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 $G := \mathrm{Gal}(K_s/K)$ 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

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

(6) Let $\wp\colon A \to A$ be a G-equivariant surjective homomorphism whose kernel, denoted μ_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

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

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 direct system of all subfields of K_s which are finite field extensions of K. For each $i \in I$, let us denote by

$$f_i\colon G \to \mathrm{Gal}(L_i/K)$$

the restriction morphism. The topology in G is the coarsest one making all the f_i continuous. Since each $\mathrm{Gal}(L_i/K)$ is a finite group, endowed with the discrete topology, it follows that the topology on G should be the smallest

Date: September 16, 2020.

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

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

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 $\tau \in G$, $\sigma \in \mathrm{Gal}(K_s/L)$ and $a \in A_L$. Since $\mathrm{Gal}(K_s/L) \trianglelefteq G$, there is some $\sigma' \in \mathrm{Gal}(K_s/L)$ such that

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

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

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

A function $f\colon \mathrm{Gal}(L/K) \longrightarrow A_L$ is called a *principal crossed homomorphism* if there exists some $a \in A_L$ such that for all $\sigma \in \mathrm{Gal}(L/K)$ 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 $H^1(\mathrm{Gal}(L/K), A_L)$.

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*

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

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 $\sigma \colon \wp^{-1}(C) \to \wp^{-1}(C)$. 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 σ is an injective homomorphism $\wp^{-1}(C) \to \wp^{-1}(C)$. 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 σ is also surjective. Hence σ restricts to a bijection $\wp^{-1}(C) \to \wp^{-1}(C)$. We obtain in this manner a group homomorphism

$$G \to \mathrm{Aut}(\wp^{-1}(C)).$$

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 elemnt 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:

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

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

Proof. We have to show that the induced morphisms

$$\varphi_1 \colon G_C \to \mathrm{Hom}(C/\wp(A_K), \mu_n) \quad \text{and} \quad \varphi_2 \colon C/\wp(A_K) \to \mathrm{Hom}(G_C, \mu_n)$$

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 σ, then $\sigma(a) = a$ for all $a \in \wp^{-1}(C)$. This means precisely that $\sigma' \in G(A/\wp^{-1}(C))$, hence $\sigma = 1_{G_C}$.

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 $\bar{c} = 0$. ◻

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 $\mathrm{Hom}(G_C, \mu_n)$ is finite. But φ_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 $\mathrm{Hom}(C/\wp(A_K), \mu_n)$ is finite, so injectivity of φ_1 shows that $[K(\wp^{-1}(C)) : K]$ is finite as well. ◻

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 $H \cong \mathrm{Hom}(H, \mathbb{Z}/n\mathbb{Z})$.*

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 $\mathbb{Z}/d\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ 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

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

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

In this case we consider the surjective homomorphism

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

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

Proposition 6. *If $K(\wp^{-1}(C))/K$ or $(C : \wp(A_K))$ are finite, then φ_1 and φ_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

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

Therefore $[K(\wp^{-1}(C)) : K] = (C : \wp(A_K))$ and φ_1 and φ_2 are isomorphisms. $\square$

Proposition 7. *Even if $[K(\wp^{-1}(C)) : K]$ and $(C : \wp(A_K))$ are not finite, φ_1 is still an isomorphism and φ_2 induces an isomorphism*

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

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

$$\begin{tikzcd}
G_C \arrow[r, hook, "\varphi_1"] \arrow[d] & \operatorname{Hom}(C/\wp(A_K), \mu_n) \arrow[d] \\
G_{C_i} \arrow[r, "\cong", "\varphi_{1,i}"'] & \operatorname{Hom}(C_i/\wp(A_K), \mu_n)
\end{tikzcd}$$

in which both horizontal arrows are the restrictions. Let $f \in \operatorname{Hom}(C/\wp(A_K), \mu_n)$ 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 φ_1. To show this, let $i \leqslant j$ and consider the diagram

$$\begin{tikzcd}
G_{C_j} \arrow[r, "\varphi_{1,j}"] \arrow[d] & \operatorname{Hom}(C_j/\wp(A_K), \mu_n) \arrow[d] \\
G_{C_i} \arrow[r, "\varphi_{1,i}"] & \operatorname{Hom}(C_i/\wp(A_K), \mu_n)
\end{tikzcd}$$

in which both vertical arrows are the restrictions. We want to check that it commutes. The isomorphism $G/G(A/\wp^{-1}(C_k)) \longrightarrow G_{C_k}$ 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 φ_1.

Before discussing the assertion about φ_2, we claim that every continuous homomorphism $g\colon G_C \longrightarrow \mu_n$ comes from some homomorphism $g_i\colon G_{C_i} \longrightarrow \mu_n$ via the restriction $f_i\colon G_C \longrightarrow G_{C_i}$. 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

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

If $\sigma|_{K(\wp^{-1}(C_i))} = \tau|_{K(\wp^{-1}(C_i))}$ and $g(\sigma) = k\xi$, then we have $i_k \leqslant i$ 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 φ_2, suppose $g \in \mathrm{Hom}(G_C, \mu_n)$ is in the image of φ_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 $g \in \mathrm{Hom}(G_C, \mu_n)$ 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 $g_i\colon G_{C_i} \longrightarrow \mu_n$, where $f_i\colon G_C \longrightarrow G_{C_i}$ denotes the restriction. This means that in the commutative square

$$\begin{tikzcd} C_i/\wp(A_K) \arrow[r, "\varphi_{2,i}"] \arrow[d, hook] & \mathrm{Hom}(G_{C_i}, \mu_n) \arrow[d] \\ C/\wp(A_K) \arrow[r, "\varphi_2"] & \mathrm{Hom}(G_C, \mu_n) \end{tikzcd}$$

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

Proof. This follows from injectivity of

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

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 $\sigma \in \mathrm{Gal}(K_s/L) = G(A/\wp^{-1}(C))$. 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 $\mathrm{Gal}(K_s/L) \subseteq G(A/a)$, 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. We have seen that... □

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

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