The Fellowship of the Group

Clifton Cunningham

October 13, 2008

Introduction

One Ring to rule them all, One Ring to find them,
One Ring to bring them all and in the darkness bind them
— J. R. R. Tolkien, The Lord of The Rings.

The Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is of the most important objects in mathematics today; the elements of this group are those ring automorphisms of an algebraic closure of the rational numbers that fix every rational number. This group – called the absolute Galois group of $\mathbb{Q}$ – is infinite, non-abelian and comes equipped with a topology; with respect to this topology, this topological group is compact and totally disconnected.

To understand a topological group is to understand its continuous representations (over various fields) and, quite frankly, continuous representations of the absolute Galois group of the rational numbers are not well understood. One-dimensional representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ are quite simple, and tremendous progress has been made recently regarding two-dimensional representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in conjunction with elliptic curves and automorphic representations of $GL(2)$, but in general there are more conjectures than theorems regarding the continuous representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The purpose of this text is to equip the reader with the tools necessary to define the topological group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, understand its one-dimensional representations (called cyclotomic characters), see some examples of irreducible two-dimensional representations (coming from elliptic curves), and understand the definition of the Artin L-functions attached to continuous representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. This is a natural – if somewhat ambitious – objective for a first course in Galois theory, especially for students interested in algebraic number theory. As such, these notes assume a good undergraduate background in groups, rings, topology and category theory (functors, natural transformations, adjunctions, limits and colimits, products and coproducts, push-out and pull-back).

In 1923 Emile Artin explained how to associate a Dirichlet series —

called an *Artin L-function* — to any complex, finite-dimensional continuous representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. You already know one example: the Artin L-function for the trivial representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is the Riemann Zeta function. Artin conjectured that each Artin L-function (the Dirichlet series is easily seen to converge when the real part of the complex variable is sufficiently large) admits unique meromorphic continuation to the entire complex plane. Although some instances of this conjecture have been proved, the full conjecture remains an open problem to this day.

The Artin conjecture is related to a series of conjectures made by Robert Langlands in 1966 — affectionately known as the *Langlands Programme* every since — which predicts a relation between Galois representations and automorphic representations. The relation is through L-functions: Artin L-functions, in the case of Galois representations, and automorphic L-functions, in the case of automorphic representations.

Number theorists used to boast that they were safe from the vagaries of mathematical fashion, as no applications of the subject could possibly be found. This absurd claim was certainly meant to be provocative, but it was rendered rediculous when the proof of Fermat's Last Theorem lead to new cryptosystems which are now, only a few years later, ubiquitous in information security. This has not gone unnoticed, and cryptography research groups have sprung up around the world, with programs attracting significant numbers of talented students interested in applications of number theory to information security. These students need a course in Galois theory which will allow them to read research papers in Galois representations and L-functions, which are basic objects in modern number theory.

At the same time, many students of pure mathematics have been electrified by the progress in number theory in recent years, including, but not limited to, the proof of the Shimura-Tanyama-Weil conjecture. Many of these students sense - correctly - that the Langlands Program provides a unifying framework with which to understand this work and from which to attack open problems. These students need a course in Galois theory which will give them tools to eventually understand how certain Galois representations parametrize L-packets of automorphic representations.

Standard introductory textbooks in Galois theory serve neither group of students by dwelling on classical aspects of Galois theory, since these results do little to explain why ℓ-adic representations of the absolute Galois group over the rational numbers are some of the most important and mysterious objects in mathematics today. Indeed, most introductory courses in Galois theory include neither the ℓ-adic numbers, the absolute Galois group over the rational numbers, nor the topology necessary to define Galois represen-

tations.

By contrast, this text is intended to appeal to readers looking for a fairly direct route to Galois representations, and is unapologetically ahistorical. In this course, the reader will find no treatment of the hallowed topics of Galois theory such as soluble polynomials or compass and straightedge constructions. These are indeed lamentable lacunae, but the classical topics are treated very well in existing introductory literature. Moreover, this omission seems as small price to pay in order to be able to go directly to the central concepts and principles necessary to study Galois representations.

The result is a treatment of Galois theory with three defining features.

Categorical. Galois theory straddles two categories and therefore, at its heart, concerns functors and natural transformations. In this course, the term 'Galois extension' is defined in terms of an adjoint pair of functors. We do not, however, assume any great familiarity with category theory apart from the very basic definitions; all other concepts and results needed from category theory are provided in the text. As a result, this course provides an introduction to category theory at the same time that it introduces Galois theory, by considering an important adjoint pair of functors. We also make a fairly detailed study of limits and colimits (over various categories) of these functors. Adjoint functors, limits and colimits are ubiquitous in modern mathematics and these students will benefit from early exposure to these central concepts.

Topological. Every Galois group is a *topological* group. In this course, the main theorems are stated and proved for arbitrary Galois extensions, not just finite Galois extensions. Of course, there are many excellent elementary treatments of Galois theory which include infinite Galois extensions, but for the most part they begin by studying the finite theory and then treating infinite Galois extensions as a sort of add-on. By contrast, we incorporate infinite Galois extensions into the discussion from the very beginning, and the big theorems in this course (such as the 'Galois is Normal and Separable' Theorem, and the Fundamental Theorem of Galois Theory) are stated and proved in that context. This is made possible by extensive use limits and colimits over various categories.

Arithmetical. As indicated above, our ultimate goal is to provide students, as efficiently as possible, with the machinery necessary to study Galois representations and associated L-functions. This is the

third and most important defining feature of our treatment of Galois theory. This course introduces the inertia and decomposition subgroups of the absolute Galois groups of number fields, and also provides some simple examples of ℓ-adic Tate modules for curves, together with the action of the absolute Galois group on these modules. In this way we produce explicit examples of some important one- and two-dimensional ℓ-adic representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Galois Theory is an old subject with a dramatic history reaching back into antiquity, but the future of Galois theory is certain to rival the glory of its past. Despite the recent breakthroughs in the construction and properties of Galois representations and related automorphic representations, much work remains to be done. Discussions of Galois groups as internal symmetry groups and Pierre Cartier's cosmic galois group, together with the ever tightening connections between number theory and physics though modular forms and moonshine, suggest that Galois theory may one day play an important role in physics too. Work in these areas will require many people, and it is our hope that these notes will help recruit new students to these burgeoning fields.

Whatever the future of Galois Theory, one thing is clear: Frodo's ring is actually a group — the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Welcome to the Fellowship of the Group.

My profound thanks to Claude Laflamme and his 'circle-tastic' Galois theory students 2008 for their help improving these notes. Many thanks also to Robin Cockett.

Contents

1 The Galois adjunction **11**
- 1.1 A field guide to fields . . . 11
- 1.2 Subfields and subgroups . . . 14
- 1.3 The Galois correspondence . . . 15
- 1.4 The Galois adjunction . . . 17
- 1.5 Chapter 1 exercises . . . 20

2 Galois extensions **23**
- 2.1 Kaplansky subfields . . . 23
- 2.2 Algebraic extensions . . . 24
- 2.3 Galois extensions . . . 28
- 2.4 Chapter 2 exercises . . . 29

3 Finite Extensions **31**
- 3.1 Finite extensions . . . 31
- 3.2 Dedekind-Artin Theorem . . . 33
- 3.3 Chapter 3 exercises . . . 36

4 Simple Extensions **39**
- 4.1 Simple extensions . . . 39
- 4.2 Finite simple extensions . . . 40
- 4.3 Relative algebraic closure . . . 41
- 4.4 Factoring homomorphisms by simple extensions . . . 42
- 4.5 Universal property of simple extensions . . . 43
- 4.6 Chapter 4 exercises . . . 45

5 Profinite Extensions **47**
- 5.1 Finitely generated extensions . . . 47
- 5.2 Profinite extensions . . . 49
- 5.3 Chapter 5 exercises . . . 51

6 Profinite groups **53**
6.1 Profinite groups . . . 53
6.2 Galois groups are profinite . . . 54
chapter: profinite groups
6.3 Chapter 6 exercises . . . 55

7 Splitting Extensions **57**
7.1 Splitting extensions . . . 57
7.2 Another perspective on splitting extensions . . . 58
7.3 Factoring homomorphisms by finite splitting extensions . . . 59
7.4 Existence of finite splitting extensions . . . 61
7.5 General splitting extensions . . . 61
7.6 Absolute Algebraic closures . . . 63
chapter: splitting extensions
7.7 Chapter 7 exercises . . . 65

8 Normal Extensions and the Restriction Theorem **67**
8.1 Normal extensions . . . 67
8.2 An exact sequence . . . 68
8.3 Restriction . . . 69
chapter: normal extensions
8.4 Chapter 8 exercises . . . 70

9 Separable extensions **71**
9.1 Separable extensions . . . 71
chapter: separable extensions
9.2 Chapter 9 exercises . . . 72

10 Galois iff Normal and Separable **73**
10.1 Galois iff Normal and Separable . . . 73
chapter: Galois iff normal and separable
10.2 Chapter 10 exercises . . . 76

11 The Fundamental Theorem **79**
11.1 The Krull topology . . . 79
11.2 Galois (topological) groups . . . 81
11.3 Closed subgroups . . . 82
11.4 The Fundamental Theorem . . . 84
11.5 The Galois Equivalence . . . 86
chapter: FTGT
11.6 Chapter 11 exercises . . . 87

12 Some Important Galois Groups **91**
12.1 The Pruffer ring . . . 91
12.2 Some subgroups of the absolute Galois group of finite fields . 97
12.3 Some subgroups of the absolute Galois group of the Rationals 100
12.4 p-adic numbers . . . 103

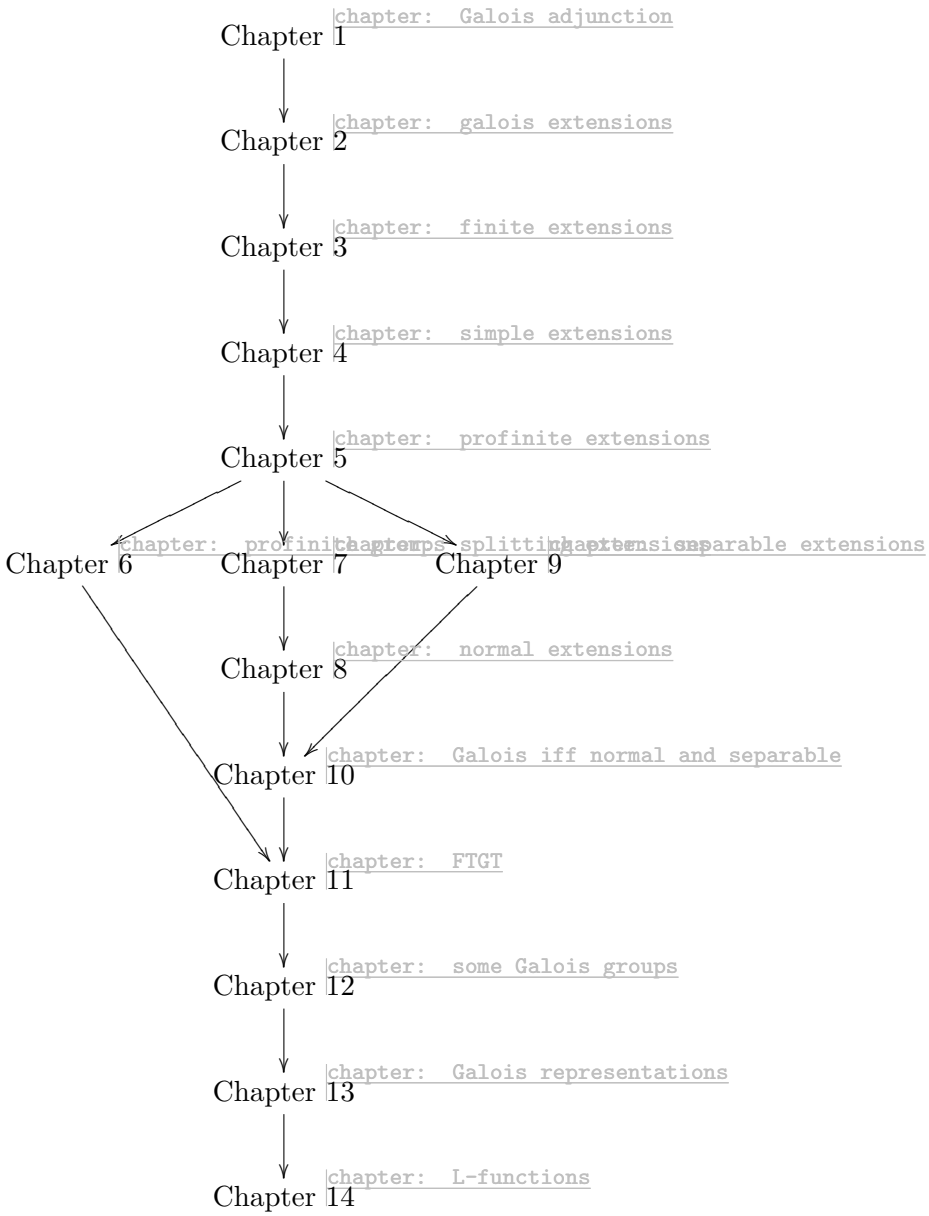
12.5 Decomposition subgroups . . . 106
12.6 Inertia subgroups . . . 107
chapter: some Galois groups
12.7 Chapter 12 exercises . . . 108

13 Galois Representations **109**
13.1 Ramification . . . 109
13.2 Cyclotomic characters . . . 109
13.3 Tate module of the multiplicative group . . . 110
13.4 The Tate module of an elliptic curve . . . 112
13.5 ℓ-adic representations . . . 112
13.6 Complex representations . . . 112
chapter: Galois representations
13.7 Chapter 13 exercises . . . 112

14 Artin L-functions **113**

15 Solutions **115**
chapter: Galois adjunction
15.1 Chapter 1 solutions . . . 115
chapter: galois extensions
15.2 Chapter 2 solutions . . . 121
chapter: finite extensions
15.3 Chapter 3 solutions . . . 121
chapter: simple extensions
15.4 Chapter 4 solutions . . . 121
chapter: profinite extensions
15.5 Chapter 5 solutions . . . 122
chapter: splitting extensions
15.6 Chapter 7 solutions . . . 123
chapter: normal extensions
15.7 Chapter 8 solutions . . . 124
chapter: separable extensions
15.8 Chapter 9 solutions . . . 124
chapter: profinite groups
15.9 Chapter 6 solutions . . . 126
chapter: FTGT
15.10 Chapter 11 solutions . . . 126
chapter: some Galois groups
15.11 Chapter 12 solutions . . . 133
chapter: Galois representations
15.12 Chapter 13 solutions . . . 134
chapter: L-functions
15.13 Chapter 14 solutions . . . 136

Lietfaden


chapter: Galois adjunction
Chapter 1
chapter: galois extensions
Chapter 2
chapter: finite extensions
Chapter 3
chapter: simple extensions
Chapter 4
chapter: profinite extensions
Chapter 5
chapter: profinite groups
Chapter 6
chapter: splitting fields
Chapter 7
chapter: separable extensions
Chapter 9
chapter: normal extensions
Chapter 8
chapter: Galois iff normal and separable
Chapter 10
chapter: FTGT
Chapter 11
chapter: some Galois groups
Chapter 12
chapter: Galois representations
Chapter 13
chapter: L-functions
Chapter 14

Chapter 1

The Galois adjunction

Galois adjunction

1.1 A field guide to fields

First things first: What is a field?

Definition 1 *A field is a non-zero commutative ring with identity in which every non-zero element is a unit.*

In this section we look at some equivalent characterizations of fields.

position: ideals

Proposition 1 *Let A be a non-zero commutative ring with identity. Then A is a field if and only if (0) and A are the only ideals of A.*

Proof. (Observe that $(0) = \{0\}$.) Let A be a field. Suppose I is an ideal of A and $I \neq (0)$. Then I contains a non-zero element, say a. Then $(a) \subseteq I$. Since A is a field and a is non-zero, it is a unit, so $(a) = A$. Thus, $I = A$.

Conversely, let A be a non-zero commutative ring with identity such that (0) and A are the only ideals of A. Let a be a non-zero element of A. Then (a) is not the trivial ideal (0), and thus $(a) = A$. In particular, $1 \in (a)$, whence $ab = 1$ for some $b \in A$. We have shown that every non-zero element of A is a unit, and thus that A is a field. ■

Our next characterization of fields requires a definition: for an arbitrary commutative ring with identity, let $\mathrm{Specm}(A)$ denote the set of maximal ideals of A. This is commonly referred to as the maximal ideal spectrum of A.

n: maximal ideals

Proposition 2 *Let A be a non-zero commutative ring with identity; then A is a field if and only if* $\mathrm{Specm}(A) = \{(0)\}$.

Proof. Suppose A is a field. By Proposition 1, A has exactly two ideals: (0) and A itself. Thus, $\mathrm{Specm}(A) = \{(0)\}$.

Conversely, suppose A is a non-zero commutative ring with identity and $\mathrm{Specm}(A) = \{(0)\}$. Let $a \in A$ be a non-zero element of A. Then the ideal (a) generated by a is not the zero ideal. Since $(0) \subset (a)$ and (0) is maximal, it follows that $(a) = A$. In particular, $1 \in (a)$, in which case $1 = ab$ for some $b \in A$. Thus a is a unit. We have shown that every non-zero element of A is a unit, and thus that A is a field. ■

In fact, we can improve this result, if we assume Zorn's lemma, as we shall do. The next proposition will not be used very often in these notes, but it does makes clear just how thoroughly we adopt Zorn's lemma. Let $\mathrm{Spec}(A)$ denote the set of prime ideals of A; this is commonly referred to as the prime ideal spectrum of A. Recall that $\mathrm{Specm}(A) \subseteq \mathrm{Spec}(A)$ when A is a cring.

Proposition 3 *Let A be a non-zero commutative ring with identity; then A is a field if and only if* $\mathrm{Spec}(A) = \{(0)\}$.

Proof. Suppose A is a field. Then $\mathrm{Specm}(A) = \{(0)\}$, by Proposition 2. Since $\mathrm{Specm}(A) \subset \mathrm{Spec}(A)$ and since there are no other proper ideals of A (by Proposition 1), $\mathrm{Spec}(A) = \{(0)\}$.

Conversely, suppose A is a non-zero commutative ring with identity and $\mathrm{Spec}(A) = \{(0)\}$. Since $\mathrm{Specm}(A) \subseteq \mathrm{Spec}(A)$ it follows that either $\mathrm{Specm}(A)$ is empty or $\mathrm{Specm}(A) = \{(0)\}$. The first case contradicts Zorn, which is equivalent to the Axiom of Choice and which we accept in this course, so $\mathrm{Specm}(A) = \{(0)\}$. Now it follows from Proposition 2 that A is a field. ■

Henceforth we use the term cring for a commutative ring with identity, and cring homomorphism for a ring homomorphism between crings which maps the identity of the domain to the identity of the codomain.

Let CRING denote the category of crings and let FIELD denote the category of fields; thus, in FIELD, objects are fields, maps are cring homomorphisms between fields, composition is given by function composition and identities are identity functions. If K and L are fields, then

$$\mathrm{Hom}_{\mathrm{FIELD}}(K, L) = \mathrm{Hom}_{\mathrm{CRING}}(K, L).$$

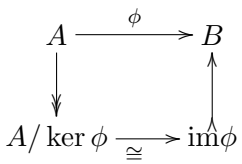
Thus, the category of fields is a *full subcategory* of the category of crings.

Our final proposition in this section comes from thinking more closely about homomorphisms. Proposition 4 goes straight to the heart of the matter and reveals a special feature of the category of fields: all homomorphism are injective!

tion: injections

Proposition 4 *Let A be a non-zero commutative ring with identity. Then A is a field if and only if, for every non-zero cring B, every homomorphism $A \to B$ is injective.*

Proof. Suppose A is a field. Let B be a non-zero cring. Suppose $\phi \in \mathrm{Hom}_{\mathrm{CRING}}(A, B)$. The First Isomorphism Theorem (FIT) gives the following commutative diagramme.



Now $\ker\phi$ is an ideal of A, and A is a field, so $\ker\phi = (0)$ or $\ker\phi = A$, by Proposition 1. Suppose, for a contradiction, that $\ker\phi = A$. Then the ring $A/\ker\phi$ is the zero ring, so $\mathrm{im}\phi$ is $\{0\}$. In particular, $\phi(1_A) = 0_B$. From the definition of maps in cring we see that this is possible only if $0_B = 1_B$, in which case B is the zero ring. This is the desired contradiction, showing that $\ker\phi = (0)$. It follows immediately that ϕ is injective.

proposition: ideals

Conversely, suppose A is a non-zero cring such that $\mathrm{Hom}_{\mathrm{CRING}}(A, B)$ consists entirely of injections, for every non-zero cring B. Suppose, for a contradiction, that A is not a field. Then, by Proposition 1 A has a non-zero proper ideal I. Let $B = A/I$. Since I is proper, this is a non-zero cring. Consider the quotient map $\phi : A \to A/I$. Since $\ker\phi = I$ is non-zero, ϕ is not a injective. This is the desired contradiction, showing that A is a field. ■

proposition: ideals

proposition: injections

Proposition 4 shows that every map of fields may be factored as an isomorphism followed by an inclusion. This means that if one is willing to pass from the category of fields to the category of fields up to isomorphism,[1] then one may view every map as an inclusion. It is common in the literature to do exactly that, and consequently to regard any homomorphism of fields $K \to L$ as an inclusion. We will *not* proceed that way in this course, unless indicated otherwise. In particular, we use the term extension to refer to any homomorphism of fields; consequently, in this course, the terms 'extension', 'field homomorphism' and 'subfield' are synonymous.

There is something to be gained by not working in the category of fields up to isomorphism; after all, every isomorphism of fields is an identity in

[1] This is an example of a category obtained by so-called localization; the category of fields up to isomorphism is the category obtained by localizing the category of fields by isomorphisms.

the category of fields up to isomorphism, so automorphism groups are particularly boring if we pretend all fields homomorphisms are inclusions. On the other hand, there is something to be lost by resisting the urge to treat all field homomorphisms as though they were inclusions: the extra notation required is a bit cumbersome and potentially distracting. Nonetheless, we have decided that precision outweighs convenience and consequently will fastidiously work in the category of fields, unless explicitly indicated otherwise.

1.2 Subfields and subgroups

Let Y be an object in an arbitrary category. Let SUB(Y) denote the category of subobjects of Y; thus, an object in SUB(Y) is a monic (see Exercise 1.10) with codomain Y (*i.e.,* a monic map $\alpha : X \to Y$ in the ambient category), and a map from $\alpha : X \to Y$ to $\beta : X' \to Y$ in SUB(Z) is a commutative triangle

exercise: monic

(1.1)

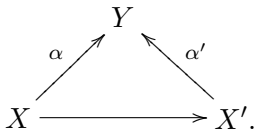


diagramme: map-L

Composition in SUB(Y) is indicated by the diagramme,

(1.2)

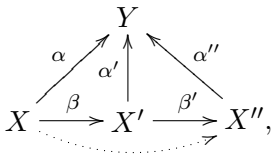
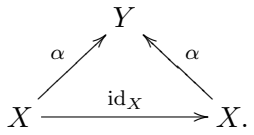


diagramme: compos

and the identity $\mathrm{id}_{\alpha:X\to Y}$ is the triangle

(1.3)



Notice that there is an obvious forgetful functor from SUB(Y) to the ambient category, taking $\alpha : X \to Y$ to X and taking the 'triangle' $X \to X' \to Y$ to $X \to X'$. For obvious reasons, it is common to make implicit use of this functor.

In this course we need two cases of this construction. For any field L, the category of subfields of L is the category in which: objects are subfields of L, which is to say, field homomorphisms $\alpha : K \to L$; and maps from the subfield $\alpha : K \to L$ to the subfield $\alpha' : K' \to L$ are field homomorphisms $\beta : K \to K'$

such that $\alpha = \alpha' \circ \beta$. Proposition 4 shows that every field homomorphism is injective, and in Exercise 1.10 you will show that every injective field homomorphism is monic in the category FIELD and every monic in FIELD is injective. Consequently, the category of subfields of L is precisely $\mathrm{SUB}(L)$, for any field L. The category $\mathrm{SUB}(L)$ will be of primary importance in this course.

We will also make extensive use of the category of subgroups of G, for certain groups G. In Exercise 1.10 you will also show that every injective group homomorphism is monic in the category of groups and every monic in the category of groups is injective. Thus, the category of subgroups of G is precisely $\mathrm{SUB}(G)$, for any group G. We will work extensively with the category $\mathrm{SUBAut}(L)$, where L is a field.

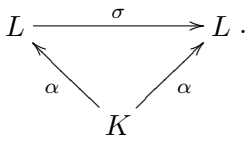
1.3 The Galois correspondence

The Galois correspondence is a pair of contravariant functors, one from $\mathrm{SUB}(L)$ to $\mathrm{SUBAut}(L)$, and the other functor in the opposite direction. In this section we define these functors; in the next section we show that they form an adjoint pair of contravariant functors. Throughout this section, L is a fixed but arbitrary field.

Let $\alpha : K \to L$ be a subfield. The group $\mathrm{Aut}(L/K)$ of automorphisms of L over K (commonly denoted $\mathrm{Aut}_K(L)$) is defined by

$$\mathrm{Aut}(L/K) = \left\{ \sigma \in \mathrm{Aut}(L) \;\middle|\; \sigma \circ \alpha = \alpha \right\}.$$

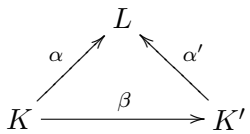
Observe that $\mathrm{Aut}(L/K)$ is the subgroup of $\sigma \in \mathrm{Aut}(L)$ such that the following diagramme commutes.



Definition 2 *Let L be a fixed but arbitrary field. Let*

$$\mathrm{Aut}(L/\ ) : \mathrm{SUB}(L) \to \mathrm{SUBAut}(L)$$

be the contravariant functor taking $\alpha : K \to L$ to $\mathrm{Aut}(L/K) \hookrightarrow \mathrm{Aut}(L)$ and taking



(1.4)

to

$$\begin{array}{ccc} & \mathrm{Aut}(L) & \\ \nearrow & & \nwarrow \\ \mathrm{Aut}(L/K') & \longrightarrow & \mathrm{Aut}(L/K) \end{array} \tag{1.5}$$

where each arrow is inclusion. We also use the notation $\mathrm{Aut}(L/\alpha)$ *for* $\mathrm{Aut}(L/K) \hookrightarrow \mathrm{Aut}(L)$. *We refer to* $\mathrm{Aut}(L/\ )$ *as the automorphism functor (for* L*).*

To be sure, this definition is premature — we really should show that the automorphism functor really does define a contravariant functor. Instead, this is left as an exercise (Exercise 1.19) with the promise that it is really quite simple, and give an example instead.

exercise: Galois functor

Next, we define a functor from $\textsc{subAut}(L)$ to $\textsc{sub}(L)$. Let $\varphi : H \to \mathrm{Aut}(L)$ be an object in the category of subgroups of $\mathrm{Aut}(L)$; thus, $\varphi : H \to \mathrm{Aut}(L)$ is an injective group homomorphism. Let L^H be the field of elements of L fixed by the action of H (or the fix of H in L, for short) given by $\varphi : H \to \mathrm{Aut}(L)$; thus,

$$L^H := \{u \in L \mid \varphi(h)(u) = u, \forall h \in H\}.$$

Since L^H is a subfield of L, L^H is an object in $\textsc{sub}(L)$.

definition: fix functor

Definition 3 *Let* L *be a fixed but arbitrary field. Let*

$$\mathrm{Fix}(\ /L) : \textsc{subAut}(L) \to \textsc{sub}(L)$$

be the contravariant functor sending the object $\varphi : H \to \mathrm{Aut}(L)$ *in* $\textsc{subAut}(L)$ *to* $L^H \hookrightarrow L$ *and sending the map*

$$\begin{array}{ccccc} & & \mathrm{Aut}(L) & & \\ & \nearrow^{\varphi} & & \nwarrow_{\varphi'} & \\ H & & \xrightarrow{\psi} & & H' \end{array}$$

in $\textsc{subAut}(L)$ *to*

$$\begin{array}{ccc} & L & \\ \nearrow & & \nwarrow \\ L^{H'} & \longrightarrow & L^H, \end{array}$$

where the group homomorphisms are all inclusions. We will sometimes write $\mathrm{Fix}(\varphi/L)$ *for* $L^{\mathrm{dom}\varphi} \hookrightarrow L$ *will refer to* $\mathrm{Fix}(\ /L)$ *as the fix functor (for* L*).*

Again, this definition should be preceded by the work necessary to see that it makes sense; fortunately, the required work is quite straightforward (Exercise 1.20).

1.4 The Galois adjunction

Definition 4 *The Galois functors for L is the pair of contravariant functors $(\mathrm{Aut}(L/\ ), \mathrm{Fix}(\ /L))$ consisting of the automorphism functor for L and the fix functor for L (see Definitions 2 and 3).*

Having just defined the Galois functors,

$$\mathrm{SUB}(L) \underset{\mathrm{Aut}(L/\ )}{\overset{\mathrm{Fix}(\ /L)}{\rightleftarrows}} \mathrm{SUB}\mathrm{Aut}(L),$$

it is natural to consider the result of composing these functors. While the functors $\mathrm{Aut}(L/\ )$ and $\mathrm{Fix}(\ /L)$ are not equivalences, they are closely related, as we shall now see.[2]

Proposition 5 *The Galois functors form an adjoint pair of contravariant functors.*

Proof. Fix L (a field). We begin by defining a natural transformation

$$\eta_L : \mathrm{id}_{\mathrm{SUB}(L)} \to \mathrm{Fix}(\ /L) \circ \mathrm{Aut}(L/\ ),$$

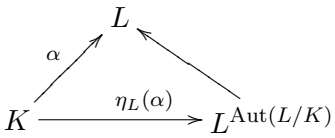
where $\mathrm{id}_{\mathrm{SUB}(L)}$ denotes the identity functor on the category of subfields of L. Let $\alpha : K \to L$ be a subfield of L. Then

$$\begin{aligned} (\mathrm{Fix}(\ /L) \circ \mathrm{Aut}(L/\ ))(K) &= \mathrm{Fix}(\ /L)(\mathrm{Aut}(L/K)) \\ &= L^{\mathrm{Aut}(L/K)}. \end{aligned}$$

Compare this with $\mathrm{id}_{\mathrm{SUB}(L)}(K) = K$. Recall that $\sigma \in \mathrm{Aut}(L/K)$ implies $\sigma \circ \alpha = \alpha$, in which case $\sigma(\alpha(u)) = \alpha(u)$ for each $u \in K$. Thus, the image of

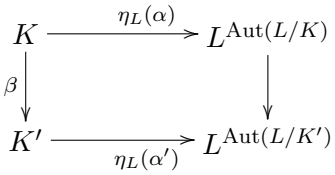
[2] From the reaction of the class to this proposition, it is clearly very important to include the definition of 'adjoint pair of contravariant functors' in the (still missing) 'Appendix on Category Theory'.

$\alpha : K \to L$ is actually contained in $L^{\mathrm{Aut}(L/K)}$. With this in mind, let $\eta_L(\alpha)$ be the map of subfields of L given by the triangle



$$u \longmapsto \alpha(u).$$

To see that η_L is a natural transformation, observe that the following diagramme commutes if $\beta : K \to K'$ is a map of subfields from $\alpha : K \to L$ to $\alpha' : K' \to L$, in which case $\alpha = \alpha' \circ \beta$.



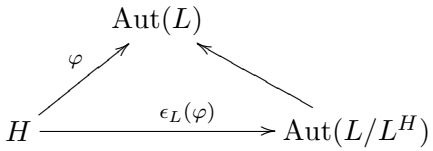
Next, we define a natural transformation

$$\epsilon_L : \mathrm{id}_{\mathrm{SUBAut}(L)} \to \mathrm{Aut}(L/\ ) \circ \mathrm{Fix}(\ /G),$$

where $\mathrm{id}_{\mathrm{SUBAut}(L)}$ denotes the identity functor in $\mathrm{SUBAut}(L)$. Let $\varphi : H \to \mathrm{Aut}(L)$ be a subgroup. Then

$$\begin{aligned}(\mathrm{Aut}(L/\ ) \circ \mathrm{Fix}(\ /L))(H) &= \mathrm{Aut}(L\ )(L^H) \\ &= \mathrm{Aut}(L/L^H)\end{aligned}$$

Now, let $\epsilon_L(\varphi)$ be the map (in the category of subgroups of $\mathrm{Aut}(L)$) from $\varphi : H \to \mathrm{Aut}(L)$ to $\mathrm{Aut}(L/L^H) \to \mathrm{Aut}(L)$ given by the triangle



$$h \longmapsto \varphi(h)$$

We leave it to the reader to demonstrate that ϵ_L, just defined, is indeed a natural transformation.

Now, we must show that the natural transformations η_L and ϵ_L satisfy an important property. For every subfield K of L.

$$\mathrm{Aut}(L/K) = \mathrm{Aut}(L/L^{\mathrm{Aut}(L/K)})$$

It follows that the natural transformation η_L induces an isomorphism of functors

$$\mathrm{Aut}(L/\ ) \cong \mathrm{Aut}(L/\ ) \circ \mathrm{Fix}(\ /L) \circ \mathrm{Aut}(L/\ ).$$

Likewise, because

$$L^H = L^{\mathrm{Aut}(L/L^H)}$$

for every subgroup $H \to \mathrm{Aut}(L)$, the natural transformation ϵ_L induces an isomorphism of functors

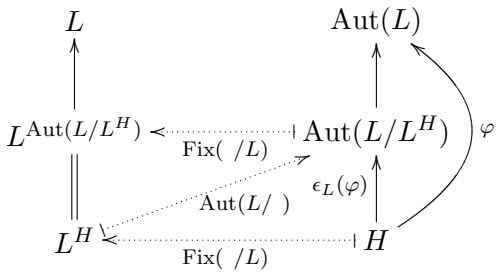
$$\mathrm{Fix}(\ /L) \cong \mathrm{Fix}(\ /L) \circ \mathrm{Aut}(L/\ ) \circ \mathrm{Fix}(\ /L)$$

The details are left to the reader (there is a lot of detail missing in this proof). ■

proposition: adjunction

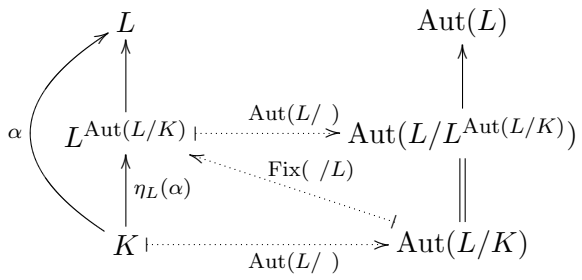
Proposition 5 has important consequences, as any adjoint pair establishes an *equivalence* of certain closely associated categories, as we shall see in the next section. Before moving on, let us recapitulate one more time by drawing a diagramme to represent what we have just learned:

$\mathrm{SUB}(L)$ $\mathrm{SUB}\mathrm{Aut}(L)$



and

$\text{SUB}(L)$ $\text{SUB}\text{Aut}(L)$



chapter: Galois adjunction

1.5 Chapter 1 exercises

: integral domain vs field

Exercise 1.1 *Let A be a cring. Prove: If A is a field, then A contains no zero-divisors. Is the converse true? More precisely, if A is a non-zero cring and A has no zero divisors, does it follow that A is a field? What if A is finite?*

exercise: zero field

Exercise 1.2 *Is the zero ring a cring? Let A be a cring. Show that $1_A = 0_A$ if and only if A is the zero ring. Is the cring 0 a field?*

exercise: Specm

Exercise 1.3 *Recall that every maximal ideal is prime, so $\text{Specm}(A) \subseteq \text{Spec}(A)$. Can you find an example of a cring for which this inclusion is an equality? Can you find an example of a cring for which this inclusion is strict?*

exercise: Spec

Exercise 1.4 *If K is a field then $\text{Spec}(K) = \{(0)\}$, so the set of prime ideals of K is a singleton. Is the converse true? More precisely, if A is a non-zero cring and $\text{Spec}(A)$ is a singleton, does it follow that A is a field?*

exercise: Spec K[x]

Exercise 1.5 *If K is a field then $\text{Spec}(K[x]) = \text{Specm}(K[x]) \cup \{(0)\}$. Let A be a non-zero cring. If $\text{Spec}(A[x]) = \text{Specm}(A[x]) \cup \{(0)\}$, does it follows that A is a field?*

exercise: prime

Exercise 1.6 *Let $\phi : A \to B$ be a cring homomorphism. Suppose $\mathfrak{p}$ is a prime ideal of B. Show that $\phi^{-1}\mathfrak{p}$ is a prime ideal of A. Define $\text{Spec}(\phi) : \text{Spec}(B) \to \text{Spec}(A)$ by $\text{Spec}(\phi)(\mathfrak{p}) = \phi^{-1}\mathfrak{p}$. Show that this defines a contravariant functor from the category of crings to the category of sets. (This functor is of primary importance in algebraic geometry.)*

Exercise 1.7 *Let L be a field. Show that $\mathrm{id}_L : L \to L$ is a terminal object in the category of subfields of L. Let L_0 denote the prime subfield of L (so L_0 is the field generated by 1_L in L). Show that inclusion $L_0 \to L$ is an initial object in the category of subfields of L.*

Exercise 1.8 *Let L be a field and let L_0 denote the prime subfield of L. Show that $\mathrm{Aut}(L/L_0) = \mathrm{Aut}(L)$.*

Exercise 1.9 *Let G be a group. Show that $1 \to G$ is an initial object in the category of subgroups of G and that $\mathrm{id}_G : G \to G$ is a terminal object in the category of subgroups of G.*

exercise: monic

Exercise 1.10 *In any category, a map ϕ is said to be a monic if*

$$\forall \alpha, \beta \qquad (\phi \circ \alpha = \phi \circ \beta \implies \alpha = \beta).$$

Show that the notion of monic and injective homomorphism coincide in the category of sets, fields and groups. Do these notions coincide in the category of crings? (You should be aware that there are two senses of the word 'monomorphism'; people with a predilection for category theory often refer to monics as monomorphisms, while others refer to injective homomorphisms as monomorphisms.)

roup monomorphism

Exercise 1.11 *Consider Diagramme* diagramme: map-L *1.1. Show that, since the triangle commutes, it follows that $\gamma : X \to Y$ is monic.*

exercise: PGL(2)

Exercise 1.12 *Show that $\mathrm{Aut}(\mathbb{Q}(t)/\mathbb{Q})$ contains $t \mapsto \frac{at+b}{ct+d}$ for all $ad - bc \neq 0$. Conclude that $\mathrm{Aut}(\mathbb{Q}(t)/\mathbb{Q})$ is infinite and non-abelian.*

Exercise 1.13 *Determine which of the following rings are fields. If a field, find its dimension as a vector space over k and find the group of all field automorphisms which are k-linear; if not a field, find some zero-divisors. Consider $k[x]/(x+1)$, $k[x]/(x^2+1)$, $k[x]/(x^2+x+1)$, $k[x]/(x^3+x^2+x+1)$ and $k[x]/(x^4+x^3+x^2+x+1)$ where k is $\mathbb{Q}$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$ or $\mathbb{F}_5$.*

exercise: Zorn

Exercise 1.14 *Let A be a cring. Is there some ideal I in A such that A/I is a field?*

ercise: subfields

Exercise 1.15 *Let L be a field. Show that the category of subfields of L contains products, co-products, pull-backs and push-outs.*

ercise: subgroups

Exercise 1.16 *Let G be a field. Show that the category of subgroups of G contains products, co-products, pull-backs and push-outs.*

Garling, Exercise 5.4

Exercise 1.17 *Suppose K is a field and that f and g are relatively prime in $K[x]$. Show that $f - yg$ is irreducible in $K(y)[x]$.*

Exercise 1.18 *Let p be a prime number. Show that $1 + x + x^2 + \cdots + x^{p-1}$ is irreducible over $\mathbb{Q}$. (Hint: let $x = y + 1$).*

exercise: Galois functor

Exercise 1.19 *Verify that* $\mathrm{Aut}(L/\ )$*, as defined in Definition* definition: aut functor *2, really is a contravariant functor.*

exercise: fix functor

Exercise 1.20 *Verify that* $\mathrm{Aut}(L/\ )$*, as defined in Definition* definition: fix functor *3, really is a contravariant functor.*

Chapter 2

Galois extensions

galois extensions

chapter: Galois adjunction

Chapter 1 contained quite a bit of category theory, and it is easy to get lost in the details. However, having made it this far, we are ready to harvest the fruits of our labours.

2.1 Kaplansky subfields

ection: Kaplansky
nition: Kaplansky

Definition 5 *Let L be a field. A subfield $\alpha : K \to L$ is a Kaplansky subfield of L if*

$$L^{\mathrm{Aut}(L/K)} = \alpha(K).$$

A subgroup $f : G \to \mathrm{Aut}(L)$ is a Kaplansky subgroup of $\mathrm{Aut}(L)$ if

$$\mathrm{Aut}(L/L^G) = f(G).$$

Lemma 1 *$K \to L$ is Kaplansky if $\eta_L(K)$ is an isomorphism, and $G \to \mathrm{Aut}(L)$ is Kaplansky if $\epsilon_L(G)$ is an isomorphism.*

subsection: adjunction

Proof. Combine the definition of the Galois adjunction (see Section 1.4, especially the proof of Proposition 5), with Definition 5. ■

proposition: adjunction definition: Kaplansky

Kaplansky category

Definition 6 *The category of Kaplansky subfields of L, denoted by $\textsc{kapsub}(L)$, is the full subcategory of $\textsc{sub}(L)$ consisting of Kaplansky subfields; likewise, the category of Kaplansky subgroups of $\mathrm{Aut}(L)$, denoted by $\textsc{kapsub}\mathrm{Aut}(L)$, is the full subcategory of $\textsc{sub}\mathrm{Aut}(L)$ consisting of Kaplansky subgroups.*

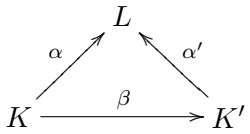
sition: Kaplansky

Proposition 6 *$\mathrm{Aut}(L/\ )$ restricts to an equivalence from the category of Kaplansky subfields of L to the category of Kaplansky subgroups of $\mathrm{Aut}(L)$. Likewise, $\mathrm{Fix}(\ /L)$ restricts to an equivalence from the category of Kaplansky subgroups of $\mathrm{Aut}(L)$ to the category of Kaplansky subfields of L.*

Proof. (Exercise 2.1.) ■

Take a moment to think about Definitions 5 and 6 and Proposition 6. Taken together, these say that an extension $K \to L$ is Kaplansky if it is an object in the largest full subcategory of $\text{SUB}(L)$ for which $\text{Aut}(L/\ )$ is an equivalence of categories. In other words, we have *defined* the notion of a Kaplansky extension in terms of a property of the Galois functors.

Since $\text{KAPSUB}(L)$ is a *full* subcategory of $\text{SUB}(L)$, maps in $\text{KAPSUB}(L)$ are triangles



where $\alpha : K \to L$ and $\alpha' : K' \to L$ are Kaplansky extensions and $\beta : K \to K'$ is any field homomorphism for which $\alpha = \alpha' \circ \beta$. In particular, note that $\beta : K \to K'$ need not be a Kaplansky extension. In Exercise 2.4 you are asked to find an example of this phenomenon.

Proposition 7 *The image of* $\text{SUB}(L)$ *under* $\text{Aut}(L/\ )$ *is contained in the category of Kaplansky subgroups of* $\text{Aut}(L)$ *ad the image of* $\text{SUBAut}(L)$ *under* $\text{Fix}(\ /L)$ *is contained in the category of Kaplansky subfields of* L*.*

Proof. This is no more than a re-statement of one consequence of the Galois adjunction (Proposition 5). Suppose $\varphi : H \to \text{Aut}(L)$ is contained in the image of $\text{SUB}(L)$ under $\text{Aut}(L/\ )$. Then $H = \text{Aut}(L/K)$ for some subfield $\alpha : K \to L$. Then $\text{Aut}(L/L^H) = \text{Aut}(L/L^{\text{Aut}(L/K)})$. Since $\text{Aut}(L/L^{\text{Aut}(L/K)}) = \text{Aut}(L/K)$ by Proposition 5, and since $\text{Aut}(L/K) = H$, we have $\text{Aut}(L/L^H) = H$, so $\varphi : H \to \text{Aut}(L)$ is a Kaplansky subgroup. Likewise, suppose $\alpha : K \to L$ is contained in the image of $\text{SUBAut}(L)$ under $\text{Fix}(\ /L)$. Then $K = L^H$ for some subgroup $\varphi : H \to \text{Aut}(L)$. Then $L^{\text{Aut}(L/K)} = L^{\text{Aut}(L/L^H)}$. Since $L^{\text{Aut}(L/L^H)} = L^H$ by Proposition 5, and since $L^H = K$, we have $L^{\text{Aut}(L/K)} = K$, so $\alpha : K \to L$ is a Kaplansky subfield. ■

As we shall soon wee (in Section 2.3), a subfield $K \to L$ is called a *Galois subfields* if it is Kaplansky and $K \to L$ is an algebraic extension, in the sense explained in Section 2.2.

2.2 Algebraic extensions

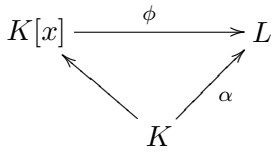
The study of algebraic extensions of a field K is inextricably linked to the ring $K[x]$, so we begin this section by recalling that $K[x]$ is a principal ideal

cring and that

$$\mathrm{Spec}(K[x]) = \mathrm{Specm}(K[x]) \cup \{(0)\}.$$

Let us also take this moment to fix some notation: for each field L and $u \in L$, we write $\epsilon_u : L[x] \to L$ for the unique splitting of $L \to L[x]$ such that $\epsilon_u(x) = u$; we refer to ϵ_u as evaluation at u; we will often write $p(u)$ for $\epsilon_u(p)$, where $p \in L[x]$.

Now, let $\alpha : K \to L$ be a fixed extension of fields and consider the set $\mathrm{Hom}_K(K[x], L)$ of cring homomorphisms $\phi : K[x] \to L$ such that the triangle



is commutative.

Lemma 2 *If $\phi \in \mathrm{Hom}_K(K[x], L)$ then $\ker\phi$ is a prime ideal of $K[x]$.*

Proof. If $p_1p_2 \in \ker\phi$ then $\phi(p_1p_2) = 0$ so $\phi(p_1)\phi(p_2) = 0$, in which case $\phi(p_1) = 0$ or $\phi(p_2) = 0$ (since (0) is a prime ideal of K by Proposition 3). Thus, $p_1 \in \ker\phi$ or $p_2 \in \ker\phi$. ■

proposition: prime ideals

ition: algebraic

Definition 7 *An extension $K \to L$ is an algebraic extension if the image of the map*

$$\begin{array}{rcl} \mathrm{Hom}_K(K[x], L) & \to & \mathrm{Spec}(K[x]) \\ \phi & \mapsto & \ker\phi \end{array}$$

is contained in $\mathrm{Specm}(K[x])$*; otherwise, the extension is a transcendental extension.*

definition: algebraic

Some of you may recognize the geometric nature of Definition 7. The set $\mathrm{Spec}(K[x])$ is the set underlying the affine line $\mathbb{A}^1_K$ as a K-scheme and $\mathrm{Hom}_K(K[x], L)$ is precisely the set of L-valued points in $\mathbb{A}^1_K$ as a K-scheme. Thus, Definition 7 may be paraphrased as follows: *$K \to L$ is algebraic if and only if every L-valued point on $\mathbb{A}^1_K$ is closed.*

definition: algebraic

Our next goal is to understand this definition. We begin by noticing that $\mathrm{Hom}_K(K[x], L)$ is not so complicated.

Lemma 3 *The function $\mathrm{Hom}_K(K[x], L) \to L$ defined by $\phi \mapsto \phi(x)$ is a bijection.*

Proof. If we write $\alpha_x : K[x] \to L[x]$ for the obvious extension of $\alpha : K \to L$, then it is clear that $\epsilon_u \circ \alpha_x$ is an element of $\mathrm{Hom}_K(K[x], L)$, for each $u \in L$. A moment's reflection shows that every element of $\mathrm{Hom}_K(K[x], L)$ takes this form, since if $\phi \in \mathrm{Hom}_K(K[x], L)$ then

$$\begin{aligned}
\phi(\sum_i a_i x^i) &= \sum_i \phi(a_i)\phi(x)^i \\
&= \sum_i \phi(\iota(a_i))\phi(x)^i \\
&= \sum_i \alpha(a_i)\phi(x)^i \\
&= \epsilon_{\phi(x)}(\sum_i \alpha(a_i)x^i) \\
&= \epsilon_{\phi(x)} \circ \alpha_x(\sum_i a_i x^i).
\end{aligned}$$

This shows that the map $\phi \mapsto \phi(x)$ is a surjection $\mathrm{Hom}_K(K[x], L) \to L$. Another moment's reflection shows that $\epsilon_u \circ \alpha_x = \epsilon_{u'} \circ \alpha_x$ if and only if $u = u'$, so the surjection is also a bijection. ■

proposition: algebraic

Proposition 8 *$\alpha : K \to L$ is algebraic if and only if*

$$\forall u \in L, \exists p \in K[x], \quad \alpha_x(p)(u) = 0.$$

Proof. (Exercise 2.3.) ■

exercise: algebraic
proposition: algebraic

Proposition 8 leads to the following definition.

inition: algebraic element

Definition 8 *Let $\alpha : K \to L$ be an extension. An element $u \in L$ is an algebraic over K if $\ker(\epsilon_u \circ \alpha_x)$ is a maximal ideal. In this case we write $m_{u,K} \in K[x]$ for the unique monic polynomial generator for $\ker(\epsilon_u \circ \alpha_x)$; this is called the minimal polynomial for u over K. Otherwise, $u \in L$ is transcendental over K.*

We finish this section with a few miscellaneous facts about algebraic extensions. Let $\mathrm{End}(L/K)$ denote the set of field homomorphisms $L \to L$ (endomorphisms of L) which factor over K. This set is closed under composition, and composition endows $\mathrm{End}(L/K)$ with the structure of a monoid. When $K \to L$ is algebraic, this monoid is actually a group, as the next lemma shows.

lemma: endo is iso

Lemma 4 *If $K \to L$ is algebraic then $\mathrm{End}(L/K) = \mathrm{Aut}(L/K)$.*

Proof. Suppose $K \to L$ is algebraic and $\sigma \in \mathrm{End}(L/K)$. We must show that σ is surjective. Pick $u \in L$. Let X be the set of roots of $m_{u,K}$ in L; thus, $X = \{v \in L \mid \alpha_x(m_{u,K})(v) = 0\}$. (Here we used the hypothesis that L is algebraic over K and Proposition 8.) Then σ restricts of a map $X \to X$ (show this!). Since σ is injective (Proposition 4), so too is the function $X \to X$. Since X is finite (by the Fundamental Theorem of Algebra), $X \to X$ is also surjective. Thus, there is some $v \in X$ such that $\sigma(v) = u$, concluding the proof of Lemma 4. ■

proposition: algebraic
proposition: injections
lemma: endo is iso

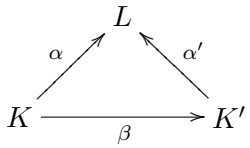
ebraic isomorphism

Lemma 5 *Every isomorphism of fields is an algebraic extension.*

Proof. Let $\alpha : K \to L$ be an isomorphism. Pick $u \in L$. Then the minimal polynomial for u over K is $m_{u,K} = x - \alpha^{-1}(u)$, since $m_{u,K}$ is irreducible, monic, has coefficients in K and $\alpha_x(m_{u,K})(u) = u - u = 0$. Thus, $\alpha : K \to L$ is algebraic. ■

gebraic permanence

Lemma 6 *Suppose $\alpha = \alpha' \circ \beta$. If α is algebraic then α' and β are algebraic.*



Proof. Suppose α is algebraic. Pick $u \in L$. Consider $m_{u,K} \in K[x]$ (which exists since $\alpha : K \to L$ is algebraic). Now, $\alpha'_x(\beta_x(m_{u,K}))(u) = \alpha_x(m_{u,K})(u) = 0$, so $\ker(\epsilon_u \circ \alpha'_x)$ is maximal, which shows that u is algebraic over K'. Since $u \in L$ was arbitrary, it follows that $\alpha' : K' \to L$ is algebraic. Now, pick $v \in K'$. Since $\alpha : K \to L$ is algebraic and $\alpha'(v) \in L$, it follows that $\alpha'(v)$ is algebraic over K. Write

$$m_{\alpha'(v),K} = \sum_i b_i x^i \in K[x]^\times,$$

Since $\alpha_x(m_{\alpha'(v),K})(\alpha'(v)) = 0$, it follows that

$$\alpha_x(\sum_i b_i x^i)(\alpha'(v)) = \sum_i \alpha(b_i)\alpha'(v)^i = 0.$$

Since $\alpha = \alpha' \circ \beta$, we have

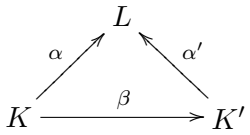
$$\sum_i \alpha' \circ \beta(b_i)\alpha'(v^i) = 0.$$

Thus, $\alpha'(\sum_i \beta(b_i)v^i) = 0$. Since α' is a monomorphism, $\sum_i \beta(b_i)v^i = 0$. Thus, $\beta_x(\sum_i b_i x^i)(v) = 0$, in which case $\beta_x(m_{\alpha'(v),K})(v) = 0$. This shows that, $\ker(\epsilon_v \circ \beta_x)$ is a maximal ideal, which shows that v is algebraic over K. Since $v \in K'$ was arbitrary, it follows that $\beta : K \to K'$ is an algebraic extension. ■

Now that you are comfortable with the notion of algebraic extensions, it is time to form a category.

nition: algebraic category

Definition 9 *The category of algebraic subfields of L, denoted by* $\textsc{algsub}(L)$*, is the full subcategory of* $\textsc{sub}(L)$ *formed by algebraic extensions into L. Thus, objects in* $\textsc{algsub}(L)$ *are subfields $\alpha : K \to L$ such that L is an algebraic extension of K and maps in* $\textsc{algsub}(L)$ *are triangles*



for which $\alpha : K \to L$ and $\alpha' : K' \to L$ are algebraic.

lemma: algebraic perma

Note that $\beta : K \to K'$ need not be algebraic in this diagramme, Lemma 6 shows that $\textsc{algsub}(L)$ and $\textsc{kapsub}(L)$ have rather different properties; in particular, if α is algebraic and $\alpha = \alpha' \circ \beta$ then α' and β are both algebraic. By contrast hand, there are many examples (such as that provided in Exercise 2.4) of Kaplansky extensions α for which β is not Kaplansky even though $\alpha = \alpha' \circ \beta$.

exercise: composition

2.3 Galois extensions

section: Galois

definition: Galois

Definition 10 *Let L be a field. The category of Galois subfields of L, denoted by* $\textsc{galsub}(L)$ *is the full subcategory*

$$\textsc{galsub}(L) = \textsc{algsub}(L) \cap \textsc{kapsub}(L).$$

An extension $K \to L$ is a Galois extension if it is an object in $\textsc{galsub}(L)$*.*

Notice that we have not defined the term 'Galois subgroup' here. There is a reason: Galois groups are *topological* groups, and we have not yet defined the relevant topology (called the 'Krull topology'). All in good time. (Or, go to Definition 25 now and work backward through the text.)

definition: galois group

chapter: normal extensions

In Chapter 8 we assemble various important properties of Galois subfields, and ultimately find a completely different characterization of Galois

extensions (Theorem GNST 10). For now, we make a very simple observations concerning Galois extensions.

Galois isomorphism

Lemma 7 *Every isomorphism of fields is a Galois extension of fields.*

Proof. Let $\alpha : K \to L$ be an isomorphism. If $\sigma \in \mathrm{Aut}(L/K)$ then $\alpha = \sigma \circ \alpha$. Since α is an isomorphism, $\alpha \circ \alpha^{-1} = \sigma \circ \alpha \circ \alpha^{-1}$ so $\mathrm{id}_L = \sigma$. Now, $\mathrm{Aut}(L/K) = \{\mathrm{id}_L\}$ so $L^{\mathrm{Aut}(L/K)} = L^{\{\mathrm{id}_L\}} = L$. Recalling the definition of the natural transformation η_L from Section 1.4, we see that $\eta_L(\alpha) = \alpha$. Since α is an isomorphism it follows from Definition 5 that α is Kaplansky. We already saw (Lemma 5 that α is algebraic, so α is Galois, by Definition 10. ■

2.4 Chapter 2 exercises

ercise: Kaplansky

Exercise 2.1 *Prove Proposition 6.*

is correspondence

Exercise 2.2 *Let L be a field. Show, as claimed above, that $\mathrm{Aut}(L/\ )$ is an equivalence from the category of Kaplansky subfields of L to the category of Kaplansky subgroups of $\mathrm{Aut}(L)$.*

ercise: algebraic

Exercise 2.3 *Prove Proposition 8.*

ise: composition

Exercise 2.4 *1. Show that $\mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2})$ is algebraic but not Kaplansky and therefore not Galois. Show that $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is algebraic and Kaplansky and therefore Galois. Show that the composition $\mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ is algebraic and Kaplansky and therefore Galois.*

2. Show that $\mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt[4]{2})$ are algebraic and Kaplansky and therefore Galois. Show that the composition $\mathbb{Q} \to \mathbb{Q}(\sqrt[4]{2})$ is algebraic but not Kaplansky and therefore not Galois.

asic finite galois

Exercise 2.5 *Consider the extension $\mathbb{Q} \to \mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$. Is this extension Galois? Find the dimension and the Galois group of this extension.*

Exercise 2.6 *Find the minimal polynomial $\sqrt{2}$ and for $\sqrt{3}$ and then find the minimal polynomial for $\sqrt{2}\sqrt{3}$ and for $\sqrt{2} + \sqrt{3}$.*

Exercise 2.7 *Find the minimal polynomial for $e^{2\pi i/5}$ over $\mathbb{Q}$; find the minimal polynomial for $\cos(2\pi/5)$ over $\mathbb{Q}$.*

Exercise 2.8 *Find the minimal polynomial for $e^{2\pi i/7}$ over $\mathbb{Q}$; find the minimal polynomial for $\cos(2\pi/7)$ over $\mathbb{Q}$.*

ise: endo is iso

Exercise 2.9 *Is the converse to Lemma 4 true?*

Chapter 3

Finite Extensions

finite extensions

3.1 Finite extensions

Let $\alpha : K \to L$ be a field homomorphism. Then L is a vector space over K with the following definition:

$$\begin{aligned} K \times L &\to L \\ (k, u) &\mapsto \alpha(k)u. \end{aligned}$$

(One often writes ku for $\alpha(k)u$.) Thus, we can apply a basic invariant from the theory of vector spaces to field extensions.

efinition: degree

Definition 11 *Let $K \to L$ be an extension. The degree of L over K is the dimension of L as a vector space over K. This number, which may be infinite, is denoted $\dim_K(L)$ or $[L : K]$. If the degree of L over K is finite, then we say $K \to L$ is a finite extension; otherwise, $K \to L$ is an infinite extension.*

sition: tower law

Proposition 9 (Tower Law) *Let $K \to K'$ and $K' \to L$ be field homomorphisms; then*

$$[L : K] = [L : K'] \times [K' : K].$$

Proof. Let $\beta : K \to K'$ and $\alpha' : K' \to L$ be field homomorphisms. Set $\alpha := \alpha' \circ \beta$. Then $\alpha : K \to L$ is a field homomorphism so L is a vector spaces over K. This proposition is a consequence of the following statement: if $\{u_i \mid i \in I\} \subset L$ is a basis for L over K' and if $\{v_j \mid j \in J\} \subset K'$ is a basis for K' over K, then $\{\alpha'(v_j)u_i \mid (i, j) \in I \times J\}$ is a basis for L over K. Let

us see why this is true. Suppose $u \in L$. Since $\{u_i \mid i \in I\}$ is a basis for L over K', we uniquely write

$$u = \sum_{i \in I} \alpha'(a_i) u_i,$$

where $a_i \in K'$ and all but finitely many a_i are zero. Since $\{v_j \mid j \in J\}$ is a basis for K' over K and each a_i is contained in K', for each $i \in I$ we uniquely write

$$a_i = \sum_{j \in J} \beta(b_{ij}) v_j$$

where $b_{ij} \in K$ and all but finitely many b_{ij} are zero as j runs over J. Notice that all but finitely b_{ij} are non-zero as (i,j) runs over $I \times J$. Therefore,

$$\begin{aligned} u &= \sum_{i \in I} \alpha'(a_i) u_i \\ &= \sum_{i \in I} \alpha' \left(\sum_{j \in J} \beta(b_{ij}) v_j \right) u_i \\ &= \sum_{(i,j) \in I \times J} \alpha' \circ \beta(b_{ij}) \alpha'(v_j) u_i \\ &= \sum_{(i,j) \in I \times J} \alpha(b_{ij}) \alpha'(v_j) u_i. \end{aligned}$$

This shows that $\{\alpha'(v_j)u_i \mid (i,j) \in I \times J\}$ spans L as a vector space over K. To see that $\{\alpha'(v_j)u_i \mid (i,j) \in I \times J\}$ is linearly independent over K, suppose $\sum_{(i,j) \in I \times J} \alpha(c_{ij})\alpha'(v_j)u_i = 0$ with $c_{ij} \in K$. As above, observe that $\sum_{(i,j) \in I \times J} \alpha(c_{ij})\alpha'(v_j)u_i = \sum_{i \in I} \alpha' \left(\sum_{j \in J} \beta(c_{ij}) v_j \right) u_i$. Since $\sum_{j \in J} \beta(c_{ij}) v_j \in K'$ for each i and since $\{u_i \mid i \in I\}$ is a basis for L over K', it follows that $\sum_{j \in J} \beta(c_{ij}) v_j = 0$. Since each $c_{ij} \in K$ and $\{v_j \mid j \in J\}$ is a basis for K' over K, it follows that $c_{ij} = 0$ for each $i \in I$ and $j \in J$. This shows that $\{\alpha'(v_j)u_i \mid (i,j) \in I \times J\} \subset L$ is linearly independent over K and completes the proof that $\{\alpha'(v_j)u_i \mid (i,j) \in I \times J\}$ is a basis for L over K. ■

Corollary 1 *Suppose $\alpha = \alpha' \circ \beta$. Then α is a finite extension if and only if α' and β are both finite extensions.*

: finite implies algebraic

Proposition 10 *If $\alpha : K \to L$ is finite then $\alpha : K \to L$ is algebraic.*

Proof. Suppose $\alpha : K \to L$ is finite; let $\dim_K(L) = n$. Pick $u \in L$. Then the set $\{1, u, u^2, \ldots u^n\}$ is linearly dependent over K. Thus, $\sum_i \alpha(a_i)u^i = 0$ for some $a_i \in K$ not all zero. Define $f \in K[x]^\times$ by $f = \sum_i a_i x^i$. Then $\alpha_x(f)(u) = 0$, whence $u \in L$ is algebraic over K by Proposition 8. ■ proposition: algebraic

3.2 Dedekind-Artin Theorem

Now we can prove a lovely result: all finite subgroups of $\mathrm{Aut}(L)$ are Kaplansky subgroups! The proof will require several lemmata, each of which is rather delightful in its own right.

lemma: Dedekind **Lemma 8 (Dedekind)** *Let G be a group and let K be a field. The set $\mathrm{Hom}_{\mathrm{GROUP}}(G, K^\times)$ of group homomorphism $G \to K^\times$ is linearly independent in the K-vector space of functions $\mathrm{Hom}_{\mathrm{SET}}(G, K)$.*

Proof. First, let us confirm that $\mathrm{Hom}_{\mathrm{SET}}(G, K)$ really is a K-vector space. Let

$$\begin{aligned} \mathrm{Hom}_{\mathrm{SET}}(G, K) \times \mathrm{Hom}_{\mathrm{SET}}(G, K) &\to K \\ (f_1, f_2) &\mapsto f_1 + f_2 \end{aligned}$$

be the usual thing: $f_1 + f_2$ is defined by $(f_1 + f_2)(g) := f_1(g) + f_2(g)$. Then $\mathrm{Hom}_{\mathrm{SET}}(G, K)$ is an abelian group with identity $0 : G \to K$ defined by $0(g) := 0_K$ for all $g \in G$. Scalar multiplication in $\mathrm{Hom}_{\mathrm{SET}}(G, K)$ is given by

$$\begin{aligned} K \times \mathrm{Hom}_{\mathrm{SET}}(G, K) &\to K \\ (u, f) &\mapsto uf \end{aligned}$$

where $(uf)(g) := uf(g)$. Again, it is easy to verify that scalar multiplication is distributive and satisfies all the other required properties in order to endow $\mathrm{Hom}_{\mathrm{SET}}(G, K)$ with the structure of a K-vector space.

Now, suppose the lemma is false. Thus, there is a *minimal*, *finite* set $\{\chi_1, \ldots, \chi_n\}$ of (distinct) characters of G such that

$$\sum_{i=1}^{n} a_i \chi_i = 0, \tag{3.1}$$

where not all a_i are 0. Since $\chi_1 \neq \chi_2$ there is some $h \in G$ such that $\chi_1(h) \neq \chi_2(h)$. Evaluate the equation above at arbitrary g and multiply by

$\chi_1(h)$, then evaluate the equation above at hg, and subtract:

$$a_1\chi_1(h)\chi_1(g) + \sum_{i=2}^{n} a_i\chi_1(h)\chi_i(g) = 0$$
$$a_1\chi_1(h)\chi_1(g) + \sum_{i=2}^{n} a_i\chi_i(h)\chi_i(g) = 0$$
$$\sum_{i=2}^{n} a_i(\chi_1(h) - \chi_i(h))\chi_i(g) = 0$$

Since this clearly contradicts the minimality of the set $\{\chi_1, \ldots, \chi_n\}$, this completes the proof of the lemma. ■

position: finite extension

Proposition 11 *If $K \to L$ is a finite extension then $\left|\mathrm{Aut}(L/K)\right| \leq [L : K]$.*

Proof. We begin by showing that if $\alpha : K \to L$ is finite then $\left|\mathrm{Aut}(L/K)\right|$ is finite. Let $\{u_1, \ldots, u_n\}$ be a basis for L over K. Suppose $\sigma \in \mathrm{Aut}(L/K)$. Then σ is completely determined by the values $\{\sigma(u_1), \ldots, \sigma(u_n)\}$. For each $1 \leq i \leq n$, let consider the minimal polynomial $m_{u_i,K}$ for u_i over K and observe that $\alpha_x(m_{u_i,K})(\sigma(u_i)) = \sigma(\alpha_x(m_{u_i,K})(u_i)) = \sigma(0) = 0$; thus, $\sigma(u_i)$ is a root of $\alpha_x(m_{u_i,K})$. Since there are only finitely many roots of $\alpha_x(m_{u_i,K})$ in L for each i (by the Fundamental Theorem of Algebra), there are only finitely many automorphisms $\sigma \in \mathrm{Aut}(L/K)$.

Write $\mathrm{Aut}(L/K) = \{\sigma_1, \ldots, \sigma_m\}$ and consider the matrix

$$A = \begin{bmatrix} \sigma_1(u_1) & \sigma_1(u_2) & \cdots & \sigma_1(u_n) \\ \sigma_2(u_1) & \sigma_2(u_2) & \cdots & \sigma_2(u_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_m(u_1) & \sigma_m(u_2) & \cdots & \sigma_m(u_n) \end{bmatrix}$$

The lemma claims that $m \leq n$, so, for a contradiction, suppose $n < m$. Then the rank of A is at most n, so the rows are linearly dependent in L^m. Consequently, there are $a_1, \ldots, a_m \in L$ such that $\sum_{i=1}^{m} a_i\sigma_i(u_j) = 0$ for all $1 \leq j \leq n$ and the a_i are not all 0. Since each σ_i is determined by its values at the u_j, it follows that $\sum_{i=1}^{m} a_i\sigma_i = 0$.

Now, observe that $L^\times$ is a group and that each $\sigma \in \mathrm{Aut}(L/K)$ restricts to a group homomorphism $\sigma|_{L^\times} : L^\times \to L^\times$, which is a character. Since these characters are all distinct, it follows that set $\{\sigma_1|_{L^\times}, \ldots, \sigma_m|_{L^\times}\}$ is linearly independent, by Lemma 8. But, from the paragraph above we have $\sum_{i=1}^{m} a_i\sigma_i|_{L^\times} = 0$. This contradiction proves the lemma. ■

lemma: Dedekind

n: Dedekind-Artin **Theorem 1 (Dedekind-Artin)** *Let L be a field. If $\varphi : H \to \mathrm{Aut}(L)$ is a finite subgroup then $[L : L^H] = \left|H\right|$ and $\varphi : H \to \mathrm{Aut}(L)$ a Kaplansky subgroup.*

Proof. Recall that a subgroup $\varphi : H \to \mathrm{Aut}(L)$ is Kaplansky if $H = \mathrm{Aut}(L/K)$ for some Galois subfield $K \to L$ of L. Let $K = L^H$ and write $H\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$, so $n = \left|H\right|$.

We begin by showing that $K \to L$ is a finite extension. In fact, we will prove something stronger: $K \to L$ is finite and $\dim_K(L) = n$. Suppose this is not the case. Then there exists a set $\{u_1, \ldots u_{n+1}\}$ of elements from L which are linearly independent over K. Consider the matrix

$$A = \begin{bmatrix} \varphi(\sigma_1)(u_1) & \varphi(\sigma_1)(u_2) & \cdots & \varphi(\sigma_1)(u_{n+1}) \\ \varphi(\sigma_2)(u_1) & \varphi(\sigma_2)(u_2) & \cdots & \varphi(\sigma_2)(u_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi(\sigma_n)(u_1) & \varphi(\sigma_n)(u_2) & \cdots & \varphi(\sigma_n)(u_{n+1}) \end{bmatrix}$$

Then the columns of A are linearly dependent in L^n. Let k be the cardinality of the smallest set of linearly dependent columns of A. Without loss of generality, we may assume the first k columns of A are linearly dependent. Thus, there are $a_i \in L$ such that

$$\forall 1 \leq j \leq n, \quad \sum_{i=1}^{k} a_i \varphi(\sigma_j)(u_i) = 0.$$

Without loss of generality we may assume $a_1 = 1$. Now, if each coefficient a_i were in $\alpha(K)$, then we would have $\varphi(\sigma_j)(\sum_{i=1}^{k} a_i u_i) = 0$, in which case $\sum_{i=1}^{k} a_i u_i = 0$. Of course, this is impossible since $\{u_1, \ldots u_{n+1}\}$ are linearly independent over K. Accordingly, for some $1 \leq i \leq k$, a_i is not in $\alpha(K)$.

Now, pick $\sigma \in H$. Applying σ to the displayed equation above gives

$$\forall 1 \leq j' \leq n, \quad \sum_{i=1}^{k} \varphi(\sigma)(a_i)\varphi(\sigma_{j'})(u_i) = 0.$$

(Here we use the fact that there is a permutation $j \mapsto j'$ of n such that $\sigma \circ \sigma_j = \sigma_{j'}$ for each $1 \leq j \leq n$.) Subtracting these equations gives

$$\forall 1 \leq j \leq n, \quad \sum_{i=2}^{k} (a_i - \varphi(\sigma)(a_i))\varphi(\sigma_j)(u_i) = 0.$$

(Here we use the fact that $a_1 = 1$ and $\sigma(1) = 1$.) Minimality of k implies $a_i = \varphi(\sigma)(a_i)$ for each $1 \leq i \leq k$. Since $\sigma \in H$ was arbitrary, we have $a_i \in L^H = K$ for each i, which contradicts the conclusion of the paragraph above. This contradication proves that $\dim_K(L) = n$.

proposition: adjunction

Now, $\varphi : H \to \mathrm{Aut}(L)$ maps into $\mathrm{Aut}(L/L^H)$ by Proposition 5. Since $\mathrm{Aut}(L/L^H) = \mathrm{Aut}(L/K)$ is finite (by the work above) and φ is a monic group homomorphism and therefore injective (by Exercise 1.10), it follows that $\big|H\big| \leq \mathrm{Aut}(L/L^H)$. On the other hand, $\big|\mathrm{Aut}(L/L^H)\big| \leq [L : K]$ by Proposition 11. Since $[L : K] = \big|H\big|$ by the work above, we have $\big|H\big| = \big|\mathrm{Aut}(L/L^H)\big|$. It follows that the $\varphi(H) = \mathrm{Aut}(L/L^H)$, which means $\varphi : H \to \mathrm{Aut}(L)$ is a Kaplansky subgroup. ■

exercise: monic

proposition: finite extension

theorem: finite Galois

Theorem 2 *A finite extension $K \to L$ is Galois if and only if*

$$\big|\mathrm{Aut}(L/K)\big| = [L : K].$$

Proof. Suppose $K \to L$ is a finite Galois extension. Then $\mathrm{Aut}(L/K)$ is finite by Proposition 11. Since $K = L^{\mathrm{Aut}(L/K)}$, it follows from Theorem 1 that $\big|\mathrm{Aut}(L/K)\big| = [L : K]$.

proposition: finite extension

theorem: Dedekind-Arti

Conversely, suppose $K \to L$ is a finite extension and $\big|\mathrm{Aut}(L/K)\big| = [L : K]$. Let $M = L^{\mathrm{Aut}(L/K)}$. Since $\mathrm{Aut}(L/K)$ is finite it is Kaplansky, by Theorem 1; thus, $\mathrm{Aut}(L/K) = \mathrm{Aut}(L/L^K)$. Let $M = L^K$. Then $\mathrm{Aut}(L/K) = \mathrm{Aut}(L/M)$. Since $\big|\mathrm{Aut}(L/K)\big| = \dim_K(L)$ by hypothesis and since $\big|\mathrm{Aut}(L/M)\big| = \dim_M(L)$ by Theorem 1, it follows that $\dim_K(L) = \dim_M(L)$, in which case $M = K$. But now, $K = L^{\mathrm{Aut}(L/K)}$ so $K \to L$ is Kaplansky. Since $K \to L$ is finite, it is algebraic, by Proposition 10. Thus, $K \to L$ is Galois. ■

theorem: Dedekind-Artin

theorem: Dedekind-Artin

proposition: finite implies alg

corollary: finite functor

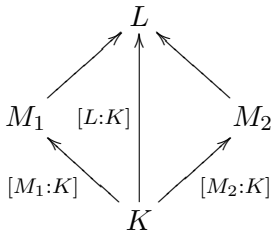
Corollary 2 *Let L be a field. The automorphism functor $\mathrm{Aut}(L/\ )$ takes finite extensions $K \to L$ to finite subgroups of $\mathrm{Aut}(L)$ and the fix functor $\mathrm{Fix}(\ /L)$ takes finite subgroups of $\mathrm{Aut}(L)$ to finite extensions into L.*

chapter: finite extensions

3.3 Chapter 3 exercises

Exercise 3.1 *Prove the following theorem. Suppose $M_1 : K$ and $M_2 : K$ are extensions. Let $L : K$ be a co-product of $M_1 : K$ and $M_2 : K$. Then $L : K$ is finite if and only if $M_1 : K$ and $M_2 : K$ are finite, in which case $[L : K] \leq [M_1 : K][M_2 : K]$ and $[M_1 : K]|[L : K]$ and $[M_2 : K]|[L : K]$. If, moreover, $[M_1 : K]$ and $[M_2 : K]$ are relatively prime, then $[L : K] = [M_1 :$*

$K][M_2 : K]$.



Chapter 4

Simple Extensions

simple extensions

4.1 Simple extensions

efinition: simple

Definition 12 *Let $\alpha : K \to L$ be a field extension and let u be an element of L. Let $\alpha(K)(u)$ denote the intersection in L of all subsets of L which are fields and which contain $\alpha(K) \cup \{u\}$. (When suppressing the notation α, one writes $K(u)$ for $\alpha(K)(u)$.) Define $\alpha_u : K \to \alpha(K)(u)$ by $\alpha_u(x) = \alpha(x)$; thus, α_u is just α with restricted codomain. Then $\alpha_u : K \to \alpha(K)(u)$ is a called a simple extension. Let $\alpha^u : \alpha(K)(u) \to L$ be the unique field homomorphism such that $\alpha = \alpha^u \circ \alpha_u$.*

In fact, the simple extension $K \to \alpha(K)(u)$ admits another description, which is very useful.

oposition: simple

Proposition 12 *Let $\alpha : K \to L$ be a field homomorphism. Let $\epsilon_u : L[x] \to L$ denote the cring homomorphism defined by $\epsilon_u(f) = f(u)$. Let $\alpha(K)[u]$ denote the image of $\epsilon_u \circ \alpha_x$, where $\alpha_x : K[x] \to L[x]$ is the obvious cring homomorphism. Then $\alpha(K)(u)$ is the quotient field of the integral domain $\alpha(K)[u]$.*

Proof. (Exercise 4.1.) exercise: simple ■

ollary: injective

Corollary 3 *For any field M, the map*

$$\begin{aligned} \mathrm{Hom}_K(\alpha(K)(u), M) &\to M \\ \beta &\mapsto \beta(u) \end{aligned}$$

is injective.

4.2 Finite simple extensions

proposition: very simple

Proposition 13 *Let $\alpha : K \to L$ be a field homomorphism. Then $\alpha_u : K \to \alpha(K)(u)$ is finite if and only if u is algebraic over K, in which case $\alpha(K)[u] = \alpha(K)(u)$.*

Proof. If $K \to K(u)$ is finite then $K \to K(u)$ is algebraic, by Proposition 10. By Proposition 8, it follows that u is algebraic over K. This established one part of Proposition 13.

To see the converse, consider the following diagramme,

$$\begin{array}{ccc} K[x] & \xrightarrow{\epsilon_u \circ \alpha_x} & L \\ \downarrow & & \uparrow \\ K[x]/\ker(\epsilon_u \circ \alpha_x) & \xrightarrow[\cong]{\overline{\epsilon_u \circ \alpha_x}} & \mathrm{im}(\epsilon_u \circ \alpha_x) \end{array}$$

which commutes by the FIT. Now $\mathrm{im}(\epsilon_u \circ \alpha_x) = K[u]$ (see Proposition 12). On the other hand, $\ker(\epsilon_u \circ \alpha_x) = (m_{u,K})$, which is a maximal ideal (see Definition 7). Thus, $K[x]/\ker(\epsilon_u \circ \alpha_x)$ is a field. Since $\overline{\epsilon_u \circ \alpha_x}$ is an isomorphism, it follows that $K[u]$ is a field, whence $K[u] = K(u)$. Now, the inclusion $K \to K[x]$ and the quotient map $K[x] \to K[x]/(m_{u,K})$ are both cring homomorphisms, and K and $K[x]/(m_{u,K})$ are both fields, so the composition $K \to K[x]/(m_{u,K})$ is a field homomorphism. The Euclidean Division Algorithm tells us that $K[x]/(m_{u,K})$ is a finite dimensional vector space over K. Thus, $K \to K(u)$ is finite. ■

proposition: finite simple

Proposition 14 *Let $\alpha : K \to L$ be a field homomorphism. Suppose $u \in L$ is algebraic over K. Let $n = \deg(m_{K,u})$. Then $\{1, u, u^2, \ldots, u^{n-1}\}$ is a basis for $\alpha(K)(u)$ over K. In particular, $\alpha_u : K \to K(u)$ is finite and $[\alpha(K)(u) : K] = \deg(m_{u,K})$.*

Proof. Pick $a \in \alpha(K)(u)$. By Definition 12 and Proposition 13 there is some $f \in K[x]$ such that $a = \epsilon_u(f)$. By the Euclidean Division Theorem, $f = qm_{u,K} + r$ for some $q, r \in K[x]$ with $r = 0$ or $\deg r < n$. Now $\epsilon_u(f) = \epsilon_u(q)\epsilon_u(m_{u,K}) + \epsilon_u(r)$ so $\epsilon_u(f) = \epsilon_u(r)$. Thus, $a = \epsilon_u(r)$. Since $r \in K[x]$ and $r = 0$ or $\deg(r) < n$ it follows that a is a linear combination of $\{1, u, u^2, \ldots, u^{n-1}\}$ over K. In other words, $\{1, u, u^2, \ldots, u^{n-1}\}$ spans $K(u)$ over K. To see that $\{1, u, u^2, \ldots, u^{n-1}\}$ is linearly independent over K, suppose $\sum_{i=0}^{n-1} a_i \cdot u^i = 0$ with $a_i \in K$. Let $g = \sum_{i=0}^{n-1} a_i x^i$. Then $\epsilon_u(g) = 0$, so $g = hm_{u,K}$ for some $h \in K[x]$. If $g \neq 0$ then

$n - 1 \geq \deg(g) = \deg(h) + \deg(m_{u,K}) \geq n$. Since this is clearly impossible, $g = 0$. This concludes the proof that $\{1, u, u^2, \ldots, u^{n-1}\}$ is a basis for $K(u)$ over K. It follows immediately that $n = [K(u) : K]$. ■

mple automorphisms

Proposition 15 *Let $K \to L$ be an algebraic extension and let $u \in L$ be algebraic over K. Let $\{u_1, \ldots, u_k\}$ be the distinct roots of $m_{u,K}$ in $K(u)$. Then*

$$\mathrm{Aut}(K(u)/K) = \{\sigma_1, \ldots, \sigma_k\},$$

where each σ_i is defined by the condition $\sigma_i(u) = u_i$.

Proof. Suppose $\sigma \in \mathrm{Aut}(K(u)/K)$. Next, observe that $\sigma(u)$ is a root of $m_{u,K}$ since $m_{u,K}(\sigma(u)) = \sigma(m_{u,K}(u)) = \sigma(0) = 0$. Thus, for each $\sigma \in \mathrm{Aut}(K(u)/K)$ there is some $1 \leq i \leq k$ such that $\sigma(u) = u_i$. Let us adopt the convention that $u_1 = u$. Moreover, since $\{1, u, u^2, \ldots, u^{\deg(m_{u,K})-1}\}$ is a basis for $K(u)$ over K (by Proposition 14), it follows that σ is completely determined by the condition $\sigma(u) = u_i$ for some i.

proposition: finite simple

It remains to show that each i from 1 to k actually corresponds to an automorphism of $K(u)$ over K. Let us see if we can define an automorphism σ_i in $\mathrm{Aut}(K(u))/K)$ by the conditions: $\sigma(u) = u_i$ and $\sigma(c) = c$ for each $c \in K$. Recall that $K(u) = K[u]$, by Proposition 13. Thus, each element of $K(u)$ takes the form $f(u)$, for some $f \in K[x]$. Since $\sigma_i(f(u)) = f(u_i)$, we see that σ_i is essentially evaluation at u_i, which is a cring homomorphism. ■

proposition: very simple

4.3 Relative algebraic closure

Proposition 16 *Let $K \to K$ be a field homomorphism. The set of elements of L which are algebraic over K form a subfield of L.*

Proof. Suppose u and v are elements of L which are algebraic over K. The extension $K \to K(u, v)$ is finite by Proposition 19. Since $K(u + v)$ is a subfield of $K(u, v)$, $K \to K(u + v)$ is finite by Proposition 9. Thus, $K \to K(u+v)$ is algebraic, by Proposition 10. Thus, $u+v$ is algebraic over K, by Proposition 14. Thus, the set of elements of L which are algebraic over K is closed under addition. A similar argument shows that this set is

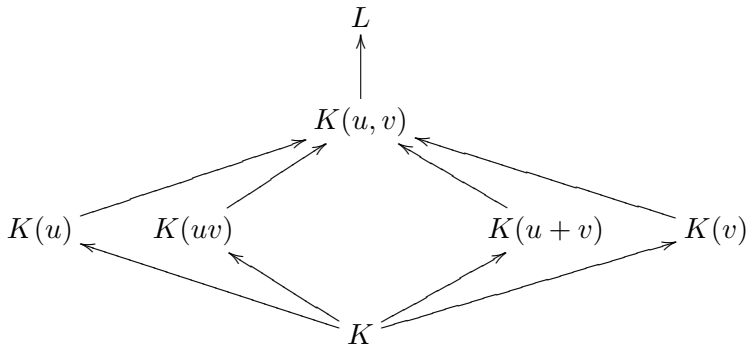
proposition: generated extension

proposition: tower law

proposition: finite implies algebraic

proposition: finite simple

also closed under multiplication.



It only remains to show that the set of non-zero elements of L which are algebraic over $K$is closed under inversion $x \mapsto \frac{1}{x}$. To see this, suppose $u \in L^\times$ is algebraic over K. Define $f_{u^{-1},K} \in K[x]^\times$ by $f_{u^{-1},K}(x) = x^{\deg_K K(u)} m_{u,K}(x^{-1})$. (A priori, $f_{u^{-1},K} \in K(x)$, but a moments thought will show you that $f_{u^{-1},K}$ is indeed a polynomial.) Since $f_{u^{-1},K}$ is non-zero and $\alpha_x(f_{u^{-1},K})(u^{-1}) = 0$, it follows that u^{-1} is algebraic over K. ■

The elegance of the proof of the proceeding proposition is one of the best illustrations of the utility of thinking about the vector space defined by a field homomorphism.

4.4 Factoring homomorphisms by simple extensions

The next result is very elementary but very important, and it will be used repeatedly in the rest of the course. To state it, we require one standard definition: for any extensions $\alpha : K \to M$ and $\beta : K \to L$, let $\mathrm{Hom}_K(M, L)$ denote the set of field homomorphisms $\gamma : M \to L$ such that $\beta = \gamma \circ \alpha$.

toring by simple extensions

Proposition 17 *Let $\alpha : K \to K(u)$ be a finite simple extension. Let $\beta : K \to L$ be any homomorphism. Then*

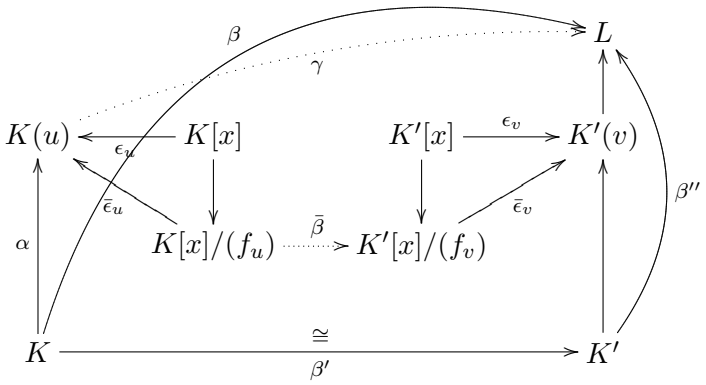
$$\begin{aligned} \epsilon_u : \mathrm{Hom}_K(K(u), L) &\to L \\ \gamma &\mapsto \gamma(u) \end{aligned}$$

is injective and maps onto the set of roots of $\beta_x(m_{u,K})$ in L.

Proof. Suppose $\gamma \in \mathrm{Hom}_K(K(u), L)$ and let $v = \epsilon_u(\gamma)$, so $v = \gamma(u)$. Then $\beta_x(m_{u,K})(v) = \beta_x(m_{u,K})(\gamma(v)) = \gamma_x \circ \alpha_x(m_{u,K}(\gamma(u)) = \gamma(\alpha_x(m_{u,K})(u)) =$

$\gamma(0) = 0$, so v is a root of $\beta_x(m_{u,K})$ in L. Moreover, it is clear that γ is completely determined by $\gamma(u)$, since its domain of $K(u)$, it is K-linear, and $K(u)$ is simple and generated by u. Thus, the map $\epsilon_u : \gamma \mapsto \gamma(u)$ is injective on $\mathrm{Hom}_K(K(u), L)$ and maps into the set of roots of $\beta_x(m_{u,K})$ in L.

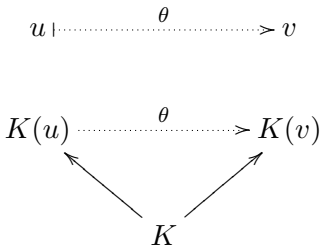
Next we show that $\epsilon_u : \mathrm{Hom}_K(K(u), L) \to L$ maps onto the set of roots of $\beta_x(m_{u,K})$ in L. Let v be a root of $\beta_x(m_{u,K})$ in L. We will construct an extension $\gamma : K(u) \to L$ from $\mathrm{Hom}_K(K(u), L)$. Begin by factoring $\beta = \beta'' \circ \beta'$ where β' is an isomorphism and β'' is an inclusion and consider the diagramme below, which is created using the FIT.



Define: $\gamma := \bar{\epsilon}_v \circ \bar{\beta} \circ \bar{\epsilon}_u^{-1}$. Clearly this is an element of $\mathrm{Hom}_K(K(u), L)$. ■

corollary: A1

Corollary 4 *If $K \to K(u)$ and $K \to K(v)$ are finite extensions then there is some $\theta \in \mathrm{Hom}_K(K(u), K(v))$ with $\theta(u) = v$ if and only if $m_{u,K} = m_{v,K}$; in this case, θ is an isomorphism and is unique.*

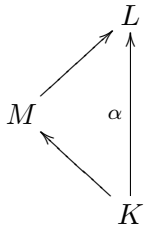


4.5 Universal property of simple extensions

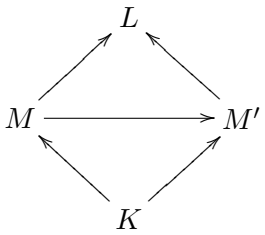
Simple extensions satisfy a universal property. To understand this, we require a new definition.

ion: intermediate category

Definition 13 *Let $\alpha : K \to L$ be a field homomorphism. In the category of fields intermediate between K and L, denoted by $\text{INT}(L/K)$, objects are commuting triangles*



and maps are commuting diagrammes



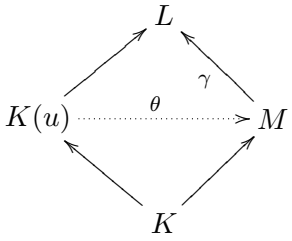
where $K \to M \to L$ and $K \to M' \to L$ are objects. Composition and identities are defined in the obvious way.

lemma: simple universal

Lemma 9 *Let $\alpha : K \to L$ be a field homomorphism. Suppose $u \in L$. Then $\alpha(K)(u)$ is an object of $\text{INT}(L/K)$ and it satisfies the following univeral property: if $K \to M \xrightarrow{\gamma} L$ is an object of $\text{INT}(L/K)$ and $u \in \gamma(M)$, then there is a unique $\theta : \alpha(K)(u) \to M$ such that Diagramme 4.1 commutes.*

diagramme: simple universal

(4.1) diagramme: simple



definition: simple

Proof. By definition (Definition 12), $K(u)$ is a subset of L, contains $\alpha(K)$, and is also a field; thus $\alpha(K)(u)$ is a subfield of L and an extension of K. In other words, $\alpha(K)(u)$ is an object of $\text{INT}(K/L)$ with $\alpha_u : K \to K(u)$ given by $\alpha_u(k) = \alpha(k)$ and $\alpha(K)(u) \to L$ given by inclusion.

Now, suppose $K \xrightarrow{\beta} M \xrightarrow{\gamma} L$ is an object of $\text{INT}(L/K)$; thus, $\alpha = \gamma \circ \beta$. Suppose $u \in \gamma(M)$. Then $u = \gamma(v)$ for a unique $v \in M$. Using Proposition 12, define $\theta : K(u) \to M$ by $\theta(u) = v$ and $\theta(\alpha(a)) = \beta(a)$ for each

proposition: simple

$a \in K$. By the second part of this definition, $\theta \circ \alpha_u = \beta$. By the first part of the definition of θ, $\gamma(\theta(u)) = \gamma(v) = u$; since $u = \alpha^u(u)$, it follows from Corollary 3 that $\gamma \circ \theta = \alpha^u$. Thus, the diagramme above commutes.

To see that θ is the unique field homomorphism making the diagramme commute, suppose $\theta' : \alpha(K)(u) \to M$ also has this property. Then $\gamma(\theta'(u)) = \gamma(\theta(u))$. Since γ is injective, $\theta'(u) = \theta(u)$. Thus, $\theta' = \theta$ by Corollary 3 again. ■

4.6 Chapter 4 exercises

Exercise 4.1 *Prove Proposition 12.*

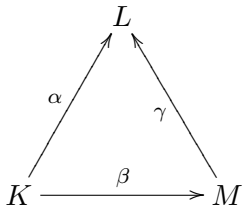
Exercise 4.2 *Suppose $K \to K(u)$ is a finite simple extension. Define $T_u : K(u) \to K(u)$ by $T_u(x) = xu$. Then T_u is clearly K-linear. Show that the characteristic polynomial of T_u is the minimal polynomial for u over K.*

Exercise 4.3 *In $K(t)$ (rational functions in t), consider the subfield $K(u)$ where $u = t^2$. Show that the extension $K(u) \to K(t)$ is algebraic.*

Exercise 4.4 *Fix $K \to L$. Fix $u, v \in L$. Show that $K(u)(v) = K(v)(u) = K(u, v)$. Conclude that $K(u_1, \ldots, u_i) = K(u_1, \ldots, u_{i-1})(u_i)$ for each $1 \leq i \leq n$.*

Exercise 4.5 *Suppose u is algebraic over K, not contained in K, and that v is transcendental over K. Show that $K \to K(u, v)$ is not simple.*

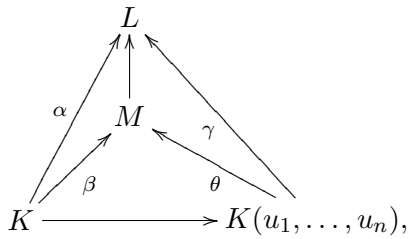
Exercise 4.6 *Let $\alpha : K \to L$ be a field homomorphism. Fix $\{u_1, \ldots, u_n\} \subset L$. Show that $K \to K(u_1, \ldots, u_n) \to L$ satisfies the following universal property: if the following diagramme commutes,*



with $\{u_1, \ldots, u_n\} \subset \mathrm{im}\gamma$, then there is a unique field homomorphism

$$\theta : K(u_1, \ldots, u_n) \to M$$

such that the following diagramme commutes



where $K \to K(u_1, \ldots, u_n) \to L$ *are given above.*

Exercise 4.7 *Let* $K \to L$ *be a field homomorphism. Suppose* $u_1, \ldots, u_n \in L$ *are algebraic over* K*. Then* $K[u_1, \ldots, u_n] = K(u_1, \ldots, u_n)$*.*

Chapter 5

Profinite Extensions

ofinite extensions

5.1 Finitely generated extensions

ection: generated

It is not true that every algebraic extension is finite. To explore this issue further, we require another definition.

nition: generated

Definition 14 *Let $\alpha : K \to L$ be a field extension and let X be a subset of L. Let $K(X)$ denote the intersection (in L) of all subfields of L which contain X and $\alpha(K)$; this is called the extension (of K) generated by X.*

definition: generated definition: simple

Observe that Definition 14 extends Definition 12; in particular, for every K and $u \in L$, the simple extension $K \to K(u)$ is the extension generated by $\{u\}$.

Example 1 *The simple extension $\mathbb{Q} \to \mathbb{Q}(x)$ is generated by x and the simple extension $\mathbb{Q} \to \mathbb{Q}(e^{2\pi i/n})$ is generated by $e^{2\pi i/n}$; observe that $\mathbb{Q} \to \mathbb{Q}(x)$ an infinite extension if and only if x is transcendental over $\mathbb{Q}$, while $\mathbb{Q} \to \mathbb{Q}(e^{2\pi i/n})$ is a finite extension.*

sition: generated

Proposition 18 *Let $K \to L$ be a field homomorphism and let X be a subset of L. Then*

$$K(X) = \bigcup_{\substack{Y \subseteq X \\ Y \text{ finite}}} K(Y).$$

exercise: generated

Proof. (Exercise 5.1.) ■

enerated extension

Proposition 19 *Let $K \to L$ be a field homomorphism and let X be a subset of L. Then $K \to K(X)$ is algebraic if and only if each $u \in X$ is algebraic over K. If this is the case and X is finite, then $K \to K(X)$ is finite.*

Proof. (Exercise 5.2.) ■

nition: finitely generated

Definition 15 *If Y is a finite set, then $K \to K(Y)$ is said to be finitely generated over K.*

raic and finitely generated

Proposition 20 *$K \to L$ is finite if and only if it is algebraic and finitely generated.*

Proof. Suppose $K \to L$ is finite. In Proposition 10 we have already seen that $K \to L$ is algebraic. Let $n = \dim_K(L)$ and let $(u_1, u_2, \ldots, u_n)$ be a basis for L as a vector space over K. Then every element of L takes the form $\sum_i k_i \cdot u_i$ with $k_i \in K$. Thus, $L \subseteq K(u_1, u_2, \ldots, u_n)$, and in fact, $L = K(u_1, u_2, \ldots, u_n)$. Thus, $K \to L$ is finitely generated.

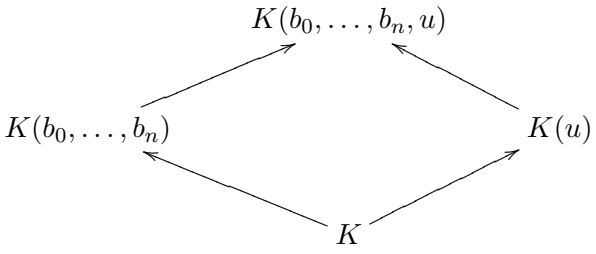
Conversely, suppose $K \to L$ is algebraic and finitely generated. Then $L = K(u_1, u_2, \ldots, u_n)$ where each u_i is algebraic over K. By Exercise **??**, $K(u_1, \ldots, u_i) = K(u_1, \ldots, u_{i-1})(u_i)$ for each $1 \leq i \leq n$. Thus, $K \to L$ can be written as a composition of finite extensions. The result now follows from Proposition 9. ■

As an application of these ideas, we are now able to prove the converse of Lemma 6.

tion: algebraic permanence

Proposition 21 *Suppose $\alpha = \beta \circ \gamma$. Then α is algebraic if and only if β and γ are algebraic.*

Proof. In Lemma 6 we showed that if α is algebraic then so are β and γ; here we prove the converse. Suppose, therefore, that $\beta : M \to L$ and $\gamma : K \to M$ are algebraic. Pick $u \in L$. Consider $m_{u,M} \in M[x]^\times$, which exists since $\beta : M \to L$ is algebraic. Write $m_{u,M} = \sum_{i=0}^{n} b_i x^i$ and consider the diagramme below.



Since $\gamma : K \to M$ is algebraic and $b_i \in M$ for each $1 \leq i \leq n$, it follows from Proposition 19 that $K \to K(b_0, \ldots, b_n)$ is finite. Since u is a root of $\beta_x(m_{u,M}) \in K(b_0, \ldots, b_n)[x]$, it follows that u is algebraic over $K(b_0, \ldots, b_n)$,

so $K(b_0, \ldots, b_n) \to b_0, \ldots, b_n, u)$ is finite. Thus, the two extensions on the left-hand side of the diagramme above are finite. It now follows from Proposition 9 that $K \to K(u)$ is finite, so u is algebraic over K (again, by Proposition 19). ■

proposition: tower law
proposition: generated extension

5.2 Profinite extensions

rofinite extension

Definition 16 *A field homomorphism $\alpha : K \to L$ is profinite if it is a direct limit of finite extensions of K.*

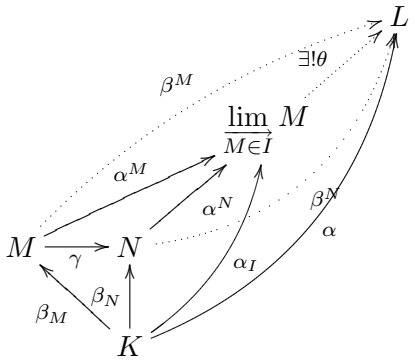
In fact, this notion is equivalent to the definition of 'algebraic extension', as we shall soon see. As preparation for the proof of this fact, we consider an important example of a category of finite extensions of K.

raic iff profinite

Proposition 22 *Every algebraic extension is profinite and every profinite extension is algebraic.*

Proof. Suppose $\alpha : K \to L$ is algebraic. Let $I = I(L/K)$ denote the category of intermediate fields M for which $[M : K]$ is finite. Let F denote the forgetful functor from I to the category of extensions of K. Then he colimit of F over I is precisely the direct limit $\varinjlim_{M \in I} M$. Also observe that I has an initial object (K itself is finite extension of K contained in L) as thus the direct limit in question does indeed exist. In particular, $\varinjlim_{M \in I} M$ is a field equipped with a map $\alpha_I : K \to \varinjlim_{M \in I} M$. We will exhibit an isomorphism $\theta : \varinjlim_{M \in I} M \to L$ in the category of extensions of K (which is to say, $\alpha = \theta \circ \alpha_I$).

Recall the universal property of $\varinjlim_{M \in I} M$: for each $\gamma : M \to N$ in I there are maps α^M and α^N and θ pictured below making the diagramme commute.



Moreover, for every $M \in I$, the map α^M is defined by $\alpha^M(u) = [u]_M$, where, as in Section **??**, $[u]_M$ denotes the equivalence class of $u \in M$ in the disjoint union $\coprod_{M \in I} M$ under the equivalence relation $u \sim u'$ defined by $\gamma(u) = \gamma'(u')$ for some map γ from I. We claim that θ is an isomorphism; to show this, we will exhibit its inverse.

Suppose $u \in L$ and consider $\alpha_u : K \to K(u)$ (see Definition 12). Since $K \to L$ is algebraic, the simple extension $\alpha_u : K \to K(u)$ is finite, by Proposition 14. Since $K(u)$ is a subset of L, it comes equipped with a field homomorphism into L, which we denote $\beta^{K(u)} : K(u) \to L$. Thus, $K(u)$ is an object in category I. Notice that $\beta^{K(u)}(u) = u$. Using notation from Section **??**, define $\theta' : L \to \varinjlim_{M \in I} M$ by $\theta'(u) = [u]_{K(u)}$; thus, $\theta'(u) = \alpha^{K(u)}(u)$. Then, for each $u \in L$,

$$\begin{aligned} \theta \circ \theta'(u) &= \theta([u]_{K(u)}) \\ &= \theta \circ \alpha^{K(u)}(u) \\ &= \beta^{K(u)}(u) \\ &= u \end{aligned}$$

and

$$\begin{aligned} \theta' \circ \theta([u]_{K(u)}) &= \theta' \circ \theta(\alpha^{K(u)}(u)) \\ &= \theta' \circ \theta \circ \alpha^{K(u)}(u) \\ &= \theta' \circ \beta^{K(u)}(u) \\ &= \theta'(u) \\ &= [u]_{K(u)} \end{aligned}$$

so $\theta' = \theta^{-1}$. This completes the proof of the first statement of Proposition 22.

The second part of Proposition 22 is easy to prove. Suppose $\alpha : K \to L$ is profinite; thus, there is some category I of finite extensions of K, and an isomorphism $\theta : \varinjlim_{M \in I} M \to L$ with $\alpha = \theta \circ \alpha_I$, where $\alpha_I : K \to \varinjlim_{M \in I} M$. Each element of $\varinjlim_{M \in I} M$ takes the form $[u]_M$ for some $M \in I$ and some $u \in M$ (see Section **??**). But $M \in I$ implies $K \to M$ is finite, which implies $K \to M$ is algebraic, by Proposition 10. Thus, $u \in M$ is algebraic. By Proposition 8, it follows that $\alpha_I : K \to \varinjlim_{M \in I} M$ is algebraic. Since $\alpha = \theta \circ \alpha_I$, it follows from Proposition 21 that α is algebraic, thus completing the proof of Proposition 22. ■

chapter: profinite extensions

5.3 Chapter 5 exercises

ercise: generated

Exercise 5.1 *Prove Proposition* proposition: generated *18.*

enerated extension

Exercise 5.2 *Prove Proposition* proposition: generated extension *19.*

se: direct limits

Exercise 5.3 *Show that direct limits exist in the category of fields and in the category of extensions of K.*