The Fellowship of the Group

September 14, 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.

Contents

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.*

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: the four elements in* $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2 + x + 1)$ *are* $0 + (x^2 + x + 1)$, $1 + (x^2 + x = 1)$, $x + (x^2 + x = 1)$ *and* $1 + x + (x^2 + x = 1)$ *and all but the first is a unit. Other examples of fields:* $\mathbb{Q}$, $\mathbb{Z}/(p)$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$.

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.

roposition: maximal ideals

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

proposition: ideals

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. Recall that $\mathrm{Specm}(A) \subseteq \mathrm{Spec}(A)$.

proposition: prime ideals

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

proposition: maximal id

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

proposition: ideals

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. ■

proposition: maximal ideals

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,

[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.

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.

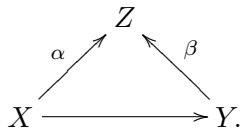
There is something to be gained by not working in the category of fields up to isomorphism; after all, every isomorphism of fields is an identity in the category of fields up to isomorphism, so Galois groups are particularly boring if we pretend all fields homomorphisms are inclusions. On the other hand, 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

Let Z be an object in an arbitrary category. Let $\textsc{sub}(Z)$ denote the category of subobjects of X; thus, an object in $\textsc{sub}(Z)$ is a monic (see Exercise 1.11) with codomain Z (*i.e.,* a monic map $\alpha : X \to Z$ in the ambient category), and a map from $\alpha : X \to Z$ to $\beta : Y \to Z$ in $\textsc{sub}(Z)$ is a commutative triangle

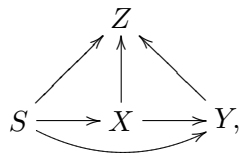
exercise: monic

(1.1) diagramme: map-L



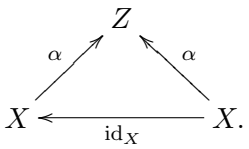
Composition in $\textsc{sub}(Z)$ is indicated by the diagramme,

(1.2) diagramme: compos



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

(1.3)



Notice that there is an obvious forgetful functor from $\textsc{sub}(Z)$ to the ambient category, taking $\alpha : X \to Z$ to X and taking the 'triangle' $X \to Y \to Z$ to $X \to Y$. We will often 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 $\alpha : M \to L$; 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 $\alpha = \beta \circ \gamma$. Proposition 4 shows that every field homomorphism is injective, and in Exercise 1.11 you will show that every injective field homomorphism is monic and every monic field homomorphism is injective. Thus, the category of subfields of L is precisely $\text{SUB}(L)$. The category $\text{SUB}(L)$ will be of primary importance in this course.

We will also make extensive use of the category $\text{SUB}(\text{Aut}(L))$, where L is a field, as above.

1.3 The Galois functors

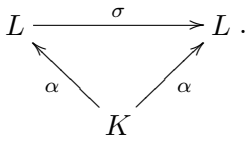
The Galois correspondence is a pair of contravariant functors, one from $\text{SUB}(L)$ to $\text{SUB}(\text{Aut}(L))$, and the other functor in the opposite direction. In this section we define these functors; in the next section we show that they form an adjoint pair of contravariant functors.

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

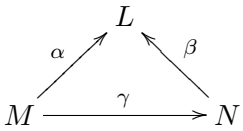
Let $\alpha : K \to L$ be a subfield. The group $\text{Aut}(L/K)$ of **automorphisms of L over K** is defined by

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

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

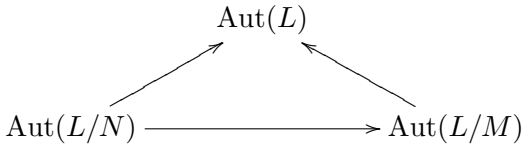


Next, let γ be a map in the category of subfields of L; thus, γ is a commuting triangle



(1.4)

Consider the commuting triangle



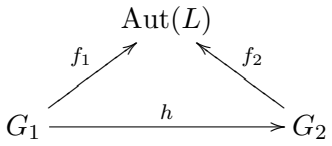
(1.5)

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 $\sigma \in \mathrm{Aut}(L/M)$.

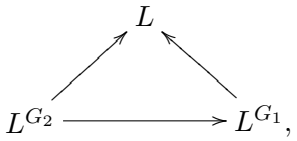
We now define a functor from $\textsc{sub}(\mathrm{Aut}(L))$ to $\textsc{sub}(L)$. Let $f : G \to \mathrm{Aut}(L)$ be an object in the category of subgroups of $\mathrm{Aut}(L)$; thus, $f : G \to \mathrm{Aut}(L)$ is an injective group homomorphism. Let L^G be the field of elements of L fixed by the action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

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

Since L^G is a field, L^G is an object in $\textsc{sub}(L)$. Next, consider the map h in the category of subgroup of $\mathrm{Aut}(L)$ 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.

galois functors

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

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

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

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

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

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

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

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

1.4 The Galois adjunction

ction: 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.

tion: adjunction

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

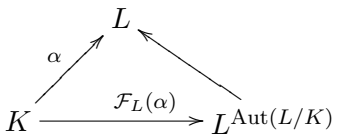
Proof. We begin by defining a natural transformation

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

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

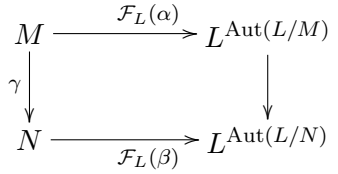
$$\begin{aligned}(\mathrm{Fix}(\ /L) \circ \mathrm{Aut}(L/\ ))(K) &= \mathrm{Fix}(\ /L)(\mathrm{Aut}(L/K)) \\ &= L^{\mathrm{Aut}(L/K)}.\end{aligned}$$

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



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

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 $\alpha = \beta \circ \gamma$.



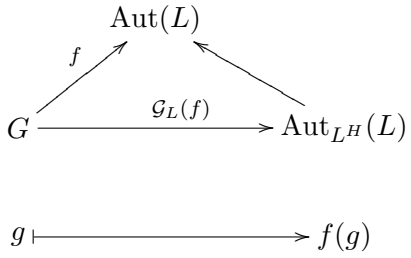
Next, we define a natural transformation

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

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



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

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

Proposition 6

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

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

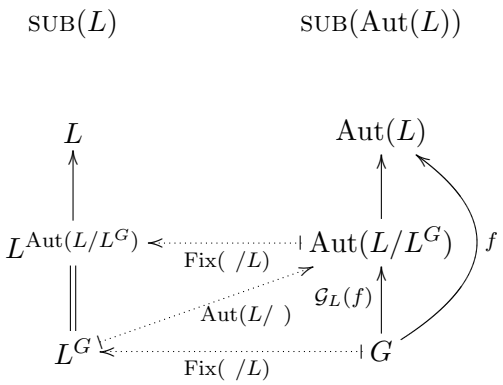
$$\mathrm{Fix}(\ /L) \cong \mathrm{Fix}(\ /L) \circ \mathrm{Aut}(L/\ ) \circ \mathrm{Fix}(\ /L)$$

because

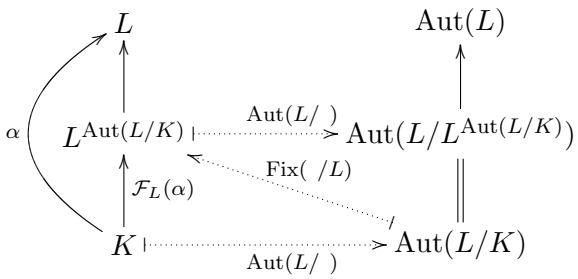
$$L^G = L^{\mathrm{Aut}(L/L^G)}$$

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

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



and



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* $\mathrm{Specm}(A) \subseteq \mathrm{Spec}(A)$. *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: Spec

Exercise 1.4 *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?*

ercise: Spec K[x]

Exercise 1.5 *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 1.6 *Find* the *addition and multiplication table for a field $\mathbb{F}_9$ with nine distinct elements. Find a non-isomorphic cring R with 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: prime

Exercise 1.7 *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* $\mathrm{Spec}(\phi)(\mathfrak{p}) = \phi^{-1}\mathfrak{p}$*. 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 1.8 *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 1.9 *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 1.10 *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 1.11 *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.)

ercise: group monomorphism

Exercise 1.12 *Consider Diagramme 1.1. Show that, since the triangle commutes, it follows that $\gamma : X \to Y$ is monic.*

diagramme: map-L

exercise: PGL(2)

Exercise 1.13 *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 1.14 *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 1.15 *Let A be a cring. Is there some ideal I in A such that A/I is a field?*

exercise: subfields

Exercise 1.16 *Let L be a field. Show that the category of subfields of L contains products, co-products, pull-backs and push-outs. 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 $x = y + 1$).*

Chapter 2

Galois extensions

galois extensions

2.1 Kaplansky subfields

ection: Kaplansky
nition: Kaplansky

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. 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.

sition: Kaplansky

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.*

exercise: Kaplansky

Proof. (Exercise 2.1.) ∎

By definition, Galois subfields of L are Kaplansky subfields $K \to L$ which satisfy one other condition, explained in Section 2.2.

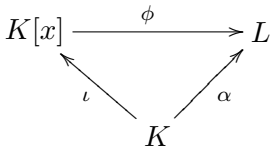
section: algebraic extensions

2.2 Algebraic extensions

tion: 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 proposition: prime ideal
$\phi(p_1) = 0$ 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: algebraic

Definition 4 *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. definition: algebraic
Thus, Definition 4 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

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

■

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

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

exercise: algebraic
Proof. (Exercise 2.3.) ■
proposition: algebraic
Proposition 8 leads to the following definition.

algebraic element **Definition 5** *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.

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

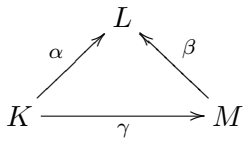
Proof. Suppose $K \to L$ is algebraic and $\sigma \in \mathrm{End}(L/K)$. We must show that σ is surjective. Pick $u \in L$. Let X be the set of roots of $m_{u,K}$ in L.

(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 20).

2.3 Galois extensions

Definition 6 *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 20 now and work backward through the text.)

In Chapter 7 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 6. ■

2.4 Chapter 2 exercises

Exercise 2.1 *Prove Proposition 7.*

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* $\mathrm{Aut}(L)$.

Exercise 2.3 *Prove Proposition 8.*

exercise: composition

Exercise 2.4 *Show that* $\mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2})$ *is not Galois, while the composition* $\mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$ *is Galois. Is* $\mathbb{Q} \to \mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$ *Galois? Also, show that* $\mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt[4]{2})$ *are both Galois, but the composition* $\mathbb{Q} \to \mathbb{Q}(\sqrt[4]{2})$ *is not Galois.*

rcise: basic 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* $\mathbb{Q}$*.*

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

efinition: degree

Definition 7 *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 $K \to M$ 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.*

: finite implies algebraic

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. ■

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 lemmas, each of which is rather delightful in its own right.

roposition: finite functor

Proposition 11 *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 $1 \le i \le n$, 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 7 (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

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

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:

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

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

finite extension

Lemma 8 *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 11). Write $\mathrm{Aut}(L/K) = \{\sigma_1, \ldots, \sigma_m\}$ and consider the matrix

proposition: finite functor

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

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: Dedekind-Artin

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

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 11. Since $H \subset \mathrm{Aut}(L/K)$, it follows that $\big|\mathrm{Aut}(L/K)\big| \geq \big|H\big|$. Now, $[L : K] \geq \big|\mathrm{Aut}(L/K)\big|$ by Lemma 8, so $[L : K] \geq \big|H\big|$. For a contradiction, suppose $\big|H\big| < [L : K]$. Let $n = \big|H\big|$ 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

proposition: finite functor

lemma: finite extension

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

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 $\sigma_j(\sum_{i=1}^k a_iu_i) = 0$, in which case $\sum_{i=1}^k a_iu_i = 0$. 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. ■

em: finite Galois

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

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

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

proposition: finite functor theorem: Dedekind-Artin

Conversely, suppose $K \to L$ is a finite extension and $\left|\mathrm{Aut}(L/K)\right| = [L : K]$. 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 $\left|\mathrm{Aut}(L/K)\right| = \dim_K(L)$ by hypothesis and since $\left|\mathrm{Aut}(L/M)\right| = \dim_M(L)$ 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 algebraic

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