The Fellowship of the Group

September 7, 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.

One of the most important objects in mathematics today is the group consisting of those ring automorphisms of an algebraic closure of the rational numbers that fix every rational number. This group – called the absolute Galois group of $\mathbb{Q}$ and denoted $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ – 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). 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. As such, these notes assume a good undergraduate background in groups, rings, topology, and a little complex analysis; a knowledge of the basic definitions of category theory (functors, natural transformations, adjunctions, limits and colimits, products and co-products, push-out and pull-back) is also assumed.[1]

[1] I would like to add a brief appendix on category theory which will review these notions;

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 Roberts 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

for now, however, this appendix is under construction.

objects in mathematics. 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 representations.

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 this book 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. Welcome to the Fellowship of the Group.

Contents

Chapter 1

The 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.*

Example 1 $\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$ *is not a field because* 2 *is not a unit. By contrast,* $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2 + x + 1)$ *is a field with four elements.*

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

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. 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.

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. ■

The next proposition will not be used very often in these notes, but it does makes clear just how thoroughly we adopt the Axiom of Choice. Let $\mathrm{Spec}(A)$ denote the set of prime ideals of A; this is commonly referred to as the **prime ideal spectrum** of A. Observe that $\mathrm{Specm}(A) \subseteq \mathrm{Spec}(A)$.

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, $\mathrm{Spec}(A) = \{(0)\}$.

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 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 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!

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.

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow & & \uparrow \\ A/\ker\phi & \xrightarrow[\cong]{} & \mathrm{im}\phi \end{array}$$

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.

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 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 Galois 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. 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

For any field L, the **category of subfields** of L — denoted $\textsc{sub}(L)$ — is the category in which: objects are subfields of L, which is to say, field homomorphisms $\alpha : M \to L$; and maps from the subfield $\alpha : M \to L$ to the subfield $\beta : N \to L$ are field homomorphisms $\gamma : M \to N$ such that $\alpha = \beta \circ \gamma$. You should think of a map in $\textsc{sub}(L)$ as a commuting triangle.

$$\begin{array}{ccc} & L & \\ {\scriptstyle\alpha}\nearrow & & \nwarrow{\scriptstyle\beta} \\ M & \xrightarrow[\gamma]{} & N \end{array} \tag{1.1}$$

Composition of maps in $\textsc{sub}(L)$ is defined in the obvious way. The category $\textsc{sub}(L)$ will be of primary importance in this course.

For any group G, the **category of subgroups of** G — denoted $\textsc{sub}(G)$ — is the category in which: objects are injective group homomorphisms into G; and maps from $f_1 : G_1 \to G$ to $f_2 : G_2 \to G$ are group homorphisms $h : G_1 \to G_2$ such that $f_1 = h \circ f_2$. As above, you should think of a homomorphism in $\textsc{sub}(G)$ as a commuting triangle.

$$\begin{array}{ccc} & G & \\ {\scriptstyle f_1}\nearrow & & \nwarrow{\scriptstyle f_2} \\ G_1 & \xrightarrow[h]{} & G_2 \end{array} \tag{1.2}$$

Composition of maps in $\textsc{sub}(G)$ is defined in the obvious way.

1.3 The Galois functors

The Galois correspondence is a pair of contravariant functors, one from $\textsc{sub}(L)$ to $\textsc{sub}(\mathrm{Aut}(L))$, and the other functor in the opposite direction. In

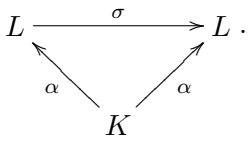
this section we define these functors; in the next section we show that they form an adjoint pair of contravariant functors.

Throughout this section, L is a fixed but arbitrary field.

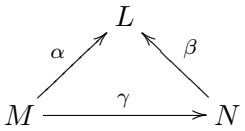
Let $\alpha : K \to L$ be a subfield. The group $\mathrm{Aut}(L/K)$ of **automorphisms of L over K** is defined by

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

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

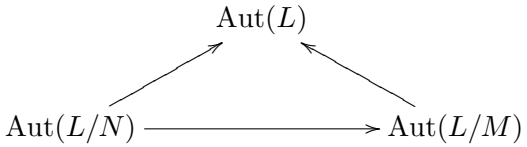


Next, let γ be a map in the category of subfields of L; thus, γ is a commuting triangle



(1.3)

Consider the commuting triangle



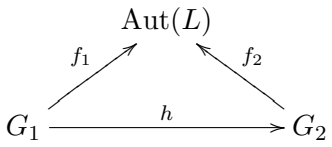
(1.4)

where each arrow is the map $\sigma \mapsto \sigma$, which is clearly a group monomorphism. To see that that $\mathrm{Aut}(L/M)$ is a subgroup of $\mathrm{Aut}(L/N)$, argue as follows. Suppose $\sigma \in \mathrm{Aut}(L/M)$. Then $\sigma \circ \beta = \beta$. Pre-compose with γ to give $\sigma \circ \beta \circ \gamma = \beta \circ \gamma$. Since $\alpha = \beta \circ \gamma$ we have $\sigma \circ \alpha = \alpha$, from which is follows that $\sigma \in \mathrm{Aut}(L/M)$.

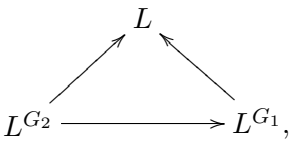
We now define a functor from $\textsc{sub}(\mathrm{Aut}(L))$ to $\textsc{sub}(L)$. Let $f : G \to \mathrm{Aut}(L)$ be an object in the category of subgroups of $\mathrm{Aut}(L)$; thus, $f : G \to \mathrm{Aut}(L)$ is an injective group homomorphism. Let L^G be the field of elements of L fixed by the action of G on L given by $f : G \to \mathrm{Aut}(L)$; thus,

$$L^G = \{u \in L \;\big|\; f(g)(u) = u, \forall g \in G\}.$$

Since L^G is a field, L^G is an object in $\text{SUB}(L)$. Next, consider the map h in the category of subgroup of $\text{Aut}(L)$ given by the following triangle



let L^h denote the map in the category of subfields of L given by the triangle



where the group homomorphisms are all inclusions. To see that this is defined, we must check that $u \in L^{G_2}$ implies $u \in L^{G_1}$. To that end, suppose $u \in L^{G_2}$. Then $f_2(g_2)(u) = u$ for all $g_2 \in G_2$. Suppose $g_1 \in G_2$. Then $h(g_1) \in G_2$, so $f_2(h(g_1))(u) = u$. Since $f_2(h(g_1)) = f_2 \circ h(g_1)$ and since $f_2 \circ h = f_1$, it follows that $f_1(g_1)(u) = u$. Since this is true for all $g_1 \in G_1$, we have shown that $u \in L^{G_1}$.

This section is summarised by the following definition.

Definition 2 *Let L be a fixed but arbitrary field. The* **Galois functors** *for L is the pair of contravariant functors $(\text{Aut}(L/\ ), \text{Fix}(L/\ ))$, where $\text{Aut}(L/\ ) : \text{SUB}(L) \to \text{SUB}(\text{Aut}(L))$ is defined by*

$$\text{Aut}(L/\ ): \qquad \text{SUB}(L) \longrightarrow \text{SUB}(\text{Aut}(L))$$

$$\textit{(objects)} \qquad K \longmapsto \text{Aut}(L/K)$$

$$\textit{(maps)} \qquad (M \to N) \longmapsto (\text{Aut}(L/M) \hookrightarrow \text{Aut}(L/N)).$$

and $\text{Fix}(\ /L) : \text{SUB}(\text{Aut}(L)) \to \text{SUB}(L)$ *is defined by*

$$\text{Fix}(\ /L): \qquad \text{SUB}(\text{Aut}(L)) \longrightarrow \text{SUB}(L)$$

$$\textit{(objects)} \qquad G \longmapsto L^G$$

$$\textit{(maps)} \qquad (G_1 \to G_2) \longmapsto (L^{G_2} \hookrightarrow L^{G_2}).$$

1.4 The Galois adjunction

Having just defined a pair of 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.

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

Proof. We begin by defining a natural transformation

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

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

$$\begin{array}{ccc} & & L \\ & \overset{\alpha}{\nearrow} & \\ K & \xrightarrow{\mathcal{F}_L(\alpha)} & L^{\mathrm{Aut}(L/K)} \end{array}$$

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

To see that $\mathcal{F}_L$ is a natural transformation, observe that the following diagramme commutes if $\gamma : M \to N$ is a map of subfields from $\alpha : M \to L$ to

$\beta : N \to L$, in which case $\alpha = \beta \circ \gamma$.

$$\begin{array}{ccc} M & \xrightarrow{\mathcal{F}_L(\alpha)} & L^{\mathrm{Aut}(L/M)} \\ {\scriptstyle\gamma}\downarrow & & \downarrow \\ N & \xrightarrow[\mathcal{F}_L(\beta)]{} & L^{\mathrm{Aut}(L/N)} \end{array}$$

Next, we define a natural transformation

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

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

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

Now, let $\mathcal{G}_L(G)$ be the map (in the category of subgroups of $\mathrm{Aut}(L)$) from $G \to \mathrm{Aut}(L)$ to $\mathrm{Aut}_{L^H}(L) \to \mathrm{Aut}(L)$ given by the triangle

$$\begin{array}{ccc} & \mathrm{Aut}(L) & \\ {\scriptstyle f}\nearrow & & \nwarrow \\ G & \xrightarrow{\mathcal{G}_L(f)} & \mathrm{Aut}_{L^H}(L) \end{array}$$

$$g \longmapsto f(g)$$

We leave it to the reader to demonstrate that $\mathcal{G}_L$, just defined, is indeed a natural transformation. ■

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 ending this section, we make one more observation concerning the Galois functors $(\mathrm{Aut}(L/\ ), \mathrm{Fix}(\ /L))$.

Proposition 6

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

Proof. The natural transformation $\mathcal{F}_L$ induces an isomorphism of functors

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

because

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

for every subfield K of L, and the natural transformation $\mathcal{G}_L$ induces an isomorphism of functors

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

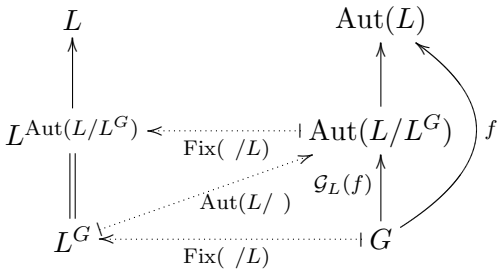
because

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

for every subgroup G of $\mathrm{Aut}(L)$. ■

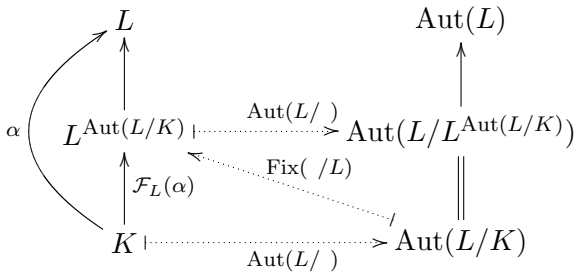
Here is another way to represent what we have just learned:

$\textsc{sub}(L)$ $\qquad\qquad$ $\textsc{sub}(\mathrm{Aut}(L))$



and

$\textsc{sub}(L)$ $\qquad\qquad$ $\textsc{sub}(\mathrm{Aut}(L))$



1.5 Kaplansky subfields

Definition 3 *Let L be a field. A subfield K of L is a* **Kaplansky subfield** *of L if*

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

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

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

In otherwords, $K \to L$ is Kaplansky if $\mathcal{F}_L(K)$ is an isomorphism, and $G \to \mathrm{Aut}(L)$ is Kaplansky if $\mathcal{G}_L(G)$ is an isomorphism.

Thus, these notions define two full subcategories and an equivalence between them.

Definition 4 *The* **category of Kaplansky subfields of** *L is the full subcategory of* $\textsc{sub}(L)$ *consisting of Kaplansky subfields. Likewise, the* **category of Kaplansky subgroups of** $\mathrm{Aut}(L)$ *is the full subcategory of* $\textsc{sub}(\mathrm{Aut}(L))$ *consisting of Kaplansky subgroups.*

Proposition 7 $\mathrm{Aut}(L/\ )$ *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.*

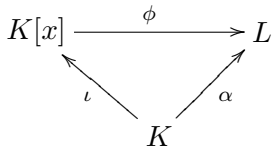
Proof. (Exercise 15.) ■

In this course we will restrict our attention to subfields of L which satisfy a further condition, as explained in Section 1.6.

1.6 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 $\iota : L \to L[x]$ 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 1 *If $\phi \in \mathrm{Hom}_K(K[x], L)$ then $\ker \phi$ is a prime ideal of $K[x]$.*

Proof. If $p_1 p_2 \in \ker \phi$ then $\phi(p_1 p_2) = 0$ 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 $p_2 \in \ker \phi$. ■

Definition 5 *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**.

Some of you may recognize the geometric nature of this definition. 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 5 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.*

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

Lemma 2 *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 moments 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

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

■

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

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

Proof. (Exercise 19.) ■

Proposition 8 leads to the following definition.

Definition 6 *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.

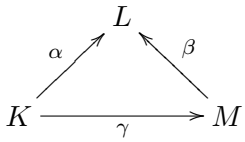
Lemma 3 *If $K \to L$ is algebraic then $\mathrm{End}(L/K) = \mathrm{Aut}(L/K)$.*

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. (Here we used the hypothesis that L is algebraic over K and Proposition 8.) Then σ restricts of a map $X \to X$. Since σ is injective (Proposition 4), so is the function $X \to X$. Since X is finite, $X \to X$ is also surjective. Thus, there is some $v \in X$ such that $\sigma(v) = u$, concluding the proof of Lemma 3. ■

Lemma 4 *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. ■

Lemma 5 *Suppose $\alpha = \beta \circ \gamma$. If α is algebraic then β and γ are algebraic.*



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

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

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

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

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

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

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

In fact, the converse to Lemma 5 is also true, but the proof result requires more work (see Proposition 18).

1.7 Galois subfields/extensions

Definition 7 *Let L be a field. A Kaplansky subfield K of L is a* **Galois subfield** *of L (or a* **Galois extension** *of K) if it is an algebraic extension.*

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 19 now and work backward through the text.)

In Chapter 3 we assemble various important properties of Galois subfields, and ultimately find a completely different characterization of Galois extensions (Theorem 9). For now, we make a very simple observations concerning Galois extensions.

Lemma 6 *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 $\mathcal{F}_L$ from Section 1.4, we see that $\mathcal{F}_L(\alpha) = \alpha$. Since α is an isomorphism it follows from Definition 3 that α is Kaplansky. We already saw (Lemma 4 that α is algebraic, so α is Galois, by Definition 7. ■

In due course we will see that if $\beta \circ \alpha$ is Galois then β is Galois, but α need not be Galois. We will also see that if α and β are both Galois, it does not follows that $\beta \circ \alpha$ is Galois. However, if α is Galois and β is arbitrary, then a push-out (α, β') of (α, β) exists, and α' is Galois.

1.8 Chapter 1 exercises

Exercise 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 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 3 *Recall that every maximal ideal is prime, so $\mathrm{Specm}(A) \subseteq \mathrm{Spec}(A)$. 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 4 *If K is a field then* $\mathrm{Spec}(K) = \{(0)\}$*, 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* $\mathrm{Spec}(A)$ *is a singleton, does it follow that A is a field?*

Exercise 5 *If K is a field then* $\mathrm{Spec}(K[x]) = \mathrm{Specm}(K[x]) \cup \{(0)\}$*. Let A be a non-zero cring. If* $\mathrm{Spec}(A[x]) = \mathrm{Specm}(A[x]) \cup \{(0)\}$*, does it follows that A is a field?*

Exercise 6 *Find* the *addition and multiplication table for a field $\mathbb{F}_9$ with nine distinct elements. Find a non-isomorphic cring with R nine elements. Find the isomorphism type of the group $\mathbb{F}_9^\times$ of units in $\mathbb{F}_9$; likewise for R^*. List all groups of order $|\mathbb{F}_9^\times|$, up to isomorphism.*

Exercise 7 *Let L be a field and let L_0 denote the prime subfield of L. Show that* $\mathrm{Aut}(L) = \mathrm{Aut}_{L_0}(L)$*.*

Exercise 8 *Let R be a cring. Prove the following: If $r \in R$ is a unit then r is not a zero-divisor. Is the converse true? What if R is finite?*

Exercise 9 *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* $\mathrm{Spec}(\phi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *by* $\mathrm{Spec}(\phi)(\mathfrak{p}) = \phi^{-1}\mathfrak{p}$*. Extend this definition to a contrariant functor from the category of crings to the category of sets. (This functor lies at the heart of algebraic geometry.)*

Exercise 10 *Let L be a field. Show that* $\mathrm{id}_L : L \to L$ *is a termimal 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 11 *Let L be a field and let L_0 denote the prime subfield of L. Show that there is a canonical isomorphism of groups* $\mathrm{Aut}_{L_0}(L) \cong \mathrm{Aut}(L)$*. More generally, let $K \to L$ be any map of fields and let K_0 be the prime subfield of K. Show that there is a canonical isomorphism of groups* $\mathrm{Aut}_{K_0}(L) \cong \mathrm{Aut}(L)$*.*

Exercise 12 *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 13 *Suppose $X \to Z$ and $Y \to Z$ are group homomorphisms in Diagramme 1.2. Show that, together with the fact that the triangle commutes, it follows that the group homomorphism $X \to Y$ is also a group monomorphism.*

Exercise 14 *Notice that the Galois group of* $\mathbb{Q}(t)$ *over* $\mathbb{Q}$ *includes* $t \mapsto \frac{at+b}{ct+d}$ *for all* $ad-bc \neq 0$. *Thus,* $PGL(2,\mathbb{Q}) \subseteq \mathrm{Gal}(\mathbb{Q}(t)/\mathbb{Q})$. *(We will see later that these two groups are equal!) Thus,* $\mathrm{Gal}(\mathbb{Q}(t)/\mathbb{Q})$ *is infinite and non-abelian, since* $PGL(2,\mathbb{Q})$ *is infinite and non-abelian.*

Exercise 15 *Prove Proposition 7.*

Exercise 16 *Let* L *be a field. Show, as claimed above, that* $\mathrm{Gal}(L/\ )$ *is an equivalence from the category of Kaplansky subfields of* L *to the category of Kaplansky subgroups of* $\mathrm{Aut}(L)$.

Exercise 17 *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 18 *If* K *is a field then* $\mathrm{Spec}(K) = \{(0)\}$, *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* $\mathrm{Spec}(A)$ *is a singleton, does it follow that* A *is a field?*

Exercise 19 *Prove Proposition 8.*

Exercise 20 *Show that* $\mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2})$ *is not Kaplansky, while* $\mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ *is Kaplansky. Is* $\mathbb{Q} \to \mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$ *Kaplansky? Also, show that* $\mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt[4]{2})$ *are both Kaplansky, but the composition* $\mathbb{Q} \to \mathbb{Q}(\sqrt[4]{2})$ *is not Kaplansky.*

Exercise 21 *Let* L *be a field. Show that the category of subfields of* L *contains products, co-products, pull-backs and push-outs.*

Chapter 2

Finite and Profinite Extensions

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

Definition 8 *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***.*

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

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

Proof. Clearly, this proposition is a consequence of the following statement: if $\{u_i \mid i \in I\}$ is a basis for L over M and $\{v_j \mid j \in J\}$ is a basis for M over K, then $\{u_i v_j \mid (i, j) \in I \times J\}$ 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 M,

we write $u = \sum_{i\in I} a_i u_i$ for some $a_i \in M$. Since $\{v_j \mid j \in J\}$ is a basis for M over K, we write $a_i = \sum_{j\in J} b_{ij} v_j$ for some $b_{ij} \in K$. Therefore, $u = \sum_{i\in I} a_i u_i = \sum_{i\in I} u_i \sum_{j\in J} b_{ij} v_j = \sum_{(i,j)\in I\times J} b_{ij} u_i v_j$. This shows that $\{u_i v_j \mid (i,j) \in I \times J\}$ spans L over K. To see that $\{u_i v_j \mid (i,j) \in I \times J\}$ is linearly independent, suppose $\sum_{(i,j)\in I\times J} c_{ij} u_i v_j = 0$ with $c_{ij} \in K$. Then $\sum_{j\in J} v_j \sum_{i\in I} c_{ij} u_i = 0$. Since $\sum_{i\in I} c_{ij} u_i \in M$ and $\{v_j \mid j \in J\}$ is a basis for M over K, it follows that $\sum_{i\in I} c_{ij} u_i = 0$ for each $j \in J$. Since $c_{ij} \in K$ and $\{u_i \mid i \in I\}$ is a basis for L over M, it follows that $c_{ij} = 0$ for each $i \in I$ and $j \in J$. This shows that $\{u_i v_j \mid (i,j) \in I \times J\}$ is linearly independent over K and completes the proof that $\{u_i v_j \mid (i,j) \in I \times J\}$ is a basis for L over K. ■

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

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

Proof. Suppose $K \to L$ 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, $\sum_i a_i \cdot u^i = 0$ 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. ■

2.2 Simple extensions

Definition 9 *Let $\alpha : K \to L$ be a field extension and let u be an element of L. Let $K(u)$ denote the intersection in L of all subsets of L which contain u, $\alpha(K)$ and are fields. Define $\alpha_{K(u)} : K \to K(u)$ by $\alpha_{K(u)}(x) = \alpha(x)$; thus, $\alpha_{K(u)}$ is just α with restricted codomain. Then $\alpha_{K(u)} : K \to K(u)$ is a* **simple extension**.

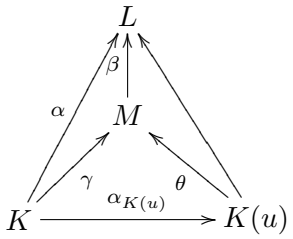
In fact, the simple extension $K \to K(u)$ admits another description, which is very useful.

Lemma 7 *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 $K[u]$ denote the image of $\epsilon_u \circ \alpha_x$, where $\alpha_x : K[x] \to L[x]$ is the obvious cring homomorphism. Then $K(u)$ is the quotient field of the integral domain $K[u]$.*

Proof. (Exercise 22.) ■

Lemma 8 *Let $\alpha : K \to L$ be a field homomorphism. Suppose $u \in L$. Then $K(u)$ is intermediate between K and L and has the following univeral property: If $\alpha = \beta \circ \gamma$ and $u \in \mathrm{im}(\beta)$, then there is a unique $\theta : K(u) \to \mathrm{dom}(\beta)$ such that $\beta \circ \delta = \alpha^{K(u)}$.*

Proof. (Exercise 23.) ■



Proposition 11 *Let $K \to L$ be a field homomorphism. Then $K \to K(u)$ is finite if and only if u is algebraic over K, in which case $K[u] = K(u)$.*

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 11.

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 Lemma 7). On the other hand, $\ker(\epsilon_u \circ \alpha_x) = (m_{u,K})$, which is a maximal ideal (see Definition 5). 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. ■

The next proposition is almost just a corollary of this proof, but it is well worth stating on its own.

Proposition 12 *Let $K \to L$ 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 $K(u)$ over K. In particular, $K \to K(u)$ is finite and $[K(u) : K] = \deg(m_{u,K})$.*

Proof. Pick $a \in K(u)$. By Definition 9 and Proposition 11 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 $g = hm_{K,u}$ 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 $n = [K(u) : K]$. ■

Proposition 13 *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 12), it follows that σ is completely determined by the condition $\sigma(u) = u_i$ for some i.

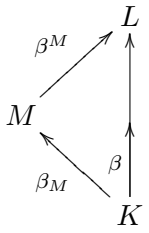
It remains to show that each i from 1 to k actually corresponds to an automorphism of $K(u)$ over K. Let us see if we can define an automorphism σ_i in $\mathrm{Aut}(K(u))/K)$ by the conditions: $\sigma(u) = u_i$ and $\sigma(c) = c$ for each $c \in K$. Recall that $K(u) = K[u]$, by Proposition 11. Thus, 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. ■

2.3 Profinite extensions

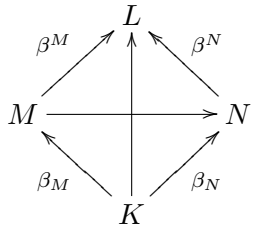
Definition 10 *We say that a field homomorphism $\alpha : K \to L$ is* **profinite** *if it is a direct limit of extensions of K.*

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.

Let $K \to L$ be an algebraic extension. Let $I = I(L/K)$ denote the category of fields intermediate between K and L and which are finite extensions of K; thus, objects of I are commuting triangles



with $[M : K]$ finite, and maps are commuting diagrammes



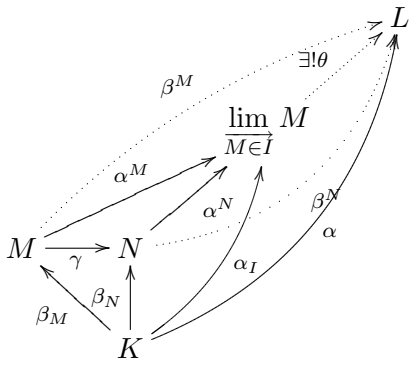
where $[M : K]$ and $[N : K]$ are finite.

Proposition 14 *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 $\varinjlim_{M \in I} M$ (see Proposition 56): 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 9.5, $[u]_M$ 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 $\alpha_{K(u)} : K \to K(u)$ (see Definition 9). Since $K \to L$ is algebraic, the simple extension $\alpha_{K(u)} : K \to K(u)$ is finite, by Proposition 12. 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 9.5, 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 14.

The second part of Proposition 14 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 9.5). 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 18 that α is algebraic, thus completing the proof of Proposition 14. ■

2.4 Generated extensions

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

Definition 11 *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.**

Observe that Definition 11 extends Definition 9; in particular, for every K and $u \in L$, the simple extension $K \to K(u)$ is the extension generated by $\{u\}$.

Example 2 *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.*

Proposition 15 *Let $K \to L$ be a field homomorphism and let X be a subset of L. Then*

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

Proof. (Exercise 24.) ■

Proposition 16 *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 25.) ■

Definition 12 *If Y is a finite set, then $K \to K(Y)$ is said to be* **finitely generated over** *K.*

Proposition 17 *$K \to L$ 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.

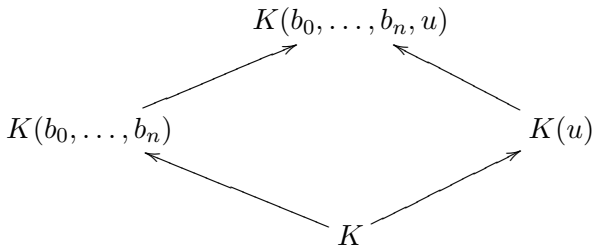
Conversely, suppose $K \to L$ is algebraic and finitely generated. Then $L = K(u_1, u_2, \ldots, u_n)$ where each u_i is algebraic over K. By Lemma **??** we know that $K(u_1, \ldots, u_i) = K(u_1, \ldots, u_{i-1})(u_i)$ for each $1 \leq i \leq n$. Thus, $K \to L$ can be written as a composition of finite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

As an application of these ideas, we are now able to prove the converse of Lemma 5.

Proposition 18 *Suppose $\alpha = \beta \circ \gamma$. Then α is algebraic if and only if β and γ are algebraic.*

Proof. In Lemma 5 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.

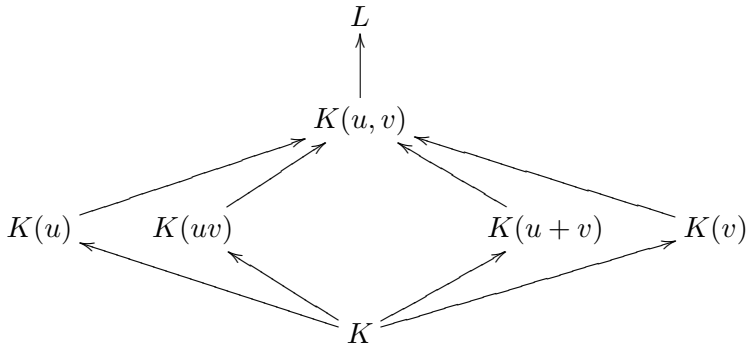


Since $\gamma : K \to M$ is algebraic and $b_i \in M$ for each $1 \leq i \leq n$, it follows from Proposition 16 that $K \to K(b_0, \ldots, b_n)$ is finite. Since u is a root of $\beta_x(m_{u,M}) \in K(b_0, \ldots, b_n)[x]$, it follows that u is algebraic over $K(b_0, \ldots, b_n)$, so $K(b_0, \ldots, b_n) \to b_0, \ldots, b_n, u)$ 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 16). ■

2.5 Relative algebraic closure

Proposition 19 *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 16. 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 12. Thus, the set of elements of L which are algebraic over K is closed under addition. A similar argument shows that this set is 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.

2.6 All finite subgroups are Kaplansky subgroups

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

Proposition 20 *Let L be a field. The functor $\mathrm{Aut}(L/\ )$ takes finite extensions $K \to L$ to finite subgroups of $\mathrm{Aut}(L)$ and the functor $\mathrm{Fix}(\ /L)$ takes finite subgroups of $\mathrm{Aut}(L)$ to finite extensions into L.*

Proof. We begin by showing that if $K \to L$ is finite then $\left|\mathrm{Aut}(L/K)\right|$ is finite. Let $\{u_1, \ldots, u_n\}$ be a basis for L over K. Then $L = K(u_1, \ldots, u_n)$. 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 $m_{u_i,K}(\sigma(u_i)) = \sigma(m_{u_i,K}(u_i)) = \sigma(0) = 0$; thus, $\sigma(u_i)$ is a root of $m_{u_i,K}$. Since there are finitely many roots of $m_{u_i,K}$ for each i, there are only finitely many automorphisms $\sigma \in \mathrm{Aut}(L/K)$.

Let H be a finite subgroup of $\mathrm{Aut}(L)$ and let $K = L^H$. (under construction) ■

Lemma 9 (Dedekind) *Let G be a group and let K be a field. The set $\mathrm{Hom}_{groups}(G, K^\times)$ is linearly independent in the K-vector space of functions $\mathrm{Hom}_{sets}(G, K)$.*

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

$$\sum_{i=1}^{n} a_i \chi_i = 0, \tag{2.1}$$

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. ■

Lemma 10 *If $K \to L$ is a finite extension then $\left|\mathrm{Aut}(L/K)\right| \leq [L : K]$.*

Proof. We have already seen that if $K \to L$ is finite then $\mathrm{Aut}(L/K)$ is finite (see Proposition 20). 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 Dedekind's Lemma. But, from the paragraph above we have $\sum_{i=1}^{m} a_i\sigma_i|_{L^\times} = 0$. This contradiction proves the lemma. ■

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

Proof. Recall that a subgroup H of $\mathrm{Aut}(L)$ is Kaplansky if $H = \mathrm{Aut}(L/K)$ for some Galois subfield $K \to L$.

Let $K = L^H$. Then $K \to L$ is finite and $\mathrm{Aut}(L/K)$ is finite, by Proposition 20. Since $H \subset \mathrm{Aut}(L/K)$, it follows that $\left|\mathrm{Aut}(L/K)\right| \geq \left|H\right|$. Now, $[L:K] \geq \left|\mathrm{Aut}(L/K)\right|$ by Lemma 10, so $[L:K] \geq \left|H\right|$. For a contradiction, suppose $\left|H\right| < [L:K]$. Let $n = \left|H\right|$ and write $H = \{\sigma_1, \ldots, \sigma_n\}$. Since $[L:K] > n$ there exists a set $\{u_1, \ldots u_{n+1}\}$ of elements from L which are linearly independent over K. Consider the matrix

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

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

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

Without loss of generality we may assume $a_1 = 1$. Now, if each coefficient a_i were in K, then we would have $\sigma_j(\sum_{i=1}^k a_i u_i) = 0$, 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 K.

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

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

(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

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

(Here we use the fact that $a_1 = 1$ and $\sigma(1) = 1$.) Minimality of k implies $a_i = \sigma(a_i)$ 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 completes the proof of the proposition. ■

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 20). Since $K = L^{\mathrm{Aut}(L/K)}$, it follows from Theorem 1 that $\big|\mathrm{Aut}(L/K)\big| = [L : K]$.

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. ■

2.7 Chapter 2 exercises

Exercise 22 *Prove Lemma 7.*

Exercise 23 *Prove Lemma 8.*

Exercise 24 *Prove Proposition 15.*

Exercise 25 *Prove Proposition 16. Hint: Suppose $X \subseteq L$ is finite; show that $K \to K(X)$ is profinite.*

Exercise 26 *Consider the extension $\mathbb{Q} \to \mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$. Is this galois? Find the dimension and the Galois group of this extension.*

Exercise 27 *Find the minimal polynomial $m_{u,\mathbb{Q}}$ for $u = e^{2\pi i/7} \in \mathbb{C}$ over $\mathbb{Q}$ and find the splitting field F for this polynomial. Find the group $\mathrm{Aut}(F/\mathbb{Q})$. Find the minimal polynomial for $v = \cos(2\pi/7) \in \mathbb{R}$ over $\mathbb{Q}$ find the splitting field E for this polynomial. Find the group $\mathrm{Aut}(E/\mathbb{Q})$.*

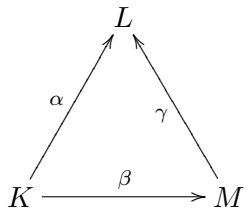
Exercise 28 *Describe the galois group of the splitting field F in $\mathbb{C}$ for $x^n - 1 \in \mathbb{Q}[x]$, where $n \in \mathbb{N}^\times$. Find an integer n so that $\mathbb{Q}(\sqrt{5})$ is a subfield of F. In this case, is $\mathbb{Q}(\sqrt{5}) = F \cap \mathbb{R}$?*

Exercise 29 *Consider the polynomial $f = ax^4 + bx^3 + cx^2 + bx + a \in \mathbb{Q}[x]$. Find a condition on $a, b, c \in \mathbb{Q}$ which ensures that f is irreducible. (This is tricky!) Find a splitting field extension F for $f \in \mathbb{Q}[x]$. Compute $\mathrm{Aut}_{\mathbb{Q}}(F)$ and $\dim_{\mathbb{Q}}(F)$.*

Exercise 30 *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 31 *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.*

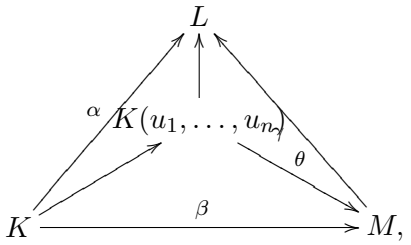
Exercise 32 *Let $\alpha : K \to L$ be a field homomorphism. Fix $\{u_1, \ldots, u_n\} \subset L$. Show that $K \to K(u_1, \ldots, u_n) \to L$ satisfies the following universal property: if the following diagramme commutes,*



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

Exercise 34 *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 35 *Fix $K \to L$. Fix $u, v \in L$. Show that $K(u)(v) = K(v)(u) = K(u, v)$.*

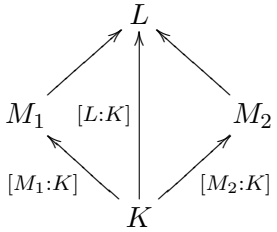
Exercise 36 *Suppose u is algebraic over K, not contained in K, and that v is transcendental over K. Show that $K \to K(u,v)$ is not simple.*

Exercise 37 *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 38 *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 39 *Find the minimal polynomial for $e^{2\pi i/7}$ over $\mathbb{Q}$; find the minimal polynomial for $2\cos(2\pi/7)$ over $\mathbb{Q}$.*

Exercise 40 *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 $[L : K] = [M_1 : K][M_2 : K]$.*



Exercise 41 *Consider the polynomial $f = x^4 - x^3 - 5x^2 - x + 1 \in \mathbb{Q}[x]$. Show that f is irreducible. Find a splitting field extension $E : \mathbb{Q}$ for f. Compute the Galois group G of $E : \mathbb{Q}$. Find all subgroups of G. Find all subfields F of E corresponding to subgroups of G. In each case, compute $\mathrm{Gal}E/F$ and $[E : F]$.*

Exercise 42 *Let K be a field of characterstic p and let F be the 'geometric Frobenius morphism' of $K[x]$ definend by $F(x) = x^p$. Prove: if $f \in K[x]$ is irreducible and $f' = 0$, then $f = g \circ F$ for some $g \in K[x]$.*

Exercise 43 *Let K be a field of characteristic $p \neq 0$ and define $F : K[x] \to K[x]$ by $F(\alpha) = \alpha$ for $\alpha \in K$ and $F(x) = x^p$. Prove: if $f \in K[x]$ is irreducible and $f' = 0$ (where f' denotes the formal derivative of f) then $f = F(g)$ for some $g \in K[x]$.*