Commuting-Liftable Subgroups of Galois Groups

Adam Topaz

A Dissertation

in

Mathematics

Presented to the Faculties of the University of Pennsylvania in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

2013

_____

Florian Pop, Professor of Mathematics
Supervisor of Dissertation

_____

Jonathan Block, Professor of Mathematics
Graduate Group Chairperson

Dissertation Committee:
Florian Pop, Professor of Mathematics
David Harbater, Professor of Mathematics
Jonathan Block, Professor of Mathematics

Acknowledgments

First and foremost, I would like to thank my advisor, Florian Pop, whose encouragement and support has been invaluable throughout the last five years. He has always been eager to discuss mathematics and share with me his acute intuition and vast knowledge. His advice has been instrumental in shaping my mathematical personality and his guidance helped form the way I think about math. This project would never have succeeded without his mentorship.

The ideas that turned into this thesis were first conceived in the summer of 2011 during a two-month visit to the Hausdorff Institute for Mathematics in Bonn, Germany. I would like to thank HIM for the excellent working and living conditions during these two months. Also, I would like to particularly thank Moshe Jarden, Dan Haran and Lior Bary-Soroker for their interest in this work and for several discussions while at HIM and also later on.

I would like to specifically thank Jochen Koenigsmann. It was during the workshop on valuation theory in positive characteristic at the Mathematical Village in Şirince, Turkey in 2011 where he shared in my hope that the theory of commuting-

pairs should "work with enough roots of unity." This hope eventually developed into this thesis.

I would also like to thank Jakob Stix. I first realized the potential importance of "minimized inertia/decomposition groups" after I discussed with him the earliest version of the commuting-pairs theory during my short visit to Heidelberg.

I would like to thank Ján Mináč for his constant encouragement and enthusiasm. His continued interest in my work truly means a lot to me. I also thank John Swallow for being at the origins of my interest in Galois theory and for being a mentor during my last two years at Davidson College – my mathematical path would have been drastically different if it wasn't for him.

There are many professors who have helped me in various ways during graduate school, and I thank all of them. I am particularly grateful to David Harbater for encouraging me to speak in the Galois seminar and for numerous discussions; Ted Chinburg for orals preparation, classes on algebraic K-theory and class field theory, and his interest in my work; Steve Shatz for endless encouragement, motivation and advice; Jonathan Block for helping me realize the importance of algebraic topology and usefulness of homological algebra; and Tony Pantev helping me develop a broad base of knowledge in algebra. They all made my time at UPenn both stimulating mathematically and very enjoyable. I would also like to acknowledge and thank the cornerstone of the UPenn math department: Janet, Monica and Paula; I would have been completely lost without them.

There are many friends who have helped me both socially and mathematically in the last several years and to whom I owe my sincerest gratitude. I cannot list them all, but here are the names of just a few: Justin Curry, Tyler Kelly, Ying Zhang, Victor Lu, Marco Radeschi, Ryan Eberhart, Ryan Manion, Shanshan Ding, Aaron Silberstein, Andrew Obus, Asher Auel, Alberto García-Raboso, Elaine So.

I owe everything to my parents, Rachel and Tony Topaz. They always had full faith that I could accomplish all of my goals – whether academic or otherwise. Their unconditional support has brought me to where I am today.

And finally, I would like to thank Ivey McAliley. You delayed and changed your own goals so that I could accomplish mine. You have sacrificed so much so that we could be together in Philadelphia, and I cannot thank you enough. No words can adequately describe my appreciation for this. I am excited about our next adventure.

ABSTRACT

Commuting-Liftable Subgroups of Galois Groups

Adam Topaz

Florian Pop, Advisor

Let n denote either a positive integer of ∞, let ℓ be a fixed prime and let K be a field of characteristic different from ℓ. In the presence of sufficiently many roots of unity, we show how to recover much of the decomposition/inertia structure of valuations in the $\mathbb{Z}/\ell^n$-elementary abelian Galois group of K, while using only the group-theoretical structure of the $\mathbb{Z}/\ell^N$-abelian-by-central Galois group of K whenever N is sufficiently large with respect to n. Moreover, if $n = 1$ then $N = 1$ suffices, while if $n \neq \infty$, we provide an *explicit* $N_0 \neq \infty$, as a function of n and ℓ, for which all $N \geq N_0$ suffice above. In the process, we give a complete classification of so-called "commuting-liftable subgroups" of elementary-abelian Galois groups and prove that they always arise from valuations.

Contents

Chapter 1

Introduction

What information is encoded in Galois groups? This question is at the origins of anabelian geometry. Several results in the subject suggest that, in many special but important cases, the answer is "everything" when one deals with all of the Galois-theoretical information. For instance, the celebrated Neukirch-Uchida-Iwasawa-Pop theorem [Neu69b], [Neu69a], [Uch76], [Pop94], [Pop00] shows that an infinite field K which is finitely generated over its prime subfield is completely characterized by its absolute Galois group $G_K = \mathrm{Gal}(\bar{K}|K)$. These results form the birational portion of a collection of conjectures proposed by Grothendieck in his famous letter to Faltings [Gro97]. Grothendieck's vision was that certain objects (varieties resp. function fields, etc.) should be completely determined by their Galois theory (étale fundamental group resp. absolute Galois group, etc.), and thus dubbed **anabelian**, when there is **sufficiently rich** interplay between the arithmetic and geometric

portions of the Galois group.

Going beyond Grothendieck's original intuition, in the early 1990's Bogomolov [Bog91] introduced a program whose final goal is to reconstruct function fields of **purely geometric nature** (i.e. function fields over an algebraically closed field of transcendence degree ≥ 2) from **almost-abelian** pro-ℓ Galois-theoretical information. This program has since been carried through for function fields over the algebraic closure of a finite field by Bogomolov-Tschinkel [BT08] in dimension 2 and by Pop [Pop12] in general. Bogomolov's program suggests that the birational geometry of such geometric function fields should be encoded even in very small Galois groups. If successful, this program would go far beyond Grothendieck's original birational anabelian philosophy – see [Sza04] for more on the connection between Bogomolov's program and Grothendieck's birational anabelian geometry.

While one cannot expect analogous results to hold true for arbitrary fields as there are many non-isomorphic fields which have isomorphic absolute Galois groups, one can still recover much of the arithmetic/geometric information of the base-field using Galois theory. For instance, essentially all of the information about the structure of valuations of a field is encoded in its absolute Galois group (see [Koe03]). Actually, such results which detect valuations, called the "local-theory," are the essential first step in the birational anabelian results mentioned above. On the other hand, in light of Bogomolov's program among other results, current trends in the literature suggest that these so-called "almost-abelian" Galois groups play

an essential role in encoding various important properties of a field. The purpose of this thesis is to develop a theory which recovers valuations using almost-abelian Galois groups in arbitrary situations.

1.1 Local Theories

The first key step in most strategies towards anabelian geometry is to develop a **local theory**, by which one recovers inertia and/or decomposition groups of "points" using the given Galois theoretic information. In the context of anabelian curves, for example, one should eventually detect decomposition groups of closed points of the given curve within its étale fundamental group. On the other hand, in the birational setting, which is the focus of the present work, this corresponds to detecting decomposition groups of arithmetically and/or geometrically meaningful places of the function field under discussion within its Galois groups.

The first instance of a local theory is the famous Artin-Shreier theorem from the 1920's which relates torsion elements of absolute Galois groups to orderings of a field; this theorem is considered by many to be the first result in birational anabelian geometry. On the other hand, the first local-theory involving valuations is Neukirch's group-theoretical characterization of decomposition groups of finite places of global fields [Neu69b]. This was the basis for the celebrated Neukirch-Uchida-Iwasawa theorem mentioned above. The Neukirch-Uchida-Iwasawa theorem was expanded by Pop to all higher dimensional finitely generated fields by developing a local-theory

based on his q-Lemma [Pop94], [Pop00]. The q-Lemma deals with the **absolute pro-q Galois theory** of fields – dealing with q-Sylow subgroups of absolute Galois groups – and, as with Neukirch's result, works only in arithmetical situations.

On the other hand, at about the same time, two non-arithmetically based methods were proposed for detecting valuations. The first approach uses the theory of rigid elements which was first introduced by Ware [War81] in the context of quadratic forms and further developed by many including [AEJ87], [Koe95], [Efr99] in the context of valuation theory. Rigid elements have since been used in Galois theoretical settings to detect valuations using Galois groups. In the pro-ℓ case, one can detect inertia/decomposition groups of ℓ-tamely branching valuations of almost arbitrary fields using the **full pro-ℓ Galois group** as the input – see [EN94], [Efr95] for the pro-2 situation and [EK98] for the pro-ℓ situation with $\ell \neq 2$. Moreover, using rigid elements one can also detect inertia/decomposition groups associated to almost arbitrary valuations of arbitrary fields using the **absolute Galois group** as the input [Koe03]. The main benefit of this approach is that it works for **arbitrary fields** (which contain sufficiently many roots of unity in the pro-ℓ case); the draw-back is that the input – the full pro-ℓ Galois group resp. absolute Galois group of a field – is completely unapproachable in terms calculation except for very few exceptional cases (see [Koe98]).

The second approach is Bogomolov's theory of commuting liftable pairs in Galois groups which was first proposed in [Bog91] and further developed together with

Tschinkel in [BT02]. The benefit of this theory is that it requires certain **"almost-abelian" pro-ℓ Galois groups** as its input, which are far more computable in comparison with the full pro-ℓ Galois group; however, this theory only works for fields which **contain an algebraically closed subfield**. Nevertheless, this theory was a key technical tool in the local theory needed to settle Bogomolov's program in birational anabelian geometry for function fields over the algebraic closure of finite fields – see Bogomolov-Tschinkel [BT08] in dimension 2 and Pop [Pop10b],[Pop12] in general.

Until now, the two approaches – that of rigid elements versus that of commuting-liftable pairs – remained almost completely separate in the literature, with a few notable exceptions. Pop suggested in his Oberwolfach report [Pop06a] that the two methods should be linked, even in the analogous $(\mathbb{Z}/\ell^n)$-abelian-by-central situation, but unfortunately never followed up with the details. Also, the work done by Mahé,Ináč and Smith [MMS04] in the $(\mathbb{Z}/2)$-abelian-by-central situation, and Efrat-Ináč [EM11b] in special cases of the $(\mathbb{Z}/\ell)$-abelian-by-central situation suggest a connection between the two methods in this analogous context.

The purpose of this thesis is to provide an approach which unifies the method of commuting pairs with the method of rigid elements. At the same time, we provide simpler arguments for the pro-ℓ abelian-by-central assertions of [BT02], and prove more general versions of these assertions which assume only that the field contains μ_{ℓ^∞} and not necessarily an algebraically closed subfield as required by [BT02]. Our

theory also generalizes many of the Galois-theoretical results arising from the theory of rigid elements. The following Main Theorem is a summary of the more detailed Theorems 1.4.1 and 1.4.2.

Main Theorem. *Let $n \geq 1$ or $n = \infty$ be given. Then there exists an explicit function $\mathbf{R}(n)$ taking values in $\{1, 2, \ldots, \infty\}$ and satisfying: $\mathbf{R}(1) = 1$, $\mathbf{R}(n) \geq n$, and $\mathbf{R}(n) \neq \infty$ if $n \neq \infty$, so that for all $N \geq \mathbf{R}(n)$ the following holds. Let K be a field such that $\operatorname{Char} K \neq \ell$ which contains $\mu_{2\ell^N}$. Then there is a group-theoretical recipe which recovers (minimized) inertia and decomposition subgroups in the maximal $\mathbb{Z}/\ell^n$-elementary-abelian Galois group of K using the group-theoretical structure encoded in the $\mathbb{Z}/\ell^N$-abelian-by-central Galois group of K.*

1.2 Overview

We now give a brief overview of the two local-theories mentioned above. Let K be a field with $\operatorname{Char} K \neq \ell$ which contains the ℓ^{th} roots of unity $\mu_\ell \subset K$. Denote by $K(\ell)$ the maximal pro-ℓ Galois extension of K (inside a chosen separable closure of K) so that $\mathcal{G}_K := \operatorname{Gal}(K(\ell)|K)$ is the maximal pro-ℓ quotient of the absolute Galois group G_K of K. Let w be a valuation of $K(\ell)$ and denote by $v = w|_K$ its restriction to K; denote by $k(w)$ the residue field of w and $k(v)$ the residue field of

v and assume that $\mathrm{Char}\, k(v) \neq \ell$. We denote by $T_{w|v} \leq Z_{w|v} \leq \mathcal{G}_K$ the inertia resp. decomposition subgroup of $w|v$ inside $\mathcal{G}_K$. Recall that $Z_{w|v}/T_{w|v} = \mathcal{G}_{k(v)}$ and that the canonical short exact sequence

$$1 \to T_{w|v} \to Z_{w|v} \to \mathcal{G}_{k(v)} \to 1$$

is split. Moreover, since $\mathrm{Char}\, k(v) \neq \ell$, $T_{w|v}$ is a free abelian pro-ℓ group of the same rank as $v(K^\times)/\ell$, and the action of $\mathcal{G}_{k(v)}$ on $T_{w|v}$ factors via the ℓ-adic cyclotomic character. Thus, if $\sigma \in T_{w|v}$, $\tau \in Z_{w|v}$ are given non-torsion elements so that the closed subgroup $\langle \sigma, \tau \rangle$ is non-pro-cyclic, then $\langle \sigma, \tau \rangle = \langle \sigma \rangle \rtimes \langle \tau \rangle \cong \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell$ is a semi-direct product. Here and throughout we denote by $\langle S \rangle$ the closed subgroup generated by S.

Rigid elements were first considered by Ware [War81] in the context of quadratic forms, then further developed in the context of valuation theory and/or Galois theory by Arason-Elman-Jacob in [AEJ87], Engler-Nogueria in [EN94], Koenigsmann in [Koe95], Engler-Koenigsmann in [EK98], Efrat in [Efr95], [Efr99], [Efr07] and also by others. In a few words, the theory of rigid elements in the context of pro-ℓ Galois groups (as in [EN94], [Efr95], [EK98]) asserts that the only way the situation in the previous paragraph can arise is from valuation theory. More precisely, let K be a field such that $\mathrm{Char}\, K \neq \ell$ and $\mu_\ell \subset K$. If $\sigma, \tau \in \mathcal{G}_K$ are non-torsion elements such that $\langle \sigma, \tau \rangle = \langle \sigma \rangle \rtimes \langle \tau \rangle$ is non-pro-cyclic, then there exists a valuation w of $K(\ell)$ such that, denoting $v = w|_K$, one has $\mathrm{Char}\, k(v) \neq \ell$, $v(K^\times) \neq v(K^{\times \ell})$, $\sigma, \tau \in Z_{w|v}$ and $\langle \sigma, \tau \rangle / (\langle \sigma, \tau \rangle \cap T_{w|v})$ is cyclic. The key technique in this situation

is the explicit "creation" of valuation rings inside K using rigid elements and so-called "ℓ-rigid calculus" developed, for instance, in [Koe95] and/or [Efr99]. Indeed, under the assumption that $\mathcal{G}_K = \langle \sigma, \tau \rangle = \langle \sigma \rangle \rtimes \langle \tau \rangle$ as above, one shows that K has sufficiently many "strongly-rigid elements" to produce an ℓ-Henselian valuation v of K with $v(K^\times) \neq v(K^{\times \ell})$ and $\mathrm{Char}\, k(v) \neq \ell$.

Assume, on the other hand, that $\mu_{\ell^\infty} \subset K$. In this case, we denote by

$$\Pi_K^a := \frac{\mathcal{G}_K}{[\mathcal{G}_K, \mathcal{G}_K]}, \quad \text{and} \quad \Pi_K^c := \frac{\mathcal{G}_K}{[\mathcal{G}_K, [\mathcal{G}_K, \mathcal{G}_K]]}$$

the maximal pro-ℓ abelian resp. maximal pro-ℓ abelian-by-central Galois groups of K; this terminology and notation was introduced by Pop [Pop10b]. In the above context, assume again that $\mathrm{Char}\, k(v) \neq \ell$, then the ℓ-adic cyclotomic character of K (and of $k(v)$) is trivial. Hence, $\mathcal{G}_{k(v)}$ acts trivially on $T_{w|v}$; we conclude that $Z_{w|v} \cong T_{w|v} \times \mathcal{G}_{k(v)}$ and recall that $T_{w|v}$ is abelian. Denote by K^{ab} the Galois extension of K such that $\mathrm{Gal}(K^{ab}|K) = \Pi_K^a$, $v^{ab} := w|_{K^{ab}}$, $T_v := T_{v^{ab}|v}$ and $Z_v := Z_{v^{ab}|v}$; since Π_K^a is abelian, T_v and Z_v are independent of choice of w. We deduce that for all $\sigma \in T_v$ and $\tau \in Z_v$, there exist lifts $\tilde{\sigma}, \tilde{\tau} \in \Pi_K^c$ of $\sigma, \tau \in \Pi_K^a$ which commute in Π_K^c; since Π_K^c is a central extension of Π_K^a, we conclude that *any lifts* $\tilde{\sigma}, \tilde{\tau} \in \Pi_K^c$ of $\sigma, \tau \in \Pi_K^a$ commute as well – such a pair $\sigma, \tau \in \Pi_K^a$ is called **commuting-liftable**.

Bogomolov and Tschinkel's theory of commuting-liftable pairs [BT02] asserts that, under the added assumption that K contains an algebraically closed subfield $k = \bar{k}$, the only way a commuting pair can arise is via a valuation as described

above.[1] The method of loc.cit. uses the notion of a "flag function;" in particular, this is a homomorphism $K^\times \to \mathbb{Z}_\ell$ which corresponds, via Kummer theory, to an element in T_v for some valuation v. One then considers $\sigma, \tau \in \Pi_K^a$ as elements of $\mathrm{Hom}(K^\times, \mathbb{Z}_\ell) = \mathrm{Hom}(K^\times/k^\times, \mathbb{Z}_\ell)$ via Kummer theory, and produces the corresponding map:

$$\Psi = (\sigma, \tau) : K^\times/k^\times \to \mathbb{Z}_\ell^2 \subset \mathbb{A}^2(\mathbb{Q}_\ell).$$

When one views $K^\times/k^\times = \mathbb{P}_k(K)$ as an infinite dimensional projective space over k, the assumption that σ, τ are a commuting-liftable-pair ensures that Ψ sends **projective lines** to **affine lines**. This severe restriction on Ψ is then used to show that some $\mathbb{Z}_\ell$-linear combination of σ and τ is a flag function.

As mentioned above, the theory of commuting-liftable pairs was originally outlined by Bogomolov in [Bog91], where he also introduced a program in birational anabelian geometry for fields of purely geometric nature – i.e. function fields over an algebraically closed field of characteristic different from ℓ and dimension ≥ 2 – which aims to reconstruct such function fields K from the Galois group Π_K^c. If $\mathrm{Char}\, K > 0$, the above technical theorem eventually allows one to detect the decomposition and inertia subgroups of **quasi-divisorial valuations** inside Π_K^a using the group-theoretical structure encoded in Π_K^c (see Pop [Pop10b]). In particular, for

[1] It turns out that $\mathrm{Char}\, k(v) \neq \ell$ is not needed in order to produce a commuting-liftable pair, under a modified notion of decomposition and inertia. It turns out that valuations with residue characteristic equal to ℓ can and do arise from commuting-liftable pairs, as we will see in this thesis.

function fields K over the algebraic closure of a finite field, one can detect the decomposition/inertia structure of **divisorial valuations** inside Π_K^a using Π_K^c. While Bogomolov's program in its full generality is far from being complete, it has been carried through for function fields $K|k$, $k = \overline{\mathbb{F}}_p$ over the algebraic closure of a finite field by using Bogomolov's theory of commuting-liftable pairs to develop the local theory (see [BT02] and [Pop11] for more on the local theory).

In this thesis, we obtain analogous results to those in the theory of commuting-liftable pairs, for the $(\mathbb{Z}/\ell^n)$-abelian-by-central and the pro-ℓ-abelian-by-central situations, by elaborating on and using the theory of rigid elements, while working under less restrictive assumptions than Bogomolov and Tschinkel's approach. We now begin by introducing some technical assumptions and notation.

1.3 Notation

For the remainder of the discussion, ℓ will denote a fixed prime. A "subgroup" in the context of profinite groups will always mean a closed subgroup, and all homomorphisms we consider will be continuous. For an abelian group A, we will denote by $\widehat{A}$ the ℓ-adic completion of A; namely:

$$\widehat{A} := \lim_n A/\ell^n.$$

To simplify the notation somewhat, for a field F we will denote by $\widehat{F} = \widehat{F^\times}$, the ℓ-adic completion of $F^\times$.

Let K be a field whose characteristic is different from ℓ. Let n denote either a positive integer or $n = \infty$ and assume that $\mu_{2\ell^n} \subset K$. In this case, we denote by $\mathcal{G}_K^{a,n}$ the maximal $(\mathbb{Z}/\ell^n)$-abelian (resp. pro-ℓ abelian if $n = \infty$) and $\mathcal{G}_K^{c,n}$ the maximal $(\mathbb{Z}/\ell^n)$-abelian-by-central (resp. pro-ℓ-abelian-by-central) Galois groups of K. Explicitly, denote by $\mathcal{G}_K^{(2,n)} := [\mathcal{G}_K, \mathcal{G}_K] \cdot (\mathcal{G}_K)^{\ell^n}$ and $\mathcal{G}_K^{(3,n)} = [\mathcal{G}_K, \mathcal{G}_K^{(2,n)}] \cdot (\mathcal{G}_K^{(2,n)})^{\ell^n}$, then

$$\mathcal{G}_K^{a,n} := \mathcal{G}_K / \mathcal{G}_K^{(2,n)}, \quad \text{and} \quad \mathcal{G}_K^{c,n} := \mathcal{G}_K / \mathcal{G}_K^{(3,n)}.$$

The canonical projection $\Pi : \mathcal{G}_K^{c,n} \twoheadrightarrow \mathcal{G}_K^{a,n}$ induces the following maps; we denote $\ker \Pi$ additively. First, $[\bullet, \bullet] : \mathcal{G}_K^{a,n} \times \mathcal{G}_K^{a,n} \to \ker \Pi$ defined by $[\sigma, \tau] = \tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}$ where $\tilde{\sigma}, \tilde{\tau} \in \mathcal{G}_K^{c,n}$ are some lifts of $\sigma, \tau \in \mathcal{G}_K^{a,n}$; since Π is a central extension, this is well-defined and bilinear. Second, $(\bullet)^\pi : \mathcal{G}_K^{a,n} \to \ker \Pi$ defined by $\sigma^\pi = \tilde{\sigma}^{\ell^n}$ (resp. $\sigma^\pi = 0$ if $n = \infty$) where, again, $\tilde{\sigma} \in \mathcal{G}_K^{c,n}$ is some lift of $\sigma \in \mathcal{G}_K^{a,n}$; since Π is a central extension with kernel killed by ℓ^n, this map is well defined and, if $\ell \neq 2$, this map is linear. We will furthermore denote by $\sigma^\beta = 2 \cdot \sigma^\pi$, thus $(\bullet)^\beta$ is a linear map $\mathcal{G}_K^{a,n} \to \ker \Pi$ regardless of ℓ.

A pair of elements $\sigma, \tau \in \mathcal{G}_K^{a,n}$ will be called a **commuting-liftable** pair (or a **CL-pair** for short) provided that $[\sigma, \tau] \in \langle \sigma^\beta, \tau^\beta \rangle$. Our definition of a CL-pair diverges from Bogomolov-Tschinkel's definition since we must account for situations where the cyclotomic character is non-trivial; in fact, if $\mu_{\ell^\infty} \subset K$, our notion of a CL-pair agrees with Bogomolov and Tschinkel's. For a (closed) subgroup $A \leq \mathcal{G}_K^{a,n}$,

we denote by

$$\mathbf{I}^{\mathrm{CL}}(A) = \{\sigma \in A \ : \ \forall \tau \in A, \ [\sigma, \tau] \in \langle \sigma^{\beta}, \tau^{\beta} \rangle\}.$$

Then $\mathbf{I}^{\mathrm{CL}}(A)$ is a subgroup[2] of A; the group $\mathbf{I}^{\mathrm{CL}}(A)$ is the so-called "commuting-liftable-center" of A.

Remark 1.3.1. Let K be a field such that $\operatorname{Char} K \neq \ell$ and $\mu_{2\ell} \subset K$, and let $A \leq \mathcal{G}_K^{a,1}$ be given. In this case, we can give an alternative definition for $\mathbf{I}^{\mathrm{CL}}(A)$ which is the same definition given in [Top12]. Using this alternative definition, our main results generalize the situation of [EM11b]. Namely, for $A \leq \mathcal{G}_K^{a,1}$ one has $\mathbf{I}^{\mathrm{CL}}(A) = \{\sigma \in A \ : \ \forall \tau \in A, \ [\sigma, \tau] \in A^{\beta}\}$. See Remark 12.0.4 for the proof of this equivalence.

Suppose v is a valuation of K. We will denote by $\Gamma_v = v(K^{\times})$ the value group, $\mathcal{O}_v$ the valuation ring with valuation ideal $\mathfrak{m}_v$, and $k(v) = \mathcal{O}_v/\mathfrak{m}_v$ the residue field of v. We reserve the notation $U_v = \mathcal{O}_v^{\times}$ for the v-units and $U_v^1 = 1 + \mathfrak{m}_v$ for the v-principal units. We denote by $K^{a,n} = K(\sqrt[\ell^n]{K})$ the Galois extension of K such that $\mathrm{Gal}(K^{a,n}|K) = \mathcal{G}_K^{a,n}$, and pick a prolongation v' of v to $K^{a,n}$. We denote by $T_v^n := T_{v'|v}$ and $Z_v^n = Z_{v'|v}$ the decomposition and inertia subgroups of $v'|v$ inside $\mathcal{G}_K^{a,n}$; since $\mathcal{G}_K^{a,n}$ is abelian, these groups are independent of choice of v'. Moreover,

[2]This is not immediate if $n \neq \infty$, but follows from Theorem 12.0.2. See also Remark 1.3.1 and/or 12.0.4 for the case $n = 1$. See also Proposition 13.0.8 alongside the main results of the paper to see that this definition of $\mathbf{I}^{\mathrm{CL}}$ is indeed sufficient in the context of valuation theory.

we introduce the **minimized** decomposition and inertia subgroups:

$$D_v^n := \mathrm{Gal}(K^{a,n}|K(\sqrt[\ell^n]{U_v^1})), \quad \text{and} \quad I_v^n := \mathrm{Gal}(K^{a,n}|K(\sqrt[\ell^n]{U_v})).$$

Observe that $I_v^n \leq D_v^n$; more importantly, however, $I_v^n \leq T_v^n$ and $D_v^n \leq Z_v^n$ with equality whenever $\mathrm{Char}\, k(v) \neq \ell$ (see Proposition 13.0.6). It turns out that the minimized inertia and decomposition groups, $I_v^n \leq D_v^n$, have an abelian-by-central Galois theoretical structure which resembles that of the usual inertia and decomposition, even for valuations whose residue characteristic is ℓ; see Proposition 13.0.8 for the details. In particular, for any valuation v of K, one has $I_v^n \leq \mathbf{I}^{\mathrm{CL}}(D_v^n)$ regardless of $\mathrm{Char}\, k(v)$, just as $T_v^n \leq \mathbf{I}^{\mathrm{CL}}(Z_v^n)$ for v with $\mathrm{Char}\, k(v) \neq \ell$ as discussed above.

We denote by $\mathcal{W}_{K,n}$ the collection of valuations v of K which satisfy the following conditions:

1. Γ_v contains no non-trivial ℓ-divisible convex subgroups.

2. v is maximal among all valuations w such that $D_v^n = D_w^n$ and Γ_w contains no non-trivial ℓ-divisible convex subgroups; i.e. for all refinements w of v such that $D_w^n = D_v^n$ as subgroups of $\mathcal{G}_K^{a,n}$, one has $I_w^n = I_v^n$.

Furthermore, denote by $\mathcal{V}_{K,n}$ the subset of valuations $v \in \mathcal{W}_{K,n}$ such that $k(v)^\times/\ell^n$ (resp. $\widehat{k(v)}$ if $n = \infty$) is non-cyclic. It turns out that many valuations of interest are contained in $\mathcal{W}_{K,n}$. For instance, if K is a function field over an algebraically closed field k, then all Parshin chains of divisors are contained in $\mathcal{W}_{K,n}$ and, if

the transcendence degree of $K|k$ is ≥ 2, then those Parshin chains of non-maximal length are contained in $\mathcal{V}_{K,n}$ (this is also true when k is a "strongly" ℓ-closed field – see Example 8.1.2).

Remark 1.3.2. Using the results of this thesis, we can give an alternative equivalent definition for $\mathcal{V}_{K,n}$, in the case where $\operatorname{Char} K \neq \ell$ and $\mu_{2\ell^n} \subset K$, which is much easier to describe – see Lemma 8.2.6 and Theorem 12.0.2. $\mathcal{V}_{K,n}$ is precisely the collection of valuations v of K such that:

1. Γ_v contains no non-trivial ℓ-divisible convex subgroups.

2. $I_v^1 = \mathbf{I}^{\mathrm{CL}}(D_v^1) \neq D_v^1$.

In particular, we see that $\mathcal{V}_{K,m} = \mathcal{V}_{K,n}$ for all $m \leq n$.

In a similar way, we will denote by $\mathcal{V}'_{K,n}$ the collection of valuations v of K which satisfy the following conditions:

1. $\operatorname{Char} k(v) \neq \ell$.

2. Γ_v contains no non-trivial ℓ-divisible convex subgroups.

3. v is maximal among all valuations w such that $\operatorname{Char} k(w) \neq \ell$, $D_v^n = D_w^n$ and Γ_w contains no non-trivial ℓ-divisible convex subgroups; i.e. for all refinements w of v such that $\operatorname{Char} k(w) \neq \ell$ and $D_w^n = D_v^n$ as subgroups of $\mathcal{G}_K^{a,n}$, one has $I_w^n = I_v^n$.

4. $\mathcal{G}_{k(v)}^{a,n}$ is non-cyclic.

Observe that any valuation $v \in \mathcal{V}_{K,n}$, whose residue characteristic is different from ℓ, lies in $\mathcal{V}'_{K,n}$. Moreover, note that $\mathcal{V}_{K,n} = \mathcal{V}'_{K,n}$ provided that $\operatorname{Char} K > 0$. In general, however, the two sets are quite different.

Denote by $\mathbb{N}$ the collection of positive integers and $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$; we declare that $\infty > n$ for all $n \in \mathbb{N}$. If $N \geq n$ and $\mu_{\ell^N} \subset K$, we will denote the canonical map $\mathcal{G}_K^{a,N} \to \mathcal{G}_K^{a,n}$ by $f \mapsto f_n$. Furthermore, for an extension $L|K$ of fields, we will denote by $f \mapsto f_K$ the canonical map $\mathcal{G}_L^{a,n} \to \mathcal{G}_K^{a,n}$. These two maps commute: $(f_n)_K = (f_K)_n$.

1.4 Main Results

The main goal of this thesis is to produce a function $\mathbf{R} : \overline{\mathbb{N}} \to \overline{\mathbb{N}}$, satisfying the following conditions:

- If $n \in \mathbb{N}$ then $\mathbf{R}(n) \in \mathbb{N}$.
- $\mathbf{R}(1) = 1$ and $\mathbf{R}(\infty) = \infty$.
- $\mathbf{R}(n) \geq n$ for all $n \in \overline{\mathbb{N}}$.

so that Theorems 1.4.1 and 1.4.2 below hold true. While we succeed to construct such a function $\mathbf{R}$ (in the notation introduced in Part II, $\mathbf{R}(n) = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$ suffices), we do not expect that our function is optimal. However, the requirement that $\mathbf{R}(1) = 1$ and $\mathbf{R}(\infty) = \infty$ ensures that Theorems 1.4.1 and 1.4.2 include the main results of [Top12] and therefore also [BT02] as special cases. See also

Theorem 1.4.2 parts (1) and (2) along with Remark 1.3.1 in comparison with the main theorems of [EN94], [Efr95], [EK98], and also the main theorem of [EM11b]. In particular, our Theorem 1.4.2 generalizes these previous results in almost all cases.

Theorem 1.4.1. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{R}(n)$. Let K be a field such that* $\operatorname{Char} K \neq \ell$ *and $\mu_{2\ell^N} \subset K$.*

1. *Let $D \leq \mathcal{G}_K^{a,n}$ be given. Then there exists a valuation v of K such that $D \leq D_v^n$ and $D/(D \cap I_v^n)$ is cyclic if and only if there exists a CL-group $D' \leq \mathcal{G}_K^{a,N}$ such that $D'_n = D$.*

2. *Let $I \leq D \leq \mathcal{G}_K^{a,n}$ be given. Then there exists a valuation $v \in \mathcal{V}_{K,n}$ such that $I = I_v^n$ and $D = D_v^n$ if and only if the following hold:*

   (a) *There exist $D' \leq \mathcal{G}_K^{a,N}$ such that $(\mathbf{I}^{\mathrm{CL}}(D'))_n = I$ and $D'_n = D$.*

   (b) *$I \leq D \leq \mathcal{G}_K^{a,n}$ are maximal with this property – i.e. if $D \leq E \leq \mathcal{G}_K^{a,n}$ and $E' \leq \mathcal{G}_K^{a,N}$ is given such that $E'_n = E$ and $I \leq (\mathbf{I}^{\mathrm{CL}}(E'))_n$, then $D = E$ and $I = (\mathbf{I}^{\mathrm{CL}}(E'))_n$.*

   (c) *$\mathbf{I}^{\mathrm{CL}}(D) \neq D$ (i.e. D is not a CL-group).*

In particular, Theorem 1.4.1 part 2 provides a group theoretical recipe to detect $I_v^n \leq D_v^n$ for $v \in \mathcal{V}_{K,n}$ using only the group-theoretical structure of $\mathcal{G}_K^{c,N}$, whenever $\mu_{2\ell^N} \subset K$ where $N = \mathbf{R}(n)$.

By enlarging the group $\mathcal{G}_K^{c,N}$ we can detect which of those valuations v in the theorem above have residue characteristic different from ℓ. This therefore gives a group-theoretical recipe to detect the usual decomposition and inertia subgroups associated to valuations $v \in \mathcal{V}_{K,n}$ whose residue characteristic is different from ℓ.

Theorem 1.4.2. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{R}(n)$. Let K be a field such that $\operatorname{Char} K \neq \ell$ and $\mu_{2\ell^N} \subset K$.*

1. *Let $D \leq \mathcal{G}_K^{a,n}$ be given and denote by $L := (K^{a,n})^D$. Then there exists a valuation v of K such that $\operatorname{Char} k(v) \neq \ell$, $D \leq Z_v^n$ and $D/(D \cap T_v^n)$ is cyclic if and only if there exists a CL-group $D' \leq \mathcal{G}_L^{a,N}$ such that $(D'_n)_K = D$.*

2. *Assume that $\mathbf{I}^{\mathrm{CL}}(\mathcal{G}_K^{a,n}) \neq \mathcal{G}_K^{a,n}$ and consider $(\mathbf{I}^{\mathrm{CL}}(\mathcal{G}_K^{a,N}))_n =: T$. Then there exists a (possibly trivial) valuation $v \in \mathcal{V}_{K,n}$ such that $\operatorname{Char} k(v) \neq \ell$, $T = T_v^n$ and $\mathcal{G}_K^{a,n} = Z_v^n$.*

3. *Let $v \in \mathcal{V}_{K,n}$ be given and denote by $I := I_v^n \leq D_v^n =: D$, $L := (K^{a,n})^D$. Then $\operatorname{Char} k(v) \neq \ell$ if and only if there exist $I' \leq D' \leq \mathcal{G}_L^{a,N}$ such that:*

   (a) $I' \leq \mathbf{I}^{\mathrm{CL}}(D')$.

   (b) $(I'_n)_K = I$ and $(D'_n)_K = D$.

   Moreover, if these equivalent conditions hold then $I = I_v^n = T_v^n$ and $D = D_v^n = Z_v^n$.

4. *Let $I \leq D \leq \mathcal{G}_K^{a,n}$ be given and denote by $L := (K^{a,n})^D$. Then there exists a*

valuation $v \in \mathcal{V}'_{K,n}$ such that $I = T_v^n$ and $D = Z_v^n$ if and only if the following hold:

(a) There exist $D' \leq \mathcal{G}_L^{a,N}$ such that $((\mathbf{I}^{\mathrm{CL}}(D'))_n)_K = I$ and $(D'_n)_K = D$.

(b) $I \leq D \leq \mathcal{G}_K^{a,n}$ are maximal with this property – i.e. if $D \leq E \leq \mathcal{G}_K^{a,n}$ and $E' \leq \mathcal{G}_{L_E}^{a,N}$ (where $L_E := (K^{a,n})^E$) is given such that $(E'_n)_K = E$ and $I \leq ((\mathbf{I}^{\mathrm{CL}}(E'))_n)_K$, then $D = E$ and $I = ((\mathbf{I}^{\mathrm{CL}}(E'))_n)_K$.

(c) $\mathbf{I}^{\mathrm{CL}}(D) \neq D$ (i.e. D is not a CL-group).

Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{R}(n)$. Denote by $\mathcal{G}_K^{M,n}$ the smallest quotient of $\mathcal{G}_K$ for which $\mathcal{G}_L^{c,N}$ is a subquotient for all $K \subset L \subset K^{a,n}$. Therefore, Theorem 1.4.1 part 2 along with Theorem 1.4.2 part 3 provide a group-theoretical recipe to detect $T_v^n \leq Z_v^n$ for valuations $v \in \mathcal{V}_{K,n}$ such that $\mathrm{Char}\, k(v) \neq \ell$, using only the group-theoretical structure of $\mathcal{G}_K^{M,n}$. Moreover, part 4 of this theorem provides a group-theoretical recipe to detect $T_v^n \leq Z_v^n$ for valuations $v \in \mathcal{V}'_{K,n}$ using only the group-theoretical structure of $\mathcal{G}_K^{M,n}$.

1.5 A Guide Through the Thesis

In part I, we give an overview of valuation theory. We review the notions of coarsening/refinement of valuations and the approximation theorem. We also give a brief, but fairly comprehensive summary of decomposition theory of valuations and the theory of rigid elements. Finally, we review the construction of generalized Gauß

valuations which are certain special valuations of function fields; these valuations will play an important role providing some surprising examples and corollaries in Chapter 15.

In Part II, we develop the underlying theory which proves the main results of the paper. This theory works for an arbitrary field K, and is based on an abstract notion of "C-pairs" (Definition 6.0.6) which is related to a condition in the Milnor K-theory of the field (Proposition 10.2.1). The main theorem of this part, and perhaps the most important theorem in this thesis, is the "Main Theorem of C-Pairs" (Theorem 6.1.1) which relates our notion of C-pairs to restrictions on from rigid elements and thus on the corresponding valuations. We then deduce results which are analogous to the Theorems 1.4.1 and 1.4.2, but in the abstract setting of C-pairs – this is mostly all done in Section 8.2 and Chapter 9. Finally, we give our K-theoretic characterization of C-pairs which characterizes C-pairs using certain canonical quotients of Milnor K-theory (see Section 10.2). The main results in Part II, in particular, give a method to recover/detect valuations using mod-ℓ^n Milnor K-theory. Namely, one is able to recover the map $K^\times/\ell^n \to \Gamma_v/\ell^n$ induced by a valuation v using $K_*^M(K)/\ell^N$, for $N \geq \mathbf{R}(n)$.

In Part III, we provide the Galois-theoretic analogue of a C-pair using Kummer theory and the Merkurjev-Suslin theorem. More precisely, when we identify elements of $\mathcal{G}_K^{a,n}$ as homomorphisms from K to $\mathbb{Z}/\ell^n$ resp. $\mathbb{Z}_\ell$ using Kummer Theory, we prove that the abstract notion of a C-pair is equivalent to the notion of a CL-pair

(Definition 11.1.2) as defined above (see Theorem 12.0.2). The Main Theorems of the thesis, Theorems 1.4.1 and 1.4.2, are then a mere translation of the main results from Part II to the Galois-theoretical setting using the results of Part III. In Chapter 15, we prove the following corollary which provides a sufficient condition to detect whether or not $\operatorname{Char} K = 0$ using the Galois group $\mathcal{G}_K^{M,n}$:

Corollary 1.5.1. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{R}(n)$. Let K be a field such that $\operatorname{Char} K = 0$ and $\mu_{2\ell^N} \subset K$. Assume that there exists a field F such that $\operatorname{Char} F > 0$, $\mu_{2\ell^N} \subset F$ and $\mathcal{G}_K^{M,n} \cong \mathcal{G}_F^{M,n}$. Then for all $v \in \mathcal{V}_{K,n}$ one has $\operatorname{Char} k(v) \neq \ell$.*

As a consequence of this, we find many examples of fields K of characteristic 0 whose maximal pro-ℓ Galois group $\mathcal{G}_K$ is not isomorphic to $\mathcal{G}_F$ for any field F of positive characteristic (which also contains $\mu_{2\ell}$).

Corollary 1.5.2. *Suppose that K is one of the following:*

- *A function field over a number field k such that $\mu_{2\ell} \subset k$, and $\dim(K|k) \geq 1$.*
- *A function field over a strongly ℓ-closed[3] field k (e.g. k an algebraically closed field) of characteristic 0 such that $\dim(K|k) \geq 2$.*

Then there does not exist a field F such that $\mu_{2\ell} \subset F$, $\operatorname{Char} F > 0$ and $\mathcal{G}_K \cong \mathcal{G}_F$.

This is obtained by proving that, for K as in the corollary above, $\mathcal{V}_{K,1}$ contains a valuation whose residue characteristic is ℓ; it is here that we use the construction

[3]See Example 8.1.2 for the definition of a strongly ℓ-closed field.

of Chapter 5. Actually, such valuations exist in much more general situations than the two classes of examples above and thus many more examples exist. However, the two classes of examples above are of particular interest in birational anabelian geometry and so we've mentioned these explicitly.

To summarize, here is a sketch of the proofs of our main results (Theorems 1.4.1 and Theorem 1.4.2) along with the surrounding results of the thesis:

The Abstract Setting:

1. For a field K define $\mathcal{G}_K^a(n) = \mathrm{Hom}(K^\times/\pm 1, \mathbb{Z}/\ell^n)$ if $n \in \mathbb{N}$ resp. $\mathcal{G}_K^a(n) = \mathrm{Hom}(K^\times, \mathbb{Z}_\ell)$ if $n = \infty$. Two elements $\sigma, \tau \in \mathcal{G}_K^a(n)$ are called a C-pair provided that $\sigma(x)\tau(1-x) = \sigma(1-x)\tau(x)$ for all $x \neq 0, 1$.

2. If $\sigma, \tau \in \mathcal{G}_K^a(n)$ lift to a C-pair $\tilde{\sigma}, \tilde{\tau} \in \mathcal{G}_K^a(N)$ for $N \geq \mathbf{R}(n)$, then σ, τ come about from a valuation (Theorem 6.1). Conversely, valuations provide many C-pairs (Chapter 6).

3. In the presence of a certain configuration of C-pairs, the valuations which come about from the "Main Theorem of C-Pairs" are comparable (Chapter 7).

4. If K contains sufficiently many roots of unity, one has a supply of C-pairs which lift to C-pairs in $\mathcal{G}_K^a(N)$, for $N \geq \mathbf{R}(n)$, arising from valuations. This allows us to detect which elements of $\mathcal{G}_K^a(n)$ are trivial on U_v^1 and which

are trivial on U_v for v in a special class of valuations $\mathcal{V}_{K,n}$ (Section 8.2). We prove that $\mathcal{V}_{K,n}$ contains essentially all valuations of geometric origin (Example 8.1.2).

5. We then prove analogous results to those above which further restrict the residue characteristic to be different from ℓ provided that our given C-pairs lift to C-pairs in $\mathcal{G}_L^a(N)$ for $N\mathbf{R}(n)$ and for certain field extensions $L|K$ (Chapter 9).

6. Finally, we prove that $\sigma, \tau \in \mathcal{G}_K^a(n)$ form a C-pair if and only if the quotient $K_2^M(K)/\langle\{K^\times, T\}\rangle$ is sufficiently non-trivial, where $T = \ker\sigma \cap \ker\tau$ (see Proposition 10.2.1).

The Galois Theoretical Setting:

1. Here we deal with the situation where Char $K \neq \ell$ and K contains sufficiently many roots of unity. In this case, we identify $\mathcal{G}_K^{a,n}$ with $\mathcal{G}_K^a(n)$ using Kummer Theory. Under this isomorphism (which depends on a choice of isomorphism $\mu_{\ell^n} \cong \mathbb{Z}/\ell^n$), a C-pair maps to a CL-pair (see Definition 11.1.2 for the definition of CL-pairs and Theorem 12.0.2 for the equivalence of the two notions).

2. Theorem 1.4.1 is then a reformulation of the results of Section 8.2 using this equivalence (see Theorem 14.0.10).

3. The proof of Theorem 1.4.2 uses the equivalence of C-pairs with CL-pairs, along with the results of Chapter 9 and proofs similar to those in Section 8.2

(see Theorem 14.0.11).

4. Using Theorem 1.4.2 and/or 14.0.11, if $\mathcal{G}_K \cong \mathcal{G}_F$ for some field F of positive characteristic which contains sufficiently many roots of unity, then all valuations $v \in \mathcal{V}_{K,n}$ have residue characteristic different from ℓ. This is because $\operatorname{Char} F = \operatorname{Char} k(w)$ for all valuations w of F and thus, if $\operatorname{Char} F \neq \ell$, the equivalent conditions of Theorem 14.0.11 claim (3) always hold true.

5. Therefore, if $\mathcal{V}_{K,n}$ contains a valuation of residue characteristic ℓ (and thus $\operatorname{Char} K = 0$), then $\mathcal{G}_K \ncong \mathcal{G}_F$ for all such F; this is Corollary 15.0.12.

6. If K is a function field of transcendence degree ≥ 1 over a number field or a function field of transcendence degree ≥ 2 over an algebraically closed field (or, more generally, a strongly ℓ-closed field), then $\mathcal{V}_{K,n}$ contains a valuation of residue characteristic ℓ. The proof of this statement uses the argument from Example 8.1.2, along with the construction of so-called "generalized Gauß valuations" which are described in Chapter 5, to find a valuation $v \in \mathcal{V}_{K,n}$ whose residue characteristic is ℓ.

Part I

Valuation Theory

Chapter 2

Valuations of a Field

Let K be a field and $\mathcal{O} \subset K$ a subring. We say that $\mathcal{O}$ is a **valuation ring** provided that for all $x \in K^\times$ either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. It is easy to see from this definition that $\mathcal{O}$ is integrally closed in K. Indeed if $x \in K \smallsetminus \mathcal{O}$ then $x^{-1} \in \mathcal{O}$. Thus there cannot exist a monic equation in K:

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0, \quad a_i \in \mathcal{O}$$

for otherwise, multiplying the equation above by $x^{-(n-1)}$, we have

$$x = -a_1 + \cdots + x^{-(n-1)} a_n \in \mathcal{O}.$$

A **valuation** v of K is a surjective homomorphism $v : K^\times \to \Gamma_v$ onto a totally ordered abelian group Γ_v which satisfies the ultra-metric inequality:

$$v(x + y) \geq \min(v(x), v(y));$$

here and throughout we will formally set $v(0) = \infty > \Gamma_v$. If $v(x) < v(y)$ then

the ultra-metric inequality implies $v(x+y) = v(x)$; indeed if $v(x+y) > v(x)$ then $v(x) = v((x+y)-y) \geq \min(v(x+y), v(-y)) > v(x)$ which is absurd. To each valuation v of K we can associate a valuation ring $\mathcal{O}_v = \{x \in K \ : \ v(x) \geq 0\}$. We will say that two valuations v, w are **equivalent** provided that $\mathcal{O}_v = \mathcal{O}_w$. In the sequel, we will not distinguish between equivalent valuations.

Conversely, suppose that $\mathcal{O}$ is a valuation ring of K. Then we can construct a valuation $v_{\mathcal{O}} : K^\times \to K^\times/\mathcal{O}^\times =: \Gamma_{\mathcal{O}}$ where $\Gamma_{\mathcal{O}}$ is totally ordered by the rule: $a \cdot \mathcal{O}^\times \leq b \cdot \mathcal{O}^\times$ if and only if $b/a \in \mathcal{O}$. It is easy to see that the valuation ring associated to $v_{\mathcal{O}}$ is precisely $\mathcal{O}$ and thus there is a 1-1 correspondence between valuation rings of K and equivalence classes of valuations v of K.

A field K endowed with a valuation v will be called a **valued field** and denoted (K, v). From the discussion above, we see that $\mathcal{O}_v \smallsetminus \mathcal{O}_v^\times = \{x \in K \ : \ v(x) > 0\}$ is an ideal of $\mathcal{O}_v$; thus $\mathcal{O}_v$ is a local ring with unique maximal ideal $\mathfrak{m}_v = \{x \in K \ : \ v(x) > 0\}$. We call $\mathcal{O}_v$ the **valuation ring** associated to v, $\mathfrak{m}_v$ the **valuation ideal** of v, $\Gamma_v = v(K^\times) \cong K^\times/\mathcal{O}_v^\times$ the **value group** of v, and $k(v) = \mathcal{O}_v/\mathfrak{m}_v$ the **residue field** of v; for $x \in \mathcal{O}_v$ we will usually denote by $\bar{x}$ the image of x in $k(v)$. Also, we will sometimes denote by $k(v) = kv$ in places where the former notation is too cumbersome. The subset $U_v^1 := 1 + \mathfrak{m}_v$ is a multiplicative group of $U_v := \mathcal{O}_v^\times$; we call U_v^1 the **principal v-units** and U_v the **v-units** of v. These groups fit into two canonical short exact sequences:

1. $1 \to U_v \to K^\times \xrightarrow{v} \Gamma_v \to 1$

2. $1 \to U_v^1 \to U_v \xrightarrow{x \mapsto \bar{x}} k(v)^\times \to 1$

These short exact sequences will be of utmost importance later on, especially in their relationship with decomposition/inertia groups.

2.1 Coarsenings of Valuations

Let Γ be a totally ordered group. We say that a subgroup Δ of Γ is **convex** in Γ provided that for all $a, b \in \Delta$ and $\gamma \in \Gamma$ with $a \leq \gamma \leq b$, one has $\gamma \in \Delta$. Let (K, v) be a valued field and suppose Δ is a convex subgroup of Γ_v. Then the composition $v' : K^\times \xrightarrow{v} \Gamma_v \twoheadrightarrow \Gamma_v/\Delta =: \Gamma_{v'}$ is again a valuation of K. We see from the definition that $\mathcal{O}_{v'} \supset \mathcal{O}_v$. In fact, the set $\mathfrak{p}_\Delta := \{x \in K \ : \ v(x) > \Delta\}$ is a prime ideal of $\mathcal{O}_v$ and $\mathcal{O}_{v'} = (\mathcal{O}_v)_{\mathfrak{p}_\Delta}$ is the localization of $\mathcal{O}_v$ at this prime; it is easy to see that $\mathfrak{p}_\Delta = \mathfrak{m}_{v'}$.

On the other hand, any over-ring $\mathcal{O}_v \subset \mathcal{O}'$ with $\mathcal{O}' \subset K$ is a valuation ring of K (this is immediate from the definition of a valuation ring); say that v' is an associated valuation to $\mathcal{O}'$ so that $\mathcal{O}_{v'} = \mathcal{O}'$. Consider the surjective homomorphism $\Gamma_v = K^\times/U_v \to K^\times/U_{v'} = \Gamma_{v'}$; the kernel of this homomorphism must be a convex subgroup Δ of Γ_v as the map $\Gamma_v \twoheadrightarrow \Gamma_{v'}$ respects the ordering. And, denoting by $\mathfrak{p}_\Delta$ as above, we see again that $\mathcal{O}' = \mathcal{O}_{v'} = (\mathcal{O}_v)_{\mathfrak{p}_\Delta}$.

Lastly, given a prime ideal $\mathfrak{p}$ of $\mathcal{O}_v$, we can consider the over-ring $(\mathcal{O}_v)_\mathfrak{p} = \mathcal{O}_{v'}$. By considering the canonical surjective homomorphism $\Gamma_v \to \Gamma_{v'}$ as above with kernel Δ, we find that $\mathfrak{p}_\Delta = \mathfrak{p}$. Thus we obtain the following proposition:

Proposition 2.1.1. *Suppose that (K, v) is a valued field. Then there is a 1-1 correspondence between the following sets:*

1. *Convex subgroups Δ of Γ_v.*

2. *Prime ideals of $\mathcal{O}_v$.*

3. *Over-rings $\mathcal{O}' \supset \mathcal{O}_v$ contained in K.*

The correspondences are defined as follows:

1. *To a convex subgroup Δ, associated the prime ideal $\mathfrak{p}_\Delta = \{x \in K \ : \ v(x) > \Delta\}$ resp. the valuation ring associated to the valuation $v' : K^\times \xrightarrow{v} \Gamma_v \twoheadrightarrow \Gamma_v/\Delta =: \Gamma_{v'}$.*

2. *To a prime ideal $\mathfrak{p}$ of $\mathcal{O}_v$, associate the over-ring $(\mathcal{O}_v)_\mathfrak{p} =: \mathcal{O}_{v'}$ resp. the convex subgroup $\Delta = \ker(\Gamma_v \twoheadrightarrow \Gamma_{v'})$.*

3. *To an over-ring $\mathcal{O}_{v'} \supset \mathcal{O}_v$, associate the convex subgroup $\Delta = \ker(\Gamma_v \twoheadrightarrow \Gamma_{v'})$ resp. the prime ideal $\mathfrak{p} = \mathfrak{m}_{v'}$ (this is an ideal of $\mathcal{O}_v$).*

If w is a valuation of K with $\mathcal{O}_w \supset \mathcal{O}_v$ as above, we will say that w is a **coarsening** of v and write $w \leq v$. One easily finds that the following conditions are, in fact, equivalent:

1. w is a coarsening of v.

2. $U_v \subset U_w$.

3. $U_w^1 \subset U_v^1$.

Thus, if $w \leq v$, we obtain two short exact sequences:

1. $1 \to U_w/U_v \to \Gamma_v \to \Gamma_w \to 1$ and

2. $1 \to U_v^1/U_w^1 \to U_v/U_w^1 \to k(v)^\times \to 1$.

Of course, the field itself K is a valuation ring of K which is a coarsening of every other valuation of K; we call this valuation the trivial valuation and observe that its value group is $\{0\}$, its units are $K^\times$, its principal units are $\{1\}$ and its residue field is K.

One very important fact about coarsenings of a valuation v, is that they are *totally ordered*. In other words, if w_1, w_2 are two coarsenings of v then $w_1 \leq w_2$ or $w_2 \leq w_1$. This fact will be used again and again in the remainder of the discussion. To prove this property, by Proposition 2.1.1, it suffices to prove that the prime ideals of $\mathcal{O}_v$ are totally ordered, and we show this in the following proposition:

Proposition 2.1.2. *Let (K, v) be a valued field. Then any two ideals of $\mathcal{O}_v$ are comparable with respect to inclusion. In particular, any two elements of the following sets are comparable by Proposition 2.1.1:*

1. *Convex subgroups Δ of Γ_v.*

2. *Prime ideals of $\mathcal{O}_v$.*

3. *Over-rings $\mathcal{O}' \supset \mathcal{O}_v$ contained in K (and thus also coarsenings of v).*

Proof. Suppose $\mathfrak{a} = (a)$ and $\mathfrak{b} = (b)$ are principal ideals of $\mathcal{O}_v$. Since either $a/b \in \mathcal{O}_v$ or $b/a \in \mathcal{O}_v$ we see that either $a \in (b)$ or $b \in (a)$ and thus $(a) \subset (b)$ or $(b) \subset (a)$.

If $\mathfrak{a}$ and $\mathfrak{b}$ are arbitrary ideals with $b \in \mathfrak{b} \smallsetminus \mathfrak{a}$ and $a \in \mathfrak{a}$, then we must have $(a) \subset (b)$; the other option is $(b) \subset (a)$ which would imply that $b \in \mathfrak{a}$. Thus $\mathfrak{a} \subset \mathfrak{b}$. □

2.2 Compositions of Valuations

In the previous subsection, we saw how to coarsen valuations – i.e. make the value group *smaller*. In this subsection, we will see how to refine valuations – i.e. make the value group *bigger*.

Suppose that (K, v) is a valued field and w is a valuation of $k(v)$. Consider the subring $\mathcal{O}$ of $\mathcal{O}_v$ which is the pre-image of $\mathcal{O}_w \subset k(v)$ under the canonical projection $\mathcal{O}_v \to k(v)$. Then $\mathcal{O}$ is a valuation ring of K, and we denote by $w \circ v$ the associated valuation – this is called the **valuation-theoretic composition** of v and w. In fact, it is immediate that v is a coarsening of $w \circ v$ and the kernel Δ of the canonical projection $\Gamma_{w \circ v} \twoheadrightarrow \Gamma_v$ is canonically isomorphic to Γ_w; i.e. we obtain the following canonical short exact sequence of value groups:

$$0 \to \Gamma_w \to \Gamma_{w \circ v} \to \Gamma_v \to 0.$$

Conversely, if $\mathcal{O}_{v'} \subset \mathcal{O}_v$ is a subring which is also a valuation ring (whose associated valuation is v') then the image $\mathcal{O}_w$ of $\mathcal{O}_{v'}$ in $k(v)$ is again a valuation

ring (with associated valuation w). In this case, v' will be called a refinement of v (note that v is a coarsening of v'); we will write $v' \geq v$ and denote the induced valuation on $k(v)$ by v'/v. In particular, one has $v'/v \circ v = v'$, and the corresponding value groups fit into the following short exact sequence:

$$0 \to \Gamma_{v'/v} \to \Gamma_{v'} \to \Gamma_v \to 0.$$

We summarize the discussion in the following proposition:

Proposition 2.2.1. *Let (K, v) be a valued field. Then there is a 1-1 correspondence between refinements of v and the valuations w of $k(v)$ defined by sending a refinement v' of v to v/v' (defined above) resp. sending w to $w \circ v$ (defined above).*

Moreover, if v' is a refinement of v, then $k(v') = k(v'/v)$ and one has a canonical short exact sequence of ordered groups:

$$0 \to \Gamma_{v'/v} \to \Gamma'_v \to \Gamma_v \to 0.$$

Lastly, the coarsening of v' associated to $\Gamma_{v'/v}$, considered as a convex subgroup of $\Gamma_{v'}$ (see Proposition 2.1.1) is precisely v.

2.3 The Approximation Theorem

In this subsection we will recall the general analogue of a well-known result from basic number theory called the approximation theorem which deals with the p-adic absolute values resp. the Archemedian absolute values of a number field. We will

provide the statement of the theorem without proof, referring the reader to [EP05] Theorem 2.4.1 for the detailed proof.

Two valuations v, w of a field K are called **independent** provided that the finest common coarsening of v and w is the trivial valuation – i.e. K is generated, as a ring, by $\mathcal{O}_v$ and $\mathcal{O}_w$.

Theorem 2.3.1 (The Approximation Theorem for Independent Valuations)**.** *Suppose that $v_1, \cdots, v_m$ are pairwise independent valuations of a field K. Let $\gamma_i \in \Gamma_{v_i}$, $i = 1, \ldots, m$ be given and $a_1, \ldots, a_m \in K$. Then there exists $x \in K$ such that $v_i(x - a_i) > \gamma_i$ for all $i = 1, \ldots, m$.*

We explicitly state and prove the following corollary of the approximation theorem since it will be used later on.

Corollary 2.3.2. *Let v, w be two valuations of a field K. Then the following conditions are equivalent:*

1. *v, w are independent.*
2. *$U_v \cdot U_w = K^\times$.*
3. *$U_v^1 \cdot U_w^1 = K^\times$.*

Proof. The following implications are trivial: (3) $\Rightarrow$ (2) $\Rightarrow$ (1). Thus, it suffices to prove that (1) $\Rightarrow$ (3). We know from the approximation theorem that for any given $a \in K^\times$, there exists an x such that $v(x-1) > 0$ and $w(x-a) > w(a)$. Thus

$x \in U_v^1$ while $w(x/a - 1) > 0$ implies that $x/a \in U_w^1$. Thus $a/x \in U_w^1$ as well and so $a = x \cdot (a/x) \in U_v^1 \cdot U_w^1$. Therefore we see that $K^\times = U_v \cdot U_w = U_v^1 \cdot U_w^1$. $\square$

Chapter 3

Decomposition Theory of Valuations

Hilbert's Decomposition theory deals with the behavior of valuations in Galois extensions of valued fields. In this chapter, we will state many facts about decomposition, inertia and ramification groups of valuations which will be used later on, but this will be done without proof. The details behind all of these facts, most of which are in fact theorems, can be found in [ZS75] which is still, in the author's opinion, the best source for ramification theory of general valuations.

An extension of valued fields $(K, v) \subset (L, w)$ is an extension of the underlying fields $L|K$ so that $\mathcal{O}_v = K \cap \mathcal{O}_w$; alternatively, one has an embedding $\Gamma_v \subset \Gamma_w$ of value groups so that the restriction of $w : L^\times \to \Gamma_w$ to $K^\times$ is precisely $v : K^\times \to \Gamma_v$. In this case we will also say that w is a **prolongation** of v to $L|K$ and write $w|v$.

Observe that $U_w \cap K^\times = U_v$ and $\mathfrak{m}_w \cap K = \mathfrak{m}_v$; we thus obtain an extension of residue fields $k(w)|k(v)$ and, in particular, $U_w^1 \cap K = U_v^1$.

If $L|K$ is an algebraic extension and v is a valuation of K, we can describe all prolongations of v to L as follows. Consider the integral closure $\widetilde{\mathcal{O}}_v$ of $\mathcal{O}_v$ in $L|K$. Suppose $\mathfrak{m}$ is a maximal ideal of $\widetilde{\mathcal{O}}_v$ and that $\mathfrak{m} \cap \mathcal{O}_v = \mathfrak{m}_v$. Then the localization $(\widetilde{\mathcal{O}}_v)_{\mathfrak{m}}$ is a valuation ring of L which prolongs $\mathcal{O}_v$. Moreover, any prolongation of v to $L|K$ arises in this way. We will denote by $\mathfrak{X}_v(L)$ the prolongations of v to $L|K$ (as always, we identify equivalent valuations).

Suppose that $w \in \mathfrak{X}_v(L)$ and $\sigma \in \mathrm{Aut}(L|K)$. Then $w \circ \sigma$ is again a prolongation of v to $L|K$; we say that $w \circ \sigma$ is **conjugate** to w. It is easy to see that $\mathcal{O}_{w\circ\sigma} = \sigma^{-1}\mathcal{O}_w$ as subrings of L; indeed, $w(x) \geq 0$ iff $w \circ \sigma(\sigma^{-1}x) \geq 0$. In particular, we see that $\mathrm{Aut}(L|K)$ acts on $\mathfrak{X}_v(L)$.

3.1 General Decomposition Theory of Valuations

Suppose that $K'|K$ is a Galois extension, v is a valuation of K and $v' \in \mathfrak{X}_v(K')$ is fixed. Thus, in particular, $(K, v) \subset (K', v')$ is an extension of valued fields. We define the decomposition group of $v'|v$ to be:

$$Z_{v'|v} := \{\sigma \in \mathrm{Gal}(K'|K) \ : \ \sigma(\mathcal{O}_{v'}) = \mathcal{O}_{v'}\}$$

The extension $k(v')|k(v)$ is normal and, since $\sigma\mathfrak{m}_{v'} = \mathfrak{m}_{v'}$ for any $\sigma \in Z_{v'|v}$, such a σ induces a $k(v)$-automorphism of $k(v')$. Thus we obtain a canonical homomor-

phism $Z_{v'|v} \to \mathrm{Aut}(kv'|kv)$ which is known to be surjective. The kernel of this homomorphism is called the inertia group of $v'|v$ defined as:

$$T_{v'|v} = \{\sigma \in Z_{v'|v} \ : \ \forall x \in K', \ v'(\sigma x - x) > 0\}.$$

Thus we have a canonical short exact sequence

$$(\dagger) : \ 1 \to T_{v'|v} \to Z_{v'|v} \to \mathrm{Aut}(kv'|kv) \to 1.$$

Denote by $\mu(kv')$ the set of roots of unity inside $k(v')$. Then one has a canonical pairing:

$$\Psi_{v'|v} : T_{v'|v} \times \Gamma_{v'}/\Gamma_v \to \mu(kv')$$

which is defined by $(\sigma, v'(x)) \mapsto \overline{\sigma x/x}$. The right kernel of this pairing is trivial while the left kernel is the ramification group of $v'|v$ defined as:

$$V_{v'|v} = \{\sigma \in T_{v'|v} \ : \ \forall x \in K' \ v'(\sigma x - x) > v'(x)\}.$$

Denote by $p = \mathrm{Char}\, k(v) = \mathrm{Char}\, k(v')$. Then $V_{v'|v}$ is the unique Sylow-p-subgroup of $T_{v'|v}$ if $p \neq 0$ and $V_{v'|v}$ is trivial if $p = 0$; in fact, $V_{v'|v}$ is a normal subgroup of $Z_{v'|v}$. In other words, we see that $T_{v'|v}/V_{v'|v}$ is abelian and one has a perfect pairing $T_{v'|v}/V_{v'|v} \times \Gamma_{v'}/\Gamma_v \to \mu(kv')$. Moreover, the action of $\mathrm{Aut}(kv'|kv)$ is compatible with $\Psi_{v'|v}$ in the natural sense, and, in particular, the action of $\mathrm{Aut}(kv'|kv)$ on $T_{v'|v}/V_{v'|v}$ induced by $(\dagger)$ factors via the cyclotomic character $\mathrm{Aut}(kv'|kv) \to \mathrm{Aut}(kv(\mu(kv'))|kv)$.

Denote by K_Z resp. K_T resp. K_V the fixed field of $Z_{v'|v}$ resp. $T_{v'|v}$ resp. $V_{v'|v}$

of $K'|K$ and denote by v_Z resp. v_T resp. v_V the restriction of v' to K_Z resp. K_T resp. K_V. Then the following hold:

1. The following value groups are equal: $\Gamma_v = \Gamma_{v_Z} = \Gamma_{v_T}$.

2. $kv = kv_Z$ and $kv_T|kv_Z = kv_T|kv_Z$ is the maximal separable sub-extension of $kv'|kv = kv'|kv_Z$; thus $kv_T|kv_Z$ is Galois and $\mathrm{Aut}(kv'|kv) = \mathrm{Gal}(kv_T|kv_Z)$.

3. The extension $K_v|K_T$ is totally tamely ramified – namely $kv_V = kv_T$ and the p-primary component of $\Gamma_{v_V}/\Gamma_{v_T}$ is trivial.

As $K'|K$ is Galois, the action of $\mathrm{Gal}(K'|K)$ on $\mathfrak{X}_v(K')$ is transitive. As we've mentioned above, $V_{v'|v}$ and $T_{v'|v}$ are both normal subgroups of $Z_{v'|v}$. More precisely, we have the following fact about conjugation by elements of $\mathrm{Gal}(K'|K)$. Suppose that v'' is another element of $\mathfrak{X}_v(K')$ and say that $v'' = v' \circ \sigma$ (equivalently $\sigma(\mathcal{O}_{v''}) = \mathcal{O}_{v'}$ and/or $\sigma^{-1}(\mathcal{O}_{v'}) = \mathcal{O}_{v''}$). Then $\sigma Z_{v''|v}\sigma^{-1} = Z_{v'|v}$, $\sigma T_{v''|v}\sigma^{-1} = T_{v'|v}$ and $\sigma V_{v''|v}\sigma^{-1} = V_{v'|v}$.

3.2 Compatability Properties

Using the notation above, suppose that K_0 is a sub-extension of $K'|K$ and v_0 denotes the restriction of v' to K_0. Thus we have a tower of valued fields $(K, v) \subset (K_0, v_0) \subset (K', v')$. Then $Z_{v'|v} \cap \mathrm{Gal}(K'|K_0) = Z_{v'|v_0}$, $T_{v'|v} \cap \mathrm{Gal}(K'|K_0) = T_{v'|v_0}$ and $V_{v'|v} \cap \mathrm{Gal}(K'|K_0) = V_{v'|v_0}$. If moreover $K_0|K$ is Galois, then the restriction map

$\mathrm{Gal}(K'|K) \twoheadrightarrow \mathrm{Gal}(K_0|K)$ induces canonical surjective homomorphisms $Z_{v'|v} \twoheadrightarrow Z_{v_0|v}$, $T_{v'|v} \twoheadrightarrow T_{v_0|v}$ and $V_{v'|v} \twoheadrightarrow V_{v_0|v}$.

Suppose that w is a valuation of $k(v)$ and w' is a prolongation of w to $k(v')$; then $w' \circ v' =: v'_1$ is a prolongation of $w \circ v =: v_1$. One has the following canonical inclusion of subgroups of $\mathrm{Gal}(K'|K)$:

$$T_{v'|v} \leq T_{v'_1|v_1} \leq Z_{v'_1|v_1} \leq Z_{v'|v}.$$

Moreover, the image of $T_{v'_1|v_1}$ resp. $Z_{v'_1|v_1}$ under the canonical surjection $Z_{v'|v} \twoheadrightarrow \mathrm{Aut}(kv'|kv)$ is precisely $T_{w'|w}$ resp. $Z_{w'|w}$; here we define the decomposition/inertia for a normal extension (which may or may not be Galois) in the same way as for a Galois extension.

3.3 The Pro-ℓ Case

In this subsection we will investigate the pro-ℓ-abelian situation. So, let ℓ be a fixed prime and assume that $\mathrm{Char}\, K, \mathrm{Char}\, kv \neq \ell$ and $\mu_\ell \subset K$. Consider the maximal pro-ℓ extension $K(\ell)$ of K and denote the Galois group $\mathcal{G}_K = \mathrm{Gal}(K(\ell)|K)$. Choose a prolongation v_ℓ of v to $K(\ell)$. Then $k(v_\ell) = kv(\ell)$ and the corresponding short exact sequence (see (†)) is split:

$$1 \to T_{v_\ell|v} \to Z_{v_\ell|v} \to \mathcal{G}_{kv} \to 1.$$

Thus we can describe the structure of $Z_{v_\ell|v}$ in a very precise way: $Z_{v_\ell|v} \cong T_{v_\ell|v} \rtimes \mathcal{G}_{kv}$ where the action is given by the cyclotomic character of $\mathcal{G}_{kv}$ via the perfect pairing

$T_{v_\ell|v} \times \Gamma_{v_\ell}/\Gamma_v \to \mu_{\ell^\infty}$; note that $V_{v_\ell|v} = 1$ since $\operatorname{Char} kv \neq \ell$. In particular, $T_{v_\ell|v}$ is abelian, while if $\sigma \in T_{v_\ell|v}$ and $\tau \in Z_{v_\ell|v}$ then $\sigma^{-1}\tau^{-1}\sigma\tau = \sigma^a$ for some $a \in \ell \cdot \mathbb{Z}_\ell$; more precisely, $a = -1 - \chi(\bar{\tau})$ where $\bar{\tau}$ denotes the image of τ in $\mathcal{G}_{kv}$ and $\chi : \mathcal{G}_{kv} \to (1+\ell\cdot\mathbb{Z}_\ell)^\times$ denotes the cyclotomic character of $\mathcal{G}_{kv}$. We will use this fact later when describing the structure of inertia/decomposition in certain canonical quotients of $\mathcal{G}_K$.

Chapter 4

Rigid Elements

The theory of rigid elements describes minimal conditions for the existence of a valuation v in a field K with certain boundedness conditions for the units and principal units. Suppose that (K, v) is an arbitrary valued field, $T \leq H \leq K^\times$ are subgroups with $U_v^1 \leq T$ and $U_v \leq H$. Suppose $x \notin H$. If $v(x) > 0$ then $1 \pm x \in T$ while if $v(x) < 0$ then $1 \pm x \in x \cdot T$; thus $1 \pm x \in T \cup x \cdot T$. On the other hand, $x \cdot t \notin H$ for all $t \in T$ and thus $1 \pm x \cdot T \subset T \cup x \cdot T$; therefore:

$$T \pm x \cdot T \subset T \cup x \cdot T.$$

Suppose that $T \leq K^\times$ is an arbitrary subgroup and $H \leq K^\times$ is a subgroup which contains T as well as all $x \notin T$ for which $T \pm x \cdot T \not\subset T \cup x \cdot T$; in particular, if $x \notin H$ then $T \pm x \cdot T \subset T \cup x \cdot T$. The theory of rigid elements provides an explicit method for constructing a valuation v of K using such a $T \leq H$ in almost all cases. For such a $T \leq H$, define:

1. $\mathcal{O}^-(H,T) = \{x \in K \ : \ x \notin H \ \text{ and } \ 1+x \in T\}$.

2. $\mathcal{O}^+(H,T) = \{x \in K^\times \ : \ x \in H \ \text{ and } \ x \cdot \mathcal{O}(T,H)^- \subset \mathcal{O}^-(T,H)\}$.

3. $\mathcal{O}(H,T) = \mathcal{O}^-(T,H) \cup \mathcal{O}^+(T,H)$.

4. $U(H,T) = \{x \in \mathcal{O}^+(H,T) \ : \ x^{-1} \in \mathcal{O}^+(H,T)\}$.

The goal of this construction is for $\mathcal{O}(H,T)$ to be a valuation ring with unit group $U(H,T)$ and we'll see that many cases this actually works as intended. The idea is that H can be used to determine the relationship between the value of *certain* $x, y \in K^\times$. More precisely, if $x, y \in K^\times$ have different H-cosets, $x \cdot H \neq y \cdot H$, the resulting valuation v will satisfy $v(x) < v(y)$ iff $x+y \in x \cdot T$. In most situations, this provides enough information to define the valuation v and the construction above is the result of this procedure.

The following theorem is a general summary of the theory of rigid elements in the context of valuation theory. This theorem is essentially a reorganization of the main results of Arason-Elman-Jacob [AEJ87]. Since it is not immediately clear how one can derive these statements from loc.cit., this theorem will require some proof; in statement (2) below, loc.cit. proves the equivalence of (a) and (b) while the equivalence of (c) is not explicitly considered.

Theorem 4.0.1 (Arason-Elman-Jacob [AEJ87])**.** *Let K be an arbitrary field, and let $T \leq H \leq K^\times$ be given so that H contains all $x \notin T$ with $T \pm x \cdot T \not\subset T \cup x \cdot T$. Then the following hold:*

1. *If $\mathcal{O}(H,T)$ is a valuation ring, with associated valuation w, then $U_w^1 \leq T$, $U(H,T) = U_w$ and $U_w \leq H$.*

2. *The following conditions are equivalent:*

   (a) *$\mathcal{O}(H,T)$ is a valuation ring.*

   (b) *$1 + \mathcal{O}^-(H,T) \subset \mathcal{O}^+(H,T)$.*

   (c) *There exists some valuation v of K so that $U_v \leq H$ and $U_v^1 \leq T$.*

3. *There exists a $H \leq \widetilde{H}$ with $\#(\widetilde{H}/H) \leq 2$ so that $\mathcal{O}(\widetilde{H},T)$ is a valuation ring.*

4. *If there exists an $x \in H \smallsetminus T$ such that $T \pm x \cdot T \not\subset T \cup x \cdot T$, then $\mathcal{O}(H,T)$ is a valuation ring.*

5. *If there exists a valuation v of K so that $U_v^1 \leq T$ and $U_v \leq H$ then $\mathcal{O}_v \subset \mathcal{O}(H,T)$. In particular, denoting by w the valuation associated to $\mathcal{O}(H,T)$, w is a coarsening of v.*

Proof. To 1. This follows from Theorem 2.10, Remark 2.5 and Observation 2.3 (3) of [AEJ87].

To 2. $(a) \Leftrightarrow (b)$ is again Theorem 2.10 and Remark 2.5 of loc.cit.; $(b) \Rightarrow (c)$ follows from statement (1) along with Theorem 2.10 of loc.cit.. It remains to show that $(c) \Rightarrow (b)$. Observe that whenever $x \notin H$ then $v(x) \neq 0$ so that $1 + x \in T$ iff $v(x) > 0$ and $1 + x \in x \cdot T$ iff $v(x) < 0$. Suppose that $y \in \mathcal{O}^-(H,T)$; we need to show that $1 + y \in \mathcal{O}^+(H,T)$. I.e. we need to show that, if $x \in \mathcal{O}^-(H,T)$, then $(1 + y) \cdot x \in \mathcal{O}^-(H,T)$; equivalently, $1 + x \cdot (1 + y) \in T$.

So, let x, y be given as above. Then $x, y \in \mathcal{O}^-(H,T)$ and thus $v(x), v(y) > 0$. Now we see that $v(x \cdot (1+y)) = v(x) > 0$ so that $1 + x \cdot (1+y) \in U_v^1 \leq T$, as needed.

To 3. This is Theorem 2.16 of loc.cit..

To 4. This follows from Proposition 2.14 of loc.cit. (Proposition 2.14 of loc.cit. is actually stronger than we need).

To 5. It follows from the definitions immediately that $U_v \leq U(H,T)$. Thus, if $\mathcal{O}(H,T)$ is a valuation ring with associated valuation w then $U_v \leq U_w$ from statement (1). Thus $w \leq v$ and so $\mathcal{O}_v \subset \mathcal{O}_w$, as required. □

The following follows immediately from theorem above; this corollary unravels the definition/construction of $\mathcal{O}(H,T)$ above and attempts to axiomatize those subgroups H which contain the units of a valuation ring in the simplest possible way.

Corollary 4.0.2. *Let K be a field and let $H \leq K^\times$ be given. The following are equivalent:*

1. *There exists a valuation v of K such that $U_v \leq H$.*

2. *$-1 \in H$, for all $x \in K^\times \smallsetminus H$ one has $1 + x \in H \cup xH$, and whenever $x, y \in K^\times \smallsetminus H$ are such that $1 + x, 1 + y \in H$, one has $1 + x(1 + y) \in H$.*

Proof. First assume that there exists a valuation v such that $U_v \leq H$. Let $x \in K^\times \smallsetminus H$ be given. Then, in particular, $v(x) \neq 0$ and thus $1 + x \in U_v$ iff $v(x) > 0$;

also, $1 + x \in x \cdot U_v$ iff $v(x) < 0$. Thus $1 + x \in H \cup x \cdot H$ for all such x. Moreover, if $x, y \notin H$ and $1 + x, 1 + y \in H$ one has $v(x), v(y) > 0$ and thus, similarly to the proof of 4.0.1 (2), $v(x \cdot (1 + y)) > 0$ so that $1 + x(1 + y) \in H$ as required.

The converse, which is the non-trivial direction, follows from [AEJ87] Theorem 2.10 taking $T = H$ in loc.cit.. Using our summary in Theorem 4.0.1, this is precisely the equivalence of (b) and (a) of statement (2), in the situation where $H = T$ and $-1 \in H$. □

Remark 4.0.3. In the case where $K^{\times \ell^n} \leq H$ and ℓ is odd, the condition of Corollary 4.0.2 can be made simpler. Using the notation of Corollary 4.0.2, the following are equivalent in this case:

1. There exists a valuation v of K such that $U_v \leq H$.

2. For all $x \in K^\times \smallsetminus H$ one has $1 + x \in H \cup xH$.

Again, see [AEJ87] Theorem 2.10 and/or our summary in Theorem 4.0.1 for the proof of the non-trivial direction of this claim.

Chapter 5

Generalized Gauß Valuations

In this chapter we will recall the classical construction of generalized Gauß valuations and their relationship with geometry. The valuations constructed below are very special as so-called "valuations with no relative defect." For the purposes of the rest of the work, we will not require a discussion of relative-defect in general so we will refer the interested reader to the appendix of Pop [Pop06b]; below, we also use the notation of loc.cit..

Let K be a function field over k, assume that k is relatively algebraically closed in K, and say v_0 is a valuation of k. Let $\mathcal{T}_0 = (t_1, \ldots, t_r)$ be an ordered collection of k-algebraically independent elements of K and extend $\mathcal{T}_0$ to $\mathcal{T} = (t_1, \ldots, t_d)$ a transcendence base for $K|k$; denote by $\mathcal{T}_1 = (t_{r+1}, \ldots, t_d)$. We will consider the rational function fields $k(\mathcal{T}_1) \subset k(\mathcal{T})$.

For a polynomial $p(\mathbf{t}) = p(t_{r+1}, \ldots, t_d) \in k[\mathcal{T}_1]$, say $p(\mathbf{t}) = \sum_{\mathbf{i}} a_{\mathbf{i}} t^{\mathbf{i}}$ (where $\mathbf{i}$ is a

multi-index), define

$$v_1(p(\mathbf{t})) := \min_{\mathbf{i}} v_0(a_{\mathbf{i}}).$$

Then v_1 extends to a unique valuation v_1 on $k(\mathcal{T}_1)$ which satisfies the following properties:

1. $\Gamma_{v_1} = \Gamma_{v_0}$.

2. $v_1|_k = v_0$.

Now consider the totally ordered abelian group:

$$\Gamma_v =: \Gamma_{v_0} \oplus \mathbb{Z} \cdot \gamma_1 \oplus \cdots \oplus \mathbb{Z} \cdot \gamma_r$$

which we endow with the lexicographic order – namely, $\langle \gamma_r \rangle$ is the unique minimal non-trivial convex subgroup of Γ_v. Then v_1 extends to a unique valuation v of $k(\mathcal{T})$ with value group Γ_v as above, which is defined by the following two properties:

1. $v|_{k(\mathcal{T}_1)} = v_1$ and

2. $v(t_i) = \gamma_i$ for $i = 1, \ldots, r$.

The residue field $k(v)$ of v is precisely $k(v_1)$ which is the rational function field $kv_0(\bar{t}_{r+1}, \ldots, \bar{t}_d)$; here $\bar{t}_i$ denotes the image of t_i in $k(v)$.

Lastly, since K is a finite extension of $k(\mathcal{T})$ and k is relatively algebraically closed in K, we see that v has prolongations w to K whose value group is of the form

$$\Gamma_w = \Gamma_{v_0} \oplus \mathbb{Z} \cdot \tilde{\gamma}_1 \oplus \cdots \oplus \mathbb{Z} \cdot \tilde{\gamma}_r.$$

And we immediately see that $k(w)$ is a function field of transcendence degree $d-r$ over $k(v_0)$.

Moreover, the groups $\Delta_i = \langle \tilde{\gamma}_i, \cdots, \tilde{\gamma}_r \rangle$, for $i = 1, \cdots, r+1$ are convex. The coarsening w_i of w associated with Δ_i has a residue field $k(w_i)$ which is a function field in $d-i+1$ variables over $k(v_0)$.

Remark 5.0.4. A valuation v which arises using the process outlined above is called a **quasi-r-divisorial** valuation. By taking a coarsening associated to the convex subgroup $\langle \gamma_{s+1}, \ldots, \gamma_r \rangle$, one obtains a valuation v' whose value group is canonically isomorphic to $\Gamma_{v_0} \oplus \mathbb{Z} \cdot \tilde{\gamma}_1 \cdots \mathbb{Z} \cdot \tilde{\gamma}_s$ and this is a quasi-s-divisorial valuation. If v_0 is the trivial valuation on k, then the corresponding valuations are, actually, compositions of divisorial valuations in the usual sense.

In the sequel, we will only use these quasi-divisorial valuations as examples of valuations v of a function field K which satisfy the following properties:

1. The restriction of v to k is v_0.

2. The value group Γ_v contains no non-trivial (ℓ-)divisible convex subgroup.

3. If k is ℓ-closed, then $\Gamma_v/\ell^\infty = \mathbb{Z} \cdot \tilde{\gamma}_1 \oplus \cdots \oplus \mathbb{Z} \cdot \tilde{\gamma}_r$.

The precise construction of such valuations v will not matter too much – in Chapter 15, we will only use such v as examples of valuations with these properties above.

Part II

Detecting Valuations: the Abstract Setting

Chapter 6

C-pairs and Valuations

We now begin to move from the very general and elementary setting of rigid elements towards Galois theory. The results in Part II are still completely general and elementary in nature in the sense that almost all of these results hold true for completely arbitrary fields. The main benefit of the formulation here is in its connections with Galois theory as will become apparent later on.

In this chapter, we introduce our general setting, while in the subsequent chapters of Part II, we develop the general theory which shows how to recover/detect valuations in this setting.

We denote by $\mathbb{N} = \{1, 2, 3, \ldots\}$ the set of positive integers and $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$ the set of positive integers together with ∞. We declare that $\infty > n$ for all $n \in \mathbb{N}$. Recall that ℓ denotes a prime which is fixed throughout.

For positive integers n and r, we denote by

1. $\mathbf{M}_r(n) = (r+1) \cdot n - r$,

2. $\mathbf{N}'(n) = (6\ell^{3n-2} - 7) \cdot (n-1) + 3n - 2$,

3. $\mathbf{N}(n) = \mathbf{M}_1(\mathbf{N}'(n))$.

To make the notation consistent, we denote by $\mathbf{M}_r(\infty) = \mathbf{N}(\infty) = \infty$. In particular, $\mathbf{N}(n) \geq \mathbf{M}_1(n) \geq n$ for all $n \in \overline{\mathbb{N}}$, and $\mathbf{N}(n), \mathbf{M}_r(n) \in \mathbb{N}$ if and only if $n \in \mathbb{N}$. Also, observe that $\mathbf{M}_r(1) = \mathbf{N}'(1) = \mathbf{N}(1) = 1$, and $\mathbf{M}_r(\infty) = \mathbf{N}'(\infty) = \mathbf{N}(\infty) = \infty$.

The definition of $\mathbf{N}'$ and $\mathbf{N}$ is a technicality and should not be considered as important; in particular, we do not expect that this $\mathbf{N}$ is optimal. The precise formula for $\mathbf{N}'$ (and thus of $\mathbf{N}$) will come in to play when proving Theorem 6.1.1. This theorem, which is a generalization of the main theorem concerning commuting pairs from [BT02], is the key technical tool which lets us detect valuations in both the Galois theoretical and non-Galois theoretical settings. In fact, all the results in this thesis have been written in such a way that, if Theorem 6.1.1 holds with a different formula for $\mathbf{N}$, then so do the rest of the results of the paper which detect valuations – we use Theorem 6.1.1 purely as a black box. On the other hand, the definition of $\mathbf{M}_r$ will play an essential role throughout, and the importance of $\mathbf{M}_r$ can be immediately seen in our "cancellation principle" (Lemma 6.0.5).

We will use the following notation:

$$\Lambda_n := \varprojlim_{m|n} \mathbb{Z}/\ell^m = \begin{cases} \mathbb{Z}/\ell^n, & n \in \mathbb{N} \\ \mathbb{Z}_\ell, & n = \infty \end{cases}$$

In the context of pro-ℓ Galois theory, we will also denote by $\Lambda_n(i) = \Lambda_n \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(i)$ the i^{th} Tate twist of Λ_n; this notation will not be needed until Part III and in most situations we will choose an isomorphism of Galois modules $\Lambda_n(i) \cong \Lambda_n$ when applicable.

Throughout we will tacitly use the following trivial observation which we dub the "Cancellation Principle" which allows us to "divide" (or "cancel") in equations involving elements of the ring Λ_n; of course one must pay a price for this, and here is where $\mathbf{M}_r$ comes in to play.

Lemma 6.0.5 (The Cancellation Principle)**.** *For a positive integer n, we denote by $\mathbf{M}_r(n) = (r+1)\cdot n - r$. Assume that $R \geq (r+1)\cdot n - r = \mathbf{M}_r(n)$. Let $a, b, c_1, \ldots, c_r \in \mathbb{Z}/\ell^R$ be given; assume that $c_i \neq 0 \mod \ell^n$ and that $ac_1 \cdots c_r = bc_1 \cdots c_r$. Then $a = b \mod \ell^n$.*

Proof. Let a be the minimal positive integer such that $\ell^a \cdot c_1 \cdots c_r = 0$ as an element of $\mathbb{Z}/\ell^R$. Then the map $\mathbb{Z}/\ell^a \to \mathbb{Z}/\ell^R$ defined by $x \mapsto x \cdot c_1 \cdots c_r$ is injective. On the other hand, as $c_i \neq 0 \mod \ell^n$, we observe that $a \geq R - rn + r \geq n$ and this proves the claim. □

Let M be an Λ_n-module. A collection of non-zero elements $(f_i)_i$, $f_i \in M$ will be called **quasi-independent** provided that

$$\sum_i a_i f_i = 0 \text{ almost all } a_i = 0 \Rightarrow a_i f_i = 0 \ \forall i.$$

A generating set which is quasi-independent will be called a quasi-basis. Observe

that any finitely generated Λ_n-module M has a quasi-basis of unique finite order which is equal to $\dim_{\mathbb{Z}/\ell}(M/\ell)$. Indeed, any finitely generated Λ_n-module M can be considered as a $\mathbb{Z}_\ell$-module via the canonical homomorphism $\mathbb{Z}_\ell \to \Lambda_n$. Since $\mathbb{Z}_\ell$ is a principal ideal domain, we see that a finitely generated $\mathbb{Z}_\ell$-module M can written as a direct product of cyclic submodules:

$$M = \prod_{i=1}^{m} \langle \sigma_i \rangle$$

and in this case, if all $\sigma_i \neq 0$, then $(\sigma_i)_i$ form a quasi-basis for M and m is the rank of M.

Another trivial observation which we will use frequently in our arguments is the following. Let $m, m' \in M$ be elements of the Λ_n-module M. Then $\langle m, m' \rangle$, the Λ_n-submodule generated by m, m', is cyclic if and only if $m \in \langle m' \rangle$ or $m' \in \langle m \rangle$. Indeed if $a, b \in \Lambda_n$ then $a|b$ or $b|a$ since Λ_n is a quotient of a discrete valuation ring.

Let K be a field and $n \in \overline{\mathbb{N}}$ be given. We denote by:

$$\mathcal{G}_K^a(n) := \mathrm{Hom}^{\mathrm{cont}}(K^\times / \pm 1, \Lambda_n);$$

endowed with the point-wise convergence topology, we consider $\mathcal{G}_K^a(n)$ as a pro-ℓ group. This pro-ℓ group should be thought of as the abstract analogue of the maximal ℓ^n-elementary abelian Galois group of K which is isomorphic to $\mathcal{G}_K^a(n)$ in the case where $\mathrm{Char}\, K \neq \ell$ and $\mu_{2\ell^n} \subset K$; until Part III, however, we make no such sweeping assumptions on K.

If v is a valuation of K we denote by $I_v(n) = \mathrm{Hom}(K^\times / U_v, \Lambda_n) \leq \mathcal{G}_K^a(n)$ and $D_n(n) = \mathrm{Hom}(K^\times / (\pm U_v^1), \Lambda_n) \leq \mathcal{G}_K^a(n)$. The groups $I_v(n)$ resp. $D_v(n)$, which

are (closed) subgroups of $\mathcal{G}_K^a(n)$, should be thought of as the abstract analogues of inertia resp. decomposition groups by mimicking the situation in the pro-ℓ Galois case (see Proposition 13.0.6).

We will frequently pass from $\mathcal{G}_K^a(N)$ to $\mathcal{G}_K^a(n)$ when $n, N \in \mathbb{N}$ and $N \geq n$; let us, then, introduce some notation. Suppose that $f \in \mathcal{G}_K^a(N)$, then we denote by $f \mapsto f_n$ the canonical map $\mathcal{G}_K^a(N) \to \mathcal{G}_K^a(n)$ induced by the projection $\Lambda_N \twoheadrightarrow \Lambda_n$. I.e. $f_n(x) = f(x) \mod \ell^n$; here ℓ^n is understood to be 0 in $\mathbb{Z}_\ell$ if $n = \infty$.

For a subgroup $A \leq \mathcal{G}_K^a(n)$, we denote by $A^\perp$ the subgroup of $K^\times$:

$$A^\perp = \bigcap_{f \in A} \ker f.$$

This is the left kernel of the canonical pairing $K^\times \times A \to \Lambda_n$. More generally, it is easy to see that we have a canonical pairing $K^\times \times \mathcal{G}_K^a(n) \to \Lambda_n$ whose right kernel is trivial and whose left kernel is $\pm K^{\times \ell^n}$. If $n \neq \infty$, we therefore obtain a perfect pairing between $K^\times/(\pm K^{\times \ell^n})$ and $\mathcal{G}_K^a(n)$ by Pontryagin duality. On the other hand, if $n = \infty$, we have a perfect $\mathbb{Z}_\ell$-pairing between $\widehat{K}/\text{torsion}$ and $\mathcal{G}_K^a(\infty)$ where $\widehat{K} = \lim_n K^\times/\ell^n$ is the ℓ-adic completion of $K^\times$.

We now introduce our abstract notion of C-pairs. Our definition of a C-pair is motivated by Bogomolov and Tschinkel's notion under the same name [BT02]; we note, however, that our notion of C-pairs is *a priori* much less restrictive than that considered in loc.cit.. In Part III, we will show the connection between C-pairs and Galois theory while the results of this part will explore the connection between C-pairs, rigid elements, and valuations.

Definition 6.0.6. Let $f, g \in \mathcal{G}_K^a(n)$ be given. We say that f, g are a C-pair provided that for all $x \in K \smallsetminus \{0, 1\}$ one has:

$$f(1-x)g(x) = f(x)g(1-x).$$

A subgroup $A \leq \mathcal{G}_K^a(n)$ will be called a C-group provided that any pair of elements $f, g \in A$ form a C-pair. If $A = \langle f_i \rangle_i$ is generated by $f_i \in \mathcal{G}_K^a(n)$, we observe that A is a C-group if and only if f_i, f_j form a C-pair for all i, j.

For a subgroup $A \leq \mathcal{G}_K^a(n)$, we denote by $\mathbf{I}^{\mathrm{C}}(A)$ the subgroup:

$$\mathbf{I}^{\mathrm{C}}(A) = \{f \in A \ : \ \forall g \in A, \ f, g \ \text{ form a C-pair}\}.$$

and call $\mathbf{I}^{\mathrm{C}}(A)$ the C-center of A. In particular, A is a C-group if and only if $A = \mathbf{I}^{\mathrm{C}}(A)$ if and only if $A/\mathbf{I}^{\mathrm{C}}(A)$ is cyclic.

One can start to see the deep connection between C-pairs and valuations in the following two lemmas which will be used throughout. The first lemma shows that valuations give rise to very many non-trivial C-pairs while the second proves the compatibility of this fact in taking residue fields of valuations.

Lemma 6.0.7. *Let $n \in \overline{\mathbb{N}}$ be given and let (K, v) be a valued field. Suppose that $f \in D_v(n)$ and $g \in I_v(n)$ and denote by $\Psi = (f, g)$. Then for all $x \in K^\times \smallsetminus \{1\}$ one has:*

$$\langle \Psi(1-x), \Psi(x) \rangle \ \ \textit{is cyclic.}$$

In particular, f, g form a C-pair.

Proof. Denote by $\Psi = (f, g)$. If $v(x) > 0$ then $\Psi(1-x) = 0$ since $U_v^1 \leq \ker \Psi$ so we obtain the claim. If $v(x) < 0$ then $1 - x = x(1/x - 1)$ so that $\Psi(1-x) = \Psi(x)$, and this completes the proof. By replacing x with $1 - x$ if needed, the last case to consider is where $x, 1 - x \in U_v$. But then $g(x) = 0$ and $g(1-x) = 0$ so the claim is trivial. □

Suppose that (K, v) is a valued field and $f \in D_v(n)$. Then the restriction $f|_{U_v}$ descends to a homomorphism $f_v : k(v)^\times \to \Lambda_n$ such that $f_v(-1) = 0$. In particular this provides a canonical map $D_v(n) \to \mathcal{G}^a_{k(v)}(n)$. This map, in some sense, forces the C-pair property as we see in the following lemma.

Lemma 6.0.8. *Let (K, v) be a valued field and let $n \in \overline{\mathbb{N}}$ be given.*

1. *The map $D_v(n) \to \mathcal{G}^a_{k(v)}(n)$ defined by $f \mapsto f_v$ induces an isomorphism $D_v(n)/I_v(n) \cong \mathcal{G}^a_{k(v)}(n)$.*

2. *Let $f, g \in D_v(n)$ be given, then f, g form a C-pair if and only if their images f_v, g_v in $\mathcal{G}^a_{k(v)}(n)$ form a C-pair.*

Proof. To 1. Assume with no loss that $n \in \mathbb{N}$ as the $n = \infty$ case follows in the limit. Consider the short exact sequence:

$$1 \to k(v)^\times / \pm 1 \to K^\times / (\pm U_v^1) \to \Gamma_v \to 1.$$

Tensoring this with $\mathbb{Z}/\ell^n$ and noting that Γ_v is torsion-free, we obtain:

$$1 \to (k(v)^\times/\ell^n)/\pm 1 \to (K^\times/\ell^n)/(\pm U_v^1) \to \Gamma_v/\ell^n \to 1.$$

Taking $\mathrm{Hom}(\bullet, \mathbb{Z}/\ell^n)$ we deduce that the following short sequence is exact by Pontryagin Duality:

$$1 \to I_v(n) \to D_v(n) \to \mathcal{G}^a_{k(v)}(n) \to 1.$$

To 2. If f, g form a C-pair then clearly f_v, g_v are a C-pair. Conversely, assume that f_v, g_v are a C-pair. Let $x \in K \smallsetminus \{0, 1\}$ be given. If $v(x) > 0$ then $1 - x \in U_v^1 \leq \ker f \cap \ker g$. Thus, $f(1-x)g(x) = 0 = f(x)g(1-x)$. If $v(x) < 0$ then $x^{-1}(1-x) = x^{-1} - 1 \in -(U_v^1)$ so that $(1-x) \in -x \cdot (U_v^1)$. Thus, $f(1-x)g(x) = f(-x)g(x) = f(x)g(x) = f(x)g(-x) = f(x)g(1-x)$. If $v(x) = 0$ and $v(1-x) > 0$ we're in one of the previous cases with $y = 1 - x$. The last case to consider is where $x, 1-x \in U_v$. Here, we note that $f(z) = f_v(\bar{z})$ (and similarly with g) for all $z \in U_v$ where $\bar{z} = z + \mathfrak{m}_v$ denotes the image of z in $k(v)^\times$. Thus, as f_v, g_v form a C-pair, we see that $f(x)g(1-x) = f(1-x)g(x)$ when $x, 1-x \in U_v$. □

6.1 The Main Theorem of C-pairs

The following theorem is the main tool which allows us to detect valuations using C-pairs. This theorem shows that a pair $f, g \in \mathcal{G}^a_K(n)$ which can be lifted to a C-pair in $\mathcal{G}^a_K(N)$, for N sufficiently large, must come about from a valuation in a similar manner to Lemmas 6.0.7 and 6.0.8. For the most part, the following theorem will be used solely as a black box in the rest of the discussion.

Theorem 6.1.1. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{N}(n)$. Let K be an arbitrary field*

and let $f, g \in \mathcal{G}_K^a(n)$ *be given. Assume that there exist* $f'', g'' \in \mathcal{G}_K^a(N)$ *such that*

- f'', g'' *form a C-pair.*
- $f''_n = f$ *and* $g''_n = g$.

Then there exists a valuation v *of* K *such that*

- $f, g \in D_v(n)$
- $\langle f, g\rangle/(\langle f, g\rangle \cap I_v(n))$ *is cyclic (possibly trivial).*

Before we begin to prove Theorem 6.1.1, we will prove the following, quite trivial, lemma which immediately follows from the cancellation principle.

Lemma 6.1.2. *Let* $n \in \overline{\mathbb{N}}$ *be given and denote by* $M = \mathbf{M}_1(n)$.

1. *Suppose that* $a, b, c, d \in \Lambda_M$ *are given such that* $ad = bc$. *Then* $\langle (a, b), (c, d)\rangle$ mod ℓ^n *is cyclic.*
2. *In particular, let* $f, g \in \mathcal{G}_K^a(M)$ *be a given C-pair. Denote by* $\Psi = (f_n, g_n)$. *Then for all* $x \neq 1$, $\langle \Psi(1-x), \Psi(x)\rangle$ *is cyclic.*

Proof. To 1. The $n = 1$ and $n = \infty$ case are both trivial since Λ_1 and Λ_∞ are integral domains. Thus, assume that $n \in \mathbb{N}$ is arbitrary. Assume, for example, that $a = ec$ for some $e \in \mathbb{Z}/\ell^M$ (otherwise $c = ea$ for some $e \in \mathbb{Z}/\ell^M$). Then $ad = bc = edc$. If $c \neq 0 \mod \ell^n$ then we see that $de = b \mod \ell^n$ by the cancellation principle; thus $(a, b) = e \cdot (c, d) \mod \ell^n$. On the other hand, if $c = 0 \mod \ell^n$ then $a = 0 \mod \ell^n$

as well, so that $\langle (a,b),(c,d)\rangle \mod \ell^n = \langle (0,b),(0,d)\rangle \mod \ell^n$ is cyclic. Claim 2 follows immediately from Claim 1. $\square$

Proof of Theorem 6.1.1. First observe that we may, and will, assume that $N = \mathbf{N}(n)$. The proof will proceed in two main steps. First, we will prove the theorem for $n \in \mathbb{N}$ and then prove it for $n = \infty$ with a limit argument using the first case. Alternatively in the $n = \infty$ case, see [Top12] Theorem 3 in the "pro-ℓ case" which proves this case directly.

We briefly recall some facts from the theory of rigid elements (see Chapter 4) which describe the minimal conditions for the existence of valuations in fields – as in Chapter 4, we use the results of [AEJ87], but see also the various references on this subject mentioned in the introduction. For a field K, and $T \leq H \leq K^\times$, assume that $-1 \in T$ and for all $x \notin H$ one has $T + xT \subset T \cup xT$; equivalently, for all $x \notin H$ one has $1 + x \in T \cup xT$. If there exists an element $a \in K^\times \smallsetminus T$ such that $T + aT \not\subset T \cup aT$ then there exists a valuation ring $(\mathcal{O}, \mathfrak{m})$ of K such that $1 + \mathfrak{m} \leq T$ and $\mathcal{O}^\times \leq H$ (see Proposition 2.14 of loc.cit.). On the other hand, if $H = T$, then there exists a valuation ring $(\mathcal{O}, \mathfrak{m})$ of K such that $1 + \mathfrak{m} \leq T$ and $\mathcal{O}^\times \cdot T/T$ has order at most 2 (see Theorem 2.16 and/or Corollary 2.17 of loc.cit., as well as our summary in Theorem 4.0.1).

Case $n \neq \infty$:

We denote by $N = \mathbf{N}(n) = \mathbf{M}_1(\mathbf{N}'(n))$, $N' = \mathbf{N}'(n)$ and $M = \mathbf{M}_1(n)$ as defined

in § 6.1. Suppose we are given $f, g \in \mathcal{G}_K^a(n)$ as well as lifts $f'', g'' \in \mathcal{G}_K^a(N)$ which form a C-pair. The goal is to show that there exists a valuation v of K such that $f, g \in D_v(n)$ and $\langle f, g\rangle/(\langle f, g\rangle \cap I_v(n))$ is cyclic.

We denote by $f' = f''_{N'}$ and $g' = g''_{N'}$. Denote by $\Psi = (f, g)$ and $\Theta = (f', g')$, and consider $T = \ker \Psi = \ker f \cap \ker g$. By Lemma 6.1.2, for all $x \in K^\times$, $x \neq -1$ one has:

$$\langle \Theta(1 + x), \Theta(x)\rangle \text{ is cyclic.}$$

In particular, the same is true for Ψ. Denote by H the subgroup of $K^\times$ generated by T and all $x \in K^\times \smallsetminus T$ such that $1 + x \neq 1, x \mod T$ (i.e. x such that $\Psi(1+x) \neq \Psi(1), \Psi(x)$). Our central claim will be that H/T is cyclic.

Before we prove this claim, let us show how this would imply Theorem 6.1.1. First, if $H = T$, then for all $x \in K^\times$, such that $\Psi(x) \neq 0$ one has $\Psi(1 + x) = \Psi(1)$ or $\Psi(1 + x) = \Psi(x)$. I.e. if $x \notin T$ one has $1 + x \in T \cup xT$. By [AEJ87] Theorem 2.16 and/or Corollary 2.17 (see our summary Theorem 4.0.1 parts (1) and (3)) we deduce that there exists a valuation v of K such that $U_v^1 \leq T$ and $\#(U_v \cdot T/T) \leq 2$, thus proving our claim.

On the other hand, if $H \neq T$ then there exists some $x \notin T$ such that $\Psi(1+x) \neq \Psi(1), \Psi(x)$ and so $1 + x \notin T \cup xT$. Moreover, for all $x \notin H$, one has $1 + x \in T \cup xT$ by construction of H. Again by [AEJ87] Proposition 2.14 (again, see our summary Theorem 4.0.1), we deduce that there exists a valuation v of K such that $U_v^1 \leq T$ and $U_v \cdot T = H$.

Thus, what remains to be shown is that H/T is cyclic and this will be done in steps 1-5 below. In the case where $n = 1$, this claim can be obtained from [Koe98] Lemma 3.3, a form of which also appears in [Koe95], and/or [Efr99] Proposition 3.2; this lemma is the key technical tool used in order to prove the main Theorem of [EK98]. On the other hand, if $n = \infty$ and K contains an ℓ-closed field, the corresponding claim can be deduced in a similar way to [BT02] Proposition 4.1.2; this proposition is in the core of the proof of loc.cit.'s main theorem. See also [Top12] Theorem 3 where the $n = \infty$ case is proved directly, without the assumption that K contains an ℓ-closed field. Below, we prove the claim for an arbitrary $n \in \mathbb{N}$.

Main Claim: H/T is cyclic.

The remainder of this section will be devoted to the proof of this claim. To make the notation a bit less cumbersome, we will use the following convention. For $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Z}/\ell^s$, we will write:

$$\gamma_1 : \ \gamma_2 = \gamma_3$$

to mean that $\gamma_1\gamma_2 = \gamma_1\gamma_3$. Also, we will write $(i, j) = (\gamma_1 : \gamma_2 : \gamma_3)$ to mean that $i{\cdot}\gamma_1 = \gamma_2$ and $j{\cdot}\gamma_1 = \gamma_3$. Furthermore, we will use the notation $(i, j) = \gamma(\gamma_1 : \gamma_2 : \gamma_3)$ to mean that $(i, j) = (\gamma\gamma_1 : \gamma\gamma_2 : \gamma\gamma_3)$.

Suppose x, y are given such that $\Psi(1{+}x) \neq \Psi(1), \Psi(x)$ and $\Psi(1{+}y) \neq \Psi(1), \Psi(y)$ and assume that $\Theta(1 + x) = a\Theta(x)$ and $\Theta(1 + y) = b\Theta(y)$. We will show that $\langle \Psi(x), \Psi(y) \rangle$ is cyclic for all such x, y; this will suffice to show that H/T is cyclic as follows.

Assume that, indeed, $\langle \Psi(x), \Psi(y) \rangle$ is cyclic for all x, y such that $\Psi(1+x) \neq \Psi(1), \Psi(x)$, that $\Psi(1+y) \neq \Psi(1), \Psi(y)$, that $\Theta(1+x) \in \langle \Theta(x) \rangle$, and that $\Theta(1+y) \in \langle \Theta(y) \rangle$. First, we observe that H is generated by T and all $z \notin T$ such that $\Psi(1-z) \neq \Psi(1), \Psi(z)$ since $\Psi(-1) = 0$ and thus $\Psi(z) = \Psi(-z)$. For any given $z \in K^\times \smallsetminus T$, one has $\Psi(1-z) \neq \Psi(1), \Psi(z)$ iff $\Psi(1-(1-z)) \neq \Psi(1), \Psi(1-z)$. Now since Λ_n is a quotient of a discrete valuation ring and $\langle \Psi(z), \Psi(1-z) \rangle$ is cyclic, we either have $\Psi(1-z) \in \langle \Psi(z) \rangle$ or $\Psi(z) \in \langle \Psi(1-z) \rangle$. Since $\Psi(z) = \Psi(1-(1-z))$, we see that H is generated by T and all $z \notin T$ such that $\Psi(1-z) \in \langle \Psi(z) \rangle \smallsetminus \{\Psi(1), \Psi(z)\}$. If $\Psi(z) \neq 0$, we note that $\Psi(1-z) \in \langle \Psi(z) \rangle$ if and only if $\Theta(1-z) \in \langle \Theta(z) \rangle$ since Λ_n is a quotient of a discrete valuation ring and $\langle \Theta(1-z), \Theta(z) \rangle$ is cyclic. Thus our assumption ensures that H/T is generated as an Λ_n-submodule of $K^\times/T$ by the set:

$$\{z \cdot T \ : \ z \in K^\times \smallsetminus T, \ \Psi(1-z) \neq \Psi(1), \Psi(z), \ \Theta(1-z) \in \langle \Theta(z) \rangle\}.$$

But, if x, y are in this set, our assumption ensures that $\langle x \cdot T, y \cdot T \rangle$ is cyclic as a submodule of H/T. From this, again along with the fact that Λ_n is a quotient of a discrete valuation ring and that H/T is finite and killed by ℓ^n, it is easy to see that H/T is indeed cyclic.

Let us now return to the proof of our claim – i.e. we wish to prove that $\langle \Psi(x), \Psi(y) \rangle$ is cyclic for x, y as above with $\Theta(1+x) = a \cdot \Theta(x)$ and $\Theta(1+y) = b \cdot \Theta(y)$. Since $\Theta(1+1/x) = \Theta(1/x) + \Theta(1+x) = (a-1)\Theta(x) = (1-a)\Theta(1/x)$, we can assume without loss that a, b as above are units by replacing x with $1/x$ and/or

y with $1/y$ if needed. We denote by $D = f'(x)g'(y) - f'(y)g'(x)$ and take linear combinations p, q of f', g' so that:

- $(p, q)(x) = (D, 0)$ and
- $(p, q)(y) = (0, D)$.

And thus:

- $(p, q)(1 + x) = (aD, 0)$ and
- $(p, q)(1 + y) = (0, bD)$.

Furthermore, we will denote by $a' = a-1$ and $b' = b-1$. Recall that our assumptions on a, b ensure that:

- $a, a' \neq 0 \mod \ell^n$.
- $b, b' \neq 0 \mod \ell^n$.

To show that $\langle \Psi(x), \Psi(y) \rangle$ is cyclic, it will suffice to prove that $D = 0 \mod \ell^M$ by Lemma 6.1.2. Furthermore, we observe that p, q form a C-pair and $p(-1) = q(-1) = 0$. In particular for all $z, w \in K^\times$, $z \neq -w$, the following 2×2 determinant is zero:

$$\begin{vmatrix} p(z+w) - p(w) & p(z) - p(w) \\ q(z+w) - q(w) & q(z) - q(w) \end{vmatrix} = 0.$$

We will denote by $\Phi = (p, q)$ for the remainder of the proof.

Step 1: Consider $\Phi(1+x+y)$; for simplicity, denote $\Phi(1+x+y) = (P, Q)$. We can write $1+x+y = (1+x)+y$ and thus:

$$\begin{vmatrix} p(1+x+y)-p(y) & p(1+x)-p(y) \\ q(1+x+y)-q(y) & q(1+x)-q(y) \end{vmatrix} = 0.$$

Making the appropriate substitutions:

$$\begin{vmatrix} P & aD \\ Q-D & -D \end{vmatrix} = D \cdot \begin{vmatrix} P & -a \\ Q-D & 1 \end{vmatrix} = 0.$$

In other words we deduce (I) $\boxed{D: \ P+aQ = aD}$; similarly (II) $\boxed{D: \ bP+Q = bD}$ since $1+x+y = (1+y)+x$. Using equations (I) and (II), we deduce the following (in steps):

1. $D: \ P + a(bD - bP) = aD$
2. $D: \ P + ab(D-P) = aD$
3. $D: \ P(1-ab) = Da(1-b)$
4. $D: \ P(ab-1) = Dab'$
5. $D: \ P(a'b'+a'+b') = Dab'$ and in a similar way $D: \ Q(a'b'+a'+b') = Da'b$.

In particular, we deduce:

$$\boxed{\Phi(1+x+y) = D(a'b'+a'+b' : Dab' : Da'b).} \tag{6.1.1}$$

Step 2: We now consider $\Phi(2+x+y)$; for simplicity, we again denote $\Phi(2+x+y) = (P,Q)$. Since $2+x+y = 1+(1+x+y)$ one has:

$$\begin{vmatrix} p(2+x+y) & p(1+x+y) \\ q(2+x+y) & q(1+x+y) \end{vmatrix} = 0$$

Use Equation (6.1.1) and multiply the second column of this matrix by $D(a'b' + a' + b')$ to deduce:

$$D \begin{vmatrix} P & Dab' \\ Q & Dba' \end{vmatrix} = D^2 \begin{vmatrix} P & ab' \\ Q & ba' \end{vmatrix} = 0.$$

So that we deduce (III) $\boxed{D^2 :\ ba'P = ab'Q}$.

On the other hand, $2+x+y = (1+x)+(1+y)$ so that:

$$\begin{vmatrix} P - p(1+y) & p(1+x) - p(1+y) \\ Q - q(1+y) & q(1+x) - q(1+y) \end{vmatrix} = 0$$

Making the appropriate substitutions:

$$\begin{vmatrix} P & aD \\ Q - bD & -bD \end{vmatrix} = D \cdot \begin{vmatrix} P & a \\ Q - bD & -b \end{vmatrix} = 0$$

So that we deduce (IV) $\boxed{D :\ bP + aQ = abD}$. Using equations (III) and (IV), we deduce the following, in steps (recall that a, b are units):

1. $D^2 :\ ba'P = b'(abD - bP)$
2. $D^2 :\ ba'P = bb'(aD - P)$
3. $D^2 :\ P(ba' + bb') = bb'aD$

4. $D^2:\ P(a'+b') = b'aD$ and similarly $D^2:\ Q(a'+b') = a'bD$.

Thus:

$$\boxed{\Phi(2+x+y) = D^2 \cdot (a'+b' : ab'D : ba'D)} \tag{6.1.2}$$

Step 3 (an inductive step): Let m be a positive integer and denote by $A = D^e(a')^f(b')^g$ and $B = D^h(a')^i(b')^j$. Assume that the following statements hold:

- $(\mathbf{P1})(\mathbf{m}, \mathbf{A}):\quad \Phi((m-1)+mx) = A \cdot (a'b' + mb' : mDab' : 0)$.
- $(\mathbf{P2})(\mathbf{m}, \mathbf{B}):\quad \Phi(m+mx+y) = B \cdot (a'b' + mb' + a' : mDab' : Da'b)$.

We will show, in particular, that the following statements hold:

- $(\mathbf{P1})(\mathbf{m+1}, \mathbf{E})$
- $(\mathbf{P2})(\mathbf{m+1}, \mathbf{E})$

where $E = D^{\max(2,e,h)+2}(a')^{\max(f,i)+1}(b')^{\max(g,j)+1}$ is determined by the exponents of D, a', b' in A and B. To simplify the notation, we will denote:

- $\Delta_0 = a' + b'$.
- $\Delta_1 = a'b' + mb'$.
- $\Delta_2 = a'b' + mb' + a'$.

Let us first consider $(P, Q) = \Phi((m+1) + (m+1)x + y)$, and we observe that $(m+1) + (m+1)x + y = ((m-1) + mx) + (2 + x + y)$. Thus,

$$\begin{vmatrix} P - p((m-1)+mx) & p(2+x+y) - p((m-1)+mx) \\ Q - q((m-1)+mx) & q(2+x+y) - q((m-1)+mx) \end{vmatrix} = 0.$$

Now by statement $(\mathbf{P1})(\mathbf{m}, \mathbf{A})$, we deduce that:

$$A \cdot \begin{vmatrix} \Delta_1 P - mDab' & \Delta_1 p(2+x+y) - mDab' \\ Q & q(2+x+y) \end{vmatrix} = 0$$

Denote by $A' = D^{\max(2,e)}(a')^f(b')^g$ then by Equation (6.1.2) we deduce that:

$$A' \cdot \begin{vmatrix} \Delta_1 P - mDab' & \Delta_1 Dab' - \Delta_0 mDab' \\ Q & Da'b \end{vmatrix} = 0.$$

Moving some terms around a bit, we have

$$A' \cdot \begin{vmatrix} \Delta_1 P - mDab' & Dab'(\Delta_1 - \Delta_0 m) \\ Q & Da'b \end{vmatrix} = 0$$

and now substituting into Δ_1 and Δ_0 we have:

$$A' \cdot \begin{vmatrix} \Delta_1 P - mDab' & Dab'(a'b' + mb' - ma' - mb') \\ Q & Da'b \end{vmatrix} = 0$$

so that

$$A' \cdot \begin{vmatrix} \Delta_1 P - mDab' & Dab'(a'b' - ma') \\ Q & Da'b \end{vmatrix} = 0$$

and finally

$$A'Da' \cdot \begin{vmatrix} \Delta_1 P - mDab' & ab'(b' - m) \\ Q & b \end{vmatrix} = 0.$$

Thus we obtain the following equations, by steps:

1. $A'Da' :\ b(a'b' + mb')P = Qab'(b' - m) + mDabb'.$

2. $A'Da' :\ bb'(a' + m)P = Qab'(b' - m) + mDabb'.$

3. (V) $\boxed{A'Da'b' : \ Pb(a'+m) = Qa(b'-m) + mDab}$.

On the other hand, we can write $(m+1)+(m+1)x+y = (m+mx+y)+(1+x)$

so that:

$$\begin{vmatrix} P-p(1+x) & p(m+mx+y)-p(1+x) \\ Q-q(1+x) & q(m+mx+y)-q(1+x) \end{vmatrix} = 0.$$

Making the appropriate substitutions, we have

$$\begin{vmatrix} P-aD & p(m+mx+y)-aD \\ Q & q(m+mx+y) \end{vmatrix} = 0.$$

Now we use statement $(\mathbf{P2})(\mathbf{m}, \mathbf{B})$ to deduce that:

$$B \cdot \begin{vmatrix} P-aD & mDab'-\Delta_2 aD \\ Q & Da'b \end{vmatrix} = 0.$$

Rearranging a bit, we have:

$$BD \cdot \begin{vmatrix} P-aD & a(mb'-\Delta_2) \\ Q & a'b \end{vmatrix} = 0$$

and, substituting into Δ_2,

$$BD \cdot \begin{vmatrix} P-aD & a(mb'-a'b'-mb'-a') \\ Q & a'b \end{vmatrix} = 0$$

so that

$$BD \cdot \begin{vmatrix} P-aD & -aa'(b'+1) \\ Q & a'b \end{vmatrix} = 0.$$

Now recall that $b' = b - 1$; therefore

$$BD \cdot \begin{vmatrix} P - aD & -aa'b \\ Q & a'b \end{vmatrix} = 0$$

and

$$BDa' \cdot \begin{vmatrix} P - aD & -a \\ Q & 1 \end{vmatrix} = 0.$$

Thus finally, we deduce that (VI) $\boxed{BDa' : \ P + aQ = aD}$. Denote by

$$C = D^{\max(2,e,h)}(a')^{\max(f,i)}(b')^{\max(g,j)}.$$

So, using equations (V) and (VI), we deduce, in steps:

1. $Da'b'C : \ Pb(a' + m) = (aD - P)(b' - m) + mDab.$
2. $Da'b'C : \ P(b(a' + m) + b' - m) = aD(b' - m) + mDab.$
3. $Da'b'C : \ P(ba' + bm + b' - m) = a(D(b' - m) + mDb).$
4. $Da'b'C : \ P(ba' + bm + b' - m) = aD(b' - m + mb).$
5. $Da'b'C : \ P(ba' + bm + b' - m) = aD(b - 1 - m + mb).$
6. $Da'b'C : \ P(ba' + bm + b' - m) = aD((m + 1)b - (m + 1)).$
7. (VII) $\boxed{Da'b'C : \ P(ba' + bm + b' - m) = (m + 1)aDb'}$.

Let us write $ba' + bm + b' - m$ in a different way:

$$\begin{aligned} ba' + mb + b' - m &= b(a-1) + mb + b - 1 - m \\ &= ab - b + mb + b - 1 - m \\ &= ab + mb - (m+1) \end{aligned}$$

And on the other hand:

$$\begin{aligned} a'b' + (m+1)b' + a' &= (a-1)(b-1) + (m+1)(b-1) + a - 1 \\ &= ab - a - b + 1 + (m+1)b - (m+1) + a - 1 \\ &= ab + mb - (m+1) \end{aligned}$$

Therefore we have the equality $ba' + mb + b' - m = a'b' + (m+1)b' + a'$. This calculation, along with equation (VII) then implies:

$$\boxed{Da'b'C: \ P(a'b' + (m+1)b' + a') = (m+1)Dab'.} \tag{6.1.3}$$

Using euqations (6.1.3) and (VI), we see that:

1. $Da'b'C: \ (m+1)Dab' + a(a'b' + (m+1)b' + a')Q = aD(a'b' + (m+1)b' + a')$.
2. $Da'b'C: \ a(a'b' + (m+1)b' + a')Q = aD(a'b' + a')$.
3. $Da'b'C: \ (a'b' + (m+1)b' + a')Q = Da'(b'+1)$.
4. (VIII) $\boxed{Da'b'C: \ (a'b' + (m+1)b' + a')Q = Da'b}$.

Thus: $(\mathbf{P2})(\mathbf{m+1}, \mathbf{Da'b'C})$ holds and, in particular, $(\mathbf{P2})(\mathbf{m+1}, \mathbf{E})$ holds for $E = D^2a'b'C$ as above; however, we will use the stronger fact that statement $(\mathbf{P2})(\mathbf{m+1}, \mathbf{Da'b'C})$ holds true in our calculations below.

Now we consider instead $(P, Q) = \Phi(m+(m+1)x)$. We can write $m+(m+1)x = ((m-1)+mx)+(1+x)$ to deduce that:

$$\begin{vmatrix} P - p(1+x) & p((m-1)+mx) - p(1+x) \\ Q - q(1+x) & q((m-1)+mx) - q(1+x) \end{vmatrix} = 0.$$

Making the appropriate substitutions, we have

$$\begin{vmatrix} P - aD & p((m-1)+mx) - aD \\ Q & q((m-1)+mx) \end{vmatrix} = 0$$

and then, using statement $(\mathbf{P1})(\mathbf{m}, \mathbf{A})$, we have:

$$A \cdot \begin{vmatrix} P - aD & mDab' - \Delta_1 aD \\ Q & 0 \end{vmatrix} = 0.$$

Factoring out a D and substituting into Δ_1 we obtain:

$$AD \cdot \begin{vmatrix} P - aD & mb' - (a'b' + mb') \\ Q & 0 \end{vmatrix} = 0$$

and so:

$$AD \cdot \begin{vmatrix} P - aD & a'b' \\ Q & 0 \end{vmatrix} = 0.$$

Thus, we have (IX) $\boxed{Q \cdot (ADa'b') = 0}$.

Let us now furthermore denote by $(P', Q') = \Phi(m + 1 + (m + 1)x + y)$, and $\Delta_2' = a'b' + (m + 1)b' + a'$, $C' = Da'b'C$. Observe that $m + (m + 1)x = ((m + 1) + (m + 1)x + y) - (1 + y)$ so that:

$$\begin{vmatrix} P - p(1+y) & P' - p(1+y) \\ Q - q(1+y) & Q' - q(1+y) \end{vmatrix} = 0$$

and making the appropriate substitutions:

$$\begin{vmatrix} P & P' \\ Q - bD & Q' - bD \end{vmatrix} = 0.$$

Now we use the fact that $(\mathbf{P2})(\mathbf{m+1}, \mathbf{Da'b'C})$ (i.e. $(\mathbf{P2})(\mathbf{m+1}, \mathbf{C'})$) holds to deduce that:

$$C' \cdot \begin{vmatrix} P & (m+1)Dab' \\ Q - bD & Da'b - \Delta_2' bD \end{vmatrix} = 0$$

and so

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ Q - bD & a'b - \Delta_2' b \end{vmatrix} = 0.$$

Now, we observe that $ADa'b'|C'D$ so that equation (IX) above implies that:

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ -bD & a'b - \Delta_2' b \end{vmatrix} = 0$$

and, since b is a unit, we obtain

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ -D & a' - \Delta_2' \end{vmatrix} = 0.$$

Now we substitute into Δ_2' to obtain:

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ -D & a' - (a'b' + (m+1)b' + a') \end{vmatrix} = 0.$$

Thus we have

$$C'D \cdot \begin{vmatrix} P & (m+1)ab' \\ D & a'b' + (m+1)b' \end{vmatrix} = 0.$$

In particular, we obtain the following equation:

$$\boxed{E = C'D: \ P(a'b' + (m+1)b') = (m+1)Dab'}.$$

Therefore the statements $(\mathbf{P1})(\mathbf{m+1}, \mathbf{D^2a'b'C})$, $(\mathbf{P2})(\mathbf{m+1}, \mathbf{Da'b'C})$ hold. Recall that $C = D^{\max(2,e,h)}(a')^{\max(f,i)}(b')^{\max(g,j)}$. Thus, denoting by

$$E = D^{\max(2,e,h)+2}(a')^{\max(f,i)+1}(b')^{\max(g,j)+1},$$

we then deduce that the following statements hold:

$$(\mathbf{P1})(\mathbf{m+1}, \mathbf{E}), \quad (\mathbf{P2})(\mathbf{m+1}, \mathbf{E})$$

as contended.

Step 4 (calculating $\Phi((m-1)+mx)$): Our base case is $m = 1$. Indeed, observe that $\Phi(x) = (D, 0) = (a'b' + b' : Dab' : 0)$ (since $a' = a - 1$) and from Step 1 (see Equation (6.1.1)):

$$\Phi(1 + x + y) = D(a'b' + a' + b' : Dab' : Da'b).$$

Namely, the statements $(\mathbf{P1})(\mathbf{1}, \mathbf{1})$ and $(\mathbf{P2})(\mathbf{1}, \mathbf{D})$ hold true. Thus by the inductive step (Step 3) we obtain that $(\mathbf{P1})(\mathbf{2}, \mathbf{D^4a'b'})$ and $(\mathbf{P2})(\mathbf{D^4a'b'})$ are true as well.

From this, along with Step 3, we deduce that the statements $(\mathbf{P1})(\mathbf{3}, \mathbf{D^6(a')^2(b')^2})$ and $(\mathbf{P2})(\mathbf{3}, \mathbf{D^6(a')^2(b')^2})$ are true. We deduce inductively that, in general, the following statements hold:

$$(\mathbf{P1})(\mathbf{m}, \mathbf{D^{2m}(a')^{m-1}(b')^{m-1}}),\ (\mathbf{P2})(\mathbf{m}, \mathbf{D^{2m}(a')^{m-1}(b')^{m-1}}).$$

And in particular we deduce that, for any $m \geq 1$, there exists $P_m \in \mathbb{Z}/\ell^{N'}$ such that the following equation holds:

$$D^{2m}(a')^{m-1}(b')^{m-1} :\ (a'b' + mb') \cdot P_m = Dmab'.$$

Alternatively:

$$D^{2m}(a')^{m-1}(b')^{m} :\ (a' + m) \cdot P_m = Dma.$$

This means that the following equation holds for the elements $P_m, D, a', b', m, a, b \in \mathbb{Z}/\ell^{N'}$:

$$\boxed{D^{2m}(a')^{m-1}(b')^{m} \cdot Dma = D^{2m}(a')^{m-1}(b')^{m} \cdot (a' + m) \cdot P_m.} \tag{6.1.4}$$

Step 5 (Deduce that $D = 0 \mod \ell^M$): For non-zero elements $\eta \in \mathbb{Z}/\ell^s$ we will denote by $\mathbf{o}(\eta) = \mathrm{ord}_\ell(\tilde{\eta})$ where $\tilde{\eta}$ denotes some lift of η to $\mathbb{Z}_\ell$; we observe that $\mathbf{o}(rt) = \mathbf{o}(r) + \mathbf{o}(t)$ if $r, t, rt \neq 0 \mod \ell^s$.

Assume, for a contradiction, that $D \neq 0 \mod \ell^M$ so that $\mathbf{o}(D) \leq M - 1 = 2(n-1)$. Take $1 \leq m \leq \ell^{3n-2} - 1$ to be a representative for $-a' \mod \ell^{3n-2}$ and thus, in particular, $\mathbf{o}(m) \leq n - 1$. Observe that

$$N' = (6\ell^{3n-2} - 7)(n-1) + 3n - 2 \geq (6m - 1)(n-1) + 3n - 2.$$

Let us now consider the orders of the elements in the left-hand-side of Equation (6.1.4). Since $\mathbf{o}(D) \leq 2n-2$ and $\mathbf{o}(a'), \mathbf{o}(b'), \mathbf{o}(m) \leq n-1$ we deduce that:

$$2m\mathbf{o}(D) + (m-1)\mathbf{o}(a') + m\mathbf{o}(b') + \mathbf{o}(D) + \mathbf{o}(m) + 1 \leq (6m-1)(n-1) + 3n - 2$$

Moreover, we recall that $\mathbf{o}(a) = 0$. Thus left-hand-side of equation (6.1.4) is non-zero as an element of $\mathbb{Z}/\ell^{N'}$. We deduce, in particular, that $\mathbf{o}(D) + \mathbf{o}(m) = \mathbf{o}(a' + m) + \mathbf{o}(P_m)$ by Equation (6.1.4). However, $a' + m = 0 \mod \ell^{3n-2}$ so that:

$$3n - 3 \geq \mathbf{o}(D) + \mathbf{o}(m) = \mathbf{o}(a' + m) + \mathbf{o}(P_m) \geq 3n - 2$$

and this is a contradiction.

We therefore obtain that $D = 0 \mod \ell^M$, as required. Using the discussion preceeding Step 1 above, this then implies the Main Claim. And thus, finally, we've proven Theorem 6.1.1 for $n \in \mathbb{N}$.

Case $n = \infty$:

This will follow from a limit argument using the $n \in \mathbb{N}$ case proved above. Let $f, g \in \mathcal{G}_K^a(\infty)$ be a given C-pair. Equivalently, f_n, g_n form a C-pair for all $n \in \mathbb{N}$. Consider, then:

$$T := \ker f \cap \ker g, \quad T_n := \ker f_n \cap \ker g_n.$$

Then $T_n \geq T_{n+1}$ and $T = \bigcap_n T_n$. Denote by $\Psi = (f, g)$ and $\Psi_n = (f_n, g_n)$. Denote by H the subgroup generated by T and all $x \notin T$ such that $\Psi(1+x) \neq \Psi(1), \Psi(x)$.

Arguing as in the previous case, it suffices to show that

$$\mathrm{Hom}(K^\times/T, \mathbb{Z}_\ell)/\mathrm{Hom}(K^\times/H, \mathbb{Z}_\ell)$$

is topologically cyclic as a pro-ℓ group. In order to show this, it suffices to prove that $(T_n \cdot H)/T_n$ is cyclic for all $n \in \mathbb{N}$.

For each $n \in \mathbb{N}$ denote by H_n the subgroup generated by T_n and all $x \notin T_n$ such that $\Psi_n(1+x) \neq \Psi_n(1), \Psi_n(x)$. Furthermore, if $\Psi_n(x) \neq 0$ and $\Psi_n(1+x) \neq \Psi_n(1), \Psi_n(x)$ then also $\Psi_N(x) \neq 0$ and $\Psi_N(1+x) \neq \Psi_N(1), \Psi_N(x)$ for all $N \geq n$. Thus, $H_n \leq T_n \cdot H_N$ and so $H_n/T_n \leq (T_n \cdot H_N)/T_n$. Therefore $(T_n \cdot H)/T_n = \bigcup_{N \geq n}(T_n \cdot H_N)/T_n$ is an inductive union. By the first case, H_N/T_N is always cyclic (for all N) and thus $(T_n \cdot H_N)/T_n$ is cyclic for all $N \geq n$. Therefore, $(T_n \cdot H)/T_n$ is cyclic, as required. This completes the proof of Theorem 6.1.1 for all $n \in \overline{\mathbb{N}}$. $\square$

Chapter 7

Valuative Subgroups

In this chapter we prove the main theorems which allow us to detect valuations using C-pairs in a more precise way. To begin, we introduce the notion of a valuative subgroup $I \leq \mathcal{G}_K^a(n)$ which generalizes the notion of a "flag function" from [BT02]; the familiar Galois theoretical analogue of a valuative subgroup is a subgroup which is contained in an inertia group of some valuation. For a valuative subgroup $I \leq \mathcal{G}_K^a(n)$ we will associate a canonical valuation v_I which is reminiscent of Pop's notion of a core of a valuation in a Galois extension; our definition also agrees with the valuation of the form $\mathcal{O}(H, H)$ constructed in [AEJ87] – see the definition in Chapter 4. To a valuative element $f \in \mathcal{G}_K^a(n)$, we also associate a canonical valuation v_f which resembles Pop's canonical valuation associated to an inertia element – see [Pop10b]. It turns out, as we will soon see, that the C-pair property is intimately related to the comparability of these canonical valuations v_I; we will show that,

in certain cases, we can "glue" valuative subgroups together to produce a larger *valuative* subgroup.

In this section we will use results from the theory of rigid elements. While one can use many references in the subject to deduce these results (see e.g. the overview in the introduction), we will take [AEJ87] to be our reference of choice as we did in Chapter 4. We begin by recalling some minimal conditions for the existence of a valuation relative to a subgroup $H \leq K^\times$.

Definition 7.0.3. A subgroup $H \leq K^\times$ will be called **valuative** if it satisfies the equivalent conditions of Corollary 4.0.2 – i.e. H satisfies one of the following equivalent conditions:

1. There exists a valuation v of K so that $U_v \leq H$.

2. For all $x, y \in K^\times \smallsetminus H$ one has $1 + x \in H \cup x \cdot H$; and, if $1 + x, 1 + y \in H$, then $1 + x \cdot (1 + y) \in H$ as well.

Similarly, $I \leq \mathcal{G}_K^a(n)$ will be called valuative provided that $I^\perp$ is valuative – equivalently there exists a valuation v of K such that $I \leq I_v(n)$. We also say that $f \in \mathcal{G}_K^a(n)$ is valuative provided that $\ker(f)$ is valuative – equivalently there exists a valuation v of K such that $f \in I_v(n)$.

Lemma 7.0.4. *Let K be a field and let H be a valuative subgroup of $K^\times$. Then there exists a unique coarsest valuation v_H such that $U_{v_H} \leq H$. If w is a valuation of K such that $U_w \leq H$, then v_H is a coarsening of w; moreover $w = v_H$ if and*

only if $w(H)$ contains no non-trivial convex subgroups.

In particular, let $I \leq \mathcal{G}_K^a(n)$ be a valuative subgroup. Then there exists a unique coarsest valuation v_I, depending only on I, such that $I \leq I_{v_I}(n)$. If $I \leq I_w(n)$ then v_I is coarser than w. Moreover, $v_I = w$ if and only if $w(I^\perp)$ contains no non-trivial convex subgroups.

Proof. Let w be any valuation such that $U_w \leq H$ and consider the coarsening v of w which corresponds to the quotient of Γ_w by the maximal convex subgroup of $w(H)$. This is the coarsest coarsening v of w such that $U_v \leq H$. By construction, $v(H)$ contains no non-trivial convex subgroups. We deduce that whenever $x, y \in K^\times$ such that $v(x) = v(y) \mod v(H)$ but $v(x) < v(y)$, there exists a $z \in K^\times$ such that $v(x), v(y) \neq v(z) \mod v(H)$ and $v(x) < v(z) < v(y)$.

Now suppose $h \in H$ and $x \notin H$. Then $v(h) \neq v(x)$; moreover $v(h) < v(x)$ iff $h + x \in H$ and $v(h) > v(x)$ iff $h + x \in x \cdot H$. An element $h \in H$ such that $1 + x = h + x \mod H$ for all $x \in K^\times \smallsetminus H$ must be in U_v by the discussion above. We deduce that U_v depends only on H and K, but not at all on the original choice of w. Indeed, U_v is precisely the set of all $h \in H$ such that for all $x \in K^\times \smallsetminus H$ one has $1 + x = h + x \mod H$. □

Definition 7.0.5. We make the following definitions:

1. Suppose $H \leq K^\times$ is a valuative subgroup. We denote by v_H the canonical valuation associated to H as described in Lemma 7.0.4. I.e. v_H is the unique coarsest valuation such that $U_{v_H} \leq H$.

2. Similarly, suppose $I \leq \mathcal{G}_K^a(n)$ is valuative. We denote by v_I the valuation v_H for $H = I^\perp$. I.e. v_I is the unique coarsest valuation such that $I \leq I_{v_I}(n)$.

3. If $f \in \mathcal{G}_K^a(n)$ is a given valuative element, we denote by $v_f := v_{\langle f \rangle} = v_{\ker f}$.

The way we will be able to "glue" valuative subgroups is by proving that their associated valuations are comparable. Our first result which proves comparability of valuations is the following avatar of the approximation theorem:

Lemma 7.0.6. *Let v_1, v_2 be two valuations and assume that f is a non-valuative element of $\mathcal{G}_K^a(n)$ such that $f \in D_{v_1}(n) \cap D_{v_2}(n)$. Then v_1, v_2 are comparable.*

Proof. Denote by w the valuation associated to the finest common coarsening of v_1, v_2; i.e. $\mathcal{O}_w = \mathcal{O}_{v_1} \cdot \mathcal{O}_{v_2}$. Denote by $H = \ker f$. As $U_{v_1}^1, U_{v_2}^1 \leq H$, $H \neq K^\times$ and w is a coarsening of v_1, v_2 we deduce from the Approximation Theorem that w is non-trivial – indeed otherwise v_1, v_2 would be independent valuations and therefore $(U_{v_1}^1) \cdot (U_{v_2}^1) = K^\times$ by Corollary 2.3.2.

Consider $H_w \leq k(w)^\times$ the kernel of the canonical surjection $k(w)^\times \to U_w \cdot H/H$. Denote by $w_i = v_i/w$. One has $U_{w_i}^1 \leq H_w$ while, if both w_i are non-trivial, they must be independent. However, we note that $H_w \neq k(w)^\times$ since $U_w \cdot H/H \cong k(w)^\times/H_w$ and U_w is not contained in H by our assumption on f. In particular, either w_1 or w_2 must be trivial and so v_1, v_2 are comparable. □

The following proposition and the remarks which proceed it are the main techniques we use to prove the comparability of our canonical valuations v_H in certain

situations, and thus prove the existence of many valuative subgroups.

Proposition 7.0.7. *Let $f, g \in \mathcal{G}_K^a(n)$ be given valuative elements. Denote by $\Psi = (f, g)$. Then the following are equivalent:*

1. *v_f and v_g are comparable.*

2. *$\langle f, g\rangle$ is valuative.*

3. *$\langle \Psi(1-x), \Psi(x)\rangle$ is cyclic for all $x \in K^\times \smallsetminus \{1\}$.*

Proof. Clearly (1) and (2) are equivalent by Lemma 7.0.4 and (2) $\Rightarrow$ (3) follows from Lemma 6.0.7. Thus, it remains to show that (3) $\Rightarrow$ (2). Denote by $\Psi = (f, g)$ and denote by $T = \ker \Psi$. Assume that whenever $x \neq 0, 1$ one has:

$$\langle \Psi(1-x), \Psi(x)\rangle \text{ is cyclic.}$$

Since $\Psi(-1) = 0$, one equivalently has: $\langle \Psi(1+x), \Psi(x)\rangle$ is cyclic whenever $x \neq 0, -1$. Since Λ_n is a quotient of a discrete valuation ring, we deduce that this condition is equivalent to: $\Psi(1+x) = a \cdot \Psi(x)$ or $\Psi(x) = a \cdot \Psi(1+x)$ for some $a \in \Lambda_n$.

Let $x \notin T$ be given; we will first show that $\Psi(1+x) = \Psi(1)$ or $\Psi(1+x) = \Psi(x)$. As f, g are valuative, we recall that, for all $x \neq 0$ such that $f(x) \neq 0$, one has $f(1+x) = f(1)$ or $f(x)$ and similarly with g. Assume first that $\Psi(1+x) = a \cdot \Psi(x)$. Thus: $f(1+x) = af(x)$ and $g(1+x) = ag(x)$. We have some cases to consider. First, if $g(x) = 0$ or $f(x) = 0$ we trivially have $\Psi(1+x) = \Psi(1)$ or $\Psi(x)$. On the

other hand, suppose $f(x), g(x) \neq 0$. Assume, for example, that $f(1+x) = f(x)$ and $g(1+x) = g(1) = 0$. Then $f(x) = af(x)$ and $ag(x) = 0$. But then a must be a unit in Λ_n (in fact $a \in 1 + \ell\Lambda_n$) and so $g(x) = 0$ which contradicts our assumption. We therefore deduce that $f(1+x) = f(x)$ iff $g(1+x) = g(x)$ and $f(1+x) = 0$ iff $g(1+x) = 0$. In particular, $\Psi(1+x) = \Psi(x)$ or $\Psi(1+x) = \Psi(1)$.

On the other hand, if $\Psi(x) = a\Psi(1+x)$ but $\ell|a$, this contradicts the fact that f and g are valuative and $\Psi(x) \neq 0$. Thus, we've shown that whenever $\Psi(x) \neq 0$ one has $\Psi(1+x) = \Psi(1)$ or $\Psi(1+x) = \Psi(x)$.

Assume now that $x, y \notin T$ are given such that $\Psi(1+x) = \Psi(1+y) = 0$. We will show that $\Psi(1+x(1+y)) = 0$. Observe that $\Psi(1+x(1+y)) = a\Psi(x)$ with $a = 0$ or $a = 1$, since $\Psi(1+y) = 0$ and $\Psi(x) = \Psi(x(1+y)) \neq 0$. Assume first that $\Psi(y) = -\Psi(x)$ then $f(x) = 0$ iff $f(y) = 0$ and $g(x) = 0$ iff $g(y) = 0$. If $f(x) = 0$ then $f(1+x(1+y)) = 0$ as well from the above and similarly for g. If $f(x) \neq 0$ then $f(1+x(1+y)) = 0$ since f is valuative and similarly for g; see Corollary 4.0.2.

On the other hand, assume that $\Psi(x) \neq -\Psi(y)$. Then $\Psi(1+x(1+y)) = \Psi(t+xy) = b\Psi(xy)$ for some $t \in T$ and $b = 0$ or $b = 1$. Furthermore, $\Psi(1+x(1+y)) = a \cdot \Psi(x)$ where $a = 0$ or $a = 1$, as above. But then $a\Psi(x) = b\Psi(xy)$, $a, b \in \{0, 1\}$, $\Psi(x), \Psi(y) \neq 0$ and $\Psi(xy) \neq 0$; the only possibility for this is if $a, b = 0$. Now using Corollary 4.0.2, we deduce that T is indeed valuative – i.e. $\langle f, g\rangle$ is a valuative subgroup of $\mathcal{G}_K^a(n)$. □

Remark 7.0.8. In this remark we will compare the condition of Proposition 7.0.7

with the C-pair property. Let $f, g \in \mathcal{G}_K^a(n)$ be given and denote by $\Psi = (f, g)$. Assume that $n = 1$ or $n = \infty$. Since Λ_n is a domain in this case, the following are equivalent:

1. $\langle \Psi(1-x), \Psi(x) \rangle$ is cyclic for all $x, \neq 0, 1$.

2. f, g form a C-pair.

For general $n \in \overline{\mathbb{N}}$, however, this is completely false. However, we can say the following in general using the cancellation principle or, more precisely, Lemma 6.1.2.

Let $n \in \overline{\mathbb{N}}$ be arbitrary and denote by $M = \mathbf{M}_1(n) = 2n-1$ ($M = \mathbf{M}_1(\infty) = \infty$). Let $f, g \in \mathcal{G}_K^a(n)$ be given, denote by $\Psi = (f, g)$ and assume that $\langle \Psi(1-x), \Psi(x) \rangle$ is cyclic for all $x \neq 0, 1$. Then f, g trivially form a C-pair.

Conversely, assume that $f', g' \in \mathcal{G}_K^a(M)$ form a C-pair and denote by $\Psi = (f'_n, g'_n)$. Then $\langle \Psi(1-x), \Psi(x) \rangle$ is cyclic for all $x \neq 0, 1$. Let us recall the proof of this fact from Lemma 6.1.2. Assume, for example, that $g'(1-x) = ag'(x)$ (the other option is $g'(1-x) = bg'(x)$ and we simply replace x with $1-x$ in this case). As $f'(1-x)g'(x) = f'(x)g'(1-x)$ we deduce that:

$$f'(1-x)g'(x) = f'(x)ag'(x).$$

By the cancellation principle, we deduce that, if $g(x) \neq 0$, one has $f(1-x) = af(x)$. Thus $\Psi(1-x) = a\Psi(x)$. On the other hand, $g(x) = 0$ implies that $g(1-x) = ag(x) = 0$ so that still $\langle \Psi(1-x), \Psi(x) \rangle$ is cyclic.

Using the fact that for any valuation v of K the canonical map $I_v(\mathbf{M}_1(n)) \to I_v(n)$ is surjective (since $\Gamma_v = K^\times/U_v$ is torsion-free), along with Proposition 7.0.7 and the discussion of Remark 7.0.8, we deduce the following fact which summarizes the discussion:

Lemma 7.0.9. *Let $f, g \in \mathcal{G}_K^a(n)$ be valuative elements. Then the following are equivalent:*

1. *v_f and v_g are comparable.*

2. *$\langle f, g\rangle$ is valuative.*

3. *There exists a C-pair $f', g' \in \mathcal{G}_K^a(\mathbf{M}_1(n))$ such that $f'_n = f$, $g'_n = g$.*

The results above allow us to say when a subgroup generated by valuative elements is itself valuative. Indeed, assume that I is valuative and $f \in I$; then v_f is a coarsening of v_I by Lemma 7.0.4. Thus, if $f_i \in \mathcal{G}_K^a(n)$ are valuative, then the following are equivalent:

1. $I = \langle f_i\rangle_i$ is valuative.

2. $v_i := v_{f_i}$ are comparable.

Moreover, when these equivalent statements hold, then v_I is the valuation-theoretic supremum of the v_i; we recall our convention that $w \leq v$ provided w is a coarsening of v (i.e. $\mathcal{O}_w \supset \mathcal{O}_v$).

Now that we've explored the connection between C-pairs and elements of $I_v(n)$, we next treat $D_v(n)$ as well in the following lemma:

Lemma 7.0.10. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $M = \mathbf{M}_1(n)$. Let K be a field and let $f \in \mathcal{G}_K^a(M)$ be a valuative element. Suppose that $g \in \mathcal{G}_K^a(M)$ forms a C-pair with f. Denote by $v = v_{f_n}$. Then $g_n \in D_v(n)$.*

Proof. For sake of notation, we will assume that $n \in \mathbb{N}$, but the proof in the $n = \infty$ case is virtually identical. Let $x \in K^\times$ be given such that $v(x) > 0$ and $f(x) \neq 0 \mod \ell^n$. Then $f(1-x) = 0 \mod \ell^n$ implies that $f(1-x) = 0$ as well – indeed, f is valuative so $f(1-x) = f(1)$ or $f(x)$ and $f(x) \neq 0 \mod \ell^n$. Then $f(1-x) = 0$ and thus $f(x)g(1-x) = 0$. Since $f(x) \neq 0 \mod \ell^n$, we deduce from the cancellation principle that $g(1-x) = 0 \mod \ell^n$.

On the other hand, if $v(y) > 0$ yet $f(y) = 0 \mod \ell^n$, by Lemma 7.0.4, there exists x such that $0 < v(x) < v(y)$ and $f(x) \neq 0 \mod \ell^n$. Now by the first case, we deduce that $g(1-x) = 0 \mod \ell^n$. Moreover, $v(x + y(1-x)) = v(x)$ and so $f(x+y(1-x)) = f(x) \neq 0 \mod \ell^n$; thus $g((1-x)(1-y)) = g(1-(x+y(1-x)) = 0 \mod \ell^n$ by the first case. But this implies that $g(1-y) = 0 \mod \ell^n$ as well. Therefore, $g(U_v^1) = 0 \mod \ell^n$, as required. □

We are now ready to state the main theorem of the paper which deals with C-groups. This theorem, along with Theorem 12.0.2 directly generalizes the main theorem of [BT02].

Theorem 7.0.11. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_1(n))$. Let $D'' \leq \mathcal{G}_K^a(N)$ be given and assume that D'' is a C-group. Then $D := D''_n$ contains a valuative subgroup $I \leq D$ such that*

- D/I *is cyclic.*

- $D \leq D_{v_I}(n)$.

Proof. Denote by $M = \mathbf{M}_1(n)$ and $D' = D''_M$. Consider the subgroup I' of D' generated by all valuative elements $f \in D'$. By Theorem 6.1.1, D'/I' is cyclic. Moreover, by Lemma 7.0.9 and Remark 7.0.8, I' is valuative, since v_f and v_g are comparable for any $f, g \in I'$ as $\mathbf{N}(M) \geq \mathbf{M}_1(M)$; thus $I := I'_n$ is valuative as well. Moreover, by Lemma 7.0.10, for all $d \in D := D'_n$ and $i \in I$, one has $d \in D_{v_i}(n)$. Since $v_I = \sup_{i \in I} v_i$ is the valuation-theoretic supremum of v_i as $i \in I$ varies, we have $d \leq D_{v_I}(n)$. Thus $D \leq D_{v_I}(n)$, as required. □

We now prove a theorem which allows us to detect the groups $I_v(n)$ within subgroups of $D_v(n)$. This will be needed later on in order to detect $I_v(n)$ and $D_v(n)$ precisely in certain situations.

Theorem 7.0.12. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let $I'' \leq D'' \leq \mathcal{G}_K^a(N)$ be given and denote by $I = I''_n$ and $D = D''_n$. Assume that whenever $i \in I''$ and $d \in D''$, i, d form a C-pair (i.e. $I'' \leq \mathbf{I}^{\mathrm{C}}(D'')$). Assume moreover that D is not a C-group. Then I is valuative and $D \leq D_{v_I}(n)$.*

Proof. Denote by $M = \mathbf{M}_1(n)$ and denote by $I' = I''_M$ and $D' = D''_M$. Arguing similarly to Theorem 7.0.11 (i.e. using Lemma 7.0.10), it suffices to prove that every $f \in I'$ is valuative. Assume for a contradiction that $f \in I'$ is non-valuative and let $g_1, g_2 \in D'$ be given such that $\langle f, g_i \rangle$ is non-cyclic – we will show that

$\langle f, g_1, g_2\rangle$ must form a C-group. Then, as we vary over all g_1, g_2, we deduce that D' (and thus D) is a C-group as well which provides the required contradiction.

For the remainder of the proof, denote by $M' = \mathbf{M}_2(M) = \mathbf{M}_2(\mathbf{M}_1(n))$. Take lifts $f' \in I''_{M'}$ and $g'_i \in D''_{M'}$ for f resp. g_i. Then by Theorem 6.1.1, there exist valuations v_i such that:

- $\langle f', g'_i\rangle \in D_{v_i}(M')$
- $\langle f', g'_i\rangle/(\langle f', g'_i\rangle \cap I_{v_i}(M'))$ is cyclic.

For $i = 1$ and $i = 2$, we deduce that there exists $(a_i, b_i) \in \Lambda^2_{M'} \smallsetminus \ell \cdot \Lambda^2_{M'}$ with $a_i f' + b_i g'_i \in I_{v_i}(M')$. Indeed otherwise $\langle f', g'_i\rangle \cap I_{v_i}(M')$ is contained in $\langle \ell \cdot f', \ell \cdot g'_i\rangle = \ell \cdot \langle f', g'_i\rangle$ but $\langle f', g'_i\rangle/\ell$ is non-cyclic by our assumption that $\langle f', g'_i\rangle$ is non-cyclic.

Since f is non-valuative we deduce that $b_i g'_i \neq 0 \mod \ell^M$ and thus $b_i \neq 0 \mod \ell^M$. Indeed, if a_i is a unit and $b_i g'_i = 0 \mod \ell^M$, this would imply that f is valuative. On the other hand, if b_i is a unit, then $b_i g'_i \neq 0 \mod \ell^M$ since $g_i \neq 0 \mod \ell^M$. Furthermore, since f' is non-valuative, the v_i must be comparable by Lemma 7.0.6. In particular, $\langle f', a_1 f' + b_1 g'_1, a_2 f' + b_2 g'_2\rangle = \langle f', b_1 g'_1, b_2 g'_2\rangle$ forms a C-group by Lemma 6.0.7 and Proposition 7.0.7. By the cancellation principle, $\langle f, g_1, g_2\rangle$ form a C-group as well. Indeed, for all $x \in K^\times \smallsetminus \{1\}$ one has:

$$b_1 b_2 g'_1(1-x) g'_2(x) = b_1 b_2 g'_1(x) g'_2(1-x);$$

thus we also have $g_1(1-x)g_2(x) = g_1(x)g_2(1-x)$ by the cancellation principle since $b_1, b_2 \neq 0 \mod \ell^M$ and $M' = \mathbf{M}_2(M)$. □

Chapter 8

Detecting Valuations using C-pairs

In this chapter, we show how to detect precisely the subgroups $D_v(n)$ and $I_v(n)$ for certain "maximal" valuations v. We also show that, in the case of function fields, these "maximal" valuations include the Parshin chains of divisors.

First, let us make a few observations. Note that when $\mathcal{G}_K^a(n)$ is cyclic, one cannot expect to detect anything. This is perhaps best illustrated with two contrasting examples. First consider $K = \mathbb{C}((t))$. Then $\mathcal{G}_K^a(n)$ is cyclic by Kummer theory, the whole $\mathcal{G}_K^a(n)$ is valuative and its corresponding valuation is the t-adic one. On the other hand, consider $K = \overline{\mathbb{F}}_p(\mu_\ell)$ $(p \neq \ell)$. By Kummer theory, $\mathcal{G}_K^a(n)$ is again cyclic, but K has no non-trivial valuations since $K \subset \bar{\mathbb{F}}_p$. In particular, when $\mathcal{G}_K^a(n)$ is cyclic, we cannot expect to determine whether anything is valuative. Because of

this observation and the compatibility in taking residue fields (see Lemma 6.0.8), one cannot expect to detect $I_v(n)$ within $D_v(n)$ when $\mathcal{G}^a_{k(v)}(n)$ is cyclic.

Furthermore, in light of Theorem 7.0.12, in order to detect $I_v(n)$ and $D_v(n)$, we will need to ensure that the canonical maps $I_v(N) \to I_v(n)$ and $D_v(N) \to D_v(n)$ are surjective so that we have sufficiently many C-pairs of $\mathcal{G}^a_K(n)$ which lift to C-pairs in $\mathcal{G}^a_K(N)$. The first map, $I_v(N) \to I_v(n)$ is always surjective as Γ_v is torsion-free; on the other hand, the map $D_v(N) \to D_v(n)$ need not be surjective. Fortunately, it is surjective in two important cases which we consider below. First, if K contains sufficiently many roots of unity (and thus the same is true for $k(v)$) this map is surjective. Secondly, if $N = n$, this map is trivially surjective; denoting $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$ as in Theorem 7.0.12, we see that $N = n$ iff $n = 1$ or $n = \infty$.

We will therefore eventually consider two separate cases. First will be the case where K contains sufficiently many roots of unity – more precisely, we will require that the polynomial $X^{2\ell^n} - 1$ splits completely in K while making no other assumptions on K (in particular $\operatorname{Char} K$ might still be ℓ in which case this condition is always satisfied). Second will be the case where $n = 1$ or $n = \infty$ in which case $\mathbf{N}(n) = \mathbf{M}_r(n) = n$. However, we will begin by introducing the set of valuations v of K for which we will be able to detect $I_v(n)$ and $D_v(n)$ precisely. This set, which we denote by $\mathcal{V}_{K,n}$ will be essentially independent of choice of n (see Lemma 8.2.6) and will contain almost all valuations of arithmetic/geometric interest in the usual contexts of birational anabelian geometry.

8.1 The set $\mathcal{V}_K$

Definition 8.1.1. Let $n \in \overline{\mathbb{N}}$ be given and denote by $N := \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field.

Consider the following conditions on a valuation v of K:

1. Γ_v contains no non-trivial ℓ-divisible convex subgroups. Equivalently by Lemma 7.0.4, $v = v_I$ for $I = I_v(n)$; indeed, $v(I^\perp) = \ell^n \cdot \Gamma_v$ contains the convex subgroup Δ if and only if Δ is ℓ^n-divisible if and only if Δ is ℓ-divisible, since Δ, Γ_v and Γ_v/Δ are all torsion-free.

2. v is maximal among all valuations w such that $D_v^n = D_w^n$ and Γ_w contains no non-trivial ℓ-divisible convex subgroups; i.e. for all refinements w of v such that $D_w^n = D_v^n$ as subgroups of $\mathcal{G}_K^{a,n}$, one has $I_w^n = I_v^n$.

3. $\mathcal{G}_{k(v)}^a(n)$ is non-cyclic.

We will denote by $\mathcal{V}_{K,n}$ the collection of valuations v of K which satisfy conditions (1),(2),(3) above. For the sake of Example 8.1.2 and some of the arguments in this chapter, we will also denote by $\mathcal{W}_{K,n}$ the collection of valuations v which satisfy only conditions (1) and (2), although we will not use $\mathcal{W}_{K,n}$ in the statement of any theorem.

We also introduce notation for the group-theoretical analogue of $\mathcal{V}_{K,n}$, which will make the statements of Remarks 8.2.5 and 8.3.4 much more elegant and intuitive. We denote by $\mathcal{D}_{K,n}$ the collection of subgroups $D \leq \mathcal{G}_K^a(n)$ endowed with $I \leq D$

which satisfy the following conditions:

1. There exist $D' \leq \mathcal{G}_K^a(N)$ such that $(\mathbf{I}^{\mathrm{C}}(D'))_n = I$, $D'_n = D$.

2. $I \leq D \leq \mathcal{G}_K^a(n)$ are maximal with this property. Namely, if $D \leq E \leq \mathcal{G}_K^a(n)$ and $E' \leq \mathcal{G}_K^a(N)$ is given such that $E'_n = E$ and $I \leq (\mathbf{I}^{\mathrm{C}}(E'))_n$, then $D = E$ and $I = (\mathbf{I}^{\mathrm{C}}(E'))_n$.

3. $\mathbf{I}^{\mathrm{C}}(D) \neq D$ (i.e. D is not a C-group).

To make the notation simpler in Remarks 8.2.5 and 8.3.4, we introduce notation for subsets relative to a given fixed valuation v in $\mathcal{V}_{K,n}$. Namely, given a fixed $v \in \mathcal{V}_{K,n}$ we will consider the following subsets of $\mathcal{V}_{K,n}$ resp. $\mathcal{D}_{K,n}$.

1. We denote by $\mathcal{D}_{v,n}$ the subset of $\mathcal{D}_{K,n}$ consisting of $I \leq D$ such that $I_v(n) \leq I \leq D \leq D_v(n)$.

2. We denote by $\mathcal{V}_{v,n}$ the subset of $\mathcal{V}_{K,n}$ consisting of valuations finer than v.

The set $\mathcal{V}_{K,n}$ contains many valuations of arithmetic/geometric interest. The main examples of such valuations arise from prime divisors as will be shown in the following example.

To keep the discussion as general as possible, we introduce some terminology. We will say that a field k is **strongly ℓ-closed** provided that for any finite extension $k'|k$ one has $(k')^{\times} = (k')^{\times \ell}$. If $\mathrm{Char}\, k \neq \ell$, then k is strongly ℓ closed if and only if the ℓ-Sylow subgroups of G_k are all trivial. Also, if $\mathrm{Char}\, k = \ell$, then k is strongly ℓ

closed if and only if k is perfect. In particular, all algebraically closed fields of any characteristic are strongly ℓ-closed.

Observe that, if v_0 is a valuation of a strongly ℓ-closed field k, then $k(v_0)$ is also strongly ℓ-closed. In this example, we will show that geometric Parshin chains (i.e. compositions of valuations of a function field associated to Weil prime divisors) are elements of $\mathcal{W}_{K,n}$, where K is a function field over a strongly ℓ-closed field k. In particular the non-degenerate Parshin chains of non-maximal length will lie in $\mathcal{V}_{K,n}$ while the non-degenerate maximal length Parshin chains will lie in $\mathcal{W}_{K,n} \setminus \mathcal{V}_{K,n}$. This will be done in two steps. First, we show that valuations associated to Weil prime divisors lie in $\mathcal{W}_{K,n}$ for function fields $K|k$ as above; in fact we will prove a more general statement about valuations whose residue field is a function field. Second, we will show that compositions of valuations from $\mathcal{W}_n$ lie in $\mathcal{W}_n$ and this will hold for arbitrary fields.

Example 8.1.2. Our first claim will, in particular, imply that valuations associated to prime divisors (and more generally quasi-prime divisors) are elements of $\mathcal{W}_{K,n}$, and in most cases of $\mathcal{V}_{K,n}$. The second claim concerns the valuation-theoretic compositions of valuations in $\mathcal{W}_n$. Together, these two claims imply that Parshin-chains of (quasi-)prime divisors of non-maximal length are elements of $\mathcal{V}_{K,n}$ while the chains of maximal length are elements of $\mathcal{W}_{K,n}$.

Prime Divisors: Suppose K is a field in which the polynomial $X^{2\ell^n} - 1$ splits completely. Let v be a valuation of K such that Γ_v contains no non-trivial ℓ-divisible

convex subgroups and that $k(v)$ is a function field over a strongly ℓ-closed field k. We claim that $v \in \mathcal{W}_{K,n}$.

To prove this claim, first assume that $k(v)|k$ has transcendence degree ≥ 1. Assume that w is a refinement of v and that $D_w(n) = D_v(n)$. Then $I_v(n) \leq I_w(n) \leq D_w(n) = D_v(n)$. We must show that $I_v(n) = I_w(n)$. Denote by $F = k(v)$ and consider the valuation $w/v =: w'$ of F induced by w. Observe that $I_v(n) = I_w(n)$ if and only if $I_{w'}(n) = 1$ as a subgroup of $\mathcal{G}_F^a(n)$ since we have a canonical isomorphism $I_w(n)/I_v(n) \cong I_{w/v}(n)$. Thus, we can assume without loss of generality that $n = 1$ (see e.g. Lemma 8.2.1 and/or Lemma 8.2.6).

Assume, for a contradiction, that $0 \neq f \in I_{w'}(1)$ and denote by $T = \ker f$. Then $F^\times/T = \langle x \mod T \rangle \cong \mathbb{Z}/\ell$. Furthermore, for all $g \in \mathcal{G}_F^a(1)$, f, g form a C-pair by Lemma 6.0.7. In particular, for all $H \leq F^\times$, $F^{\times\ell} \leq H$, such that $F^\times/H \cong \mathbb{Z}/\ell$, the group $\mathrm{Hom}(F^\times/(H \cap T), \mathbb{Z}/\ell)$ is a C-group.

Now assume that x, y are $\mathbb{Z}/\ell$ independent in $F^\times/\ell$. Then we can choose T_0 such that $F^{\times\ell} \leq T_0 \leq T \leq F^\times$ and $F^\times/T_0 = \langle x, y \rangle \cong \mathbb{Z}/\ell \times \mathbb{Z}/\ell$. Thus, $\mathrm{Hom}(F^\times/T_0, \mathbb{Z}/\ell)$ is a C-group. By the K-theoretic criterion for C-pairs (see Proposition 10.2.1, the proof of which is self-contained) we deduce, in particular, that $\{x, y\}_{T_0} \neq 0$ as an element of $K_2^M(F)/T_0$ (see Chapter 10 for a review of the definition of Milnor K-theory mod T_0). In particular, $\{x, y\} \neq 0$ as an element of $K_2^M(F)/\ell$.

We will show that this provides a contradiction. First, since $x \notin F^{\times\ell}$ and k is

strongly ℓ-closed, we deduce that x is transcendental over k. Consider the subfield $L = \overline{k(x)} \cap F$ the relative algebraic closure of $k(x)$ (the rational function field) inside F. Our aim will be to find $y \in k(x)^\times$ so that the images of x, y in $L^\times/\ell$ are independent.

If $\operatorname{Char} k \neq \ell$, the existence of such a y is trivial since the image of the canonical map $k(x)^\times/\ell \to L^\times/\ell$ is infinite – in fact, the image has finite index in $L^\times/\ell$ by Kummer theory since $L|k(x)$ is a finite extension and $\mu_\ell \subset k$. If, on the other hand, $\operatorname{Char} k = \ell$, we see that k is perfect and, since $x \notin L^{\times\ell}$, the extension $L|k(x)$ is separable. Consider the unique complete normal model C for $L|k$ together with the (possibly branched) cover $C \to \mathbb{P}^1_k$ induced by $k(x) \to L$. By the approximation theorem, there exists a prime divisor P of $\mathbb{P}^1_k$ and a function $y \in k(x)^\times$ such that P is unramified in the cover $C \to \mathbb{P}^1_k$, $P \neq 0, \infty$, and $v_P(y) = 1$ (here v_P denotes the valuation associated to P). Since P is unramified in C, for any prolongation P' of P to C, one also has $v_{P'}(y) = 1$. Moreover, as $P \neq 0, \infty$ and the divisor associated to x is precisely $0 - \infty$, we deduce that y is not a power of x in $L^\times/\ell$.

We now recall a theorem of Milnor stating that the following sequence is exact:

$$0 \to K_2^M(k) \to K_2^M(k(x)) \to \bigoplus_{P \in \mathbb{A}^1_k} K_1^M(k(P)) \to 0$$

where the last map is the sum of the tame symbols associated to v_P, as P ranges over the prime divisors of $\mathbb{P}^1_k$ with support in $\mathbb{A}^1_k = \operatorname{Spec} k[x]$. However, the extension $k(P)|k$ is finite and thus $k(P)^{\times\ell} = k(P)^\times$ since k is strongly ℓ-closed. Also, this implies that $K_2^M(k)/\ell = 0$. Thus, we deduce that $K_2^M(k(x))/\ell = 0$ and so $\{x, y\} = 0$

in $K_2^M(F)/\ell$. Moreover, since L is relatively algebraically closed in F and x, y are independent in $L^\times/\ell$, they must also be independent in $F^\times/\ell$. This provides the desired contradiction to the discussion above, as we've produced an element $y \in F^\times$ such that x, y are independent in $F^\times/\ell$ and $\{x, y\} = 0$. Thus we've proven that $v \in \mathcal{W}_{K,n}$. Since $\mathcal{G}^a_{k(v)}(n)$ is non-cyclic (as $k(v)$ is a function field of transcendence degree ≥ 1) we see that, actually, $v \in \mathcal{V}_{K,n}$.

On the other hand, if the transcendence degree of $k(v)|k$ is 0, we observe that $k(v)^\times$ is ℓ-divisible since k is strongly ℓ-closed, and so $v \in \mathcal{W}_{K,n} \smallsetminus \mathcal{V}_{K,n}$ trivially.

Compositions of Valuations: We now show that compositions of valuations in $\mathcal{W}_n$ lie in $\mathcal{W}_n$. Suppose that $v \in \mathcal{W}_{K,n}$ is given and $w \in \mathcal{W}_{k(v),n}$. Denote by $w' = w \circ v$ the valuation theoretic composition of v and w. By considering the short exact sequence of value groups:

$$1 \to \Gamma_w \to \Gamma_{w'} \to \Gamma_v \to 1$$

we see immediately that $\Gamma_{w'}$ contains no non-trivial ℓ-divisible convex subgroups since both Γ_w and Γ_v satisfy this condition. Furthermore, suppose that w'' is a refinement of w' such that $D_{w'}(n) = D_{w''}(n)$. Observe that v is a coarsening of w', and thus of w''. Since $D_{w'}(n) = D_{w''}(n)$, we also have $D_w(n) = D_{w''/w}(n)$ and thus $I_w(n) = I_{w''/v}(n)$ (this is condition (2) for $w \in \mathcal{W}_{k(v),n}$). Hence $I_{w'}(n) = I_{w''}(n)$ as well.

8.2 Sufficiently Many Roots of Unity

In this section, we show how to detect $D_v(n)$ and $I_v(n)$ for valuations $v \in \mathcal{V}_{K,n}$ using C-pairs, in the situation where K contains sufficiently many roots of unity. Note however that we do not require our field K to have residue characteristic different from ℓ, but rather that $X^{\ell^N} - 1$ splits completely for sufficiently large N depending on n; this property is inherited in the residue field of any valuation (since valuation rings are integrally closed). The main benefit of this property is the following lemma. However we observe that the statements of the following lemma hold without the assumption that $X^{2\ell^N} - 1$ splits completely in the case where $N = n$ (this observation will be used in the following section).

Lemma 8.2.1. *Let (K, v) be a valued field. Let $N, n \in \overline{\mathbb{N}}$ be given with $N \geq n$ and assume furthermore that the polynomial $X^{2\ell^N} - 1$ splits completely in K (we make no assumptions on* $\operatorname{Char} K$*); if $N = \infty$ we take this to mean that $X^{2\ell^m} - 1$ splits for all $m \in \mathbb{N}$. Then the following hold:*

1. *The following canonical maps are surjective:*
   - $\mathcal{G}_K^a(N) \to \mathcal{G}_K^a(n)$.
   - $I_v(N) \to I_v(n)$.
   - $D_v(N) \to D_v(n)$.
2. *The rank of $\mathcal{G}_K^a(N)$ (as a pro-ℓ-group) is the same as that of $\mathcal{G}_K^a(n)$.*

3. *Let $w \geq v$ be valuations of K and consider the inclusion of subgroups of $\mathcal{G}_K^a(N)$:*

$$I_v(N) \leq I_w(N) \leq D_w(N) \leq D_v(N).$$

Then $I_v(N) = I_w(N)$ iff $I_v(n) = I_w(n)$ and $D_w(N) = D_v(N)$ iff $D_w(n) = D_v(n)$.

Proof. To 1. This is trivial if $n = \infty$, and thus we can assume that both $N, n \in \mathbb{N}$ as the case where $N = \infty$ would follow immediately from this. The Pontryagin dual of the map $\mathcal{G}_K^a(N) \to \mathcal{G}_K^a(n)$ is precisely the map:

$$K^\times/\ell^n \xrightarrow{\ell^{N-n}} K^\times/\ell^N.$$

Indeed our assumption that $X^{2\ell^N} - 1$ splits completely ensures that $-1 \in K^{\times \ell^N}$. Thus, it suffices to prove that this map is injective. Suppose $x \in K^\times$ is given such that $x^{\ell^{N-n}} = y^{\ell^N}$. Then $x = y^{\ell^n} \cdot \zeta$ for some ζ such that $\zeta^{\ell^{N-n}} = 1$. But our assumptions ensure that $\zeta \in K^{\times \ell^n}$ which shows that indeed this map is injective. Dually, the map $\mathcal{G}_K^a(N) \to \mathcal{G}_K^a(n)$ is surjective.

The second claim is trivial as $\Gamma_v = K^\times/U_v$ is torsion-free. The proof of the third claim follows from the first one applied to $k(v)$, along with the fact that $D_v(N)/I_v(N) = \mathcal{G}_{k(v)}^a(N)$ and $D_v(n)/I_v(n) = \mathcal{G}_{k(v)}^a(n)$ (see Lemma 6.0.8). Indeed, the fact that $X^{2\ell^N} - 1$ splits in K implies that the same polynomial splits in $k(v)$ so that the map $\mathcal{G}_{k(v)}^a(N) \to \mathcal{G}_{k(v)}^a(n)$ is surjective.

To 2. As above, we can assume with no loss that $N, n \in \mathbb{N}$. Arguing as in part

(1), one has:

$$\ell^n \cdot \mathcal{G}_K^a(N) = \mathrm{Hom}(K^\times/\pm 1, \ell^n \cdot \Lambda_N).$$

Thus the surjective map $\mathcal{G}_K^a(N) \to \mathcal{G}_K^a(n)$ corresponds precisely to $\mathcal{G}_K^a(N) \to \mathcal{G}_K^a(N)/\ell^n = \mathcal{G}_K^a(n)$ and this proves the claim using the Burnside basis theorem.

To 3. By (1), $I_v(N) = I_w(N)$ implies that $I_v(n) = I_w(n)$ and similarly $D_v(N) = D_w(N)$ implies that $D_v(n) = D_w(n)$. To prove the converse it suffices to assume that v is the trivial valuation by replacing K with $k(v)$ and w by w/v; indeed $I_w(n)/I_v(n) = I_{w/v}(n)$ and $D_w(n)/I_v(n) = D_{w/v}(n)$; see e.g. the first part of Lemma 6.0.8. As such, assume that $I_w(n) = 1$ then $\Gamma_w = \ell^n \cdot \Gamma_w$ and so $\Gamma_w = \ell^N \cdot \Gamma_w$ since Γ_w is torsion-free; this implies that $I_w(N) = 1$. On the other hand, assume that $D_w(n) = \mathcal{G}_K^a(n)$. Then $U_w^1 \leq K^{\times \ell^n}$. Let $x \in U_v^1$ be given, then $x = y^{\ell^n}$ for some $y \in K^\times$. Applying w to both sides we deduce that $y \in U_w$. Denote by $a \mapsto \bar{a}$ the map $U_w \to k(w)^\times$. Then $\bar{y}^{\ell^n} = \bar{1}$ so that there exists a $\bar{z} \in k(w)^\times$ such that $\bar{z}^{\ell^{N-n}} = \bar{y}$; indeed, we recall that the polynomial $X^{\ell^N} - 1$ splits in K. Thus, $y = z^{\ell^{N-n}} \cdot a$ for some $a \in U_w^1$. And thus $x = z^{\ell^N} a^{\ell^n}$. But as $a \in K^{\times \ell^n}$ we deduce that $a^{\ell^n} \in K^{\times \ell^{2n}}$. Proceeding inductively, we deduce in this way that $x \in K^{\times \ell^N}$. This shows that, indeed $D_w(N) = \mathcal{G}_K^a(N)$, as required. □

Proposition 8.2.2. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_1(n)))$. Let K be a field and assume that $X^{2\ell^N} - 1$ splits completely in K (we do not make any assumptions on* Char K*). Let $D \leq \mathcal{G}_K^a(n)$ be given. Then the following are equivalent:*

1. *There exists a valuation v of K such that $D \leq D_v(n)$ and $D/(D \cap I_v(n))$ is*

cyclic.

2. There exists a subgroup $D' \leq \mathcal{G}_K^a(N)$ such that D' is a C-group and $D'_n = D$.

Proof. First assume that D' exists as above. Then (1) follows from Theorem 7.0.11. Conversely, assume that there exists a valuation v of K such that $D \leq D_v(n)$ and $D/(D \cap I_v(n))$ is cyclic. Denote by $I = D \cap I_v(n)$ and choose $f \in D$ such that $\langle I, f\rangle = D$. Choose $f' \in D_v(N)$ a lifting of f via Lemma 8.2.1 and consider the pre-image $I' \leq I_v(N)$ of $I \leq I_v(n)$ under the surjective map $I_v(N) \to I_v(n)$. Then $I'_n = I$ and $f'_n = f$. Moreover, by Lemma 6.0.7, we see that $\langle I', f'\rangle$ is a C-group. Taking $D' = \langle I', f'\rangle$ we obtain (2). □

Proposition 8.2.3. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field and assume that $X^{2\ell^N} - 1$ splits completely in K (we do not make any assumptions on* Char K*). Assume that $\mathbf{I}^{\mathrm{C}}(\mathcal{G}_K^a(n)) \neq \mathcal{G}_K^a(n)$, consider $I' = \mathbf{I}^{\mathrm{C}}(\mathcal{G}_K^a(N))$ and denote by $I = I'_n$. Then I is valuative, $v := v_I \in \mathcal{V}_{K,n}$, $I = I_v(n)$ and $D_v(n) = \mathcal{G}_K^a(n)$.*

Proof. We know that I is valuative and, denoting $v = v_I$, $D_v(n) = \mathcal{G}_K^a(n)$ from Theorem 7.0.12. On the other hand, $D_v(N) = \mathcal{G}_K^a(N)$ by Lemma 8.2.1 and so we see that $I_v(N) \leq I'$ by Lemma 6.0.7; thus $I_v(n) \leq I \leq I_v(n)$ so that $I = I_v(n)$.

Let us show that $v \in \mathcal{W}_{K,n}$. Suppose that w is a refinement of v such that $D_v(n) = \mathcal{G}_K^a(n) = D_w(n)$. Then, as above, $I_w(N) \leq I'$ so that $I_w(n) \leq I_v(n) \leq I_w(n)$ and thus $I_w(n) = I_v(n)$. Moreover, $\mathcal{G}_{k(v)}^a(n) = \mathcal{G}_K^a(n)/I$ is non-cyclic since $\mathcal{G}_K^a(n)$ is not a C-group and $I \leq \mathbf{I}^{\mathrm{C}}(\mathcal{G}_K^a(n))$; thus we see that $v \in \mathcal{V}_{K,n}$. □

Theorem 8.2.4. *Let $n \in \mathbb{N}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field and assume that $X^{2\ell^N} - 1$ splits completely in K (we do not make any assumptions on* Char K*). Let $I \leq D \leq \mathcal{G}_K^a(n)$ be given. Then there exists a valuation $v \in \mathcal{V}_{K,n}$ such that $I = I_v(n)$ and $D = D_v(n)$ if and only if the following holds:*

1. *There exist $D' \leq \mathcal{G}_K^a(N)$ such that $(\mathbf{I}^{\mathrm{C}}(D'))_n = I$, $D'_n = D$.*

2. *$I \leq D \leq \mathcal{G}_K^a(n)$ are maximal with this property. Namely, if $D \leq E \leq \mathcal{G}_K^a(n)$ and $E' \leq \mathcal{G}_K^a(N)$ is given such that $E'_n = E$ and $I \leq (\mathbf{I}^{\mathrm{C}}(E'))_n$, then $D = E$ and $I = (\mathbf{I}^{\mathrm{C}}(E'))_n$.*

3. *$\mathbf{I}^{\mathrm{C}}(D) \neq D$ (i.e. D is not a C-group).*

Proof. Let $I \leq D$ be given which satisfy conditions (1)-(3) as above. Then I is valuative and $D \leq D_v(n)$, where $v = v_I$, by Theorem 7.0.12. Consider $I' = I_v(N) \leq D_v(N) = D'$. By Lemma 8.2.1, one has $I'_n = I_v(n)$ and $D'_n = D_v(n)$. Furthermore, by Lemma 6.0.7, $I' \leq \mathbf{I}^{\mathrm{C}}(D')$. Thus, $I \leq I_v(n) = I'_n \leq (\mathbf{I}^{\mathrm{C}}(D'))_n =: J$ and $D \leq D_v(n) = D'_n$. By assumption (2) on $I \leq D$ we deduce that $I = J$ and $D = D_v(n)$. Moreover, by Theorem 7.0.12, J is valuative and $D_v(n) \leq D_{v_J}(n)$. But $I_v(n) \leq J \leq I_{v_J}(n)$ implies that v is coarser than v_J so that $D_{v_J}(n) \leq D_v(n)$. Thus, $D_v(n) = D_{v_J}(n)$ and $I = I_v(n)$, as required.

Since $v = v_I$, we see immediately by the definition of v_I that Γ_v contains no non-trivial convex ℓ-divisible subgroups so that v satisfies assumption (1) of $\mathcal{W}_{K,n}$. Assume that w is a refinement of v (i.e. v is coarser than w) such that $D_v(n) =$

$D_w(n)$. Then $I_v(n) \leq I_w(n) \leq D_w(n) = D_v(n)$. But then:

$$I_v(n) \leq I_w(n) \leq (\mathbf{I}^{\mathrm{C}}(D_w(N)))_n \leq (D_w(N))_n = D_w(n) = D_v(n)$$

implies that $I_v(n) = I_w(n)$ by assumption (2) on $I \leq D$, thus $v \in \mathcal{W}_{K,n}$. Moreover, $\mathcal{G}^a_{k(v)}(n) = D_v(n)/I_v(n)$ is non-cyclic as $D_v(n)$ is not a C-group by assumption (3) (see Lemma 6.0.7), so we deduce that $v \in \mathcal{V}_{K,n}$.

Conversely assume that $v \in \mathcal{V}_{K,n}$ is given. By Lemma 6.0.7, we have $I_v(N) \leq \mathbf{I}^{\mathrm{C}}(D_v(N)) \leq D_v(N)$ and by Lemma 8.2.1 we obtain:

$$I_v(n) \leq (\mathbf{I}^{\mathrm{C}}(D_v(N)))_n \leq D_v(n).$$

Moreover, $I := (\mathbf{I}^{\mathrm{C}}(D_v(N)))_n$ is valuative and $D_v(n) \leq D_{v_I}(n)$ by Theorem 7.0.12. Since $I_v(n) \leq I$, v_I is a refinement of v we see that $D_{v_I}(n) \leq D_v(n) \leq D_{v_I}(n)$ and so $D_v(n) = D_{v_I}(n)$. Thus, $I_v(n) = I$ by condition (2) on $v \in \mathcal{V}_{K,n}$ from Definition 8.1.1.

Let us now show that $I := I_v(n) \leq D_v(n) =: D$ satisfy the condition (2) required by $\mathcal{D}_{K,n}$. Assume that $E' \leq \mathcal{G}^a_K(N)$ and $D \leq E := E'_n$ and $I \leq (\mathbf{I}^{\mathrm{C}}(E'))_n =: J$. By Theorem 7.0.12, J is valuative and $D \leq E \leq D_w(n)$ where $w = v_J$. But since $I \leq J \leq D_w(n)$, v is a coarsening of w and so, similarly to above, we deduce that $D = D_w(n)$. Now the condition (2) of $v \in \mathcal{V}_{K,n}$ of Definition 8.1.1 ensures that $I_v(n) = I_w(n) = I$, as required.

Lastly, we must show that D is not a C-group – i.e. condition (3) of the theorem. Assume for a contradiction that D is a C-group; equivalently, $\mathcal{G}^a_{k(v)}(n)$ is a C-group

by Lemma 6.0.8. However, $\mathcal{G}^a_{k(v)}(n)$ is non-cyclic and thus $\mathcal{G}^a_{k(v)}(1)$ is non-cyclic as well by Lemma 8.2.1. But $\mathcal{G}^a_{k(v)}(n)$ being a C-group implies that $\mathcal{G}^a_{k(v)}(1)$ is a C-group as well. Thus, applying Theorem 7.0.11 with $n = 1$, there exists a valuative subgroup $J \leq \mathcal{G}^a_{k(v)}(1)$ such that $\mathcal{G}^a_{k(v)}(1) = D_{w'}(1)$ where $w' = v_J$ and $D_{w'}(1)/I_{w'}(1)$ is cyclic. But by Lemma 8.2.1, $D_{w'}(n) = \mathcal{G}^a_{k(v)}(n)$ and $D_{w'}(n)/I_{w'}(n)$ is cyclic as well. Denote by $w = v \circ w'$ so that $I_v(n) \leq I_w(n) \leq D_w(n) = D_v(n)$, with $D_w(n)/I_w(n)$ cyclic. But this contradicts condition (2) of $v \in \mathcal{V}_{K,n}$ from Definition 8.1.1 as $D_v(n)/I_v(n) = \mathcal{G}^a_{k(v)}(n)$ is non-cyclic and thus $I_v(n) \neq I_w(n)$. □

Remark 8.2.5. Let $n \in \overline{\mathbb{N}}$ be given. Suppose that K is a field in which the polynomial $X^{2\ell^N} - 1$ splits completely for $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Then map $v \mapsto I_v(n) \leq D_v(n)$ defines a bijection $\mathcal{V}_{K,n} \to \mathcal{D}_{K,n}$.

Let $v \in \mathcal{V}_{K,n}$ be given. By Lemma 6.0.8, the bijection $\mathcal{V}_{K,n} \to \mathcal{D}_{K,n}$ restricts to a bijection $\mathcal{V}_{v,n} \to \mathcal{D}_{v,n}$. Furthermore, this restricted bijection is compatible with the bijection $\mathcal{V}_{k(v),n} \to \mathcal{D}_{k(v),n}$ via the canonical bijections $\mathcal{V}_{k(v),n} \to \mathcal{V}_{v,n}$ and $\mathcal{D}_{k(v),n} \to \mathcal{D}_{K,n}$.

We conclude this subsection by providing an alternative definition of $\mathcal{V}_{K,n}$, as promised in Remark 1.3.2 from the introduction. This will prove that $\mathcal{V}_{K,n}$ is independent of n whenever n is small enough relative to the number of roots of unity contained in K.

Lemma 8.2.6. *Let $n \in \overline{\mathbb{N}}$ be given and let K be a field in which $X^{2\ell^n} - 1$ splits completely. Then $\mathcal{V}_{K,n}$ is precisely the collection of valuations v of K such that:*

1. Γ_v *contains no non-trivial* ℓ*-divisible convex subgroups.*

2. $I_v(1) = \mathbf{I}^{\mathrm{C}}(D_v(1)) \neq D_v(1)$.

In particular, $\mathcal{V}_{K,n} = \mathcal{V}_{K,m}$ *for all* $m \leq n$.

Proof. The argument of this lemma is similar to that of Theorem 8.2.4. Denote by $\mathcal{V}$ the collection of valuations satisfying the two conditions (1),(2) of the lemma. First, let us show that $\mathcal{V} \subset \mathcal{V}_{K,n}$. Let $v \in \mathcal{V}$ be given; we need show the following conditions:

(a) Γ_v contains no non-trivial ℓ-divisible convex subgroups.

(b) If w is a refinement of v such that $D_w(n) = D_v(n)$ then $I_w(n) = I_v(n)$.

(c) $\mathcal{G}^a_{k(v)}(n)$ is non-cyclic.

Condition (1) for $v \in \mathcal{V}$ is precisely (a). First, as $\mathbf{I}^{\mathrm{C}}(D_v(1)) \neq D_v(1)$, we see that $\mathcal{G}^a_{k(v)}(n) = D_v(n)/I_v(n)$ is non-cyclic since $I_v(n) \leq \mathbf{I}^{\mathrm{C}}(D_v(n))$; thus we obtain (c). Suppose that w is a refinement of v such that $D_w(n) = D_v(n)$. Consider $I_v(1) \leq I_w(1) \leq D_w(1) \leq D_v(1)$. By Lemma 6.0.7, we see that:

$$\mathbf{I}^{\mathrm{C}}(D_v(1)) = I_v(1) \leq I_w(1) \leq \mathbf{I}^{\mathrm{C}}(D_v(1)) \leq D_w(1) = D_v(1).$$

Thus, $I_w(1) = I_v(1)$, and by Lemma 8.2.1, we see that $I_w(n) = I_v(n)$ as well.

Conversely we show that $\mathcal{V}_{K,n} \subset \mathcal{V}$; assume that $v \in \mathcal{V}_{K,n}$. Then condition (1) of $\mathcal{V}$ holds trivially. Let us show that $I_v(1) = \mathbf{I}^{\mathrm{C}}(D_v(1)) \neq D_v(1)$. Clearly, $I_v(1) \leq \mathbf{I}^{\mathrm{C}}(D_v(1))$ by Lemma 6.0.7. Denote by $I = \mathbf{I}^{\mathrm{C}}(D_v(1))$. Then by Theorem 7.0.12, I is

valuative and, denoting by $w = v_I$, one has $D_v(1) \leq D_w(1)$. Since w is a refinement of v we see that $D_w(1) = D_v(1)$ and thus $D_w(n) = D_v(n)$ by Lemma 8.2.1. By the definition of $\mathcal{V}_{K,n}$ we see that $I_w(n) = I_v(n)$ and thus $I \leq I_w(1) = I_v(1) \leq I$ so that $I = I_v(1)$. Also, $\mathcal{G}^a_{k(v)}(n)$ is non-cyclic and thus $\mathcal{G}^a_{K(v)}(1)$ is non-cyclic by Lemma 8.2.1 – in particular, $D_v(1)/I$ cannot be cyclic, as required. □

8.3 $n = 1$ or $n = \infty$

Throughout this subsection, n will denote either 1 or ∞. The key property to notice is that Λ_n is a domain and that $\mathbf{N}(n) = \mathbf{M}_r(n) = n$ (in fact, 1 and ∞ are the only fixed points of $\mathbf{N}$ and of $\mathbf{M}_r$). The proofs of the results below are virtually identical (and in fact much easier) to those in §8.2 using this observation. Indeed, the added assumption that $X^{2\ell^N} - 1$ splits in K was only used in the fact that $D_v(N) \to D_v(n)$ is surjective. In this case, $N = n$ so that this is trivially satisfied. We therefore omit the proofs in this subsection as they would be identical (and actually end up being much simpler) to the corresponding proof from section 8.2.

Proposition 8.3.1. *Let $n = 1$ or $n = \infty$ and let K be an arbitrary field. Let $D \leq \mathcal{G}^a_K(n)$ be given. Then the following are equivalent:*

1. *There exists a valuation v of K such that $D \leq D_v(n)$ and $D/(D \cap I_v(n))$ is cyclic.*

2. *D is a C-group.*

Proposition 8.3.2. *Let $n = 1$ or $n = \infty$ and let K be an arbitrary field. Assume that $\mathbf{I}^{\mathrm{C}}(\mathcal{G}_K^a(n)) \neq \mathcal{G}_K^a(n)$ and consider $I = \mathbf{I}^{\mathrm{C}}(\mathcal{G}_K^a(n))$. Then I is valuative, $v := v_I \in \mathcal{V}_{K,n}$, $I = I_v(n)$ and $D_v(n) = \mathcal{G}_K^a(n)$.*

Theorem 8.3.3. *Let $n = 1$ or $n = \infty$. Let K be an arbitrary field and let $I \leq D \leq \mathcal{G}_K^a(n)$ be given. Then there exists a valuation $v \in \mathcal{V}_{K,n}$ such that $I = I_v(n)$ and $D = D_v(n)$ if and only if the following holds:*

1. *$I = \mathbf{I}(D)$.*
2. *$I \leq D \leq \mathcal{G}_K^a(n)$ are maximal with this property. Namely, if $D \leq E \leq \mathcal{G}_K^a(n)$ and $I \leq \mathbf{I}^{\mathrm{C}}(E)$, then $D = E$ and $I = \mathbf{I}^{\mathrm{C}}(E)$.*
3. *$\mathbf{I}^{\mathrm{C}}(D) \neq D$ (i.e. D is not a C-group).*

Remark 8.3.4. Suppose that K is an arbitrary field and $n = 1$ or $n = \infty$. Then map $v \mapsto I_v(n) \leq D_v(n)$ defines a bijection $\mathcal{V}_{K,n} \to \mathcal{D}_{K,n}$.

Let $v \in \mathcal{V}_{K,n}$ be given. By Lemma 6.0.8, the bijection $\mathcal{V}_{K,n} \to \mathcal{D}_{K,n}$ restricts to a bijection $\mathcal{V}_{v,n} \to \mathcal{D}_{v,n}$. Furthermore, this restricted bijection is compatible with the bijection $\mathcal{V}_{k(v),n} \to \mathcal{D}_{k(v),n}$ via the canonical bijections $\mathcal{V}_{k(v),n} \to \mathcal{V}_{v,n}$ and $\mathcal{D}_{k(v),n} \to \mathcal{D}_{K,n}$.

Chapter 9

Restricting the Characteristic

In this chapter, we use C-pairs to specify which valuations have residue characteristic different from ℓ, in the situation where K has characteristic different from ℓ as well. In order to do this, we will need to force the C-pair property in a field extension of K which contains the ℓ^n-th roots of U_v^1. Later on, this condition will have a very natural Galois-theoretic interpretation which arises from decomposition theory.

Throughout this section we fix $n \in \overline{\mathbb{N}}$. Let $L|K$ be an extension of fields. We recall that the restriction map $\mathcal{G}_L^a(n) \to \mathcal{G}_K^a(n)$ is denoted by $f \mapsto f_K$. For a subgroup $H \leq K^\times$ we denote by $L_H := K(\sqrt[\ell^n]{H})$ (if $n = \infty$ we denote $K(\sqrt[\ell^\infty]{H}) := \bigcup_{m\in\mathbb{N}} K(\sqrt[\ell^m]{H})$); here, for $S \subset K$ and n finite, $K(\sqrt[\ell^n]{S})$ is a field obtained by adjoining *some* root of $X^{\ell^n} - s$ to K as $s \in S$ varies. For a subgroup $A \leq \mathcal{G}_K^a(n)$ we will also denote by $L_A := L_{A^\perp}$.

Lemma 9.0.5. *Let $n \in \overline{\mathbb{N}}$ be given. Let (K, v) be a valued field such that* $\operatorname{Char} K \neq \ell$. *Denote by $L := K(\sqrt[\ell^n]{U_v^1})$ and w a chosen prolongation of v to L. Let Δ be the convex subgroup of Γ_v generated by $v(\ell)$ (this is trivial unless* $\operatorname{Char} k(v) = \ell$). *Then $\Delta \leq \ell^n \cdot \Gamma_w$ (here we denote by $\ell^\infty \cdot \Gamma_v = \bigcap_{m \in \mathbb{N}} \ell^m \cdot \Gamma_v$).*

Proof. We can assume with no loss that $n \in \mathbb{N}$ as the $n = \infty$ case follows from this. If $\operatorname{Char} k(v) \neq \ell$ then $v(\ell) = 0$ and the lemma is trivial. So assume that $\operatorname{Char} k(v) = \ell$. Let $x \in K^\times$ be such that $0 < v(x) \leq v(\ell)$ and so $1 + x \in L^{\times \ell^n}$. Take $y \in L$ such that $1 + x = (1 + y)^{\ell^n}$. Note that $y \in \mathcal{O}_w$ and, since $1 + x = (1 + y)^{\ell^n} = 1 + y^{\ell^n} \mod \mathfrak{m}_w$, we deduce that $y \in \mathfrak{m}_w$. Expanding the equation $1 + x = (1 + y)^{\ell^n}$ we see that $x = \ell \cdot y \cdot \epsilon + y^{\ell^n}$ for some $\epsilon \in \mathcal{O}_w$. But $w(x) \leq w(\ell) < w(\ell \cdot y \cdot \epsilon)$ since $w(y) > 0$ and $w(\epsilon) \geq 0$; thus, $w(x) = w(y^{\ell^n})$ by the ultrametric inequality. □

Proposition 9.0.6. *Let $n \in \overline{\mathbb{N}}$ be given. Let K be a field such that* $\operatorname{Char} K \neq \ell$. *Suppose that $I \leq \mathcal{G}_K^a(n)$ and $D \leq \mathcal{G}_K^a(n)$ are given. Denote by $L := L_D$ and assume that there exists $I' \leq \mathcal{G}_L^a(n)$ such that I' is valuative (denote $w' = v_{I'}$ and $w = w'|_K$), $I'_K = I$ and $D \leq D_w(n)$. Then I is valuative, $D \leq D_{v_I}(n)$ and* $\operatorname{Char} k(v_I) \neq \ell$.

Proof. First, as I' is valuative and $I = I'_K$, we see that $I \leq I_w(n)$ and is indeed valuative. Moreover, as $D \leq D_w(n)$ and $v_I =: v$ is a coarsening of w, we see that $D \leq D_v(n)$ as well; indeed, recall that v is the coarsening of w which corresponds to the maximal convex subgroup of $w(I^\perp)$. On the other hand, since $D \leq D_w(n)$ we see that $\sqrt[\ell^n]{U_w^1} \subset L$.

Denote by Δ the convex subgroup of Γ_w generated by $w(\ell)$. If $n \in \mathbb{N}$, we

consider the canonical injective map induced by taking the dual of the surjective map $I' \twoheadrightarrow I$:

$$\Gamma_w/w(I^\perp) \hookrightarrow \Gamma_{w'}/w'((I')^\perp).$$

By Lemma 9.0.5, we deduce that $\Delta \leq w(I^\perp)$ since $\Delta \leq \ell^n \cdot \Gamma_{w'} \leq w'((I')^\perp)$. Therefore, Δ is contained in the kernel of the canonical projection $\Gamma_w \to \Gamma_v$. In particular, $v(\ell) = 0$ so that $\operatorname{Char} k(v) \neq \ell$.

On the other hand, if $n = \infty$, the $\mathbb{Z}_\ell$-dual of $I' \twoheadrightarrow I$ is the injective map:

$$\widehat{\Gamma}_w/\widehat{w}(I^\perp) \hookrightarrow \widehat{\Gamma}_{w'}/\widehat{w}'((I')^\perp).$$

Observe that the image of Δ lies in the kernel of this map. Thus, the image of Δ under the map $\Gamma_w \to \widehat{\Gamma}_w$ is contained in $\widehat{w}(I^\perp)$; therefore, we still see that Δ is contained in the kernel of $\Gamma_w \twoheadrightarrow \Gamma_v$ since the kernel of $\Gamma_w \to \widehat{\Gamma}_w$ is $\ell^\infty \cdot \Gamma_w \leq w(I_w(\infty)^\perp)$. □

We now prove three theorems which are analogous to the main results of Chapter 7. The main different is that here we show how to ensure that the valuations produced have residue characteristic different from ℓ provided the same is true for K. First is the analogue of Theorem 6.1.1:

Theorem 9.0.7. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(n)$. Let K be a field such that $\operatorname{Char} K \neq \ell$, let $f, g \in \mathcal{G}_K^a(n)$ be given and denote by $L := L_H$ where $H = \ker f \cap \ker g = \langle f, g \rangle^\perp$. Assume that there exist $f'', g'' \in \mathcal{G}_L^a(N)$ such that*

- *f'', g'' form a C-pair.*

- $(f''_n)_K = f$ *and* $(g''_n)_K = g$.

Then there exists a valuation v *of* K *such that*

- $f, g \in D_v(n)$
- $\langle f, g\rangle/(\langle f, g\rangle \cap I_v(n))$ *is cyclic (possibly trivial).*
- $\operatorname{Char} k(v) \neq \ell$.

Proof. Denote by $f' = f''_n$ and $g' = g''_n$. Then by Theorem 6.1.1, there exists a valuation w' of L such that $f', g' \in D_{w'}(n)$ and $\langle f', g'\rangle/(\langle f', g'\rangle \cap I_{w'}(n))$ is cyclic. Denote by $w = w'|_K$, $I = (\langle f', g'\rangle \cap I_{w'}(n))_K$ and $D = \langle f, g\rangle$, and observe that $D \leq D_w(n)$. Thus, the claim follows from Proposition 9.0.6. □

Next is the analogue of Theorem 7.0.11:

Theorem 9.0.8. *Let* $n \in \overline{\mathbb{N}}$ *be given and denote by* $N = \mathbf{N}(\mathbf{M}_1(n))$. *Let* K *be a field such that* $\operatorname{Char} K \neq \ell$. *Let* $D \leq \mathcal{G}^a_K(n)$ *be given and assume that there exists* $D'' \leq \mathcal{G}^a_{L_D}(N)$ *such that* D'' *is a C-group and that* $D = (D''_n)_K$. *Then there exists a valuative subgroup* $I \leq D$ *such that:*

- D/I *is cyclic.*
- $D \leq D_{v_I}(n)$.
- $\operatorname{Char} k(v_I) \neq \ell$.

Proof. Denote by $L := L_D$ and $D' = D''_n \leq \mathcal{G}^a_L(n)$. By Theorem 7.0.11, there exists a valuative subgroup $I' \leq D'$ such that $D' \leq D_{w'}(n)$ where $w' = v_{I'}$ is the valuation of L corresponding to I', and D'/I' is cyclic. Denote by $I = I'_K$, then D/I is cyclic as $D = D'_K$. Moreover, observe that $D \leq D_w(n)$ where $w = w'|_K$. By Proposition 9.0.6, I is valuative, $\operatorname{Char} k(v_I) \neq \ell$ and $D \leq D_{v_I}(n)$, as required. □

We finish the chapter with the analogue of Theorem 7.0.12:

Theorem 9.0.9. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field such that $\operatorname{Char} K \neq \ell$. Let $I \leq D \leq \mathcal{G}^a_K(n)$ be given and denote by $L := L_D$. Assume that there exists $I'' \leq D'' \leq \mathcal{G}^a_L(N)$ such that $I'' \leq \mathbf{I}^{\mathrm{C}}(D'')$, $(I''_n)_K = I$, $(D''_n)_K = D$, and that $D \neq \mathbf{I}^{\mathrm{C}}(D)$. Then I is valuative, $D \leq D_{v_I}(n)$ and $\operatorname{Char} k(v_I) \neq \ell$.*

Proof. The proof of this theorem is similar to the proof of Theorem 9.0.8 using Theorem 7.0.12 instead of Theorem 7.0.11 along with, again, Proposition 9.0.6. □

Remark 9.0.10. Using Theorem 9.0.7 resp. 9.0.8 resp. 9.0.9 instead of the analogous Theorem 6.1.1 resp. 7.0.11 resp. 7.0.12, one can prove results analogous to those in Chapter 8 while considering only valuations whose residue characteristic is different from ℓ. We will not state these results explicitly, as their Galois-theoretical analogues are already stated in Theorem 1.4.2 and/or 14.0.11.

Chapter 10

Milnor K-theory

As we move closer towards Galois theory, in this chapter we describe the connection of the C-pair property with Milnor K-theory. Later on, we will use our K-theoretic characterization of C-pairs, along with the Merkurjev-Suslin theorem and results involving free presentations of pro-ℓ Galois groups, to translate from the abstract situation of C-pairs to the Galois-theoretical setting of CL-pairs.

10.1 Definition and Properties

Let K be any field. The usual construction of the Milnor K-ring is as follows:

$$K_n^M(K) = \frac{(K^\times)^{\otimes n}}{\langle a_1 \otimes \cdots \otimes a_n \ : \ \exists\ 1 \leq i < j \leq n,\ a_i + a_j = 1 \rangle}.$$

The tensor product makes $K_*^M(K) := \bigoplus_n K_n^M(K)$ into a graded-commutative ring. We denote by $\{\bullet, \bullet\}$ the product $K_1^M(K) \times K_1^M(K) \to K_2^M(K)$. That is, we denote

by $\{x,y\} \in K_2^M(K)$ the product of $x, y \in K^\times = K_1^M(K)$. The following properties are well-known (see e.g. [GS06] Chapter 7):

1. $\{x,-1\} = \{x,x\}$.

2. $\{x,y\} = -\{y,x\}$.

We also consider certain canonical quotients of the Milnor K-theory ring. Let $T \leq K^\times$ be given. We define $K_*^M(K)/T$ as the quotient of $K_*^M(K)$ by the graded ideal generated by $T \leq K^\times = K_1^M(K)$ or explicitly as follows:

$$K_n^M(K)/T = \frac{(K^\times/T)^{\otimes n}}{\langle a_1 \cdot T \otimes \cdots \otimes a_n \cdot T \ : \ \exists\ 1 \leq i < j \leq n,\ 1 \in a_i \cdot T + a_j \cdot T \rangle}.$$

As before, the tensor product makes $K_*^M(K)/T = \bigoplus_n K_n^M(K)/T$ into a graded-commutative ring. We denote the product in this ring by $\{\bullet,\bullet\}_T$. Moreover, one has a surjective map of graded-commutative rings: $K_*^M(K) \twoheadrightarrow K_*^M(K)/T$. Since $\{x,-1\} = \{x,x\}$, we also see that $\{x,-1\}_T = \{x,x\}_T$. For more on the arithmetical properties of these canonical quotients of the Milnor K-ring, refer to Efrat [Efr06a], [Efr07] where they are systematically studied. Since the precise definition of $K_0^M(K)/T$ will not be needed in the sequel, we will leave this ambiguous. However, we will mention that the most natural choice is $K_0^M(K)/T = \Lambda_n$ provided that $K^{\times \ell^n} \leq T$.

Suppose that $T \leq K^\times$ and $-1 \in T$. Then the canonical surjective map $(K^\times/T) \otimes (K^\times/T) \twoheadrightarrow K_2^M(K)/T$ factors through

$$\wedge^2(K^\times/T) = \frac{(K^\times/T) \otimes (K^\times/T)}{\langle x \otimes x \ : \ x \in K^\times/T \rangle}.$$

Moreover, the kernel of the canonical surjective map $\wedge^2(K^\times/T) \to K_2^M(K)/T$ is generated by $z \wedge (1-z)$ for z varying over the elements of $K^\times \smallsetminus \{1\}$ (in fact, z varying over $K^\times \smallsetminus T$ suffices as well).

Suppose that $n \in \mathbb{N}$ and $\pm K^{\times \ell^n} \leq T \leq K^\times$ is given such that $K^\times/T$ has rank 2. Say e.g. that $K^\times/T$ is generated by the two elements x, y:

$$K^\times/T = x^{\mathbb{Z}/\ell^{n-a}} \times y^{\mathbb{Z}/\ell^{n-b}} \cong \mathbb{Z}/\ell^{n-a} \times \mathbb{Z}/\ell^{n-b}.$$

Then $\wedge^2(K^\times/T) \cong \mathbb{Z}/\ell^{n-a} \wedge \mathbb{Z}/\ell^{n-b}$ is generated by $x \wedge y$ and has order $\ell^{n-\max(a,b)}$. In particular, we see that $K_2^M(K)/T = \langle \{x,y\}_T \rangle$ is cyclic of order ℓ^{n-c} where $c \geq \max(a,b)$, since $K_2^M(K)/T$ is a quotient of $\wedge^2(K^\times/T)$. This observation will become extremely important in our K-theoretic characterization of C-pairs.

10.2 K-Theoretic Characterization of C-pairs

We now prove our K-theoretic characterization of C-pairs. Given a pair of elements $f, g \in \mathcal{G}_K^a(n)$, we consider $T = \ker(f) \cap \ker(g)$ and observe that $(f,g) : K^\times/T \to \Lambda_n^2$ is injective. In particular, if n is finite then so is $K^\times/T$. Without changing $\langle f, g \rangle$, and thus without changing T, we can assume without loss of generality that f, g are quasi-independent – thus $\langle f, g \rangle = \langle f \rangle \oplus \langle g \rangle$. Furthermore, if the order of f is ℓ^{n-a} and the order of g is ℓ^{n-b}, then (f,g) has image $(\ell^a\mathbb{Z}/\ell^n\mathbb{Z}) \oplus (\ell^b\mathbb{Z}/\ell^n\mathbb{Z})$; thus (f,g) induces an isomorphism $K^\times/T \to (\ell^a\mathbb{Z}/\ell^n\mathbb{Z}) \oplus (\ell^b\mathbb{Z}/\ell^n\mathbb{Z})$. Therefore $K^\times/T$ is generated by two elements x, y which can be chosen so that furthermore

$(f,g)(x) = (\ell^a, 0)$ and $(f,g)(y) = (0, \ell^b)$. This will be the starting point for the argument of our K-theoretic characterization of C-pairs.

Proposition 10.2.1 (K-theoretic characterization of C-pairs)**.** *Let $n \in \mathbb{N}$ be given. Let $f, g \in \mathcal{G}_K^a(n)$ be given quasi-independent elements of order ℓ^{n-a} resp. ℓ^{n-b}; in particular,*

$$\langle f, g \rangle = \langle f \rangle \oplus \langle g \rangle \cong (\mathbb{Z}/\ell^{n-a}) \cdot f \oplus (\mathbb{Z}/\ell^{n-b}) \cdot g.$$

Denote by $T = \ker f \cap \ker g$ and say that $K_2^M(K)/T$ has order ℓ^{n-c}. Then f, g form a C-pair if and only if $c \leq a + b$.

On the other hand, let $f, g \in \mathcal{G}_K^a(\infty)$ be given. Then f, g form a C-pair if and only if f_n, g_n form a C-pair for all $n \in \mathbb{N}$.

Proof. If $f, g \in \mathcal{G}_K^a(\infty)$, the fact that f, g form a C-pair if and only if f_n, g_n form a C-pair for all $n \in \mathbb{N}$ follows immediately from the definition. Let us therefore show the first statement concerning $n \in \mathbb{N}$, and note that a similar K-theoretic criterion for $n = \infty$ is given in Remark 10.2.3.

Let $n \in \mathbb{N}$ be given and let f, g be quasi-independent elements of $\mathcal{G}_K^a(n)$ as in the statement of the proposition. Thus, $K^\times/T$ has quasi-independent generators which are dual to f, g which we denote by x, y:

$$K^\times/T = x^{\mathbb{Z}/\ell^{n-a}} \times y^{\mathbb{Z}/\ell^{n-b}}.$$

Denote by $\Psi = (f, g)$ then $\Psi(x) = (\ell^a, 0)$ and $\Psi(y) = (0, \ell^b)$. Say that $z = x^h y^i \mod T$ and $(1 - z) = x^j y^k \mod T$ where $h, i, j, k \in \mathbb{Z}/\ell^n$; equivalently, one has

$\Psi(z) = (\ell^a h, \ell^b i)$ and $\Psi(1-z) = (\ell^a j, \ell^b k)$. Since $\{z, 1-z\} = 0$ we deduce that $(hk - ij) \cdot \{x, y\}_T = 0$ and thus $(hk - ij) = 0 \mod \ell^{n-c}$. Assume that $c \leq a + b$; thus we see that $\ell^{a+b} \cdot (hk - ij) = 0 \mod \ell^n$ and so $f(z)g(1-z) = f(1-z)g(z)$. As z was arbitrary, we see that f, g form a C-pair.

Conversely, assume that f, g are a C-pair and assume with no loss that $a \geq b$. Let $z \in K^\times$ be given and say $\Psi(z) = (\ell^a h, \ell^b i)$, $\Psi(1-z) = (\ell^a j, \ell^b k)$ as above with $h, i, j, k \in \mathbb{Z}/\ell^n$. Since f, g are a C-pair, we see that $\ell^{a+b} \cdot (hk - ij) = 0$. On the other hand, $K_2^M(K)/T = \wedge^2(K^\times/T)/\langle z' \wedge (1-z') \ : \ z' \neq 0, 1\rangle$. Recall that $\wedge^2(K^\times/T)$ is generated by $x \wedge y$ and has order ℓ^{n-a}. For z as above, one has $z \wedge (1-z) = (hk - ij) \cdot (x \wedge y)$ so that $\wedge^2(K^\times/T)/\langle z \wedge (1-z)\rangle \cong \mathbb{Z}/\ell^{n-c}$ for some $c \leq a + b$. Varying over all z', we see that $K_2^M(K)/T \cong \mathbb{Z}/\ell^{n-c}$ where $c \leq a + b$, as required. □

Remark 10.2.2. Proposition 10.2.1 provides a K-theoretic characterization of C-pairs in terms of $T = \langle f, g\rangle^\perp$. Since A is a C-group if and only if any pair $f, g \in A$ form a C-pair, this thereby provides a K-theoretic characterization of C-groups. In this remark, we prove an alternative characterization of C-groups A in the case where $n = 1$ which resembles the usual conditions related to rigidity – this K-theoretic condition and its relationship with rigid elements has been extensively studied and developed by Efrat [Efr07], [Efr06a], [Efr06b] in the case where $n = 1$. The case where $n = \infty$ is also treated in detail by the author in [Top12].

Let $A \leq \mathcal{G}_K^a(n)$ be given and denote by $T = A^\perp$. Proposition 10.2.1 gives

a precise recipe to decide whether or not A is a C-group using the structure of $K_*^M(K)/T$. Indeed, we immediately see that the following conditions are equivalent:

1. A is a C-group.

2. For all subgroups $A_0 \leq A$ of rank 2, A_0 is a C-group.

3. For all subgroups $T_0 \leq K^\times$ such that $T \leq T_0 \leq K^\times$ and $K^\times/T_0$ has rank 2, $K_*^M(K)/T_0$ satisfies the equivalent conditions of Proposition 10.2.1.

On the other hand, in the case where $n = 1$, we can provide a direct characterization of C-groups $A \leq \mathcal{G}_K^a(1)$, without the need for an auxiliary T_0, as follows; see also [Top12] Lemma 2.12. Let $A \leq \mathcal{G}_K^a(1)$ be given and denote by $T = A^\perp$. Then the following are equivalent:

1. A is a C-group.

2. For all subgroups $T \leq T_0 \leq K^\times$ such that $K^\times/T_0 = \langle x \mod T_0, y \mod T_0 \rangle$ has rank 2, one has $\{x, y\}_{T_0} \neq 0$ as an element of $K_2^M(K)/T_0$.

3. For all $x, y \in K^\times$ such that $(x \mod T), (y \mod T)$ are $\mathbb{Z}/\ell$ independent in $K^\times/T$ one has $\{x, y\}_T \neq 0$ as an element of $K_2^M(K)/T$.

4. For all $x \in K^\times \smallsetminus T$ one has $\langle 1 - x, x \rangle \mod T$ is cyclic.

5. For all $T \leq H \leq K^\times$ and $x \in K^\times \smallsetminus H$ one has $\langle 1 - x, x \rangle \mod H$ is cyclic.

6. The canonical map $\wedge^2(K^\times/T) \to K_2^M(K)/T$ is an isomorphism.

7. For all $T \leq H \leq K^\times$, the canonical map $\wedge^2(K^\times/H) \to K_2^M(K)/H$ is an isomorphism.

Indeed, (1) $\Leftrightarrow$ (2) is Proposition 10.2.1, while (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (6) $\Rightarrow$ (3) and (5) $\Rightarrow$ (7) $\Rightarrow$ (2) follow immediately from the definitions. In particular, the equivalence of conditions (1) and (6) above give a direct characterization of C-groups $A \leq \mathcal{G}_K^a(1)$ based on the structure of $K_*^M(K)/T$ where $T = A^\perp$.

Remark 10.2.3. Passing to the limit over $n \in \mathbb{N}$ and using Proposition 10.2.1, we can obtain a similar K-theoretic method to detect C-pairs in $\mathcal{G}_K^a(\infty)$. Denote by $\widehat{K}_i^M(K)$ the ℓ-adic completion of $K_i^M(K)$ and denote by $\widehat{K} = \widehat{K}_1^M(K)$ the ℓ-adic completion of $K^\times$. By the universal property of completions one has:

$$\mathcal{G}_K^a(\infty) = \mathrm{Hom}^{\mathrm{cont}}(\widehat{K}/\pm 1, \mathbb{Z}_\ell).$$

Moreover, $\widehat{K}$/torsion is in perfect $\mathbb{Z}_\ell$-duality with $\mathcal{G}_K^a(\infty)$. Let $f, g \in \mathcal{G}_K^a(\infty)$ be given and consider f, g as homomorphisms $\widehat{K} \to \mathbb{Z}_\ell$; assume that $\langle f, g\rangle$ is non-cyclic. If $f = \ell^a \cdot f'$ and $g = \ell^b \cdot g'$ then f, g form a C-pair if and only if f', g' form a C-pair. Therefore, we can assume without loss that, first, $\mathcal{G}_K^a(\infty)/\langle f, g\rangle$ is torsion-free and, second, that f, g are $\mathbb{Z}_\ell$-independent. In particular $\langle f \mod \ell, g \mod \ell\rangle$ is non-cyclic and f_n, g_n are quasi-independent elements of $\mathcal{G}_K^a(n)$ both of order $\mathbb{Z}/\ell^n$. We denote by $T = \ker f \cap \ker g$ considered as a closed $\mathbb{Z}_\ell$-submodule of $\widehat{K}$; i.e. here we consider f, g as continuous homomorphism $\widehat{K} \to \mathbb{Z}_\ell$. Thus we can find generators x, y for $\widehat{K}/T$ such that $\widehat{K}/T = x^{\mathbb{Z}_\ell} \times y^{\mathbb{Z}_\ell}$ with $(f, g)(x) = (1, 0)$ and $(f, g)(y) = (0, 1)$.

Moreover, denote by $T_n = \ker f_n \cap \ker g_n$, and observe that $\widehat{K}/T = \lim_n K^\times/T_n$. From this we see that $\widehat{K}_2^M(K)/T = \lim_n K_2^M(K)/T_n$ is a cyclic $\mathbb{Z}_\ell$-module generated by $\{x, y\}_T$. Recall that f, g form a C-pair if and only if f_n, g_n form a C-pair for all $n \in \mathbb{N}$. We thus deduce from Proposition 10.2.1 that f, g form a C-pair if and only if $\{x, y\}_T$ has infinite order – i.e. $\widehat{K}_2^M(K)/T = \mathbb{Z}_\ell \cdot \{x, y\}_T \cong \mathbb{Z}_\ell$. Thus, we see that f, g form a C-pair if and only if the canonical map $\widehat{\wedge}^2(\widehat{K}/T) \to \widehat{K}_2^M(K)/T$ is an isomorphism.

Furthermore, one should remark that Proposition 10.2.1 allows us to detect valuations using the Milnor K-theory of the field. Indeed, using the results of Chapter 8, we need to construct $\mathcal{G}_K^a(n)$ along with the C-pairs from Milnor K-theory. First, assume that ℓ is odd and n is finite. Then $\mathcal{G}_K^a(n) = \mathrm{Hom}(K^\times/\ell^n, \mathbb{Z}/\ell^n) = \mathrm{Hom}(K_1^M(K)/\ell^n, \mathbb{Z}/\ell^n)$, and Proposition 10.2.1 shows how to detect precisely the C-pairs in $\mathcal{G}_K^a(n)$ using $K_*^M(K)/\ell^n$. Thus, one can detect valuations of K using $K_*^M(K)/\ell^N$ when N is sufficiently large with respect to n.

On the other hand, if $\ell = 2$, consider the kernel H of the map:

$$K^\times/2^{n+1} \xrightarrow{x \mapsto x^2} K^\times/2^{n+1}.$$

Then $K^\times/\langle K^{\times 2^n}, -1\rangle = (K^\times/2^{n+1})/H$. Thus, we can reconstruct $\mathcal{G}_K^a(n)$ from $K^\times/2^{n+1} = K_1^M(K)/2^{n+1}$ and furthermore detect C-pairs using Proposition 10.2.1 from $K_*^M(K)/2^{n+1}$ and/or $K_*^M(K)/2^n$. Again, one can therefore detect valuations of K using $K_*^M(K)/2^N$ when N is sufficiently large with respect to n.

Lastly, if $n = \infty$ and ℓ is arbitrary, we consider $\widehat{K} = \widehat{K}_1^M(K)$ and observe that

the image of -1 in $\widehat{K}$ is either trivial or is the unique element in $\widehat{K}$ whose square is trivial. Thus, we obtain $\mathcal{G}_K^a(\infty) = \mathrm{Hom}(\widehat{K}/\pm 1, \mathbb{Z}_\ell)$ from $\widehat{K}_1^M(K)$. Also, by the discussion above, we obtain the C-pairs in $\mathcal{G}_K^a(\infty)$ from $\widehat{K}_*^M(K)$. Thus, one can detect valuations of K using $\widehat{K}_*^M(K)$.

In particular, if K is a field of characteristic different from ℓ, we obtain a recipe to detect valuations $v \in \mathcal{V}_{K,n}$ using the cup-product structure of the cohomology ring $H^*(K, \Lambda_N(*))$ where $N \geq n$ is sufficiently large (as above). In the presence of sufficiently many roots of unity (or if $n = 1, \infty$), this provides a recipe to recover the corresponding maps $H^1(K, \Lambda_n(1)) = K^\times/\ell^n \xrightarrow{v} \Gamma_v/\ell^n$ for $v \in \mathcal{V}_{K,n}$ as dual to the inclusion $I_v(n) \hookrightarrow \mathcal{G}_K^a(n)$, resp. $H^1(K, \mathbb{Z}_\ell(1)) = \widehat{K} \xrightarrow{\widehat{v}} \widehat{\Gamma}_v$ as dual to the inclusion $I_v(\infty) \hookrightarrow \mathcal{G}_K(\infty)$.

Part III

Detecting Valuations: the Galois Theoretical Setting

Chapter 11

Galois Cohomology

Let K be a field of characteristic different from ℓ such that $\mu_\ell \subset K$. Recall that $K(\ell)$ denotes the maximal pro-ℓ Galois extension of K (inside some chosen algebraic closure) and that $\mathcal{G}_K = \mathrm{Gal}(K(\ell)|K)$ denotes the maximal pro-ℓ Galois group of K. Also recall that $\mathcal{G}_K^{a,n}$ denotes the maximal Λ_n-elementary abelian quotient of $\mathcal{G}_K$ (we reintroduce this notation below). In this chapter we will build up the required cohomological machinery which will be required for Chapter 12. In the following chapter, we give a Galois-theoretic characterization of the C-pair property of elements $f, g \in \mathcal{G}_K^a(n)$ under an identification $\mathcal{G}_K^{a,n} \cong \mathcal{G}_K^a(n)$, for fields K such that $\mathrm{Char}\, K \neq \ell$ and $\mu_{2\ell^n} \subset K$, via Kummer theory. Throughout Chapters 11, 12 and 13 we will work with a fixed $n \in \overline{\mathbb{N}}$.

11.1 Central Descending Series

Let $\mathcal{G}$ be an arbitrary pro-ℓ group. We recall the Λ_n-central descending series of $\mathcal{G}$:

$$\mathcal{G}^{(1,n)} = \mathcal{G}, \quad \mathcal{G}^{(m+1,n)} = [\mathcal{G}, \mathcal{G}^{(m,n)}] \cdot (\mathcal{G}^{(m,n)})^{\ell^n}.$$

For simplicity we denote by $\mathcal{G}^{a,n} = \mathcal{G}/\mathcal{G}^{(2,n)}$ and $\mathcal{G}^{c,n} = \mathcal{G}/\mathcal{G}^{(3,n)}$.

We will denote by $H^*(\mathcal{G}) := H^*_{\text{cont}}(\mathcal{G}, \Lambda_n)$ throughout this section. Recall, if n is finite, that the short exact sequence:

$$1 \to \mathbb{Z}/\ell^n \xrightarrow{\ell^n} \mathbb{Z}/\ell^{2n} \to \mathbb{Z}/\ell^n \to 1$$

produces the Bockstein homomorphism:

$$\beta : H^1(\mathcal{G}) \to H^2(\mathcal{G})$$

which is the connecting homomorphism in the associated long exact sequence in cohomology. Note that the Bockstein map β is taken to be the trivial homomorphism if $n = \infty$.

One has a well-defined Λ_n-bilinear map:

$$[\bullet, \bullet] : \mathcal{G}^{a,n} \times \mathcal{G}^{a,n} \to \mathcal{G}^{(2,n)}/\mathcal{G}^{(3,n)}$$

defined by $[\sigma, \tau] = \tilde{\sigma}^{-1}\tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}$ where $\tilde{\sigma} \in \mathcal{G}^{c,n}$ resp. $\tilde{\tau} \in \mathcal{G}^{c,n}$ denotes a lift of $\sigma \in \mathcal{G}^{a,n}$ resp. $\tau \in \mathcal{G}^{a,n}$ to $\mathcal{G}^{c,n}$. Similarly, one has a map:

$$(\bullet)^\pi : \mathcal{G}^{a,n} \to \mathcal{G}^{(2,n)}/\mathcal{G}^{(3,n)}$$

defined by $\sigma^\pi = \tilde{\sigma}^{\ell^n}$ (here we define $\sigma^\pi = 0$ if $n = \infty$) where again $\tilde{\sigma} \in \mathcal{G}^{c,n}$ denotes some lift of $\sigma \in \mathcal{G}^{a,n}$ to $\mathcal{G}^{c,n}$. The map $\sigma \mapsto \sigma^\pi$ is Λ_n-linear if $\ell \neq 2$. We will denote $\sigma^\beta = 2 \cdot \sigma^\pi$; thus the map $(\bullet)^\beta : \mathcal{G}^{a,n} \to \mathcal{G}^{(2,n)}/\mathcal{G}^{(3,n)}$ is Λ_n-linear regardless of ℓ (see [NSW08] Proposition 3.8.3).

Lemma 11.1.1. *Let $\mathcal{G}$ be a pro-ℓ group. Then*

$$\ker(H^2(\mathcal{G}^{a,n}) \to H^2(\mathcal{G})) = \ker(H^2(\mathcal{G}^{a,n}) \to H^2(\mathcal{G}^{c,n})).$$

In particular, let $f, g \in Hom(\mathcal{G}, \Lambda_n) = H^1(\mathcal{G}^{a,n}) = H^1(\mathcal{G}^{c,n}) = H^1(\mathcal{G})$ be given. The following are equivalent:

1. *$f \cup g = 0 \in H^2(\mathcal{G})$.*
2. *$f \cup g = 0 \in H^2(\mathcal{G}^{c,n})$.*

Proof. The fact that

$$\ker(H^2(\mathcal{G}^{a,n}) \to H^2(\mathcal{G})) \supset \ker(H^2(\mathcal{G}^{a,n}) \to H^2(\mathcal{G}^{c,n}))$$

is trivial. Assume that $x \in \ker(H^2(\mathcal{G}^{a,n}) \to H^2(\mathcal{G}))$ and consider the spectral sequence in cohomology associated to the group extension $\mathcal{G} \twoheadrightarrow \mathcal{G}^{a,n}$. Then $x = d_2(\xi)$ for some $\xi \in H^1(\mathcal{G}^{(2,n)})^{\mathcal{G}}$. Observe that the inflation map $H^1(\mathcal{G}^{(2,n)}/\mathcal{G}^{(3,n)})^{\mathcal{G}^{c,n}} \to H^1(\mathcal{G}^{(2,n)})^{\mathcal{G}}$ is an isomorphism. By the functoriality of the spectral sequence associated to a group extension above versus the group extension $\mathcal{G}^{c,n} \twoheadrightarrow \mathcal{G}^{a,n}$, we deduce that $x \in \ker(H^2(\mathcal{G}^{a,n}) \to H^2(\mathcal{G}^{c,n}))$ as required. □

Definition 11.1.2. Let $\mathcal{G}$ be a pro-ℓ group and let $\sigma, \tau \in \mathcal{G}^{a,n}$ be given. We say that σ, τ form a CL-pair provided that:

$$[\sigma, \tau] \in \langle \sigma^{\beta}, \tau^{\beta} \rangle.$$

If $\ell \neq 2$ we note that this condition is equivalent to $[\sigma, \tau] \in \langle \sigma^{\pi}, \tau^{\pi} \rangle$ as 2 is invertible in Λ_n. Furthermore, as $(\bullet)^{\beta}$ is linear and $[\bullet, \bullet]$ is bilinear, if $\langle \sigma', \tau' \rangle = \langle \sigma, \tau \rangle$ and σ, τ form a CL-pair, then σ', τ' form a CL-pair as well. A subgroup $A \leq \mathcal{G}^{a,n}$ will be called a CL-group provided that any pair of elements $\sigma, \tau \in A$ form a CL-pair.

For a subgroup $A \leq \mathcal{G}^{a,n}$, we denote by $\mathbf{I}^{\mathrm{CL}}(A)$ the subset:

$$\mathbf{I}^{\mathrm{CL}}(A) = \{\sigma \in A \ : \ \forall \tau \in A, \ \sigma, \tau \ \text{ form a CL-pair.}\}$$

and call $\mathbf{I}^{\mathrm{CL}}(A)$ the CL-center of A. In particular, A is a CL-group if and only if $A = \mathbf{I}^{\mathrm{CL}}(A)$.

Remark 11.1.3. Let $\mathcal{G}$ be a pro-ℓ group and let $A \leq \mathcal{G}^{a,n}$ be given. Suppose $A = \langle \sigma_i \rangle_i$ is generated by $(\sigma_i)_i$. Note, the fact that $(\sigma_i)_i$ are pairwise CL does not imply that A is CL for a general pro-ℓ group $\mathcal{G}$. This fact will be a consequence of Theorem 12.0.2 in the case where $\mathcal{G} = \mathcal{G}_K$ for a field K of characteristic different from ℓ which contains $\mu_{2\ell^n}$.

Furthermore, suppose A is an arbitrary subgroup of $\mathcal{G}^{a,n}$. We note that $\mathbf{I}^{\mathrm{CL}}(A)$ is not a subgroup of A but merely a subset. It will be a consequence of Theorem 12.0.2, in the case where $\mathcal{G} = \mathcal{G}_K$ for a field K as above, that $\mathbf{I}^{\mathrm{CL}}(A) \leq A$ is indeed a subgroup which agrees with $\mathbf{I}^{\mathrm{C}}(A)$ of Part II under the Kummer identification

$\mathcal{G}_K^{a,n} = \mathrm{Hom}(K^\times, \Lambda_n(1)) \cong \mathcal{G}_K^a(n)$.

11.2 Free Presentations

We now recall some basic facts about free presentations of pro-ℓ groups. For a reference, see e.g. [NSW08] Chapter 3.9. Let $\mathcal{G}$ be a pro-ℓ group and $S \to \mathcal{G}$ a free presentation such that the induced map $S^{a,n} \to \mathcal{G}^{a,n}$ is an isomorphism, and denote by T the kernel of $S \to \mathcal{G}$. Say that $(\tilde{\gamma}_i)_{i\in\Lambda}$ is a free generating set of S and denote the image of $\tilde{\gamma}_i$ in $S^{a,n}$ by γ_i; we consider γ_i also as an element of $\mathcal{G}^{a,n}$ via the isomorphism above. We furthermore denote by $(x_i)_{i\in\Lambda}$ the Λ_n-basis for $H^1(S)$ which is dual to $(\gamma_i)_i$ and choose a total ordering for the index set Λ; by abuse of notation, we will also denote by $(x_i)_{i\in\Lambda}$ the corresponding Λ_n-basis for $H^1(\mathcal{G})$ given by the canonical isomorphism $H^1(\mathcal{G}) \xrightarrow{\cong} H^1(S)$. Every element of $S^{(2,n)}/S^{(3,n)}$ has a unique representation as:

$$\rho = \prod_{i<j} [\gamma_i, \gamma_j]^{a_{ij}(\rho)} \cdot \prod_r (\gamma_r^\pi)^{b_r(\rho)}.$$

As $T \leq S^{(2,n)}$, we can restrict a_{ij} and b_r to homomorphisms $T \to \Lambda_n$. Moreover, the spectral sequence associated to the extension:

$$1 \to T \to S \to \mathcal{G} \to 1$$

induces an isomorphism $d_2 : H^1(T)^{\mathcal{G}} \to H^2(\mathcal{G})$. This is because both S and T have ℓ-cohomological dimension ≤ 1 and the inflation $H^1(\mathcal{G}) \to H^1(S)$ is an isomorphism.

Thus, we obtain a canonical perfect pairing:

$$(\bullet, \bullet) : H^2(\mathcal{G}) \times \left(\frac{T}{[S,T] \cdot T^{\ell^n}} \right) \to \Lambda_n$$

defined by $(\xi, \rho) = (d_2^{-1}\xi)(\rho)$. We can describe this pairing explicitly using the cup product and Bockstein (see [NSW08] Propositions 3.9.13 and 3.9.14) as follows:

- $(x_i \cup x_j, \bullet) = -a_{ij}(\bullet)$, $i < j$.
- $(\beta x_r, \bullet) = -b_r(\bullet)$.

Suppose that K is a field with $\operatorname{Char} K \neq \ell$ and $\mu_{2\ell^n} \subset K$, as above. In this context, we will fix, once and for all, an isomorphism of G_K-modules $\Lambda_n(1) \cong \Lambda_n$ and use it tacitly throughout. Recall the canonical perfect pairing arising from Kummer theory:

$$\mathcal{G}_K^{a,n} \times K^\times/\ell^n \to \mathbb{Z}/\ell^n(1) \text{ if } n \neq \infty, \quad \mathcal{G}_K^{a,n} \times \widehat{K} \to \mathbb{Z}_\ell(1) \text{ if } n = \infty.$$

Using our fixed isomorphism $\Lambda_n \cong \Lambda_n(1)$, we thus obtain an identification of $\mathcal{G}_K^{a,n}$ with $\mathcal{G}_K^a(n)$ using the pairing above. On the other hand, the Merkurjev-Suslin theorem states that $K_2^M(K)/\ell^n \cong H^2(K, \mathbb{Z}/\ell^n(2))$ if $n \neq \infty$ resp. $\widehat{K}_2^M(K) \cong H^2(K, \mathbb{Z}_\ell(2))$ if $n = \infty$. Thus, the cup product $H^1(K, \Lambda_n(1)) \otimes H^1(K, \Lambda_n(1)) \xrightarrow{\cup} H^2(K, \Lambda_n(2))$ is surjective. In particular, the inflation map $H^2(\mathcal{G}_K^{a,n}) \to H^2(\mathcal{G}_K)$ is surjective as well. This observation will allow us to describe $K_2^M(K)/\ell^n$ resp. $\widehat{K}_2^M(K)$ via the pairings described above.

Proposition 11.2.1. *Let K be a field such that* $\mathrm{Char}\, K \neq \ell$ *and $\mu_{\ell^n} \subset K$. Choose a free presentation $S \to \mathcal{G}_K$ where S is a free pro-ℓ group such that $S^{a,n} \to \mathcal{G}_K^{a,n}$ is an isomorphism, and denote by R the kernel of the canonical surjective map $S^{c,n} \to \mathcal{G}_K^{c,n}$. Then one has a canonical perfect pairing:*

$$H^2(\mathcal{G}_K) \times R \to \Lambda_n$$

induced by the free presentation. This pairing is compatible with the canonical perfect pairing:

$$H^2(S^{a,n}) \times S^{(2,n)}/S^{(3,n)} \to \Lambda_n$$

via the inflation map $H^2(S^{(a,n)}) = H^2(\mathcal{G}_K^{a,n}) \to H^2(\mathcal{G}_K)$ resp. the inclusion $R \hookrightarrow S^{(2,n)}/S^{(3,n)}$.

Proof. Take a minimal free presentation $S \to \mathcal{G}_K$ as in the proposition and denote by T the kernel of this map. The spectral sequence associated to this extension induces an isomorphism:

$$d_2 : H^1(T)^S \to H^2(\mathcal{G}_K)$$

so it suffices to show that the canonical map:

$$T/[S,T]T^{\ell^n} \to T \cdot S^{(3,n)}/S^{(3,n)} = R$$

is an isomorphism; clearly this is a surjective map. Taking Λ_n-duals of the composition

$$T/[S,T]T^{\ell^n} \to T \cdot S^{(3,n)}/S^{(3,n)} \hookrightarrow S^{(2,n)}/S^{(3,n)},$$

we obtain the inflation map $H^2(\mathcal{G}_K^{a,n}) \to H^2(\mathcal{G}_K)$. This map is surjective by the Merkurjev-Suslin theorem (see the discussion preceding this proposition). Thus $T/[S,T]T^{\ell^n} \to S^{(2,n)}/S^{(3,n)}$ is injective by Pontryagin duality so that $T/[S,T]T^{\ell^n} \to T \cdot S^{(3,n)}/S^{(3,n)} = R$ is injective as well.

The compatibility with the canonical pairing

$$H^2(S^{a,n}) \times S^{(2,n)}/S^{(3,n)} \to \Lambda_n$$

is immediate by the functoriality of the situation, along with our requirement that $S^{a,n} \to \mathcal{G}_K^{a,n}$ is an isomorphism. □

Chapter 12

CL-pairs versus C-pairs

Having developed our general theory using C-pairs in Part II which allows us to detect valuations using the abstract notion of C-pairs, in this chapter we will apply our results to Galois theory. Namely, we will show the equivalence of our two notions – that of C-pairs (a purely abstract notion in $\mathcal{G}_K^a(n)$) and that of CL-pairs (a purely group-theoretical notion in $\mathcal{G}_K^{a,n}$ and $\mathcal{G}_K^{c,n}$).

Let K be a field whose characteristic is different from ℓ, $n \in \overline{\mathbb{N}}$ and $\mu_{\ell^n} \subset K$, as above. Our fixed isomorphism $\Lambda_n(1) \cong \Lambda_n$ allows us to explicitly express the Bockstein morphism $\beta : H^1(\mathcal{G}_K, \Lambda_n) \to H^2(\mathcal{G}_K, \Lambda_n)$ using Milnor K-theory as follows. First, if $n = \infty$ this map is trivial, so there is nothing to say. Let us assume that $n \in \mathbb{N}$. It seems to be well known that the cup product $\mathbf{1} \cup \delta : H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) \otimes \mu_{\ell^n} \to H^2(\mathcal{G}_K, \mu_{\ell^n})$ is precisely the map $\beta \cup \mathbf{1}$ where δ denotes the canonical map $K^\times \to H^1(K, \mu_{\ell^n})$ (see [EM11a] Proposition 2.6 for a precise reference). Denote by

ω the fixed generator of μ_{ℓ^n} which corresponds to $1 \in \mathbb{Z}/\ell^n$ under our isomorphism $\mu_{\ell^n} = \langle\omega\rangle \cong \mathbb{Z}/\ell^n$. This induces isomorphisms $H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) \cong H^1(G_K, \mu_{\ell^n}) \cong K_*^M(K)/\ell^n$ and $H^2(\mathcal{G}_K, \mathbb{Z}/\ell^n) \cong H^2(G_K, \mu_{\ell^n}^{\otimes 2}) \cong K_2^M(K)/\ell^n$. Under these induced isomorphisms, the Bockstein morphism $H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) \to H^2(\mathcal{G}_K, \mathbb{Z}/\ell^n)$ corresponds to the map $K_1^M(K)/\ell^n \to K_2^M(K)/\ell^n$ defined by $x \mapsto \{x, \omega\}$. Namely, the following diagram commutes:

$$\begin{array}{ccccccc} K_1^M(K)/\ell^n & \xrightarrow{\cong} & H^1(K, \mu_{\ell^n}) & \xrightarrow{\cong} & H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) & = & H^1(\mathcal{G}_K, \mathbb{Z}/\ell^n) \\ \downarrow{\scriptstyle x\mapsto\{x,\omega\}} & & \downarrow{\scriptstyle \text{induced}} & & \downarrow{\scriptstyle \beta\cup\mu_{\ell^n}} & & \downarrow{\scriptstyle \beta} \\ K_2^M(K)/\ell^n & \xrightarrow{\cong} & H^2(K, \mu_{\ell^n}^{\otimes 2}) & \xrightarrow{\cong} & H^2(\mathcal{G}_K, \mu_{\ell^n}) & \xrightarrow{\cong} & H^2(\mathcal{G}_K, \mathbb{Z}/\ell^n) \end{array}$$

where the isomorphisms on the left are canonical given by the Galois symbol, while the isomorphisms on the right are induced by our fixed isomorphism $\mu_{\ell^n} = \langle\omega\rangle \cong \mathbb{Z}/\ell^n$. We will use this fact in the remainder of the thesis without reference to this commutative diagram. Also, we will tacitly use our isomorphism $\Lambda_n \cong \Lambda_n(1)$ to identify $H^m(\mathcal{G}_K, \Lambda_n(i))$ with $H^m(\mathcal{G}_K, \Lambda_n)$ whenever we're dealing with a field K which contains μ_{ℓ^n}.

Theorem 12.0.2. *Let K be a field such that* $\operatorname{Char} K \neq \ell$ *and $\mu_{2\ell^n} \subset K$. Let $\sigma, \tau \in \mathcal{G}_K^{a,n}$ be given. Consider σ, τ as homomorphisms $\sigma, \tau : K^\times \to \Lambda_n$ via our chosen isomorphism of G_K-modules $\Lambda_n(1) \cong \Lambda_n$ and the Kummer pairing. Then σ, τ form a CL-pair if and only if they form a C-pair.*

Proof. We can assume that $n \in \mathbb{N}$ is finite for then we obtain the $n = \infty$ case in the limit as in Proposition 10.2.1 along with the comment at the end of this

proof. Also, we can assume that $\langle \sigma, \tau \rangle$ is non-cyclic for otherwise the claim is trivial. Furthermore, we can assume without loss that σ, τ are quasi-independent so that $\langle \sigma, \tau \rangle = \langle \sigma \rangle \times \langle \tau \rangle$. As such, we can choose a minimal generating set $(\sigma_i)_{i \in \Lambda}$ for $\mathcal{G}_K^{a,n}$ so that $1, 2 \in \Lambda$, $\sigma_1^{\ell^a} = \sigma$ and $\sigma_2^{\ell^b} = \tau$. We denote also by $(\tilde{\sigma}_i)_i$ a corresponding (convergent) set of generators for $\mathcal{G}_K$ and $(x_i)_i$ the dual basis for $H^1(\mathcal{G}_K) = K^\times/\ell^n$ associated to $(\sigma_i)_i$. Consider σ_i as homomorphisms $K^\times \to \Lambda_n$ and denote by $H_0 = \ker \sigma_1 \cap \ker \sigma_2$ and $H = \ker \sigma \cap \ker \tau$. Then $H_0 \leq H$, $K^\times/H_0$ is a free rank 2 $\mathbb{Z}/\ell^n$-module generated by x_1, x_2 and $H = \langle H_0, x_1^{\ell^{n-a}}, x_2^{\ell^{n-b}} \rangle$.

Assume first that σ, τ form a CL-pair. Denote by $A = \langle \sigma_1, \sigma_2 \rangle$ and $A^c = \langle \tilde{\sigma}_1, \tilde{\sigma}_2 \rangle$ mod $\mathcal{G}_K^{(3,n)} \leq \mathcal{G}_K^{c,n}$. Consider the following commutative diagram:

$$\begin{array}{ccc} H^1(\mathcal{G}_K^{a,n}) \times H^1(\mathcal{G}_K^{a,n}) & \xrightarrow{\inf \circ \cup} & H^2(\mathcal{G}_K^{c,n}) \\ \downarrow{\scriptstyle \mathrm{res} \times \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\ H^1(A) \times H^1(A) & \xrightarrow[\inf \circ \cup]{} & H^2(A^c) \end{array}$$

Via our Kummer isomorphism $H^1(\mathcal{G}_K^{a,n}) \cong K^\times/\ell^n$, the restriction map $H^1(\mathcal{G}_K^{a,n}) \to H^1(A)$ corresponds precisely to the projection $K^\times/\ell^n \to K^\times/H_0$. By Lemma 11.1.1, the top map factors via $K_2^M(K)/\ell^n$ and therefore the bottom map factors via $K_2^M(K)/H_0$. Let F be the free pro-ℓ group on generators $\tilde{\gamma}_1, \tilde{\gamma}_2$, and consider the surjective map $F \to A^c$ defined by $\tilde{\gamma}_i \mapsto \tilde{\sigma}_i \mod \mathcal{G}_K^{(3,n)}$; denote by T the kernel this presentation $F \to A^c$ and γ_i the image of $\tilde{\gamma}_i$ in $F^{a,n}$. As $\sigma_1^{\ell^a}, \sigma_2^{\ell^b}$ form a CL-pair, we see that $T \cdot F^{(3,c)}/F^{(3,c)} = T/F^{(3,c)}$ contains an element of the form:

$$\rho = [\gamma_1, \gamma_2]^{\ell^{a+b}} \cdot (\gamma_1^\beta)^{c_1 \cdot \ell^a} \cdot (\gamma_2^\beta)^{c_2 \cdot \ell^b}.$$

We recall the pairing associated to the presentation $F \to A^c$,

$$(\bullet, \bullet) : H^2(A^c) \times \left(\frac{T}{[F,T] \cdot T^{\ell^n}} \right) \to \mathbb{Z}/\ell^n,$$

satisfies $(x_1 \cup x_2, \rho) = -\ell^{a+b}$ and thus $K_2^M(K)/H_0 = \langle \{x_1, x_2\}_{H_0} \rangle$ has order ℓ^{n-c_0} for some c_0 such that $c_0 \leq a+b$. On the other hand, since $H = \langle H_0, x_1^{\ell^{n-a}}, x_2^{\ell^{n-b}} \rangle$, we see that $K_2^M(K)/H = \langle \{x_1, x_2\}_{H_0} \rangle / \langle \{x_1^{\ell^{n-a}}, x_2\}_{H_0}, \{x_1, x_2^{\ell^{n-b}}\}_{H_0} \rangle$. Thus, $K_2^M(K)/H$ has order ℓ^{n-c} where $\max(a,b,c_0) = c \leq a+b$. Therefore σ, τ form a C-pair by the K-theoretic criterion (Proposition 10.2.1).

Conversely, assume that σ, τ form a C-pair. Let $S \to \mathcal{G}_K$ be a minimal free presentation associated to the minimal generating set $(\tilde{\sigma}_i)_i$; i.e. S is free on $(\tilde{\gamma}_i)_i$ and $\tilde{\gamma}_i \mapsto \tilde{\sigma}_i$ under the map $S \to \mathcal{G}_K$ so that $S^{a,n} \to \mathcal{G}_K^{a,n}$ is an isomorphism. We also denote by γ_i the image of $\tilde{\gamma}_i$ in $S^{a,n}$. Furthermore, we denote by R the kernel of the induced surjective map $S^{c,n} \to \mathcal{G}_K^{c,n}$. Then $K_2^M(K)/H$ is a rank-1 quotient of $K_2^M(K)/\ell^n$ which corresponds via the pairing of Proposition 11.2.1 to a rank-1 subgroup of R, generated by, say

$$\rho = \prod_{i<j} [\gamma_i, \gamma_j]^{a_{ij}} \cdot \prod_r (\gamma_r^\pi)^{b_r}.$$

As $x_i \in H$ for all $i \neq 1, 2$ we deduce that $\rho = [\gamma_1, \gamma_2]^{a_{12}} \cdot (\gamma_1^\pi)^{b_1} \cdot (\gamma_2^\pi)^{b_2}$. Recall that ω denotes the generator of μ_{ℓ^n} which corresponds to $1 \in \mathbb{Z}/\ell^n$. Write $\omega = x_1^{-2j} x_2^{2k}$ mod H (recall that $\mu_{2\ell^n} \subset K$ so that ω is indeed a square in $K^\times$) then:

- $(\{x_1, x_2\}_H, \rho) = -a_{12}$
- $(\{x_1, \omega\}_H, \rho) = 2k(\{x_1, x_2\}_H, \rho) = -2ka_{12} = -b_1$.

- $(\{x_2, \omega\}_H, \rho) = 2j(\{x_1, x_2\}_H, \rho) = -2ja_{12} = -b_2$.

where $(\bullet, \bullet)$ denotes the pairing of Proposition 11.2.1, identifying $K_2^M(K)/H$ with the corresponding quotient of $H^2(\mathcal{G}_K)$. Thus:

$$\rho = ([\gamma_1, \gamma_2](\gamma_1^\beta)^k(\gamma_2^\beta)^j)^{a_{12}}.$$

Since $\langle\rho\rangle$ is in a perfect pairing with $K_2^M(K)/H = \langle\{x_1, x_2\}_H\rangle$, we deduce from the K-theoretic criterion (Proposition 10.2.1) that $a_{12} \in \mathbb{Z}/\ell^n$ has (additive) order ℓ^{n-c} where $c \leq a + b$. In particular, $\ell^{a+b} = a_{12} \cdot t$ for some t so that there exists an element of R of the form:

$$\rho^t = [\gamma_1, \gamma_2]^{\ell^{a+b}}(\gamma_1^\beta)^{k\ell^{a+b}}(\gamma_2^\beta)^{j\ell^{a+b}} = [\gamma_1^{\ell^a}, \gamma_2^{\ell^b}] \cdot ((\gamma_1^{\ell^a})^\beta)^{k\ell^b}((\gamma_2^{\ell^b})^\beta)^{j\ell^a}$$

and in particular we deduce that $[\sigma, \tau] \in \langle\sigma^\beta, \tau^\beta\rangle$ as required. To conclude the theorem in the case where $n = \infty$, we note that j, k above would have been zero provided that $\mu_{\ell^\infty} \subset K$. □

Remark 12.0.3. As an immediate corollary of Theorem 12.0.2 we deduce the following. Given $(\sigma_i)_i \in \mathcal{G}_K^{a,n}$ which are pairwise CL, then any pair $\sigma, \tau \in \langle\sigma_i\rangle_i$ form a CL-pair. We note that this doesn't follow immediately from the definition of CL-pairs. We also deduce that, for $A \leq \mathcal{G}_K^{a,n}$, the subset $\mathbf{I}^{\mathrm{CL}}(A) \subset A$ is indeed a subgroup which corresponds to $\mathbf{I}^{\mathrm{C}}(A)$ as defined in Part II under the isomorphism $\mathcal{G}_K^{a,n} \cong \mathcal{G}_K^a(n)$ arising from Kummer theory.

Remark 12.0.4. Let K be a field such that $\mathrm{Char}\, K \neq \ell$ and $\mu_{2\ell} \subset K$ and let $A \leq \mathcal{G}_K^{a,1}$ be given. Using Remark 10.2.2, we can now give an alternative definition for $\mathbf{I}^{\mathrm{CL}}(A)$.

Namely, in this remark we will show that:

$$\mathbf{I}^{\mathrm{CL}}(A) = \{\sigma \in A \ : \ \forall \tau \in A, \ [\sigma, \tau] \in A^{\beta}\} =: I.$$

Observe that $\mathbf{I}^{\mathrm{CL}}(A) \leq I$ by definition and so it suffices to prove that $I \leq \mathbf{I}^{\mathrm{CL}}(A)$. We will identify $\mathcal{G}_K^a(1)$ and $\mathcal{G}_K^{a,1}$ via Kummer theory, as well as the notions of C-pairs resp. CL-pairs using Theorem 12.0.2.

Denote by $T = A^{\perp}$ and $H = I^{\perp}$ and suppose that $T \leq G \leq H \leq K^{\times}$ is given such that H/G is cyclic. We will show that $\mathrm{Hom}(K^{\times}/G, \mathbb{Z}/\ell) \leq A$ is a C-group, therefore proving that $\langle I, f \rangle$ is a C-group for all $f \in A$. This would immediately imply that $I \leq \mathbf{I}^{\mathrm{CL}}(A)$ as required above.

Let $x_1 \in K^{\times} \smallsetminus H$ and $x_2 \in K^{\times} \smallsetminus T$ be given such that ($x_1 \mod T$) and ($x_2 \mod T$) are $\mathbb{Z}/\ell$-independent. We can therefore complete x_1, x_2 to a $\mathbb{Z}/\ell$-basis $(x_i)_i$ for $K^{\times}/T$, with dual basis $(\sigma_i)_i$ for A, in such a way so that $\sigma_1 \in I$. Thus, we see that $[\sigma_1, \sigma_2] \in \langle \sigma_i^{\beta} \rangle_i$ by the definition of I. Arguing as in the first part of the proof of Theorem 12.0.2, we will deduce that $\{x_1, x_2\}_T \neq 0$. Indeed, choose lifts (continuously) $\sigma_i^c \in \mathcal{G}_K^{c,1}$ for σ_i, denote by $A^c = \langle \sigma_i^c \rangle_i$, F the free pro-ℓ-group on $(\gamma_i)_i$, and $F \twoheadrightarrow A^c$ a free presentation sending γ_i to σ_i^c. Denote by R the kernel of $F \to A^c$; thus $R/F^{(3,1)}$ contains an element of the form:

$$\rho = [\gamma_1, \gamma_2] \cdot \prod_r (\gamma_i^{\beta})^{b_r}.$$

And, as in the proof of Theorem 12.0.2, we see that $(x_1 \cup x_2, \rho) = 1$ where $(\bullet, \bullet)$ is the pairing of Proposition 11.2.1. Thus $\{x_1, x_2\}_T \neq 0$ since the cup product

$H^1(A, \mathbb{Z}/\ell) \times H^1(A, \mathbb{Z}/\ell) = H^1(A^c, \mathbb{Z}/\ell) \times H^1(A^c, \mathbb{Z}/\ell) \to H^2(A^c, \mathbb{Z}/\ell)$ factors through $K_2^M(K)/T$.

Now suppose that $x \in K^\times \smallsetminus G$ is given and consider $1 - x \in K^\times$. If either $x \notin H$ or $1 - x \notin H$, we deduce from the argument above that $\langle x, 1 - x \rangle \mod T$ is cyclic since $\{x, 1 - x\}_T = 0$ (and thus $(x \mod T), ((1 - x) \mod T)$ cannot be $\mathbb{Z}/\ell$-independent); therefore $\langle x, 1 - x \rangle \mod G$ is cyclic as well. On the other hand, if both $x, 1 - x \in H$, then $\langle x, 1 - x \rangle \mod G$ is cyclic since H/G is cyclic. Thus, G satisfies condition (4) of Remark 10.2.2 which proves that $\mathrm{Hom}(K^\times/G, \mathbb{Z}/\ell)$ is a C-group.

Chapter 13

Minimized Inertia and Decomposition Groups

We would like now to describe the structure of decomposition/inertia with respect to Kummer theory and $\mathcal{G}_K^{c,n} \twoheadrightarrow \mathcal{G}_K^{a,n}$. Let $n \in \overline{\mathbb{N}}$ and assume further that $\mu_{\ell^n} \subset K$. Say that v is a valuation of K whose residue characteristic may or may not be ℓ. Recall that $K^{a,n} = K(\sqrt[\ell^n]{K})$ denotes the maximal ℓ^n-elementary abelian extension of K and let v' be a prolongation of v to $K^{a,n}|K$. In other words, one has $\mathcal{G}_K^{a,n} = \mathrm{Gal}(K^{a,n}|K)$. Recall that Kummer theory yields a perfect pairing (here $\widehat{K} = \widehat{K^\times} = \lim_m K^\times/\ell^m$ denotes the ℓ-adic completion of $K^\times$):

$$K^\times/\ell^n \times \mathcal{G}_K^{a,n} \to \mu_{\ell^n}, \quad \text{resp.} \quad \widehat{K} \times \mathcal{G}_K^{a,n} \to \mu_{\ell^\infty} \quad \text{if } n = \infty.$$

For simplicity, we denote by $Z_v^n = Z_{v'|v}$ resp. $T_v^n = T_{v'|v}$ the decomposition and inertia subgroups of $v'|v$ inside $\mathcal{G}_K^{a,n}$; since $\mathcal{G}_K^{a,n}$ is abelian, the subgroups $T_v^n \leq Z_v^n$

are independent of choice of prolongation v'.

Motivated by the following proposition, we introduce the so-called *minimized* decomposition/inertia groups:

Definition 13.0.5. Let K be a field of characteristic different from ℓ which contains μ_{ℓ^n}. Let v be a valuation of K. We call D_v^n resp. I_v^n the minimized decomposition resp. minimized inertia group of v, defined as follows:

$$D_v^n := \mathrm{Gal}(K^{a,n}|K(\sqrt[\ell^n]{U_v^1})), \quad \text{and} \quad I_v^n := \mathrm{Gal}(K^{a,n}|K(\sqrt[\ell^n]{U_v})).$$

The proof of the following proposition can be found in [Pop10b] Fact 2.1 in the $n = \infty$ case and in [Pop11] in the $n = 1$ case, but is explicitly stated for valuations v such that $\mathrm{Char}\, k(v) \neq \ell$. It turns out that the same proof works, at least in one direction, even if $\mathrm{Char}\, k(v) = \ell$ and we summarize this in the proposition below.

Proposition 13.0.6. *Let (K, v) be a valued field such that $\mathrm{Char}\, K \neq \ell$ and $\mu_{\ell^n} \subset K$. Then $D_v^n \leq Z_v^n$ and $I_v^n \leq T_v^n$. If furthermore $\mathrm{Char}\, k(v) \neq \ell$ then these inequalities are actually equalities.*

Proof. The $n = \infty$ case follows easily from the $n \in \mathbb{N}$ case. Thus, we prove the claim for $n \in \mathbb{N}$.

Suppose $a \in K^\times$ is such that $\sqrt[\ell^n]{a} \in (K^{a,n})^{Z_v^n}$ and denote by v_Z a prolongation of v to $(K^{a,n})^{Z_v^n}$. Since $\Gamma_{v_Z} = \Gamma_v$, there exists $y \in K^\times$ such that $v(a) = \ell^n \cdot v(y)$. Moreover, as $k(v) = k(v_Z)$, there exists $z \in U_v$ such that $\sqrt[\ell^n]{a}/y \in z \cdot U_v^1$. Namely, $a/(yz)^{\ell^n} \in U_v^1$ so that $\sqrt[\ell^n]{a} \in K(\sqrt[\ell^n]{U_v^1})$. Thus, $\mathrm{Gal}(K^{a,n}|K(\sqrt[\ell^n]{U_v^1})) \leq Z_v^n$ since

$(K^{a,n})^{Z_v^n} \subset K(\sqrt[\ell^n]{U_v^1})$. The proof that $K^T := (K^{a,n})^{T_v^n} \subset K(\sqrt[\ell^n]{U_v})$ is similar using the fact that $v'(K^T) = \Gamma_v$.

Assume furthermore that $\operatorname{Char} k(v) \neq \ell$. Let (K^Z, v) be some Henselization of (K, v); recall that $K^Z \cap K^{a,n} = (K^{a,n})^{Z_v^n}$. Let $a \in U_v^1$ be given. The polynomial $X^{\ell^n} - a$ reduces mod $\mathfrak{m}_v$ to $X^{\ell^n} - 1$. Since $\operatorname{Char} k(v) \neq \ell$ one has $\mu_{\ell^n} \subset k(v)$ and this polynomial has ℓ^n unique roots in $k(v)$. Namely, $X^{\ell^n} - a$ has a root in $K^Z \cap K^{a,n} = (K^{a,n})^{Z_v^n}$. By Hensel's lemma, $K(\sqrt[\ell^n]{U_v^1}) \subset (K^{a,n})^{Z_v^n}$. The proof that $K(\sqrt[\ell^n]{U_v}) \subset (K^{a,n})^{T_v^n} =: K^T$ is similar since K^T is the maximal unramified sub-extension of $K^{a,n}|K$. □

By Proposition 13.0.6, we see that $D_v^n = Z_v^n$ and $I_v^n = T_v^n$ provided that $\operatorname{Char} k(v) \neq \ell$, while $D_v^n \leq Z_v^n$ and $I_v^n \leq T_v^n$ in general. If $\operatorname{Char} k(v) = \ell$, however, equality does not hold in general, as can be deduced from the following remark.

Remark 13.0.7. If $\operatorname{Char} K \neq \ell$, $\mu_\ell \subset K$ and $\operatorname{Char} k(v) = \ell$, one has $D_v^1 \leq T_v^1$. This can be deduced in a similar way to [Pop10a] Lemma 2.3(2); we sketch the argument below. Denote by $\lambda = \omega - 1 \in K$ where $\omega = \omega_\ell$ is our fixed generator of μ_ℓ and recall that $v(\lambda) > 0$ since $\operatorname{Char} k(v) = \ell$. Let $u \in U_v$ be given and set $u' = \lambda^\ell \cdot u + 1 \in U_v^1$. Then the extension of K corresponding to the equation $X^\ell - u'$ is precisely the same as the extension of K corresponding to the equation $Y^\ell - Y + \lambda \cdot f(Y) = u$ for some (explicit) polynomial $f(Y)$; this is done by making the change of variables $X = \lambda Y + 1$. On the other hand, the maximal $(\mathbb{Z}/\ell)$-elementary abelian Galois extension of $k(v)$ is the extension of $k(v)$ generated by roots of polynomials of

the form $X^\ell - X = \bar{u}$ for $\bar{u} \in kw$. Thus, the maximal $(\mathbb{Z}/\ell)$-elementary abelian Galois extension of $k(v)$ is a subextension of the residue extension corresponding to $K(\sqrt[\ell]{U_v^1})|K$.

Proposition 13.0.8. *Let (K, v) be a valued field such that* $\operatorname{Char} K \neq \ell$ *and $\mu_{2\ell^n} \subset K$. Let $\sigma, \tau \in D_v^n$ be given and consider them as homomorphisms $K^\times \to \Lambda_n$ via Kummer theory and our fixed isomorphism $\Lambda_n(1) \cong \Lambda_n$. Then the following hold:*

1. *If $\sigma, \tau \in I_v^n$ then $[\sigma, \tau] = 0$.*
2. *If $\sigma \in I_v^n$ and $\tau \in D_v^n$ then $[\sigma, \tau] \in \langle \sigma^\beta \rangle$; more precisely, if $\tau(\omega) = 2a \in \Lambda_n$ then $[\sigma, \tau] = -2a \cdot \sigma^\pi = -a \cdot \sigma^\beta$.*

Proof. In order to prove this claim, it suffices to assume that σ, τ are actually Λ_n-independent. Choose a minimal generating set $(\sigma_i)_i$ such that $\sigma_1 = \sigma$ and $\sigma_2 = \tau$ with corresponding dual basis $(x_i)_i$ for $H^1(K, \Lambda_n(1)) \cong H^1(\mathcal{G}_K^{a,n}, \Lambda_n)$. We then choose a corresponding free presentation $S \to \mathcal{G}_K$ and use the same notation as in the second part of the proof of Theorem 12.0.2 – in particular, R denotes the kernel of $S^{c,n} \to \mathcal{G}_K^{c,n}$. We see that it suffices to prove the stronger part of (2) since, if $\tau = \sigma_2 \in I_v^n$, we see that $\sigma_2(\omega) = 0$; in both cases, we see that $\sigma_1(\omega) = 0$ since $\omega \in U_v$. Suppose, then, that $\sigma_2(\omega) = 2a$ and denote by $H = \ker \sigma_1 \cap \ker \sigma_2$. Therefore, $\omega = x_1^{\sigma_1(\omega)} \cdot x_2^{\sigma_2(\omega)} \mod H = x_2^{2a} \mod H$. In light of Theorem 12.0.2 and Lemma 6.0.7, we see that R contains an element of the form

$$\rho = [\gamma_1, \gamma_2] \cdot (\gamma_1^\beta)^{c_1} \cdot (\gamma_2^\beta)^{c_2},$$

and arguing as in the proof of Theorem 12.0.2 we see that $\langle\rho\rangle$ is in perfect duality with $K_2^M(K)/H$ via the pairing of Proposition 11.2.1; namely, $(\{x_1, x_2\}, \rho) = 1$ and $(\beta x_i, \rho) = 2c_i$. Therefore, we see that $2c_1 = (\beta x_1, \rho) = (\{x_1, \omega\}, \rho) = 2a(\{x_1, x_2\}, \rho) = 2a$ and $2c_2 = (\beta x_2, \rho) = (\{x_2, \omega\}, \rho) = 2a(\{x_2, x_2\}, \rho) = 0$. In particular, R contains an element ρ of the form $[\gamma_1, \gamma_2] \cdot (\gamma_1^\beta)^a$. Thus, we see that $[\sigma_1, \sigma_2] = -a \cdot \sigma_1^\beta$, as required. □

We therefore obtain the following structural properties of minimized inertia and decomposition groups which are completely analogous to the usual structure of inertia/decomposition groups for valuations of characteristic different from ℓ:

Remark 13.0.9. We use the notation/context of Proposition 13.0.8. Choose a minimal generating set $(\eta_i)_i$ for I_v^n and complete it to a minimal generating set $(\eta_i)_j \cup (\tau_j)_j$ for D_v^n. Choose (continuously) lifts $\eta_i^c \in \mathcal{G}_K^{c,n}$ and $\tau_j^c \in \mathcal{G}_K^{c,n}$ for η_i and τ_j. Denote by $I^c = \langle \eta_i^c \rangle$ and $D^c = \langle \eta_i^c, \tau_j^c \rangle$. We deduce from Proposition 13.0.8 above that I^c is an **abelian normal subgroup** of D^c. Moreover, by construction we see that $D^c \cap (\mathcal{G}_K^{c,n})^{(2,n)} = (D^c)^{(2,n)}$, $I^c \cap (\mathcal{G}_K^{c,n})^{(2,n)} = (I^c)^{(2,n)} = I^c \cap (D^c)^{(2,n)}$, the image of I^c in $\mathcal{G}_K^{a,n}$ is I_v^n, the image of D^c in $\mathcal{G}_K^{a,n}$ is D_v^n and $(D^c/I^c)^{a,n} = \mathcal{G}_{k(v)}^{a,n}$.

Chapter 14

Detecting Valuations in Galois Groups

In this chapter we will translate the main results of Chapters 8 and 9 into the Galois-theoretical setting using Theorem 12.0.2. Theorems 14.0.10 and 14.0.11 are the main theorems of this thesis which provide a group-theoretical recipe to recover valuations using our Λ_N-abelian-by-central Galois groups $\mathcal{G}_K^{c,N}$ for $N \geq \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Below we restate and prove the two main theorems from the introduction, recalling that we take $\mathbf{R}(n) := \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$ in §1.4. In order to stay consistent with the body of the thesis, we will use the notation $\mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$ below.

Theorem 14.0.10. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field such that* $\operatorname{Char} K \neq \ell$ *and $\mu_{2\ell^N} \subset K$.*

1. *Let $D \leq \mathcal{G}_K^{a,n}$ be given. Then there exists a valuation v of K such that $D \leq D_v^n$*

and $D/(D\cap I_v^n)$ is cyclic if and only if there exists a CL-group $D' \leq \mathcal{G}_K^{a,N}$ such that $D'_n = D$.

2. *Let $I \leq D \leq \mathcal{G}_K^{a,n}$ be given. Then there exists a valuation $v \in \mathcal{V}_{K,n}$ such that $I = I_v^n$ and $D = D_v^n$ if and only if the following hold:*

   (a) *There exist $D' \leq \mathcal{G}_K^{a,N}$ such that $(\mathbf{I}^{\mathrm{CL}}(D'))_n = I$ and $D'_n = D$.*

   (b) *$I \leq D \leq \mathcal{G}_K^{a,n}$ are maximal with this property – i.e. if $D \leq E \leq \mathcal{G}_K^{a,n}$ and $E' \leq \mathcal{G}_K^{a,N}$ is given such that $E'_n = E$ and $I \leq (\mathbf{I}^{\mathrm{CL}}(E'))_n$, then $D = E$ and $I = (\mathbf{I}^{\mathrm{CL}}(E'))_n$.*

   (c) *$\mathbf{I}^{\mathrm{CL}}(D) \neq D$ (i.e. D is not a CL-group).*

Proof. Using our isomorphism $\Lambda_N \cong \Lambda_N(1)$, along with the observation that $-1 \in K^{\times \ell^N}$, we obtain isomorphisms using Kummer theory, $\phi_m : \mathcal{G}_K^{a,m} \cong \mathcal{G}_K^a(m)$ for all $m \leq N$ which are compatible with the projections $\mathcal{G}_K^{a,M} \to \mathcal{G}_K^{a,m}$ resp. $\mathcal{G}_K^a(M) \to \mathcal{G}_K^a(m)$ for $m \leq M \leq N$. Furthermore, let $H \leq K^\times$ be given. Via these isomorphisms, the subgroup $\mathrm{Gal}(K^{a,m}|K(\sqrt[\ell^m]{H}))$ of $\mathcal{G}_K^{a,m}$ is mapped isomorphically onto $\mathrm{Hom}(K^\times/H, \Lambda_m) \leq \mathcal{G}_K^a(m)$. Thus, in particular, I_v^m is mapped isomorphically onto $I_v(m)$ and D_v^m is mapped isomorphically onto $D_v(m)$ for all valuations v of K and $m \leq N$. By Theorem 12.0.2, these isomorphisms send CL-pairs to C-pairs and in particular, $\mathbf{I}^{\mathrm{CL}}(A)$ is sent to $\mathbf{I}^{\mathrm{C}}(\phi_m A)$ for $A \leq \mathcal{G}_K^{a,m}$. Now, in light of these compatible identifications, we immediately see the first part of Theorem 14.0.10 follows from Proposition 8.2.2, and the second part from Theorem 8.2.4. □

Before we proceed to prove the next main theorem, let us first recall some notation from the introduction. We denote by $\mathcal{V}'_{K,n}$ the collection of (possibly trivial) valuations v of K such that:

1. $\mathrm{Char}\, k(v) \neq \ell$.

2. Γ_v contains no non-trivial ℓ-divisible convex subgroups.

3. v is maximal among all valuations w such that $\mathrm{Char}\, k(w) \neq \ell$, $D^n_v = D^n_w$ and Γ_w contains no non-trivial ℓ-divisible convex subgroups; i.e. for all refinements w of v such that $\mathrm{Char}\, k(w) \neq \ell$ and $D^n_w = D^n_v$ as subgroups of $\mathcal{G}_K^{a,n}$, one has $I^n_w = I^n_v$.

4. $\mathcal{G}^{a,n}_{k(v)}$ is non-cyclic.

Thus $\mathcal{V}'_{K,n}$ is the analogue of $\mathcal{V}_{K,n}$ when one only considers valuations with residue characteristic different from ℓ. As such, we observe that $\mathcal{V}_{K,n} = \mathcal{V}'_{K,n}$ whenever $\ell \neq \mathrm{Char}\, K > 0$. For an arbitrary field K on the other hand, one has the potentially proper inclusion:

$$\{v \in \mathcal{V}_{K,n} \ : \ \mathrm{Char}\, k(v) \neq \ell\} \subset \mathcal{V}'_{K,n}.$$

We now restate Theorem 1.4.2 using the notation of the paper.

Theorem 14.0.11. *Let $n \in \overline{\mathbb{N}}$ be given and let $N \geq \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field such that* $\mathrm{Char}\, K \neq \ell$ *and $\mu_{2\ell^N} \subset K$.*

1. *Let* $D \leq \mathcal{G}_K^{a,n}$ *be given and denote by* $L := (K^{a,n})^D$. *Then there exists a valuation* v *of* K *such that* $\operatorname{Char} k(v) \neq \ell$, $D \leq Z_v^n$ *and* $D/(D \cap T_v^n)$ *is cyclic if and only if there exists a CL-group* $D' \leq \mathcal{G}_L^{a,N}$ *such that* $(D'_n)_K = D$.

2. *Assume that* $\mathbf{I}^{\mathrm{CL}}(\mathcal{G}_K^{a,n}) \neq \mathcal{G}_K^{a,n}$ *and consider* $(\mathbf{I}^{\mathrm{CL}}(\mathcal{G}_K^{a,N}))_n =: T$. *Then there exists a (possibly trivial) valuation* $v \in \mathcal{V}_{K,n}$ *such that* $\operatorname{Char} k(v) \neq \ell$, $T = T_v^n$ *and* $\mathcal{G}_K^{a,n} = Z_v^n$.

3. *Let* $v \in \mathcal{V}_{K,n}$ *be given and denote by* $I := I_v^n \leq D_v^n =: D$, $L := (K^{a,n})^D$. *Then* $\operatorname{Char} k(v) \neq \ell$ *if and only if there exist* $I' \leq D' \leq \mathcal{G}_L^{a,N}$ *such that:*

   (a) $I' \leq \mathbf{I}^{\mathrm{CL}}(D')$.

   (b) $(I'_n)_K = I$ *and* $(D'_n)_K = D$.

   Moreover, if these equivalent conditions hold then $I = I_v^n = T_v^n$ *and* $D = D_v^n = Z_v^n$.

4. *Let* $I \leq D \leq \mathcal{G}_K^{a,n}$ *be given and denote by* $L := (K^{a,n})^D$. *Then there exists a valuation* $v \in \mathcal{V}'_{K,n}$ *such that* $I = T_v^n$ *and* $D = Z_v^n$ *if and only if the following hold:*

   (a) *There exist* $D' \leq \mathcal{G}_L^{a,N}$ *such that* $((\mathbf{I}^{\mathrm{CL}}(D'))_n)_K = I$ *and* $(D'_n)_K = D$.

   (b) $I \leq D \leq \mathcal{G}_K^{a,n}$ *are maximal with this property – i.e. if* $D \leq E \leq \mathcal{G}_K^{a,n}$ *and* $E' \leq \mathcal{G}_{L_E}^{a,N}$ *(where* $L_E := (K^{a,n})^E$*) is given such that* $(E'_n)_K = E$ *and* $I \leq ((\mathbf{I}^{\mathrm{CL}}(E'))_n)_K$, *then* $D = E$ *and* $I = ((\mathbf{I}^{\mathrm{CL}}(E'))_n)_K$.

(c) $\mathbf{I}^{\mathrm{CL}}(D) \neq D$ *(i.e.* D *is not a CL-group).*

Proof. Using our chosen isomorphism $\Lambda_n \cong \Lambda_n(1)$, we obtain the same compatible isomorphisms $\mathcal{G}_K^{a,m} \cong \mathcal{G}_K^a(m)$ for all $m \leq N$, as in the proof of Theorem 1.4.1. We furthermore obtain similar isomorphisms $\mathcal{G}_F^{a,m} \cong \mathcal{G}_F^a(m)$ for all field extensions $F|K$, in a compatible way with the isomorphisms $\mathcal{G}_K^{a,m} \cong \mathcal{G}_K^a(m)$. We will tacitly use these compatible isomorphisms and also the equivalence of "C-pairs" and "CL-pairs."

We will further make use of the following observation. Suppose $D \leq Z_v^n$ and denote by $L := (K^{a,n})^D$. Choose a prolongation w of v to L. Then the image of the canonical map $Z_w^n \to Z_v^n$ has image D. Moreover, the image of $T_w^n \to T_v^n$ is precisely $D \cap T_v^n$. In particular, we see that the image of the canonical map $Z_w^N \to Z_v^n$ is D and the image of $T_w^N \to T_v^n$ is $D \cap T_v^n$. Furthermore, we recall that by Proposition 13.0.6, $I_v^m = T_v^m$ and $D_v^m = Z_v^m$ whenever $\operatorname{Char} k(v) \neq \ell$ and $m \leq N$.

To 1. Let $D \leq \mathcal{G}_K^{a,n}$ be given and denote by $L := (K^{a,n})^D$. Assume first that there exists a CL-group $D' \leq \mathcal{G}_L^{a,N}$ such that $(D'_n)_K = D$. By Theorem 9.0.8, there exists a valuative subgroup $I \leq D$ such that $\operatorname{Char} k(v_I) \neq \ell$, $D \leq D_{v_I}^n$, and D/I is cyclic.

Conversely, assume that there exists a valuation v such that $\operatorname{Char} k(v) \neq \ell$, $D \leq Z_v^n$ and $D/(D \cap T_v^n)$ is cyclic. Denote by $I = D \cap T_v^n$ and choose $f \in D$ such that $D = \langle I, f \rangle$. Choose a prolongation v' of v to L. By the observation above, along with the discussion of §3.3, there exits $f' \in Z_{v'}^N$ such that $(f'_n)_K = f$. Moreover, I is contained in the image of the canonical map $T_{v'}^N \to T_v^n$; we denote

by I' the pre-image of I in $T^N_{v'}$. By Lemma 6.0.7 and/or the discussion of §3.3, $D' = \langle I', f' \rangle$ is a CL-group and $(D'_n)_K = D$.

To 2. Denote by $I = (\mathbf{I}^{\mathrm{CL}}(\mathcal{G}^{a,N}_K))_n$. By Proposition 8.2.3, $I = I_{v_I}(n)$ and $\mathcal{G}^{a,n}_K = D_{v_I}(n)$. Moreover, by Theorem 9.0.9, $\mathrm{Char}\, k(v_I) \neq \ell$, as needed.

To 3. Let $v \in \mathcal{V}_{K,n}$ be given and denote by $I = I^n_v$ and $D = D^n_v$, and $L := (K^{a,n})^D$. Assume first that there exists $I' \leq \mathbf{I}^{\mathrm{CL}}(D') \leq \mathcal{G}^{a,N}_L$ such that $(I'_n)_K = I$ and $(D'_n)_K = D$. By Theorem 9.0.9, I is valuative, $D \leq D^n_{v_I}$ and $\mathrm{Char}\, k(v_I) \neq \ell$. On the other hand, $v = v_I$ by our assumption on v and I. Therefore, we see that $\mathrm{Char}\, k(v) \neq \ell$.

Conversely, assume that $\mathrm{Char}\, k(v) \neq \ell$. Then $I = T^n_v$ and $D = Z^n_v$. Choose a prolongation w of v to L and consider

$$I' := T^N_w = I^N_w \leq D^N_w = Z^N_w =: D'.$$

By Lemma 6.0.7 and/or decomposition theory (see the discussion of §3.3), we see that $I' \leq \mathbf{I}^{\mathrm{CL}}(D')$, as required.

To 4. The proof of this is almost identical to the proof of Theorem 8.2.4 using the results of Chapter 9 instead of the results of Chapter 8 along with the discussion about decomposition theory in §3.3 (see in particular the remarks at the beginning of the proof); in particular, here we use Theorem 9.0.7 instead of Theorem 6.1.1, Theorem 9.0.8 instead of Theorem 7.0.11, and Theorem 9.0.9 instead of Theorem 7.0.12. □

Chapter 15

Structure of Pro-ℓ Galois Groups

In this chapter we provide a surprising corollary to the theory developed in this thesis. Namely, we give may examples of fields K whose characteristic is zero which contain $\mu_{2\ell}$ so that the maximal pro-ℓ Galois group $\mathcal{G}_K$ is not isomorphic (as an abstract pro-ℓ group) to $\mathcal{G}_F$ for any field F of positive characteristic which contains $\mu_{2\ell}$. By Theorem 14.0.11, we know that for $v \in \mathcal{V}_{K,1}$, $\operatorname{Char} k(v) \neq \ell$ if and only if there exists $I' \leq \mathbf{I}^{\mathrm{CL}}(D') \leq D' \leq \mathcal{G}_L^{c,N}$ (where $L := L_{D_v^n}$) so that $(D'_K)_n = D_v^n$ and $(I'_K)_n = I_v^n$; this is a purely group-theoretical condition which can be tested using a canonical quotient of $\mathcal{G}_K$, which we denote by $\mathcal{G}_K^{M,n}$ (which we introduce below).

Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. As in the introduction, we denote by $\mathcal{G}_K^{M,n}$ the smallest quotient of $\mathcal{G}_K$ for which $\mathcal{G}_L^{c,N}$ is a subquotient for all $K \subset L \subset K^{a,n}$. In other words, denote by $L^{c,N}$ the extension of L such that $\operatorname{Gal}(L^{c,N}|L) = \mathcal{G}_L^{c,N}$; take $K^{M,n}$ to be the compositum of the fields $L^{c,N}$ as L varies

over all fields such that $K \subset L \subset K^{a,n}$ then $\mathcal{G}_K^{M,n} = \mathrm{Gal}(K^{M,n}|K)$. In particular, $\mathcal{G}_K^{M,n}$ is a characteristic quotient of $\mathcal{G}_K$ and the assignment $\mathcal{G}_K \mapsto \mathcal{G}_K^{M,n}$ is functorial.

Corollary 15.0.12. *Let $n \in \overline{\mathbb{N}}$ be given and denote by $N = \mathbf{N}(\mathbf{M}_2(\mathbf{M}_1(n)))$. Let K be a field such that $\mathrm{Char}\, K = 0$ and $\mu_{2\ell^N} \subset K$. Assume that there exists a field F such that $\ell \neq \mathrm{Char}\, F > 0$, $\mu_{2\ell^N} \subset F$ and $\mathcal{G}_K^{M,n} \cong \mathcal{G}_F^{M,n}$. Then for all $v \in \mathcal{V}_{K,n}$, one has $\mathrm{Char}\, k(v) \neq \ell$.*

Proof. Observe that for any valuation v of F, $\mathrm{Char}\, F = \mathrm{Char}\, k(v)$. This therefore follows from Theorem 1.4.2 part 3. □

We recall that k is strongly ℓ-closed provided that for all finite extensions $k'|k$ one has $(k')^\times = (k')^{\times \ell}$. For instance, any perfect field of characteristic ℓ is strongly ℓ-closed, and all algebraically closed fields are strongly ℓ-closed.

Corollary 15.0.13. *Suppose that K is one of the following:*

- *A function field over a number field k such that $\mu_{2\ell} \subset k$, and $\dim(K|k) \geq 1$.*
- *A function field over a strongly ℓ-closed field k of characteristic 0 such that $\dim(K|k) \geq 2$.*

Then there does not exist a field F such that $\mu_{2\ell} \subset F$, $\mathrm{Char}\, F > 0$ and $\mathcal{G}_K^{M,1} \cong \mathcal{G}_F^{M,1}$. In particular, for all fields F such that $\mu_{2\ell} \subset F$ and $\mathrm{Char}\, F > 0$, one has $\mathcal{G}_K \ncong \mathcal{G}_F$ as abstract pro-ℓ groups.

Proof. Using Corollary 15.0.12, it suffices to find a valuation $v \in \mathcal{V}_{K,1}$ such that $\mathrm{Char}\, k(v) = \ell$. Furthermore, using the argument of Example 8.1.2, it suffices to find

a valuation v of K such that Γ_v contains no non-trivial ℓ-divisible convex subgroups, and $k(v)$ is a function field over perfect field of characteristic ℓ. In both cases, if $\dim(K|k) \geq 2$, there exists such a valuation, taking, for example, v a quasi-prime divisor prolonging the ℓ-adic valuation of $\mathbb{Q} \subset k$; see e.g. the Appendix of [Pop06b] and in particular Facts 5.4-5.6 and Remark 5.7 of loc.cit. Alternatively, see our summary in Chapter 5. Namely, in the notation of Chapter 5, take v_0 to be any valuation of k whose residue characteristic is ℓ, and take r satisfying $0 < r < d$; then the corresponding valuation v of K will work.

On the other hand, if $\dim(K|k) = 1$ in the first case, we can choose a model for K, $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_\ell$, where $\mathcal{O}_\ell$ denotes some prolongation of the ℓ-adic valuation to k; then take v the valuation associated to some prime divisor in the special fiber of $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_\ell$. In the notation of Chapter 5, we take v_0 to be an ℓ-adic valuation of k, and $r = 0$; then the corresponding valuation v of K will work. $\square$

Bibliography

[AEJ87] J. Arason, R. Elman, and B. Jacob. Rigid elements, valuations, and realization of Witt rings. *J. Algebra*, 110(2):449–467, 1987.

[Bog91] F. A. Bogomolov. On two conjectures in birational algebraic geometry. In *Algebraic geometry and analytic geometry (Tokyo, 1990)*, ICM-90 Satell. Conf. Proc., pages 26–52. Springer, Tokyo, 1991.

[BT02] F. A. Bogomolov and Y. Tschinkel. Commuting elements of Galois groups of function fields. In *Motives, polylogarithms and Hodge theory, Part I (Irvine, CA, 1998)*, volume 3 of *Int. Press Lect. Ser.*, pages 75–120. Int. Press, Somerville, MA, 2002.

[BT08] F. A. Bogomolov and Y. Tschinkel. Reconstruction of function fields. *Geom. Funct. Anal.*, 18(2):400–462, 2008.

[Efr95] I. Efrat. Abelian subgroups of pro-2 Galois groups. *Proc. Amer. Math. Soc.*, 123(4):1031–1035, 1995.

[Efr99] I. Efrat. Construction of valuations from K-theory. *Math. Res. Lett.*, 6(3-4):335–343, 1999.

[Efr06a] I. Efrat. Quotients of Milnor K-rings, orderings, and valuations. *Pacific J. Math.*, 226(2):259–275, 2006.

[Efr06b] I. Efrat. *Valuations, orderings, and Milnor K-theory*, volume 124 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2006.

[Efr07] I. Efrat. Compatible valuations and generalized Milnor K-theory. *Trans. Amer. Math. Soc.*, 359(10):4695–4709 (electronic), 2007.

[EK98] A. J. Engler and J. Koenigsmann. Abelian subgroups of pro-p Galois groups. *Trans. Amer. Math. Soc.*, 350(6):2473–2485, 1998.

[EM11a] I. Efrat and J. Mináč. On the descending central sequence of aboslute Galois groups. *American Journal of Mathematics*, 133(6):1503–1532, 2011.

[EM11b] I. Efrat and J. Mináč. Small Galois groups that encode valuations. *Acta Arithmetica (to appear)*, May 2011.

[EN94] A. J. Engler and J. B. Nogueira. Maximal abelian normal subgroups of Galois pro-2-groups. *J. Algebra*, 166(3):481–505, 1994.

[EP05] A. J. Engler and A. Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[Gro97] A. Grothendieck. Brief an G. Faltings. In *Geometric Galois actions, 1*, volume 242 of *London Math. Soc. Lecture Note Ser.*, pages 49–58. Cambridge Univ. Press, Cambridge, 1997.

[GS06] P. Gille and T. Szamuely. *Central simple algebras and Galois cohomology*, volume 101 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[Koe95] J. Koenigsmann. From p-rigid elements to valuations (with a Galois-characterization of p-adic fields). *J. Reine Angew. Math.*, 465:165–182, 1995. With an appendix by Florian Pop.

[Koe98] J. Koenigsmann. Pro-p Galois groups of rank ≤ 4. *Manuscripta Math.*, 95(2):251–271, 1998.

[Koe03] J. Koenigsmann. Encoding valuations in absolute Galois groups. In *Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999)*, volume 33 of *Fields Inst. Commun.*, pages 107–132. Amer. Math. Soc., Providence, RI, 2003.

[MMS04] L. Mahé, J. Mináč, and T. L. Smith. Additive structure of multiplicative subgroups of fields and Galois theory. *Doc. Math.*, 9:301–355, 2004.

[Neu69a] J. Neukirch. Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen. *J. Reine Angew. Math.*, 238:135–147, 1969.

[Neu69b] J. Neukirch. Kennzeichnung der p-adischen und der endlichen algebraischen Zahlkörper. *Invent. Math.*, 6:296–314, 1969.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, second edition, 2008.

[Pop94] F. Pop. On Grothendieck's conjecture of birational anabelian geometry. *Ann. of Math. (2)*, 139(1):145–182, 1994.

[Pop00] F. Pop. Alterations and birational anabelian geometry. In *Resolution of singularities (Obergurgl, 1997)*, volume 181 of *Progr. Math.*, pages 519–532. Birkhäuser, Basel, 2000.

[Pop06a] F. Pop. Almost commuting elements in small Galois groups, 2006. In Oberwolfach Report 25/2006, Mathematisches Forschungsinstitut Oberwolfach, Pro-p Extensions of Global Fields and pro-p Groups, May 21-27 2006, pg. 1495-1496.

[Pop06b] F. Pop. Galois theory of Zariski prime divisors. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Sémin. Congr.*, pages 293–312. Soc. Math. France, Paris, 2006.

[Pop10a] F. Pop. On the birational p-adic section conjecture. *Compos. Math.*, 146(3):621–637, 2010.

[Pop10b] F. Pop. Pro-ℓ abelian-by-central Galois theory of prime divisors. *Israel J. Math.*, 180:43–68, 2010.

[Pop11] F. Pop. $\mathbb{Z}/\ell$ abelian-by-central Galois theory of prime divisors. In *The Arithmetic of Fundamental Groups: PIA 2010*, pages 225–244. Springer-Verlag, 2011.

[Pop12] F. Pop. On the birational anabelian program initiated by Bogomolov I. *Invent. Math.*, 187(3):511–533, 2012.

[Sza04] T. Szamuely. Groupes de Galois de corps de type fini (d'après Pop). *Astérisque*, (294):ix, 403–431, 2004.

[Top12] A. Topaz. Commuting-liftable subgroups of Galois groups II. *Preprint*, 2012.

[Uch76] K. Uchida. Isomorphisms of Galois groups. *J. Math. Soc. Japan*, 28(4):617–620, 1976.

[War81] R. Ware. Valuation rings and rigid elements in fields. *Canad. J. Math.*, 33(6):1338–1355, 1981.

[ZS75] O. Zariski and P. Samuel. *Commutative algebra. Vol. II*. Springer-Verlag, New York, 1975. Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.