),$$

i.e. it suffices to show the case  $d = n$ .

In this case we consider the surjective homomorphism

$$\begin{aligned} \mathbb{Z} &\rightarrow \mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/d\mathbb{Z}) \\ 1 &\mapsto \mathrm{id}. \end{aligned}$$

Its kernel is  $d\mathbb{Z}$ , so passing to the quotient yields the desired isomorphism.  $\square$

**Proposition 6.** *If  $K(\wp^{-1}(C))/K$  or  $(C : \wp(A_K))$  are finite, then  $\varphi_1$  and  $\varphi_2$  from Proposition 3 are isomorphisms and*

$$[K(\wp^{-1}(C)) : K] = (C : \wp(A_K)).$$

*Proof.* By Proposition 4, if either of the two is finite, so is the other one. By Lemma 5 we have isomorphisms

$$C/\wp(A_K) \cong \mathrm{Hom}(C/\wp(A_K), \mu_n) \quad \text{and} \quad G_C \cong \mathrm{Hom}(G_C, \mu_n).$$

We have

$$\begin{aligned} [K(\wp^{-1}(C)) : K] &= |G_C| \\ &\leq |\mathrm{Hom}(C/\wp(A_K), \mu_n)| \\ &= |C/\wp(A_K)| \\ &\leq |\mathrm{Hom}(G_C, \mu_n)| \\ &= |G_C| \\ &= [K(\wp^{-1}(C)) : K]. \end{aligned}$$

Therefore  $[K(\wp^{-1}(C)) : K] = (C : \wp(A_K))$  and  $\varphi_1$  and  $\varphi_2$  are isomorphisms.  $\square$

**Proposition 7.** *Even if  $[K(\wp^{-1}(C)) : K]$  and  $(C : \wp(A_K))$  are not finite,  $\varphi_1$  is still an isomorphism and  $\varphi_2$  induces an isomorphism*

$$C/\wp(A_K) \cong \mathrm{Hom}_{\mathrm{cont}}(G_C, \mu_n)$$

*onto the subgroup of continuous homomorphisms.*

*Proof.* Consider the directed system  $\{C_i\}_{i \in I}$  of all subgroups  $C_i$  of  $C$  containing  $\wp(A_K)$  and such that  $(C_i : \wp(A_K))$  is finite. Since any finite intermediate extension  $K \subseteq L \subseteq K(\wp^{-1}(C))$  is contained in some  $K(\wp^{-1}(C_i))$ , we can write

$$G_C \cong \varprojlim_{i \in I} G_{C_i}.$$

Consider now for each  $i \in I$  the commutative diagram

$$\begin{array}{ccc} G_C & \xrightarrow{\varphi_1} & \text{Hom}(C/\wp(A_K), \mu_n) \\ \downarrow & & \downarrow \\ G_{C_i} & \xrightarrow[\varphi_{1,i}]{\cong} & \text{Hom}(C_i/\wp(A_K), \mu_n) \end{array}$$

in which both vertical arrows are the restrictions. Let  $f \in \text{Hom}(C/\wp(A_K), \mu_n)$  and consider for each  $i \in I$  its restriction  $f|_{C_i/\wp(A_K)}$ , which comes from a unique  $\sigma_i \in G_{C_i}$ . This yields a family of automorphisms  $(\sigma_i)_{i \in I}$ . We claim that this is a compatible family, giving therefore an element in  $G_C$  which maps to  $f$  and proving surjectivity of  $\varphi_1$ . To show this, let  $i \leq j$  and consider the diagram

$$\begin{array}{ccc} G_{C_j} & \xrightarrow{\varphi_{1,j}} & \text{Hom}(C_j/\wp(A_K), \mu_n) \\ \downarrow & & \downarrow \\ G_{C_i} & \xrightarrow{\varphi_{1,i}} & \text{Hom}(C_i/\wp(A_K), \mu_n) \end{array}$$

in which both vertical arrows are the restrictions. We want to check that it commutes. The isomorphism  $G/G(A/\wp^{-1}(C_k)) \rightarrow G_{C_k}$  is given by restriction of automorphisms for all  $k \in I$ . So every  $\tau \in G_{C_j}$  can be written as  $\sigma|_{K(\wp^{-1}(C_j))}$  for some  $\sigma \in G$ . For  $c \in C_i \subseteq C_j$  and  $a \in \wp^{-1}(c)$  we have then

$$\varphi_{1,i}(\tau|_{K(\wp^{-1}(C_i))})(\bar{c}) = \sigma(a) - a = \varphi_{1,j}(\tau)|_{C_i/\wp(A_K)}(\bar{c}),$$

showing commutativity of the diagram and thus finishing the proof of bijectivity of  $\varphi_1$ .

Before discussing the assertion about  $\varphi_2$ , we claim that every continuous homomorphism  $g: G_C \rightarrow \mu_n$  comes from some homomorphism  $g_i: G_{C_i} \rightarrow \mu_n$  via the restriction  $f_i: G_C \rightarrow G_{C_i}$ . Indeed, let  $\xi \in \mu_n$  be a generator. Given such  $g$  and given some  $k\xi \in \mu_n$  in the image of  $g$ , say  $k\xi = g(\sigma)$ , the preimage  $g^{-1}(k\xi)$  is open in  $G_C$ . Since the fibers of the restrictions form a basis for the topology on  $G_C$ , there exists some  $i_k \in I$  such that  $f_{i_k}^{-1}f_{i_k}(\sigma) \subseteq g^{-1}(g(\sigma))$ . Let now  $i = \max_k \{i_k\}$  and define

$$\begin{aligned} g_i: G_{C_i} &\longrightarrow \mu_n \\ \sigma|_{K(\wp^{-1}(C_i))} &\longmapsto g(\sigma). \end{aligned}$$

If  $\sigma|_{K(\wp^{-1}(C_i))} = \tau|_{K(\wp^{-1}(C_i))}$  and  $g(\sigma) = k\xi$ , then we have  $i_k \leq i$  and therefore

$$\tau \in f_i^{-1}f_i(\sigma) \subseteq f_{i_k}^{-1}f_{i_k}(\sigma) \subseteq g^{-1}(g(\sigma)),$$

showing that  $g_i$  is well-defined. And by construction  $g = g_i \circ f_i$ , proving the claim.

Moving on to the assertion about  $\varphi_2$ , suppose  $g \in \text{Hom}(G_C, \mu_n)$  is in the image of  $\varphi_2$ , say  $g = \varphi_2(\bar{c})$ . Then it is continuous, because the formula we used to define it involves only the continuous action of  $G$  on  $A$  and the continuous group operations in  $A$ . But we can also check this directly: by homogeneity it suffices to show that

$$g^{-1}(0) = \{\sigma \in G_C \mid \sigma(a) - a = 0 \text{ for } a \in \wp^{-1}(c)\}$$

is closed in  $G_C$ , which is true because its preimage under the quotient map is the closed subgroup  $G(A/\wp^{-1}(c))$  of  $G$ . Conversely, suppose  $g \in \text{Hom}(G_C, \mu_n)$  is a continuous homomorphism. Then by our previous claim we may find some  $i \in I$  such that  $g = g_i \circ f_i$  for

some  $g_i: G_{C_i} \rightarrow \mu_n$ , where  $f_i: G_C \rightarrow G_{C_i}$  denotes the restriction. This means that in the commutative square

$$\begin{array}{ccc} C_i/\wp(A_K) & \xrightarrow{\varphi_{2,i}} & \text{Hom}(G_{C_i}, \mu_n) \\ \downarrow & & \downarrow \\ C/\wp(A_K) & \xrightarrow{\varphi_2} & \text{Hom}(G_C, \mu_n) \end{array}$$

our  $g$  lies in the image of the right vertical arrow. By Proposition 6 the top horizontal arrow is an isomorphism. Hence  $g$  also lies in the image of  $\varphi_2$ .  $\square$

#### 4. MAIN THEOREM OF KUMMER THEORY

Recall from the previous section that  $C \subseteq A_K$  is a subgroup such that  $\wp(A_K) \subseteq C$  and  $\{C_i\}_{i \in I}$  is the directed system of all subgroups  $C_i$  of  $C$  containing  $\wp(A_K)$  such that  $(C_i : \wp(A_K))$  is finite.

**Lemma 8.**  $K(\wp^{-1}(C))/K$  is an abelian extension with exponent  $d$  dividing  $n$ .

*Proof.* This follows from injectivity of

$$\text{Gal}(K(\wp^{-1}(C))/K) \rightarrow \text{Hom}(C/\wp(A_K), \mu_n),$$

which was shown in Proposition 3.  $\square$

**Lemma 9.** Let  $L/K$  be a field extension with  $L \subseteq K_s$ . Then  $C := \wp(A_L) \cap A_K$  is a subgroup of  $A_K$  with the property that  $\wp(A_K) \subseteq C$ .

*Proof.* Since  $A_K \subseteq A_L$ , it follows that  $\wp(A_K) \subseteq \wp(A_L)$ . It remains to show that  $\wp(A_K) \subseteq A_K$ . Let  $a \in A_K$  and let  $\sigma \in G$ . Then using  $G$ -equivariance of  $\wp$  and the fact that  $a \in A_K$  we have

$$\sigma(\wp(a)) = \wp(\sigma(a)) = \wp(a),$$

hence  $\wp(a) \in A_K$  as well.  $\square$

**Lemma 10.** Let  $L := K(\wp^{-1}(C))$  and  $L_i := K(\wp^{-1}(C_i))$  for each  $i \in I$ . Then

$$A_L = \bigcup_{i \in I} A_{L_i}.$$

*Proof.* We show first the inclusion  $\supseteq$ . Let  $a \in A_{L_i}$  for some  $i \in I$ , i.e. for all  $\sigma \in G(A/\wp^{-1}(C_i))$  we have  $\sigma(a) = a$ . Let then  $\sigma \in G(A/\wp^{-1}(C))$ , which is by definition the set of automorphisms  $\tau \in G$  such that  $\tau(b) = b$  for all  $b \in \wp^{-1}(C)$ . Since  $a \in \wp^{-1}(C_i) \subseteq \wp^{-1}(C)$ , we deduce that  $\sigma(a) = a$ .

We move on to the inclusion  $\subseteq$ . Let  $a \in A_L$ , i.e.  $\sigma(a) = a$  for all  $\sigma \in \text{Gal}(K_s/L) = G(A/\wp^{-1}(C))$ . Consider the open subgroup  $G(A/a) \subseteq G$ . The corresponding field  $K(a) \subseteq K_s$  is finite over  $K$ , as we saw in Lemma 1. And since  $\text{Gal}(K_s/L) \subseteq G(A/a)$ , we have  $K(a) \subseteq L$ . Since  $K(a)$  is finite over  $K$  we may find some index  $i \in I$  such that  $K(a) \subseteq L_i$ , hence

$$a \in A_{K(a)} \subseteq A_{L_i}.$$

$\square$

**Theorem 11.** *Viewing abelian extensions of  $K$  as subfields of  $K_s$ , there is an inclusion-preserving bijection:*

$$\{C \trianglelefteq A_K \text{ s.t. } \wp(A_K) \subseteq C\} \leftrightarrow \{L/K \text{ abelian w/ exponent dividing } n\}.$$

*Given  $C \trianglelefteq A_K$  as above, the corresponding field extension is*

$$\Phi(C) := K(\wp^{-1}(C));$$

*and conversely, given  $L/K$  as above, the corresponding subgroup is*

$$\Psi(L) := \wp(A_L) \cap A_K.$$

*Proof.* The functions  $\Phi$  and  $\Psi$  are well-defined by Lemma 8 and Lemma 9 respectively.

Let us check first that  $\Psi \circ \Phi = \text{id}$ . Let  $C \subseteq A_K$  be a subgroup such that  $\wp(A_K) \subseteq C$  and let  $L = K(\wp^{-1}(C))$ . We denote  $\wp(A_L) \cap A_K$  by  $C'$ , so that the goal is showing that  $C' = C$ .

We start with the inclusion  $C \subseteq C'$ . The subgroup  $A_L \subseteq A$  consists of all  $a \in A$  which are fixed by the automorphisms in  $\text{Gal}(K_s/L) = G(A/\wp^{-1}(C))$ , which in turn are precisely the automorphisms fixing all the elements in  $\wp^{-1}(C)$ . Hence  $\wp^{-1}(C) \subseteq A_L$  and therefore  $C \subseteq \wp(A_L) \cap A_K = C'$ .

Moving on to the other inclusion  $C' \subseteq C$ , the first thing we claim is that  $G(A/A_L) = G(A/\wp^{-1}(C))$ . Indeed, from  $\wp^{-1}(C) \subseteq A_L$  we immediately deduce  $G(A/A_L) \subseteq G(A/\wp^{-1}(C))$ . And conversely, if  $\sigma \in G$  fixes every element in  $\wp^{-1}(C)$ , then it is an automorphism in  $\text{Gal}(K_s/L)$  by definition. But every element  $b \in A_L$  satisfies  $\tau(b) = b$  for all  $\tau \in \text{Gal}(K_s/L)$ , hence  $\sigma$  fixes every element in  $A_L$  as well. Hence  $G(A/A_L) = G(A/\wp^{-1}(C))$ . In particular,  $K(A_L) = K(\wp^{-1}(C)) = L$ . But we have seen already that  $C \subseteq C'$ , so  $\wp^{-1}(C) \subseteq \wp^{-1}(C')$  and

$$L = K(\wp^{-1}(C)) \subseteq K(\wp^{-1}(C')) \subseteq K(A_L) = L.$$

This implies that  $K(\wp^{-1}(C)) = K(\wp^{-1}(C'))$ . In particular, if we are in the situation of finite index, then we can apply Proposition 6 to conclude that  $C = C'$ . Indeed, both field extensions have the same degrees, so both  $C$  and  $C'$  have the same index over  $\wp(A_K)$ . Equality follows then from the already proven inclusion  $C \subseteq C'$ . This finishes the case in which  $C$  has finite index over  $\wp(A_K)$ , and the general case follows from this case thanks to Lemma 10, because

$$C' = \wp(A_L) \cap A_K = \bigcup_{i \in I} \wp(A_{L_i}) \cap A_K = \bigcup_{i \in I} C'_i = \bigcup_{i \in I} C_i = C.$$

It remains to show that  $\Phi \circ \Psi = \text{id}$  as well. Let  $L/K$  be an abelian extension with exponent  $d$  dividing  $n$ . Let  $C := \wp(A_L) \cap A_K$ . Then  $\wp^{-1}(C) \subseteq A_L$ . Indeed, if  $\wp(a) = \wp(b) \in A_K$  with  $b \in A_L$  and  $\sigma \in \text{Gal}(K_s/L) \subseteq G$ , then  $\sigma(a) - b \in \mu_n = \ker(\wp)$ , because

$$\wp(\sigma(a)) = \sigma(\wp(a)) = \wp(a) = \wp(b).$$

But  $b \in A_L$  implies that  $\sigma(b) = b$ , hence  $\sigma(a - b) \in \mu_n \subseteq A_K$ . In particular, since  $\sigma^{-1} \in G$ , we have

$$a - b = \sigma^{-1}(\sigma(a - b)) = \sigma(a - b) = \sigma(a) - b,$$

thus  $\sigma(a) = a$  and  $a \in A_L$ , showing the desired inclusion. Therefore  $\wp^{-1}(C)$  is fixed by  $\text{Gal}(K_s/L)$ , i.e.  $G(A/\wp^{-1}(C)) \supseteq \text{Gal}(K_s/L)$ . Hence  $K(\wp^{-1}(C)) \subseteq L$ , and we need to show that this inclusion is an equality.

We want to reduce to the case of finite cyclic field extensions in order to apply Axiom 2. Write  $L/K$  as the composite field of all intermediate fields finite over  $K$ . Each such intermediate field  $L'/K$  will again be an abelian extension, because every subgroup of  $\text{Gal}(L/K)$  is normal and the quotient of two abelian groups is abelian. In turn, the structure theorem for finitely generated abelian groups tells us that we can find subgroups  $H_j \subseteq \text{Gal}(L'/K)$  such that each  $\text{Gal}(L'/K)/H_j$  is cyclic and such that

$$\bigcap H_j = \{0\}.$$

Therefore we can write  $L/K$  as the composite of a family  $\{L_\alpha\}_{\alpha \in \Lambda}$  of finite cyclic extensions. We were trying to show that  $L \subseteq K(\wp^{-1}(C))$ . If we manage to show that  $L_\alpha \subseteq K(\wp^{-1}(C_\alpha))$  with  $C_\alpha = \wp(A_{L_\alpha}) \cap A_K$  for each  $\alpha \in \Lambda$ , then each  $L_\alpha$  is contained in  $K(\wp^{-1}(C))$  as well, because  $C_\alpha \subseteq C$ . So  $L \subseteq K(\wp^{-1}(C))$  would follow, and we may therefore assume that  $L/K$  is a finite cyclic extension.

Assume then that  $L/K$  is a finite cyclic extension. Consider the surjective homomorphism

$$\begin{aligned} q: \text{Gal}(L/K) &\longrightarrow G_C \\ \sigma &\longmapsto \sigma|_{K(\wp^{-1}(C))}. \end{aligned}$$

By Galois correspondence, it suffices to show that  $q$  is an isomorphism. To show that it is an isomorphism, it is enough to show that  $\text{Gal}(L/K)$  and  $G_C$  have the same cardinality. By Lemma 5 it is in turn enough to show that the induced homomorphism

$$\begin{aligned} q^*: \text{Hom}(G_C, \mu_n) &\longrightarrow \text{Hom}(\text{Gal}(L/K), \mu_n) \\ f &\longmapsto f \circ q \end{aligned}$$

is an isomorphism. Surjectivity of  $q$  implies that  $q^*$  is injective, so it remains only to show surjectivity of  $q^*$ . Let  $g: \text{Gal}(L/K) \rightarrow \mu_n$  be a homomorphism and let  $\sigma, \sigma' \in \text{Gal}(L/K)$ . Then

$$g(\sigma \circ \sigma') = g(\sigma) + g(\sigma') = g(\sigma) + \sigma(g(\sigma')),$$

the second equality being due to the fact that  $g(\sigma') \in \mu_n \subseteq A_K$  and therefore  $\sigma(g(\sigma')) = g(\sigma')$ . We are implicitly using here that the action of  $G$  on  $A$  induces a well-defined action of  $\text{Gal}(L/K)$  on  $A_L$ , and therefore on  $\mu_n \subseteq A_L$ . Indeed, if  $\tilde{\sigma}$  and  $\tilde{\tilde{\sigma}}$  are extensions of a given  $\sigma \in \text{Gal}(L/K)$  to  $K_s$ , then  $\tilde{\sigma} - \tilde{\tilde{\sigma}}$  is in the kernel of the restriction homomorphism, i.e. is in  $\text{Gal}(K_s/L)$ . So if  $a \in A_L$ , then  $\tilde{\sigma}(a) = \tilde{\tilde{\sigma}}(a)$ . From the equation above we see then that  $g$  is a 1-cocycle representing a cohomology class in  $H^1(\text{Gal}(L/K), A_L)$ . Axiom 2 implies that  $g$  is a 1-coboundary, i.e. there exists some  $a \in A_L$  such that  $g(\sigma) = a - \sigma(a)$  for all  $\sigma \in \text{Gal}(L/K)$ . Since the image of  $g$  is in  $\mu_n = \ker(\wp)$ , we see that  $\wp(a) = \wp(\tilde{\sigma}(a)) = \tilde{\sigma}(\wp(a))$  for all  $\tilde{\sigma} \in G$ , i.e.  $\wp(a) \in A_K$ . But since  $a \in A_L$ , we also have  $\wp(a) \in \wp(A_L)$ . Thus  $\wp(a) \in \wp(A_L) \cap A_K = C$  and  $a \in \wp^{-1}(C)$ . But then for all  $\tau \in G(A/\wp^{-1}(C))$  we have  $\tau(a) = a$ , so that we may define a homomorphism

$$\begin{aligned} f: G_C &\longrightarrow \mu_n \\ \sigma &\longmapsto a - \sigma(a). \end{aligned}$$

This  $f$  verifies  $g = f \circ q$ , showing surjectivity of  $q^*$  as we wanted.  $\square$



## REFERENCES

- [Bos18] Siegfried Bosch. *Algebra—from the viewpoint of Galois theory*. Birkhäuser Advanced Texts: Basler Lehrbücher. [Birkhäuser Advanced Texts: Basel Textbooks]. Birkhäuser/Springer, Cham, german edition, 2018.

PEDRO NÚÑEZ

ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG, MATHEMATISCHES INSTITUT

ERNST-ZERMELO-STRASSE 1, 79104 FREIBURG IM BREISGAU (GERMANY)

*Email address:* [pedro.nunez@math.uni-freiburg.de](mailto:pedro.nunez@math.uni-freiburg.de)

*Homepage:* <https://home.mathematik.uni-freiburg.de/nunez>

I would like to thank the DFG-Graduiertenkolleg GK1821 “Cohomological Methods in Geometry” for their support!