Coding Complete Theories in Galois Groups

William James Andrew Gray

Doctor of Philosophy
University of Edinburgh
2003

Abstract

James Ax showed that, in each characteristic, there is a natural bijection from the space of complete theories of pseudo-finite fields, in first order logic, to the set of conjugacy classes of procyclic subgroups of the absolute Galois group of the prime field. I show that when the set of subgroups of a profinite group is considered to have the Vietoris (a.k.a. hyperspace, finite, exponential, neighbourhood) topology the aforementioned bijection is a homeomorphism. Thus we can think of the space of complete theories of pseudo-finite fields of a given characteristic as being encoded in the absolute Galois group of the prime field.

I go on to show that there is a natural way of encoding the whole space of complete theories of pseudo-finite fields (i.e. without dependence on characteristic) in the absolute Galois group of the rationals. To do this I use: the theory of the algebraic p-adics; the relationship between the absolute Galois group of the p-adics and the absolute Galois group of the field with p elements; the structure of the absolute Galois group of the p-adics given by Iwasawa; Krasner's lemma for henselian fields; and the Vietoris topology.

At the same time, we consider the theory of algebraically closed fields with a generic automorphism (*ACFA*). By taking the theory of the fixed field, there is a surjective (but not injective) map from the space of complete theories of *ACFA* to the space of complete theories of pseudo-finite fields. For the space of complete theories of *ACFA*, there is also a bijective Galois correspondence, in each characteristic, given by restricting the automorphism to the algebraic closure of the prime field. I show that this correspondence is a homeomorphism and that there is an analogous way of encoding the whole space in the absolute Galois group of the rationals.

Acknowledgements

My greatest thanks are to my supervisor Angus Macintyre for being an excellent mentor. After each of our meetings I felt uplifted and inspired. Thanks to my second supervisor Antony Maciocia who has been supportive in many matters and cultivated my interests in logic as an undergraduate. The EPSRC studentship has given me the financial support that I needed and for this I would like to express my gratitude.

There are many members of the model theory community who have helped me over the past four years. I am grateful to them all and especially to my contemporaries with whom I have shared ideas and many a good night out.

Thanks to my office mates who have helped so frequently with problems big and small, and in particular to Laura for reading a draft of this thesis and giving comments on style and clarity.

Finally special thanks to my family and Maria for constant support and companionship.

Declaration

I declare that this thesis was composed by myself and that the work contained therein is my own, except where explicitly stated otherwise in the text.

(*William James Andrew Gray*)

Table of Contents

Introduction

In this thesis, I will give a new characterisation of the complete theories of pseudo-finite fields and of algebraically closed fields with a generic automorphism. I give detailed definitions of pseudo-finite fields and of algebraically closed fields with a generic automorphism in Chapter 1. There we see that, from Ax's work on pseudo-finite fields, there is, in each characteristic, a natural bijection from the complete theories of pseudo-finite fields to conjugacy classes of subgroups of the absolute Galois group of the prime field. We exhibit a similar bijection for algebraically closed fields with an automorphism and show that the two bijections are related.

The Vietoris topology has a long history dating back to the early days of general topology. As we shall see in Chapter 2, it is a topology on the set of closed subsets of a topological space such that (provided the space is T_1) the set of singletons is a homeomorphic copy of the space. Moreover it is closely related to the Hausdorff metric (which is a metric on the closed subsets of a metric space).

The absolute Galois group of a field carries the usual profinite topology. In Chapter 3, we consider the conjugacy classes of subgroups as a subspace of the double Vietoris space of the absolute Galois group of a field. This allows us to show that both the bijections of Chapter 1 are homeomorphisms and hence that the full structure of the space of complete theories is captured in our characterisation.

The bijections of Chapter 1 depend on the characteristic but, in Chapter 4, we will see that we may remove this dependence. For this, we give a new bijection of the space of complete theories of pseudo-finite fields in all characteristics with conjugacy classes of subgroups of the absolute Galois group of the rationals. This space is again given the Vietoris topology and the bijection is shown to be a homeomorphism. We finish the chapter by showing that similar results hold for algebraically closed fields with a generic automorphism.

Finally, in Chapter 5, we discuss the possibilities of extending the results to type spaces.

Chapter 1

Pseudo-finite Fields, *ACFA* and Procyclic Groups

In this chapter, I will introduce the protagonists of this thesis. These are pseudo-finite fields, algebraically closed fields with an automorphism and procyclic groups. In each case I will give background and results, which will be of relevance in later chapters.

1.1 Some notions from model theory

The purpose of this section is to introduce some of the concepts from model theory that will be fundamental later on. It is not meant to contain all the definitions from model theory that I will use. In particular, I will not define what it means for a structure (e.g. a group, a field) to satisfy a formula; I will just say that this is the formal definition of a formula being true in that structure and rely on the reader's intuition or knowledge of what that means. For the fine detail of the subject, I refer the reader to [CK], [Ho] or any of the other excellent model theory texts.

We will mainly be working in two first order logical languages: the language of fields and the language of fields with an automorphism. The *language of fields* $\mathcal{L}$ is the normal language of first order logic with equality and the symbols $\{+, -, \cdot, 0, 1\}$. The *language of fields with an automorphism* $\mathcal{L}_\sigma$ is $\mathcal{L}$ with a symbol σ for the automorphism. Thus the structures we will be considering in the language $\mathcal{L}$ are fields, and in $\mathcal{L}_\sigma$ fields with a specified automorphism.

A *theory* in a language is any consistent set of sentences (i.e. formulas without free variables). A structure $\mathcal{M}$ is a *model* of the theory T, written $\mathcal{M} \models T$, if $\mathcal{M}$ satisfies T (i.e. all the sentences of T are true in $\mathcal{M}$). A theory is *complete* if for every sentence φ, either $\varphi \in T$ or $\neg\varphi \in T$. Note, therefore, that each structure

$\mathcal{M}$ has a complete theory $Th(\mathcal{M})$ associated to it, namely all the sentences which are satisfied by $\mathcal{M}$. If for structures $\mathcal{M}$ and $\mathcal{N}$ we have that $Th(\mathcal{M}) = Th(\mathcal{N})$ then we say that $\mathcal{M}$ and $\mathcal{N}$ are *elementarily equivalent*, written

$$\mathcal{M} \equiv \mathcal{N}.$$

This is a weaker condition than isomorphism; for instance, it is easy to see that in $\mathcal{L}$ all algebraically closed fields of a given characteristic are elementarily equivalent, yet, for example, $\mathbb{Q}^{\text{alg}} \ncong \mathbb{C}$ because they are of a different cardinality. Nevertheless, the fact that it is weaker condition can be useful when classification up to isomorphism is inappropriate (for example see [P]).

We will now see that it is possible to isolate, in a first order way, the characteristic of the fields for a given theory. For all primes p, if T is a theory in $\mathcal{L}$ or $\mathcal{L}_\sigma$, then the models of

$$T \cup \{\underbrace{1 + \cdots + 1}_{p \text{ times}} = 0\}$$

are exactly the characteristic p models of T. Furthermore, the models of

$$T \cup \{\underbrace{1 + \cdots + 1}_{p \text{ times}} \neq 0 : p \text{ prime}\}$$

are exactly the characteristic 0 models of T. Thus it is possible to refer to the theory of T of characteristic p or of characteristic 0.

For a theory T, a complete theory R such that $T \subset R$ is called a *completion* of T. The set of all completions of T, written $S_0(T)$, has a natural topology on it making it into a Stone space, see [Jo, p69]. Indeed, it is often referred to as the *Stone space* of T. The basic clopen sets of the topology are given by

$$X_\varphi = \{S \in S_0(T) : \varphi \in S\}$$

where φ is a sentence. In Chapters 3 and 4, I will give a new characterisation of these spaces for the theories called *Psf* and *ACFA* which I will now explain.

1.2 Pseudo-finite fields

It is well known (and elementary to prove from the compactness theorem) that there are no theories which have models of unbounded finite cardinality but only have finite models. Thus for the theory of finite fields (i.e. the collection of sentences true in all finite fields) there are infinite models. These are called *pseudo-finite fields*. The following example of a pseudo-finite field involves the theory of ultraproducts. These are defined in nearly all model theory texts (for example see [Ho] or [CK]). Later on, I will give an example of a pseudo-finite field which does not involve ultraproducts.

Example 1.1. Let Q be the set of prime powers and let $\mathcal{U}$ be a non-principal ultrafilter on Q. Then the ultraproduct

$$\prod \mathbb{F}_q/\mathcal{U}$$

is a pseudo-finite field (of characteristic 0).

Pseudo-finite fields were first introduced by Ax in his studies of the applications of logic to Diophantine problems [A1]. He went on to study them in their own right [A2] to show, amongst other things, that the theory is decidable. I will summarise the parts of Ax's paper that we will need. My exposition is derived from Chatzidakis's excellent survey article [C2], as well as Ax's original paper.

Ax shows that the following properties of a field are expressible in $\mathcal{L}$:

- perfect
- there is a unique extension of each degree
- PAC

where PAC stands for *pseudo algebraically closed* and means that every absolutely irreducible variety over the field has a rational point. We will call the theory given by the sentences expressing the above properties *Psf*, and we will see at the end of this section that the pseudo-finite fields are axiomatised by *Psf*.

Note that each finite field satisfies the first two properties above but no finite field satisfies the third. Even so, as a consequence of the following theorem of Lang and Weil [LW], we will see that each pseudo-finite field is a model of *Psf*.

Theorem 1.2. *Let V be an absolutely irreducible variety and let V be defined over $\mathbb{F}_q$ by r polynomials in n variables each of total degree at most e. Then, there is a constant C, depending only on e, n and r, such that if V is of dimension d, we have*

$$|card(V(\mathbb{F}_q)) - q^d| \leq Cq^{d-(1/2)}$$

where $V(\mathbb{F}_q)$ is the set of $\mathbb{F}_q$ rational points of V.

Consider a variety V as in the theorem above and note that we may consider V as a variety defined over $\mathbb{F}_s$ for any $\mathbb{F}_s \supset \mathbb{F}_q$. Suppose that $\mathrm{card}(V(\mathbb{F}_s)) = 0$ for all such fields $\mathbb{F}_s$. Then, by the theorem above, we get

$$s^d \leq Cs^{d-(1/2)}$$

which for large enough s cannot be true (because C depends only on V).

The following formulas of $\mathcal{L}$ are well known:

$\theta_{\geq n} \equiv \exists x_1, \ldots, x_n \bigwedge_{i \neq j} x_i \neq x_j$ the sentence expressing that there are n distinct elements.

$\psi_{f_1,\ldots,f_m}(\overline{y})$ the formula expressing that the polynomials $f_1, \ldots, f_m$ (whose coefficients are given by the tuple $\overline{y}$) define an absolutely irreducible variety (see [C1]).

$\varphi_{f_1,\ldots,f_m}(\overline{x}, \overline{y}) \equiv f_1(\overline{x}) = 0 \wedge \cdots \wedge f_m(\overline{x}) = 0$ the formula expressing that $\overline{x}$ is a rational point of the variety defined by $f_1, \ldots, f_m$.

By the argument in the preceding paragraph, we know that there is an N such that the sentence

$$\theta_{\geq N} \longrightarrow \forall \overline{y}\, [\psi_{f_1,\ldots,f_m}(\overline{y}) \rightarrow \exists \overline{x}\, \varphi_{f_1,\ldots,f_m}(\overline{x}, \overline{y})]$$

is a member of the theory of finite fields. Therefore the pseudo-finite fields are PAC and hence each pseudo-finite field is a model of *Psf*.

To give another example of a model of *Psf*, I will introduce the *supernatural numbers.*

Definition 1.3. Let p_i be the i-th prime number. The *supernatural numbers* are formal products of the form

$$\prod_i p_i^{r_i}$$

where the $r_i \in \mathbb{N} \cup \{0, \infty\}$.

Example 1.4. To each algebraic extension F of $\mathbb{F}_p$ we associate a supernatural number $s = \prod p_i^{r_i}$ where

$$r_i = \sup\{n : \mathbb{F}_{p^{p_i^n}} \subset F\}.$$

It is easily seen that this yields a bijective correspondence between the algebraic extensions of $\mathbb{F}_p$ and the supernatural numbers. By an abuse of notation, we can thus write the algebraic extensions of $\mathbb{F}_p$ as $\mathbb{F}_{p^s}$ for each supernatural number s. I now claim that the field $\mathbb{F}_{p^s} \models Psf$ if

$r_i < \infty$ for all i

and $r_i > 0$ for infinitely many i.

Proof of claim. The field is perfect because it is an algebraic extension of $\mathbb{F}_p$, and by the first condition above it has a unique extension of each degree. Thus we only need to show that it is PAC.

By the second condition $\mathbb{F}_{p^s}$ is an infinite extension of $\mathbb{F}_p$ and hence is infinite. Therefore by Theorem 1.2, each absolutely irreducible variety defined over $\mathbb{F}_{p^s}$ has a rational point in a subfield of $\mathbb{F}_{p^s}$ and hence $\mathbb{F}_{p^s}$ is PAC. □

Ax states the following lemma in [A2]. For a proof, see [A1] and [Po]. For a field extension F/E we will write $Sol_E(F)$ for the set of polynomials in one variable over E that have a root in F.

Lemma 1.5. *If F, F' are algebraic extensions of a field E, then*

$$Sol_E(F) = Sol_E(F') \iff F \cong_E F'.$$

For a field F let $Abs(F)$ be the absolute numbers of F i.e. the elements of F that are algebraic over the prime field. Ax shows that elementary equivalence of two models of Psf is determined by the absolute numbers.

Theorem 1.6 ([A2] Theorem 4, p255). *Let $F, F' \models Psf$. Then*

$$F \equiv F' \iff Abs(F) \cong Abs(F').$$

Proof. ($\Rightarrow$) Follows from Lemma 1.5. ($\Leftarrow$) see [A2]. □

Corollary 1.7. *Let $F, F' \models Psf$ and suppose that F and F' are of the same characteristic. Then*

$$F \equiv F' \iff Sol_P(Abs(F)) = Sol_P(Abs(F'))$$

where P is the prime field.

Proof. Lemma 1.5 and Theorem 1.6. □

From the corollary above we can see that the complete theories of Psf are determined by sentences of the form

$$\exists x \ f(x) = 0$$

where f is a polynomial over the integers. This was subsequently taken further by Ax's student Kiefe [Ki]. She extended the language $\mathcal{L}$ by an n-ary relation symbol S_n, called a solvability predicate, for each positive integer n. In the new language $\mathcal{L}_S$ the theory *Psf* is extended by taking

$$Psf \cup \{\forall y_0, \dots, y_n (S_n(y_0, \dots, y_n) \leftrightarrow \exists x (y_0 x^n + y_1 x^{n-1} + \dots + y_n = 0)) \mid n \in \mathbb{Z}_{>0}\}.$$

Then by an application of Shoenfield's Theorem [Sh] she proves that the new language has elimination of quantifiers [H, p66].

Returning to Ax's work, we can ask which fields of absolute numbers can be the absolute numbers of a model of *Psf*. He gives us these theorems.

Theorem 1.8 ([A2] Theorem 7, p262). *A field K of absolute numbers is isomorphic to $Abs(\mathcal{K})$ for some non-principal ultraproduct $\mathcal{K}$ of finite fields if, and only if, K has at most one extension of each degree. If $char K = 0$ we may take $\mathcal{K}$ to be a non-principal ultraproduct of the finite prime fields. If $char K = p$ we may take $\mathcal{K}$ to be a non-principal ultraproduct of the characteristic p finite fields.*

Theorem 1.9 ([A2] Theorem 8, p262). *A field F is pseudo-finite if, and only if, $F \equiv \mathcal{K}$ for some non-principal ultraproduct $\mathcal{K}$ of the finite fields.*

Corollary 1.10 ([A2] Theorem 9, p262). $F \models Psf \iff F$ *is pseudo-finite.*

Proof. ($\Leftarrow$) By Theorem 1.2. ($\Rightarrow$) By Theorem 1.9 and Example 1.1. □

Thus in characteristic 0, if a field of absolute numbers has at most one extension of each degree then it is isomorphic to the absolute numbers of some pseudo-finite field. In characteristic p, every field of absolute numbers is isomorphic to the absolute numbers of some pseudo-finite field. Note, however, that by Example 1.4 only certain fields of absolute numbers are themselves pseudo-finite.

1.3 *ACFA*

Recall that if we take a non-principal ultraproduct of finite fields then the resulting field is pseudo-finite. Inspired by this, Macintyre considered taking a non-principal ultraproduct of the fields $\mathbb{F}_p^{\mathrm{alg}}$ with the automorphism $x \mapsto x^{p^m}$. More precisely, in $\mathcal{L}_\sigma$ we take the ultraproduct

$$(\widetilde{F}, \tilde{\sigma}) = \prod (F, \sigma)/\mathcal{U}$$

where $F = \mathbb{F}_p^{\mathrm{alg}}$ and σ is a power of the Frobenius automorphism. As an immediate consequence of the construction, we get that the field $\widetilde{F}$ is algebraically closed and that the fixed field of $\tilde{\sigma}$ is pseudo-finite.

This idea led to the study in model theory of fields with an automorphism. Outside model theory these had already been studied and had been christened *difference fields* because of a link with difference equations (see [Co]). In [M], Macintyre gives an account of difference fields similar in spirit to Ax's work on pseudo-finite fields. Chatzidakis, Hrushovski and Peterzil [CH],[CHP] have taken Macintyre's results a lot further to give stability theoretic results and results of the type of Zil'ber trichotomy [HZ]. There are good notes written on the subject by Marker [Mar] and Chatzidakis [C3]. I will give a summary of the material relevant to this thesis, drawing mainly on Macintyre's account [M].

We will be considering only the *existentially closed* (e.c.) difference fields. These are defined as being the difference fields (F, σ) such that if a finite system of polynomials in

$$\ldots, \sigma^{-2}(\overline{x}), \sigma^{-1}(\overline{x}), \overline{x}, \sigma(\overline{x}), \sigma^2(\overline{x}), \ldots$$

where $\overline{x}$ is the tuple $x_1, \ldots, x_n$ and $\sigma(\overline{x})$ is the tuple $\sigma(x_1), \ldots \sigma(x_n)$, has a solution in an extension (F', σ') of (F, σ) then it has a solution in (F, σ). (This is equivalent to the standard notion of e.c. structures from model theory because, for example, the solvability of $f(x) \neq 0$ is equivalent to the solvability of $\exists y \; yf(x) = 1$.)

Lemma 1.11. *Any difference field extends to an existentially closed difference field.*

Proof. This can be proved on the grounds of general theory, see [Si], or as a consequence of the axiomatisation given below, see [CH]. □

Macintyre shows that the e.c. difference fields are (first order) axiomatised by the sentences saying that the field is algebraically closed and by the conjunction of axioms called Axiom H (H for Hrushovski).

Axiom H. Let V be a closed subvariety of $\mathbb{A}^n(F)$ and let $\sigma(V)$ be its conjugate variety, which is also a closed subvariety of $\mathbb{A}^n(F)$. Thus $V \times \sigma(V)$ is a closed subvariety of $\mathbb{A}^{2n}(F)$. Then for every closed subvariety W of $V \times \sigma(V)$, such that a generic point of W projects to a generic point of V and $\sigma(V)$ under the natural projection maps (see diagram below), there exist $x_1, \ldots, x_n \in F$ such that $(x_1, \ldots, x_n, \sigma(x_1), \ldots, \sigma(x_n)) \in W$.

$$\begin{tikzcd}
 & & V \\
W \arrow[r] & V \times \sigma(V) \arrow[ur, "\pi_1"] \arrow[dr, "\pi_2"'] & \\
 & & \sigma(V)
\end{tikzcd}$$

The theory given by the axioms above is called *ACFA*. It is unclear from the literature where the term *ACFA* first arose, but it appears to stand for "algebraically closed fields with a generic automorphism" [Mar]. (Here generic is a synonym for e.c.)

Our main concern later will be the completions of *ACFA*. The following theorem shows that the completions are determined by the characteristic and the action of the automorphism on the algebraic closure of the prime field.

Theorem 1.12. *Let (F_1, σ_1) and (F_2, σ_2) be models of ACFA of the same characteristic and let $P \subset F_1, F_2$ be the prime field. Then*

$$(P^{\mathrm{alg}}, \sigma_1|_{P^{\mathrm{alg}}}) \cong (P^{\mathrm{alg}}, \sigma_2|_{P^{\mathrm{alg}}}) \iff (F_1, \sigma_1) \equiv (F_2, \sigma_2).$$

Proof. Suppose that $(P^{\mathrm{alg}}, \sigma_1|_{P^{\mathrm{alg}}}) \cong (P^{\mathrm{alg}}, \sigma_2|_{P^{\mathrm{alg}}})$. Then by picking a different embedding of P^{alg} in F_2, if necessary, we may assume $\sigma_1|_{P^{\mathrm{alg}}} = \sigma_2|_{P^{\mathrm{alg}}}$. Then F_1/P^{alg} and F_2/P^{alg} are regular extensions [FJ, p111]. Hence $F_1 \otimes_{P^{\mathrm{alg}}} F_2$ is a domain [J, p203] and there is a map $\sigma_1 \otimes \sigma_2$ extending σ_1 and σ_2 to this domain. Thus let (F_3, σ_3) be the field of fractions of $F_1 \otimes_{P^{\mathrm{alg}}} F_2$ with the induced extended automorphism. By Lemma 1.11 we get an extension (F_4, σ_4) of (F_3, σ_3) such that $(F_4, \sigma_4) \models ACFA$. Thus we have the following picture.

$$\begin{tikzcd}
 & (F_4, \sigma_4) & \\
 & (F_3, \sigma_3) \arrow[u, dash] & \\
(F_1, \sigma_1) \arrow[ur, dash] & & (F_2, \sigma_2) \arrow[ul, dash] \\
 & (P, \sigma) \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}$$

Any theory whose models are all e.c. is model complete [Ho, Theorem 8.3.1]. Thus *ACFA* is model complete and hence

$$(F_1, \sigma_1) \equiv (F_4, \sigma_4) \equiv (F_2, \sigma_2).$$

Conversely, suppose that $(F_1, \sigma_1) \equiv (F_2, \sigma_2)$. Let E be an arbitrary Galois extension of P with primitive element a. Let $f(x)$ be the minimum polynomial of a over P. Also since E is a normal extension, E is fixed setwise by σ_1. In particular $\sigma_1(a) \in E$, and hence $\sigma_1(a) = g(a)$ for some polynomial g over P. Now consider the sentence

$$\exists x\, [f(x) = 0 \wedge \sigma(x) = g(x)].$$

Since (F_1, σ_1) and (F_2, σ_2) agree on this sentence, there is an isomorphism τ of $(E, \sigma_1|_E)$ and $(E, \sigma_2|_E)$. Note that τ is a member of $\mathcal{G}(E/P)$ and that if $\delta \in \mathcal{G}(E/P)$ commutes with $\sigma_1|_E$, then $\tau\delta$ is also an isomorphism of $(E, \sigma_1|_E)$ and $(E, \sigma_2|_E)$.

Let I be an index set and let $\{E_i : i \in I\}$ be the set of all Galois extensions of the prime field. Now order the index set by inclusion, i.e. $E_i \subset E_j$ implies $i \leq j$. As we saw above, for each i there is a finite set H_i of isomorphisms of $(E_i, \sigma_1|_{E_i})$ and $(E_i, \sigma_2|_{E_i})$. Furthermore, for each $\tau \in H_i$ and $j \leq i$, we have $\tau|_{H_j} \in H_j$. Therefore the set $\{H_i : i \in I\}$, together with restriction maps form an inverse system. Since we know each H_i is non-empty and finite, $\varprojlim H_i$ is non-empty, by [W, Proposition 1.1.5], and we are done. □

The proof of the converse above can be done in one line by using a standard result on elementary equivalence, isomorphism and ultrapowers [CK, Corollary 6.1.2]. The reason I have chosen to give the proof without using this result is that it is suggestive of the quantifier elimination in *Psf* by solvability predicates. Indeed, Macintyre proves the analogous result, which I shall outline here.

For each $n \in \mathbb{N}$ extend the language $\mathcal{L}$ by n-ary relation symbols $S_{f,\overline{g},\overline{h}}$ where:

- $\overline{g}$ and $\overline{h}$ are the tuples of polynomials $g_1, \ldots, g_m$ and $h_1, \ldots, h_m$
- f and g_i and h_i, for $i \leq m$, are members of

$$\mathbb{Z}[\overline{x}_0, \overline{x}_1, \overline{y}_1, \overline{x}_2, \overline{y}_2, \ldots, \overline{x}_k, \overline{y}_k, t].$$

Now define $ACFA_S$ to be $ACFA$ together with the following axioms

$$\begin{aligned}\forall \overline{v}\ S_{f,\overline{g},\overline{h}}(\overline{v}) \longleftrightarrow \exists t \Big[& f(\overline{v}, \ldots, \sigma^{-k}(\overline{v}), t) = 0 \wedge \\ & \bigwedge_{i=1}^{m} \sigma(g_i(\overline{v}, \ldots, \sigma^{-k}(\overline{v}), t)) = h_i(\overline{v}, \ldots, \sigma^{-k}(\overline{v}), t)\Big]\end{aligned}$$

where $\overline{v}, \ldots, \sigma^{-k}(\overline{v})$ is an abbreviation of

$$\begin{aligned}& v_1, \ldots, v_n, \sigma(v_1), \ldots, \sigma(v_n), \sigma^{-1}(v_1), \ldots, \sigma^{-1}(v_n), \sigma^2(v_1), \ldots, \sigma^2(v_n), \\ & \quad \sigma^{-2}(v_1), \ldots, \sigma^{-2}(v_n), \ldots, \ldots, \sigma^k(v_1), \ldots, \sigma^k(v_n), \sigma^{-k}(v_1), \ldots, \sigma^{-k}(v_n).\end{aligned}$$

Theorem 1.13 ([M], p177). *$ACFA_S$ has quantifier elimination.*

Macintyre also proves decidability results similar to those of Ax.

1.4 Procyclic groups

Recall that a *profinite group* is an inverse limit of a system of finite groups and a *procyclic group* is an inverse limit of a system of cyclic groups. Here we will present several characterisations of procyclic groups, all of which are standard, but scattered throughout the literature. We then show that the absolute Galois group of a pseudo-finite field is procyclic.

Let G be a profinite group and let X be a subset of G. Then X *generates G topologically* if G is the closure of the abstract group generated by X.

Theorem 1.14. *G is procyclic if, and only if, G is topologically generated by one element.*

Proof. Suppose that $G = \varprojlim H_i$ is procyclic. For each i, let X_i be the set of generators of H_i. It can be seen that the X_i's form an inverse system and, by [W, Proposition 1.1.5], we have $X := \varprojlim X_i$ is non-empty. Then, by [W, Proposition 4.1.1] any element of X generates G.

Conversely, suppose that G is generated by some $\alpha \in G$. Thus the image of α in each H_i generates H_i and so we are done. □

The following example of a procyclic group will be fundamental in the later chapters.

Example 1.15. Consider the inverse system on $\{\mathbb{Z}/n\mathbb{Z} : n \in \mathbb{N}\}$ given by the maps $x + n\mathbb{Z} \mapsto x + m\mathbb{Z}$ if $m|n$. Define $\widehat{\mathbb{Z}}$ to be the inverse limit of this system. Thus $\widehat{\mathbb{Z}}$ is a procyclic group and if we identify $x \in \mathbb{Z}$ with $x+n\mathbb{Z}$ for each n in the inverse limit then we get a natural embedding of $\mathbb{Z}$ in $\widehat{\mathbb{Z}}$. Under this embedding we have that $\widehat{\mathbb{Z}}$ is topologically generated by 1.

Lemma 1.16 ([W], Proposition 1.5.3). *Let G be profinite.*

(i) There is a unique continuous map $\widehat{\mathbb{Z}} \times G \longrightarrow G$ such that $(n, g) \mapsto g^n$ for $n \in \mathbb{Z}$. So if $g \in G$ and $z \in \widehat{\mathbb{Z}}$, then the 'power' g^z is defined.

(ii) If $g \in G$ and $z_1, z_2 \in \widehat{\mathbb{Z}}$ then (i) $g^{z_1+z_2} = g^{z_1}g^{z_2}$ and (ii) $(g^{z_1})^{z_2} = g^{z_1z_2}$.

(iii) If $g_1, g_2 \in G$ and $z \in \widehat{\mathbb{Z}}$, and if g_1, g_2 commute, then $(g_1g_2)^z = g_1^zg_2^z$.

Thus we can use the elements of $\widehat{\mathbb{Z}}$ as powers in a profinite group. By the following lemma, we have the natural extension of the idea of taking powers of a generator in a cyclic group.

Lemma 1.17. *Let G be a procyclic group. Then α generates G topologically if, and only if, $G = \{\alpha^z : z \in \widehat{\mathbb{Z}}\}$.*

Proof. From [W, Proposition 4.1.1], we have that α generates G topologically if, and only if, α generates G/N for all open normal subgroups N of G. Note also that since G is compact we have that $[G : N]$ is finite for all open normal subgroups [W, Lemma 0.3.1(c)].

Suppose that α generates G, and let $g \in G$. Let N be an open normal subgroup of G and let $n = [G : N]$. Since α generates G, we have $gN = \alpha^m N$ for some $m \in \{0, \ldots, n-1\}$. By running N over all the open normal subgroups of G we get an inverse system of $m \in \mathbb{Z}/n\mathbb{Z}$. However, note that in the inverse system we do not necessarily have the groups $\mathbb{Z}/n\mathbb{Z}$ for all $n \in \mathbb{N}$. Nevertheless there is a $z \in \widehat{\mathbb{Z}}$ such that the image of z in $\mathbb{Z}/n\mathbb{Z}$ is m for all $\mathbb{Z}/n\mathbb{Z}$ in our inverse system. Then it can be seen that $\alpha^z = g$.

Conversely, suppose that $G = \{\alpha^z : z \in \widehat{\mathbb{Z}}\}$. As before consider G/N where N is an open normal subgroup of G. Then it can be seen that αN generates G/N. □

Consider now the following well-known theorem from group theory.

Theorem 1.18 ([H], Theorem 12.5.3, p190). *A group of order p^n which contains only one subgroup of order p^m, where $1 < m < n$, is cyclic.*

As a consequence we get the following theorem.

Theorem 1.19. *Let F be a perfect field and let $G(F)$ be its absolute Galois group.*

(i) F has at most one extension of each degree if, and only if, $G(F)$ is procyclic.

(ii) F has exactly one extension of each degree if, and only if, $G(F) \cong \widehat{\mathbb{Z}}$.

Proof. In both (i) and (ii) sufficiency is immediate. Thus we prove necessity in both cases:

(i) Suppose that F has at most one extension of each degree. Let E/F be an extension of degree n and note that the uniqueness implies that E/F is normal. It is now sufficient to show that $G = \mathcal{G}(E/F)$ is cyclic.

If n is a prime power then Theorem 1.18 implies that G is cyclic. Moreover if n is not a prime power, then by the same reasoning we have that the Sylow subgroups of G are cyclic. (Note that our supposition implies that for each prime $p|n$ there is only one Sylow p-subgroup.) Let H and K be distinct Sylow subgroups, and let $h \in H$ and $k \in K$. Then by normality we have $khk^{-1} \in H$ and $hk^{-1}h^{-1} \in K$, and hence $khk^{-1}h^{-1} \in H \cap K = 1$. Thus H and K commute and so G is the direct product of its Sylow subgroups. Therefore G is cyclic.

(ii) By (i), $G(F)$ is procyclic, so let α be a generator. Then the map $z \mapsto \alpha^z$ is the required isomorphism. □

We can see from the axiomatisation of *Psf* that the absolute Galois group of a pseudo-finite field is $\widehat{\mathbb{Z}}$. Furthermore we have the following corollary.

Corollary 1.20. *The absolute Galois group of the absolute numbers of a pseudo-finite field is procyclic.*

Proof. By Theorem 1.19 and Theorems 1.8 and 1.9. □

1.5 *ACFA* and *Psf*

It can be seen from sections 1.2 and 1.3 that there are many similarities between *ACFA* and *Psf*. In this section we will highlight the relationship between the complete theories of *ACFA* and *Psf*. The following theorem, which is attributed to van den Dries, shows that it is the fixed field in *ACFA* that determines this relationship. For a field automorphism σ, we will use $Fix(\sigma)$ to denote the fixed field.

Theorem 1.21 ([M], p169). *If* $(F, \sigma) \models ACFA$ *then* $Fix(\sigma) \models Psf$.

Thus we may define a map from $S_0(ACFA)$ to $S_0(Psf)$ which takes a theory of *ACFA* to the theory of its fixed field. (Recall that $S_0(T)$ for a theory T was defined in Section 1.1.) We will now investigate the properties of this map.

Let X be the basic open subset of $S_0(Psf)$ defined by the sentence φ. By the results of Section 1.2 we have that

$$\varphi \equiv \theta(\exists x\ f_1(x) = 0, \ldots, \exists x\ f_n(x) = 0)$$

where $f_1, \ldots, f_n$ are polynomials over $\mathbb{Z}$ and θ is a boolean polynomial. Thus the inverse image of X is the set determined by

$$\varphi_\sigma \equiv \theta(\exists x[\sigma(x) = x \wedge f_1(x) = 0], \ldots, \exists x[\sigma(x) = x \wedge f_n(x) = 0]).$$

Therefore the map is continuous.

We will now show that the map is surjective. Let $T \in S_0(Psf)$ and let F be a model of T. Thus by Corollary 1.20 we have that $G(Abs(F))$ is procyclic. Let σ_0 be a generator of $G(Abs(F))$. Now we may extend $(Abs(F)^{\mathrm{alg}}, \sigma_0)$ to a model (K, σ) of $ACFA$ by Lemma 1.11. Therefore $Th(K, \sigma)$ gets mapped to T and the map is surjective.

The map, however, is not injective because of the following example of two automorphisms of $\mathbb{Q}^{\mathrm{alg}}$ which generate the same group but are not elementarily equivalent. A simple lemma from group theory is needed first.

Lemma 1.22. *Let $\theta : H \to K$ be a surjective homomorphism of finite cyclic groups and let k be a generator of K. Then there is an $h \in H$ such that $\theta(h) = k$ and h generates H.*

Proof. We know that

$$H \cong C_{p_1^{m_1}} \times \cdots \times C_{p_n^{m_n}}$$

and

$$K \cong C_{p_1^{r_1}} \times \cdots \times C_{p_s^{r_s}}$$

where $p_1, \ldots, p_n$ are distinct primes, $1 \leq r_i \leq m_i$ for each $i = 1, \ldots, s$ and $s \leq n$. Thus θ is defined by its coordinate maps θ_i from $C_{p_i^{m_i}}$ onto $C_{p_i^{r_i}}$ for $i = 1, \ldots, s$. Since the product of generators of the component cyclic groups of H is a generator of H (and similarly for K), we need only check for each generator d_i of $C_{p_i^{r_i}}$ that there is a generator c_i of $C_{p_i^{m_i}}$ such that $\theta_i(c_i) = d_i$. It is, however, easily checked that for all c_i such that $\theta_i(c_i) = d_i$ we have that c_i generates $C_{p_i^{m_i}}$. □

Example 1.23. Let ζ be a primitive fifth root of unity and let F be a characteristic 0 pseudo-finite field such that $[F(\zeta) : F] = 4$. Now let σ_0 and τ_0 be the elements of $\mathcal{G}(F(\zeta)/F)$ defined by

$$\sigma_0 : \zeta \mapsto \zeta^2 \qquad \tau_0 : \zeta \mapsto \zeta^3$$

and notice that each of σ_0 and τ_0 generate $\mathcal{G}(F(\zeta)/F)$.

By the lemma above we can get an inverse system of generators extending σ_0 and extending τ_0. Thus, by taking inverse limits, we can lift σ_0, τ_0 to generators σ, τ (respectively) of $G(F)$.

The example above gives two automorphisms σ, τ on F^{alg} which generate the same procyclic group. Thus if we extend σ, τ to models $(K, \sigma'), (L, \tau')$ of $ACFA$, we will have

$$Abs(Fix(\sigma')) \cong Abs(Fix(\tau'))$$

and hence $Fix(\sigma') \equiv Fix(\tau')$ by Theorem 1.6. The construction, however, is such that

$$(K, \sigma') \models \forall y\, (y^5 = 1 \rightarrow \sigma(y) = y^2)$$
$$(L, \tau') \models \forall y\, (y^5 = 1 \rightarrow \sigma(y) = y^3)$$

and hence $Th(K, \sigma') \neq Th(L, \tau')$. Therefore the map from $S_0(ACFA)$ to $S_0(Psf)$ described above is not injective.

I will finish this section by summarising its results in the theorem below.

Theorem 1.24. *There is a natural continuous, surjective but not bijective map from $S_0(ACFA)$ to $S_0(Psf)$ which takes a theory of ACFA to the theory of its fixed field.*

1.6 Stone spaces and Galois groups

In Section 1.2, we saw that there is a one-one correspondence between $S_0(Psf)$ and the extensions of the prime field that have at most one extension of each degree (Theorems 1.8 and 1.9). By Theorem 1.19, we have that a field has at most one extension of each finite degree if, and only if, its absolute Galois group is procyclic.

Lemma 1.25. *Let C_1, C_2 be closed subgroups of the absolute Galois group of a field F. Then*

$$Fix(C_1) \cong Fix(C_2) \iff C_1 \textit{ is conjugate to } C_2.$$

Proof. Let $\tau : Fix(C_1) \rightarrow Fix(C_2)$ be an isomorphism. Let N be a normal extension of F such that $Fix(C_1)$, and hence $Fix(C_2)$, is a subfield of N. By Galois theory, τ lifts to an automorphism of N and hence to an automorphism $\tilde{\tau}$ of F^{alg}. It is now an easy calculation to show that $\tilde{\tau} C_1 \tilde{\tau}^{-1} = C_2$ and hence that C_1 and C_2 are conjugate.

Conversely, if we suppose that $\delta C_1 \delta^{-1} = C_2$, then it is again easy to show that $\delta|_{Fix(C_1)}$ is the required isomorphism. □

Let Psf_p be the theory of Psf of characteristic p. Then by the lemma and discussion above, for each characteristic p (including $p = 0$) we have established a one-one correspondence between the conjugacy classes of closed procyclic subgroups of the absolute Galois group of the prime field and $S_0(Psf_p)$. Recall that, for each prime p, we have $G(\mathbb{F}_p)$ is abelian and procyclic and hence we may restate the correspondence in the following form:

Theorem 1.26. *For each prime p, let SG_p be the set of closed subgroups of $G(\mathbb{F}_p)$. Let CSG_C be the set of conjugacy classes of closed procyclic subgroups of $G(\mathbb{Q})$. Then:*

(i) For each prime p, there is a bijection $\Phi_p : S_0(Psf_p) \longrightarrow SG_p$ such that if $F \models Psf_p$, then $\Phi_p(Th(F)) = G(Abs(F))$.

(ii) There is a bijection $\Phi_0 : S_0(Psf_0) \rightarrow CSG_C$, with the property that, if $F \models Psf_0$, then $\Phi_0(Th(F))$ is the conjugacy class of $G(\mathbb{Q})$ such that any member of $\Phi_0(Th(F))$ has fixed field isomorphic to $Abs(F)$.

There are analogous bijections for the complete theories of $ACFA$ of each characteristic. This time, though, a complete theory will be mapped to the conjugacy class of an element in the absolute Galois group. However, because $G(\mathbb{F}_p)$ is abelian, the conjugacy classes are just singletons in this case. As with Psf, let $ACFA_p$ be the theory of $ACFA$ of characteristic p (where p may be 0).

Theorem 1.27. *(i) For each prime p, there is a bijection $\Theta_p : S_0(ACFA_p) \longrightarrow G(\mathbb{F}_p)$ such that if $(K, \sigma) \models ACFA_p$ then $\Theta_p(Th(K, \sigma)) = \sigma|_{\mathbb{F}_p^{\mathrm{alg}}}$.*

(ii) Let $G(\mathbb{Q})_C$ be the set of conjugacy classes of $G(\mathbb{Q})$. There is a bijection $\Theta_0 : S_0(ACFA_0) \rightarrow G(\mathbb{Q})_C$ such that if $(K, \sigma) \models ACFA_0$ then $\Theta_0(Th(K, \sigma))$ is the conjugacy class containing the element $\sigma|_{\mathbb{Q}^{\mathrm{alg}}}$.

Proof. By Theorem 1.12 and Lemma 1.11. □

If we consider the map in Section 1.5 we get the following commuting diagrams.

$$\begin{tikzcd}
S_0(ACFA_p) \arrow[r, "\Theta_p"] \arrow[d] & G(\mathbb{F}_p) \arrow[d] \\
S_0(Psf_p) \arrow[r, "\Phi_p"] & SG_p
\end{tikzcd}
\qquad
\begin{tikzcd}
S_0(ACFA_0) \arrow[r, "\Theta_0"] \arrow[d] & G(\mathbb{Q})_C \arrow[d] \\
S_0(Psf_0) \arrow[r, "\Phi_0"] & CSG_C
\end{tikzcd}$$

In both diagrams the left vertical arrow is the map taking $T \in S_0(ACFA)$ to the theory of its fixed field. In the diagram on the left, the right vertical arrow is the map taking an element of $G(\mathbb{F}_p)$ to the procyclic group generated by it. In the diagram on the right, the right vertical arrow is the map taking a conjugacy class $[x]$ of $G(\mathbb{Q})_C$ to the conjugacy class of groups that are generated by each member of $[x]$.

The bijections in the two theorems above are useful because they characterise the complete types of *Psf* and *ACFA* without having to use the absolute numbers of a field. (The absolute numbers of a field only really make sense when you fix the algebraic closure of the prime field, and so the characterisation above is more invariant.) Recall that there is the natural profinite topology on the absolute Galois group of a field (and indeed on any profinite group). How does this relate under the bijections above to the natural topology on $S_0(Psf)$ and $S_0(ACFA)$ described in Section 1.1? We shall see in Chapter 3 that all the bijections above are homeomorphisms when the spaces CSG_C, SG_p and $G(\mathbb{Q})_C$ are given the Vietoris topology coming from the topology on the absolute Galois group. Thus, in the next Chapter, I will define and give the properties of the Vietoris topology.

Chapter 2

The Vietoris Topology

For a topological space X, let $\mathcal{C}(X)$ be the set of closed, non-empty subsets of X. If X is a metric space with metric d, recall that the *Hausdorff metric* d_H is the metric on $\mathcal{C}(X)$ defined by

$$d_H(A,B) = \max\{\sup_{a\in A}\inf_{b\in B} d(a,b),\ \sup_{b\in B}\inf_{a\in A} d(a,b)\}$$

for $A, B \in \mathcal{C}(X)$. The Vietoris topology is a generalisation to topological spaces of the Hausdorff metric. It is thus a way to define a topology on $\mathcal{C}(X)$ which is induced by that of X. As we will see, it is a good choice for the topology because the Vietoris space inherits many of the properties of the underlying space and there is a natural notion of convergence. For a brief history and references on the Vietoris topology, see [Jo, p 121].

2.1 A base and a subbase

To start with, I will give Vietoris's definition from his 1922 paper[1].

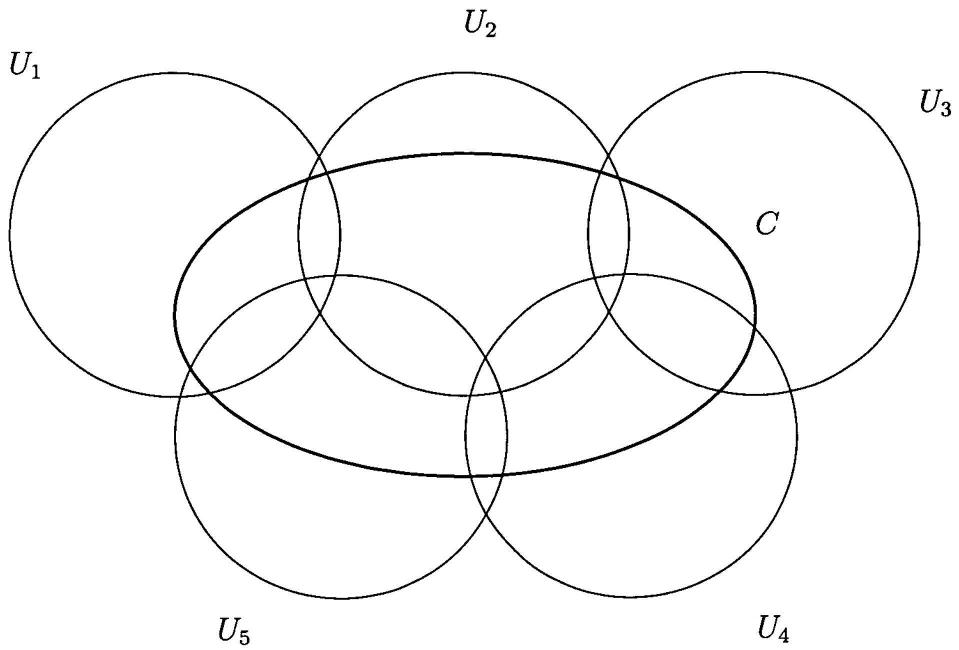
Definition 2.1 ([V], p259). Let X be a topological space. The Vietoris space of X, denoted $\mathcal{V}(X)$, is the topology on $\mathcal{C}(X)$ with basic open sets

$$\langle U_1, \dots, U_n \rangle := \{C \in \mathcal{C}(X) : C \subset \bigcup_{i=1}^{k} U_i \text{ and } C \cap U_i \neq \emptyset \text{ for } i = 1, \dots, k\}$$

for each finite collection $U_1, \dots, U_n$ of open sets of X.

We illustrate the definition in the diagram below:

[1] Leopold Vietoris (born June 4th 1891, died April 9th 2002) was also famous for being the oldest living Austrian man. His last mathematical publication was in 1995.



We must, of course, check that the sets given in the definition form a base. For this it is sufficient to see that

(i) $\mathcal{V}(X) = \langle X \rangle$

(ii) For any open sets $U_1, \ldots, U_n, V_1, \ldots, V_m$, we have

$$\langle U_1, \ldots, U_n \rangle \cap \langle V_1, \ldots, V_m \rangle = \langle V \cap U_1, \ldots, V \cap U_n, U \cap V_1, \ldots, U \cap V_m \rangle$$

where $U = \bigcup_{i=1}^{n} U_i$ and $V = \bigcup_{i=1}^{m} V_i$.

It is worth pointing out that $\langle U \rangle$ is the set of all closed sets contained in the set U, and $\langle X, U \rangle$ is the set of all closed sets having non-trivial intersection with U. Some authors have used the notation U^+ for $\langle U \rangle$ and U^- for $\langle X, U \rangle$. It is more enlightening to think of the Vietoris topology in terms of these sets.

Lemma 2.2. *The sets $\langle U \rangle$ and $\langle X, U \rangle$ for each open set U form a subbase of the Vietoris topology.*

Proof. By construction, the subbase is a subset of the base given in the definition, and so we just need to check that the topology generated by the subbase contains the Vietoris topology. This can be seen by the equality

$$\langle U_1, \ldots, U_n \rangle = \langle \bigcup_{i=1}^{n} U_i \rangle \cap \langle X, U_1 \rangle \cap \cdots \cap \langle X, U_n \rangle$$

□

Remark 2.3. The set $\langle X, U\rangle$ is the complement of all the closed sets contained in $X \setminus U$ and so for any closed set C, we have that $\langle C\rangle := \{D \in \mathcal{C}(X) : D \subset C\}$ is closed. Thus we think of the lemma as saying that the Vietoris topology is the coarsest topology such that

(i) $\langle U\rangle$ is open whenever $U \subset X$ is open

(ii) $\langle C\rangle$ is closed whenever $C \subset X$ is closed.

2.2 Properties in common with X

It was Vietoris who originally showed that X is compact if, and only if, $\mathcal{V}(X)$ is compact. Almost thirty years later, Michael [Mi] greatly expanded on Vietoris's work to give a near exhaustive list of the properties which get carried over from X to $\mathcal{V}(X)$. Because of the quantity of results, Michael's proofs are very concise, so I have included the results that we need from his paper with proofs.

First we will prove Vietoris's theorem. The proof here is from a paper by Frink [Fr] written in terms of lattices. It will require an expansion of the subbase for the Vietoris topology given above.

Lemma 2.4. *The sets*

$$\begin{aligned} U \circledcirc V &= \langle U\rangle \cup \langle X, V\rangle \\ &= \{C \in \mathcal{C}(X) \mid C \subset U \text{ or } C \cap V \neq \emptyset\}, \end{aligned}$$

where U, V are open sets such that $V \subset U$, form a subbase for the Vietoris topology.

Proof. Follows from $\langle U\rangle = U \circledcirc \emptyset$ and $\langle X, U\rangle = U \circledcirc U$ for each open set $U \subset X$. □

Theorem 2.5 ([V]). *Let X be a topological space. Then X is compact if, and only if, $\mathcal{V}(X)$ is compact.*

Proof ([Mi],[Fr]). Suppose that X is compact. By Alexander's Lemma it is sufficient to show that every cover of $\mathcal{V}(X)$ by subbasic sets of the form above has a finite subcover. Thus let $U_\alpha \circledcirc V_\alpha$ be a cover of $\mathcal{V}(X)$.

If the V_α form a cover of X then we can find a finite subcover, say $V_{\alpha_1}, \dots, V_{\alpha_n}$. It is then the case that $U_{\alpha_1} \circledcirc V_{\alpha_1}, \dots, U_{\alpha_n} \circledcirc V_{\alpha_n}$ cover $\mathcal{V}(X)$ because any set in $\mathcal{V}(X)$ will have non-trivial intersection with one of the V_{α_i}. So suppose that the V_α do not form a cover of X. Consider the non-empty closed subset $X - \bigcup_\alpha V_\alpha$.

This must be in $U_\beta - V_\beta$ for some β (since $U_\alpha \circledcirc V_\alpha$ cover $\mathcal{V}(X)$). Thus $U_\beta \cup \bigcup_\alpha V_\alpha$ form a cover of X, and so take a finite subcover, say $U_\beta, V_{\alpha_1}, \ldots, V_{\alpha_m}$. Then $U_\beta \circledcirc V_\beta, U_{\alpha_1} \circledcirc V_{\alpha_1}, \ldots, U_{\alpha_m} \circledcirc V_{\alpha_m}$ are a finite subcover of $\mathcal{V}(X)$.

Conversely suppose that $\mathcal{V}(X)$ is compact, and let U_α be a covering of X by open sets. The sets $\langle X, U_\alpha \rangle$ thus form a covering of $\mathcal{V}(X)$, so take a finite subcovering, say $\langle X, U_{\alpha_1} \rangle, \ldots, \langle X, U_{\alpha_n} \rangle$. The sets $U_{\alpha_1}, \ldots, U_{\alpha_n}$ thus form a finite subcover of X and we are done. □

In later chapters, we shall frequently use this standard result from topology.

Theorem 2.6 ([Ke], Theorem 8, p141). *Let f be a continuous function carrying the compact topological space X onto the topological space Y. Then Y is compact, and if Y is Hausdorff and f is one to one then f is a homeomorphism.*

If X is T_1, then, by definition, for each $x \in X$, the set $\{x\}$ is closed, and hence $\{x\} \in \mathcal{V}(X)$. Thus, for such an X, there is a natural embedding of X in $\mathcal{V}(X)$. We will see that if $\mathcal{V}(X)$ is compact and Hausdorff, then X is homeomorphic to its image in $\mathcal{V}(X)$.

Lemma 2.7. *Suppose that $\mathcal{V}(X)$ is compact and Hausdorff, and let f be the map taking $x \in X$ to $\{x\} \in \mathcal{V}(X)$. Then $f : X \to f(X)$ is a homeomorphism.*

Proof. Observe that $f(X)$ is Hausdorff and that, by Theorem 2.5 X is compact. Thus by Theorem 2.6, it is sufficient to show that f is continuous, but this is obvious because

$$f^{-1}(\langle U_1, \ldots, U_n \rangle) = \bigcap_{i=1}^{n} U_i$$

for a basic open set $\langle U_1, \ldots, U_n \rangle$ of $\mathcal{V}(X)$. □

The theorem below contains the results we will need from [Mi]. In contrast to Michael, we will use the currently standard definition of a Stone space as being a compact, Hausdorff and totally disconnected space. (This, however, is not to say that Michael does not prove (iii) from the theorem below—see 4.9.6 and 4.13.2 of [Mi].) There are many equivalent formulations of the property totally disconnected; the one we will use below is that there is a base of clopen sets.

Theorem 2.8 ([Mi], Section 4). *Let X be a topological space and $\mathcal{V}(X)$ the Vietoris space. Then:*

(i) X is compact and Hausdorff $\iff$ $\mathcal{V}(X)$ is compact and Hausdorff.

(ii) *X is second countable, compact and Hausdorff $\iff$ $\mathcal{V}(X)$ is second countable, compact and Hausdorff.*

(iii) *X is a Stone space $\iff$ $\mathcal{V}(X)$ is a Stone space.*

Proof. In each case, sufficiency follows from Theorem 2.5 and Lemma 2.7. We will now prove necessity.

(i) Suppose that X is compact and Hausdorff. By Theorem 2.5, we only need to show $\mathcal{V}(X)$ is Hausdorff. Let $A, B \in \mathcal{V}(X)$ be distinct sets. Without loss of generality, assume that there is an $x \in A$ such that $x \notin B$. Since X is compact and Hausdorff, there exists disjoint open sets $U, V \subset X$ such that $x \in U$ and $B \subset V$. Therefore $B \in \langle V \rangle$ and $A \in \langle X, U \rangle$. Moreover $\langle V \rangle \cap \langle X, U \rangle = \emptyset$ because $V \cap U = \emptyset$.

(ii) Suppose that X is second countable, compact and Hausdorff. It is only left to show that $\mathcal{V}(X)$ is second countable. Let $\mathcal{U} = \{U_i : i \in \mathbb{N}\}$ be a countable base for X, and we may assume, without loss of generality, that $\mathcal{U}$ is closed under taking finite unions. We will now see that the sets $\langle U_{i_1}, \ldots, U_{i_n} \rangle$ form a base of $\mathcal{V}(X)$, from which it follows that $\mathcal{V}(X)$ is second countable.

Let $\langle V_1, \ldots, V_m \rangle$ be a basic open set in $\mathcal{V}(X)$ (i.e. $V_1, \ldots, V_m$ are arbitrary open sets). Let $C \in \langle V_1, \ldots, V_m \rangle$, and let

$$\mathcal{U}_C = \{U_j \in \mathcal{U} : U_j \subset V_i \text{ for some } i = 1, \ldots, m \text{ and } U_j \cap C \neq \emptyset\}.$$

The set $\mathcal{U}_C$ is an open cover of C and hence has a finite subcover. Thus by taking a finite subcover and extending, if necessary, by members of $\mathcal{U}_C$, we can get a subcover

$$\mathcal{U}'_C = \{U_{j_1}, \ldots, U_{j_s}\}$$

such that for all $i = 1, \ldots, m$, there exists a k such that $U_{j_k} \subset V_i$. As a consequence of this construction we have that

$$C \in \langle \mathcal{U}'_C \rangle := \langle U_{j_i}, \ldots, U_{j_s} \rangle \subset \langle V_1, \ldots, V_m \rangle$$

and hence

$$\bigcup_{C \in \langle V_1, \ldots, V_m \rangle} \langle \mathcal{U}'_C \rangle = \langle V_1, \ldots, V_m \rangle.$$

(iii) By the proof of (ii), it is sufficient to note that, if the sets $U_1, \ldots, U_n \subset X$ are clopen, then the set $\langle U_1, \ldots, U_n \rangle \subset \mathcal{V}(X)$ is clopen (which follows from a similar argument to that in Remark 2.3). □

2.3 Convergence

Recall that a *local base* at a point x in a topological space X is a family of open neighbourhoods of x such that every open neighbourhood of x contains a member of the family [Ke, p50]. I will now give a definition of first countable and, for comparison, I will also give a definition of second countable.

Definition 2.9. Let X be a topological space.

(i) X is *first countable* if at every point there is a countable local base.

(ii) X is *second countable* if it has a countable base.

Remark 2.10. An uncountable space with the discrete topology is first, but not second, countable because a local base at the point x is given by $\{x\}$.

Theorem 2.11 ([Ke], p72). *Let X be a first countable topological space. Then a set $U \subset X$ is open if, and only if, each sequence converging to a point in U is eventually in U.*

Thus, in the first countable case, it is possible to describe the topology in terms of sequences (in general one must consider nets, see [Ke, Chapter 2]). The following lemmas show that there is a very natural notion of convergence in the Vietoris topology.

Lemma 2.12. *Let X be first countable and let (V_n) be a sequence in $\mathcal{V}(X)$. If (V_n) converges to V in $\mathcal{V}(X)$, then for each $x \in V$, there is a sequence (x_n) such that $x_n \in V_n$ and (x_n) converges to x.*

Proof. Let $x \in V$ and let (U_n) be a local base of x. By replacing U_j with $\bigcap_{i \leq j} U_i$, if necessary, we may assume that $U_i \supset U_j$ for $i < j$. Since V_n converges to V in $\mathcal{V}(X)$, for each i, there is an N_i such that for all $j \geq N_i$ we have $V_j \in \langle X, U_i \rangle$. Furthermore, we can pick the N_i such that the sequence (N_n) is strictly increasing. We can thus create a sequence converging to x as follows: first for $i < N_0$, pick any $x_i \in V_i$; then at stage $j+1$, for each i such that $N_j \leq i < N_{j+1}$ pick any $x_i \in V_i \cap U_j$. □

Under different assumptions the notion of convergence also works the other way.

Lemma 2.13. *Let X be a regular topological space. Let (V_i) be a sequence in $\mathcal{V}(X)$ converging to V and let (v_i) be a sequence in X converging to v such that $v_i \in V_i$, for each i. Then $v \in V$.*

Proof. Suppose not. Let U_1 and U_2 be disjoint sets such that $V \subset U_1$ and $v \in U_2$. Then for some N, for all $i \geq N$, we have $V_i \subset U_1$ and $v_i \in U_2$, which is a contradiction. □

The spaces we shall be considering in Chapters 3 and 4 are the absolute Galois group of a prime field. A base for the topology on these groups is given by the cosets of open normal subgroups of finite index. The open normal subgroups of finite index are in bijective correspondence with finite Galois extensions of the field, and hence the groups are second countable. We may therefore take advantage of the lemmas given above.

Chapter 3

Coding the complete theories in each characteristic

Recall from Section 1.6 the following notation:

SG_p the set of closed subgroups of $G(\mathbb{F}_p)$
CSG_C the set of conjugacy classes of closed procyclic subgroups of $G(\mathbb{Q})$
$G(\mathbb{Q})_C$ the set of conjugacy classes of $G(\mathbb{Q})$

and define

CSG the set of closed procyclic subgroups of $G(\mathbb{Q})$.

Recall, from Theorem 1.26 and 1.27, that, for each prime p, there are natural bijections

$$S_0(Psf_p) \xrightarrow{\Phi_p} SG_p \qquad\qquad S_0(ACFA_p) \xrightarrow{\Theta_p} G(\mathbb{F}_p)$$

and, in the characteristic 0 case, there are natural bijections

$$S_0(Psf_0) \xrightarrow{\Phi_0} CSG_C \qquad\qquad S_0(ACFA_0) \xrightarrow{\Theta_0} G(\mathbb{Q})_C$$

In this chapter, we will see that all the maps above are homeomorphisms when we consider the codomains with the Vietoris topology. We will first prove this for the maps Φ_p and Φ_0 and in the final section we will see that the proofs carry over easily to the maps Θ_p and Θ_0.

3.1 The Vietoris topology on profinite groups

The goal of this section is to show that CSG_C and SG_p are closed subspaces of $\mathcal{V}(\mathcal{V}(G(\mathbb{Q})))$ and $\mathcal{V}(G(\mathbb{F}_p))$ respectively. As an immediate consequence of

Theorem 2.8 we get that both CSG_C and SG_p are Stone spaces (as are $S_0(Psf_0)$ and $S_0(Psf_p)$).

The fact that SG_p is closed follows immediately from this easy lemma.

Lemma 3.1. *Let G be a regular second countable topological group and $\mathcal{V}(G)$ the induced Vietoris space. The set of closed subgroups of G is a closed subset in $\mathcal{V}(G)$.*

Proof. Let (H_n) be a sequence of closed subgroups with limit H in $\mathcal{V}(G)$. We will show H is a subgroup. Let $g, h \in H$. It is sufficient to show $gh^{-1} \in H$.

By applying Lemma 2.12 there are sequences g_n and h_n, converging to g and h respectively, such that $g_n, h_n \in H_n$ for each n. We have that each H_n is a group and so we get that $g_n h_n^{-1} \in H_n$ for each n. Since multiplication is continuous, we get that the limit of $(g_n h_n^{-1})$ is gh^{-1}. Therefore by Lemma 2.13 we have that $gh^{-1} \in H$. □

We will now see that the set CSG of closed procyclic subgroups of $G(\mathbb{Q})$ is closed in $\mathcal{V}(G(\mathbb{Q}))$. Recall from Section 1.4 that there is a natural notion of taking powers from $\widehat{\mathbb{Z}}$ in a profinite group and that a subgroup H of a profinite group is procyclic if, and only if, there is an element α such that

$$H = \{\alpha^z : z \in \widehat{\mathbb{Z}}\}.$$

Lemma 3.2. *Let G be a second countable profinite group and let $\mathcal{V}(G)$ be the induced Vietoris space. The set of procyclic subgroups is a closed subset of $\mathcal{V}(G)$.*

Proof. First note that by Theorem 2.8 we have that $\mathcal{V}(G)$ is a second countable Stone space.

Now consider a sequence of procyclic groups (H_n) in $\mathcal{V}(G)$ converging to H. By Lemma 3.1, it is sufficient to show that H is procyclic. For each n, let α_n be a generator of H_n. Since G is compact, by taking a subsequence, we can assume that the sequence (α_n) converges to an $\alpha \in G$. Furthermore by Lemma 2.13, we have that $\alpha \in H$. We will now show that $H = \{\alpha^z : z \in \widehat{\mathbb{Z}}\}$.

Let $h \in H$. From Lemma 2.12, there exists a sequence (h_n) converging to h such that $h_n \in H_n$. By Lemma 1.17, we can write $h_n = \alpha_n^{z_n}$ for each n, where $z_n \in \widehat{\mathbb{Z}}$. Since $\widehat{\mathbb{Z}}$ is compact, we can take a subsequence (z_{n_k}) converging to a $z \in \widehat{\mathbb{Z}}$. Therefore by the continuity of the 'power' map we get that $(\alpha_{n_k}^{z_{n_k}})$ converges to α^z, and since G is Hausdorff $\alpha^z = h$. □

We are concerned with CSG_C, the conjugacy classes of closed procyclic subgroups. We first need to show that they are points of

$$\mathcal{V}(CSG) \subset \mathcal{V}(\mathcal{V}(G(\mathbb{Q}))).$$

This follows from the corollary after the lemma below.

Lemma 3.3. *Let G be a second countable, compact and Hausdorff topological group. Let (H_n) be a sequence in $\mathcal{V}(G)$ converging to H and g_n be a sequence in G converging to g. Then the sequence $(g_n H_n g_n^{-1})$ converges to gHg^{-1}.*

Proof. Let $\langle U_1, \ldots, U_m \rangle$ be a basic open neighbourhood of gHg^{-1}, where the sets $U_1, \ldots, U_m$ are open in G. Pick $h_1, \ldots, h_m \in H$ such that $gh_ig^{-1} \in U_i \cap gHg^{-1}$. By Lemma 2.12, for each i, we can take a sequence (h_{in}) converging to h_i, where $h_{ij} \in H_j$ for each j and by the continuity of multiplication in G, we have $(g_n h_{in} g_n^{-1})$ converges to gh_ig^{-1}. For each $i \in \{1, \ldots, m\}$, let N_i be such that for all $j \geq N_i$ we have $g_j h_{ij} g_j^{-1} \in U_i$. Take $N = \max\{N_1, \ldots, N_m\}$. So for all $j \geq N$ we get that $g_j H_j g_j^{-1} \cap U_i \neq \emptyset$ for all $i \in \{1, \ldots, m\}$.

Let $U := \bigcup_{i=1}^m U_i$. It is now sufficient to show that there is an M such that for every $j \geq M$ we have $g_j H_j g_j^{-1} \subset U$. If this is not the case, then we may take a subsequence $(g_{n_k} H_{n_k} g_{n_k}^{-1})$ such that $g_{n_j} H_{n_j} g_{n_j}^{-1} \not\subset U$ for all j. So pick, for each j, an element $g_{n_j} h_{n_j} g_{n_j}^{-1} \notin U$. Since G is compact, by taking another subsequence we may assume that (h_{n_k}) converges to an h, which, by Lemma 2.13, is in H. (Note that the conditions of Lemma 2.13 are satisfied because a compact Hausdorff space is normal and so, in particular, it is regular.) Therefore $(g_{n_k} h_{n_k} g_{n_k}^{-1})$ converges to ghg^{-1}, and U is a neighbourhood of ghg^{-1} such that $g_{n_j} h_{n_j} g_{n_j}^{-1} \notin U$ for each j, contradiction. □

Corollary 3.4. *Let G be a second countable profinite group and let H be a closed subgroup of G. Then the conjugacy class of H in G, denoted $[H]$, is a closed subset of $\mathcal{V}(G)$.*

Proof. Let (K_n) be a convergent sequence in $[H]$. Then, for each n, we can write $K_n = g_n H g_n^{-1}$. Since G is compact, by taking a convergent subsequence, we can assume that (g_n) converges to some $g \in G$. Thus, by Lemma 3.3, (K_n) converges to $gHg^{-1} \in [H]$. □

We will now see that the set of conjugacy classes of closed subgroups is closed, and from this we can show our desired result.

Lemma 3.5. *Let G be a second countable profinite group and let $SG \subset \mathcal{V}(G)$ be the set of closed subgroups of G. Let $C \subset SG$ be a closed subset of $\mathcal{V}(G)$. Then the set of conjugacy classes in $\mathcal{V}(C)$ is closed in $\mathcal{V}(\mathcal{V}(G))$.*

Proof. Let $([H_n])$ be a convergent sequence in $\mathcal{V}(C)$. Since $\mathcal{V}(G)$ is compact, by taking a convergent subsequence, we can assume that (H_n) converges to some $H \in C$. It is now sufficient to show that $([H_n])$ converges to $[H]$.

Suppose that $gHg^{-1} \in [H]$, but then we have that (gH_ng^{-1}) is a sequence converging to gHg^{-1}. Thus, by Lemma 2.13 we have that gHg^{-1} is in the limit of $([H_n])$.

Conversely, suppose that K is in the limit of $([H_n])$. Then, by Lemma 2.12, we have that K is the limit of a sequence $(g_nH_ng_n^{-1})$, for some $g_n \in G$. By compactness, we can assume that (g_n) converges to some $g \in G$ and thus by Lemma 3.3, we get that $K = gHg^{-1}$. □

Corollary 3.6. *CSG_C is a closed subspace of $\mathcal{V}(\mathcal{V}(G(\mathbb{Q})))$.*

3.2 Vietoris and quotient spaces

As in the previous section let CSG be the set of closed procyclic subgroups in $\mathcal{V}(G(\mathbb{Q}))$. You may have been wondering what would have happened if, in the previous section, instead of considering the conjugacy classes as points in a double Vietoris space, we had considered taking the quotient of CSG by conjugacy, that is, the space $CSG/\sim$, where $\sim$ is the equivalence relation $H \sim K \iff H$ is conjugate to K. The purpose of this short section is to show that these two spaces are in fact homeomorphic.

First, I will prove a more general result. Recall that a partition of a topological space is a disjoint family of subsets whose union is the whole space.

Theorem 3.7. *Let X be a second countable, compact and Hausdorff topological space and let $\mathcal{V}(X)$ be the Vietoris space. Suppose that the closed subset $C \subset \mathcal{V}(X)$ forms a partition of X and let $\sim$ be the induced equivalence relation. Then the spaces $X/\sim$ and C are homeomorphic.*

Proof. Let $q : X \to X/\sim$ be the quotient map and let $f : X/\sim \to C$ be the obvious bijection. We have the following diagram

$$\begin{tikzcd} X \arrow[rr, "g"] \arrow[dr, "q"'] & & C \\ & X/\sim \arrow[ur, "f"'] & \end{tikzcd}$$

where $g = f \circ q$. From the diagram, it can be seen that it is sufficient to show:

$$A \text{ is closed in } C \iff g^{-1}(A) \text{ is closed in } X.$$

Suppose, then, that $g^{-1}(A)$ is closed in X. Now let (V_n) be a sequence in A that converges to a $V \in C$, and consider an $x \in V$. By Lemma 2.12, we get a sequence (x_n) converging to x such that $x_i \in V_i$ for all i. We then get that $x \in g^{-1}(A)$ and so $V \in A$.

Conversely, suppose that A is closed in C, and let (x_n) be a sequence in $g^{-1}(A)$. Now consider the sequence $(g(x_n))$ in A. Since C is compact, we may take a convergent subsequence. By Lemma 2.13, we have that x is in the limit of the convergent subsequence and hence $x \in g^{-1}(A)$. □

Corollary 3.8. *The spaces $CSG_{\mathcal{C}}$ and $CSG/\sim$ are homeomorphic.*

3.3 The homeomorphism for *Psf*

We are now ready to show Φ_0 and Φ_p are homeomorphisms.

Recall that, in Section 3.1, we introduced the notation CSG for the set of closed procyclic subgroups of $G(\mathbb{Q})$. Hence we have the following inclusions:

$$CSG \subset \mathcal{V}(G(\mathbb{Q}))$$
$$CSG_{\mathcal{C}} \subset \mathcal{V}(CSG) \subset \mathcal{V}(\mathcal{V}(G(\mathbb{Q})))$$

Theorem 3.9. *The map $\Phi_0 : S_0(Psf_0) \to CSG_{\mathcal{C}}$, defined in Theorem 1.26, is a homeomorphism.*

Proof. By Theorem 2.6, it is sufficient to show that Φ_0 is continuous. Let A be a closed subset in $CSG_{\mathcal{C}}$. Consider a sequence (T_n) in $\Phi_0^{-1}(A)$ which converges to $T \in S_0(Psf_0)$. We thus want to show that $T \in \Phi_0^{-1}(A)$. Now consider the corresponding sequence in A, i.e. (X_n) where $X_i = \Phi_0(T_i)$ for each i. By taking a subsequence we may assume that (X_n) converges to an $X \in A$. It is thus sufficient to show $\Phi_0^{-1}(X) = T$.

From Theorem 1.6, we know that T is determined by the statements of the form

$$\theta_f \equiv \exists x f(x) = 0$$

where f is a polynomial over the integers. Hence T is determined by the θ_f such that f is irreducible over $\mathbb{Q}$.

Suppose that $\theta_f \in T$. Thus, by the base for the topology on $S_0(Psf_0)$ given in Section 1.1, there is an N, such that $\theta_f \in T_i$, for all $i \geq N$. Let α be a root of $f(x)$ and let $H = G(\mathbb{Q}(\alpha))$. We have that H is a clopen set of $G(\mathbb{Q})$ and so $\langle H \rangle$ is clopen in $\mathcal{V}(G(\mathbb{Q}))$. Thus $Y := \langle H \rangle \cap CSG$ is a clopen set of CSG. Since $CSG_{\mathcal{C}} \subset \mathcal{V}(CSG)$, we have also that $Z := \langle CSG, Y \rangle \cap CSG_{\mathcal{C}}$ is a clopen set. We observe that Z is the conjugacy classes in $G(\mathbb{Q})$ of closed procyclic subgroups of H.

Pick an $i \geq N$ and a pseudo-finite field F_i such that $F_i \models T_i$. Since $\theta_f \in T_i$, we have that a conjugate of α is in $Abs(F_i)$, that is $\sigma(\alpha) \in Abs(F_i)$ for some $\alpha \in G(\mathbb{Q})$. Thus

$$\mathbb{Q} \subset \mathbb{Q}(\sigma(\alpha)) \subset Abs(F_i)$$

and by the Galois correspondence,

$$G(\mathbb{Q}) \supset \sigma H \sigma^{-1} \supset G(Abs(F_i))$$

So, by the definition of Φ_0, we have $X_i = [G(Abs(F_i))]$ and by the construction of Z above we have $X_i \in Z$. Hence $X_i \in Z$, for every $i \geq N$, and so $X \in Z$. Therefore $\theta_f \in \Phi_0^{-1}(X)$.

Now suppose that $\theta_f \notin T$ or equivalently, $\neg\theta_f \in T$ and let Z be as above. Since $CSG_C \setminus Z$ is closed we can use the argument above to show that $X \in CSG_C \setminus Z$. Thus $\neg\theta_f \in \Phi_0^{-1}(X)$, and therefore $\Phi_0^{-1}(X) = T$. □

As a corollary to the proof above we get.

Corollary 3.10. *For each prime p, the map $\Phi_p : S_0(Psf_p) \to SG_p$ is a homeomorphism.*

Proof. Let A be a closed subset in SG_p, and, with the analogous definitions to the above proof, we need to show $\Phi_p^{-1}(X) = T$. We now have that T is determined by the sentences θ_f such that f is irreducible over $\mathbb{F}_p$.

Let α be a root of $f(x)$ and let $H = G(\mathbb{F}_p(\alpha))$. From the previous proof, it is now sufficient to note that $Z := \langle H \rangle \cap SG_p$ is a clopen set of SG_p. □

3.4 ...and for *ACFA*

In this section we will show that Θ_0 and Θ_p are homeomorphisms.

In analogy with Section 3.1, we must first show that $G(\mathbb{Q})_C$, the set of conjugacy classes of $G(\mathbb{Q})$, is a subset of $\mathcal{V}(G(\mathbb{Q}))$ and then that this subset is closed.

Lemma 3.11. *Let G be a second countable profinite group. Let $x \in G$ and let $[x]$ be the conjugacy class of x. Then $[x]$ is a closed subset of G.*

Proof. Let $(g_n x g_n^{-1})$ be a convergent sequence in G. Then, by compactness, there is a subsequence (g_{n_k}) which converges to some $g \in G$. Thus by continuity of multiplication $(g_n x g_n^{-1})$ converges to gxg^{-1}. □

Lemma 3.12. *Let G be a second countable profinite group and let G_C be the set of conjugacy classes of G. Then G_C is a closed subset of $\mathcal{V}(G)$.*

Proof. Let $([x_n])$ be a sequence in G_C converging to $X \in \mathcal{V}(G)$. By taking a subsequence, we may assume that (x_n) converges to some $x \in G$. It is now sufficient to show $[x] = X$.

Pick an arbitrary element, say gxg^{-1}, of $[x]$. We know, however, that $gx_ig^{-1} \in [x_i]$ for each i and so by Lemma 2.13 we have $gxg^{-1} \in X$. On the other hand, consider a $z \in X$. Then, by Lemma 2.12, there is a sequence $(g_nx_ng_n^{-1})$ converging to z. By compactness, there will be a convergent subsequence of (g_n), converging to some $g \in G$, and hence $z = gxg^{-1}$. □

Remark 3.13. As before, we note that, by Theorem 3.7, $G(\mathbb{Q})_C$ is just the quotient space.

Theorem 3.14. *The map $\Theta_0 : S_0(ACFA_0) \to G(\mathbb{Q})_C$, defined in Theorem 1.27, is a homeomorphism.*

Proof. We proceed in the same way as in the proof of Theorem 3.9. Thus let A be a closed subset in $G(\mathbb{Q})_C$. Let (T_n) be a sequence in $\Theta_0^{-1}(A)$ converging to $T \in S_0(ACFA_0)$ and, without loss of generality, $([\sigma_n]) := (\Theta_0(T_n))$ converges to $[\sigma] \in A$. I will show that $\Theta_0^{-1}([\sigma]) = T$.

By the proof of Theorem 1.12, we know that T is determined by statements of the form

$$\theta_{f,g} \equiv \exists x \ (f(x) = 0 \wedge \sigma(x) = g(x))$$

where f, g are polynomials over $\mathbb{Q}$. Note that $\theta_{f,g}$ is not quite a sentence of $\mathcal{L}_\sigma$, but if we let $r, s \in \mathbb{Z}$ be the product of the denominators of the coefficients in f, g respectively, we can consider

$$\theta'_{f,g} \equiv \exists x \ (rf(x) = 0 \wedge \sigma(sx) = sg(x))$$

which is a sentence of $\mathcal{L}_\sigma$. Thus we will write $\theta_{f,g} \in T$ for $\theta'_{f,g} \in T$. Furthermore, we need only consider $\theta_{f,g}$ where f is the minimum polynomial of a primitive element α of a normal extension of $\mathbb{Q}$ and $g(\alpha)$ is a root of f. Let f be such a polynomial. Let $H = G(\mathbb{Q}(\alpha))$ and so $H \lhd G(\mathbb{Q})$. Now for $\tau \in G(\mathbb{Q})$ we have that $\theta_{f,g}$ holds if, and only if, $\theta_{f,g}$ holds for all elements of τH. Moreover it can be seen that $\theta_{f,g}$ holds for τ if, and only if, it holds for all conjugates of τ. So let Y be the union of all the cosets of H for which $\theta_{f,g}$ holds. Hence we note that Y is clopen, because it can be considered to be a finite union, and that Y is closed under conjugation.

We now consider the clopen set of $G(\mathbb{Q})_C$ induced by Y, that is

$$Z := \langle Y \rangle \cap G(\mathbb{Q})_C.$$

By definition, $[\tau] \in Z$ if, and only if, $\theta_{f,g}$ holds for each conjugate of τ.

Pick an $i \in \mathbb{N}$ and a $(K, \tau_i) \models T_i$. Thus $\theta_{f,g} \in T_i$ if, and only if, $(K, \tau_i) \models \theta_{f,g}$. By the definition of Θ_0, we have $[\tau_i|_{\mathbb{Q}^{\mathrm{alg}}}] = [\sigma_i]$. Therefore $(K, \tau_i) \models \theta_{f,g}$ if, and only if, $\theta_{f,g}$ holds for each conjugate of σ_i. But as we noted above $\theta_{f,g}$ holds for each conjugate of σ_i if, and only if, $[\sigma_i] \in Z$.

We therefore have:

$$\begin{aligned} \theta_{f,g} \in T &\iff \exists N \text{ such that } \theta_{f,g} \in T_i \text{ for all } i \geq N \\ &\iff \exists N \text{ such that } [\sigma_i] \in Z \text{ for all } i \geq N \\ &\iff [\sigma] \in Z \\ &\iff \theta_{f,g} \in \Theta_0^{-1}([\sigma]) \end{aligned}$$

□

The proof can be modified in the same way as in the previous section to give:

Corollary 3.15. *For each prime p, the map $\Theta_p : S_0(ACFA_p) \to G(\mathbb{F}_p)$ is a homeomorphism.*

To finish, I will make some observations. Firstly, by Theorem 3.7, $G(\mathbb{Q})_C$ can be thought of as a quotient space. Thus both Theorem 3.14 and Corollary 3.15 can be stated and proved without reference to the Vietoris topology. Secondly, Corollary 3.15 defines a natural group structure on the spaces $S_0(ACFA_p)$ and although this is clear from the material on *ACFA* already published I do not think it has been explicitly stated before.

Chapter 4

Coding the complete theories

In this chapter we shall extend the results of the previous chapter to show that the whole space of complete theories of *Psf* can be thought of as lying in the double Vietoris space of $G(\mathbb{Q})$. The spaces $S_0(Psf_p)$ will be shown to be homeomorphic to collections of subgroups of $G(\mathbb{Q})$ which will be denoted by $G_0(Psf_p)$. We will then take the union of these spaces to obtain the space $G_0(Psf)$ which will be shown to be homeomorphic to $S_0(Psf)$. As in the previous chapter, we will show, in the final section, that we can adapt the proofs to the *ACFA* case.

4.1 Group theory preliminaries

We begin with some standard definitions from group theory. Let G be a profinite group and N a closed normal subgroup of G. In this case we will say that G is an *extension* of N. A *complement* of N is a closed subgroup K such that $N \cap K = 1$ and $G = NK$. If the extension G of N has a complement K then we will say that the extension *splits*, and that G is the *semi-direct product* of N by K, written $K \ltimes N$. The general properties of the semi-direct product of profinite groups are given in [W, p22]. We note from there that $K \ltimes N$ is homeomorphic (but not isomorphic) to $K \times N$ and that multiplication is given by $(k_1, n_1)(k_2, n_2) = (k_1k_2, k_2^{-1}n_1k_2n_2)$ where $k_1, k_2 \in K$ and $n_1, n_2 \in N$.

Lemma 4.1. *Let (G_n) be a convergent sequence of closed subgroups of a first countable profinite group and let $G_i = K_i \ltimes N_i$ for each i. Assume also that the sequences (K_n) and (N_n) converge to K and N respectively. Then (G_n) converges to $K \ltimes N$.*

Proof. Let G be the limit of G_n and let $g \in G$. Then by Lemma 2.12 there is a sequence (g_n) such that $g_n \in G_n$ and (g_n) converges to g. Furthermore, for each

n, we have $g_n = k_n h_n$ for some $k_n \in K_n$ and $h_n \in N_n$. By taking convergent subsequences, if necessary, we may assume that (k_n) converges to some $k \in K$ and (h_n) converges to some $h \in N$. By the continuity of multiplication, we now have that $g = kh \in K \ltimes N$.

Now suppose that $kh \in K \ltimes N$. Then, by Lemma 2.12, there are sequences (k_n) and (h_n) converging to k and h respectively and such that, for each n, we have $k_n \in K_n$ and $h_n \in N_n$. Thus the sequence $(k_n h_n)$ converges to kh and, by Lemma 2.13, we have $kh \in G$. □

Lemma 4.2. *Let G be a group and let H, K, L be closed subgroups of G. If $G = (H \ltimes K) \ltimes L$, then $G = H \ltimes (K \ltimes L)$.*

Proof. We first show that $G = H \ltimes KL$. To show that $KL \lhd G$, consider $gKLg^{-1}$ for some $g \in G$. Since that $G = (H \ltimes K) \ltimes L$, we may write $g = hkl$ where $h \in H, k \in K$ and $l \in L$. Thus we have

$$gKLg^{-1} = hklKLl^{-1}k^{-1}h^{-1} = hKLh^{-1} = hKh^{-1}hLh^{-1} = KL.$$

Now suppose that some $x \in H \cap KL$. Thus $x = kl$ for some $k \in K$ and $l \in L$ but then $k^{-1}x = l$. Since $x \in H$ and $G = (H \ltimes K) \ltimes L$, this means that $l = 1$ and hence $x = k = 1$. Therefore $G = H \ltimes KL$.

Now we will show that $KL = K \ltimes L$. Since L is a closed normal subgroup of G, it is a closed normal subgroup of KL. Moreover since $(H \ltimes K) \cap L = 1$, we have that $K \cap L = 1$. Therefore $KL = K \ltimes L$ and hence $G = H \ltimes (K \ltimes L)$. □

Our concern later will be the case where G is a profinite group. In this case we must check that in the lemma above the subgroup KL is closed in G, but this is just a consequence of the fact that G is compact and Hausdorff (by [W, Lemma 0.3.1]).

Remark 4.3. The converse to the above lemma is not true. Consider the finite group of order 27 given by

$$G = \langle a, b, c : a^3 = b^3 = c^3 = 1, ba = abc, cb = bc, ca = ac \rangle.$$

Let A, B, C be the subgroups generated by a, b, c respectively. Then we see that $G = A \ltimes (B \ltimes C)$, but $a^{-1}Ba$ is the subgroup generated by bc and hence $G \neq (A \ltimes B) \ltimes C$.

4.2 Henselian fields

Recall that a pair $(K, |.|)$ where K is a field and $|.|$ is an absolute value on K is called a valued field [FT, p64]. We will say that $(K, |.|)$ is *henselian* if, and only if, there is a unique extension of $|.|$ to each algebraic extension of K. A good general reference for henselian fields is [A3]. There it is shown that a valued field is henselian if, and only if, it satisfies an analogue of Hensel's Lemma and hence we have that $\mathbb{Q}_p$ with the p-adic absolute value is henselian. It is trivial, but worth pointing out, that if K is henselian with respect to some absolute value then any algebraic extension of K with the unique induced absolute value will be henselian.

We will now prove some results for henselian fields in close analogy with [NSW, pp369,662,663]. If $(K, |.|)$ is henselian, then there is no harm in thinking of $|.|$ as a function on K^{alg} and we will do this without further comment. The following lemma is well known for p-adic fields but in fact it holds for henselian fields.

Krasner's Lemma. *Let K be a henselian field with respect to a nonarchimedean absolute value. Let $\alpha \in K^{\mathrm{alg}}$ be separable over K and let $\alpha = \alpha_1, \ldots, \alpha_n$ be the conjugates of α over K. Suppose that for $\beta \in K^{\mathrm{alg}}$ we have*

$$|\alpha - \beta| < |\alpha - \alpha_i|$$

for $i = 2, \ldots, n$. Then $K(\alpha) \subseteq K(\beta)$.

Proof. Let N be the normal closure of $K(\alpha, \beta)$ and consider the Galois field extension $N/K(\beta)$. Let $\sigma \in \mathcal{G}(N/K(\beta))$ and note that because the extension of $|.|$ to N is unique we have $|\sigma(x)| = |x|$ for each $x \in N$.

Thus

$$|\beta - \sigma(\alpha)| = |\sigma(\beta - \alpha)| = |\beta - \alpha| < |\alpha - \alpha_i|$$

for $i = 2, \ldots, n$ and so

$$|\alpha - \sigma(\alpha)| = |\alpha - \beta + \beta - \sigma(\alpha)| \leq \max\{|\alpha - \beta|, |\beta - \sigma(\alpha)|\} < |\alpha - \alpha_i|$$

for $i = 2, \ldots, n$ and hence $\sigma(\alpha) = \alpha$. Therefore $\alpha \in K(\beta)$. □

We can also prove a stronger form of Krasner's Lemma. Recall that if $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $g = b_n x^n + \cdots + b_0$ are polynomials over $(K, |.|)$ then

$$|f - g| := \max_i |a_i - b_i|.$$

Lemma 4.4. *Let K be a henselian field with respect to a nonarchimedean absolute value $|.|$ and let f be a polynomial over K with non-zero discriminant. Then for every polynomial g over K with $|f-g|$ sufficiently small, the splitting fields of f and g coincide.*

Proof. Let α be a root of f. Now for $|f-g|$ sufficiently small we get that $|g(\alpha)| = |g(\alpha) - f(\alpha)|$ is small. By writing $g(x) = d\prod_{i=1}^{n}(x-\beta_i)$ we see that $|\alpha - \beta_j|$ is small for some root β_j.

Let $f(x) = c\prod_{i=1}^{n}(x-\alpha_i)$ and let

$$\varepsilon = \min\{|\alpha_i - \alpha_j| : i \neq j\}.$$

Thus we can pick a $g(x) = d\prod_{i=1}^{n}(x-\beta_i)$ such that for each i there is an $s(i) \in \{1,\dots,n\}$ with $|\alpha_i - \beta_{s(i)}| < \varepsilon$. Note that if $i \neq j$, then by the ultrametric inequality we get

$$\max\{|\alpha_i - \beta_{s(i)}|, |\beta_{s(i)} - \beta_{s(j)}|, |\beta_{s(j)} - \alpha_j|\} \geq |\alpha_i - \alpha_j| \geq \varepsilon$$

but since $|\alpha_i - \beta_{s(i)}|, |\alpha_j - \beta_{s(j)}| < \varepsilon$ we must have

$$|\beta_{s(i)} - \beta_{s(j)}| \geq \varepsilon. \qquad (*)$$

In particular the map s is a bijection.

Now for each α_i we have

$$|\alpha_i - \beta_{s(i)}| < \varepsilon \leq \min_{j\in\{1,\dots,i-1,i+1,\dots,n\}} |\alpha_i - \alpha_j|$$

and by Krasner's Lemma we get that $\alpha_i \in K(\beta_{s(i)})$. Similarly, by (*), for each β_i we have

$$|\alpha_{s^{-1}(i)} - \beta_i| < \varepsilon \leq \min_{j\in\{1,\dots,i-1,i+1,\dots,n\}} |\beta_i - \beta_j|$$

and by Krasner's Lemma we get that $\beta_i \in K(\alpha_{s^{-1}(i)})$. Therefore the splitting fields coincide. □

Recall that two absolute values $|.|_1$ and $|.|_2$ of K are equivalent if there exists a positive real number α such that $|x|_1^{\alpha} = |x|_2$ for all $x \in K$, and they are inequivalent otherwise [FT, p64].

Weak Approximation Theorem ([FT], p66). *Let $|.|_1, \dots, |.|_n$ denote inequivalent absolute values on K. Given a positive real number ε and given $x_1, \dots, x_n$ in K, then we can find $y \in K$ such that for each $i = 1, \dots, n$*

$$|y - x_i|_i < \varepsilon.$$

We can now prove a theorem which we will need in the next section.

Theorem 4.5. *Let K be henselian with respect to two inequivalent nonarchimedean absolute values $|.|_1$ and $|.|_2$. Then K is separably closed.*

Proof. Let f be an irreducible separable polynomial of degree n over K, and let $g = \prod_{i=1}^{n}(x - \beta_i)$ where $\beta_1, \ldots, \beta_n$ are distinct elements of K. Because $|.|_1$ and $|.|_2$ are inequivalent, by the weak approximation theorem, for every $\varepsilon > 0$, there exists a polynomial h over K such that $|f - h|_1 < \varepsilon$ and $|g - h|_2 < \varepsilon$. Thus by Lemma 4.4, we can pick h such that the splitting fields of f and g coincide and hence f splits in K. □

Remark 4.6. There are valuations that do not correspond to an absolute value with codomain $\mathbb{R}$ [FJ, pp 13 and 173]. It is possible to define Henselian fields in terms of a valuation (for example see [A3]) and the proofs of the results in this section would translate over easily. Thus the results in this section hold for all Henselian fields.

Alternatively, Macintyre has shown me that there is an equivalence of valuations and nonarchimedean absolute values where the codomain of the absolute value is a real closed field. (This result is well known but appears not to have been published.) Thus we can see that the results above hold for valuations because there is no use of the completeness of $\mathbb{R}$ in any of the proofs.

4.3 The space $G_0(Psf_p)$

In this section we will define the space $G_0(Psf_p)$ and show that it is naturally homeomorphic to $S_0(Psf_p)$. Let K be an algebraic extension of $\mathbb{Q}$. We will say that $\mathfrak{p}$ is a prime of K if $\mathfrak{p}$ is a prime ideal of the ring of integers of K.

Let $\mathfrak{p}$ be a prime of $\mathbb{Q}^{\text{alg}}$ lying over (p) and let $i : \mathbb{Q}^{\text{alg}} \longrightarrow \mathbb{Q}_p^{\text{alg}}$ be the embedding induced by $\mathfrak{p}$. Recall that the *decomposition group* of $\mathfrak{p}$ is the subgroup of $G(\mathbb{Q})$ defined by

$$G_{\mathfrak{p}} := \{\sigma \in G(\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

It should be pointed out that for another choice of a prime lying over (p) we would get a conjugate of $G_{\mathfrak{p}}$ in $G(\mathbb{Q})$ as the decomposition group. As a consequence of the following theorem, we will show that $G_{\mathfrak{p}} \cong G(\mathbb{Q}_p)$.

Theorem 4.7 ([NSW], p369). $\mathbb{Q}_p^{\text{alg}} = i(\mathbb{Q}^{\text{alg}})\mathbb{Q}_p$.

Proof. It is only necessary to show that $\mathbb{Q}_p^{\text{alg}} \subseteq i(\mathbb{Q}^{\text{alg}})\mathbb{Q}_p$ since the reverse inclusion is trivial. Thus let $\alpha \in \mathbb{Q}_p^{\text{alg}}$ and let f be the minimum polynomial of α over $\mathbb{Q}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, we can choose a polynomial g over $\mathbb{Q}$ that is arbitrarily close to f. Since $\mathbb{Q}_p$ is henselian, Lemma 4.4 applies and $\alpha \in \mathbb{Q}_p(i(\beta_1), \dots, i(\beta_n))$ where $\beta_1, \dots, \beta_n$ are the roots of g in $\mathbb{Q}^{\mathrm{alg}}$. Thus

$$\alpha \in i(\mathbb{Q}(\beta_1, \dots, \beta_n))\mathbb{Q}_p \subseteq i(\mathbb{Q}^{\mathrm{alg}})\mathbb{Q}_p$$

□

For each finite extension K of $\mathbb{Q}$, we have that $G_{\mathfrak{p}_K} \cong \mathcal{G}(i(K)\mathbb{Q}_p/\mathbb{Q}_p)$ where $\mathfrak{p}_K$ is the restriction of $\mathfrak{p}$ to K. We therefore have that $G_{\mathfrak{p}}$ is topologically isomorphic to $\mathcal{G}(i(\mathbb{Q}^{\mathrm{alg}})\mathbb{Q}_p/\mathbb{Q}_p)$. Thus, by the theorem above, we get that $G_{\mathfrak{p}}$ is topologically isomorphic to $G(\mathbb{Q}_p)$.

We will now consider the fixed field of $G_{\mathfrak{p}}$. Recall from [FT, pp 61 and 64] that there is an equivalence between primes and absolute values. We will thus use the notation $|.|_{\mathfrak{p}}$ for the absolute value associated to $\mathfrak{p}$ and we may observe:

Lemma 4.8. *$Fix(G_{\mathfrak{p}})$ is henselian with respect to $|.|_{\mathfrak{p}}$.*

Proof. It is sufficient to show that in any Galois extension K of $Fix(G_{\mathfrak{p}})$ there is only one prime lying over $\mathfrak{p}_{Fix(G_{\mathfrak{p}})}$ (which is defined to be the restriction of $\mathfrak{p}$ to $Fix(G_{\mathfrak{p}})$). We know that $\mathfrak{p}_K$ lies over $\mathfrak{p}_{Fix(G_{\mathfrak{p}})}$. Thus consider some other prime $\mathfrak{q}$ of K that lies over $\mathfrak{p}_{Fix(G_{\mathfrak{p}})}$. Then, by [L, Proposition 11, p12], for some $\sigma \in \mathcal{G}(K/Fix(G_{\mathfrak{p}}))$ we have $\sigma(\mathfrak{p}_K) = \mathfrak{q}$, but $\mathcal{G}(K/Fix(G_{\mathfrak{p}})) = G_{\mathfrak{p}}/N$ for a normal subgroup N of $G_{\mathfrak{p}}$. Therefore $\sigma(\mathfrak{p}_K) = \mathfrak{p}_K = \mathfrak{q}$. □

Furthermore it may be shown that the field $Fix(G_{\mathfrak{p}})$ is elementarily equivalent to $\mathbb{Q}_p$. Such fields (i.e. subfields of $\mathbb{Q}^{\mathrm{alg}}$ elementarily equivalent to $\mathbb{Q}_p$) are called by Ax and Kochen [AK] the *algebraic p-adics.* Koenigsmann [K] and Efrat [Ef] have shown that as $\mathfrak{p}$ ranges over the primes lying over (p) the corresponding fixed fields of $G_{\mathfrak{p}}$ are all the copies of the algebraic p-adics.

By the results of the previous section we can get a good understanding of how the groups $G_{\mathfrak{p}}$ for various primes $\mathfrak{p}$ lie in $G(\mathbb{Q})$.

Lemma 4.9 ([NSW], p663). *Let $\mathfrak{p}$ and $\mathfrak{q}$ be two distinct primes of $\mathbb{Q}^{\mathrm{alg}}$. Then $G_{\mathfrak{p}} \cap G_{\mathfrak{q}} = 1$.*

Proof. We have that $Fix(G_{\mathfrak{p}} \cap G_{\mathfrak{q}})$ is an algebraic extension of $Fix(G_{\mathfrak{p}})$ and $Fix(G_{\mathfrak{q}})$, and hence it is henselian with respect to $|.|_{\mathfrak{p}}$ and $|.|_{\mathfrak{q}}$. Therefore, by Theorem 4.5 we have $Fix(G_{\mathfrak{p}} \cap G_{\mathfrak{q}}) = \mathbb{Q}^{\mathrm{alg}}$. □

Lemma 4.10 ([NSW], p663). *Let $\mathfrak{p}$ be a prime of $\mathbb{Q}^{\mathrm{alg}}$. Then $G_{\mathfrak{p}}$ is its own normaliser in $G(\mathbb{Q})$.*

Proof. Suppose that $\sigma^{-1}G_{\mathfrak{p}}\sigma = G_{\mathfrak{p}}$ for some $\sigma \in G(\mathbb{Q})$. Then $G_{\sigma(\mathfrak{p})} = G_{\mathfrak{p}}$ and hence by the lemma above $\sigma(\mathfrak{p}) = \mathfrak{p}$. Therefore, by definition, $\sigma \in G_{\mathfrak{p}}$. □

We have now established that, for each prime p, there are many copies of $G(\mathbb{Q}_p)$ in $G(\mathbb{Q})$. Any two copies that are distinct have trivial intersection and each copy is its own normaliser.

Let us now recall the structure of $G(\mathbb{Q}_p)$. We have the usual field extensions

$$\mathbb{Q}_p \subset \mathbb{Q}_p^{\text{ur}} \subset \mathbb{Q}_p^{\text{tr}} \subset \mathbb{Q}_p^{\text{alg}}$$

where $\mathbb{Q}_p^{\text{ur}}$ and $\mathbb{Q}_p^{\text{tr}}$ are respectively the maximal unramified and tamely ramified extensions of $\mathbb{Q}_p$. There appears to be no standard notation for the corresponding Galois groups. My conventions shall be:

$$U_p = \mathcal{G}(\mathbb{Q}_p^{\text{ur}}/\mathbb{Q}_p) \qquad T_p = \mathcal{G}(\mathbb{Q}_p^{\text{tr}}/\mathbb{Q}_p^{\text{ur}}) \qquad V_p = \mathcal{G}(\mathbb{Q}_p^{\text{alg}}/\mathbb{Q}_p^{\text{tr}})$$
$$G_p = \mathcal{G}(\mathbb{Q}_p^{\text{alg}}/\mathbb{Q}_p) \qquad \Gamma_p = \mathcal{G}(\mathbb{Q}_p^{\text{tr}}/\mathbb{Q}_p)$$

We show these Galois groups and field extensions in Figure 4.1.

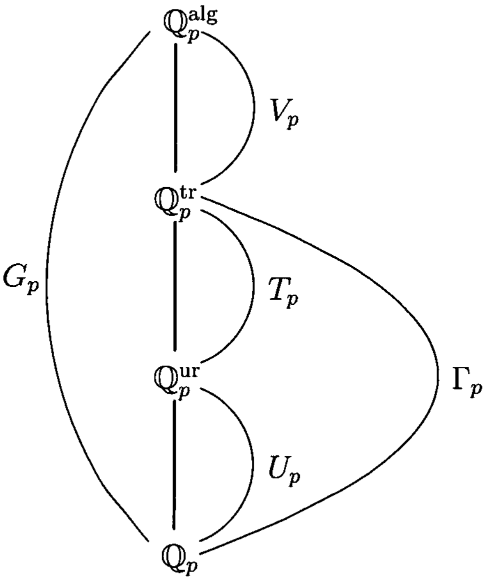

$\mathbb{Q}_p^{\text{alg}}$
V_p
$\mathbb{Q}_p^{\text{tr}}$
G_p
T_p
$\mathbb{Q}_p^{\text{ur}}$
Γ_p
U_p
$\mathbb{Q}_p$

Figure 4.1: *Field extensions of* $\mathbb{Q}_p$ *and their Galois groups*

Recall, from [CF, Corollary, p27], that for an unramified Galois extension L of $\mathbb{Q}_p$ we have an induced Galois extension K of $\mathbb{F}_p$ and vice versa. Furthermore that Galois groups $\mathcal{G}(L/\mathbb{Q}_p)$ and $\mathcal{G}(K/\mathbb{F}_p)$ are isomorphic. Thus, by the properties of the inverse limit, we have the following theorem.

Theorem 4.11 ([CF], Corollary 2, p28). *$U_p = \mathcal{G}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$ is topologically isomorphic to $G(\mathbb{F}_p)$.*

The image of the Frobenius automorphism of $G(\mathbb{F}_p)$ by the isomorphism in Theorem 4.11 is called the Frobenius automorphism (or Frobenius substitution) of U_p [CF, p28].

The following theorem, due to Iwasawa, shows that various phenomena of the Galois group of a finite extension of $\mathbb{Q}_p$ occur (with the natural profinite analogues) in G_p. Iwasawa's version was for all finite extensions of $\mathbb{Q}_p$, but here we shall just state it for $\mathbb{Q}_p$.

Theorem 4.12 ([I], p463). *In the notation above we have:*

(i) Γ_p is isomorphic to the profinite completion of the group generated by two elements σ and τ, satisfying the unique relation

$$\sigma\tau\sigma^{-1} = \tau^p.$$

The isomorphism can be taken such that σ induces the Frobenius automorphism of U_p and τ generates T_p.

(ii) V_p is the pro-p completion ([W], p26) of a free group with a countable number of free generators.

(iii) The group extension G_p of V_p splits.

From part (i) of the theorem above we get that Γ_p is a group extension of T_p which splits (the complement being the subgroup topologically generated by σ). Thus by an abuse of notation we have

$$G_p = (U_p \ltimes T_p) \ltimes V_p$$

and so by Lemma 4.2 we have

$$G_p = U_p \ltimes (T_p \ltimes V_p).$$

For the purposes of the following definition, let us fix a prime $\mathfrak{p}$ in $\mathbb{Q}^{\mathrm{alg}}$ and hence a decomposition group $G_\mathfrak{p}$, which, as we mentioned before, is isomorphic to G_p. Let $\mathbb{A}_\mathfrak{p}$ be its associated algebraic p-adic field. For each extension of $\mathbb{A}_\mathfrak{p}$ there is a corresponding extension of $\mathbb{Q}_p$. Thus we shall say that an extension of $\mathbb{A}_\mathfrak{p}$ is unramified if the corresponding extension of $\mathbb{Q}_p$ is unramified.

Definition 4.13. Let $G_0(Psf_p)$ be the set of conjugacy classes in $G(\mathbb{Q})$ of closed subgroups of $G_\mathfrak{p}$ that correspond to unramified extensions of $\mathbb{A}_\mathfrak{p}$, with the topology given by the subspace topology of the double Vietoris topology of $G(\mathbb{Q})$.

Note that because we have considered conjugacy classes the above definition does not depend on our choice of $\mathfrak{p}$.

Since G_p and $G_{\mathfrak{p}}$ are topologically isomorphic, we shall frequently think of $G_{\mathfrak{p}}$ as having the subgroups U_p, T_p and V_p with the structure from Iwasawa's theorem.

Lemma 4.14. *The space $G_0(Psf_p)$ is closed.*

Proof. Let (X_n) be a convergent sequence in $G_0(Psf_p)$, so that

$$X_i = [U_i \ltimes (T_p \ltimes V_p)]$$

for each i where U_i is a closed subgroup of U_p. We shall show that the limit X is in $G_0(Psf_p)$. Since U_p is closed, by taking a convergent subsequence, we may assume that (U_n) has a limit $U \subset U_p$. Thus by Lemma 4.1 and the proof of Lemma 3.5 we have that (X_n) converges to $[U \ltimes (T_p \ltimes V_p)]$ and we are done. □

Remark 4.15. Let $T \in S_0(Psf_p)$, where $p \neq 2$. Then the sentence

$$\exists x \ x^2 - p = 0$$

will, of course, be in T, but $x^2 - p$ generates a proper (totally ramified) extension of $\mathbb{Q}_p$ (as it is an Eisenstein polynomial). So the roots of $x^2 - p$ are not in any of the extensions between $\mathbb{A}_{\mathfrak{p}}$ and $\mathbb{A}_{\mathfrak{p}}^{\text{ur}}$. Thus we do not have the full correspondence between solvability predicates in our theory and the fixed field of its representative Galois group in $G_0(Psf_p)$ as we did in the previous chapter. This however is not a problem because by Theorem 4.11 we have

$$\mathcal{G}(\mathbb{Q}_p^{\text{ur}}/\mathbb{Q}_p) \cong G(\mathbb{F}_p).$$

Hence it is sufficient to consider the solvability predicates corresponding to unramified extensions.

Theorem 4.16. *$G_0(Psf_p)$ and $S_0(Psf_p)$ are homeomorphic.*

Proof. We first need to establish a bijection. As a consequence of Theorem 4.11, the unramified extensions of $\mathbb{Q}_p$ are in bijective correspondence with the algebraic extensions of $\mathbb{F}_p$. Since $G_{\mathfrak{p}} \cong G_p$ we have established a bijection between the subgroups of $G_{\mathfrak{p}}$ corresponding to unramified extensions of $\mathbb{A}_{\mathfrak{p}}$ and the closed subgroups of $G(\mathbb{F}_p)$, and in Section 1.6, we have shown that there is a bijection between $S_0(Psf_p)$ and the closed subgroups of $G(\mathbb{F}_p)$. Thus we only need to check that two such distinct subgroups X and Y of $G_{\mathfrak{p}}$ cannot be conjugate under the action of $G(\mathbb{Q})$. So suppose that $gXg^{-1} = Y$ for some $g \in G(\mathbb{Q})$. Since $X \subset G_{\mathfrak{p}}$ we have that

$$Y = gXg^{-1} \subset gG_{\mathfrak{p}}g^{-1}$$

but then Lemma 4.9 implies that $gG_{\mathfrak{p}}g^{-1} = G_{\mathfrak{p}}$ and so Lemma 4.10 implies that $g \in G_{\mathfrak{p}}$. However, G_p/T_pV_p is abelian and hence

$$Y = gXg^{-1} = X.$$

The remainder of the proof is now analogous to the proof of Theorem 3.9. We note, however, that by the remark above we need only consider the sentences θ_f for the polynomials f which are irreducible over $\mathbb{Q}_p$ and do not ramify at p. □

4.4 The space $G_0(Psf)$

Definition 4.17. (i) $G_0(Psf_0)$ is the set of conjugacy classes of closed procyclic subgroups of $G(\mathbb{Q})$, that is, $G_0(Psf_0)$ is CSG_C from Section 1.6.

(ii) $G_0(Psf)$ is the union of the spaces $G_0(Psf_p)$ for all primes p and $G_0(Psf_0)$

We have established a bijection for each $G_0(Psf_p)$ with $S_0(Psf_p)$ in the previous section and for $G_0(Psf_0)$ with $S_0(Psf_0)$ in Section 1.6. Moreover the spaces $G_0(Psf_p)$ are disjoint because of Lemma 4.9 and since for each prime p the groups in $G_0(Psf_p)$ are not procyclic, we get that they are disjoint from the groups in $G_0(Psf_0)$. Thus we have established a bijection $\Phi : S_0(Psf) \to G_0(Psf)$ and as mentioned before we will show that Φ is a homeomorphism. There are, however, some preliminary lemmas needed.

Lemma 4.18. *Let (p_n) be an increasing sequence of primes. Then, if the sequence $([T_{p_n} \ltimes V_{p_n}])$ in $G_0(Psf)$ converges it has the trivial group as its limit.*

Proof. Let the closed subgroup X of $G(\mathbb{Q})$ be in the limit. Then by Lemma 2.12 we have for each p_n a $R_{p_n} \in [T_{p_n} \ltimes V_{p_n}]$ such that (R_{p_n}) converges to X. For each p_n, let $\mathbb{A}_{p_n}$ be the copy of the algebraic p-adics such that $R_{p_n} \subset G(\mathbb{A}_{p_n})$.

Let N be an open normal subgroup of $G(\mathbb{Q})$. This corresponds to a finite Galois extension of $\mathbb{Q}$ for which we shall pick a primitive element α. We know that $\mathbb{Q}(\alpha)$ ramifies at only finitely many primes. Thus for large enough p_n we have

$$\mathbb{Q}(\alpha) \subset \mathbb{A}_{p_n}(\alpha) \subset \mathbb{A}_{p_n}^{\text{ur}}$$

and hence $N \supset R_{p_n}$. Therefore $X \subset N$ and since N was arbitrary we have

$$X \subset \bigcap_{N \lhd_\circ G} N = 1$$

where $N \lhd_\circ G$ means that N is an open normal subgroup of G. □

We shall say that $X \in G_0(Psf)$ is of characteristic p if $X \in G_0(Psf_p)$.

Lemma 4.19. *$G_0(Psf)$ is a closed subspace of the double Vietoris space of $G(\mathbb{Q})$.*

Proof. Let (X_n) be a convergent sequence in $G_0(Psf)$. Then the characteristic of (X_n) is either bounded or unbounded.

If the characteristic is bounded then we may pick a subsequence of constant characteristic, say q (where q is possibly 0). Hence by Lemma 4.14 (or Corollary 3.6 if $q = 0$) the limit of the sequence is in $G_0(Psf_q) \subset G_0(Psf)$.

If the characteristic is unbounded then we may pick a subsequence of strictly increasing characteristic. As above we may think of the subsequence in the following way:

$$[U_n \ltimes (T_{p_n} \ltimes V_{p_n})]$$

and by taking a further subsequence we may assume that the sequences $(U_n \ltimes (T_{p_n} \ltimes V_{p_n}))$, (U_n) and $(T_{p_n} \ltimes V_{p_n})$ converge. Then, by Lemma 4.1 and Lemma 4.18, we have that $(U_n \ltimes (T_{p_n} \ltimes V_{p_n}))$ converges to the limit U of the sequence (U_n). Each U_n is procyclic and so, by Lemma 3.2, U is procyclic. By the proof of Lemma 3.5 we get that the limit of $[U_n \ltimes (T_{p_n} \ltimes V_{p_n})]$ is $[U]$. Therefore the limit of (X_n) is in $G_0(Psf_0)$ and we are done. □

Recall that SG is the set of closed subgroups of $G(\mathbb{Q})$ and let SG_C be the conjugacy classes of closed subgroups of $G(\mathbb{Q})$. Recall from Chapter 2 that for a topological space X and open subset U we have that $\langle U \rangle$ is the set of closed sets contained in U and that $\langle X, U \rangle$ is the set of closed sets which have non-trivial intersection with U.

Theorem 4.20. *The map $\Phi : S_0(Psf) \to G_0(Psf)$ defined above is a homeomorphism.*

Proof. By an analogous argument to the first two paragraphs of the proof of Theorem 3.9 it is sufficient to show that if the sequence (T_n) in $S_0(Psf)$ converges to $T \in S_0(Psf)$ and the sequence (X_n) in $G_0(Psf)$, where $X_i = \Phi(T_i)$ for each i, converges to $X \in G_0(Psf)$, then $\Phi^{-1}(X) = T$.

Let p_i be the characteristic of T_i. Because of the base for the topology on $S_0(Psf)$ given in Section 1.1, we can have the following two cases:

Case 1: There is an N such that for all $i > N$, the characteristic of T_i is constant.

Case 2: For every finite prime p there is an N such that for all $i > N$, we have $p_i > p$.

Case 1 has been shown for finite primes in Theorem 4.16 and for characteristic 0 in Theorem 3.9. The proof of Case 2 is very similar to the proof of Theorem 3.9. We first note that T is a characteristic 0 theory and, as we observed in the proof of Theorem 3.9, it is determined by sentences of the form

$$\theta_f \equiv \exists x \; f(x) = 0$$

where f is an irreducible polynomial over the integers.

Suppose that $\theta_f \in T$. Then there is an N such that, for all $i \geq N$, we have $\theta_f \in T_i$ and f does not ramify at p_i (because f will only ramify at finitely many primes). Let α be a root of $f(x)$ and let $H = G(\mathbb{Q}(\alpha))$. We have that H is a clopen set of $G(\mathbb{Q})$ and so $Y := \langle H \rangle \cap SG$ is a clopen subset of SG. Thus

$$B := \langle SG_{\mathcal{C}}, Y \rangle \cap G_0(Psf)$$

is a clopen set of $G_0(Psf)$. Since f does not ramify at p_i, we get

$$\mathbb{A}_{p_i} \subset \mathbb{A}_{p_i}(\alpha) \subset \mathbb{A}_{p_i}^{\mathrm{ur}}$$

for each $i \geq N$ and each copy of $\mathbb{A}_{p_i}$. Hence we have that $X_i \in B$ for every $i \geq N$ and so $X \in B$. Therefore $\theta_f \in \Phi^{-1}(X)$.

Now suppose that $\neg\theta_f \in T$. Since B is open, we have $G_0(Psf) - B$ is closed and the same argument as above shows that $X \in G_0(Psf) - B$. Therefore $\neg\theta_f \in \Phi^{-1}(X)$ and the proof is complete. □

4.5 The space $G_0(ACFA)$

Let $\mathfrak{p}$ be a prime of $\mathbb{Q}^{\mathrm{alg}}$ lying over (p) and let $G_{\mathfrak{p}} \subset G(\mathbb{Q})$ be its decomposition group. As we have explained above, there is a normal subgroup $N_{\mathfrak{p}} \lhd G_{\mathfrak{p}}$ consisting of the automorphisms which fix the maximal unramified extension of $\mathbb{A}_{\mathfrak{p}}$. (The subgroup $N_{\mathfrak{p}}$ was called $T_p \ltimes V_p$ because of the splitting properties of $G_{\mathfrak{p}}$.)

Definition 4.21. (i) $G_0(ACFA_p)$ is the set of conjugacy classes (in $G(\mathbb{Q})$) of cosets of $N_{\mathfrak{p}}$ by elements of $G_{\mathfrak{p}}$.

(ii) $G_0(ACFA_0)$ is the set of conjugacy classes of singleton subsets of $G(\mathbb{Q})$.

(iii) $G_0(ACFA)$ is the union of the spaces $G_0(ACFA_p)$ for each prime p and the space $G_0(ACFA_0)$.

Remark 4.22. As was the case with $G_0(Psf_p)$, because we have taken conjugacy classes the definition of $G_0(ACFA_p)$ does not depend on the choice of p. In the space $G_0(ACFA_0)$ a typical element is $[\{g\}]$ where $g \in G(\mathbb{Q})$. We recall from Lemma 2.7 that $G(\mathbb{Q})$ is homeomorphic to the subspace of $\mathcal{V}(G(\mathbb{Q}))$ consisting of singletons. Thus the space $G_0(ACFA_0)$ is a subspace of $\mathcal{V}(\mathcal{V}(G(\mathbb{Q})))$ which is homeomorphic to $G(\mathbb{Q})_{\mathcal{C}}$.

We now proceed with the familiar sequence of lemmas.

Lemma 4.23. *The space $G_0(ACFA_p)$ is closed.*

Proof. Let (X_n) be a convergent sequence in $G_0(ACFA_p)$. Then, without loss of generality, we may consider $X_i = [g_i N_\mathrm{p}]$, for each i. By taking a convergent subsequence, we may assume that (g_n) converges to some $g \in G$. Then, as in the *Psf* case, we get that (X_n) converges to $[gN_\mathrm{p}] \in G_0(ACFA_p)$. □

Lemma 4.24. *For each p there is a natural homeomorphism from $S_0(ACFA_p)$ to $G_0(ACFA_p)$.*

Proof. By Corollary 3.15, for each p there is a natural homeomorphism from $S_0(ACFA_p)$ to $G(\mathbb{F}_p)$. In the discussion following Theorem 4.7, we showed that G_p is topologically isomorphic to G_p $(= G(\mathbb{Q}_p))$. By Theorem 4.11, we have that $G(\mathbb{F}_p)$ and $U_p = \mathcal{G}(\mathbb{Q}_p^{ur}/\mathbb{Q}_p)$ are topologically isomorphic and after Theorem 4.12 we observed that $U_p \cong G_p/(T_p \ltimes V_p)$. Thus $G_\mathrm{p}/N_\mathrm{p}$ is topologically isomorphic to $G(\mathbb{F}_p)$. Hence, by Lemma 4.9 and Lemma 4.10, we have a natural bijection $\theta : G(\mathbb{F}_p) \to G_0(ACFA_p)$.

We could now proceed as in the proof of Theorem 3.14 but we will show directly that θ is a homeomorphism. By Theorem 2.6 it is sufficient to show that θ is continuous. Thus let A be a closed subset of $G_0(ACFA_p)$ and let (g_n) be a convergent sequence in $\theta^{-1}(A)$ with limit $g \in G(\mathbb{F}_p)$. For each n, let $[k_n N_\mathrm{p}] = \theta(g_n)$ where $k_n \in G_\mathrm{p}$. Since $G(\mathbb{F}_p)$ is topologically isomorphic to $G_\mathrm{p}/N_\mathrm{p}$, we have that $(k_n N_\mathrm{p})$ converges to $kN_\mathrm{p} \in G_\mathrm{p}/N_\mathrm{p}$ where $\theta(g) = [kN_\mathrm{p}]$. Hence by the proof of Lemma 3.5, we have $([k_n N_\mathrm{p}])$ converges to $[kN_\mathrm{p}]$. Since $[kN_\mathrm{p}] \in A$, we have $g \in \theta^{-1}(A)$ and therefore $\theta^{-1}(A)$ is closed. □

Lemma 4.25. *$G_0(ACFA)$ is a closed subspace of the double Vietoris space of $G(\mathbb{Q})$.*

Proof. From the proof of Lemma 4.19 we see that is sufficient to show that if (X_n) is a convergent sequence in $G_0(ACFA)$ of strictly increasing characteristic, then its limit is in $G_0(ACFA)$. For each i, we may think of X_i as $[g_i N_{\mathfrak{p}_i}]$ where $\mathfrak{p}_i$ is a prime of $G(\mathbb{Q})$ lying over the prime corresponding to the characteristic of X_i and $g_i \in G_{\mathfrak{p}_i}$. By taking convergent subsequences, we may assume that the sequences (g_n) and $(N_{\mathfrak{p}_n})$ converge, and then by Lemma 4.18 we get that (X_n) converges to $[\{g\}]$ where g is the limit of (g_n). □

Theorem 4.26. *Let $\Theta : S_0(ACFA) \to G_0(ACFA)$ be the bijection constructed from the bijections for $S_0(ACFA_p)$ and $S_0(ACFA_0)$. Then Θ is a homeomorphism.*

Proof. We have the usual set-up: (T_n) is a sequence in $S_0(ACFA)$ converging to T and (X_n) is the sequence in $G_0(ACFA)$, which converges to X, such that, for each i, we have $X_i = \Theta(T_i)$.

Let p_i be the characteristic of T_i. As in Theorem 4.20, we can have the following two cases:

Case 1: There is an N such that for all $i > N$, the characteristic of T_i is constant.

Case 2: For every finite prime p there is an N such that for all $i > N$, we have $p_i > p$.

Case 1 has been dealt with in Lemma 4.24 and Remark 4.22. In Case 2, T is a characteristic 0 theory and hence is determined by statements of the form

$$\theta_{f,g} \equiv \exists x \ (f(x) = 0 \wedge \sigma(x) = g(x))$$

where f and g are polynomials over $\mathbb{Q}$ and f is the minimum polynomial of the primitive element α of a normal extension of $\mathbb{Q}$ and $g(\alpha)$ is a root of f. As in the proof of Theorem 3.14 we are really considering the sentences

$$\theta'_{f,g} \equiv \exists x \ (rf(x) = 0 \wedge \sigma(sx) = sg(x))$$

where $r, s \in \mathbb{Z}$ are the products of the denominators of the coefficients of the polynomials f, g respectively.

Pick a $\theta_{f,g}$ as described in the previous paragraph. As in the proof of Theorem 3.14 let Y be the clopen set consisting of all the elements of $G(\mathbb{Q})$ such that $\theta_{f,g}$ holds. We know that a general element of $G_0(ACFA)$ may be thought of as $[B]$ where B is a certain coset or a singleton. (The conjugacy classes of cosets will come from $G_0(ACFA_p)$ and the conjugacy classes of singletons will come from

$G_0(ACFA_0)$.) Thus define the clopen set

$$Z := \{[B] \in G_0(ACFA) : B \subset Y\}.$$

Still working with the $\theta_{f,g}$ that we picked in the previous paragraph, there exists an N_0 such that for all $i \geq N_0$, we have that f does not ramify at p_i and p_i does not divide r, s or any of the coefficients of $rf(x)$ and $sg(x)$. Pick some $i \geq N_0$ and let $(K_i, \tau_i) \models T_i$. We now have

$$\begin{aligned} \theta_{f,g} \in T_i &\iff (K_i, \tau_i) \models \theta_{f,g} \\ &\iff (\mathbb{F}_{p_i}^{\mathrm{alg}}, \tau_i|_{\mathbb{F}_{p_i}^{\mathrm{alg}}}) \models \theta_{f,g} \end{aligned}$$

We observed in the proof of Lemma 4.24 that $G_{\mathfrak{p}_i}/N_{\mathfrak{p}_i}$ is topologically isomorphic to $G(\mathbb{F}_{p_i})$. Let $\sigma_i \in G(\mathbb{Q})$ be such that $\sigma_i N_{\mathfrak{p}_i}$ is the image of τ_i under this isomorphism. Then by the properties of this map [CF, p27] we have $(\mathbb{F}_{p_i}^{\mathrm{alg}}, \tau_i|_{\mathbb{F}_{p_i}^{\mathrm{alg}}}) \models \theta_{f,g}$ if, and only if, $(\mathbb{Q}^{\mathrm{alg}}, \sigma_i) \models \theta_{f,g}$. Thus

$$\begin{aligned} \theta_{f,g} \in T_i &\iff (\mathbb{Q}^{\mathrm{alg}}, \sigma_i) \models \theta_{f,g} \\ &\iff \sigma_i \in Y \\ &\iff [\sigma_i N_{\mathfrak{p}_i}] \in Z \end{aligned}$$

But, by the definition of Θ, we have that $\Theta(T_i) = [\sigma_i N_{\mathfrak{p}_i}]$ and so

$$\theta_{f,g} \in T_i \iff X_i = \Theta(T_i) \in Z$$

Therefore

$$\begin{aligned} \theta_{f,g} \in T &\iff \exists N \geq N_0 \text{ such that } \theta_{f,g} \in T_i \text{ for all } i \geq N \\ &\iff \exists N \geq N_0 \text{ such that } X_i \in Z \text{ for all } i \geq N \\ &\iff X \in Z \\ &\iff \theta_{f,g} \in \Theta_0^{-1}(X). \end{aligned}$$

□

Chapter 5

Discussion: coding types

The most important aspect of this work is to give a less syntactic description of the space of complete theories of *Psf* and *ACFA*. Ax described a complete theory of *Psf* by giving a characteristic and the absolute numbers. To give the absolute numbers, however, requires a choice of the algebraic closure of the prime field to be made. We have seen that Ax was really just associating to each complete theory a conjugacy class of procyclic subgroups in the Vietoris space of the absolute Galois group of the prime field. We then saw that this could be taken further to give the complete theories in all characteristics as a subspace of the Vietoris space of $G(\mathbb{Q})$. It is desirable to extend this formulation to types; first, though, I will give a brief definition of types (for more detail see [H]).

A set of formulas in n variables is said to be *finitely satisfiable* if for each finite subset Σ, the sentence $\exists x \bigwedge \Sigma$ has a model. An *n-type* is a maximal finitely satisfiable set of formulas in n variables. For a theory T, the set of n-types of T is denoted $S_n(T)$. It is a Stone space with respect to the topology which has basic clopen sets

$$\{p \in S_n(T) : \varphi(x) \in p\}$$

where $\varphi(x)$ is a formula and x is a tuple of n variables. Note that the space of complete theories of T, which is denoted $S_0(T)$, can be thought of as the space of 0-types of T. Thus, the natural extension of the results in the previous two chapters is to ask whether there is a Galois characterisation of the n-type spaces of *Psf* and *ACFA*.

We will first consider the *Psf* case. To link the n-types with a Galois object, we will use *Galois stratifications.* Galois stratifications were first introduced by Fried and Sacerdote [FS] to show that there is a primitive recursive decision procedure for the theory of finite fields. The ideas of Galois stratifications were then extended by Fried, Haran and Jarden ([FHJ],[FJ]) to a class of fields, which they call Frobenius fields, that includes the class of pseudo-finite fields. I will briefly describe Galois stratifications in terms of the more recent work on Galois stratifications by Denef and Loeser [DL]. This will involve a lot of the language of algebraic geometry for which I refer the reader to [Mum], [EH] or [Ha].

A morphism of schemes $h : C \longrightarrow A$ is a *Galois cover* if

- C and A are reduced, irreducible and normal
- h is étale
- there is a finite group $G(C/A)$, the Galois group, acting on C such that A is isomorphic to the quotient C/G in such a way that h is the composition of the quotient morphism with the isomorphism.

If $A = SpecR$ and $C = SpecS$ are affine then $h : C \longrightarrow A$ is a Galois cover if, and only if, the corresponding extension of the quotient fields of R and S is Galois and in this case $G(C/A)$ is just the Galois group of the quotient field extension. For a variety X we define a *Galois stratification* to be

$$\mathcal{A} = \langle X, h_i : C_i \longrightarrow A_i, Con(A_i) : i \in I \rangle$$

such that the set I is finite, the A_i's form a partition of X and, for each i, the map h_i is a Galois cover and $Con(A_i)$ is a conjugacy class of subgroups of $G(C_i/A_i)$.

Let us now consider a variety X over $Spec\,\mathbb{Z}$. For each prime (p) we will denote the fibre of X at (p) by X_p. We will define the *Artin symbol* $Ar_M(a)$ first for characteristic p and then for characteristic 0. Let M be a field of characteristic p and let X have the Galois stratification $\mathcal{A}$. Let a be an M-rational point of X_p and let $a \in A_{i,p}$. Define $Ar_M(a)$ to be the conjugacy class of subgroups of $G(C_i/A_i)$ consisting of the decomposition subgroups at a. Now let M be a field of characteristic 0 and let a be an M-rational point of X. Let A_i be the stratum such that $a \in A_i$ and define as before $Ar_M(a)$ to be the decomposition subgroups of $G(C_i/A_i)$ at a. We will write $Ar_M(a) \subset Con(\mathcal{A})$ for $Ar_M(a) \subset Con(A_i)$.

Let $\mathcal{A} = \langle \mathbb{A}^{m+n}_{\mathbb{Z}}, h_i : C_i \longrightarrow A_i, Con(A_i) : i \in I \rangle$ be a Galois stratification of $\mathbb{A}^{m+n}_{\mathbb{Z}}$. A Galois formula $\theta(y)$ is an expression of the form

$$Q_1 x_1 \ldots Q_m x_m Ar(x, y) \subset Con(\mathcal{A})$$

where Q_i is either $\forall$ or $\exists$, $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_n)$. We will write $M \models \theta(b)$ if

$$Q_1 x_1 \ldots Q_m x_m Ar_M(x, b) \subset Con(\mathcal{A})$$

where the quantifiers $Q_1, \ldots, Q_m$ range over M.

From [DL] and [FJ] we have the following theorems:

Theorem 5.1. *For each formula $\varphi(y)$ of $\mathcal{L}$, there exists a Galois formula $\theta(y)$ such that for each field M and $a = (a_1, \ldots, a_n) \in M^n$ we have*

$$M \models \varphi(a) \iff M \models \theta(a)$$

Theorem 5.2. *Let $\mathcal{A}$ be a Galois stratification of $\mathbb{A}_{\mathbb{Z}}^{m+n}$ and let $\theta(y)$ be the Galois formula*

$$Q_1 x_1 \ldots Q_m x_m Ar(x, y) \subset Con(\mathcal{A}).$$

Then there exists a $k \in \mathbb{Z}$ and a Galois stratification $\mathcal{B}$ of $\mathbb{A}_{\mathbb{Z}[1/k]}^{m+n}$ such that for every pseudo-finite field M, with $char(M) \nmid k$ and $a \in M^n$, we have

$$M \models \theta(a) \iff Ar_M(a) \subset Con(\mathcal{B}).$$

Thus Galois formulas are an extension of the language of fields and for pseudo-finite fields there is quantifier elimination in Galois formulas.

Let us now return to n-types. Thus let $T \in S_n(Psf)$. It is easy to see that we may define a prime ideal I_T of $\mathbb{Z}[x_1, \ldots, x_n]$ by taking

$$f(x) \in I_T \iff (f(x) = 0) \in T.$$

This ideal will define an irreducible and reduced subscheme of $\mathbb{A}_{\mathbb{Z}}^n$. By normalising, we can get a normal, irreducible and reduced subscheme of $\mathbb{A}_{\mathbb{Z}}^n$. The quantifier elimination for Galois formulas suggests that we should consider conjugacy classes of subgroups of the Galois groups of Galois covers of the normal subscheme. By taking a projective limit, we will obtain a conjugacy class of subgroups of the absolute Galois group of the fraction field of the ring corresponding to the scheme. Thus to each n-type we may attach a normal, irreducible and reduced subscheme of $\mathbb{A}_{\mathbb{Z}}^n$ and a conjugacy class of subgroups of the absolute Galois group of the function field.

Consider the procedure above in the 0-type case (i.e. the case of complete theories). Recall that $\mathbb{A}_{\mathbb{Z}}^0$ is just the prime ideals of $\mathbb{Z}$. So, the prime ideal attached to a given theory will be (p) where p is the characteristic of the theory. Thus as in Chapter 3 we will be associating a theory of Psf to its characteristic and a conjugacy class of subgroups of the absolute Galois group of the prime field.

There is another way of thinking of type spaces. Take the language $\mathcal{L}$ and extend it by the constant symbols $c_1, \ldots, c_n$. Call this new language $\mathcal{L}_{\bar{c}}$. It can be seen that the space of complete theories in $\mathcal{L}_{\bar{c}}$ is the same as the space of n-types in $\mathcal{L}$. Thus to extend the results of Chapter 4 and to code the whole type space it is natural to think in terms of a Galois object associated with $\mathbb{Q}(\overline{X})$ or $\mathbb{Q}[\overline{X}]$. For $\mathbb{Q}(\overline{X})$, the most obvious choice of Galois object is the absolute Galois group and for $\mathbb{Q}[\overline{X}]$, it is the étale fundamental group. (The étale fundamental group of a variety is a projective limit of automorphism groups of Galois covers of the variety, see [Mur] or [Mil].)

We will also need a way of identifying varieties with our Galois object. Recall that in Chapter 4 we associated the characteristic p theories with subgroups of the absolute Galois group of a copy of the algebraic p-adics. In the case of types, as we saw above, it is not just the characteristic that is defined by the quantifier free formulas, it is a variety. Thus, for any given variety, there needs to be a subset of our Galois object that relates to the Galois covers of the variety. These considerations suggest that the Galois object might be a sheaf-like construction made from varieties with their Galois covers.

Let us now consider the type spaces of *ACFA*. I have spent some time working on extending Galois formulas to *ACFA*, but I have yet to find a satisfactory solution. It is, however, known (see [CH, p2998]) that a particular n-type is determined by a σ-ideal and the action of the automorphism on the étale covers of the corresponding variety. We can see that the quantifier elimination for Galois formulas is intimately related to Kiefe's quantifier elimination for pseudo-finite fields in terms of solvability predicates. Macintyre's solvability predicates are a generalisation of Kiefe's and so these give us an idea of the general form of a solution. Thus we will need to consider a variety, its conjugates, a Galois cover and some information relating to σ.

To conclude, here are the problems that have been formulated in the discussion above and which I hope will form the basis of future work:

Problem 1 What are the Galois objects for encoding the type spaces of *Psf* and *ACFA*?

Problem 2 What is the analogue of Galois stratifications for *ACFA*?

Bibliography

[A1] J. Ax. Solving diophantine problems modulo every prime. *Annals of Mathematics* **85**(1967), 161–183.

[A2] J. Ax. The elementary theory of finite fields. *Annals of Mathematics* **88**(1968), 239–271.

[A3] J. Ax. A metamathematical approach to some problems in number theory. *Proceedings of Symposia in Pure Mathematics* **20**(1971), 161–190. 1969 Institute on Number Theory.

[AK] J. Ax and S. Kochen. Diophantine problems over local fields II. *American Journal of Mathematics* **87**(1965), 631–648.

[CF] J. W. S. Cassels and A. Fröhlich, eds. *Algebraic Number Theory*. Academic Press, 1967.

[CK] C. C. Chang and H. J. Keisler. *Model Theory*, volume 73 of *Studies in Logic*. North-Holland, third edition, 1990.

[C1] Z. Chatzidakis. Definable subgroups of algebraic groups over pseudo-finite fields. In *Model theory of groups and automorphism groups (Blaubeuren, 1995)*, volume 244 of *London Mathematical Society Lecture Note Series*, pp. 73–89. Cambridge University Press, 1997.

[C2] Z. Chatzidakis. Model theory of finite fields and pseudo-finite fields. *Annals of Pure and Applied Logic* **88**(1997), 95–108.

[C3] Z. Chatzidakis. Model theory of difference fields lecture notes. Available at `http://www.logique.jussieu.fr/www.zoe/index.html` (6/6/03).

[CH] Z. Chatzidakis and E. Hrushovski. Model theory of difference fields. *Transactions of the American Mathematical Society* **351**(1999), 2997–3071.

[CHP] Z. Chatzidakis, E. Hrushovski, and Y. Peterzil. Model theory of difference fields, II: periodic ideals and the trichotomy in all characteristics. *Proceedings of the London Mathematics Society* **85**(2002) 3, 257–311.

[Co] R. M. Cohn. *Difference Algebra.* Number 17 in Interscience Tracts in Pure and Applied Mathematics. Interscience Publishers, 1965.

[DL] J. Denef and F. Loeser. Definable sets, motives and p-adic integrals. *Journal of the American Mathematical Society* **14**(2000), 429–469.

[Ef] I. Efrat. A Galois-theoretic characterization of p-adically closed fields. *Israel Journal of Mathematics* **91**(1995), 273–284.

[EH] D. Eisenbud and J. Harris. *The Geometry of Schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, 2000.

[FHJ] M. D. Fried, D. Haran, and M. Jarden. Galois stratification over Frobenius fields. *Advances in Mathematics* **51**(1984), 1–35.

[FJ] M. D. Fried and M. Jarden. *Field Arithmetic*, volume 11 of *Modern Surveys in Mathematics*. Springer-Verlag, 1986.

[FS] M. D. Fried and G. Sacerdote. Solving diophantine problems over all residue class fields of a number field and all finite fields. *Annals of Mathematics* **104**(1976), 203–233.

[Fr] O. Frink. Topology in lattices. *Transactions of the American Mathematical Society* **51**(1942), 569 - 582.

[FT] A. Fröhlich and M. J. Taylor. *Algebraic number theory.* Number 27 in Cambridge studies in advanced mathematics. Cambridge University Press, 1991.

[H] M. Hall. *The Theory of Groups*. The Macmillan Company, New York, 1959.

[Ha] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, 1977.

[Ho] W. Hodges. *Model Theory*. Number 42 in Encyclopedia of mathematics and its applications. Cambridge University Press, 1993.

[HZ] E. Hrushovski and B. Zilber. Zariski geometries. *Journal of the American Mathematical Society* **9**(1996), 1–56.

[I] K. Iwasawa. On Galois groups of local fields. *Transactions of the American Mathematical Society* **80**(1955) 2, 448–469.

[J] N. Jacobson. *Lectures in Abstract Algebra*, volume III - Theory of Fields and Galois Theory. Van Nostrand, 1964.

[Jo] P. T. Johnstone. *Stone spaces.* Number 3 in Cambridge studies in advanced mathematics. Cambridge University Press, 1982.

[Ke] J. L. Kelly. *General Topology.* The University Series in Higher Mathematics. D. Van Nostrand Company, Inc., 1955.

[Ki] C. Kiefe. Sets definable over finite fields: Their zeta-functions. *Transactions of the American Mathematical Society* **223**(1976), 45–59.

[K] J. Koenigsmann. From p-rigid elements to valuations (with a Galois-characterization of p-adic fields). *Journal für die reine und angewandte Mathematik* **465**(1995), 165–182.

[L] S. Lang. *Algebraic Number Theory.* Addison-Wesley, 1970.

[LW] S. Lang and A. Weil. Number of points of varieties in finite fields. *American Journal of Mathematics* **76**(1954), 819–827.

[M] A. Macintyre. Generic automorphisms of fields. *Annals of Pure and Applied Logic* **88**(1997), 165–180.

[Mar] D. Marker. *ACFA* seminar. Available at `http://www.math.uic.edu/~marker/` (30/5/03).

[Mi] E. Michael. Topologies on spaces of subsets. *Transactions of the American Mathematical Society* **71**(1951), 152–182.

[Mil] J. S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series.* Princeton University Press, 1980.

[Mum] D. Mumford. *The Red Book of Varieties and Schemes*, volume 1358 of *Lecture Notes in Mathematics.* Springer-Verlag, 1988.

[Mur] J. P. Murre. *Lectures on an introduction to Grothendieck's theory of the fundamental group.* Tata Institute of Fundamental Research, Bombay, 1967.

[NSW] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*, volume 323 of *A Series of Comprehensive Studies in Mathematics*. Springer, 2000.

[Po] B. Poizat. Une preuve d'un théorème de James Ax sur les extensions algébriques de corps. *Comptes Rendus des Séances de l'Academie des Sciences. Series A — Sciences Mathématiques* **291**(1980), 245.

[P] F. Pop. Elementary equivalence versus isomorphism. Notes for a course at the Arizona Winter School in 2003. Available at `http://swc.math.arizona.edu/~swcenter/newaws/03Notes.html` (6/6/03).

[Sh] J. Shoenfield. A theorem on quantifier elimination. *Symposia Mathematica* **V**(1970), 173–176.

[Si] H. Simmons. Existentially closed structures. *Journal of Symbolic Logic* **37**(1972), 293–310.

[V] L. Vietoris. Bereiche zweiter ordnung. *Monatshefte für Mathematik und Physik* **32**(1922), 258–280.

[W] J. S. Wilson. *Profinite Groups*. Number 19 in London Mathematical Society Monographs New Series. Oxford University Press, 1998.

Index