ON A FAMILY OF ABELIAN ℓ-EXTENSIONS THAT ARE CYCLIC OR BICYCLIC

CLIFFORD CHAN

Abstract. Consider an abelian extension L/k whose degree is a prime power. We can write it as the compositum of cyclic extensions L_i/k that are linearly disjoint over k. We provide necessary and sufficient conditions that characterize the family of degrees $[KL_iL_j : K]$ for an intermediate field $k \subseteq K \subseteq L$. Those degrees determine the structure of the Galois group of the extensions KL_iL_j/K (and of their compositum).

1. Introduction

Consider an abelian extension L/k whose degree is a prime power. We can write L/k as the compositum of cyclic extensions L_i/k (for $i = 1, \dots, r$) that are linearly disjoint. For any intermediate field $k \subseteq K \subseteq L$ we are interested in describing the degrees

$$[KL_iL_j : K] \qquad \text{for } i, j = 1, \dots, r\,.$$

Supposing the degrees $[L_i : k]$ to be known, this is equivalent to describe the degrees

$$[(K \cap L_iL_j) : k]\,.$$

These degrees are not independent. We are able to provide necessary and sufficient conditions that characterize them:

Theorem 1. *Necessary and sufficient conditions for a family $\{d_{ij}\}_{ij}$ of positive integers to satisfy $d_{ij} = [(K \cap L_iL_j) : k]$ for some field $k \subseteq K \subseteq L$ are the following:*

$$d_{ii} \mid [L_i : k] \qquad \textit{and} \qquad d_{ii} \cdot d_{jj} \mid d_{ij} \quad \textit{and} \quad d_{ij} \mid d_{ii} \cdot [L_j : k] \qquad \textit{(for all } i \neq j\textit{)}$$

and, for every distinct $i_1, i_2, i_3 \in \{1, \dots, r\}$, the following integers are either all equal or two are equal and the third one is strictly larger:

$$\frac{d_{xy}}{d_{xx} \cdot d_{yy}} \qquad x, y \in \{i_1, i_2, i_3\} \quad \textit{with} \quad x \neq y\,.$$

We also investigate the structure of the Galois groups.

Theorem 2. *The Galois group of $(K \cap L_iL_j)/k$ is an abelian group of order a prime power with at most two cyclic components (thus the group structure is determined by the size and the exponent). Its size is d_{ij}, and its exponent is*

$$\frac{d_{ij}}{\min(d_{ii}, d_{jj})}\,.$$

2010 *Mathematics Subject Classification.* Primary: 11R20; Secondary: 11R18.

Key words and phrases. Abelian extensions, Number fields, Degree, Arithmetic functions.

Theorem 3. *The structure of the Galois group of the compositum of the extensions*

$$(K \cap L_i L_j)/k \qquad i,j = 1,\dots,r$$

is determined by (and it can be explicitly described in terms of) the family of degrees $[(K \cap L_i L_j) : k]$ *by varying* $i,j = 1,\dots,r$.

Our problem has been motivated by the fact that the degrees of a family of cyclotomic extensions of number fields plays a key role in Artin's Conjecture on primitive roots (see for example the survey by Moree [1]), and so it is meaningful to study the interdependencies of those degrees. Our investigation can be pursued by considering the intersection of the given field K with the compositum of three or more of the cyclic fields L_i.

We prove our main results in Section 6, relying on a formal setting with tuples that we introduce in Section 2. This note is self-contained, beyond basic facts on group theory and Galois theory that can be found e.g. in [2].

2. Setup for radical functions

Let r, N be positive integers with $N \geqslant 2$. We consider $(\mathbb{Z}/N\mathbb{Z})^r$, namely the additive group of all r-tuples whose entries are in $\mathbb{Z}/N\mathbb{Z}$.

We let $I = \{1, 2 \dots, r\}$ and we call $\mathcal{P}(I)$ the power set of I. We call 0_r the zero r-tuple and $\hat{i}_r$ the tuple with 1 at entry i and 0 everywhere else. We call π_i the i-th projection, namely the map that associates to an r-tuple its i-th entry. Fix a subgroup A of $(\mathbb{Z}/N\mathbb{Z})^r$. For any $J \subseteq I$ we define the following subgroup of A:

$$A_J := \{u \in A | \pi_i(u) = 0 \ \forall i \notin J\}. \tag{1}$$

We have $A_\varnothing = \{0_r\}$ and $A_I = A$. To ease notation we let $J_i = \{i\}$ and $J_{ij} = \{i,j\}$, and we write $A_i := A_{J_i}$ and $A_{ij} := A_{J_{ij}}$. We also define A_{i+j} to be the smallest subgroup of A containing A_i and A_j.

We use the analogous definitions if the group $(\mathbb{Z}/N\mathbb{Z})^r$ is replaced by $\prod_{i=1}^r \mathbb{Z}/N_i\mathbb{Z}$, where $N_1, \dots, N_r$ are positive integers.

Definition 4. We consider the following function:

$$F : \mathcal{P}(I) \to \mathbb{Z}_{\geqslant 1}, F(J) = |A_J|. \tag{2}$$

We also consider the function

$$G : \mathcal{P}(I) \to \mathbb{Z}_{\geqslant 1}, G(J) = \left| A_J / \left(\sum_{J' \subsetneq J} A_{J'} \right) \right|. \tag{3}$$

To determine the values of these functions it suffices to understand their ℓ-adic valuation for every prime number ℓ. This is why we fix a prime number ℓ and study the composition of F (respectively, G) with the ℓ-adic valuation. We may then replace, without loss of generality,

the integers N_i by the powers of ℓ with the same ℓ-adic valuation. Moreover, we may clearly neglect the trivial cyclic components. So our tuple group is now

$$\prod_{i=1}^{r} \mathbb{Z}/\ell^{E_i}\mathbb{Z} \qquad E_1, \dots, E_r > 0\,.$$

Definition 5. We consider the *radical function*

$$f : \mathcal{P}(I) \to \mathbb{Z}_{\geqslant 0},\ f(J) = v_\ell\,|A_J|\,. \tag{4}$$

and the *radical step function*

$$g : \mathcal{P}(I) \to \mathbb{Z}_{\geqslant 0}, g(J) = v_\ell \left| A_J / \left(\sum_{\substack{J' \subsetneq J \\ J' \neq \varnothing}} A_{J'} \right) \right|\,. \tag{5}$$

Example 6. Suppose that $r = 1$, so that $\mathcal{P}(I) = \{\varnothing, I\}$. Then we have

$$f(\varnothing) = g(\varnothing) = 0 \qquad \text{and} \qquad f(I) = g(I) = v_\ell|A|\,.$$

Remark 7. *For any $r \geqslant 1$ we have $f(\varnothing) = g(\varnothing) = 0$ and $f(I) = v_\ell|A|$. Moreover, for every $J \subseteq J' \subseteq I$ we have $g(J) \leqslant f(J) \leqslant f(J')$. However, we do not necessarily have $g(J) \leqslant g(J')$. For example, consider $r = 2$ and $A = A_1 \neq \{0_r\}$: we have $f(I) = f(J_1) > 0$ and $f(J_2) = 0$ hence $g(I) = f(I) - f(J_1) - f(J_2) = 0$ while $g(J_1) = f(J_1) > 0$.*

Remark 8. *For every $\hat{J} \subseteq J \subseteq I$ we have $f(J) - g(J) \geqslant f(\hat{J}) - g(\hat{J})$. Indeed, we have*

$$f(J) - g(J) = v_\ell \left| \sum_{J' \subsetneq J} A_{J'} \right| \geqslant v_\ell \left| \sum_{J' \subsetneq \hat{J}} A_{J'} \right| = f(\hat{J}) - g(\hat{J})\,.$$

3. Radical functions of level 1 and 2

We keep the notation of the previous section. A *radical function of level n* (where $1 \leqslant n \leqslant r$) is the restriction of the radical function f to the subsets of I that have at most n elements:

$$f_n : \{J \in \mathcal{P}(I); |J| \leqslant n\} \to \mathbb{Z}_{\geqslant 0},\ f_n(J) = v_\ell\,|A_J|\,. \tag{6}$$

We similarly restrict the domain of the function g as in (5) and we call such function a *radical step function of level n*. We note that, if $1 \leqslant n \leqslant N \leqslant r$, then f_n (respectively, g_n) is the restriction of f_N (respectively, g_N).

Example 9 (Level 1 radical functions)**.** Consider a radical function f_1 of level 1. It is determined by its values $f_1(\varnothing) = 0$ and $f_1(A_i) = v_\ell\,|A_i|$ for $i = 1, \dots, r$. The possible radical functions are the functions $\mathcal{F}$ on $\{J \in \mathcal{P}(I); |J| \leqslant 1\}$ that satisfy $\mathcal{F}(\varnothing) = 0$ and $\mathcal{F}(J_i) := b_i$ where the b_i are arbitrary integers in the interval from 0 to E_i. It is clear that the radical function f_1 of level 1 stemming from the group A is such that $f_1(A_i)$ is in the above interval. Indeed, this value is the ℓ-adic valuation of the size of a cyclic group of exponent dividing ℓ^{E_i}. Conversely, given integers b_i in the above intervals, a group whose level 1 radical function f_1 equals $\mathcal{F}$ is

$$A := \left\langle \ell^{E_1 - b_1}\hat{1}_r, \dots, \ell^{E_r - b_r}\hat{r}_r \right\rangle \cong \mathbb{Z}/\ell^{b_1}\mathbb{Z} \times \mathbb{Z}/\ell^{b_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/\ell^{b_r}\mathbb{Z}\,.$$

We now suppose that $r \geqslant 2$. Given a function

$$\mathcal{F} : \{J \in \mathcal{P}(I); |J| \leqslant 2\} \to \mathbb{Z}_{\geqslant 0}\,, \tag{7}$$

for every i we define $b_i := \mathcal{F}(J_i)$ and for every $i < j$ we define $b_{ij} := \mathcal{F}(J_{ij})$. Moreover, we define $c_{ij} := b_{ij} - (b_i + b_j)$.

Theorem 10. *A function as in* (7) *such that $\mathcal{F}(\varnothing) = 0$ is a level* 2 *radical function associated to a subgroup of $\prod_{i=1}^r \mathbb{Z}/\ell^{E_i}\mathbb{Z}$ if and only if all of the following conditions are met:*

1. *For every $i \in I$ we have $0 \leqslant b_i \leqslant E_i$.*
2. *For every distinct i, j we have*
$$b_i + b_j \leqslant b_{ij} \leqslant \min\{E_j + b_i, E_i + b_j\}$$
(equivalently, we have $0 \leqslant c_{ij} \leqslant \min\{E_i - b_i, E_j - b_j\}$).
3. *For every distinct i, j, k the three integers c_{ij}, c_{jk}, c_{ki} are either all equal or there is a unique maximal element, while the other two elements are equal.*

Theorem 11. *A function*

$$\mathcal{G} : \{J \in \mathcal{P}(I); |J| \leqslant 2\} \to \mathbb{Z}_{\geqslant 0} \tag{8}$$

such that $\mathcal{G}(\varnothing) = 0$ is a level 2 *radical step function associated to a subgroup of $\prod_{i=1}^r \mathbb{Z}/\ell^{E_i}\mathbb{Z}$ if and only if all of the following conditions are met:*

1. *For every $i \in I$ we have $0 \leqslant \mathcal{G}(J_i) \leqslant E_i$.*
2. *For every distinct i, j we have*
$$0 \leqslant \mathcal{G}(J_{ij}) \leqslant \min\{E_i - \mathcal{G}(J_i), E_j - \mathcal{G}(J_j)\}\,.$$
3. *For every distinct i, j, k the three integers $\mathcal{G}(J_{ij}), \mathcal{G}(J_{jk}), \mathcal{G}(J_{ki})$ are either all equal or there is a unique maximal element, while the other two elements are equal.*

Example 12. Suppose that $r = 2$. Consider a function $\mathcal{F}$ as in (7) such that $\mathcal{F}(\varnothing) = 0$. Theorem 10 states that $\mathcal{F}$ is a level 2 radical function associated to a subgroup of $\mathbb{Z}/\ell^{E_1}\mathbb{Z} \times \mathbb{Z}/\ell^{E_2}\mathbb{Z}$ if and only if we have

$$0 \leqslant b_1 \leqslant E_1 \qquad 0 \leqslant b_2 \leqslant E_2 \qquad b_1 + b_2 \leqslant b_{12} \leqslant \min\{E_2 + b_1, E_1 + b_2\}\,. \tag{9}$$

The conditions from Theorem 11 on the corresponding level 2 radical step function $\mathcal{G}$ are

$$0 \leqslant b_1 \leqslant E_1 \qquad 0 \leqslant b_2 \leqslant E_2 \qquad 0 \leqslant c_{12} \leqslant \min\{E_1 - b_1, E_2 - b_2\}\,. \tag{10}$$

We call $\sum_{i,j} A_{ij}$ the subgroup generated by the A_{ij}'s. The following remark may easily be generalized to higher levels:

Remark 13. *The level* 2 *radical function f associated to a subgroup A of $\prod_{i=1}^r \mathbb{Z}/\ell^{E_i}\mathbb{Z}$ completely determines (respectively, it is determined by) the l evel* 2 *radical step function g associated to A. Indeed, we have for $i \neq j$*

$$g(J_{ij}) = f(J_{ij}) - f(J_i) - f(J_j) \qquad g(J_i) = f(J_i) \qquad f(\varnothing) = g(\varnothing) = 0\,.$$

Moreover, the level 2 radical function (respectively, level 2 radical step function) is the same for A and for $A \cap \sum_{i,j} A_{ij}$.

Remark 14. *Different groups may have the same radical function (respectively, radical step function), for example the cyclic groups* $\langle(1 \bmod \ell^{E_1}, 1 \bmod \ell^{E_2})\rangle$ *and* $\langle(1 \bmod \ell^{E_1}, 2 \bmod \ell^{E_2})\rangle$ *for* $r = 2$ *and* $\ell > 2$*. Conversely, two isomorphic groups may have different radical functions, consider for example the cyclic groups* $\langle(1 \bmod \ell^{E_1}, 1 \bmod \ell^{E_2})\rangle$ *and* $\langle(1 \bmod \ell^{E_1}, 0 \bmod \ell^{E_2})\rangle$ *for* $r = 2$*.*

Moreover, composing a permutation on I with a radical function (respectively, a radical step function) results in the same kind of function.

Setting $c_{ij} := \mathcal{G}(J_{ij})$, Condition (3) of Theorem 11 is clearly satisfied if all the c_{ij}'s are equal, or if all but one of these integers are equal and the remaining integer is strictly larger. In the following example we show a level 2 radical step function where the family of c_{ij}'s is not as in those two above cases:

Example 15. Let $A = \left\langle (1,-1,0,0), (0,\ell^2,-\ell^2,0), (0,0,\ell^4,-\ell^4)\right\rangle$ be a subgroup of $(\mathbb{Z}/\ell^5\mathbb{Z})^4$. Clearly the generators of A generate A_{12}, A_{23} and A_{34} respectively. The tuples $(\ell^2,0,-\ell^2,0)$, $(\ell^4,0,0,-\ell^4)$ and $(0,\ell^4,0,-\ell^4)$ generate A_{13}, A_{14} and A_{24} respectively.

Let $c_{ij} := g(J_{ij})$, where g is the level 2 radical step function associated to A. Condition (3) of Theorem 11 holds for g. From the explicit description of the groups A_{ij}'s we deduce that $c_{12} = 5$, $c_{13} = c_{23} = 3$ and $c_{14} = c_{24} = c_{34} = 1$.

4. Proof of the classification of level 2 radical functions

Lemma 16. *Let $i, j \in I$ with $i \neq j$.*

(1) We have $g(J_{ij}) = c_{ij} = v_\ell|A_{ij}/A_{i+j}|$. In particular, we have $c_{ij} \geqslant 0$.
(2) The group A_{ij}/A_{i+j} is cyclic. Moreover, if $A_i = A_j = \{0_r\}$, the two non-zero entries of a non-zero tuple in A_{ij} must have the same order.

Proof. For the first equality, we may reason as done for the case $r = 2$ (see Example 12) by neglecting the zero entries beyond the indices i, j. The second equality is because we have $A_i \cap A_j = \{0_r\}$ hence

$$g(J_{ij}) = v_\ell\left|A_{J_{ij}}/(A_{J_i} + A_{J_j})\right| = v_\ell\left|A_{ij}/A_{i+j}\right| .$$

The cyclicity of A_{ij}/A_{i+j} means that, given any two elements $u, u' \in A_{ij}$, one is a multiple of the other up to an element of A_{i+j}. Up to exchanging u, u' there is some integer λ such that $\pi_i(u - \lambda u') = 0$ and hence $u = \lambda u' \bmod A_j$. Finally, we prove the last assertion by contradiction. If w.l.o.g. there is a tuple such that the i-th entry has order ℓ^x and the j-th entry has order ℓ^X with $X > x$, then the ℓ^x multiple of the given tuple is a non-zero tuple in A_j, contradiction. □

Proof of Theorem 11. We use the notation $b_i := \mathcal{G}(J_i)$ and $c_{ij} := \mathcal{G}(J_{ij})$ and $G := \prod_i \mathbb{Z}/\ell^{E_i}\mathbb{Z}$.

Suppose that $\mathcal{G}$ is the level 2 radical step function associated to a subgroup A of G. To show the necessity of condition (1) we may restrict the function to $\{J \subseteq I; |J| \leqslant 1\} \to \mathbb{Z}_{\geqslant 1}$ and apply Example 9.

The smallest subgroup of A that contains A_i for every i is $L_1 := \prod_i \pi_i(A_i) \cong \prod_i \mathbb{Z}/\ell^{b_i}\mathbb{Z}$. Moreover, the quotient of G modulo L_1 can be identified with $G' := \prod_i \mathbb{Z}/\ell^{E_i - b_i}\mathbb{Z}$. The group $A' := A/L_1$ can then be identified with a subgroup of G'. Let $\mathcal{G}'$ be the level 2 radical step function of A'. By the choice of L_1 we have $A'_i = \{0_r\}$ for every i and hence $\mathcal{G}'(J_{ij}) = v_\ell|A'_{ij}|$. Since $A_{ij} \cap L_1 = A_{i+j}$ we have $A'_{ij} \cong A_{ij}/A_{i+j}$ and hence $\mathcal{G}'(J_{ij}) = \mathcal{G}(J_{ij})$.

We may then show the necessity of conditions (2) and (3) for $\mathcal{G}$ by proving them for $\mathcal{G}'$. By Lemma 16(2), the group A'_{ij} is generated by a tuple whose i-th and j-th entry have order $\ell^{c_{ij}}$. As the i-th entry has order dividing $\ell^{E_i - b_i}$ (and similarly for the j-th entry), condition (2) holds. To show condition (3), we may assume w.l.o.g. that $\mathcal{G}'(J_{ij}) \geqslant \mathcal{G}'(J_{jk}) \geqslant \mathcal{G}'(J_{ik})$ and prove $\mathcal{G}'(J_{jk}) = \mathcal{G}'(J_{ik})$. By taking a suitable multiple of the generator of A'_{ij}, its j-th entry is the same as the one of the generator of A'_{jk}. We conclude because the difference tuple is in A'_{ik} and has the same order of the generator of A'_{jk}.

Conversely, suppose that $\mathcal{G}$ satisfies the conditions in the statement, and hence the same holds for $\mathcal{G}'$ w.r.t. the group G' (where we replace b_i by 0 and we keep the same value for c_{ij}). We claim that $\mathcal{G}'$ is the level 2 radical step function associated to a subgroup A' of G'. Then the preimage of A' under the quotient map $G \to G/L_1 = G'$ is a subgroup A of G such that $\mathcal{G}$ is the level 2 radical step function associated to A. We are then reduced to the case of a level 2 radical step function $\mathcal{G}$ such that $b_i = 0$ for every i.

Define the tuples $t_{ij} := \ell^{E_i - c_{ij}}\hat{i}_r - \ell^{E_j - c_{ij}}\hat{j}_r$, noticing that it is a difference of tuples of order $\ell^{c_{ij}}$. Consider the group $A' := \langle t_{ij} | i < j \rangle$. To conclude it suffices to prove w.l.o.g. that $A'_{12} = \langle t_{12} \rangle$. The inclusion $A'_{12} \supseteq \langle t_{12} \rangle$ is clear. Now let t be a tuple in A'_{12}, and write

$$t = \sum_{i<j} \lambda_{ij} t_{ij} = \sum_{i<j} \lambda_{ij}\ell^{E_i - c_{ij}}\hat{i}_r - \lambda_{ij}\ell^{E_j - c_{ij}}\hat{j}_r$$

for some integers λ_{ij}. If $r = 2$, clearly t is a multiple of t_{12}, so suppose that $r > 2$.

We claim that we may write (possibly with a different choice of the integers λ_{ij})

$$t = \sum_{i<j<r} \lambda_{ij} t_{ij}\,.$$

By iterating the analogous procedure, we also have a similar decomposition with $i < j < 3$, which gives the requested inclusion. To prove the claim, we show that

$$\sum_{i<r} \lambda_{ir} t_{ir} = 0_r \bmod \langle t_{ij} | i < j < r \rangle\ .$$

This is clear if all coefficients λ_{ir} are 0. There cannot be precisely one coefficient which is non-zero because $\pi_r(t) = 0$ and hence

$$\sum_{i<r} \lambda_{ir}\ell^{E_r - c_{ir}} = 0\,.$$

Now we suppose that there are two non-zero coefficients λ_{ir} and λ_{jr} with $i < j$ and show that the above sum is congruent to a sum that has more zero coefficients, leading to the desired property by iteration. Consider the three numbers c_{ij}, c_{ir}, c_{jr} and suppose w.l.o.g. that $c_{ir} = \min(c_{jr}, c_{ij})$ (the case where c_{jr} is the minimum being analogous). We conclude by setting to

zero the coefficient of t_{ir}, which is possible (without introducing more non-zero coefficients) because we can write

$$t_{ir} - \ell^{c_{jr}-c_{ir}} \cdot t_{jr} = \ell^{E_i-c_{ir}}\hat{i}_r - \ell^{E_j-c_{ir}}\hat{j}_r = \ell^{c_{ij}-c_{ir}} t_{ij} \,.$$

□

Proof of Theorem 10. This follows from Theorem 11 and Remark 13. □

5. The structure of the group of tuples

We keep the notation of the previous sections. Suppose that we want to study, more precisely, the group structure of the groups A_J for $J \subseteq I$. As $A_\varnothing$ is the trivial group, we may suppose that $J \neq \varnothing$. Moreover, if J is a singleton, then A_J is clearly cyclic. Finally, for level 2 radical functions (respectively, radical step functions) we only consider sets J that have almost two elements. So we may now suppose that $J = \{i, j\}$ has two elements. Since the tuples in A_J have at most two non-zero entries, the group A_J has at most two cyclic components. Then the group structure of A_J is determined by its size and exponent. Indeed, if the size is ℓ^X and the exponent is ℓ^x (where $x \leqslant X$) then the group structure is

$$\mathbb{Z}/\ell^x\mathbb{Z} \times \mathbb{Z}/\ell^{X-x}\mathbb{Z}$$

and the group is cyclic if and only if $X = x$.

Proposition 17. *For every $i \neq j$, the exponent of the group A_{ij} is*

$$\ell^{c_{ij}+\max\{b_i,b_j\}} = \ell^{b_{ij}-\min\{b_i,b_j\}} \,.$$

Consequently, A_{ij} is cyclic if and only if $b_i = 0$ or $b_j = 0$.

Proof. The exponent of A_{ij} is the highest order of a set of generators. By the proof of Theorem 11 we have for some integer z_{ij} coprime to ℓ

$$A_{ij} = \left\langle \ell^{E_i-b_i-c_{ij}}\hat{i}_r + z_{ij}\ell^{E_j-b_j-c_{ij}}\hat{j}_r, \ell^{E_i-b_i}\hat{i}_r, \ell^{E_j-b_j}\hat{j}_r \right\rangle$$

and the result follows. □

In the following results we focus on the tuples in A that are sums of tuples having at most two non-zero entries:

Theorem 18. *The size of the groups A_i and of the groups A_{ij} for all $i \neq j$ determines the group structure of*

$$\sum_{i,j} A_{ij} \,.$$

The group structure is described explicitly (in terms of the known quantities) thanks to Lemma 19 and Proposition 20.

Proof. The given information amounts to knowing the level 2 radical step function associated to A. By Lemma 19 we may reduce to the case where $c_{ij} > 0$ holds for every $i \neq j$. Then we may conclude by applying Proposition 20. □

Lemma 19. *Let $r \geqslant 2$, and suppose that $A = \sum_{i \neq j} A_{ij}$. There exists a partition of I into non-empty sets $I_1, \dots, I_m$ (for some $m \geqslant 1$) such that $A = A_{I_1} A_{I_2} \cdots A_{I_m}$ and such that the following holds for the level 2 radical step function of A: we have $g(J_{ij}) = 0$ for distinct $i, j \in I$ if and only if i and j belong to different sets of the partition.*

Proof. It suffices to iterate (at most r times) the following procedure (noticing that $g(J_{ij}) > 0$ for i, j in the same set of the partition only holds after the last iteration). Suppose that $g(J_{xy}) = 0$ holds for some $x \neq y$ in I. Then we partition $I = I_1 \cup I_2$, where

$$I_1 := \{i \in I \setminus \{x\} | g(J_{ix}) = 0\}$$

and $I_2 := I \setminus I_1$, the sets I_1 and I_2 being non-empty (because $y \in I_1$ and $x \in I_2$).

If $i \in I_1$ and $j \in I_2$, then we have $g(J_{ij}) = 0$ because $c_{ix} = 0$ while $c_{jx} > 0$ and hence $c_{ij} = 0$ by Theorem 11.

Moreover, we have $A = A_{I_1} A_{I_2}$. Indeed, the inclusion $\supseteq$ clearly holds. The other inclusion follows from the fact that for every $i \in I_1$ and $j \in I_2$ we have $A_{ij} = A_{i+j}$ because $g(J_{ij}) = 0$. □

We are then reduced to study level 2 radical step functions on I such that $g(J_{ij}) > 0$ holds for every distinct $i, j \in I$.

Proposition 20. *Let $r \geqslant 2$, and suppose that $A = \sum_{i \neq j} A_{ij}$. Moreover, suppose that the level 2 radical step function g associated to A satisfies $c_{ij} > 0$ for every $i \neq j$. Then we have*

$$A \cong \prod_{i=1}^{r} \mathbb{Z}/\ell^{a_i}\mathbb{Z} \quad \textit{with} \quad a_1 \geqslant a_2 \geqslant \cdots \geqslant a_r \geqslant 0 \quad \textit{and} \quad a_{r-1} > 0\,.$$

We have

$$a_1 := \max_{i,j \in I}(c_{ij} + b_i)$$

and we let i_1 be the smallest index such that $a_1 = \max_{i \in I \setminus \{i_1\}}(c_{i_1 i} + b_{i_1})$. For $2 \leqslant k \leqslant r-1$ we define

$$a_k := \max_{i,j \in I \setminus \{i_1, \dots, i_{k-1}\}} (c_{ij} + b_i)\,,$$

where i_k is the smallest index such that $a_k = \max_{i \in I \setminus \{i_1, \dots, i_k\}}(c_{i_k i} + b_{i_k})$. Finally, we define $a_r = b_{i_r}$, where $\{i_r\} = I \setminus \{i_1, \dots, i_{r-1}\}$.

In particular, the exponent of A has ℓ-adic valuation $\max_{i,j \in I}(c_{ij} + b_i)$, while the size of A is given by

$$v_\ell |A| = b_1 + \cdots + b_r + \sum_{h=1}^{r-1} \max_{j \neq i_1, \dots, i_h} c_{i_h j}\,.$$

Proof. Without loss of generality, up to reordering the indices, we may assume that $i_k = k$. We prove the statement by induction on $r \geqslant 2$. The base case $r = 2$ can be derived from Proposition 17. Indeed (since $b_1 \geqslant b_2$ by our assumption on i_1) we have

$$A = A_{12} \cong \mathbb{Z}/\ell^{c_{12}+b_1}\mathbb{Z} \times \mathbb{Z}/\ell^{b_2}\mathbb{Z}\,.$$

Now we let $r \geqslant 3$, suppose that the statement is true for $r-1$ and prove it for r. Let j be an index such that $a_1 = c_{1j} + b_1$. We note that $a_1 = \max_{i,k}(c_{ik} + b_k) \geqslant c_{1j} + b_j$ and thus $b_1 \geqslant b_j$. By Lemma 16 the group A_{1j}/A_{1+j} is cyclic with size $\ell^{c_{1j}}$, and it is generated by the class of some $t \in A_{1j}$. The order of $\ell^{c_{1j}}t \in A_{1+j}$ is $\ell^{\max\{b_1,b_j\}} = \ell^{b_1}$. Indeed, if the order were smaller, $\ell^{c_{1j}-1}t$ (recall that $c_{1j} > 0$) has the first entry in common with an element of A_1 hence it is in A_{1+j}, contradiction. For later use, since $b_1 \geqslant b_j$, the order of t is the same as the order of $\pi_1(t)$ (notice that, if $b_1 = b_j$, the two non-zero entries of t must have the same order).

Thus the exponent of A is at least a_1. To prove the equality, recall that any tuple in A is the sum of tuples having at most two non-zero entries, so we are left to bound the exponent of A_{ij} for $i \neq j$, and we conclude by Proposition 17 because $c_{ij} + \max(b_i, b_j) \leqslant a_1$.

Set $A' := A_{I\setminus\{1\}}$ and apply the induction hypothesis to A' by neglecting the first entry (which is zero). Since $i_1 = 1$, the integers $a_2, \ldots, a_r$ do not depend on the on the first entry. We obtain that

$$A' \cong \prod_{i=2}^{r} \mathbb{Z}/\ell^{a_i}\mathbb{Z} \quad \text{with} \quad a_2 \geqslant \cdots \geqslant a_r \geqslant 0 \quad \text{and} \quad a_{r-1} > 0\,.$$

Since $\langle t\rangle \cong \mathbb{Z}/\ell^{a_1}\mathbb{Z}$ and the exponent of A is ℓ^{a_1}, we conclude by proving $A' \cong A/\langle t\rangle$. We show that the quotient homomorphism $\phi : A' \to A/\langle t\rangle$ is bijective. If $\phi(u) = \phi(u')$ for some $u, u' \in A'$, there exists an integer λ such that $u - u' = \lambda t$. Since $\pi_1(u) = \pi_1(u') = 0$ we get $\pi_1(\lambda t) = 0$ hence $\lambda t = 0_r$, which gives $u = u'$. To show surjectivity, take $u \in A$. Since the exponent of A is ℓ^{a_1}, we have $v_\ell \circ \pi_1(u) \leqslant E_1 - a_1 = v_\ell \circ \pi_1(t)$. We deduce that by subtracting from u a suitable multiple of t we obtain an element of A' and we conclude. □

6. Application of radical functions to study abelian extensions

We first prove the three results from the Introduction. We describe how the investigation of Galois groups amounts to the investigation of their Pontryagin duals.

If F'/F is an abelian extension of fields of degree a power of ℓ, then the Pontryagin dual of $\mathrm{Gal}(F'/F)$, which we denote by $G(F'/F)$, is isomorphic to $\mathrm{Gal}(F'/F)$. Since $\mathrm{Gal}(L/k)$ is isomorphic to the product of the groups $\mathrm{Gal}(L_i/k)$, we deduce that

$$G(L/k) \cong \prod_{i=1}^{r} G(L_i/K)\,.$$

For every i, j the following diagram consists of surjective homomorphisms and it gives a pushout because the restriction map $\mathrm{Gal}(L/L_iL_j) \to \mathrm{Gal}(K/(K \cap L_iL_j))$ is surjective:

$$\begin{array}{ccc} \mathrm{Gal}(L/k) & \longrightarrow & \mathrm{Gal}(K/k) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(L_iL_j/k) & \longrightarrow & \mathrm{Gal}((K \cap L_iL_j)/k) \end{array}$$

By duality, the following diagram consists of injective homomorphisms and it gives a pullback:

$$\begin{array}{ccc} G(L/k) & \longleftarrow & G(K/k) \\ \uparrow & & \uparrow \\ G(L_iL_j/k) & \longleftarrow & G((K\cap L_iL_j)/k) \end{array}$$

Thus, considering the images of these groups in $G(L/k)$, we have

$$G'((K\cap L_iL_j)/k) = G'(K/k)\cap G'(L_iL_j/k)\,. \tag{11}$$

Let $I=\{1,\dots,r\}$ and define integers E_i such that $G(L_i/k)\cong \mathbb{Z}/\ell^{E_i}\mathbb{Z}$. Thus we have

$$G(L/k)\to \prod_{i=1}^{r}\mathbb{Z}/\ell^{E_i}\mathbb{Z}\,.$$

We can fix such an isomorphism such that $G(L_iL_j/k)$ corresponds to the subgroup of the tuples whose entries in $I\setminus\{i,j\}$ are zero. From (11) we deduce that, denoting by $A(K)$ the tuple group associated to $G'(K/k)$, the tuple group $A(K)_i$ (respectively, $A(K)_{ij}$) is associated to $G'((K\cap L_i)/k)$ (respectively, $G'((K\cap L_iL_j)/k)$ for $i\neq j$).

Proof of Theorem 1. Consider the function

$$f:\{J\subseteq I;|J|\leqslant 2\}\to\mathbb{Z}_{\geqslant 0}\qquad f(J)=\begin{cases}0 & J=\varnothing\\ v_\ell(d_{ii}) & J=J_i\\ v_\ell(d_{ij}) & J=J_{ij}\,.\end{cases} \tag{12}$$

Suppose that the d_{ij}'s are the degrees associated to an intermediate extension K. Then we have

$$f(J_i)=v_\ell(A(K)_i)\qquad f(J_{ij})=v_\ell(A(K)_{ij})$$

and hence f is the level 2 radical function associated to the tuple group $A(K)$. So the quantities $b_i=v_\ell(d_{ii})$ and $b_{ij}=v_\ell(d_{ij})$ satisfy the conditions in Theorem 10 and we deduce the conditions on the d_{ij}'s in the statement.

Conversely, suppose that the d_{ij}'s satisfy the conditions in the statement. Then by Theorem 10 the function f is the radical function associated to a tuple group $A\subseteq\prod_{i=1}^r\mathbb{Z}/\ell^{E_i}\mathbb{Z}$ and w.l.o.g. we may suppose that $A\subseteq\sum_{i,j}A_{i,j}$.

We then construct an intermediate extension K such that $d_{ij}=[(K\cap L_iL_j):k]$ holds for every i,j. Indeed, A corresponds to a subgroup of $G(L/k)$ and hence to a quotient of $\mathrm{Gal}(L/k)$. As the latter group is abelian, this quotient corresponds to an intermediate Galois extension $k\subseteq K\subseteq L$. □

Proof of Theorem 2. The first assertion is immediate. The assertions on the size and the exponent follow from the proof of Theorem 1 and Proposition 17. □

Proof of Theorem 3. This is the application of Theorem 18 to the setting described in this section, the level 2 radical function being (12). □

6.1. **On the degree of cyclotomic extensions.** We let K be a field of characteristic zero, and work within an algebraic closure of K. We call ζ_n a primitive n-th root of unity and denote by $\mathbb{Q}_n$ the n-th cyclotomic field. If K is a field of characteristic zero, the relative degree of the cyclotomic extensions of K is given by the function

$$\mathbb{Z}_{\geqslant 1} \to \mathbb{Z}_{\geqslant 1} \qquad n \mapsto [K(\zeta_n) : K] = \frac{\varphi(n)}{[(K \cap \mathbb{Q}_n) : \mathbb{Q}]},$$

where φ is Euler's Phi function. To study this function it suffices to study the ℓ-adic valuation of its values for all prime numbers ℓ. So we fix a prime number ℓ and consider instead the function

$$\mathbb{Z}_{\geqslant 1} \to \mathbb{Z}_{\geqslant 0} \qquad n \mapsto v_\ell\left([K(\zeta_n) : K]\right).$$

This function depends only on the largest subextension K' of $K \cap (\cup_{n\geqslant 1}\mathbb{Q}_n)$ such that any finite subextension of $K'/\mathbb{Q}$ has degree a power of ℓ. So we replace K by K'.

We fix some positive integer N and study the restriction of the above function to the set of divisors d of N having at most two prime factors. We may then replace K by $K \cap \mathbb{Q}_N$. For simplicity, we suppose that $\mathbb{Q}_4 \subseteq K$ if $\ell = 2$.

We can write $N = \ell^v N'$ for some integer N' that is coprime to ℓ. Since we only consider the ℓ-part of the extension $K(\zeta_N)/K$ we may suppose without loss of generality that N' is square-free. For every prime divisor p_i of N' we define the cyclic extension $L_i/\mathbb{Q}$ as the largest ℓ-subextension of $\mathbb{Q}(\zeta_{p_i})/\mathbb{Q}$. If $v > 0$, we similarly define $L_0/\mathbb{Q}$ by considering $\mathbb{Q}(\zeta_{\ell^v})/\mathbb{Q}$.

The family of degrees (and also the group structures) of the extensions $K(\zeta_d)/K$ may then be studied thanks to our main results. Indeed, the finitely many cyclic extensions L_i's and L_0 defined above have degree a power of ℓ, are linearly independent, and K is contained in their compositum. One thing to be clarified is that we could have $0 < v_\ell(d) < v$. Write $d = \ell^{v_\ell(d)}d'$. To solve this issue we observe that the degree (respectively, the Galois group structure) of $K(\zeta_d)/K$ is determined by the ones of $K(\zeta_{d'})/K$ and $K(\zeta_{\ell^v d'})/K$.

Acknowledgements. We thank Gabor Wiese for Remark 14 and Antonella Perucca for suggesting the problem and streamlining the arguments.

References

[1] P. Moree, Artin's primitive root conjecture — a survey, *Integers*, 12 (2012), 1305–1416.
[2] S. Lang, Algebra, Revised third edition, Grad. Texts in Math., 211, Springer-Verlag, New York, 2002. xvi+914 pp. ISBN: 0-387-95385-X.

Department of Mathematics, University of Luxembourg, 6 av. de la Fonte, 4364 Esch-sur- Alzette, Luxembourg

Email address: chiwa.chan@uni.lu