Field Theory

Pete L. Clark

Thanks to Asvin Gothandaraman and David Krumm for pointing out errors in these notes.

Contents

CHAPTER 1

Introduction

1. Provenance

Some portion of the theory of fields is part of the traditional mathematical curriculum at both the undergraduate and graduate levels. Undergraduates who take a year of algebra will probably learn enough about finite degree field extensions to cover the basics of Galois theory (perhaps in characteristic 0, where separability is automatic). In a graduate algebra course there may not be time cover much more field theory than this, but many students of algebra – as well as many other branches of mathematics that draw upon algebra in a crucial way, including but not limited to number theory, algebraic and differential geometry, algebraic topology and some parts of combinatorics – will need to learn (or at least, have access to) a larger body of field theory than is taught in these standard courses, and moreover more advanced courses in field theory are in my experience virtually unheard of.

There are interesting cultural differences across various subdisciplines of mathematics. Compared to most other areas of mathematics, the standard survey texts in algebra are unusually long and unusually sophisticated. The most widely used contemporary texts are probably those by Dummit–Foote [**DF**] and Lang [**La**]. When I took undergraduate "honors algebra" in 1995-1996, we used the first edition of Dummit–Foote, which is 658 pages and was indeed pitched, according to the foreword, at a diverse audience including first and second year undergraduates and also graduate studets. The latest edition [**DF**] is 932 pages, and it is usually used in graduate courses. Perhaps because of this transition through editions, it seems better pitched at actual first year graduate students than most other standard texts. The first edition of Lang's *Algebra* was 508 pages. The latest edition [**La**] is 914 pages. Unlike the text of Dummit–Foote, I didn't acquire a copy of Lang's text until shortly after I got my PhD in an algebraic field. I read it as a young assistant professor....with enormous pleasure. As a reference work for "general algebra" it is *almost* unequalled – at the time of this writing in October 2025 it has 1368 MathSciNet citations – and for a sufficiently mature audience it is simply a lovely work. That it is (or was, within my own memory) used in actual first year algebra courses is bizarre, since much of it seems pitched well beyond all but the most mature and capable early graduate students.

The one treatment that may surpass Lang's is Jacobson's *Basic Algebra*, which comes in two parts [**Ja1**], [**Ja2**], together comprising 1185 pages. These texts provide a view of algebra as seen by one of the leading algebraists of the twentieth century. The second volume touches upon many of the same topics as the first volume, but with an increased sophistication. In particular both volumes treat field theory, the first volume concentrating on finite Galois extensions an the second

treating some much more specialized and advanced topics.

There are some other texts – uniformly of more modest length than the tomes referred to above – that treat exclusively field theory. Among these I want to mention texts by Artin [**Ar**], Karpilovsky [**Kr**], Morandi [**Mo**], Roman [**Rm**], Rotman [**Rt**], Weintraub [**We**], Cox [**Cx**] and Milne [**Mi**]. Artin's text is surely the most influential here: he approached Galois theory via his theorem that for any finite group G acting effectively by automorphisms on a field K with invariant field K^G, then K/K^G is a finite Galois extension with Galois group G. From this result the Galois correspondence can be deduced in a couple of pages. Essentially all subsequent expositions of Galois theory have followed Artin's approach.

I am a mathematican working in number theory and arithmetic geometry, with some side interests in commutative algebra. I've taught graduate courses in these and related areas for about twenty years, and I usually find myself "reminding" students of pieces of field theory that they have not seen before (or have forgotten, or didn't learn in the form I wish to use, or....). Almost all of these reminders can be found in one or more of the aforementioned texts, but I came to find it convenient to have my own notes that I could point to: they are freely accessible online, they contain material that was (at least at some point) that I'd fully digested and understood, and things could be presented in a form that was ready for me to use in my own courses.

These notes were the beginnings of the present text. They've received sporadic development over a period of about 15 years. At this point they mean to be a rather comprehensive text on general field theory, suitable for reading by graduate sudents in mathematics (and everyone else with this level of mathematical background and skill).

2. Features of this Text

One distinctive feature in this text is an interest in cardinalities of infinite sets. I think I acquired this interest by reading several of Kaplansky's texts (including, at a rather young age, his *Set Theory and Metric Spaces*), in which he seemed to delight rather than shy away from cardinality issues. Thus in this text quantities like the dimension of a vector space, the degree of a field extension, the transcendence degree and so forth are *cardinal numbers*. Whereas for a finite degree field extension K/F we have $[K : F] \leq \#\operatorname{Aut}(K/F)$, with equality if and only if K/F is Galois, for an infinite degree algebraic Galois extension K/F, both $[K : F]$ and $\#\operatorname{Aut}(K/F)$ are infinite, an we always have $[K : F] < \#\operatorname{Aut}(K/F)$. We also show that the automorphism group of an algebraically closed field F has cardinality $2^{\#F}$, and if $F/\mathbb{Q}$ is an algebraically closed, transcendendental extension, we show that the number of conjugacy classes of involutions in the group $\operatorname{Aut}(F)$ is $2^{\#F}$.

Field theory is probably the oldest branch of mathematics, and most of the results in this text are between one hundred and two hundred years old. Nevertheless I have searched the literature and tried to include some comparatively recent results,

concentrating on those that are not too specialized. In this text, we cover or discuss work of Aliabadi [**Al18**], Apostol [**Ap70**], van Bommel–Costa–Elkies–Keller–Schiavone–Voight [**vBCEKSV25**], Brown–Craven–Pelling [**BCP86**], Berlekamp [**Be78**], Butler–McKay [**BM83**], Barquero-Sanchez–Calvo-Monge [**BSCM25**], Clark [**Cl12**], Craven–Csordas [**CC77**], Charnow [**Ch70**], Craven [**Cr75**], [**Cr97**], Dieudonné [**Di74**], Faith [**Fa61**], Fine–Gordon–Smith [**FGS71**], Gilmer [**Gi68**], Hou [**Ho20**], Isaacs [**Is80**], [**Is85**], Isaacs–Moulton [**IM98**], Jacobson–Vélez [**JV90**], Jensen–Yui [**JY82**], Kang [**Ka00**], Khare [**Kh09**], Kiehlmann [**Ki13**], Koenigsmann [**Ko05**], Kappe–Warren [**KW89**], Leptin [**Le55**], Lipman [**Li66**], Mann [**Ma64**], Marker–Steinhorn [**MS25**], Nikolov–Segal [**NS07**], Parker [**Pa74**], Pelling [**Pe81**], Poizat [**Po74**], Schnor [**Sc92**], Soicher–McKay [**SM85**], Springer [**Sp52**], Sury [**Su99**], Sutherland [**Su15**], Swan [**Sw62**], Sweedler [**Sw68**], Sonn–Zassenhaus [**SZ67**], Waterhouse [**Wa74**], Weintraub [**We21**], Yale [**Ya66**] and Zywina [**Zy15**].

This text contains nearly 400 exercises, only a small minority of which ask for proofs of stated results (and these are meant to be straightforward). As the years have passed, I have felt increasingly that it is the task of the author/instructor to prove the results of the text/course and that exercises should explore further examples and computations, show the necessity of hypotheses in results, and pursue further applications of the results presented. For instance, Elkies's use of Hilbert 90 to parametrize Pythagorean Triples and Swan's proof of Quadratic Reciprocity both occur in exercises. Occasionally exercises are asked to raise important issues, the natural resolution of which will occur later in the text.

3. Contents

Field theory is largely the theory of field *extensions* K/F and their automorphism groups $\mathrm{Aut}(K/F)$. For a field extension K/F, an element $\alpha \in K$ if **algebraic over F** if there is a nonzero univariate polynomial f with coefficients in F such that $f(\alpha) = 0$; otherwise we say that α is **transcendental** over F. For instance, looking at the extension $\mathbb{C}/\mathbb{Q}$, the numbers $\sqrt{n}$ and $\cos(\frac{2\pi}{n})$ are algebraic over $\mathbb{Q}$, while the numbers e and π are transcendental over $\mathbb{Q}$ (but we do not prove this in this text). A field extension K/F is **algebraic** if every element of K is algebraic over F; otherwise K/F is **transcendental**.

3.1. Overview of Topics Covered. In Part I we present the basic theory of algebraic field extensions. In Chapter 2, we give some attention (as is traditional) to the algebraic properties of the sets of real and complex numbers that can be constructed with a straightedge and compass. In Chapter 3 we prove the existence and uniqueness-up-to-F-algebra isomorphism of algebraically closed fields and then introduce the class of normal algebraic extensions, which get characterized in several ways: as splitting fields, in terms of containing all conjugates of any given element, and in terms of stability under embeddings into algebraically closed fields. In Chapter 4 we introduce the classes of separable and purely inseparable algebraic extensions. We give the basic structural result that an algebraic extension decomposes into a separable extension followed by a purely inseparable field extension, and we discuss how this decomposition interacts with normality. We end the chapter by determining all finite degree extensions of a finite field. Chapter 5 concerns the Primitive Element Theorem, which we construe as two different results, each

having the familiar consequence that a finite degree separable extension is monogenic. In Chapter 6, to a finite degree field extension K/F we associate the norm and trace maps, the trace (bilinear) form and the discriminant and then discuss discriminants and resultants of univariate polynomials, first with coefficients in a field and then with coefficients in any commutative ring.

Part II is devoted to Galois theory. An algebraic field extension K/F is Galois if (among other characterizations) it is both normal and separable, so Galois theory springs naturally out of the considerations of Part I. Galois theory is viewed by many as being the jewel in field theory's crown, and although I did not proceed from this as an article of faith – indeed, when I began this project I was most interested in acquiring a reference for transcendental field extensions – the final product undeniably lends support to this view. In Chapter 7, after an initial (and inessential) discussion of the Galois connection attached to any field extension, we study finite Galois extensions and give the Galois correspondence, following Artin. We then discuss various applications of finite Galois theory: the Fundamental Theorem of Algebra, the Normal Basis Theorem, and Hilbert's Theorem 90. We then turn to the theory of algebraic Galois extensions, in which following Krull, we recover a bijective correspondence by topologizing the Galois group and restricting to closed subgroups. The Krull topology endows the automorphism group $\mathrm{Aut}(K/F)$ of an algebraic Galois extension with the structure of a profinite topological group, and we digress to study some basic properties of profinite groups in their own right. We then give the algebraic Galois correspondence.

In Chapter 8 we discuss solvable extensions, the application of Galois theory that motivated Galois to invent it. This is a very classical topic, but also an extremely rich one with importance in modern algebra and number theory. One may say that this is the point in the text in which we become very interested in *specific* field extensions rather than classes or properties of field extensions. We study cyclotomic polynomials and cyclotomic extensions, Kummer theory – the study of abelian extensions under the presence of sufficiently many roots of unity – then nonabelian Kummer theory (i.e., splitting fields of polynomials $t^n - a$), then Artin–Schreier theory – the analogue of Kummer theory for abelian p-extensions in characteristic p. We end the chapter with a discusion of the results of Abel–Ruffini and Galois on solvability by radicals, first in characteristic 0 and then in characteristic $p > 0$.

In Chapter 9 we discuss a classical – but still important – perspective on finite Galois theory, that the automorphism group of a finite Galois extension L/F acts faithfully on the roots of a polynomial $f \in F[t]$ whose splitting field is L. This reveals much deeper connections with group theory than the abstract form of the Galois correspondence: we are led to study various aspects of permutation groups.

Part III is devoted to the study of transcendental field extnsions. In Chapter 10 we prove the basic structure theorem that any field extension K/F decomposes into a purely transcendental extension followed by an algebraic extension, and this leads to a discussion of transcendence bases. We prove that in a tower $F \subseteq K \subseteq L$ of field extensions, L/F is finitely generated if and only if both K/F and L/K are finitely generated. The theory of finitely generated field extensions of transcendence degree

d is really the theory of algebraic curves (when $d = 1$) and the birational geometry of d-dimensional algebraic varieties (when $d \geq 2$), which limits what can be done by purely field theoretic methods, but we prove Lüroth's Theorem, which is equivalent to the fact that if $f : \mathbb{P}^1 \to C$ is a finite morphism of nice curves defined over a field k, then $C \cong \mathbb{P}^1$. In Chapter 11 we discuss linear disjointness of field extensions, a key concept for both transcendental and algebraic field extensions, and we extend the definition of separability to transcendental field extensions and discuss separating transcendence bases. We define regular field extensions, a key concept in arithmetic geometry. In Chapter 12 we discuss derivations and differentials, with applications to one variable function fields and p-bases.

Part IV is devoted to the theory of formally real fields and ordered fields. This topic is included in the texts of van der Waerden [**vdW**], Lang[1] [**La**] and Jacobson [**Ja1**], [**Ja2**] although so as far I know it is rarely covered in basic graduate courses on the subject. Although it initially seems more specialized, this material is of interest to a general field-theoretic audience, in particular through the spectacular result of Artin–Schreier that if F is a field that is not algebraically closed but whose algebraic closure has finite degree over F, then F admits a unique ordering and $F(\sqrt{-1})$ is algebraically closed. There are also important connections with the algebraic theory of quadratic forms.

In Chapter 14 we discuss rudiments of the theory of commutative groups. In Chapter 14 we present Artin–Schreier's theory of formally real fields, including the basic result that a field can be ordered if and only if it is formally real. For an ordering P on a field K and a field extension L/K, we study when L is formally real and when the ordering P extends to L. The analogue of an algebraically closed field in the class of formally real fields is a real-closed field, but the notion of real-closed field is richer: whereas any two algebraic closures of a field F are isomorphic over F, a formally real field may admit many non-F-isomorphic (and even non isomorphisc) real-closures. Rather it is the real-closure of an *ordered* field (F, P) that is unique up to (F, P)-isomorphism, and we discuss real-closures of ordered fields in Chapter 15. This material has some teeth: using it, we give Artin's solution of Hilbert's 17th Problem: a positive semidefinite polynomial $f \in \mathbb{R}[t_1, \ldots, t_n]$ is a sum of squares in $\mathbb{R}(t_1, \ldots, t_n)$. We discuss the dichotomy of Archimedean versus non-Archimedean ordered fields. In Chapter 16 we discuss connections between ordered fields and valuation theory, which occur because a non-Archimedean ordered field carries a canonical nontrivial valuation with Archimedean ordered residue field. In particular, whether a non-Archimedean ordered field is real-closed has a nice characterization in terms of this canonical valuation. This last chapter is less self-contained: it is really for an audience who has seen at least rank 1 valuations before, and some basic results in valuation theory are stated without proof.

3.2. Less Standard Topics.

Although this text began its life as a reference for field-theoretic facts used in other graduate level courses, since then we put in a lot more to try to expose the intrinsic beauty of the subject. In each chapter after the first we have included at

[1]Much of this material is due to Artin–Schreier, and E. Artin was Lang's thesis advisor. Lang's fourth published paper [**La53**] is in this area.

least one "payoff" application of the material developed there, and some of these payoffs are not the standard ones found in other texts:

• Chapter 2 (**Field Extensions**): Our discussion of constructibility includes a statement of the Gauss–Wantzel Theorem charaterizing the integers $n \in \mathbb{Z}^{\geq 3}$ such thtat the regular n-gon is constructible. We prove half of the theorem here and return to prove the other half in Chapter 9.

• Chapter 3 (**Normal Extensions**): After giving a standard proof (due to Artin) of the existence of an algebraic closure of any field, we discuss some issues that it brings up, both set-theoretic and field-theoretic. In particular we state a theorem of Gilmer asserting that a certain process that Artin's proof performs infinitely many times actually only needs to be done once in order to attain an algebraic closure.

• Chapter 4 (**Separable Algebraic Extensions**): For every prime p, we exhibit a degree p^2 field extension in characteristic p that is inseparable but has no nontrivial purely inseparable subextension (Example 4.28). We also explore the question of when every generator of an extension $\mathbb{F}_{q^f}/\mathbb{F}_q$ of finite fields is a generator of the multiplicative group $\mathbb{F}_{q^f}^\times$.

• Chapter 5 (**The Primitive Element Theorems**): We give two versions of the Primitive Element Theorem. Primitive Element I, due to Steinitz, says that a finite degree field extension is monogenic if and only if its lattice of subextensions is finite. Primitive Element II asserts that a finite degree field extension generated by finitely many elements, all but one of which is separable, is monogenic. Both of these results imply the Primitive Element Corollary: a finite degree separable field extension is monogenic. We apply these results to study the number of subextensions of a finite degree field extension. Then we apply the Primitive Element Corollary to prove Gilmer's Theorem as stated in Chapter 4. We also state and prove a generalization due to M. Isaacs, which implies that an algebraic field extension K/F is characterized up to F-algebra isomorphism by the set of polynomials $f \in F[t]$ that have a root in K. Isaacs's Theorem deserves to be better known; at present his paper [**Is80**] has no MathSciNet citations.[2]

• Chapter 6 (**Norms, Traces, Discriminants and Resultants**): We discuss discriminants of polynomials and finite degree field extensions and their relationship. Following Kang, we characterize pure cubic extensions, including in characteristic 2. Following Swan, we present an approach to computing discriminants of polynomials using resultants and the Euclidean algorithm. As applications, we compute the discriminant of the pth cyclotomic polynomial, of the trace form of a p-power cyclotomic field, and of a general monic trinomial $t^n + at^k + b$.

• Chapter 7 (**Galois Extensions**): We discuss the Galois connection induced by an arbitrary field extension, and we explain why the Galois connection attached to a Galois extension of infinite degree is *not* perfect until we introduce the Krull

[2]Isaacs's proof includes a Zorn's Lemma argument. Many Zorn's Lemma arguments in algebra are very similar to each other, making them routine once one has mastered the template. This Zorn's Lemma argument is less routine; I would not want to present it in a classroom setting.

topology and use only closed subgroups. We discuss the Inverse Galois Problem, the Regular Inverse Galois Problem, and Noether's approach to the latter. We give Shipman's variant of Artin's Galois-theoretic proof of the Fundamental Theorem of Algebra. We give Elkies's application of Hilbert's Satz 90 to Pythagorean Triples. We give a generalization of Artin's result that K/K^G is a finite Galois extension to a compact topological group acting effectively and continuously on a field K. Using this, we deduce the Leptin–Waterhouse Theorem: every profinite group is the Galois group of some algebraic Galois extension. We classify profinite groups up to homeomorphism. We prove profinite generalizations of Lagrange's Theorem and the Sylow Theorems (except the part concerning the number of Sylow p-subgroups.) We show that for any algebraic Galois extension of infinite degree, we have an inequality (of infinite cardinals) $[K : F] < \#\operatorname{Aut}(K/F)$. Finally, we discuss strong completeness of profinite groups and show that the absolute Galois group of a global field contains finite index subgroups that are not open.

• Chapter 8 (**Solvable Extensions**): We give a substantial discussion of cyclotomic numbers, showing their irreducibility over $\mathbb{Q}$, with applications to the infinitude of primes $p \equiv 1 \pmod N$ and that every finite commutative group occurs as a Galois group over every number field. We determine the quadratic subfield of $\mathbb{Q}(\zeta_p)$, following Weintraub. We prove the fundamental Theorem on symmetric functions with coefficients in a commutative ring. We complete the proof of the Gauss–Wantzel Theorem on the constructibility of the regular n-gon. We give some criteria for when a finite degreee solvable extension is a simple radical extension, a topic that is more subtle than it first appears and is not always treated accurately: for instance we show that a simple radical cubic extension of $\mathbb{Q}$ is obtained by adjoining a cube root but that this need not be the case when $\mathbb{Q}$ is replaced by $\mathbb{Q}(\sqrt{-3})$. We then discuss solvability by radicals in positive characteristic, in which we treat both separable extensions and arbitrary extensions.

• Chapter 9 (**Classical Galois Theory**): We explain how the Inverse Galois Problem implies an a *a priori* stronger version for transitive permutation groups. The standard relationship between the discriminant of a separable polynomial and its Galois group does not apply in characteristic 2. So we introduce the Berlekamp discriminant in characteristic 2 and use it to repair this relationship. We give a result of Stickelberger relating discriminants, degrees and Möbius functions in $\mathbb{F}_q[t]$ for odd q, and using this result we give Swan's proof of the Quadratic Reciprocity Law. We use the Berlekamp discriminant to extend the Kappe–Warren classification of Galois groups of irreducible quartics into characteristic 2. We give a discussion of Galois groups of irreducible quintics. This discussion is incomplete in that we do not give a general criterion for distinguishing the Galois groups C_5 and D_5, but our discussion applies for quintics with coefficients in (some) fields other than $\mathbb{Q}$. Following Dedekind, we show that for all $n \in \mathbb{Z}^+$, the symmetric group S_n is a Galois group over $\mathbb{Q}$. We also show that each of the groups D_4, D_5, A_4, A_5, A_6, A_7 occurs as a Galois group over $\mathbb{Q}$. We give a substantial discussion of several aspects of the theory of perrmutation groups that are relevant to Galois theory, including: multiply transitive permutation groups, primitive and imprimitive permutation groups, wreath products, the classification of solvable subgroups of S_p for p a prime, and Galois's theorem on solvable permutation groups.

• Chapter 10 (**Structure of Transcendental Extensions**): We show that for a field extension K/F, the subfield lattice $\mathcal{L}(K/F)$ is Noetherian if and only if K/F is finitely generated. We show that there is a Galois correspondence between subextensions of a field extension K/F and closed (with respect to the Galois connection) subgroups of $\mathrm{Aut}(K/F)$ when K is algebraically closed of characteristic 0. We prove a theorem of Charnow: the automorphism group of an algebraically closed field F has cardinality $2^{\#F}$.

• Chapter 11 (**Linear Disjointness and Separability**): Our discussion of linear disjointness makes a distinction between "somewhere linearly disjoint" and "everywhere linearly disjoint," which is a novel feature that emerged from a MathOverflow discussion. Our discussion on when nonintersecting field extensions are linearly disjoint shows that it is sufficient for at least one of the extensions to be normal and at least one of the extensions to be separable and also that it is not sufficient for one or even both extensions to be normal. We show that a field extension K/F is regular if and only if it is separable and F is algebraically closed in K.

• Chapter 12 (**Derivations and Differentials**): We apply the results to one variable function fields, in particular showing that for a one variable function field K over a perfect ground field, any inseparable algebraic extension factors through the Frobenius map, a basic result in the algebraic geometry of curves in positive characteristic. We discuss two monotonicity theorems of C. Faith, one of which includes as a special case that if K is a subextension of a finite degree field extension L/F, then K/F needs no more generators than L/F.

• Chapter 13 (**Basics on Ordered Algebraic Structures**) We prove Levi's Theorem, characterizing ordered commutative groups among all commutative groups, and a theorem of Hölder that every Archimedean ordered commutative group can be embedded in $\mathbb{R}$. We state (but do not prove) the Hahn Embedding Theorem.

• Chapter 14 (**Formally Real Fields**) We relate Hasse–Minkowski Theorem on quadratic forms to orderings on number fields. We characterize the number fields for which -1 is a sum of two squares, a result originally due to Fein–Gordon–Smith. We give Springer's Theorem that anisotropic quadratic forms remain anisotropic after a field extension of odd finite degree. We state and prove the Grand Artin–Schreier Theorem, characterizing fields with finite absolute Galois group, from which we deduce the possible profinite orders $|\mathfrak{g}_F|$ of the absolute Galois group of a field.

• Chapter 15 (**Ordered Fields**) We prove that the Mean Value Theorem holds for polynomials over a real-closed field, and we give Sylvester's Theorem on the trace form of an étale algebra over a real-closed field. We show that the set of isomorphism classes of real-closed fields with algebraic closure isomorphic to a given algebraically closed field F of characteristic 0 are in bijection with conjugacy classes of order 2 elements in $\mathrm{Aut}(F)$. We use this to show that if F is an algebraically closed field of characteristic 0 that is transcendental over $\mathbb{Q}$, then $\mathrm{Aut}(K/F)$ has $2^{\#F}$ conjugacy classes of involutions. We discuss Archimedean ordered fields thoroughly, including completeness and rigidity properties. We define the real spectrum

of an ordered field F – the set of all orderings on F, equipped with a natural topology that makes it a Boolean space – and we state Craven's Theorem that every Boolean space is homeomorphic to the real spectrum of some field.

• Chapter 16 (**Orderings and Valuations**) None of this material is standard in general field theory texts, but most of it appears in texts on valuation theory; especially, we use the text of Engler–Prestel [**EP**] as a reference. We discuss compatibility between orderings and valuations, prove a topological form of the Baer–Krull Theorem on the space of orderings of a field compatible with a given valuation, discuss Henselian valued fields and Henseliations, and characterize real-closed fields as ordered fields whose canonical valuation is Henselian, has divisible value group and real-closed residue field. We apply these results to construct, for any infinite cadinal κ, 2^κ non-isomorphic non-Archimedean real-closed fields of cardinality κ, which completes the proof of the result mentioned above that an algebraically closed field F of characteristic 0 that is transcendental over $\mathbb{Q}$ has $2^{\#F}$ conjugacy classes of involutions: in the previous chapter we used Archimedean ordered fields to prove this result when $\#F \leq 2^{\aleph_0}$.

3.3. Omitted Topics.

• Although we give a comprehensive treatment of Galois groups of cubic and quartic polynomials, we do not discuss the explicit formulas for the roots of a cubic or quartic polynomial in terms of the coefficients. This is because (i) this is a standard topic in many other texts, including at the undergraduate level, and (ii) I have never found such formulas to be useful.

• Although we give the Artin–Schreier theory of abelian p-extensions in characteristic $p > 0$, we do not give Witt's theory of cyclic p^a-extensions in characteristic $p > 0$. This theory requires a preliminary discussion of Witt vectors. A very nice treatment is given in [**Ja2**, §8.10-8.11].

• Jacobson gave a Galois correspondence for purely inseparable algebraic extensions of exponent 1 using derivations. While this has inspired a lot of subsequent work, I decided it was too specialized to include here. It is treated in [**Ja2**, §8.17], using the Jacobson–Bourbaki correspondence [**Ja2**, §8.2].

• Tensor products of fields appear in the definition of linear disjointness, in Chapter 11 and are used to study linear disjointess throughout that chapter. They could be studied more systematically for their own benefit: e.g. a degree n field extension K/F is Galois if and only if $K \otimes_F K \cong_F F^n$.

• Related to the above: it would be natural to study étale algebras over a field F: these are finite-dimensional commutative F-algebras that are isomorphic to a finite product of finite degree separable field extensions of F. It is natural to define norms, traces and discriminants of étale F-algebras rather than just finite degree field extensions. Most of the basic theory of étale algebras already appears in my Number Theory I notes [**CL-NTI**], and arguably it is more thematic to include it there. If K/F is a field extension and A/F is an étale F-algebra, then K/F **splits A** if $A \otimes_F K \cong K^{\dim_F A}$. If F^{sep}/F is a separable algebraic closure, then

F^{sep}/F splits every étale F-algebra (indeed this follows from the fact mentioned in the previous bullet point). Then Grothendieck generalized the Galois correspondence as follows: if K/F is an algebraic Galois extension with $G := \mathrm{Aut}(K/F)$, there is a categorical anti-equivalence from the category of étale F-algebras split by K to the category of finite G-sets X in which the action $G \times X \to X$ is continuous when X is given the discrete topology. This is explained nicely in [**Mi**, Ch. 8].

• Hilbert's Irreducibility Theorem and Hilbertian fields would be a lovely continuation of the Galois theory discussed here, showing for instance that the Regular Inverse Galois Problem over $\mathbb{Q}$ implies the Inverse Galois Problem over $\mathbb{Q}$. Two good sources for this material are the texts of Fried–Jarden [**FJ**] and Serre [**Se**], but there still seems to be room for a presentation that is shorter and more concentrated than that of [**FJ**] and less geometrically sophisticated than that of [**Se**].

4. Some Conventions

For an integer N, we denote by $\mathbb{Z}^{\geq N}$ the set of integers greater than or equal to N. We also make a distinction between the **natural numbers**

$$N := \mathbb{Z}^{\geq 0}$$

and the **positive integers**

$$\mathbb{Z}^+ := \mathbb{Z}^{\geq 1}.$$

By convention, all of our rings are associative and have a multiplicative unity, called 1. Again by convention, a homomorphism of rings necessarily carries 1 to 1.

As is quite standard in modern algebra, we are assuming the Axiom of Choice. (Without it, a field need not have an algebraic closure!) We do *not* assume the Continuum Hypothesis, so there may or may not be cardinals κ with $\aleph_0 < \kappa < 2^{\aleph_0}$. Whether the Continuum Hypothesis holds turns out to matter exactly once in the text, in §7.11 (in what is certainly not a key point).

Part I

Algebraic Extensions I: Basics

CHAPTER 2

Field Extensions

1. Domains and Fraction Fields

A **domain** is a nonzero commutative ring in which there are no nonzero zero-divisors: if $xy = 0$, then at least one of x and y is 0. A **field** is a commutative ring in which each nonzero element has a multiplicative inverse. Equivalently, a field is a commutative ring R in which the only ideals are (0) and R itself.

Variations on the definition: In older terminology, a field could be non-commutative, i.e., any ring in which each nonzero element has a two-sided multiplicative inverse. We now call such things "division rings" or "division algebras." One also sometimes encounters non-associative division algebras, e.g. Cayley's octonions.

In a field F, if $xy \neq 0$ and $x \neq 0$, then x has an inverse, so

$$y = x^{-1}xy = x^{-1}0 = 0.$$

Thus every field is a domain. Every subring of a domain is also a domain, so in particular every subring of a field is a domain. Conversely, every domain is a subring of some field, as follows from the existence of the **fraction field** F of a domain R: the elements of F are equivalence classes of ordered pairs (x, y) with $x \in R$ and $y \in R \setminus \{0\}$ under the equivalence relation

$$(x_1, y_1) \sim (x_2, y_2) \iff x_1y_2 = x_2y_1.$$

(We regard the ordered pair (x, y) as corresponding to the fraction $\frac{x}{y}$.) One then checks that the operations

$$[(x_1, y_1) + [(x_2, y_2)] \coloneqq \left[\frac{x_1y_2 + x_2y_1}{y_1y_2}\right]$$

and

$$[(x_1, y_1)] \cdot [(x_2, y_2)] \coloneqq \left[\frac{x_1x_2}{y_1y_2}\right]$$

are well-defined on equivalence classes and make F into a field, in which the map

$$\iota : R \hookrightarrow F,\ x \in R \mapsto [(x, 1)]$$

is a ring embedding, which we use to view R as a subring of F. This is a special case of the localization construction in commutative algebra [**Cl-CA**, Ch. 7].

Exercise 2.1. *Let R be a domain, with fraction field F.*

a) *Show: if R is finite, then $R = F$.*
b) *Show: $\#R = \#F$.*

Many important examples of fields arise as fraction fields of domains, starting with the fact that $\mathbb{Q}$ is the fraction field of $\mathbb{Z}$.

EXAMPLE 2.1. *Let R be a commutative ring, and let $\mathbf{T}$ be a nonempty set. The* ***polynomial ring*** *$R[\mathbf{T}]$ is a commutative ring having an R-module basis the set $\prod_{t \in T} t^{a_t}$ with $a_t \in \mathbb{N}$ for all $t \in \mathbf{T}$ and $a_t = 0$ for all but finitely many $t \in T$. The multiplication operation is*

$$\left(\sum a_I t_{i_1}^{a_1} \cdots t_{i_n}^{a_n}\right)\left(\sum b_I t_{i_1}^{b_1} \cdots t_{i_n}^{b_n}\right) := \sum a_I b_I t_{i_1}^{a_1+b_1} \cdots t_{i_n}^{a_n+b_n}.$$

The unit element is $1 = \prod_{t \in T} t^0$. When $\mathbf{T} = \{t\}$, we write $R[t]$ for $R[\mathbf{T}]$, and when $\mathbf{T} = \{t_1, \ldots, t_n\}$ is finite of size n we write $R[t_1, \ldots, t_n]$ for $R[\mathbf{T}]$.

The polynomial ring $R[\mathbf{T}]$ is a domain if and only if R is a domain. Half of this is clear: since R is a subring of $R[\mathbf{T}]$, then a nonzero zero-divisor in R is a nonzero zero-divisor in $R[\mathbf{T}]$. Conversely, suppose that R is a domain. We show that $R[\mathbf{T}]$ is a domain by an inductive argument on the number of indeterminates: Step 1: The nonzero elements of $R[t]$ are of the form $f = a_n t^n + \ldots + a_1 t + a_0$ with $a_0, \ldots, a_n \in R$ and $a_n \neq 0$. In this case, we say that f has ***degree*** *n. For nonzero $f, g \in R[t]$, we have $\deg(fg) = \deg(f) + \deg(g)$... which implies that fg is not zero! Step 2: If $\mathbf{T} = \{t_1, \ldots, t_n, t_{n+1}\}$ with $n \in \mathbb{Z}^+$, then $R[\mathbf{T}] = R[t_1, \ldots, t_n][t_{n+1}]$, so it is a domain by Step 1 and induction.*
Step 3: Suppose $\mathbf{T}$ is infinite, and let $f, g \in R[\mathbf{T}]$ be nonzero elements. Each of f and g involve only finitely many elements of $\mathbf{T}$, so there is a finite subset $\mathbf{S}$ of $\mathbf{T}$ such that f and g lie in $[\mathbf{S}]$. By Step 2, $R[\mathbf{S}]$ is a domain, so $fg \neq 0$.

We recall for future use that if R is a UFD, so is $R[\mathbf{T}]$ [**Cl-CA**, Thm. 15.28c)].

Let R be a domain with fraction field F. The fraction field of $R[\mathbf{T}]$ contains F and is denoted by $F(\mathbf{T})$: its elements are formal quotients of polynomials with coefficients in F. We call $F(\mathbf{T})$ the ***rational function field over*** *F* ***in the indeterminates*** *$\mathbf{T}$. Rational function fields play a prominent role in Part III.*

EXERCISE 2.2. *Let R be a commutative ring, and let $\mathbf{T}$ be a nonempty set. Show: $\#R[\mathbf{T}] = \max(\aleph_0, \#R, \#\mathbf{T})$.*

EXERCISE 2.3. *(Universal property of polynomial rings): Let $\iota : R \to S$ be a homomorphism of commutative rings, and let $\alpha_1, \ldots, \alpha_n$ be elements of S. There is a unique R-algebra homomorphism $\Phi : R[t_1, \ldots, t_n] \to S$ which takes $t_i \mapsto \alpha_i$.*

EXERCISE 2.4. *Let R be a commutative ring, and let $(M, +)$ be a commutative monoid. The* ***monoid ring*** *$R[M]$ has an an R-module basis the set $\{t_m \mid m \in M\}$, and the multiplication operation is defined as*

$$\left(\sum_{m \in M} a_m t_m\right)\left(\sum_{m \in M} b_m t_m\right) := \sum_{(m_1, m_2) \in M^2} a_{m_1} b_{m_2} t_{m_1 + m_2}.$$

a) *Show: by taking M to be the free commutative monoid $\bigoplus_{t \in \mathbf{T}} \mathbb{N}$ on a set $\mathbf{T}$, we get the polynomial ring $R[\mathbf{T}]$.*
b) *Show: $R[M]$ is a domain if and only if all of the following hold:*
   (i) *R is a domain.*
   (ii) *M is cancellative: for all $x, y, z \in M$, $x + z = y + z$ implies $x = y$.*
   (iii) *M is torsionfree: for all $n \in \mathbb{Z}^+$ and $x, y \in M$, $nx = ny \implies x = y$.*

Exercise 2.4 thus gives us a generalization of rational function fields, namely the fraction field $F(M)$ of the monoid ring $F[M]$ of a commutative, cancellative torsion-free monoid M with coefficients in a field F. We will make use of this construction if it's the last thing we do...which it will be.

2. Generating Sets and Degrees

If F is a field, S is a ring, and $\varphi : F \to S$ is a homomorphism of rings, then since the kernel of φ is an ideal of F, φ is either injective (if its kernel is 0) or identically the zero map (if its kernel is F). Moreover, the latter case implies that $1_S = \varphi(1_F) = 0$, which happens if and only if S is the zero ring. So any homomorphism from a field into a nonzero ring – in particular into any field or domain – is injective. Thus if $\varphi : F \to K$ is a homomorphism between fields, we may equally well speak of the **field embedding** φ.

Let K be a field. If $\iota : K \to L$ is a homomorphism of fields, one says that L is an **extension field** of K. As a matter of psychology, it often seems more convenient to think of L as "lying above K" rather than K as embedding into L. We often write L/K instead of $\iota : K \to L$, notwithstanding the fact that the latter notation hides important information, namely the map ι.[1]

Let L/F be a field extension. A **subextension** of L/F is a field K such that $F \subseteq K \subseteq L$.

Exercise 2.5. *Let R be a domain with fraction field F. Show: map $\iota : R \hookrightarrow F$ is universal for ring embeddings of R into a field: that is, if K is a field and $\varphi : R \hookrightarrow K$ is an injective ring homomorphism, then there is a unique field embedding $\Phi : F \hookrightarrow K$ such that $\Phi \circ \iota = \varphi$.*

Much of field theory is devoted to an understanding of the various extension fields of a given field K. Since any field K has extensions of all sufficiently large cardinalities – $K(\mathbf{T})$ for any large enough set $\mathbf{T}$ – one obviously cannot literally hope to understand all field extensions of K. However there are two important classes of field extensions that one can at least hope to understand: the first is the class of all finitely generated field extensions of K, and the second is the class of all algebraic field extensions of K.

Let L be a field, and let $\{K_i\}_{i \in I}$ be a nonempty family of subfields of L. It is immediate that the intersection $\bigcap_{i \in I} K_i$ is also a subfield of L. Moreover if L/F is a field extension and $\{K_i\}_{i \in I}$ is a family of subextensions of L/F, then also $\bigcap_{i \in I} K_i$ is a subextension of L/F. This has the following consequence: if L/F is a field extension and S is a subset of L, then the set of subextensions of L/F containing S has a unique minimal element, namely the intersection of all subextensions K with $S \subseteq K$. We denote this subextension by $F(S)$ and call it the subextension of L/F **generated by S**. Similarly, if K is a subextension of L/F, then a **set of generators of K** is a subset S of K such that $K = F(S)$. Since $K = F(K)$, such a set of generators always exists. The following exercise gives a "bottom-up" description of $F(S)$ that is useful but can be improved upon in many special cases.

Exercise 2.6. *Let L/F be a field extension, and let S be a nonempty subset of L. Let $\mathbf{T} = \{t_s \mid s \in S\}$ be a set of indeterminates indexed by the elements of S. For $f \in F[\mathbf{T}]$, let $f_S \in F$ be obtained by evaluating $t_s \mapsto s$. Show: $F(S)$ is the set of rational expressions $\frac{f_S}{g_S}$ with $f, g \in F[\mathbf{T}]$ such that $g_S \neq 0$.*

[1]Beware: the notation L/K has nothing to do with cosets or quotients!

If L/K is a field extension, then L is a K-algebra and in particular a vector space over K. Therefore it has a well-determined (but possibly infinite) dimension, denoted by $[L : K]$. One says that the extension L/K has **finite degree**[2]if $[L : K] < \aleph_0$, i.e., if L is a finite-dmensional K-vector space. For instance, one has $[\mathbb{C} : \mathbb{R}] = 2$, so $\mathbb{C}/\mathbb{R}$ is a finite degree field extension.

THEOREM 2.2. *(Degree Multiplicativity in Towers) Let $F \subseteq K \subseteq M$ be field extensions. Then we have*

$$[M : F] = [M : K][K : F].$$

PROOF. Let $\{b_i\}_{i\in I}$ be an F-basis for K and $\{a_j\}_{j\in J}$ be a K-basis for M. We claim that $\{a_ib_j\}_{(i,j)\in I\times J}$ is an F-basis for M. This suffices, since then $[K : F] = \#I$, $[M : K] = \#J$, $[M : F] = \#(I \times J) = \#I \times \#J$.

Let $c \in M$. Then there exist $\alpha_j \in K$, all but finitely many of which are zero, such that $c = \sum_{j\in J} \alpha_j a_j$. Similarly, for each $j \in J$, there exist $\beta_{ij} \in F$, all but finitely many of which are zero, such that $\alpha_j = \sum_{i,j} \beta_{ij} b_j$, and thus

$$c = \sum_{j\in J} \alpha_j a_j = \sum_{(i,j)\in I\times J} \beta_{ij} a_i b_j,$$

so that $\{a_ib_j\}$ spans K as an F-vector space. Now suppose the set $\{a_ib_j\}$ were linearly dependent. By definition, this means that there is some finite subset $S \subset I \times J$ such that $\{a_ib_j\}_{(i,j)\in S}$ is linearly dependent, and thus there exist $\beta_{ij} \in F$, not all zero, such that

$$\sum_{(i,j)\in S} (\beta_{ij} b_j)a_i = 0.$$

Since the a_i's are K-linearly independent elements of M, we have that for all i, $\sum \beta_{ij} b_j = 0$, and then similarly, since the b_j's are linearly independent elements of K we have $\beta_{ij} = 0$ for all j. □

REMARK 2.1. *In general the degree $[L : K]$ of a field extension is a cardinal number, and the statement of Theorem 2.2 is to be interpreted as an identity of (possibly infinite) cardinals. On the other hand, when M/K and K/F are finite degree extensions, the argument shows that M/F is also a finite degree extension, and the result reduces to the usual product of positive integers. In point of fact the finite degree case is the most useful by far, and in what follows we will almost never write $[L : K]$ unless L/K has finite degree.*

A field extension L/K is **finitely generated** if $L = K(S)$ for some finite subset S of L; when this holds, the least size of such a set S is called the **number of generators** of L/K, and L/K is said to be **monogenic** if the least number of generators is at most 1.

PROPOSITION 2.3. *Let L/K be a field extension of finite degree n. Then L/K can be generated by $\lfloor \log_2 n \rfloor$ elements.*

[2]It is more common to refer to such extensions simply as **finite**, but I have always found the term "finite field extension" to be annoyingly ambiguous: couldn't it also mean that the fields are finite rather than the degree of the extension?

PROOF. We go by induction on n. If $n = 1$, then $L = K$, so L can be generated over K by $0 = \lfloor \log_2 1 \rfloor$ elements, so suppose $n > 1$ and that a field extension of degree $m < n$ can be generated by $\lfloor \log_2 m \rfloor$ elements. Let $\alpha_1 \in L \setminus K$, and put

$$d := [K(\alpha) : K],$$

so $[L : K(\alpha)] = \frac{n}{d} \leq \frac{n}{2} < n$. Let $r := \lfloor \log_2 \frac{n}{d} \rfloor$. By induction, there are elements $\beta_1, \ldots, \beta_r \in L$ such that $L = K(\alpha, \beta_1, \ldots, \beta_r)$ and thus L/K can be generated by

$$1 + \lfloor \log_2 \frac{n}{d} \rfloor \leq 1 + \lfloor \log_2 \frac{n}{2} \rfloor = \lfloor \log_2 n \rfloor$$

elements. □

EXERCISE 2.7. *There is a unique function $\Omega : \mathbb{Z}^+ \to \mathbb{N}$ such that $\Omega(1) = 0$; for all primes p, we have $\Omega(p) = 1$, and for all $m, n \in \mathbb{Z}^+$ we have $\Omega(mn) = \Omega(m) + \Omega(n)$. (So $\Omega(n)$ is the number of prime divisors of n, counted with multiplicity.)*

a) *Adapt the proof of Proposition 2.3 to show: if L/K is a field extension of degree $n \in \mathbb{Z}^+$, then L/K can be generated by $\Omega(n)$ elements.*
b) *Deduce: if for a prime number p we have $[L : K] = p$, then L/K is monogenic.*

Later on in Example 4.22 we will exhibit for all $n \in \mathbb{Z}^+$ a field extension L/K a field extension of degree 2^n for which the minimal number of generators is n, so Proposition 2.3 is sharp...although such examples exist only in characteristic 2. Anyway, Proposition 2.3 shows that finite degree field extensions are finitely generated. The converse is not true: for any field F, the extension $F(t)/F$ is monogenic but of infinite degree: $[F(t) : F] \geq \dim_F F[t] = \aleph_0$. However, the converse is true for the class of field extensions we will study in Parts I and II.

EXERCISE 2.8. *Let F be a field. Show:*

$$[F(t) : F] = \max(\#F, \aleph_0).$$

Let L/K be an extension of fields and $\alpha \in L$. We say that α is **algebraic** over K if there exists some polynomial $P(t) = t^n + a_{n-1}t^n + \ldots + a_1 t + a_0 \in K[t]$ such that $P(\alpha) = 0$. If α is not algebraic over K it is said to be **transcendental** over K. A complex number which is algebraic over $\mathbb{Q}$ is called an **algebraic number**.

EXAMPLE 2.4. *The element i is algebraic over $\mathbb{R}$ since it satisfies the equation $i^2 + 1 = 0$. It is also algebraic over $\mathbb{Q}$ for the same reason. Indeed for any $a \in \mathbb{Q}$, $a^{\frac{1}{n}}$ is algebraic over $\mathbb{Q}$. This is almost tautological, since by $a^{\frac{1}{n}}$, one generally means any complex number α such that $\alpha^n = a$, so α satisfies $t^n - a = 0$.*

The following exercise gives less trivial examples.

EXERCISE 2.9. *Let $\frac{a}{b} \in \mathbb{Q}$. Show $\cos(\frac{a}{b}\pi)$ and $\sin(\frac{a}{b}\pi)$ are algebraic.*

EXERCISE 2.10. *Show: the set of all algebraic numbers is countably infinite.*

So "most" real or complex numbers are transcendental. This was observed by Cantor and stands as a famous early application of the dichotomy between countable and uncountable sets. Earlier Liouville had constructed particular transcendental numbers, like $\sum_{n=1}^{\infty} 10^{-n!}$: an application of the Mean Value Theorem shows that a number which is "too well approximated" by rational numbers cannot be algebraic. It is of course a different matter entirely to decide whether a particular, not obviously algebraic, number which is given to you is transcendental. Let us say only

that both e and π were shown to be transcendental in the 19th century; that there were some interesting results in transcendence theory in the 20th century – e.g. e^π and $2^{\sqrt{2}}$ are transcendental – and that to this day the transcendence of many reasonable looking constants – e.g. π^e, $\zeta(3) = \sum_{n=1}^\infty \frac{1}{n^3}$ – is much beyond our reach.

The problem of determining whether particular numbers are transcendental, although certainly of interest, has little to do with modern field theory. (Rather it is part of the theory of Diophantine approximation, a branch of number theory.)

Now let L/K be a field extension and $\alpha \in L$. By Exercise 3.1.6 there is a unique K-algebra homomorphism $\Phi : K[t] \to L$, $t \mapsto \alpha$. Let I be the kernel of Φ. Since $K[t]/I$ embeds in L, it is a domain, so I is a prime ideal. Since $K[t]$ is a principal ideal domain, there are only two choices:

Case 1: $I = 0$, i.e., Φ embeds $K[t]$ into L. This means precisely that α satisfies no polynomial relations with K-coefficients, so occurs if and only if α is transcendental over K.

Case 2: $I = (P(t))$ is generated by a single irreducible polynomial $P(t)$. Since the units of $K[t]$ are precisely the nonzero elements of K, it follows that there is a unique monic polynomial $P(t)$ (i.e., with leading coefficient 1) that generates I. We call this the **minimal polynomial** of α. Evidently for $Q \in K[t]$ we have $Q(\alpha) = 0 \iff P(t) \mid Q(t)$. In particular $P(\alpha) = 0$, so that α is algebraic, and moreover Φ induces an embedding $K[t]/(P(t)) \hookrightarrow L$. If P has degree d, then we say α is algebraic of degree d; moreover, a K-basis for the left-hand side is $1, t, \ldots, t^{d-1}$, so $[L : K] = d = \deg(P)$.

Let us summarize:

THEOREM 2.5. *Let L/K be a field extension and $\alpha \in L$.*

a) *The following are equivalent:*
   (i) *The element α is algebraic of degree d over K.*
   (ii) *The K-vector space $K[\alpha]$ is finite, of degree d.*
   (iii) *The K-vector space $K(\alpha)$ is finite, of degree d.*

b) *If α is algebraic of degree d, then $K[\alpha] = K(\alpha) \cong K[t]/(P(t))$, where $f(t) \in K[t]$ is the unique degree d monic polynomial such that $f(\alpha) = 0$.*

c) *If α is transcendental over K, then $K[t] \cong K[\alpha] \subsetneq K(\alpha) \cong K(t)$.*

Thus the set of all rational expressions $\frac{P(\pi)}{Q(\pi)}$ with $P, Q \in \mathbb{Q}[t]$ is isomorphic to the rational function field $\mathbb{Q}(t)$! In other words, there is no genuinely algebraic distinction to be made between "fields of numbers" and "fields of functions": rather the distinction is between algebraic field extensions and transcendental field extensions.

A field extension L/K is **algebraic** if every $\alpha \in L$ is algebraic over K.

EXERCISE 2.11.

a) *Let K be a finite field, and let L/K be a field extension of finite degree d. Show: $\#L = (\#K)^d$. In particular, L is finite.*

b) *Let K be a finite field, and let L/K be an algebraic field extension of infinite degre. Show: $\#L = \aleph_0$.*

c) *Let K be an infinite field, and let L/K be an algebraic field extension. Show: $\#L = \#K$.*

COROLLARY 2.6. *A finite degree extension L/K of fields is algebraic.*

PROOF. We go by contraposition: suppose that L/K is transcendental, and let $\alpha \in L$ be transcendental over K. Then by Theorem 2.5c) we have

$$[K(\alpha) : K] \geq [K[\alpha] : K] = [K[t] : K] = \aleph_0,$$

so

$$[L : K] = [L : K(\alpha)][K(\alpha) : K] \geq \aleph_0. \qquad \square$$

THEOREM 2.7. *For an algebraic field extension L/F, the following are equivalent:*

(i) *We have $[L : F] < \aleph_0$.*
(ii) *The extension L/F is finitely generated.*
(iii) *There is $n \in \mathbb{Z}^+$ such that that if K is any finite degree subextension of L/F, then $[K : F] \leq n$.*

PROOF. (ii) $\implies$ (i): Suppose $L = F(\alpha_1, \ldots, \alpha_n)$. Since each α_i is algebraic over F, we have $d_i := [F(\alpha_i) : F] < \aleph_0$. For $0 \leq i \leq n-1$, we have that α_i generates $F(\alpha_1, \ldots, \alpha_i$ over $F(\alpha_1, \ldots, \alpha_{i-1})$, so

$$e_i := [F(\alpha_1, \ldots, \alpha_i) : F(\alpha_1, \ldots, \alpha_{i-1})]$$

is the degree of the minimal polynomial g_i of α_i over $F(\alpha_1, \ldots, \alpha_{i-1})$, while d_i is the degree of the minimal polynomial of α_i over F. Then $g_i \mid f_i$, so $e_i \leq d_i$. It follows that

$$[L : F] = [F(\alpha_1, \ldots, \alpha_n) : F] = e_1 \cdots e_n \leq d_1 \cdots d_n.$$

i) $\implies$ (iii): By Degree Multiplicativity, if $[L : F] = n < \aleph_0$, then $[K : F] \leq n$ for all subextensions K of L/F.
(iii) $\implies$ (ii): We go by contrapositive: suppose that L/F is not finitely generated. Then there is an infinite sequence $\{\alpha_n\}_{n=1}^{\infty}$ in L such that for all $n \in \mathbb{Z}^+$ w have $F(\alpha_1, \ldots, \alpha_{n+1}) \supsetneq F(\alpha_1, \ldots, \alpha_n)$. This implies that for all $k \in \mathbb{Z}^+$ we have $F[(\alpha_1, \ldots, \alpha_k) : F] \geq 2^k$, contradicting (ii). $\square$

REMARK 2.2. *If $R \subseteq T$ is an extension of commutative rings and S is a subset of T, we can define the **R-subalgebra of T generated by S** $R[S]$ as the intersection of all subrings of T containing R and S. More concretely, $R[S]$ is equal to the set of all $f_S \in T$ where $f \in R[\mathbf{T}]$ is a polynomial in indeterminates indexed by the elements of S and then evaluated at the elements of S. We say that T is **finitely generated as an R-algebra** if $T = R[S]$ for some finite subset S of R.*

*For a field extension K/F, having finite degree (being finitely generated as an F-module) implies being finitely generated as an F-algebra, which implies being finitely generated as a field extension. But in fact a field extension K/F is finitely generated as an F-algebra if and only if it has finite degree: this is a basic and important result in commutative algebra called **Zariski's Lemma** [**Cl-CA**, Thm. 11.1]. It follows from this and Corollary 2.6 that for no transcendental field extension K/F is K finitely generated as an F-algebra. So this "intermediate finiteness condition," while crucial in commutative algebra, is of no use in field theory.*

EXERCISE 2.12. *(Direct Limits) Let $(I, \leq)$ be a directed set: recall that this means that I is partially ordered under $\leq$ and for any $i, j \in I$ there exists $k \in I$ with $i \leq k$ and $j \leq k$. A* ***directed system of sets*** *is a family of sets $\{X_i\}_{i \in I}$ together with maps $\iota(i,j) : X_i \to X_j$ for all $i \leq j$ satisfying the natural compatibility conditions: (i) $\iota_{i,i} = 1_{X_i}$ and (ii) for all $i \leq j \leq k$, $\iota(i,k) = \iota(j,k) \circ \iota(i,j)$. By definition, the* ***direct limit*** $\lim_I X$ *is the quotient of the disjoint union $\coprod_{i \in I} X_i$ by the equivalence relation $(x, X_i) \sim (\iota(i,j)x, X_j)$ for all $i \leq j$.*

a) *Show: there are natural maps $\iota_i : X_i \to \lim_I X_i$. State and prove a universal mapping property for the direct limit.*
b) *Suppose the maps $\iota(i,j)$ are all injective. Show that the maps $\iota_i : X_i \to \lim_I X_i$ are all injective. Explain why in this case $\lim_I X_i$ is often informally referred to as the "union" of the X_i's.*
c) *In any concrete category $\mathcal{C}$ – i.e., a category whose objects are sets, for which the set of all morphisms from an object A to an object B is a subset of the set of all functions from A to B, and for which composition and identity of morphisms coincide with the usual notions of functions – one has the notion of a directed system $\{A_i\}$ of objects in $\mathcal{C}$, i.e., we have sets A_i indexed by the directed set $(I, \leq)$ and for all $i \leq j$, the function $\iota(i,j) : A_i \to A_j$ is a morphism in $\mathcal{C}$. Give a definition of the direct limit $\lim_I A_i$ in this more general context. Show that the direct limit exists in the following categories: monoids, groups, commutative groups, rings, commutative rings, fields.*
d) *Give an example of a concrete category in which directed limits do not necessarily exist.*[3]
e) *Show that a field extension L/K is algebraic if and only if it is the direct limit of its finite subextensions.*

Once again we say that a field extension K/F is **monogenic** if there is $\alpha \in K$ such that $K = F(\alpha)$. In this case, K/F has finite degree if and only if it is algebraic, in which case we also have $K = F[\alpha]$. When K/F has finite degree, an element α such that $K = F[\alpha]$ is called a **primitive element** for K/F.

A finite degree field extension need *not* be monogenic, but counterexamples lie some ways down from the surface. Later on, Example 4.22 shows that if k is a field of characteristic p and $k(x,y)$ is a two variable rational function field over k, then the extension $k(x,y)/k(x^p, y^p)$ has degree p^2 and is not monogenic. This is probably the simplest possible example of a nonmonogenic field extension. First of all, Corollary 5.3 will show that every finite degree *separable* field extension is monogenic. Separable algebraic extensions will be defined in Chapter 5, but for now we mention that in characteristic 0 every finite degree field extensoin is separable, while in characteristic $p > 0$, a finite degree extension of degree coprime to p is separable. By Exercise 2.7b), every extension of prime degree is monogenic. So degree p^2 in characteristic p is as simple as it gets.

EXERCISE 2.13.

a) *Let $n \in \mathbb{Z}^{\geq 2}$, and let K/F be a monogenic field extension of degree n. Suppose that the characteristic of F does* not *divide n. Show: K/F has a*

[3]Suggestion: impose some finiteness condition on one of the above categories.

primitive element α with minimal polynomial

$$f(t) = t^n + a_{n-2}t^{n-2} + \ldots + a_1 t + a_0.$$

(Hint: when $n = 2$, this is a piece of high school algebra called "completing the square." It has a straightforward generalization to any n.)

b) *Let p be a prime number, let F be a field* not *of characteristic p, and let K/F be a degree p field extension. Show: there are $a_0, \ldots, a_{p-2} \in F$ such that $K \cong F[t]/(t^p + a_{p-2}t^{p-2} + \ldots + a_1 t + a_0)$.*

For a field F, we write

$$F^2 := \{x^2 \mid x \in F\}$$

for the set of squares in F, including 0, and

$$F^{\times 2} := \{x^2 \mid x \in F^\times\}$$

for the set of nonzero squares in F. Notice that $F^{\times 2}$ is a subgroup of $F^\times$.

EXERCISE 2.14. *Let F be a field, and let $a \in F \setminus F^2$. By $F(\sqrt{a})$ we mean the quadratic field extension $F[t]/(t^2 - a)$ of F.*

a) *Suppose that the characteristic of F is not 2. Show: if K/F is a quadratic extension, then K is isomorphic as an F-algebra to $F(\sqrt{a})$ for some $a \in F \setminus F^2$.*

b) *Suppose that for $a, b \in F \setminus F^2$ we have $F(\sqrt{a}) \cong F(\sqrt{b})$. Show: $\frac{a}{b} \in F^{\times 2}$.*

EXERCISE 2.15. *Let F be a field of characteristic 2, and let K/F be a quadratic extension. Show that exactly one of the following holds:*

(i) *$K = F[\alpha]$ for an element $\alpha \in K$ with minimal polynomial $t^2 + a_0 \in F[t]$.*

(ii) *$K = F[\alpha]$ for an element $\alpha \in K$ with minimal polynomial $t^2 + t + a_0 \in F[t]$.*

3. Some Impossible Constructions

The results we have derived so far do not look very deep to modern eyes, but they were recognized in the 19th century to imply negative solutions to several of the longest standing open problems in mathematics. Namely, the Greeks were interested in **constructibility** of quantities using a compass and a straightedge.

We recall one basic setup: under certain conditions we can construct **points**, **lines** and **circles** in the Euclidean plane $\mathbb{R}^2$. These are viewed as separate types: just because we can construct a line or circle does not mean that we have constructed all the points that lie on it. A construction takes place in finitely many stages $0 \leq i \leq n$. At the end of Stage i we have constructed a finite number of points, lines and circles, and everything that we've constructed at Stage i remains constructed at Stage $i+1$. We start at the end of Stage 0, with the points $(0, 0)$ and $(1, 0)$ having been constructed and not having constructed any lines or circles. For $1 \leq i \leq n$, in Stage i we construct either a line or a circle, as follows: if after Stage $i-1$ we have constructed distinct points P_1 and P_2, then in Stage i we can construct the line L that joins them, adding that line to our supply of constructed lines. At the same time, whenever L has a unique intersection point with any previously constructed line, then we add that point to our set of constructed points, and whenever L intersects with any previously constructed circle, it does so in either one or two points, and we add those points to our set of constructed points. Alternately, if we have previously constructed a point P_1 and distinct points P_2 and P_3, in Stage i we can construct the circle with center P_1 and with radius the distance from P_2 to

P_3. Then, whenever our circle intersects with any previously constructed line, we add the (one or two) intersection points to our supply of constructed points, and whenever our circle intersects with any previously constructed circle, we add the (one or two) intersection points to our supply of constructed points.

To a point (a, b) in the Cartesian plane we can attach the complex number $a + bi$. Let us agree not to distinguish between the two: i.e., we identify $\mathbb{R}^2$ and $\mathbb{C}$ in this (extremely standard!) way. Then a complex number $\alpha = a + bi$ is constructible if there is a finite step construction at the end of which, it lies in the set of constructed points. Certainly 0 is constructible, and a nonzero complex number α is constructible if and only if $-\alpha$ is constructible: we may construct the line L joining 0 and α, the circle C centered at 0 with radius $|\alpha|$, and then $L \cap C = \{\alpha, -\alpha\}$. It is useful to think of positive constructible real numbers as *constructible lengths*: positive real number α is constructible if and only if we can construct two points P and Q with distance α.

For a subset S of $\mathbb{R}$, we put $S^{>0} := \{s \in S \mid s > 0\}$.

EXERCISE 2.16. *Let $a + bi$ be a complex number (with $a, b \in \mathbb{R}$!). Show: $a + bi$ is constructible if and only if the real numbers a and b are constructible.*

EXERCISE 2.17. *Let $\alpha, \beta \in \mathbb{R}$ be constructible numbers.*

a) *Show: $\alpha \pm \beta$ is constructible.*
b) *Show: $\alpha\beta$ is constructible.*
c) *Show: if $\alpha \neq 0$, then $\frac{1}{\alpha}$ is constructible.*
d) *Deduce: the set $\mathcal{C}_{\mathbb{R}}$ of constructible real numbers is a subfield of $\mathbb{R}$.*

EXERCISE 2.18.

a) *Let α be a positive (real) constructible number. Show: $\sqrt{\alpha}$ is constructible.*
b) *Deduce: The field $\mathcal{C}_{\mathbb{R}}$ of real constructible numbers has infinite degree over $\mathbb{Q}$.*

We now consider constructible angles, in two different (but closely related) senses. First, for $\theta \in \mathbb{R}$ we identify "the angle θ" with the complex number $e^{i\theta}$, and we say that the angle θ is constructible if $e^{i\theta}$ is constructible. Second, let (L_1, L_2) be an ordered pair of intersecting lines in the plane ($L_1 = L_2$ is allowed). This determines an angle $\theta \in [0, 2\pi)$ in a way that we may safely leave to the reader. Then if L_1 is a constructible line, then L_2 is a constructible line if and only if the angle beween them is a constructible angle. (This amounts to a classical geometric construction of "copying an angle.") This implies that sums of constructible are angles are constructible, which is the key to the following exercise.

EXERCISE 2.19.

a) *Let $\theta_1, \theta_2 \in \mathbb{R}$. Show: if the angles θ_1 and θ_2 are both constructible, then so are $\theta_1 \pm \theta_2$.*
b) *Show: the set $\mathcal{C}$ of constructible complex numbers is a subfield of $\mathbb{C}$. (Hint: write $\alpha \in C^\times$ as $re^{i\theta}$.)*
c) *Show: $[\mathcal{C} : \mathcal{C}_{\mathbb{R}}] = 2$.*

EXERCISE 2.20.

a) *Show: if the angle $\theta \in \mathbb{R}$ is constructible, then so is $\frac{\theta}{2}$.*

b) *Show: if $\alpha \in \mathcal{C}$, then $\pm\sqrt{\alpha} \in \mathcal{C}$.*

Let $F \subseteq \mathbb{R}$ be a subfield.
• Let L be a line in $\mathbb{R}^2$. We say L is **F-rational** if it is the solution set in $\mathbb{R}^2$ of an equation $ax + by + c = 0$ with $a, b, c \in F$. Then L is F-rational if it contains two distinct points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ with $x_1, x_2, y_1, y_2 \in F$.
• Let C be a circle in $\mathbb{R}^2$ with center (x_0, y_0) and radius r. We say C is **F-rational** if $x_0, y_0, r^2 \in F$. (Thus for instance $x^2 + y^2 = 2$ counts as a $\mathbb{Q}$-rational circle even though its radius, $\sqrt{2}$, does not lie in $\mathbb{Q}$.)

The point of these definitions is:

PROPOSITION 2.8. *Let F be a subfield of $\mathbb{R}$. Let L be an F-rational line, and let C, C_1, C_2 be F-rational circles, with $C_1 \neq C_2$.*

a) *We have $\#(L \cap C) \leq 2$. If the intersection consists of a single point $P = (x, y)$, then $x, y \in F$. If the intersection consists of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_1)$, then there is $d \in F \cap \mathbb{R}^{>0}$ such that $x_1, x_2, y_1, y_2 \in F(\sqrt{d})$.*
b) *We have $\#(C_1 \cap C_2) \leq 2$. If the intersection consists of a single point $P = (x, y)$, then $x, y \in F$. If the intersection consists of two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_1)$, then there is $d \in F \cap \mathbb{R}^{>0}$ such that $x_1, x_2, y_1, y_2 \in F(\sqrt{d})$.*

PROOF. a) Let C be given by the equation $(x - x_0)^2 + (y - y_0)^2 = r^2$ with $x_0, y_0, r \in F$. By interchanging x and y if necessary, we may assume that L is given by an equation $y = mx + b$ with $m, b \in F$, and then points (x, y) in $L \cap C$ satisfy

$$(x - x_0)^2 + (mx + b - y_0)^2 = r^2,$$

definining a quadratic polynomial in x with coefficients in F. If the discriminant of this quadratic is negative, there are no real solutions, so $L \cap F = \varnothing$. If the discriminant is 0, then the quadratic has a double root, so is of the form $(x - x_1)^2$, and since the coefficients lie in F, this means $x_1 \in F$, and $L \cap F$ consists of the single F-rational point $(x_1, mx_1 + b)$. If the discriminant is positive, we get two roots over $F(\sqrt{d}) \subseteq \mathbb{R}$, and for each such x_i, then $y_i = mx_i + b$ also lies in $F(\sqrt{d})$.
b) Suppose C_1 and C_2 are given by the equations

$$(x - x_1)^2 + (y - y_1)^2 = r_1^2, \ (x - x_2)^2 + (y - y_2)^2 = r_2^2$$

with $x_1, x_2, y_1, y_2, r_1^2, r_2^2 \in F$. Subtracting these equations, we get

$$(-2x_1 + 2x_2)x + (-2y_1 + 2y_2)y + x_1^2 - x_2^2 + y_1^2 - y_2^2 - r_1^2 + r_2^2 = 0,$$

which is the equation of an F-rational line L. Thus $C_1 \cap C_2 \subseteq C_1 \cap L$, and we are reduced to part a). □

REMARK 2.3. *Although the proof of Proposition 2.8b) is certainly convincing, I confess that I am slightly surprised by the result. Compare to the intersection of two ellipses: clearly there can be as many as four intersection points, and although there are some favorable special cases when the ellipses are "geometrically aligned," when both ellipses are given by equations over $\mathbb{Q}$ then in general the x- and y-coordinates of the solutions will generate a quartic extension of $\mathbb{Q}$. This quartic extension field may not be real: in particular it can happen that two ellipses have only two (real!) intersection points (x_1, y_1) and (x_2, y_2) but still $\mathbb{Q}(x_1, y_1)/\mathbb{Q}$ is a*

quartic extension. Thus for intersecting circles, the key is really that there are at most two simultaneous solutions to the two equations not only in $\mathbb{R}^2$ but also in $\mathbb{C}^2$.

Now we can prove a key algebraic property of constructible numbers. The complex number i is constructible: this is one of the most basic exercises on geometric constructions, and we leave it to the reader. So long as we are not worried about the number of steps in a construction (which we won't be), we may therefore assume that after Step 0 we have constructed the complex numbers $0, 1, i$ and the lines $y = 0$ and $x = 0$, and we put $E_0 = \mathbb{Q}$ and $F_0 \coloneqq \mathbb{Q}(i)$. Then at Stage 1 we construct either a circle or a line and add all the intersection points to our set of constructed numbers. In fact, again at the cost only of interfering with the numbering of Steps, let us suppose that at Stage 1 we construct all possible lines and circles from the points $0, 1, i$ constructed in Stage 0. Since we have three different pairs of distinct points, we can construct 3 lines, all of which are $\mathbb{Q}$-rational. The three points determine two different distances: 1 and $\sqrt{2} = |1 - i|$. So we can construct 6 circles, all of which are $\mathbb{Q}$-rational (here we take advantage of the fact that the rationality of a circle involves r^2, not r). Then we construct all of the intersection points. By Proposition 2.8, for each intersection point $P = x_P + iy_P$, there is a positive rational number d_P such that x_P, y_P lie in $\mathbb{Q}(\sqrt{d_P})$, so P lies in $\mathbb{Q}(i, \sqrt{d_P}) = F_0(\sqrt{d})$. Let $d_1, \ldots, d_n$ be all the positive rational numbers that we obtain in this way from these points P (each d_i is well-defined up to multiplication by a rational square), and put $E_1 \coloneqq E_0(\sqrt{d_1}, \ldots, \sqrt{d_n}) = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_n})$ and $F_1 \coloneqq F_0(\sqrt{d_1}, \ldots, \sqrt{d_n}) = \mathbb{Q}(\sqrt{-1}, \sqrt{d_1}, \ldots, \sqrt{d_n})$, so each point P lies in F_1. Now we continue: at Stage 2 we construct all possible lines and circles using the points constructed in Step 1. Since each point P from Step 1 has its x and y-coordinates lying in E_1, these lines and circles are E_1-rational, so each intersection point $P = x_P + iy_P$ constructed in Step 2 has the property that x_P, y_P lie in $E_1(\sqrt{D})$ for some $D \in E_1^{>0}$. Collecting all these elements as $D_1, \ldots, D_N$, we put $E_2 \coloneqq E_1(\sqrt{D_1}, \ldots, \sqrt{D_N})$ and $F_2 \coloneqq F_1(\sqrt{D_1}, \ldots, \sqrt{D_N}) = E_1(\sqrt{-1}, \sqrt{D_1}, \ldots, \sqrt{D_N})$. And we continue. Every constructible number lies in F_n for some $n \in \mathbb{Z}^+$, and every constructible real number lies in E_n for some $n \in \mathbb{Z}^+$.

This yields an algebraic description of the fields $\mathcal{C}_{\mathbb{R}}$ and $\mathcal{C}$:

THEOREM 2.9.

a) *Let $\alpha \in \mathbb{R}$. Then α is constructible if and only if there is a finite sequence of positive real numbers $\alpha_1, \ldots, \alpha_n$ such that all of the following hold:*
   (i) *$\alpha_1 \in \mathbb{Q}$;*
   (ii) *For all $1 \leq i \leq n-1$, we have $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})^{>0}$;*
   (iii) *$\alpha_n = \alpha$.*

b) *Let $\alpha \in \mathbb{C}$. Then α is constructible if and only if there is a finite sequence of complex numbers $\alpha_1, \ldots, \alpha_n$ such that all of the following hold:*
   (i) *$\alpha_1 \in \mathbb{Q}$;*
   (ii) *For all $1 \leq i \leq n-1$, we have $\alpha_i^2 \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{i-1})$;*
   (iii) *$\alpha_n = \alpha$.*

PROOF. a) Above we defined an increasing sequence of subfields $\{E_n\}_{n=0}^{\infty}$ of $\mathbb{R}$ whose union is $\mathcal{C}_{\mathbb{R}}$ and such that for all $n \geq 1$, E_n is obtained from E_{n-1} adjoining the square roots of finitely many elements of $E_{n-1}^{>0}$. Thus we have a finite tower of extensions starting at E_{n-1} and ending at E_n such that at each stage we adjoin the

square root of a positive element of a field at the previous stage. This proves half of part a). Conversely, by Exercise 2.18a), the field $\mathcal{C}_{\mathbb{R}}$ of constructible real numbers is closed under taking square roots of positive elements, so every real number $\alpha = \alpha_n$ for a tower as in part a) is constructible.
b) Let $\alpha = a+bi \in \mathcal{C}$. Then $a, b \in \mathcal{C}_{\mathbb{R}}$, so they both lie in E_n for some $n \in \mathbb{Z}^+$. Thus we get a finite tower $\alpha_1, \ldots, \alpha_n$ as in part a) such that $a, b \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, and then if take $\alpha_{n+1} := -1$, then $\alpha \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \alpha_{n+1})$. Conversely, by Exercise 2.20b), the field $\mathcal{C}$ of cosntructible complex numbers is closed under taking square roots, so every compelx number $\alpha = \alpha_n$ for a tower as in part b) is constructible. □

Because a field extension that can be broken into a finite tower of quadratic extensions has degree a power of 2, we conclude:

COROLLARY 2.10. *Let $\alpha \in \mathbb{C}$ be constructible. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2.*

It also makes sense to consider constructibility in a relative sense: namely, instead of starting at Stage 0 with $\{0, 1\}$, we can start with a subset $S \supseteq \{0, 1\}$ of $\mathbb{C}$ and ask which numbers can be constructed from S. Then Theorem 2.9 adapts easily: instead of requiring $\alpha_1 \in \mathbb{Q}$, we require that α_1 lies in the subfield of $\mathbb{R}$ generated by the real and imaginary parts of the elements of S. When $S = \{0, 1, \alpha\}$, we speak of constructions from α.

As an example of this terminology and result, it follows that we can constructively bisect angles: given $\theta \in \mathbb{R}$, from $e^{i\theta}$ we can construct $e^{i\frac{\theta}{2}}$ since it is a square root of $e^{i\theta}$.[4]
We can also consider relative constructions in $\mathbb{R}^n$ for $n \geq 3$: we start with a subset S of $\mathbb{R}^n$, and then each basic construction takes place in a two-dimensional linear subspace of $\mathbb{R}^n$.

EXERCISE 2.21. *The ancient Greeks sought to **double the cube**: given 8 points in $\mathbb{R}^3$ forming the vertices of a cube C, construct the vertices of cube whose volume is twice that of C. Assuming without loss of generality that C is the unit cube, doubling the cube involves constructing the real number $\sqrt[3]{2}$. Show: this is impossible.*

Here is a striking theorem:

THEOREM 2.11 (Lindemann, 1882). *The number π is transcendental over $\mathbb{Q}$.*

We will not prove Theorem 2.11 here, but see e.g. [**Ni39**] for a proof.

EXERCISE 2.22. *The ancient Greeks sought to **square the cicle**: given a circle C in the plane, to construct a square with area equal to the area of C. Use Lindemann's Theorem to show that squaring the circle is impossible.*

EXERCISE 2.23. *The ancient Greeks sought to **trisect the angle**: given $\theta \in \mathbb{R}$, to construct $e^{\frac{i\theta}{3}}$ from $e^{i\theta}$.*

a) *Show: the angle $\frac{2\pi}{3}$ is constructible.*
(This is the *easiest geometric construction!)*

[4]There is not really any new content here: via Exercise 2.20, the reason that we know that $\mathcal{C}$ is closed under taking square roots is that we can constructively bisect a constructible angle. The geometry behind this is that *given* an angle, we can bisect it using a compass and straightedge, which in our terminology means that angles can be constructively bisected.

b) *Show: the angle $\frac{2\pi}{9}$ is not constructible.*
(Hint: what is the minimal polynomial of $\cos(\frac{2\pi}{9})$?)
c) *Deduce: trisecting the angle is impossible.*

Exercise 2.23 raises a question: what are the constructible angles? We will immediately answer it, realize that the answer is not as interesting as it could be, and then adjust to a more interesting question.

Since by "the angle θ" we mean the complex number $e^{i\theta}$, we are asking which constructible numbers $z = x + yi$ lie on the unit circle, i.e., for ordered pairs (x, y) of constructible real numbers such that $x^2+y^2 = 1$. This implies that x is a real constructible number of absolute value at most 1, and conversely the complex numbers ± 1 are certainly constructible, while if x is a constructible real number of absolute value less than 1, then it is the x-coordinate of two points on the unit circle, whose y-coordinates are $\pm\sqrt{1-x^2}$, both of which are constructible real numbers. Thus constructible angles are parametrized by constructive real numbers x with $|x| \leq 1$.

Another way to express the above is: the angle θ is constructible if and only if $\cos\theta$ is constructible. But for a *given* θ of interest, this is not a good answer: indeed, is $\cos\theta$ constructible or not?!? Which are angles are "of interest"? Since we are doing algebra, it seems reasonable to restrict to algebraic real numbers θ. Then a theorem of Lindemann–Weierstrass asserts (in particular) that for algebraic θ, $e^{i\theta}$ is algebraic if and only if $\theta \in \mathbb{Q}$. This leads us to ask: which roots of unity are constructible? We need only look at positive rational numbers in lowest form, so let $a, n \in \mathbb{Z}^+$ be coprime. Then each of $\zeta_1 =: e^{\frac{2\pi i a}{n}}$ and $\zeta_2 = e^{\frac{2\pi i}{n}}$ is a power of the other, so we have $\mathbb{Q}(\zeta_1) = \mathbb{Q}(\zeta_2)$ and thus ζ_1 is constructible if and only if ζ_2 is, showing that any primitive nth root of unity is constructible if and only if all nth roots of unity are constructible. Since the nth roots of unity are the vertices of the regular n-gon ("the" one that lies on the unit circle), our question of constructibility of rational angles is equivalent to asking for which $n \in \mathbb{Z}^+$ the regular n-gon is constructible. This has a beautiful answer: first recall that a **Fermat prime** is a prime number of the form $2^{2^a} + 1$ for $a \in \mathbb{N}$. The number $2^{2^a} + 1$ is prime for $a \in \{0, 1, 2, 3, 4\}$ and for no other known values. It is in fact somewhat plausible that there are no other Fermat primes, but this is an open question.

THEOREM 2.12 (Gauss–Wantzel). *For $n \in \mathbb{Z}^+$, the following are equivalent:*
(i) *The regular n-gon is constructible.*
(ii) *The number n is of the form $2^a p_1 \cdots p_r$ with $a \in \mathbb{N}$ and $p_1, \ldots, p_r$ distinct Fermat primes.*

In 1801 Gauss stated Theorem 2.12 and prove that (ii) $\implies$ (i). This is not his most illustrious result, but he seems to have been quite fond of it: his tombstone has a regular 17-gon engraved on it ($17 = 2^{2^2} + 1$). Wantzel showed that (ii) $\implies$ (i) in 1837. In fact, in the same paper Wantzel showed, for the first time, the impossibility of doubling the cube and trisecting the angle.

Let us put

$$\zeta_n := e^{\frac{2\pi i}{n}}.$$

In §9.1, we will prove that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where $\varphi(n)$ is Euler's totient function: it is the number of integers $1 \leq k \leq n$ that are coprime to n, or equivalently, the

size of the unit group $(\mathbb{Z}/n\mathbb{Z})^\times$. Combining this with Corollary 2.10, we find that if the regular n-gon is constructible, then $\varphi(n)$ is a power of 2. This reduces Wantzel's part of Theorem 2.12 to an elementary number-theoretic exercise.

We remind the reader of a formula for $\varphi(n)$: for prime numbers $p_1 < \ldots < p_r$ and $a_1, \ldots, a_r \in \mathbb{Z}^+$, we have

$$\varphi(p_1^{a_1} \cdots p_r^{a_r}) = \prod_{i=1}^r (p_i^{a_i} - p_i^{a_i - 1}).$$

EXERCISE 2.24. *Let $n \in \mathbb{Z}^+$.*

a) *Suppose $\varphi(n)$ is a power of 2. Show: n is of the form $2^a p_1 \cdots p_r$ for $a \in \mathbb{N}$ and primes $2 < p_1 < \ldots < p_r$.*

b) *Suppose $n = 2^a p_1 \cdots p_r$ for $a \in \mathbb{N}$ and primes $2 < p_1 < \ldots < p_r$. Show: $\varphi(n)$ is a power of 2 if and only if $p_i - 1$ is a power of 2 for all $1 \le i \le r$.*

c) *Let $k \in \mathbb{N}$, and suppose $2^k + 1$ is prime. Show: k must be a power of 2. (Hint: let $m \in \mathbb{Z}^+$ be odd, and let $k \in \mathbb{N}$, and put $a := 2^{2^k}$. Show:*

$$2^{2^k \cdot m} + 1 = (a+1)(a^{m-1} - a^{m-2} + \ldots - a + 1).)$$

d) *Deduce: in Theorem 2.12, condition (ii) holds if and only if $\varphi(n)$ is a power of 2, and thus (i) $\implies$ (ii).*

To prove Gauss's part (i) $\implies$ (ii) of Theorem 2.12, we have to engage with the fact that having $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ be a power of 2 is necessary but not sufficient for α to be constructible. Further exploration of this requires the development of the Galois theory of solvable extensions so must wait until Chapter 9, but we mention without proof that most $\alpha \in \mathbb{C}$ that are quartic algebraic – i.e., $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ – are *not* constructible. In Chapter 9 we will also complete the proof of Theorem 2.12.

4. Subfields of Algebraic Numbers

Let L/K be an arbitrary extension of fields. Consider the set $\mathrm{Cl}_L(K)$ of all elements of L which are algebraic over K. For example, when $K = \mathbb{Q}$, $L = \mathbb{C}$ we are examining the set of all algebraic numbers, which is certainly a proper subset of $\mathbb{C}$.

PROPOSITION 2.13. *The set $\mathrm{Cl}_L(K)$ is a subfield of K.*

We often refer to $\mathrm{Cl}_L(K)$ as the **algebraic closure of K in L**.

Let us this result in a more general context, that of integral extensions of domains. The generalized proof is not much harder and will be extremely useful for any student of algebra. So: let R be a domain and S a domain which extends R, i.e., there is an injective homomorphism $R \to S$. We say that $\alpha \in S$ is **integral over** R if α satisfies a monic polynomial with R-coefficients:

$$\exists\ a_{n-1}, \ldots, a_0 \in R \mid \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

We say that the extension S/R is **integral** if every element of S is integral over R.

Note that if R and S are fields, $\alpha \in S$ is integral over R is by definition precisely the same as being algebraic over R. The next result in fact revisits the basic finiteness property of algebraic elements in this more general context.

THEOREM 2.14. *Let $R \subset T$ be rings, and $\alpha \in T$. The following are equivalent:*

(i) *The α is integral over R.*
(ii) *The ring $R[\alpha]$ is finitely generated as an R-module.*
(iii) *There is an intermediate ring $R \subset S \subset T$ such that $\alpha \in S$ and S is finitely generated as an R-module.*
(iv) *There exists a faithful $R[\alpha]$-submodule M of T which is finitely generated as an R-module.*

PROOF. (i) $\implies$ (ii): If α is integral over R, there are $a_0, \ldots, a_{n-1} \in R$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

or equivalently

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0.$$

This relation allows us to rewrite any element of $R[\alpha]$ as a polynomial of degree at most $n-1$, so that $1, \alpha, \ldots, \alpha^{n-1}$ generates $R[\alpha]$ as an R-module.
(ii) $\implies$ (iii): Take $T = R[\alpha]$.
(iii) $\implies$ (iv): Take $M = S$.
(iv) $\implies$ (i): Let $m_1, \ldots, m_n$ be a finite set of generators for M over R, and express each of the elements $m_i\alpha$ in terms of these generators:

$$\alpha m_i = \sum_{j=1}^{n} r_{ij} m_j, \ r_{ij} \in R.$$

Let A be the $n \times n$ matrix $\alpha I_n - (r_{ij})$; then recall from linear algebra that

$$AA^* = \det(A) \cdot I_n,$$

where A^* is the "adjugate" matrix (of cofactors). If $m = (m_1, \ldots, m_n)$ (the row vector), then the above equation implies $0 = mA = mAA^* = m \det(A) \cdot I_n$. The latter matrix equation amounts to $m_i \det(A) = 0$ for all i. Thus $\bullet \det(A) = \bullet 0$ on M, and by faithfulness this means $\det(A) = 0$. Since so that α is a root of the monic polynomial $\det(T \cdot I_n - (a_{ij}))$. □

LEMMA 2.15. *Let $R \subset S \subset T$ be rings. If $\alpha \in T$ is integral over R, then it is also integral over S.*

PROOF. If α is integral over R, there exists a monic polynomial $P \in R[t]$ such that $P(\alpha) = 0$. But P is also a monic polynomial in $S[t]$ such that $P(\alpha) = 0$, so α is also integral over S. □

LEMMA 2.16. *Let $R \subset S \subset T$ be rings. If S is finitely generated as an R-module and T is finitely generated as an S-module then T is finitely generated as an R-module.*

PROOF. If $\alpha_1, \ldots, \alpha_r$ generates S as an R-module and $\beta_1, \ldots, \beta_s$ generates T as an S-module, then $\{\alpha_i\beta_j\}\{1 \leq i \leq r, 1 \leq j \leq s\}$ generates T as an R-module: for $\alpha \in T$, we have

$$\alpha = \sum_j b_j\beta_j = \sum_i \sum_j (a_{ij}\alpha_i)\beta_j,$$

with $b_j \in S$ and $a_{ij} \in R$. □

COROLLARY 2.17. *(Transitivity of integrality) If $R \subset S \subset T$ are rings such that S/R and T/S are both integral, then T/R is integral.*

PROOF. For $\alpha \in S$, let $\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0 = 0$ be an integral dependence relation, with $b_i \in S$. Thus $R[b_1, \ldots, b_{n-1}, \alpha]$ is finitely generated over $R[b_1, \ldots, b_{n-1}]$. Since S/R is integral, $R[b_1, \ldots, b_{n-1}]$ is finite over R. By Lemma 2.16, $R[b_1, \ldots, b_{n-1}, \alpha]$ is a subring of T containing α and finitely generated over R, so by Theorem 2.14, α is integral over R. □

COROLLARY 2.18. *If S/R is a ring extension, then the set $I_S(R)$ of elements of S which are integral over R is a subring of S, the **integral closure of** R **in** S. Thus $R \subset I_S(R) \subset S$.*

PROOF. If $\alpha \in S$ is integral over R, $R[\alpha_1]$ is a finitely generated R-module. If α_2 is integral over R it is also integral over $R[\alpha_1]$, so that $R[\alpha_1][\alpha_2]$ is finitely generated as an $R[\alpha_1]$-module. By Lemmma 2.16, this implies that $R[\alpha_1,\ \alpha_2]$ is a finitely generated R-module containing $\alpha_1 \pm \alpha_2$ and $\alpha_1 \cdot \alpha_2$. By Theorem 2.14, this implies that $\alpha_1 \pm \alpha_2$ and $\alpha_1\alpha_2$ are integral over R. □

If $R \subset S$ such that $I_S(R) = R$, we say R is **integrally closed** in S.

PROPOSITION 2.19. *Let S be a ring. The operator $R \mapsto I_S(R)$ on subrings of R is a closure operator in the abstract sense, namely it satisfies:*
(CL1) $R \subset I_S(R)$,
(CL2) $R_1 \subset R_2 \implies I_S(R_1) \subset I_S(R_2)$.
(CL3) $I_S(I_S(R)) = I_S(R)$.

PROOF. (CL1) is the (trivial) Remark 1.1. (CL2) is obvious: evidently if $R_1 \subset R_2$, then every element of S which satisfies a monic polynomial with R_1-coefficients also satisfies a monic polynomial with R_2-coefficients. Finally, suppose that $\alpha \in S$ is such that $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$ for $a_i \in I_S(R)$. Then each a_i is integral over R, so $R[a_1, \ldots, a_n]$ is finitely generated as an R-module, and since $R[a_1, \ldots, a_n, \alpha]$ is finitely generated as an $R[a_1, \ldots, a_n]$-module, applying Lemma 2.16 again, we deduce that α lies in the finitely generated R-module $R[a_1, \ldots, a_n, \alpha]$ and hence by Theorem 2.14 is integral over R. □

PROPOSITION 2.20. *Let $R \subset S$ be an integral extension. If R is a field, so is S.*

Proof: Let L be the fraction field of S. If $0 \neq \alpha \in S$ is integral over R, then by Theorem 2.14, $R[\alpha]$ is a finite-dimensional R-submodule of L, so it is a subfield, i.e., is equal to $R(\alpha)$. So $R(\alpha) = R[\alpha] \subset S$, meaning that S contains α^{-1}.

5. Distinguished Classes

Here is an organizing principle for classes of field extensions due to S. Lang.

A class $\mathcal{C}$ of field extensions is **distinguished** if it satisfies these two properties:

(DC1) (Tower meta-property) For a tower $M/K/F$, then $M/F \in \mathcal{C}$ if and only if $M/K \in \mathcal{C}$ and $K/F \in \mathcal{C}$.
(DC2) (Base change meta-property) Let K/F be an element of $\mathcal{C}$, let L/F be any extension such that K and L are contained in a common field. Then $LK/L \in \mathcal{C}$.

We note that (DC1) and (DC2) imply the following

(DC3) (Compositum meta-property) Let K_1/F and K_2/F be elements of $\mathcal{C}$ with K_1, K_2 contained in a common field. Then $K_1K_2/F \in \mathcal{C}$.

Indeed, applying (DC2) we get that $K_1K_2/K_2 \in \mathcal{C}$. Since also $K_2/F \in \mathcal{C}$, applying (DC1) we get that $K_1K_2/F \in \mathcal{C}$.

EXERCISE 2.25.

a) *Show: the class of all finite degree extensions is distinguished.*
b) *Show: the class of all algebraic extensions is distinguished.*

Some examples of distinguished classes of extensions to come later: finitely generated extensions, separable algebraic extensions, purely inseparable algebraic extensions, solvable extensions, purely transcendental extensions.

Some nonexamples of distinguished classes of extensions to come later: normal extensions, Galois extensions, inseparable extensions, abelian extensions, not-necessarily-algebraic separable extensions.

CHAPTER 3

Normal Extensions

1. Algebraically Closed Fields

Let F be a field. A polynomial $f \in F[t]$ is **split** if every irreducible factor has degree 1. If $f \in F[t]$ is a polynomial and K/F is a field extension, we say f **splits in K** if $f \in K[t]$ is split.

PROPOSITION 3.1. *Let F be a field. The following are equivalent:*

(i) *There is no algebraic extension $K \supsetneq F$.*
(ii) *There is no finite degree extension $K \supsetneq F$.*
(iii) *There is no finite degree monogenic extension $F(\alpha) \supsetneq F$.*
(iv) *If $f \in F[t]$ is irreducible, then f has degree 1.*
(v) *If $f \in F[t]$ is nonconstant, then f has a root in F.*
(vi) *Every polynomial $f \in F[t]$ is split.*

*A field satisfying these equivalent conditions is called **algebraically closed**.*

PROOF. (i) $\implies$ (ii) $\implies$ (iii) is immediate.
$\neg$ (iv) $\implies$ $\neg$ (iii): if $f \in F[t]$ is an irreducible polynomial of degree $d > 1$ then $K \coloneqq F[t]/(f)$ is a finite degree monogenic extension of f of degree $d > 1$.
$\neg$ (v) $\implies$ $\neg$ (iv): Suppose f is nonsconstant and admits no root in F. Write $f = f_1 \cdots f_m$ as a product of irreducible polynomials; since linear polynomials have roots in F, no f_i has degree 1.
(iv) $\iff$ (v) $\iff$ (vi) is easy and familiar.
$\neg$ (i) $\implies$ $\neg$ (iv): If $K \supsetneq F$ is a proper algebraic extension, let $\alpha \in K \setminus F$, and let $f \in F[t]$ be the minimal polynomial of α over F, so f is irreducible. By assumption f is also split, so it has degree 1 and is thus of the form $t - \alpha$, contradicting the fact that $\alpha \notin F$. □

THEOREM 3.2 (Fundamental Theorem of Algebra). *The complex field $\mathbb{C}$ is algebraically closed.*

Because the existence of a nonconstant $f \in \mathbb{C}[t]$ without a root in $\mathbb{C}$ leads to absurdities in many areas of mathematics, there are many different proofs, e.g. using degree theory or complex analysis. In Chapter 7 we give a version of Artin's proof of Theorem 3.2 using Galois theory and also Sylow theory. This algebraic argument involves $\mathbb{R}$ as well as $\mathbb{C}$ and shines a spotlight on the following fact: while $\mathbb{R}$ is not algebraically closed, among non-algebraically closed fields it is "as close as possible" in that the quadratic extension $\mathbb{R}(\sqrt{-1})$ is algebraically closed. In Chapter 14 we will prove a remarkable result of Artin–Schreier (Theorem 14.18), part of which is the assertion that if a field F is not algebraically closed but has a finite degree algebraically closed extension field, then in fact $F(\sqrt{-1})$ must be algebraically closed.

PROPOSITION 3.3. *Let L/K be a field extension, with L algebraically closed. Let $\mathrm{Cl}_L(K)$ be the set of all elements of L that are algebraic over K. Then $\mathrm{Cl}_L(K)$ is algebraically closed.*

PROOF. By Proposition 3.1, if $\mathrm{Cl}_L(K)$ is not algebraically closed then there is a monogenic finite degree extension $\overline{K}(\alpha) \supsetneq \overline{K}$. Because α is algebraic over $\mathrm{Cl}_L(K)$ and $\mathrm{Cl}_L(K)$ is algebraic over K, we have by Corollary 2.17 that α is algebraic over K. Let $f \in F[t]$ be the minimal polynomial of α. By Proposition 3.1, as a polynomial over $L[t]$ we have

$$f(t) = (t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_d)$$

for some $\alpha_1, \ldots, \alpha_d \in L$. Each α_i is algebraic over K so lies in $\mathrm{Cl}_L(K)$. Moreover the $\alpha_1, \ldots, \alpha_d$ are the only roots of f in L, and thus for some i we have $\alpha = \alpha_i \in \mathrm{Cl}_L(K)$, a contradiction. □

COROLLARY 3.4. *The field $\overline{\mathbb{Q}}$ of all algebraic numbers is algebraically closed.*

PROOF. Since $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, this follows from Theorem 3.2 and Proposition 3.3. □

Let K be a field. An **algebraic closure** of K is a field extension $\overline{K}/K$ that is both algebraic and algebraically closed. It follows from Proposition 3.1 an algebraic closure of K is precisely a maximal algebraic extension of K, i..e., an algebraic extension that is not properly contained in any other algebraic extension of K.

EXERCISE 3.1. *Let K/F be an algebraic field extension. Let L/K be a field extension. Show: L is an algebraic closure of K if and only if L is an algebraic closure of F.*

2. Existence of Algebraic Closures

In this section we will show that every field admits at least one algebraic closure, a basic but nontrivial result. How might one try to prove this? Probably we can agree to start with the following easy result.

LEMMA 3.5. *Let F be a field, and let $f_1, \ldots, f_n \in F[t]$ be nonconstant polynomials, of degrees $d_1, \ldots, d_n$.*

a) *There is a finite degree field extension K/F such that each f_i has a root in K. Moreover, we can choose K so as to get $[K : F] \leq \prod_{i=1}^n d_i$.*
b) *There is a finite degree field extension K/F such that each f_i splits in K. Moreover, we can choose K so as to get $[K : F] \leq \prod_{i=1}^n (d_i!)$.*

PROOF. a) Let M be a field, and let $f \in M[t]$ be a polynomial of degree d. Let g be an irreducible factor of f, say of degree $d' \leq d$. Then $M[t]/(g)$ is a field extension of M of degree $d' \leq d$ in which g (and hence also f) has a root. By applying this procedure successively to $f_1, \ldots, f_n$ we generate a tower of field extensions $F \subseteq M_1 \subseteq \ldots \subseteq M_n$ such that for all $1 \leq i \leq n$, the polynomials $f_1, \ldots, f_i$ all have a root in M_i and $[M_i : F] \leq d_1 \cdots d_i$, so we may take $K := M_n$.
b) Let M be a field, and let $h \in M[t]$ be a polynomal of degree d. Applying part a) to h, there is a field extension M_1/M of degree at most d in which h has a root α_1 and thus we get a factorization $h(t) = (t - \alpha_1)h_2(t) \in M_1[t]$. We apply part a) to h_2 and get a field extension M_2/M_1 of degree at most $d - 1$ in which h_2 has a root

α_2 and thus we get a factorization $h(t) = (t-\alpha_1)(t-\alpha_2)h_3(t)$. Continuing in this manner, we end up with a field extension M_n of degree at most $d!$ in which h splits. Applying this procedure successively to the polynomials $f_1, \ldots, f_n$ over the field F we get a field extension K of degree at most $\prod_{i=1}^n d_i!$ in which each f_i splits. □

EXERCISE 3.2. *Let $d_1, \ldots, d_n \in \mathbb{Z}^+$.*

a) *Show: there are $f_1, \ldots, f_n \in \mathbb{Q}[t]$ of degrees $d_1, \ldots, d_n$ such that if $K/\mathbb{Q}$ is a number field (i.e., a finite degree field extension) such that each f_i has a root in K then $\prod_{i=1}^n \deg f_i \mid [K:\mathbb{Q}]$.*

b) *Show: there are $f_1, \ldots, f_n \in \mathbb{Q}[t]$ of degrees $d_1, \ldots, d_n$ such that if $K/\mathbb{Q}$ is a number field in which each f_i splits, then $\prod_{i=1}^n d_i! \mid [K:\mathbb{Q}]$.*
(Hint/warning: this is best done using algebraic number theory.)

THEOREM 3.6 (Steinitz). *Every field K can be embedded in an algebraically closed field L. Thus every field has at least one algebraic closure, namely $\mathrm{Cl}_L(K)$.*

PROOF. Step 1: Let $R = K[\mathbb{T}]$ be a polynomial ring over K indexed by a set of indeterminates t_f that are in bijection with the nonconstant polynomials $f \in K[t]$. Consider the ideal I of R generated by all polynomials of the form $f(t_f)$. We claim that I is proper: if not, there is a finite subset $\{f_1, \ldots, f_n\}$ and elements $g_1, \ldots, g_n \in R$ such that

$$g_1 f_1(t_{f_1}) + \ldots + g_n f_n(t_{f_n}) = 1.$$

By Lemma 3.4, there is a finite degree field extension F/K such that each $f_i(t)$ has a root $\alpha_i \in F$. If we evaluate $t_{f_1} = \alpha_1, \ldots, t_{f_n} = \alpha_n$ in the above equation, we get $0 = 1$: contradiction. So we may choose a maximal ideal $\mathfrak{m} \supset I$. Thus $K_1 := R/\mathfrak{m}$ is a field exetnsion of F in which each t_f is a root of f. Thus K_1/K is a field extension in which each nonconstant polynomial $f \in K[t]$ has a root.
Step 2: The natural question here is whether K_1 is algebraically closed. The remainder of the proof consists of a clever evasion of this question! Namely, we apply the construction of Step 1 to K_1, getting a field extension K_2 in which each polynomial with coefficients in K_1 has a root in K_2, and so forth: we generate a sequence of field extensions

$$K \subset K_1 \subset \ldots \subset K_n \subset \ldots.$$

The union $L = \bigcup_n K_n$ is a field, and any nonconstant polynomial $P \in L[t]$, having only finitely many nonzero coefficients lies in $K_n[t]$ for sufficiently large n, thus has a root in K_{n+1} and therefore also in L. So L is algebraically closed, and then by Proposition 3.3 the algebraic closure of K in L is an algebraic closure of K. □

Theorem 3.6 lies among the most important results in all of field theory. So we pause to discuss several aspects of it.

The proof we've given is due to Artin and is taken from [**La**]. Rather suprisingly, it uses polynomial rings in infinitely many indeterminates. Intuitively, after establishing Lemma 3.5 that for any field f and any finite set S of nonconstant polynomials $f \in F[t]$ there is a finite degree field extension $K(S)/F$ in which each $f \in S$ splits, it seems that we should just be able to "iterate" this to get an algebraic extension K_1/F in which every nonconstant $f \in F[t]$ splits. If we already had an algebraically closed field L containing F, then K_1 would just be the direct limit of its subfields $K(S)$ as S ranges over finite sets of irreducible polynomials. Of course the point is

that we don't yet have such a field L, so we need to give these iterated algebraic extensions somewhere to live. If we well-order the set of irreducible polynomials in $F[t]$, then a straightforward transfinite induction argument would give us K_1. This was how Steinitiz proved Theorem 3.6 in [**St10**]. Thus the transition from Steinitz to Lang is trading set-theoretic sophistication for algebraic sophistication.

The proof we just sketched uses that any set can be well-ordered, a set theoretic principle that is famously equivalent to the Axiom of Choice (AC). Throughout this text we freely make use of (AC), usually via another one of its equivalents, Zorn's Lemma. But this may make us wonder about the set-theoretic assumptions implicit in Lang's proof (the one we gave). The proof of Theorem 3.6 does use (AC) in a somewhat disguised way: in the assertion that a proper ideal in a ring is contained in a maximal ideal. In fact the statement that every proper ideal in a commutative ring is contained in a maximal ideal implies (AC). So it is natural to wonder whether the existence of an algebraic closure of any field implies (AC). Indeed not: it would be enough to use that every proper ideal is contained in a prime ideal: this gives us a domain, and we can take the fraction field. The assertion that every proper ideal in a commutative ring is contained in a prime ideal is known to be equivalent to the Ultrafilter Lemma (UL), which does *not* imply (AC).

It seems to be an open problem whether the existence of an algebraic closure of every field implies (UL): cf. `http://mathoverflow.net/questions/46566`. However, it is known that (AC) is required for Theorem 3.6 to hold in the sense that there is a model of Zermelo-Fraenkel set theory in which not every field admits an algebraic closure [**Je**, Thm. 10.13].

Finally, as we pointed out, the proof constructs an extension K_1/K such that every nonconstant $f \in K[t]$ has a root in K_1 and then nimbly evades the question of whether K_1 contains an algebraic closure of K. It turns out that the answer to this is affirmative. We break this up into two steps. First:

PROPOSITION 3.7. *Let L/K be a field extension. Suppose every nonconstant polynomial $f \in K[t]$ splits in L. Then the algebraic closure of K in L is algebraically closed.*

PROOF. Let $\overline{K}$ be the algebraic closure of K in L, let $f \in \overline{K}[t]$ be an irreducible polynomial, and let α be a root of f in some algebraic closure of $\overline{K}$. Then α is algebraic over $\overline{K}$, which is algebraic over K, so α is algebraic over K by Corollary 2.17. Let $g \in K[t]$ be the minimal polynomial of α. By assumption, g splits in L and its roots are algebraic over K, so g splits in $\overline{K}$, so $\alpha \in \overline{K}$. It follows that f has degree 1. By Proposition 3.1, the field $\overline{K}$ is algebraically closed. □

As for the second step: we will record the answer now, but we will need to know more of the structure theory of algebraic field extensions in order to prove it.

THEOREM 3.8. *(Gilmer [**Gi68**]) Let K/F be a field extension. If every nonconstant $f \in F[t]$ has a root in K, then every nonconstant $f \in F[t]$ splits in K.*

EXERCISE 3.3. *Show: no finite field is algebraically closed.*

EXERCISE 3.4.

a) *Show: if K is a field and $\overline{K}$ is an algebraic closure, then $\#\overline{K} = \max(\aleph_0, \#K)$.*
b) *Show: there are algebraically closed fields of all infinite cardinalities.*

3. The Magic Mapping Theorem

THEOREM 3.9. *(Magic Mapping Theorem) Let F be a field. Let K/F be an algebraic field extension, and let L/F be a field extension with L algebraically closed. Then there is an F-algebra homomorphism $\varphi : K \hookrightarrow L$.*

PROOF. Consider the partially ordered set whose elements are are pairs (M, φ) where M is a subextension of K/F and $\varphi : M \to L$ is an F-algebra homomorphism. We say that $(M_1, \varphi_1) \leq (M_2, \varphi_2)$ if $M_1 \subset M_2$ and the restriction of φ_2 to M_1 is φ_1. In this partially ordered set, any chain has an upper bound given by taking the union of the elements of the chain. So by Zorn's Lemma there is a maximal element (M, φ). We claim that $M = K$. If not, let $\alpha \in K \setminus M$, and consider the field extension $M(\alpha)/M$. Let $f \in M[t]$ be the minimal polynomial of α, so $M(\alpha) \cong M[t]/(f)$. We view L as an M-algebra via φ, and thus we may view $f \in L[t]$. Since L is algebraically closed, there is a root in L, say $\overline{\alpha}$. There is a unique M-algebra homomorphism $M(\alpha) \to L$ that maps α to $\overline{\alpha}$: it is unique because $M(\alpha) = M[\alpha]$ is generated as an M-algebra by α, and it exists because $M(\alpha) \cong M[t]/(f(t))$ so the unique M-algebra map $M[t] \to L$ that carries t to $\overline{\alpha}$ has $f(t)$ in its kernel. It follows that $M = K$. □

COROLLARY 3.10 ("Uniqueness" of Algebraic Closure). *Let $\overline{F_1}$ and $\overline{F_2}$ be two algebraic closures of a field F. There is an F-algebra isomorphism $\varphi : \overline{F}_1 \to \overline{F_2}$.*

PROOF. We may apply the Magic Mapping Theorem with $K = \overline{F_1}$ and $L = \overline{F_2}$ to get an F-algebra homomorphism $\varphi : \overline{F_1} \hookrightarrow \overline{F_2}$. Then $\overline{F_2}/\varphi(\overline{F_1}))$ is an algebraic extension of an algebraically closed field, so it cannot be proper: we have $\overline{F_2} = \varphi(\overline{F_1})$ and thus φ is an F-algebra isomorphism. □

Note the scare quotes around *uniqueness*. This is because we have shown that the algebraic closure of F is unique up to F-algebra isomorphism, but given two algebraic closures of F there is in general no *canonical* F-algebra isomorphism between them. If $\varphi, \psi : \overline{F_1} \hookrightarrow \overline{F_2}$ are two F-algebra isomomorphisms, then $\psi^{-1} \circ \varphi$ is an F-algebra automorphism of $\overline{F_1}$, and conversely: the ambiguity in the choice of isomorphism is precisely measured by the group $G_F := \mathrm{Aut}(\overline{F}_1/F)$. This group is called the **absolute Galois group of F** and is in general a very large, interesting group. In fact, we should not speak of "the" absolute Galois group of F (though we will: it is traditional to do so): it is well-defined up to isomorphism, but switching from one isomorphism $\overline{F_1} \to \overline{F_2}$ to another gives rise to an inner automorphism (i.e., a conjugation) of G. More on this later.

REMARK 3.1. *There are models of Zermelo-Fraenkel set theory – i.e., without (AC) – in which a field F can admit non-F-isomorphic algebraic closures.*

COROLLARY 3.11. *Let K_1/F and K_2/F be two algebraic field extensions. If $\varphi : K_1 \hookrightarrow K_2$ is an F-algebra embedding and $\overline{K_i}$ is an algebraic closure of K_i, then φ extends to an isomorphism $\overline{K_1} \hookrightarrow \overline{K_2}$.*

PROOF. Let $\overline{\varphi} : K_1 \hookrightarrow \overline{K_2}$ be the composition of $\varphi : K_1 \to K_2$ with the embedding $K_2 \hookrightarrow \overline{K_2}$; it is an F-algebra embedding. By Theorem 3.9, there is at least one extension of $\overline{\varphi}$ to an F-algebra embedding $\Phi : \overline{K_1} \to \overline{K_2}$. Since $\Phi(\overline{K_1}) \cong_F \overline{K_1}$, also $\Phi(\overline{K_1})$ is algebraically closed, so $\overline{K_2}/\Phi(\overline{K_1})$ is an algebraic extension of algebraically closed fields, and thus $\overline{K_2} = \Phi(\overline{K_1})$, and Φ is an F-algebra isomorphism. □

4. Conjugates

Let K/F be an algebraic field extension. We say that elements $\alpha, \beta \in K$ are **conjugate over F** if α and β have the same minimal polynomial over F. Thus if $[K(\alpha) : K] = d$, then the number of conjugates of α lying in K is at most d. We will see later that whether α has d conjugates in K is is a crucial issue: it will be so if and only if the extension $K(\alpha)/K$ is both normal (the property we are studying in this chapter, with the definition to come soon) and separable (the property we will study in the next chapter).

If K/F is an algebraic extension and $\overline{F}$ is any algebraic closure of F, then as we know there is an F-algebra homomorphism $\iota : K \hookrightarrow \overline{F}$. If $\alpha \in K$ and $f \in F[t]$ is the minimal polynomial of α, then f splits in $\overline{F}$. We call the roots of f in $\overline{F}$ the **conjugates** of α. Notice that the set of conjugates is defined only in terms of the minimal polynomial, which lies in F, so it is independent of the choice of ι.

For the remainder of this section we fix an algebraic closure $\overline{F}$ of F and only consider algebraic extensions K/F that are subextensions of $\overline{F}/F$ (again, every algebraic extension occurs this way *up to F-algebra isomorphism*). From this perspective, being conjugate over F is an equivalence relation on $\overline{F}$. Moreover, if σ is an F-algebra automorphism of $\overline{F}$, then for all $\alpha \in \overline{F}$, we have that $\sigma(\alpha)$ is a conjugate of α: indeed, for every polynomial $f \in F[t]$, we have

$$f(\alpha) = 0 \iff f(\sigma(\alpha)) = 0$$

and thus α and $\sigma(\alpha)$ have the same minimal polynomial. Conversely, if $\alpha, \beta \in \overline{F}$ are conjugate over F, then there is an F-algebra automorphism σ of $\overline{F}$ such that $\sigma(\alpha) = \beta$. Indeed, let $f \in F[t]$ be the common minimal polynomial of α and β. Then the field extensions $F(\alpha)$ and $F(\beta)$ are both isomorphic to $F[t]/(f(t))$, so there is an isomorphism

$$F(\alpha) \to F(\beta),$$

which by Corollary 3.11 extends to an automorphism of $\overline{F}$. We sum up this discussion as follows.

LEMMA 3.12 (Extension Lemma). *Let $\overline{F}$ be an algebraic closure of the field F. For $\alpha, \beta \in \overline{F}$, the following are equivalent:*

(i) *The elements α and β are conjugate over F: that is, they have the same minimal polynomial.*
(ii) *There is $\sigma \in \mathrm{Aut}(\overline{F}/F)$ such that $\sigma(\alpha) = \beta$.*

REMARK 3.2. *Recall that if a group G acts on a set X, we say that two elements $x, y \in X$ are **conjugate** if there is $g \in X$ such that $gx = y$. As we just saw, the terminology of conjugate elements of $\overline{F}$ is compatible with this: two elements of $\overline{F}$ are conjugate if and only if they are conjugate under the action of $\mathrm{Aut}(\overline{F}/F)$.*

EXERCISE 3.5. *Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Show that $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ is infinite.*

5. Splitting Fields

It follows from Proposition 3.7 that if K/F is an algebraic field extension such that every nonconstant $f \in F[t]$ splits in K, then K is an algebraic closure of F. This

view on algebraic closure opens the door to a natural and important generalization: we go from "all polynomials" to "some polynomials."

Let F be a field, and let $\mathcal{S} \subset F[t]$ be a set of nonconstant polynomials. A **splitting field** for $(F, \mathcal{S})$ is a field extension K/F satisfying the following properties:

(SF1) Every $f_i \in \mathcal{S}$ splits in K.
(SF2) No proper subextension of K satisfies (SF1), i.e., if $F \subset K' \subset K$ and every $f_i \in \mathcal{S}$ splits in K', then $K' = K$.

EXERCISE 3.6. *Suppose K/F is a splitting field for $(F, \mathcal{S})$, and K' is an F-algebra isomorphic to K. Show: K' is also a splitting field for $(F, \mathcal{S})$.*

THEOREM 3.13. *(Existence and "Uniqueness" of Splitting Fields) Let F be a field and $S \subset F[t]$ a set of nonconstant polynomials.*

a) *Let $\overline{F}$ be an algebraic closure of F. Then $\overline{F}$ contains a unique splitting field for S, namely the subfield of $\overline{F}$ obtained by adjoining to F all roots α_{ij} of all polynomials $P_i \in S$.*
b) *Splitting fields are unique up to F-algebra isomorphism.*

PROOF. It is no problem to see that the recipe of part a) does indeed construct a splitting field for F and S: clearly every polynomial in S splits in $F(\alpha_{ij})$ and conversely any subfield of $\overline{F}$ in which all the polynomials in F split must contain all the α_{ij}'s. One way to see the uniqueness up to isomorphism is to reduce to the case of uniqueness up to isomorphism of algebraic closures. Namely, let K_1, K_2 be two splitting fields for F and S. It is easy to see that (SF2) implies that K_i/F is algebraic, so let $\overline{K_i}$ be an algebraic closure of K_i. Since K_i is algebraic over F, $\overline{K_i}$ is equally well an algebraic closure of F, so by Corollary 3.10 there exists an F-algebra isomorphism $\Phi : \overline{K_1} \to \overline{K_2}$. Then $\Phi(K_1)$ is a subfield of $\overline{K_2}$ which is a splitting field for F and S, and we just saw that each algebraic closure contains a unique splitting field, so $\Phi(K_1) = K_2$ and $\Phi : K_1 \to K_2$ is an F-algebra isomorphism. □

EXERCISE 3.7. *Show that the field $K = \mathbb{Q}[\zeta_3, \sqrt[3]{2}]$ is the splitting field of $f = t^3 - 2$. Conclude that if $L \subseteq \mathbb{C}$ is such that $L \neq K$, then L is not isomorphic to K.*

6. Normal Extensions

LEMMA 3.14. *Let L/F be an algebraic field extension, and let $\iota : L \hookrightarrow L$ be an F-algebra homomorphism. Then ι is an isomorphism.*

PROOF. What we must show is that ι is surjective, so let $\alpha \in L$. Let $f \in F[t]$ be the minimal polynomial of α, and let r be the number of distinct roots of f in K. Then r is the number of distinct linear factors of $f \in L[t]$; since $\iota : L \to \iota(L)$ is an F-algebra isomorphism, r is also the number of distinct linear factors of $f \in \iota(L)[t]$ hence also the number of root of f in $\iota(L)$. Thus we must have $\alpha \in \iota(L)$, or else f would have fewer roots in $\iota(L)$ than in L. □

REMARK 3.3. *Lemma 3.14 need not hold for transcendental field extensions. For instance, if F is a field and $L = F(t)$ is a rational function field, then $\frac{f(t)}{g(t)} \mapsto \frac{f(t^2)}{g(t^2)}$ defines an F-algebra isomorphism $\iota : L \to L$ with image $F(t^2) \subsetneq F(t)$. It*

is interesting to ask for which transcendental field extensions L/F there is an F-algebra embedding $\iota : L \hookrightarrow L$ that is not an isomorphism. We will say a bit more about this in Part II.

THEOREM 3.15. *Let K/F be an algebraic field extension. Let $\overline{F}$ be an algebraic closure of K (hence also of F). The following are equivalent:*

(i) *For every F-algebra embedding $\sigma : K \hookrightarrow \overline{F}$ we have $\sigma(K) = K$.*
(ii) *K/F is the splitting field of a subset $\mathcal{S} \subseteq F[t]$.*
(iii) *Every irreducible polynomial $f \in F[t]$ with a root in K splits in K.*
(iv) *For all $\alpha \in K$, if $\beta \in \overline{F}$ is an F-conjugate of α, then $\beta \in K$.*

An extension K/F satisfying these properties is called ***normal***.[1]

PROOF. (i) $\iff$ (iv): We saw above that for $\alpha \in K$ and $\beta \in \overline{F}$, β is a conjugate of α in $\overline{F}$ if and only if there is an F-algebra homomorphism $\sigma : K \hookrightarrow \overline{F}$ such that $\sigma(\alpha) = \beta$. It follows that as we range over all F-algebra homomorphisms $\sigma : K \hookrightarrow \overline{F}$, we have that $\bigcup_\sigma \sigma(K)$ is the set of all conjugates of all elements of K. Condition (iv) holds if and only if the set of all conjugates of all elements of K is just K itself if and only if $\bigcup_\sigma \sigma(K) = K$ if and only if (by Lemma 3.14) $\sigma(K) \subseteq K$ for all σ if and only if $\sigma(K) = K$ for all $\sigma(K)$: condition (i).
(iii) $\iff$ (iv) is immediate.
(ii) $\iff$ (iv): Condition (ii) can be rephrased by saying that K is generated by adjoining to F a subset $\mathcal{S}$ of $\overline{F}$ that is stable under conjugation. Thus if (iv) holds, then (ii) holds with $\mathcal{S} = K$. Conversely, suppose that K is obtained by adjoining to F a set $\mathcal{S}$ that is stable under conjugation, and let $x \in K$. Then $x = f(\alpha_1, \ldots, \alpha_n)$ is a rational function in elements $\alpha_1, \ldots, \alpha_n \in \mathcal{S}$ with F-coefficients. Every conjugate of x in $\overline{F}$ is of the form $\sigma(x)$ for some F-automorphism σ of $\overline{F}$, and then

$$\sigma(x) = f(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) \in K,$$

since $\mathcal{S}$ is closed under conjugation. □

EXERCISE 3.8. *Let $F \subseteq K \subseteq L$ be field extensions. If L/F is normal, show that L/K is normal.*

EXAMPLE 3.16. *For each $n \geq 3$, the extension $K = \mathbb{Q}[\sqrt[n]{2}]/\mathbb{Q}$ is a non-normal extension of degree n. Indeed, let $\zeta_n = e^{2\pi i/n}$; the other roots of $t^n - 2$ in $\mathbb{C}$ are $\zeta_n^k \cdot \sqrt[n]{2}$ with $0 \leq k < n$, which are not even real numbers unless $k = 0$ or $k = \frac{n}{2}$. So $t^n - 2$ does not split over K. In this case, any extension of K which is normal over $\mathbb{Q}$ must contain all the roots of $t^n - 2$, hence must contain $\sqrt[n]{2}$ and ζ_n. Therefore the smallest normal extension is the splitting field of $t^n - 2$, which is $M = \mathbb{Q}[\sqrt[n]{2}, \zeta_n]$.*

EXERCISE 3.9.

a) *Suppose K/F is a field extension with $[K : F] \leq 2$. Show: K/F is normal.*
b) *Use the example $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ to show that if we have fields $F \subset K \subset L$ and K/F and L/K are both normal, then L/F need not be normal. (Thus normality does not satisfy the* ***tower meta-property****.)*

EXAMPLE 3.17. *Suppose F has characteristic $p > 0$. Suppose $a \in F$ is such that $f(t) = t^{p^n} - a \in F[t]$ is irreducible. Let $K = F[t]/(f(t))$, and write α for the coset $t + (f(t))$: thus $\alpha^{p^n} = a$. Then as an element of $K[t]$ we have $f(t) = (t - \alpha)^{p^n}$.*

[1]Normal field extensions are by definition algebraic.

That is, despite the fact that f has degree p^n, α is conjugate in $\overline{F}$ only to itself. Thus K/F is a normal extension.

EXERCISE 3.10. *Show: a direct limit of normal extensions is normal.*

EXERCISE 3.11.

a) *Let L/F be an extension and K_1, K_2 be subextensions. Show: $K_1 \cap K_2$ is again an extension field of F.*
b) *As above, but with any collection of intermediate field extensions $\{K_i\}_{i \in I}$.*

PROPOSITION 3.18. *Let L/F be an extension and $\{K_i\}_{i \in I}/F$ a collection of algebraic subextensions. If each K_i/F is normal, then so is $K := \bigcap_i K_i$.*

PROOF. Without loss of generality we may replace L by the algebraic extension $\mathrm{Cl}_L(F)/F$. Let $f \in F[t]$ be an irreducible polynomial with a root α in K. Then for all $i \in I$, f has a root in K_i, thus each f_i contains all the F-conjugates of α, hence so does K, so f splits in K. □

EXERCISE 3.12. *Let F be a field.*

a) *Let L/F be a field extension, let K_1, K_2 be subextensions of L/F, and let $\sigma \in \mathrm{Aut}(L/F)$. Show:*

$$\sigma(K_1K_2) = \sigma(K_1)\sigma(K_2).$$

b) *Let K_1, K_2 be two normal algebraic extensions, inside a common algebraic closure $\overline{F}$ of F. Show: the compositum K_1K_2 is a normal extension of F.*
c) *Let I be a nonempty set, and for each $i \in I$ let K_i/F be a normal algebraic field extension, inside a common algebraic closure $\overline{F}$ of F. Show: the compositum $\bigvee_{i \in I} K_i$ is a normal extension of F.*

Let K/F be an algebraic field extension, and let $\overline{K}$ be an algebraic closure of K. Then $\overline{K}/F$ is certainly normal. Since the intersection of any family of normal subextensions of $\overline{K}$ is normal, it follows that there is a unique smallest subextension L, $F \subset K \subset L \subset \overline{K}$, such that L/F is normal. If we define a **normal closure** of an extension K/F to be an extension L/K which is normal over F and such that no proper subextension is normal over F, then we just constructed a normal closure, by intersecting all normal subextensions inside an algebraic closure of K.

EXERCISE 3.13. *Let K/F be an algebraic extension. Show that any two normal closures of K/F are F-isomorphic.*

PROPOSITION 3.19. *Let K/F be a field extension of finite degree n. Then the degree of the normal closure M of K/F is at most $n!$.*

PROOF. Put $F = F_0$. Write $K = F(\alpha_1, \ldots, \alpha_d)$ and for $1 \leq i \leq d$, put $K_i = F(\alpha_1, \ldots, \alpha_i)$ and $d_i := [K_i : K_{i-1}]$. An argument almost identical to that of Lemma 3.5b) yields a field extension M/K containing all the conjugates of $\alpha_1, \ldots, \alpha_d$ and such that $[M : F] = \prod_{i=1}^d d_i!$. Thus the normal closure of K/F has degree at most $\prod_{i=1}^d d_i!$. Now

$$n = [K : F] = \prod_{i=1}^d [K_i : K_{i-1}] = \prod_{i=1}^d d_i.$$

It follows that $\prod_{i=1}^d d_i! \leq n!$: for instance take sets $S_1, \ldots, S_d$ of cardinalities $d_1, \ldots, d_d$. Then $\prod_{i=1}^d d_i!$ is the number of bijections of $S := \prod_{i=1}^n S_i$ that preserve each coordinate, while $(d_1 \cdots d_n)!$ is the number of bijectiions of S. □

The "correct" conclusion of Proposition 3.19 is that $[M : F]$ *divides* $n!$. We will prove this later: Theorem 7.20.

For a field extension K/F, we denote by $\mathrm{Aut}(K/F)$ the set of F-algebra automorphisms of K: more explicitly, this is the set of field isomorphisms $\sigma : K \to K$ such that $\sigma(x) = x$ for all $x \in F$. Composition of F-algebra automorphisms endows $\mathrm{Aut}(K/F)$ with the structure of a group.

PROPOSITION 3.20. *Let $F \subseteq K \subseteq L$ be a tower of algebraic field extensions, with L/F normal.*

a) *The following are equivalent:*
   (i) *The extension K/F is normal.*
   (iii) *Restriction of maps from L to K gives a well-defined homomorphism $r : \mathrm{Aut}(L/F) \to \mathrm{Aut}(K/F)$.*

b) *If the equivalent conditions of part a) hold, then the homomorphism $r : \mathrm{Aut}(L/F) \to \mathrm{Aut}(K/F)$ is surjective and thus realizes $\mathrm{Aut}(K/F)$ as a quotient group of $\mathrm{Aut}(L/F)$.*

PROOF. a) Let $\overline{F}$ be an algebraic closure of F containing L. First suppose that K/F is normal, and let $\sigma \in \mathrm{Aut}(L/F)$. Let $\overline{\sigma} : L \to \overline{F}$ be $\sigma : K \to K$ followed by the inclusion $L \hookrightarrow \overline{F}$. By Theorem 3.15, we have $\sigma(K) = K$, so $\sigma|_K \in \mathrm{Aut}(K/F)$ and we get a well-defined restriction map $r : \mathrm{Aut}(L/F) \to \mathrm{Aut}(K/F)$. It is immediate that it is a group homomorphism. Now suppose that K/F is *not* normal. By Theorem 3.15, there is an F-algebra embedding $\sigma : K \hookrightarrow \overline{F}$ such that $\sigma(K) \neq K$, hence by Lemma 3.14 $\sigma(K)$ is not contained in K. By Corollary 3.11, the map σ can be extended to $\overline{F}$, hence it can be extended to $\tilde{\sigma} : L \hookrightarrow \overline{F}$, and because L/F is normal, by Theorem 3.15 we have $\tilde{\sigma}(L) = L$. Moreover we have that $\tilde{\sigma}(K) = \sigma(K)$ is not contained in K, so restricting $\tilde{\sigma}$ from L to K does *not* give an element of $\mathrm{Aut}(K/F)$.
b) Since K/F is normal, we have a restriction homomorphism $r : \mathrm{Aut}(L/F) \to \mathrm{Aut}(K/F)$. If $\sigma \in \mathrm{Aut}(K/F)$ then by Corollary 3.11 σ extends to an isomorphism $\overline{\sigma} : \overline{F} = \overline{K} \to \overline{F}$, and because L/F is normal, restricting $\overline{\sigma}$ to L gives an element $\tilde{\sigma}$ of $\mathrm{Aut}(L/F)$ such that $r(\tilde{\sigma}) = \sigma$. □

7. The Extension Theorem

The following result is an immediate consequence of already developed results, but it is so useful that we state and prove it so as to be able to refer to it later on.

THEOREM 3.21 (Extension Theorem). *Let K/F be a normal field extension. For $\alpha, \beta \in K$, the following are equivalent:*

(i) *The elements α and β are conjugates over F: they have the same minimal polynomial over F.*
ii) *There is an F-algebra automorphism $s \in \mathrm{Aut}(K/F)$ such that $s(\alpha) = \beta$.*

PROOF. (i) $\implies$ (ii): When $K = \overline{F}$ is an algebraic closure of F, this is half of Lemma 3.12. In general, let $\overline{F}$ be an algebraic closure of F containing K, and let $\sigma \in \mathrm{Aut}(\overline{F}/F)$ be such that $\sigma(\alpha) = \beta$. By Theorem 3.15 we have $\sigma(K) = K$, so

$s \coloneqq \sigma|_K \in \mathrm{Aut}(K/F)$ and $s(\alpha) = \beta$.
(ii) $\implies$ (i): For any field extension K/F, if $\alpha \in K$ is algebraic over F and $\beta \in K$ is such that there is some $s \in \mathrm{Aut}(K/F)$ such that $s(\alpha) = \beta$, then let $P \in F[t]$ be the minimal polynomial of α over F. Then

$$0 = \sigma(0) = \sigma(P(\alpha)) = P(\sigma(\alpha)) = P(\beta),$$

so β is a conjugate of α over F. □

The following exercise shows that the conclusion of Theorem 3.21 need not hold when K/F is not normal.

EXERCISE 3.14. *Let $F = \mathbb{Q}$ and $K \coloneqq \mathbb{Q}(\sqrt[3]{\sqrt{2}+5})$.*

a) *Show that $\sqrt{2}$ and $-\sqrt{2}$ lie in K and are conjugate over F.*
b) *Show:* $\mathrm{Aut}(K/F) = \mathrm{Aut}(K) = \{e\}$.

CHAPTER 4

Separable Algebraic Extensions

Let K/F be an algebraic field extension. We have already explored one desirable property for K/F to have: normality. Normality can be expressed in terms of stability under F-homomorphisms into any extension field, and also in terms of irreducible polynomials: every irreducible polynomial in $F[t]$ with a root in $K[t]$ must split. There is another desirable property of an algebraic extension L/K called **separability**. In some sense it is dual to normality, but this is hard to believe at first because there is a large class of fields F for which all algebraic extensions K/F are separable, including all fields of characteristic 0. (For that matter, there are fields for which every algebraic extension is normal, like $\mathbb{R}$ and $\mathbb{F}_p$.) Like normality, separability can also be expressed in terms of polynomials and also in terms of embedding conditions. We begin with a study of polynomials.

1. Separable Polynomials

Let F be a field, and consider the univariate polynomial ring $F[t]$. Let I be a nonzero ideal of $F[t]$, and let $g \in I$ be a nonzero polynomial of least degree. For any $f \in I$, by polynomial division we may write $f = qg + r$ with $q, r \in F[t]$ and either $r = 0$ or $\deg r < \deg g$. Since $r = f - qg \in I$ and g has minimal degree among nonzero elements of I, we must have $r = 0$. Thus $I = \langle g \rangle$ is a principal ideal, so $F[t]$ is a principal ideal domain (PID). For elements a, b of a domain R, a **greatest common divisor** of a and b is an element D such that $D \mid a$ and $D \mid b$ and if any $d \in R$ divides both a and b then $d \mid D$. When a gcd exists, it is unique precisely up to multiplication by a unit of R. In any PID, a generator D of the ideal $\langle a, b \rangle$ is a gcd of a and b. For $a, b \in F[t]$, not both zero, we define $\gcd(a, b)$ to be the monic generator of the nonzero ideal $\langle a, b \rangle$.

LEMMA 4.1. *Let K/F be a field extension, and let $a, b \in F[t]$. Let $D_F \in F[t]$ be the gcd of a and b, and let $D_K \in K[t]$ be the gcd of a and b viewed as elements of $K[t]$. Then $D_F = D_K$.*

PROOF. There are $A, B \in F[t]$ such that $D_F A = a$ and $D_F B = b$, so D_F is a common divisor of a and b in $K[t]$ and thus $D_F \mid D_K$. On the other hand, there are $f, g \in F[t]$ such that $fa + gb = D_F$. Since $D_K \mid f$ and $D_K \mid g$, we have $D_K \mid D_F$. Therefore $D_F = D_K$.[1] □

For $f \in F[t]$, we define the **derivative** of f in a way that generalizes the derivative for polynomial functions $f : \mathbb{R} \to \mathbb{R}$: namely, we put

$$(a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0)' := n a_n t^{n-1} + (n-1) a_{n-1} t^{n-2} + \ldots + a_1.$$

[1] Essentially the same result holds in any extension of PIDs.

Otherwise put, the derivative $(\cdot)'$ is the unique F-linear endomorphism of $F[t]$ satisfiying the power rule:

$$\forall n \in \mathbb{N},\ (t^n)' = nt^{n-1}.$$

Needless to say, this version of the derivative is not defined via a limiting process; it is a purely algebraic gadget. To emphasize this, some call it the "formal derivative."

EXERCISE 4.1. *Let F be a field.*

a) *(Product Rule) Show: for all $f, g \in F[t]$, we have $(fg)' = f'g + fg'$.*
b) *(Chain Rule) Show: for all $f, g \in F[t]$, we have $(f(g))' = f'(g)g'$.*
c) *If $f \in F[t]$ has degree $n \geq 1$, it is immediate from the definition that $\deg f' = n-1$. If F has characteristic 0, show: $\deg f' = n-1$ and*
$$\{f \in F[t] \mid f' = 0\} = F.$$
d) *Suppose F has characteristic $p > 0$. Show:*
$$\{f \in F[t] \mid f' = 0\} = F[t^p].$$

A nonzero polynomial $f \in F[t]$ is **separable** if $\gcd(f, f') = 1$.

PROPOSITION 4.2. *Let F be a field, and let $f \in F[t]$ be a nonzero polynomial.*

a) *If f is irreducible, then f is separable if and ony if $f' \neq 0$.*
b) *If f is separable and $g \mid f$, then g is separable.*
c) *The polynomial f is separable if and only if it is squarefree (i.e., not divisibly by p^2 for any irreducible polynomial p) and every irreducible factor of f is separable.*
d) *For any field extension K/F, $f \in F[t]$ is separable if and only if $f \in K[t]$ is separable.*
e) *If F is algebraically closed, then f is separable if and only if it is squarefree.*

PROOF. For all nonzero $g \in F[t]$ and $a \in F^\times$, we have that g is separable if and only if ag is separable. So we may suppose throughout that f is monic.
a) Suppose f is irreducible. Since $\gcd(f, f')$ divides the irreducible polynomial f, we have either $\gcd(f, f') = 1$ or $\gcd(f, f') = f$ and f is separable precisely in the first case. Clearly if $f' = 0$ then $\gcd(f, f') = \gcd(f, 0) = f$. If $f' \neq 0$, then since $\deg f' < \deg f$ we have $f \nmid f' \mid \gcd(f, f')$, so $\gcd(f, f') \neq f$.
b) We go by contrapositive: suppose g is not separable, so there is a polynomial d of positive degree dividing both g and g'. Write $f = gh$. Then $f' = gh' + g'h$, so d divides both f and f'.
c) If some irreducible factor of f is inseparable, then by part b) f is inseparable. If $f = p^2 g$ for some irreducible polynomial p, then

$$f' = (p^2 g)' = 2pp'g + p^2 g',$$

so p divides both f and f' and thus f is not separable. Conversely, we may suppose that $f = p_1 \cdots p_r$ is a product of distinct monic ireducible separable polynomials. If f is not separable, then some irreducible polynomial p divides both f and f'; the former implies that $p = p_i$ for some i. We have

$$f' = p_1' p_2 \cdots p_r + p_1 p_2' p_3 \cdots p_r + \ldots + p_1 \cdots p_{r-1} p_r'.$$

In this expression every term other than the ith term is divisible by p_i, so $p_i \mid f'$ if and only if $p_i \mid (\prod_{j \neq i} p_j) p_i'$, but since $p_1, \ldots, p_r$ are nonassociate irreducible elements and p_i is separable, this is not the case.

d) This is immediate from Lemma 4.1: $\gcd(f, f')$ is the same whether it is computed in $F[t]$ or in $K[t]$.
e) If F is algebraically closed, then all irreducible factors p of f are linear, and for a linear polynomial p we have $p' \in F^\times$, so cetainly p is separable. Thus the result follows from part d). □

THEOREM 4.3. *Let F be a field, and let K be an algebraically closed field containing F. For a polynomial $f \in F[t]$ of degree $n \geq 1$, the following are equivalent:*

(i) *The polynomial f is separable.*
(ii) *In K, the polynomial f splits into distinct linear factors.*
(iii) *There are distinct elements $\alpha_1, \ldots, \alpha_n \in K$ such that $f(\alpha_i) = 0$ for all $1 \leq i \leq k$.*

PROOF. (i) $\iff$ (ii): By Proposition 4.2d), the separability of f can be checked as a polynomial in $\overline{F}[t]$, and by Proposition 4.2e), $f \in \overline{F}[t]$ is separable if and only if it is squarefree, i.e., splits into distinct linear factors.
(ii) $\iff$ (iii): This is immediate; the number of distinct roots of f in K is equal to the number of its distinct linear factors. □

COROLLARY 4.4. *Let $f \in F[t]$ be irreducible.*

a) *If F has characteristic 0, then f is separable.*
b) *Suppose F has characteristic $p > 0$.*
   (i) *f is inseparable if and only if $f = g(t^p)$ for some $g \in F[t]$.*
   (ii) *There is $a \in \mathbb{N}$ such that $f(t) = g(t^{p^a})$ for an irreducible separable polynomial $g \in F[t]$. If the distinct roots of g in an algebraic closure are $\beta_1, \ldots, \beta_m$, then the roots of f in an algebraic closure are $\beta_1^{p^{-a}}, \ldots, \beta_m^{p^{-a}}$, each with multiplicity p^a.*

PROOF. By Proposition 4.2a), f is separable if and only if $f' = 0$. If F has characteristic 0, then by Exercise 4.1c) the only polynomials with zero derivative are the constant polynomials and f has positive degree. This proves part a). Henceforth we assume that F has characteristic $p > 0$.

b) By Exercise 4.1d) we have $f' = 0$ if and only if $f = g(t^p)$ for some $g \in F[t]$ (i.e., every monomial appearing in f has degree a multiple of p), proving part (i). If f is separable, then the conclusion of (ii) holds with $a = 0$, so we may assume that f is inseparable, hence $f = g_1(t^p)$ for some $g_1 \in F[t]$. The polynomial g_1 must be irreducible, because if it factors as $h_1 h_2$ with h_1, h_2 of positive degree, then $f = h_1(t^p)h_2(t^p)$ is reducible. Now we repeat: if g_1 is not separable, then $g_1 = g_2(t^p)$ for an irreducible polynomial g_2, and so forth. Eventually we may write $f = g(t^{p^a})$ for an irreducible, separable $g \in F[t]$ and $a \in \mathbb{Z}^+$. The assertion about the roots of f and g follows immediately. □

A field F is **perfect** if every irreducible polynomial $f \in F[t]$ is separable. By Corollary 3.13, fields of characteristic 0 are perfect. If F has characteristic $p > 0$, then F is perfect if and only if no polynomial of the form $f(t) = g(t^p)$ is irreducible. This is a more interesting condition: let's explore it a bit. In the field $\mathbb{F}_p$ of order p, consider such a polynomial

$$f(t) = a_n t^{np} + a_{n-1} t^{(n-1)p} + \ldots + a_1 t^p + a_0.$$

For all $a \in \mathbb{F}_p$ we have $a^p = a$: indeed, this is clear if $a = 0$, and otherwise $a \in \mathbb{F}_p^\times$, a group of order $p-1$, so $a^{p-1} = 1$ by Lagrange's Theorem and thus $a^p = a$. So in

this case we have

$$f(t) = a_n^p t^{np} + a_{n-1}^p t^{(n-1)p} + \ldots + a_1^p t^p + a_0^p = (a_n t^n + \ldots + a_1 t + a_0)^p,$$

the last equality being because the **Frobenius map**

$$\mathfrak{f} : F \to F,\ x \mapsto x^p$$

is a field homomorphism in characteristic p. We've shown:

PROPOSITION 4.5. *For all $f \in \mathbb{F}_p[t]$, we have $f(t^p) = f(t)^p$.*

Proposition 4.5 shows that $\mathbb{F}_p$ is perfect: since $f(t^p) = f(t)^p$ is a pth power, it is certainly not reducible. The same idea carries further: in a field F of characteristic p, suppose that the Frobenius homomorphism $\mathfrak{f} : F \to F$ is surjective: that is, every element of x is a pth power. Then for

$$f(t^p) = a_n t^{np} + \ldots + a_1 t^p + a_0,$$

for $0 \leq i \leq n$ there is $b_i \in F$ such that $b_i^p = a_i$, so

$$f(t^p) = b_n^p t^{np} + \ldots + b_1^p t^p + b_0^p = (b_n t^n + \ldots + b_1 t + b_0)^p$$

so again $f(t^p)$ is not irreducible and F is perfect.

EXERCISE 4.2.

a) *Show: every finite field is perfect.*
b) *Show: every algebraically closed field is perfect.*

Now we have a key technical result:

LEMMA 4.6. *Let F be a field of characteristic $p > 0$ and $\alpha \in F \setminus F^p$. (That is, α is not a pth power in F.) Then for all $n \geq 1$, the polynomial $t^{p^n} - \alpha$ is irreducible.*

PROOF. We shall prove the contrapositive: suppose that for some $n \in \mathbb{Z}^+$ the polynomial $t^{p^n} - \alpha$ is reducible; we will show that $\alpha \in F^p$. We may write $t^{p^n} - \alpha = f(t)g(t)$, where $f(t)$ and $g(t)$ are nonconstant monic polynomials. Let K/F be an extension field containing a root β of $t^{p^n} - \alpha$, so that in $K[t]$ we have

$$t^{p^n} - \alpha = t^{p^n} - \beta^{p^n} = (t - \beta)^{p^n}.$$

Since $f(t)$ and $g(t)$ are monic, we therefore have $f(t) = (t-\beta)^r$ for some $0 < r < p^n$. Write $r = p^m s$ with $\gcd(p, s) = 1$. Note that $m < n$. Then

$$f(t) = (t^{p^m} - \beta^{p^m})^s,$$

so that the coefficient of $t^{p^m(s-1)}$ is $-s\beta^{p^m}$. This lies in F and – since $s \neq 0$ in F – we conclude $\beta^{p^m} \in F$. Thus

$$\alpha = (\beta^{p^m})^{p^{n-m}} \in F^{p^{n-m}} \in F^p$$

since $m < n$. □

We immediately deduce the following important result:

THEOREM 4.7. *For a field F of characteristic $p > 0$, the following are equivalent:*

(i) *Every irreducible polynomial $f \in F[t]$ is separable.*
(ii) *The Frobenius homomorphism $\mathfrak{f} : F \to F$ is surjective.*

PROOF. We gave the proof of (ii) $\implies$ (i) above. Inversely, if (ii) fails, there is some $\alpha \in F \setminus F^p$, and then by Lemma 4.6 the polynomial $t^p - \alpha$ is irreducible and inseparable. □

REMARK 4.1. *At some point it was popular to define a polynomial to be separable if each of its irreducible factors had distinct roots in an algebraic closure: see e.g.* [**BAI**, p. 233]. *With this definition, a field is perfect if and only if every polynomial is separable. With this alternate definition, every polynomial $f \in F[t]$ becomes separable over $\overline{F}[t]$ for any algebraic closure $\overline{F}$ of F. However, more recently algebraists have seen advantages to making definitions that are "faithfully preserved under base change." While it makes no real difference in field theory, in broader algebra this becomes more significant: for any nonconstant $f \in F[t]$, we may consider the finite-dimensional F-algebra $A_f := A[t]/(f)$. Then our definition makes it true that f is separable if and only if A_f is an* ***étale algebra****, i.e., an algebra that is semisimple and remains semisimple after arbitrary base change.*

EXERCISE 4.3. *Let F be a field of characteristic p, with an algebraic closure $\overline{F}$. Define $F^{1/p} = \{\beta \in \overline{F} \mid \beta^p \in F\}$.*

a) *Show: $F^{1/p}$ is a subextension of $\overline{F}/F$.*
b) *Define a tower of subextensions*
$$F \subseteq F^{1/p} \subseteq F^{1/p^2} \subseteq \dots F^{1/p^a} \subseteq \dots \subseteq \overline{F},$$
and show that if F is imperfect, all these inclusions are strict.
c) *Define $F^{1/p^\infty} = \bigcup_{a=1}^{\infty} F^{1/p^a}$. Show that F^{1/p^∞} is perfect and is the intersection of all perfect subextensions of $\overline{F}$. It is called the* ***perfect closure*** *of F.*

A polynomial $f \in F[t]$ is **purely inseparable** if there is exactly one $\alpha \in \overline{F}$ such that $f(\alpha) = 0$. As above, there are certainly purely inseparable polynomials over F – $(t - \alpha)^n$ for any $\alpha \in F$ and $n \in \mathbb{Z}^+$ – and what is of interest is the purely inseparable irreducible polynomials, which can only exist in characteristic $p > 0$.

PROPOSITION 4.8. *Let F be a field of characteristic $p > 0$. The irreducible, purely inseparable monic polynomials $f(t) \in F[t]$ are precisely those of the form $t^{p^a} - \alpha$ for some $a \in \mathbb{Z}^+$ and some $\alpha \in F \setminus F^p$.*

PROOF. By Lemma 4.6, any polynomial of the form $t^{p^a} - \alpha$ for $\alpha \in F \setminus F^p$ is irreducible. Conversely, let $P(t) \in F[t]$, By Proposition 3.11c), there is a polynomial $P_2(t)$ such that $P(t) = P_2(t^p)$. Since P is irreducible, so is P_2. If there are distinct $\alpha, \beta \in \overline{F}$ such that $P_2(\alpha) = P_2(\beta)$ then there are unique and distinct elements $\alpha^{\frac{1}{p}}$, $\beta^{\frac{1}{p}}$ in $\overline{F}$ such that $P(\alpha^{\frac{1}{p}}) = P(\beta^{\frac{1}{p}}) = 0$, contradicting the pure inseparability of α. Therefore P_2 must itself be irreducible purely inseparable, and an evident inductive argument finishes the proof. □

EXERCISE 4.4. *Show that the polynomial $t^6 - x$ over the field $\mathbb{F}_3[x]$ is irreducible and inseparable but not purely inseparable.*

2. Separable Algebraic Field Extensions

Let F be a field and $P(t)$ an irreducible, inseparable polynomial over F of degree $d > 1$. Consider the finite field extension $K = F[t]/(P(t))$ of F. It exhibits some strange behavior. First, the only F-algebra embedding $\sigma : K \to \overline{K}$ is the inclusion

map. Indeed, such embeddings correspond bijectively to the assignments of $t \in K$ to a root α of P in $\overline{K}$, and by assumption there are less than d such elements. It follows that the group $\mathrm{Aut}(K/F)$ of F-algebra automorphisms of F has cardinality smaller than d.

For an extension K/F, the **separable degree** $[K : F]_s$ is the cardinality of the set of F-algebra embeddings $\sigma : K \to \overline{F}$.

EXERCISE 4.5. *Show that the separable degree may be computed with respect to embeddings into any algebraically closed field containing F.*

THEOREM 4.9. *The separable degree is multiplicative in towers: if $L/K/F$ is a tower of finite degree field extensions, then $[L : F]_s = [L : K]_s[K : F]_s$.*

PROOF. Let $\sigma : F \hookrightarrow C$ be an embedding of F into an algebraically closed field. Let $\{\sigma_i\}_{i \in I}$ be the family of extensions of σ to K, and for each $i \in I$ let $\{\tau_{ij}\}_{j \in J_i}$ be the family of extensions of σ_i to L. Each σ_i admits precisely $[L : K]_s$ extensions to embeddings of L into C: in particular, the cardinality of J_i is independent of i and there are thus precisely $[L : K]_s[K : F]_s$ F-algebra embeddings τ_{ij} overall. These give all the F-algebra embeddings $L \hookrightarrow C$, so $[L : F]_s = [L : K]_s[K : F]_s$. □

COROLLARY 4.10. *Let K/F be a finite degree field extension. Then*

$$[K : F]_s \leq [K : F].$$

In particular, the separable degree is finite.

PROOF. We employ dévissage: break up K/F into a finite tower of simple extensions. Each simple extension has finite degree and by Theorem 4.9 the degree is multiplicative in towers. We are therefore reduced to the case $K = F(\alpha) \cong F[t]/(P(t))$, where $P(t)$ is the minimal polynomial for α. In this case the result is clear, since an F-algebra homomorphism of $F[t]/(P(t))$ into any field M is given by sending the image of t to a root of $P(t)$ in M, and the degree $[K : F]$ polynomial has at most $[K : F]$ roots in any field. □

In the situation of the proof of Corollary 4.10 we can say more: the separable degree $[F(\alpha) : F]_s$ is equal to the number of distinct roots of the minimal polynomial $P(t)$ of α. In particular it is equal to the degreee of the field extension if and only if $P(t)$ is a separable polynomial. Let us record this result.

PROPOSITION 4.11. *For K/F a field extension and $\alpha \in K$ algebraic over F, the following are equivalent:*

(i) *The minimal polynomial of α is a separable polynomial.*
(ii) $[F(\alpha) : F]_s = [F(\alpha) : F]$.

More generally:

THEOREM 4.12. *For a finite degree field extension K/F, the following are equivalent:*

(i) *Every element of K is separable over F.*
(ii) *We have $[K : F]_s = [K : F]$.*

*A field extension satisfying these equivalent conditions is said to be **separable**.*

PROOF. (i) $\implies$ (ii): We may write K/F as a finite tower of simple extensions:

$$F = F_0 \subseteq \ldots \subseteq F_n = K$$

such that for all i we have $F_{i+1} = F_i(\alpha_{i+1})$. Since α_{i+1} is separable over F, it is separable over F_i: indeed, the minimal polynomial for α_{i+1} over the extension field divides the minimal polynomial over the ground field. Therefore Proposition 4.11 applies and $[F_{i+1} : F_i]_s = [F_{i+1} : F_i]$ for all i. Since both the separable degree and the degree are multiplicative in towers, we conclude $[K : F]_s = [K : F]$.
(ii) $\implies$ (i): Seeking a contradiction, we suppose that there exists $\alpha \in K$ which is not separable over F. By Proposition 4.11, it follows that $[F(\alpha) : F]_s < [F(\alpha) : F]$. Now applying Theorem 4.9 and Corollary 4.10 we get

$$[K : F]_s = [K : F(\alpha)]_s[F(\alpha) : F]_s < [K : F(\alpha)][F(\alpha) : F] = [K : F]. \qquad \square$$

COROLLARY 4.13. *Finite degree separable extensions are a distinguished class of field extensions: that is, they satisfy (DC1) and (DC2) of §3.4 and thus also (DC3).*

EXERCISE 4.6. *Prove Corollary 4.13.*

THEOREM 4.14.
Let L/F be an algebraic field extension. The following are equivalent:

(i) *Every finite degree subextension of L/F is separable.*
(ii) *Every irreducible polynomial $f \in F[t]$ with a root in L is separable.*
(iii) *L is obtained by adjoining to F a set of roots of separable polynomials.*
(iv) *L is obtained by adjoining to F a set of roots of irreducible separable polynomials.*

An extension satisfying these equivalent properties is called a ***separable algebraic extension****.*

EXERCISE 4.7. *Prove Theorem 4.14.*

COROLLARY 4.15. *Algebraic separable extensions are a distinguished class of field extensions.*

EXERCISE 4.8. *Prove Corollary 4.15.*

COROLLARY 4.16. *For a family $\{K_i/F\}_{i \in I}$ of algebraic field extensions inside a common algebraically closed field M, the following are equivalent:*

(i) *For all $i \in I$, K_i/F is a separable algebraic field extension.*
(ii) *The compositum $\prod_i K_i$ is a separable algebraic field extension.*

EXERCISE 4.9. *Prove Corollary 4.16.*

Corollary 4.16 has the following important consequence: for any field extension K/F, there exists a unique maximal separable algebraic subextension $\mathrm{SepCl}_K(F)$, the **separable closure of F in K**.

EXERCISE 4.10. *A* ***separable closure (or separable algebraic closure)*** *F^{sep}/F is a separable algebraic field extension that admits no proper separable algebraic field extensions.*

a) *Show: an algebraic extension of F is a separable algebraic closure of F if and only if it is the splitting field of all separable polynomials $f \in F[t]$.*

b) *Deduce: separable algebraic closures exist, are unique up to F-algebra isomorphism and are normal over F.*
c) *Let $\overline{F}$ be an algebraic closure of F. Show: the unique separable algebraic closure of F inside $\overline{F}$ is* $\mathrm{SepCl}_{\overline{F}}(F)$.
d) *Show: $F^{\mathrm{sep}} = \overline{F}$ if and only if F is perfect.*

3. Purely Inseparable Extensions

THEOREM 4.17. *For an algebraic field extension K/F, the following are equivalent:*

(i) *There is only one F-algebra embedding $K \hookrightarrow \overline{F}$.*
(ii) *Every irreducible polynomial $f \in F[t]$ with a root in K is purely inseparable.*
(iii) *K is obtained by adjoining to F roots of purely inseparable irreducible polynomials.*
(iv) *The separable closure of K in F is F.*

EXERCISE 4.11. *Prove Theorem 4.17.*

An extension satisfying the conditions of Theorem 4.17 is **purely inseparable**.

LEMMA 4.18.

a) *The finite degree purely inseparable extensions form a distinguished class.*
b) *The purely inseparable algebraic extensions form a distinguished class that is closed under composita.*

PROOF. a) Condition (i) of Theorem 4.17 shows that a finite extension K/F is purely inseparable if and only if its separable degree $[K : F]_s$ is 1. If K/F and L/K are both finite degree extensions, then by Theorem 4.9 we have $[L : F]_s = [L : K]_s[K : F]_s$. It follows that L/F is is purely inseparable if and only if both K/F and L/K are purely inseparable: meta-property (DC1). Now let K/F be a finite degree purely inseparable extension, and let L/F be any field extension such that K and L are subfields of a common field. By Theorem 4.9, there are $\alpha_1, \ldots, \alpha_n$ in K and $a_1, \ldots, a_n \in \mathbb{Z}^+$ such that $K = F(\alpha_1^{p^{-a_1}}, \ldots, \alpha_n^{p^{-a_n}})$. Then $L = F(\alpha_1^{p^{-a_1}}, \ldots, \alpha_n^{p^{-a_n}})$. For $1 \leq i \leq n$, the element $\alpha_i^{p^{-a_i}}$ satisfies the purely inseparable polynomial $t^{p^{a_i}} - \alpha_i \in K[t]$, hence the minimal polynomial $f_i \in K[t]$ of $\alpha_i^{p^{-a_i}}$ is irreducible and purely inseparable (possibly of degree 1). By Theorem 4.17, LK/K is purely inseparable.
b) We leave this as an exercise. □

EXERCISE 4.12. *Prove Lemma 4.18b).*

EXERCISE 4.13. *Let K/F be an algebraic field extension in characteristic $p > 0$, and let $\alpha \in K$. Show: the following are equivalent:*

(i) *The extension $F(\alpha)/F$ is separable.*
(ii) *We have $F(\alpha^p) = F(\alpha)$.*
(iii) *For all $n \in \mathbb{Z}^+$, we have $F(\alpha^{p^n}) = F(\alpha)$.*

In light of Exercise 4.9b), for any algebraic field extension K/F we may define the **purely inseparable closure** of F in K to be the largest subextension of K which is purely inseparable over F.

EXERCISE 4.14. *Show that the purely inseparable closure of F in an algebraic closure $\overline{F}$ is the perfect closure F^{1/p^∞}.*

COROLLARY 4.19. *Let K/F be a purely inseparable extension of finite degree.*

a) *There is $n \in \mathbb{N}$ and a finite sequence of field extensions*

$$F = F_0 \subsetneq F_1 \subsetneq \ldots \subsetneq F_n = K$$

and for all $1 \leq i \leq n$, an element $\alpha_i \in F_i \setminus F_i^p$ such that $F_i = F_{i-1}(\alpha^{1/p})$.

b) *We have $[K : F] = p^n$ for some $n \in \mathbb{N}$.*

PROOF. a) We go by induction on the degree $d := [K : F]$. The base case $d = 1$ is trivial, so suppose that $d > 1$, i.e., there is $\alpha \in K \setminus F$. By Theorem 4.17 there is $a \in \mathbb{Z}^+$ such that the minimal polynomial of α over F is $t^{p^a} - \alpha^{p^a}$. Then for all $0 \leq i \leq a-1$ we have $[F(\alpha^{p^i}) : F(\alpha^{p^{i+1}})] = p$. If $K = F(\alpha)$, we're done; otherwise, Lemma 4.18a) implies that $K/F(\alpha)$ is purely inseparable of degree less than d, so we are done by induction.
b) This is immediate from part a). □

COROLLARY 4.20. *A purely inseparable extension is normal.*

PROOF. This follows immediately from condition (i) of Theorem 4.17. □

The flavor of these results is that many formal properties are common to both separable and purely inseparable extensions. The exceptions to this rule are the following: first, purely inseparable extensions are always normal, whereas this is most certainly not the case for separable extensions. A more subtle difference is expressed in Theorem 4.17: if K/F is **not** purely inseparable, then it must have a nontrivial separable subextension. However, if K/F is **not** separable, that does not mean that it has a nontrivial purely inseparable subextension:

A purely inseparable extension K/F has **finite exponent** if there is some $a \in \mathbb{N}$ such that for all $\alpha \in K$, we have $\alpha^{p^a} \in F$, and when this holds we define the least such a as the **exponent** of K/F. Equivalently, a field extension K/F is purely inseparable of exponent $a \geq 1$ if K is contained in $F^{p^{-a}}$ and is not contained in $F^{p^{-a+1}}$. Every finite degree purely inseparable exponent has finite exponent, but there are also infinite degree purely inseparable extensions of finite exponent.

Purely inseparable extensions of exponent one are particular benign. Let K/F be a purely inseparable extension of exponent 1 and finite degree p^n. A **p-basis** for K/F is a subset S of K of size n such that $K = F(S)$. We may construct p-bases as follows: let $\alpha_1 \in K \setminus F$, so $F(\alpha_1) \cong F[t]/(t^p - \alpha_1)$ and thus $[F(\alpha_1) : F] = p$. If $F(\alpha_1) \neq K$, then choose $\alpha_2 \in K \setminus F(\alpha_1)$, so $F(\alpha_1, \alpha_2) \cong F(\alpha_1)[t]/(t^p - \alpha_2)$ and thus $[F(\alpha_1, \alpha_2) : F(\alpha_1)] = p$ and thus $[F(\alpha_1, \alpha_2) : F] = p^2$. And so forth: having chosen $\alpha_1, \ldots, \alpha_k \in K$ such that $[F(\alpha_1, \ldots, \alpha_k) : F] = p^k$ with $1 \leq k < n$, choose $\alpha_{k+1} \in K \setminus F(\alpha_1, \ldots, \alpha_k)$. Then $S := \{\alpha_1, \ldots, \alpha_n\}$ is a p-basis for K/F, and clearly every p-basis arises in this way.

EXERCISE 4.15. *Let K/F be a field extension of degree $n \in \mathbb{Z}^{\geq 2}$, and let $\Omega(n)$ be the number of prime factors of n, counted with multiplicity. Let S be a set of generators for K/F. Show: S contains a subset S' of size $\Omega(n)$ that generates K/F.*

PROPOSITION 4.21. *Let K/F be purely inseparable of exponent 1, with finite degree p^n. Then a subset S of K/F is a p-basis if and only if it is a minimal (with respect to inclusion) set of generators for K/F. In particular, the extension K/F is generated by n elements and no fewer, so it is* not *monogenic when $n \geq 2$.*

PROOF. Every p-basis for K/F is a set of generators for K/F. Let S be a set of generators for K/F. By Exercise 4.15, S contains a subset of generators of size $\Omega(p^n) = n$, so it suffices to show that no subset T of K of size at most $n-1$ generates K/F. This follows by induction from the fact that if K/F is purely inseparable of exponent 1 and $\alpha \in K$, then $[F(\alpha) : F] \mid p$. □

EXAMPLE 4.22. *Let k be a field of characteristic $p > 0$, let $n \in \mathbb{Z}^+$, let $F := k(x_1, \ldots, x_n)$ be a rational function field in n indeterminates, and let $K := k(x_1^{1/p}, \ldots, x_n^{1/p})$. Then $K \subseteq F^{1/p}$, so K/F is purely inseparable of exponent 1. We claim that $S := \{x_1^{1/p}, \ldots, x_n^{1/p}\}$ is a p-basis for K/F, so that K/F is a finite degree field extension whose minimal number of generators is n.*

Clearly $K = F(S)$, so it suffices to show that $[K : F] = p^n$. For this, we claim that $[F(x_1^{1/p}) : F] = p$ and for all $1 \leq i \leq n-1$ that $[F(x_1^{1/p}, \ldots, x_{i+1}^{1/p}) : F(x_1^{1/p}, \ldots, x_i^{1/p})] = p$. In the first case, we need to show that the polynomial $f := t^p - x_1 \in F[t]$ is irreducible, or equivalently by Lemma 4.6, has no root in F. Because $[x_1, \ldots, x_n]$ is integrally closed, any root α of f in F would lie in $k[x_1, \ldots, x_n]$, and clearly x_1 is not a pth power in $k[x_1, \ldots, x_n]$. Similarly, for $1 \leq i \leq n-1$, put $F_i := F(x_1^{1/p}, \ldots, x_i^{1/p})$. We must show $f_i := t^p - x_{i+1} \in F_i[t]$ has no root in F_i. Since F_i is the fraction field of $k[x_1^{1/p}, \ldots, x_i^{1/p}, x_{i+1}, \ldots, x_n]$, which is isomorphic to $k[x_1, \ldots, x_n]$, it is integrally closed, so a root α of f_i in F_i would lie in $k[x_1^{1/p}, \ldots, x_i^{1/p}, x_{i+1}, \ldots, x_n]$, and x_{i+1} is a pth power in this ring if and only if it is a pth power in $[x_1, \ldots, x_n]$, which is clearly not the case.

EXERCISE 4.16. *Let k be a field of characteristic $p > 0$, and let $F := k(t_1, \ldots, t_n, \ldots)$ be a rational function field of over k in a countably infinite set of indeterminates.*

a) *Show: $[F^{1/p} : F] = \aleph_0$.*
b) *Show: the minimal cardinality for a set of generators of $F^{1/p}/F$ is $\aleph_0$.*
c) *Let κ be an infinite cardinal. Show: replacing $\aleph_0$ with κ throughout this exercise, it continues to hold. Deduce: the minimum cardinality of a generating set of an algebraic field extension can be any cardinal whatsoever.*

PROPOSITION 4.23. *Let K/F be a purely inseparable algebraic extension. Then $\mathrm{Aut}(K/F)$ is the trivial group.*

PROOF. Let $\sigma \in \mathrm{Aut}(K/F)$. Let $\alpha \in K$, and let $f \in F[t]$ be the minimal polynomial of α. Then $0 = \sigma(0) = \sigma(f(\alpha)) = f(\sigma(\alpha))$. But since α is purely inseparable over F, the only root of f in $\overline{F}$ is α, so $\sigma(\alpha) = \alpha$. Thus $\sigma = 1_K$. □

EXERCISE 4.17. *Let F be a field, let $\overline{F}$ be an algebraic closure of F, and let F^{sep} be the separable closure of F in $\overline{F}$, so F^{sep} is a separable closure of F.*

a) *Show: $\overline{F}/F^{\mathrm{sep}}$ is purely inseparable.*
b) *Since $F^{\mathrm{sep}} \subseteq \overline{F}$ are both normal over F, by Proposition 3.20 restriction from $\overline{F}$ to F^{sep} gives a surjective group homomorphism*

$$r : \mathrm{Aut}(\overline{F}/F) \to \mathrm{Aut}(F^{\mathrm{sep}}/F).$$

Show: r is an isomorphism.

In Chapter 7, we define an algebraic extension K/F to be **Galois** if it is normal and separable. Thus F^{sep}/F is not only a Galois extension of F but a maximal Galois extension of F. We call $\mathfrak{g}_F := \mathrm{Aut}(F^{\mathrm{sep}}/F)$ the **absolute Galois group of F**. In general, for a field extension K/F, we call $\mathrm{Aut}(K/F)$ the "Galois group of K/F" if and only if K/F is a Galois extension. Earlier in Chapter 3 we called $\mathrm{Aut}(\overline{F}/F)$ the absolute Galois group of F. This is against our convention, but Exercise 4.17 shows that $\mathrm{Aut}(\overline{F}/F)$ is canonically isomorphic to $\mathrm{Aut}(F^{\mathrm{sep}}/F$, so we felt we could get away with it.

4. Structural Results on Algebraic Extensions

PROPOSITION 4.24. *Suppose an algebraic extension K/F is both separable and purely inseparable. Then $K = F$.*

PROOF. For such an extension, let $\alpha \in K$. Then the minimal polynomial of α over F is both separable and purely inseparable. The only such polynomials have degree one, i.e., $\alpha \in F$. □

PROPOSITION 4.25. *Let K/F be an algebraic field extension K/F. Then the extension $K/\mathrm{SepCl}_K(F)$ is purely inseparable.*

PROOF. Since $\mathrm{SepCl}_K(F)$ is the maximal separable subextension of K/F, there cannot be a proper nontrivial separable extension of $K/\mathrm{SepCl}_K(F)$. □

In general this result is not valid the other way around: an algebraic field extension K/F *need not* be separable over its purely inseparable closure. Indeed, in the example of the previous section the purely inseparable closure F_i was F and K/F was not separable. The following two results give more information on when K is separable over F_i.

THEOREM 4.26. *For an algebraic extension K/F, let F_s and F_i be, respectively, the separable and purely inseparable closures of F in K. The following are equivalent:*

(i) $K = F_sF_i$.
(ii) *K is separable over F_i.*

PROOF. (i) $\implies$ (ii): K is obtained by adjoining to F_i roots of separable polynomials with coefficients in F, hence by polynomials with coefficients in F_s.
(ii) $\implies$ (i): If K/F_i is separable, then K/F_iF_s is separable. Similarly, since K/F_s is inseparable, K/F_iF_s is inseparable. By Proposition 4.24, $K = F_iF_s$. □

COROLLARY 4.27. *The equivalent conditions of Theorem 4.26 hold when K/F is normal. In particular they hold for $\overline{F}/F$, giving $\overline{F} = F^{\mathrm{sep}}F^{1/p^\infty}$.*

PROOF. Let $\alpha \in K \setminus F_i$. The minimal polynomial $P(t) \in F_i[t]$ of α has at least one other distinct root, say β, in an algebraic closure $\overline{F}$. Snce K/F is normal, also K/F_i is normal, so we have $\beta \in K$, and the Extension Theorem (Theorem 3.21) shows that there is an element $s \in \mathrm{Aut}(K/F_i)$ such that $s(\alpha) = \beta$. This shows that the set of elements in F that are fixed by every element of $\mathrm{Aut}(K/F_i)$ is F_i.

Later on we will see that we have proved that K/F_i is a Galois extension, which implies that it is separable. For now we argue by hand: let $\alpha = \alpha_1, \ldots, \alpha_r$ be all

the F_i-conjugates of α in K, and consider the separable polynomial The

$$R(t) \coloneqq \prod_{i=1}^{r}(t-\alpha_i) \in K[t].$$

The action of $\mathrm{Aut}(K/F_i)$ on K extends to an action on $K[t]$ by

$$s(\sum_{i=0}^{n} a_i t^i) \coloneqq \sum_{i=0}^{n} s(a_i)t^i.$$

Since element $s \in \mathrm{Aut}(K/F_i)$ permutes the roots α_i of R, we have $\sigma(R) = R$, and thus every coefficient of R is fixed by every element of $\mathrm{Aut}(K/F_i)$, so $R \in F_i[t]$. It follows that $R = P$, so P is separable, and thus K/F_i is (normal and) separable.

The second sentence of the Corollary follows immediately from the first. □

REMARK 4.2. *In* [**Li66**]*, J. Lipman calls an algebraic field extnsion K/F satisfying the equivalent conditions of theorem 4.26* ***balanced*** *and gives further characterizations of them, one of which is: K/F is balanced if and only if there is a separable algebraic extension L/K such that L/F is normal.*

We will now give a family of examples of non-balanced field extensions, following `https://math.stackexchange.com/a/1276333/299`. Similar examples were given by Sury [**Su99**].

EXAMPLE 4.28. *Let p be a prime number, let k be a field of characteristic p, and let $F \coloneqq k(x,y)$ (rational function field). Let*

$$f \coloneqq t^{p^2} + xt^p + y \in F[t],$$

which is an inseparable polynomial. By Gauss's Lemma, $f \in k(x,y)[t]$ is irreducible if and only if $f \in k[x,y,t]$ is irreducible if and only if $f \in k(x,t)[y]$ is irreducible – which it is, being linear in y. Let α be a root of f in an algebraic closure $\overline{F}$ of F, and let $K \coloneqq F(\alpha)$, so K/F is inseparable of degree p^2. Put

$$g \coloneqq t^p + xt + y \in F[t],$$

so g is irreducible and separable. If the roots of g in $\overline{F}$ are $\beta_1 = \alpha^p, \beta_2, \ldots, \beta_p$, each with multiplicity 1, then the roots of f in $\overline{F}$ are $\beta_1^{1/p} = \alpha, \beta_2^{1/p}, \ldots, \beta_p^{/p}$, each with multiplicity p. Thus $F(\alpha^p)$ is a degree p separable subextension of K/F. It follows that $[K:F]_s = p$. We claim that $F(\alpha^p)$ is the unique nontrivial proper subextension of K/F, from which it follows that K/F is inseparable but has no nontrivial purely inseparable subextension. The claim implies

$$F_i F_s = FF(\alpha^p) = F(\alpha^p) \subsetneq K,$$

so K/F is not *balanced.*

Seeking a contradiction, suppose that we have a nontrivial, proper subextension $E \neq F(\alpha^p)$ of K/F, so $[E:F] = p$. Then E/F would indeed have to be purely inseparable, and then $K = E(\alpha)$ and K/E is separable, so the minimal polynomial $h \in E[t]$ of α is separable of degree p and $h \mid f \in K[t]$. It follows that the roots of h in $\overline{f}$ are $\beta_1^{1/p}, \ldots, \beta_p^{1/p}$, and thus $f = h^p \in \overline{F}[t]$, which implies $f = h^p \in E[t]$. Thus there are $u, v \in E$ with $u^p = x$, $v^p = y$ such that $h = t^p + ut + v$. But then $E \supseteq F(x^{1/p}, y^{1/p})$, while $[F(x^{1/p}, y^{1/p}) : F] = p^2$: contradiction.

COROLLARY 4.29. *For a finite degree extension K/F, we have*

$$[K:F]_s = [\mathrm{SepCl}_K(F):F] \mid [K:F].$$

PROOF. We have $[K:F]_s = [K:\mathrm{SepCl}_K(F):F]_s[\mathrm{SepCl}_K(F):F]_s$. But the separable degree of a purely inseparable extension is 1, so the conclusion follows. □

For a finite degree extension K/F one may therefore define the **inseparable degree** $[K:F]_i$ of a finite degree extension to be $[K:F]/[K:F]_s = [K:\mathrm{SepCl}_K(F)]$.

A field is **separably closed** if it admits no proper separable algebraic field extension.

PROPOSITION 4.30. *The separable closure of a field in any algebraically closed field is separably closed.*

EXERCISE 4.18. *Prove Proposition 4.30.*

One often writes F^{sep} for a separable closure of F. Like the algebraic and normal closures, this extension is unique up to non-canonical F-algebra isomorphism.

COROLLARY 4.31. *Let K/F be a separable algebraic extension, and let F_s be the separable closure of F in K. Then K/F is normal if and only if F_s/F is normal.*

PROOF. Let $\overline{F}$ be an algebraic closure of F containing K.

Suppose that K/F is normal, and let $\sigma : K \hookrightarrow \overline{F}$ be an F-algebra embedding. By normality of K/F we have $\sigma(F_s) \subseteq K$. Since $\sigma(F_s)$ is isomorphic as an F-algebra to F_s, it is also a separable extension of F, hence $\sigma(F_s) \subseteq F_s$, and applying the same argument with σ^{-1} gives $\sigma(F_s) = F_s$. Thus F_s/F is normal.

Suppose that K/F is not normal, so there is $\alpha \in K$ such that the minimal polynomial $f \in F[t]$ of α does not split in K. If f is separable, then $\alpha \in F_s$, which shows that F_s/F is not normal. If $F(\alpha)/F$ has inseparable degree $p^a > 1$, then we may write $f = g(t^{p^a})$ with $g \in F[t]$ irreducible and separable, so $\beta := \alpha^{p^a} \in F_s$ is a root of g, and if the roots of g in $\overline{F}$ are $\beta_1 = \beta, \beta_2, \ldots, \beta_m$, then the roots of f are $\beta_1^{p^{-a}}, \ldots, \beta_m^{p^{-a}}$, each occurring with multiplicity p^a. Thus for some $1 \leq i \leq m$ we have $\beta_i^{p^{-a}} \notin K$, so $\beta_i \notin F_s$, showing that F_s/F is not normal. □

EXERCISE 4.19. *Let K/F be a normal algebraic extension, and let F_s be the separable closure of F in K. By Corollary 4.31 F_s/F is normal, so by Proposition 3.20 we have a surjective restriction homomorphism $r : \mathrm{Aut}(K/F) \to \mathrm{Aut}(F^s/F)$. Show: r is an isomorphism.*

COROLLARY 4.32. *Let K/F be an algebraic field extension.*

a) *If F is perfect, then K is perfect.*

b) *If K is perfect and $[K:F]$ is finite, then F is perfect.*

PROOF. We may assume F has characteristic $p > 0$.

a) If F is perfect, then every algebraic extension of F is separable, hence every algebraic extension of every algebraic extension of F is separable, so K is perfect.

b) Suppose that F is not perfect, so there is $x \in F \setminus F^p$. Choose $n \in \mathbb{Z}^+$ such that $p^n \geq [K:F]$. By Lemma 4.6, the polynomial $t^{p^{n+1}} - x \in F[t]$ is irreducible, hence $[F(x^{p^{-n-1}}):F] = p^{n+1} > [K:F]$, so $x^{p^{-n}} \notin K$. There is therefore some $0 \leq m \leq n$ such that $x^{p^{-m}} \in K \setminus K^p$, so K is not perfect. □

Of course, every imperfect field admits an infinite degree extension that is perfect: e.g. an algebraic closure, or minimally, a perfect closure.

5. Finite Fields

Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}$ has characteristic p, so the subfield generated by 1 is the ring $\mathbb{Z}/p\mathbb{Z}$, which we here denote by $\mathbb{F}_p$. Moreover $\mathbb{F}$ is a finite-dimensional $\mathbb{F}_p$-vector space; if its dimension is n, then $\#F = p^n$. By Theorem 4.7, a field of characteristic p is perfect if and only if the Frobenius map $\mathfrak{f} : x \mapsto x^p$ is surjective. But $\mathfrak{f}$, being a field homomorphism, is always injective, and an injective map from a finite set to itself (or between two finite sets of the same size) is bijective. So finite fields are perfect, and thus also all algebraic extensions of a finite field are perfect.

We claim that for all $n \in \mathbb{Z}^+$, there is a field extension of $\mathbb{F}_p$ of degree n and that any two degree extensions of $\mathbb{F}_p$ are isomorphic (as $\mathbb{F}_p$-algebras, which is the same as being isomorphic as fields in characteristic p). One way to show that $\mathbb{F}_p$ admits a degree n extension is to show that there is a degree n irreducible polynomial $f \in \mathbb{F}_p[t]$. This is done by a Möbius Inverseion argument in [**Cl-NT**, Cor. C.9]. We will use a different argument here, but in fact, as a consequence of the Primitive Element Theorem from the next chapter, the existence of a degree n extension of $\mathbb{F}_p$ is equivalent to the existence of a degree n irreducible polynomial over $\mathbb{F}_p$, so our approach will derive this as well.

Consider the polynomial $f(t) = t^{p^n} - t \in \mathbb{F}_p[t]$. Since $f' = p^n t^{p^n - 1} - 1 = -1$, we have $\gcd(f, f') = 1$ and thus f is separable. Let F be the splitting field of f over $\mathbb{F}_p$. Because f is separable, it has p^n distinct roots in F; let us call this set of roots S. We claim that S is a subfield of F. Clearly $0, \pm 1 \in S$ (if $p = 2$ then $-1 = 1$, but no problem); if $x, y \in S$, then $(x+y)^{p^n} = x^{p^n} + y^{p^n} = x + y$, so $x + y \in S$; similarly $(xy)^{p^n} = x^{p^n} y^{p^n} = xy$, so $xy \in S$. If $x \in S \setminus \{0\}$, then because $-1 \in S$ also $-x \in S$; and $(x^{-1})^{p^n} = (x^{p^n})^{-1} = x^{-1}$, so $x^{-1} \in S$. Also $\mathbb{F}_p \subseteq S$: once again, clearly $0 \in S$; and if $x \in \mathbb{F}_p^\times$, then by Lagrange's Theorem we have $x^{p-1} = 1$, so $x^p = x$. It follows that $S = F$ *is* the splitting field of F, and thus $F/\mathbb{F}_p$ is a field extension of degree n. So indeed degree n extensions of $\mathbb{F}_p$ exist for all $n \in \mathbb{Z}^+$.

Now let $F/\mathbb{F}_p$ be any field extension of degree n. Then $\#F^\times = p^n - 1$, so for all $x \in F^\times$ we have $x^{p^n - 1} = 1$, so for all $x \in F$ we have $x^{p^n} = x$. It follows that F is the splitting field of $f = t^{p^n} - t \in \mathbb{F}_p[t]$. By Theorem 3.13b), any two degree n extensions of $\mathbb{F}_p$ are isomorphic as $\mathbb{F}_p$-algebras.

Let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$. By what we have just said, for all $n \in \mathbb{Z}^+$, there is a unique subfield of $\overline{\mathbb{F}_p}$ of order p^n, which we denote by $\mathbb{F}_{p^n}$. Let $\alpha \in \overline{\mathbb{F}_p}$. If the minimal polynomial of α over $\mathbb{F}_p$ has degree n, then $\alpha \in \mathbb{F}_{p^n}$. It follows that

$$\overline{\mathbb{F}_p} = \bigcup_{n \in \mathbb{Z}^+} \mathbb{F}_{p^n}.$$

This is a rare example of being able to construct an algebraic closure "explicitly."

To summarize: let $q = p^a$ be any prime power. We have proved that there is a finite field $\mathbb{F}_q$ of cardinality q. Moreover, $\mathbb{F}_q$ is unique in the sense that any two

finite fields of order q are isomorphic as $\mathbb{F}_p$-algebras and every algebraically closed field of characteristic p contains a unique finite field of order q. In spite of all this we are wary of speaking of **the** finite field of order q: this is because $\mathbb{F}_q$ is unique up to $\mathbb{F}_p$-algebra isomorphism but not (when $a > 1$) up to *unique* $\mathbb{F}_p$-algebra isomorphism: that is, the group $\mathrm{Aut}(\mathbb{F}_q/\mathbb{F}_p)$ is nontrivial: indeed, the Frobenius map $\mathfrak{f} : \mathbb{F}_q \to \mathbb{F}_q$ is a field automorphism of order a. In general, we tip our hat to this phenomenon by employing scare quotes: we call $\mathbb{F}_q$ "the" finite field of order q.

The preceding discussion holds almost verbatim for extensions of any finite field:

EXERCISE 4.20. *Let p be a prime number, let $a \in \mathbb{Z}^+$, and put $q := p^a$. Let $\mathbb{F}_q$ be "the" finite field of order q. Let $\overline{\mathbb{F}_q}$ be an algebraic closure of $\mathbb{F}_q$.*

a) *Let $n \in \mathbb{Z}^+$. Show: inside $\overline{\mathbb{F}_q}$ there is a unique degree n field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ and that this extension is the splitting field of $t^{q^n} - t \in \mathbb{F}_q[t]$.*

b) *Deduce: $\overline{\mathbb{F}_q} = \bigcup_{n \in \mathbb{Z}^+} \mathbb{F}_{q^n}$.*

c) *Let $a, b \in \mathbb{Z}^+$. Show: inside $\overline{\mathbb{F}_q}$, we have*

$$\mathbb{F}_{q^a} \cap \mathbb{F}_{q^b} = \mathbb{F}_{q^{\gcd(a,b)}}$$

and

$$\mathbb{F}_q^a \mathbb{F}_q^b = \mathbb{F}_{q^{\mathrm{lcm}(a,b)}}.$$

In the next chapter, we will learn that every finite degree separable field extension K/F is monogenic: $K = F(\alpha)$ for some $\alpha \in F$. (Recall that such an α is called a primitive element for K/F.) In particular this applies to $\mathbb{F}_{q^n}/\mathbb{F}_q$. The main part of the argument applies only when the field F is infinite. Fortunately, for finite fields, there is a much more elementary proof that we give in the following exercise and explore some of its consequences.

EXERCISE 4.21.

a) *Show: the multiplicative group $\mathbb{F}_{q^n}^\times$ is cyclic.*
(Hint: Use that a noncyclic finite commutative group G has at least p^2 elements of order p for some prime $p \mid \#G$.)

b) *Show: if u generates $\mathbb{F}_{q^n}^\times$, then $\mathbb{F}_{q^n} = \mathbb{F}_q(u)$.*

c) *Show: the number of primitive elements for $\mathbb{F}_{q^n}/\mathbb{F}_q$ is $\sum_{d|n} q^d \mu(\frac{n}{d})$, where μ is the Möbius function. Also show: the number of generators for $\mathbb{F}_{q^n}^\times$ is $\varphi(q^n - 1)$, where φ is Euler's totient function.*

d) *Show: if $2^n - 1$ is prime – that is, a **Mersenne prime** – then every primitive element of $\mathbb{F}_{2^n}/\mathbb{F}_2$ is a generator of $\mathbb{F}_{2^n}^\times$.*
(For $2^n - 1$ to be prime, n must be prime. The first few n such that $2^n - 1$ is prime are 2, 3, 5, 7, 13, 17, 19, 31. It is believed that there are infinitely many Mersenne primes.)

e) *Let p be a prime number such that $2^p - 1$ is* not *prime. Show: not every primitive element of $\mathbb{F}_{2^p}/\mathbb{F}_2$ is a generator of $\mathbb{F}_{2^p}^\times$.*

f) *Let $n = 2$ and $q \geq 3$.*
- *Show: if q is odd, then*

$$\varphi(q^2 - 1) \leq \frac{q^2 - 1}{2} < q^2 - q,$$

- *Show: if q is even, then*

$$\varphi(q^2 - 1) \leq q^2 - 2q < q^2 - q.$$

Deduce: not every primitive element for $\mathbb{F}_{q^2}/\mathbb{F}_q$ is a generator for $\mathbb{F}_{q^2}^\times$.

EXERCISE 4.22. *Let F be a field in which every finite degree separable extension is normal.*

a) *Show: if K/F is a separable algebraic extension, then K/F is normal.*
b) *Show: if F is perfect and K/F is an algebraic extension, then every algebraic extension L/F is normal.*
c) *Deduce: every algebraic extension of a finite field is normal.*

CHAPTER 5

The Primitive Element Theorems

1. The Primitive Element Theorems

For some people, the "Primitive Element Theorem" is the assertion that every finite degree separable field extension is monogenic. However, there are two different stronger results that imply this result. The first Theorem, that we call **Primitive Element I**, is due to Steinitz [**St10**] and characterizes monogenic extensions among finite degree field extensions as those whose subfield lattice is finite. The second, that we call **Primitive Element II** and that we found in van der Waerden's classic text [**vdW**, §6.8] asserts that a finite degree extension generated by a finite set of elements *all but one of which* is separable must be monogenic. Each of these implies the monogenicty of finite degree separable extensions, which here we call the **Primitive Element Corollary**.

THEOREM 5.1 (Primitive Element I). *Let K/F be a finite degree field extension. The following are equivalent:*

(i) *The set of subextensions L of K/F is finite.*
(ii) *K/F is monogenic: there is $\alpha \in K$ such that $K = F[\alpha]$.*

PROOF. [**La**, pp. 243-244] Suppose first that $K = \mathbb{F}_q$ is finite. Then (i) is clear, while (ii) holds because $K^\times$ is cyclic of order $q-1$: if α is a generator of the group $K^\times$, then $K = F[\alpha]$. Henceforth we suppose that K is infinite.
(i) $\implies$ (ii): observe that for any subextension E of K/F, since (i) holds for K/F, it also holds for E/F. Writing $K = F[\alpha_1, \ldots, \alpha_n]$, we see that it is enough to prove the result in the case of extensions which are generated by two elements: a simple induction argument then recovers the general case.

So suppose that $K = F[\alpha, \beta]$. As c ranges over the infinitely many elements of F, there are only finitely many distinct subfields of K of the form $F[\alpha + c\beta]$, so there exist distinct elements c_1, c_2 of F such that

$$E = F[\alpha + c_1\beta] = F[\alpha + c_2\beta].$$

It then follows, successively, that $(c_1 - c_2)\beta \in E$, $\beta \in E$, $\alpha \in E$, so

$$F[\alpha + c_1\beta] = E = F[\alpha, \beta] = K.$$

(ii) $\implies$ (i): Suppose $K = F[\alpha]$, and let $f(t) \in F[t]$ be the minimal polynomial for α over F. For each subextension E of K/F, let $g_E(t) \in E[t]$ be the minimal polynomial for α over E. Let E' be the subextension of K/F generated by the coefficients of g_E. So $F \subset E' \subset E \subset K$; since g_E is irreducible over E, it is also irreducible over E', and thus $[K : E'] = [E'[\alpha] : E'] = [E[\alpha] : E] = [K : E]$. It follows that $E = E'$. In other words, E can be recovered from g_E and thus the map $E \mapsto g_E$ is injective. Let $\overline{F}$ be an algebraic closure of F. Then $g_E \mid f$ in $E[t]$ hence

also in $\overline{F}[t]$. Since $\overline{F}[t]$ is a UFD, there are only finitely many possibilities for g_E, hence only finitely many subextensions E. □

THEOREM 5.2 (Primitive Element II). *Let F be an infinite field with algebraic closure $\overline{F}$. Let $\alpha, \beta_1, \ldots, \beta_n \in \overline{F}$ with $\beta_1, \ldots, \beta_n$ separable over F. Then:*

a) *The extension K/F is monogenic.*
b) *More precisely, let $n \in \mathbb{Z}^+$, and let $S \subseteq F^\times$ be an infinite set. Then there are $s_1, \ldots, s_n \in S$ such that $K = F(\alpha + s_1\beta_1 + \ldots + s_n\beta_n)$.*

PROOF. Clearly it is sufficient to prove part b). We go by induction on n.
Step 1: Suppose $n = 1$. Then we must show that for $\alpha, \beta \in \overline{F}$ with β separable, there is $s \in S$ such that $F(\alpha, \beta) = F(\alpha + s\beta)$.

Let $f \in F[t]$ be the minimal polynomial of α, and let the distinct roots of f in $\overline{F}$ be $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$. Let $g \in F[t]$ be the (separable) minimal polynomial of β, and let the roots of g in $\overline{F}$ be $\beta_1 = \beta, \beta_2, \ldots, \beta_s$. For all $1 \leq i \leq r$ and $2 \leq k \leq s$ the linear equation $\alpha_i + \beta_k t = \alpha_1 + \beta_1 t$ has at most one root in F. Since S is infinite, there is $s \in S$ that is not a root of any of the above linear equations. Put

$$\theta := \alpha_1 + s\beta_1.$$

By construction, the only common root of the polynomials $g(t)$ and $f(\theta - st)$ in $\overline{F}$ is β_1. Since g is separable, the greatest common divisor of f and g in $\overline{F}[t]$ is $(t - \beta_1)$. Since g and $f(\theta - st)$ lie in $F(\theta)[t]$, by Lemma 4.1 we have $t - \beta_1 \in F(\theta)[t]$, so $\beta = \beta_1 \in F(\theta) = F(\alpha + s\beta)$, hence also $\alpha \in F(\theta)$, so $F(\theta) = F(\alpha, \beta)$.
Step 2: Let $n \in \mathbb{Z}^+$, suppose the conclusion of part b) holds for n, and let $\alpha \in \overline{F}$ and $\beta_1, \ldots, \beta_n, \beta_{n+1} \in \overline{F}$ be separable over F. By our induction hypothesis there are $s_1, \ldots, s_n \in S$ such that $F(\alpha, \beta_1, \ldots, \beta_n) = F(\alpha + \sum_{i=1}^n s_i\beta_i)$. Applying Step 1 with $\alpha := \sum_{i=1}^n s_i\beta_i$ and $\beta := \beta_{n+1}$, we get $s_{n+1} \in S$ such that

$$F(\alpha, \beta_1, \ldots, \beta_n, \beta_{n+1}) = F(\alpha + \sum_{i=1}^n s_i\beta_i, \beta_{n+1}) = F(\alpha + \sum_{i=1}^{n+1} s_i\beta_i). \qquad \square$$

REMARK 5.1. *In Theorem 5.2 the hypothesis that F be infinite is not essential: we already proved in Chapter 4 that every finite degree extension of a finite field is monogenic. Nevertheless one can ask for a proof of Theorem 5.2 in which finite fields need not be excluded. This was done by Sonn–Zassenhaus* [**SZ67**].

COROLLARY 5.3 (Primitive Element Corollary). *A finite degree separable field extension is monogenic.*

Corollary 5.3 is an immediate consequence of Primitive Element II. Once we develop the Galois correspondence, it will become an immediate consequence of Primitive Element I: if K/F is finite degree separable, with normal closure L, then L/F is a finite Galois extension, so subextensions of L/F are in bijective correspondence with subgroups of the group $\mathrm{Aut}(L/K)$, which has finite order $[L : F]$. Thus there are only finitely many subextensions of L/F, hence also only finitely many subextensions of K/F.

EXERCISE 5.1. *Let L/F be a finite degree monogenic field extension. Show: every subextension M of L/F is also monogenic.*

In fact Exercise 5.1 remains true even without the hypothesis that L/F has finite degree. This is the content of a later result, Theorem 10.4.

COROLLARY 5.4. *(Lang) Let K/F be a separable algebraic extension such that: there is $n \in \mathbb{Z}^+$ such that for all $\alpha \in K$, $[F(\alpha) : F] \leq n$. Then $[K : F] \leq n$.*

PROOF. Let $\alpha \in K$ be such that $[F(\alpha) : F]$ has maximal degree – it is no loss of generality to assume that this degree is n. We claim that $K = F(\alpha)$, which will establish the result.

Suppose that $K \supsetneq F(\alpha)$, and let $\beta \in K \setminus F(\alpha)$. Since $F(\alpha, \beta)/F$ is finite separable, by the Primitive Element Corollary (Corollary 5.3) there is $\gamma \in K$ such that $F(\alpha, \beta) = F(\gamma)$. But then we must have $[F(\gamma) : F] > [F(\alpha) : F]$, contradiction. □

In Corollary 5.4, if we remove the hypothesis that K/F is separable then the conclusion need not hold. Indeed, if K/F is purely inseparable of exponent 1, then for all $\alpha \in K$ we have $[F(\alpha) : F] \leq p$, but as we saw in §4.3, we need not have $[K : F] \leq p$.

COROLLARY 5.5. *Let k be a field of characteristic $p > 0$, let $n \in \mathbb{Z}^{\geq 2}$, let $F := k(t_1, \ldots, t_n)$ (rational function field) and let $K := k(t_1^{1/p}, \ldots, t_n^{1/p})$. Then K/F has finite degree p^n but infinitely many proper subextensions.*

PROOF. By Example 4.22, the extension K/F is not monogenic (indeed it is minimally generated by n elements), so by Primitive Element I there are infinitely many subextensions of K/F. □

For me, the existence of a finite degree field extension with infinitely many subextensions is the most startling result in this text and, in fact, one of the most counterintuitive mathematical results I have met in my adult mathematical life. (I received my PhD in mathematics blissfully ignorant of the fact that such field extensions existed. Rather I thought that standard results ruled these out, as is true in characteristic 0.) Thus we find that the subfield lattice of a finite degree field extension, though both Noetherian and Artinian – i.e., satisfying both the ascending and descending chain conditions – may be infinite.

Let K/F be a finite degree field extension, and let $\mathcal{L}(K/F)$ be the lattice of subextensions L of K/F. We can give bounds on the size of $\mathcal{K}(K/F)$ in terms of $[K : F]$ and the characteristic of K. First a crude bound in the case that $\mathcal{L}(K/F)$ is finite:

COROLLARY 5.6. *Let K/F be a monogenic field extension of finite degree n. Then the number $\#\mathcal{L}(K/F)$ of subextensions of K/F is at most 2^{n-1}.*

PROOF. Let $K = F(\alpha)$ and let $f \in F[t]$ be the minimal polynomial of α. For $E \in \mathcal{L}(K/F)$, let $g_E \in E[t]$ be the minimal polynomial of α. Again, the proof of Primitive Element I shows that the mapping $E \mapsto g_E$ is injective. In an algebraic closure $\overline{F}$ of F, we factor f as $\prod_{i=1}^n (t - \alpha_i)$ with $\alpha_1 = \alpha$. Then in $\overline{F}[t]$ we have $t - \alpha_1 \mid g_E \mid f$, hence

$$g_E \mid \prod_{i=2}^n (t - \alpha_i).$$

Since g is monic and $\overline{F}[t]$ is a UFD, there are at most 2^{n-1} choices for g_E. □

By Corollary 5.3, $\mathcal{L}(K/F)$ can only be infinite if F has characteristic $p > 0$ K/F is inseparable, hence only if $p \mid [K : F]$. Suppose that K has characteristic $p > 0$, that L/K is inseparable but $p^2 \nmid [L : K]$. Let F_s be the separable closure of K in L. Then K/F_s is purely inseparable so must be of degree p, so there is $\beta \in K/F_s$

such that $K = F_s(\beta)$. Let α be a generator for the separable extension F_s/F. Then $K = F(\alpha, \beta)$, so by Primitive Element II followed by Primitive Element I, the lattice $\mathcal{L}(K/F)$ is finite.

EXERCISE 5.2. *In characterstic $p > 0$, let K/F be a finite degree extension of inseparable degree p. Show: K/F is monogenic.*

EXERCISE 5.3. *Let p be a prime number, and let $n \in \mathbb{Z}^+$ with $p^2 \mid n$. Show: there is a field extension K/F of characteristic p and finite degree n such that the lattice $\mathcal{L}(K/F)$ of subextensions is infinite.*

PROPOSITION 5.7. *Let K/F be a monogenic purely inseparable field extension of degree p^a. Then for all $0 \leq i \leq a$ there is a unique subextension L_i of K/F with $[L_i : F] = p^i$. Thus $\mathcal{L}(K/F)$ is a finite chain of length a.*

PROOF. We may write $K = F(\alpha)$, where the minimal polynomial $f \in F[t]$ of α is irreducible and purely inseparable, hence of the form $t^{p^a} - \alpha^{p^a}$. For $0 \leq i \leq a$, put $F_i := F(\alpha^{p^{a-i}})$, so F_i is a subextension of K/F of degree p^i and we have $F_i \subseteq F_{i+1}$ for all $0 \leq i \leq a-1$. It remains to show that there are no other subextensions of K/F. Following the proof of Primitive Element I, let E be a subextension of K/F, and let $g_E \in E[t]$ be the minimal polynomial of α. Then $g_E \mid f$, so in an algebraic closure $\overline{F}$ of F we have that $g_E = (t-\alpha)^j$ for some $0 \leq j \leq p^a$. Since $K = E(\alpha)$, we have $j = \deg g_E = [K : E] \mid [K : F] = p^a$, so $g_E = (t-\alpha)^{p^i}$ for some $0 \leq i \leq a$. Thus there are at most $a+1$ possibilities for g_E, hence by the proof of Primitive Element I there are at most $a+1$ subextensions of K/F. □

EXAMPLE 5.8. *Let p be a prime number. We consider the possible sizes of $\mathcal{L}(K/F)$ as K/F ranges over field extensions of degree p^2.*
Case 1: Suppose that K/F is purely inseparable of exponent p^2. Then it is monogenic, so $\#\mathcal{L}(K/F) = 3$ by Proposition 5.7.
Case 2: Suppose that K/F is purely inseparable of exponent 1. By Proposition 4.21 K/F is not monogenic, so $\mathcal{L}(K/F)$ is infinite. It can actually be shown that in this case $\#\mathcal{L}(K/F)$ can be any infinite cardinal, but we will not do so here.
Case 3: Suppose that K/F has separable degree p, hence inseparable degree p. By Exercise 5.2, K/F is monogenic, so $\mathcal{L}(K/F)$ is finite. The separable closure F_s of F has degree p over F so is a nontrivial, proper subextension of K/F.
Case 3a: Suppose K/F is balanced, i.e., is the compositum of F_s with F_i, the purely inseparable closure of F in K. Then $[F_i : F] = p$, so F_s and F_i are two proper nontrivial subextensions of K/F. We cannot have any more: two separable subextensions of degree p over F would make K/F separable, and two inseparable extensions of degree p (hence purely inseparable) would make K/F purely inseparable. Thus in this case $\#\mathcal{L}(K/F) = 4$. This can actually occur: let k be any field of characteristic p, and let $F := k(t)$. Later we will show (cf. Exercise 8.34) that there is a separable extension $F(\alpha)/F$ of degree p. Then we can take $K := F(\alpha, t^{1/p})$.
Case 3b: Suppose that K/F is not balanced: equivalently, $F_i = F$. Then we cannot have another separable extension, for the same reasons above, and we cannot have a purely inseparable extension, since that would make $F_i \supsetneq F$. Thus in this case $\#\mathcal{L}(K/F) = 3$. Example 4.28 shows that this case actually occurs.
Case 4: Suppose K/F is separable, hence $K = F(\alpha)$ for some α in K an $\mathcal{L}(K/F)$ is finite. We will show that $\#\mathcal{L}(K/F) \leq \binom{p^2-1}{p-1} + 2$. Let E be a proper, nontrivial subextension of K/F, so $[E : F] = p$. Let $g_E \in E[t]$ be the minimal polynomial of

α; then $\deg g_E = [K : E] = p$. *One of the factors of g_E in an algebraic closure $\overline{F}$ is $(t - \alpha)$, so the remaining $p - 1$ linear factors are obtained by choosing $p - 1$ of the remaining $p^2 - 1$ roots of the minimal polynomial of α. This shows that there are at most $\binom{p^2-1}{p-1}$ choices for E, and adding 2 for the subextensions F and K gives the above bound.*

When $p = 2$, this bound can be attained: F does not have characteristic 2 and $a, b \in F^\times$ map to distinct nontrivial elements of $F^\times/F^{\times 2}$, then $F(\sqrt{a}, \sqrt{b})/F$ is a degree 4 extension with quadratic subfields $F(\sqrt{a})$, $F(\sqrt{b})$ and $F(\sqrt{ab})$. Over $F = \mathbb{Q}$ one may take $a = 2$ and $b = 3$, for instance. When F has charactersitic 2 there is an Artin–Schreier analogue of this, so that for instance one can take $F = k(t)$ for any field k of characteristic 2. When $p \geq 3$, this bound can be improved.

2. Gilmer's Theorem

We can now prove a result of Gilmer that we stated in Chapter 3.

THEOREM 5.9. *(Gilmer [**Gi68**]) Let K/F be a field extension. If every nonconstant $f \in F[t]$ has a root in K, then every nonconstant $f \in F[t]$ splits in $K[t]$.*

PROOF. Since every nonconstant polynomial is a product of irreducible polynomials, it suffices to assume that every irreducible $f \in F[t]$ splits in K.
Step 1: Suppose that f is separable, and let $\alpha_1, \ldots, \alpha_n$ be its roots in an algebraic closure of K. Then the extension $F(\alpha_1, \ldots, \alpha_n)/F$ is separable of finite degree, so by the Primitive Element Corollary there is $\theta \in F(\alpha_1, \ldots, \alpha_n)$ such that $F(\alpha_1, \ldots, \alpha_n) = F(\theta)$. Let $g \in F[t]$ be the minimal polynomial of θ. By assumption, g has a root $\varphi \in K$. Each of the F-algebras $F(\theta)$ and $F(\varphi)$ is isomorphic to $F[t]/(g)$, so $F(\theta)$ and $F(\varphi)$ are isomorphic F-algebras, and thus $F(\varphi)$ is also a splitting field for g, so g splits in $K[t]$.
Step 2: After Step 1 we may assume that F has characteristic $p > 0$. Let F_i be the purely inseparable closure of F in K. We claim that F_i is perfect: let $x \in F_i$. Then there is $a \in \mathbb{Z}^+$ such that $x^{p^a} \in F$. By hypothesis, the polynomial $t^{p^{a+1}} - x^{p^a} \in F[t]$ has a root y in K. Then $(y^p - x)^{p^a} = y^{p^{a+1}} - x^{p^a} = 0$, so $y^p = x$ and thus $y \in F_i$.
Step 3: Let $f \in F_i[t]$ be nonconstant. There is $a \in \mathbb{Z}^+$ such that $f^{p^a} \in F[t]$, so f has a root in K. By Step 2, the field F_i is perfect hence every irreducible $f \in F_i[t]$ is separable, so Step 1 shows that every nonconstant polynomial $f \in F_i[t]$ splits in $K[t]$. In particular, every nonconstant polynomial $f \in F[t]$ splits in $K[t]$. □

As we showed in Chapter 3, this has the following consequence: if L/K is a field extension such that every nonconstant $f \in K[t]$ has a root in L, then L contains an algebraic closure of K.

3. Isaacs's Theorem

For a field extension L/F, let $\mathcal{P}_F(L)$ be the set of all positive degree polynomials $f \in F[t]$ that have a root in L.

Let L_1/F and L_2/F be two field extensions. If there is an F-algebra embedding $\iota : L_1 \hookrightarrow L_2$, then $\mathcal{P}_F(L_1) \subseteq \mathcal{P}_F(L_2)$: indeed, for all $f \in F[t]$, if α is a root of f in L_1, then $\iota(\alpha)$ is a root of f in L_2. What about the converse?

It cannot be true in general: e.g. consider the two extensions $\overline{\mathbb{Q}}$ and $\mathbb{C}$ of $\mathbb{Q}$.

Since $\overline{\mathbb{Q}}$ and $\mathbb{C}$ are algebraically closed, both sets $\mathcal{P}_{\mathbb{Q}}(\overline{\mathbb{Q}})$ and $\mathcal{P}_{\mathbb{Q}}(\mathbb{C})$ are equal to the set of all positive degree polynomials in $\mathbb{Q}[t]$, so they are equal. We may embed $\overline{\mathbb{Q}}$ in $\mathbb{C}$ – indeed, it is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ – but because $\overline{\mathbb{Q}}$ is countable and $\mathbb{C}$ is uncountbably infinite, we cannot embed $\mathbb{C}$ in $\overline{\mathbb{Q}}$.

However, Isaacs [**Is80**] showed that the converse does hold if L_1/F is algebraic:

THEOREM 5.10 (Isaacs). *Let L/F be an algebraic field extension, and let M/F be a field extension. If $\mathcal{P}_F(L) \subseteq \mathcal{P}_F(M)$, there is an F-algebra embedding $\iota : L \hookrightarrow M$.*

We will prove this theorem shortly, but first let us deduce some consequences.

COROLLARY 5.11. *Let L_1/F and L_2/F be two algebraic field extensions. If $\mathcal{P}_F(L_1) = \mathcal{P}_F(L_2)$, then L_1 and L_2 are isomorphic as F-algebras.*

PROOF. Applying Theorem 5.10 with $L \coloneqq L_1$ and $M \coloneqq L_2$, we get an F-algebra homomorphism $\iota : L_1 \hookrightarrow L_2$, and applying it with $K \coloneqq L_2$ and $M \coloneqq L_1$, we get an F-algebra homomorphism $\iota' : L_2 \to L_1$. Then $\iota \circ \iota' : L_2 \to L_2$ is an F-algebra homomorphism, which by Lemma 3.14 is surjective. Therefore ι is surjective, so $\iota : L_1 \to L_2$ is an F-algebra isomorphism. □

The case of Corollary 5.11 in which L_1/F and L_2/F are both normal extensions follows from Theorem 3.13. The general case is a deeper result.

Now let L/F be a field extension such that every nonconstant $f \in F[t]$ has a root in L, let L_1 be the algebraic closure of F in L, and let L_2 be an algebraic closure of F. Then $\mathcal{P}_F(L_1) = \mathcal{P}_F(L_2)$, so Corollary 5.11 gives $L_1 \cong L_2$, and thus K contains an algebraic closure of F. In particular, every nonconstant $f \in F[t]$ splits in L: Gilmer's Theorem.

We now begin the proof of Isaacs's Theorem.

THEOREM 5.12. *Let L/F be an algebraic field extension, and let M/F be a field extension. Suppose that for every subextension K of L/F such that K/F has finite degree, there is an F-algebra embedding of K into M. Then there is an F-algebra embedding of L into M.*

PROOF. Let $\mathcal{S}$ be the set of pairs (K, σ) such that K is a subextension of K/F and $\sigma : K \hookrightarrow M$ is an F-algebra homomorphism. We endow $\mathcal{S}$ with a partial ordering $\preceq$ in which $(K_1, \iota_1) \preceq (K_2, \iota_2)$ if $K_1 \subseteq K_2$ and $(\iota_2)|_{K_1} = \iota_1$. It is easy to see that every nonempty chain in $\mathcal{S}$ has a supremum in $\mathcal{S}$ (Exercise 5.4).

An **FE-pair (or finitely extendable pair)** is an element $(K, \iota) \in \mathcal{S}$ such that for every subextension K' of L/K with K'/K of finite degree, then there is an $(K', \iota') \in \mathcal{S}$ with $(K, \iota) \preceq (K', \iota')$. Thus by hypothesis, $(F, 1_F)$ is an FE-pair. Let $\mathcal{E}$ be the subset of FE-pairs, endowed with the partial ordering it receives as a subset of $\mathcal{S}$. The plan of attack is to first to use Zorn's Lemma to show that $\mathcal{E}$ has maximal elements and second to show that any maximal element of $\mathcal{E}$ is an F-algebra embedding of L into M.

Step 1: We show that every (nonempty is sufficient, since $\mathcal{E} \neq \varnothing$) chain in $\mathcal{E}$ has an upper bound in $\mathcal{E}$. Let $\mathcal{C}$ be a nonempty chain in $\mathcal{E}$. Then $\mathcal{C}$ has a supremum (K, ι) in $\mathcal{S}$. It suffices to show that (K, ι) is an FE-pair.

Let K_1 be a finite degree subextension of L/K, so we may write $K_1 = K(S)$ for a finite set S. Then $F(S)/F$ is a finite degree extension, and since $(F, 1_F)$ is an FE-pair, the set $\Omega := \mathrm{Hom}_F(F(S), M)$ of F-algebra homomorphisms from $F(S)$ to M is nonempty and finite.

Seeking a contradiction, we suppose that for all $\omega \in \Omega$ there is $(F_\omega, \iota_\omega) \in \mathcal{C}$ such that no extension of ι_ω to $F_\omega(S)$ is also an extension of ω. Since $\mathcal{C}$ is a chain and Ω is finite, there is $(E, \iota) \in \mathcal{C}$ such that $(F_\omega, \iota_\omega) \le (E, \iota)$ for all $\omega \in \Omega$. Since (E, ι) is an FE-pair, ι extends to an F-algebra homomorphism $\theta : E(S) \hookrightarrow M$, and the restriction of θ to $F(S)$ is an element $\omega \in \Omega$, and thus the restriction of θ to $F_\omega(S)$ extends both ι_ω and ω: contradiction. Thus there is $\omega \in \Omega$ such that for every $(F_i, \iota_i) \in \mathcal{C}$, there is $(F_i(S), \theta_i) \in \mathcal{S}$ such that θ_i extends both ω and ι_i. Since $F_i(S)/F$ is generated by F_i and S, the map θ_i is uniquely determined by these conditions, so $(F_i, \iota_i) \preceq (F_j, \iota_j) \implies (F_i(S), \theta_i) \preceq (F_j(S), \theta_j)$, and by Exercise 5.4 there is a unique F-algebra homomorphism $\theta : K(S) \hookrightarrow M$ that restricts to θ_i on each $F_i(S)$. Thus $(K(S), \theta) \in \mathcal{S}$ and $(K, \iota) \preceq (K(S), \theta)$.

Step 2: By Step 1 and Zorn's Lemma, there is a maximal element (U, φ) in $\mathcal{E}$. Seeking a contradiction, we suppose that there is $\alpha \in L \setminus U$. Let Λ be the set of extensions of φ to $U(\alpha)$, so Λ is nonempty and finite. By the maximality of (U, φ), for no $\lambda \in \Lambda$ is $(U(\alpha), \lambda)$ an FE-pair. In other words, for each $\lambda \in \Lambda$ there is a finite degree subextension E_λ of $L/U(\alpha)$ such that λ does not extend to E_λ. Let E be the compositum $\bigvee_{\lambda \in \Lambda} E_\lambda$, so E/U is a finite degree field extension. Since (U, φ) is an FE-pair, there is an F-algebra homomorphism $\theta : E \hookrightarrow M$ extending U. Then $\theta|_{U(\alpha)} = \lambda$ for some $\lambda \in \Lambda$, so $\theta|_{E(\lambda)}$ is an extension of λ to E_λ: contradiction. Thus $U = L$, and $\varphi : L \hookrightarrow M$ is an F-algebra embedding, completing the proof. □

EXERCISE 5.4. *In the notation of the proof of Theorem 5.12, show: every nonempty chain in $\mathcal{S}$ has a supremum in $\mathcal{S}$.*

To complete the proof of Theorem 5.10, we need the following linear algebra fact:

PROPOSITION 5.13. *A vector space over an infinite field is not a finite union of proper linear subspaces.*

In fact, we will only need this result in the finite-dimensional case, in which case it can be proved in a single paragraph. Indeed, Theorem 5.14 below immediately implies this result, and its proof is a single paragraph. However, this fact raises a natural question: for any vector space V over a field F, what is the minimal number of proper linear subspaces needed to cover F? Answers to this question were given by Khare [**Kh09**] and independently by the present author [**Cl12**]. Since the full story takes less than two pages, we cannot resist including it here.

Let F be a field, and let V be a vector space over F. A **line** in V is a linear subspace of dimension one, while a **hyperplane** in V is a linear subspace W of V of codimension one: that is, $\dim_F V/W = 1$. A **linear covering** of V is a set $\mathcal{C}$ of proper F-linear subspaces of V such that $\bigcup_{W \in \mathcal{C}} W = V$. If $\dim V \le 1$, then V admits no linear covering, while if $\dim V \ge 2$, then the set of all hyperplanes in V is a linear covering. For a vector space V of dimension at least 2, the **linear covering number** $\mathrm{LC}(V)$ is the minimum cardinality of a linear covering of V.

Suppose $\dim V = 2$. Then every proper nontrivial linear subspace is both a line and a hyperplane, and since every element of $V \setminus \{0\}$ lies on a unique line, then the

set $\mathcal{L}$ of all lines in V is the unique linear covering of V. Choosing a basis, we may identify V with F^2, in which case every line other than the vertical line $x = 0$ is of the form $y = mx$ for a unique $m \in F$, so $\#\mathcal{L} = \#F + 1$.

If V and W are F-vector spaces with $\dim V \geq \dim W \geq 2$, then there is a surjective linear map $\pi : V \to W$, and then if $\mathcal{C}$ is a linear covering of W, then $\pi^{-1}(\mathcal{C})$ is a linear covering of V, so

$$\mathrm{LC}(V) \leq \mathrm{LC}(W) \leq \mathrm{LC}(F^2) = \#F + 1.$$

EXERCISE 5.5. *Let F be a field; let V be an F-vector space of dimension $2 \leq d < \aleph_0$.*

a) *Suppose that F is infinite. Show: the set of all linear subspaces of F and the set of all hyperplanes in F each have cardinality $\#F = \#F + 1$.*
b) *Suppose that $F = \mathbb{F}_q$ is finite. Show: the set of hyperplanes in F has cardinality $\frac{q^d-1}{q-1} = q^{d-1} + \ldots + q + 1 \geq \#F + 1$.*

THEOREM 5.14. *Let F be a field, and let V be an F-vector space of dimension $2 \leq d < \aleph_0$. Then*

$$\mathrm{LC}(V) = \#F + 1.$$

PROOF. As above, the upper bound $\mathrm{LC}(V) \leq \#F + 1$ holds for any vector space V of dimension at least 2. We will prove the converse by induction on d. The base case, $d = 2$, has already been established, so suppose that $d \geq 3$ an that every vector space of dimension $d - 1$ has linear covering number $\#F + 1$. Let $\mathcal{C}$ be a linear covering of V. By replacing every element W of $\mathcal{C}$ by a hyperplane $W \subseteq H \subsetneq V$, we get a linear covering of V by hyperplanes of equal or smaller size, so we may assume that every element of $\mathcal{C}$ is a hyperplane. Seeking a contradiction, we suppose that $\#\mathcal{C} < \#F + 1$, so by Exercise 5.5 there is a hyperplane H in V that is not an element of $\mathcal{C}$. Then $\mathcal{C}_H \coloneqq \{W \cap H \mid W \in \mathcal{C}\}$ is a linear covering of the $d-1$-dimensional F-vector space H of size less than $\#F + 1$, contradicting our inductive hypothesis. □

A linear covering $\mathcal{C}$ of a vector space V is **irredundant** if for all $W \in \mathcal{C}$, the set $\mathcal{C} \setminus \{W\}$ is no longer a linear covering of V. Clearly any *finite* linear covering contains an irredundant linear covering, since we can only remove redundant elements finitely many times. This shows that every linear covering of $\mathbb{F}_q^d$ of size $\mathrm{LC}(\mathbb{F}_q^d) = q + 1$ must be irredundant. This bolsters our intuition that irredundant linear coverings ought to be more efficient. But as we will now see, this is not the case for infinite-dimensional vector spaces over an infinite field.

THEOREM 5.15. *Let V be an F-vector space, and let $\mathcal{C}$ be an irredundant linear covering of V. Then $\#\mathcal{C} \geq \#F + 1$.*

PROOF. Let $\mathcal{C}$ be an irredundant linear covering of V, and let $W \in \mathcal{C}$. By irredundancy, there is $u \in W$ that does not lie in any other element of $\mathcal{C}$. Let $v \in V \setminus W$, and consider $\ell \coloneqq \{tu + v \mid t \in F\}$. We have $\#\ell = \#F$ and moreover $\ell \cap W = \varnothing$: indeed, if for some $t \in F$ we had $w \coloneqq tu + v \in W$, then $v = w - tu \in W$, a contradiction. If for some element $W' \neq W$ of $\mathcal{C}$ we had $\#(\ell \cap W') \geq 2$, then ℓ would be contained in W' and thus $v = 0 \cdot u + v \in W'$, a contradiction. So ℓ has at most one point in each element of $\mathcal{C} \setminus \{W\}$, but every element of ℓ lies in some point of $\mathcal{C} \setminus \{W\}$, so $\#(\mathcal{C} \setminus \{W\})) \geq \#F$ and thus $\#\mathcal{C} \geq \#F + 1$. □

THEOREM 5.16. *Let F be a field, and let V be an F-vector space of dimension at least 2.*

a) *If one of F and $\dim V$ is finite, then $\mathrm{LC}(V) = \#F + 1$.*
b) *If F and $\dim V$ are both infinite, then $\mathrm{LC}(V) = \aleph_0$.*

PROOF. a) If $\dim V$ is finite, this is Theorem 5.14. If F is finite and $\dim F$ is infinite, then $\mathrm{LC}(V) \leq \#F + 1 < \aleph_0$, so any linear covering of size $\mathrm{LC}(V)$ is irredundant. Now Theorem 5.15 givs $\mathrm{LC}(V) \geq \#F + 1$, so $\mathrm{LC}(V) = \#F + 1$.
b) Supose that F and $\dim V$ are both infinite. Chose an F-basis $\mathcal{B}$ for V and an injection $\iota : \mathbb{Z}^+ \to \mathcal{B}$; for $n \in \mathbb{Z}^+$, put $b_n := \iota(n)$. Let W_0 be the F-span of $\mathcal{B} \setminus \{b_n \mid n \in \mathbb{Z}^+\}$, and for $n \in \mathbb{Z}^+$, let W_n be the F-span of W_0 and $b_1, \ldots, b_n$. Every $v \in V$ is of the form $\alpha_0 w_0 + \sum_{n=1}^{\infty} \alpha_n b_n$ with $w_0 \in W_0$ and $\alpha_n \in F$ for all $n \in \mathbb{N}$ with $\alpha_n = 0$ for all but finitely many $n \in \mathbb{N}$, so v lies in W_n for all sufficiently large $n \in \mathbb{Z}^+$. It follows that $\mathcal{C} := \{W_n \mid n \in \mathbb{Z}^+\}$ is a countably infinite linear covering of V, so $\mathrm{LC}(V) \leq \aleph_0$. Note that $\mathcal{C}$ is *highly* redundant: a subset $\mathcal{C}'$ of $\mathcal{C}$ is a linear covering of V if and only if $\mathcal{C}'$ is infinite. Thus no subset of $\mathcal{C}$ is an irredundant linear covering of V.

As above, if $\mathrm{LC}(V) < \aleph_0$, then V would admit a finite, irredundant linear covering, contradicting Theorem 5.15 since F is infinite. Thus $\mathrm{LC}(V) = \aleph_0$. □

Indeed Theorem 5.16 immediately implies Proposition 5.13.

3.1. Proof of Isaacs's Theorem III: Finite Degree. We will now prove Theorem 5.10: let L/F be an algebraic field extension, let M/F be a field extension, and suppose that every $f \in F[t]$ that has a root in L also has a root in M. We will show that there is an F-algebra homomorphism $\iota : L \hookrightarrow M$. By Theorem 5.12, it is enough to show that for every subextension K of L/F such that K/F has finite degree, there is an F-algebra homomorphism $\iota : K \hookrightarrow M$, using the fact that every polynomial in $F[t]$ with a root in K (also has a root in L, thus) also has a root in M.

Step 1: Suppose K/F is separable. Then by the Primitive Element Corollary, we have $K = F(\alpha)$ for some $\alpha \in K$. Let $f \in F[t]$ be the minimal polynomial of f. By hypothesis, there is a root β of f in M, and thus there is a unique F-algebra homomorphism $\iota : K = F(\alpha) \hookrightarrow M$ with $\iota(\alpha) = \beta$.
Step 2: Suppose that K/F is inseparable. Since finite fields are perfect, we must have that F is infinite. Let $\overline{M}$ be an algebraic closure of M, and consider the set $\mathrm{Hom}_F(K, \overline{M})$ of F-algebra homomorphisms from K to M. The size of this set is the separable degree $[K : F]_s$, which is finite. We are trying to show that there is $\iota \in \mathrm{Hom}_F(K, \overline{M})$ such that $\iota(K) \subseteq M$. For each $\iota \in \mathrm{Hom}_F(K, \overline{M})$, put

$$W_\iota := \iota^{-1}(M),$$

so W_ι is an F-linear subspace of K. For all $\alpha \in K$, as in Step 1, there is an F-algebra homomorphism from $F(\alpha)$ to M, which by the Magic Mapping Theorem extends to some $\iota \in \mathrm{Hom}_F(K, \overline{M})$ and thus $\alpha \in W_\iota$. It follows that $\{W_\iota \mid \iota \in \mathrm{Hom}_F(K, \overline{M})\}$ is a finite covering of K by F-linear subspaces. Since F is infinite, by Corollary 5.13 for at least one $\iota \in \mathrm{Hom}_F(K, \overline{M})$ we must have $W_\iota = K$ and hence $\iota(K) \subseteq M$. This completes the proof of Isaacs's Theorem.

CHAPTER 6

Norms, Traces, Discriminants and Resultants

1. Dedekind's Lemma on Linear Independence of Characters

THEOREM 6.1 (Dedekind's Lemma). *Let M be a monoid and K a field. The set $X(M,K)$ of all monoid homomorphisms $M \to K^\times$ is linearly independent as a subset of the K-vector space K^M of all functions from M to K.*

PROOF. By definition, a subset of a vector space is linearly independent if and only if every nonempty finite subset is linearly independent. So it's enough to show that for all $N \in \mathbb{Z}^+$, every N-element subset of $X(M,K)$ is linearly independent in K^M. We show this by induction on N. The base case, $N = 1$, is immediate: the only one element linearly dependent subset of K^M is the zero function, and elements of $X(M,K)$ are nonzero at all values of M. So suppose $N \geq 2$, that every $N-1$ element subset of $X(M,K)$ is linearly independent, and let $\chi_1, \ldots, \chi_N$ be distinct elements of $X(M,K)$. Let $\alpha_1, \ldots, \alpha_N \in K$ be such that for all $x \in M$, we have

$$\alpha_1\chi_1(x) + \ldots + \alpha_N\chi_N(x) = 0. \tag{1}$$

Our goal is to show that $\alpha_1 = \ldots = \alpha_N = 0$. Since $\chi_1 \neq \chi_N$, there is $m \in M$ such that $\chi_1(m) \neq \chi_N(m)$. Substituting mx for x in (1), we get that for all $x \in M$,

$$\alpha_1\chi_1(m)\chi_1(x) + \alpha_2\chi_2(m)\chi_2(x) + \ldots + \alpha_N\chi_N(m)\chi_N(x) = 0. \tag{2}$$

Multiplying (2) by $\chi_1(m)^{-1}$ and subtracting this from (1), we get

$$\forall x \in M,\ \alpha_2\left(\frac{\chi_2(m)}{\chi_1(m)} - 1\right)\chi_2(x) + \ldots + \alpha_N\left(\frac{\chi_N(m)}{\chi_1(m)} - 1\right)\chi_N(x) = 0. \tag{3}$$

By induction, $\chi_2, \ldots, \chi_N$ are linearly independent, so $\alpha_N\left(\frac{\chi_N(m)}{\chi_1(m)} - 1\right) = 0$ and thus $\alpha_N = 0$. Thus (1) gives a linear dependence relation among the $N-1$ characters $\chi_1, \ldots, \chi_{N-1}$, so by induction $\alpha_1 = \cdots = \alpha_{N-1} = 0$. □

2. The Characteristic Polynomial, the Trace and the Norm

Let L/K be a field extension of degree $n < \infty$. For $x \in L$, the map $x\bullet : L \to L$ given by $y \in L \mapsto xy$ is an endomorphism of L as a K-vector space. That is, for all $\alpha \in K$ and $y_1, y_2 \in$L, we have $x(\alpha y_1 + y_2) = x(\alpha y_1 + y_2) = \alpha x y_1 + x y_2 = \alpha(x y_1) + (x y_2)$. We may therefore analyze the element $x \in L$ using tools of linear algebra.

Choose a K-basis $b_1, \ldots, b_n$ for L. With respect to such a basis, the linear transformation $x\bullet$ is represented by an $n \times n$ matrix, say $M(x)$.

EXAMPLE 6.2. *Take $K = \mathbb{R}$, $L = \mathbb{C}$, and the basis $(1, i)$. Let $x = a + bi$. Then $x \bullet 1 = a \cdot 1 + b \cdot i$ and $x \bullet i = -b \cdot 1 + a \cdot i$. Therefore*

$$M(x) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

EXAMPLE 6.3. *If x lies in K, then $M(x) = m_{i,j}$ is simply the scalar matrix* $\operatorname{diag}(x, \dots, x)$. *Proposition 6.4 below gives a generalization.*

We define the characteristic polynomial of x:

$$P_x(t) = \det(tI_n - M(x)) = \prod_{i=1}^{n}(t - \lambda_i).$$

Similarly we define the **trace**

$$\operatorname{Tr}_{L/K}(x) = \operatorname{tr}(M(x)) = \sum_{i=1}^{n} m_{i,i} = \sum_{i=1}^{n} \lambda_i$$

and the **norm**

$$N_{L/K}(x) = \det(M(x)) = \prod_{i=1}^{n} \lambda_i.$$

PROPOSITION 6.4. *Let $L/K/F$ be a tower of field extensions with $m = [K : F]$ and $n = [L : K]$. Let $x_1, \dots, x_m$ be a basis for K/F and $y_1, \dots, y_n$ a basis for L/K.*

a) *For any element $\alpha \in K$, if M is the matrix representing $x\bullet \in \operatorname{End}_F(K)$ with respect to $\{x_1, \dots, x_m\}$, the matrix representation of $x\bullet \in \operatorname{End}_F(L)$ with respect to the basis $\{x_i y_j\}_{1 \le i \le m, 1 \le j \le n}$, reverse lexicographically ordered, is the block diagonal matrix* $\operatorname{diag}(M, \dots, M)$, *i.e., n blocks, each equal to M.*
b) *Let $f(t)$ be the characteristic polynomial of $\alpha\bullet \in \operatorname{End}_F(K)$ and $g(t)$ be the characteristic polynomial of $x\bullet \in \operatorname{End}_F(L)$. Then $g(t) = f(t)^{[L:K]}$.*
c) *We have $N_{L/F}(x) = N_{K/F}(x)^{[L:K]}$.*
d) $\operatorname{Tr}_{L/F}(x) = [L : K] \operatorname{Tr}_{K/F}(x)$.

PROOF. We have $\alpha x_i = \sum_{k=1}^{m} m_{ki} x_k$ and hence $\alpha x_i y_j = \sum_{k=1}^{m} m_{ki}(x_k y_j)$. This establishes part a). The remaining parts follow easily by standard linear algebraic considerations. □

COROLLARY 6.5. *Let L/F be a finite degree field extension. Let α be an element of L, let $f(t)$ be the minimal polynomial of α over F, and let $g(t)$ be the characteristic polynomial of $\alpha\bullet \in \operatorname{End}_F(L)$. Then $g(t) = f(t)^{[L:F(\alpha)]}$.*

PROOF. Put $K = F(\alpha)$. The minimal polynomial f of α over F is the characteristic polynomial of $x\bullet \in \operatorname{End}_F(K)$. So the result follows from Proposition 6.4. □

PROPOSITION 6.6. *Let $L/K/F$ be a tower of finite degree field extensions. Then:*

a) $\operatorname{Tr}_{K/F} : K \to F$ *is an F-linear map.*
b) *For all $x, y \in K$, $N_{K/F}(xy) = N_{K/F}(x) N_{K/F}(y)$.*
c) *For all $c \in F$ and $x \in K$, $N_{K/F}(cx) = c^{[K:F]} N_{K/F}(x)$.*

PROOF. Parts a) and b) are standard properties of the trace and determinant of any F-linear map. Part c) follows by applying part b) and observing that for $c \in F$, $N_{K/F}(c)$ is the determinant of the scalar matrix $\mathrm{diag}(c, \ldots, c)$, i.e., $c^{[K:F]}$. □

The following key result identifies the eigenvalues of $\alpha\bullet$ in field-theoretic terms.

THEOREM 6.7. *Let K/F be a field extension of degree $n < \infty$ and separable degree n_s. Put $p^e = \frac{n}{n_s} = [K : F]_i$. Let $\overline{K}$ be an algebraic closure of K. Let $\alpha \in K$ and let $f(t)$ be the characteristic polynomial of $\alpha\bullet \in \mathrm{End}_F(K)$. Let $\tau_1, \ldots, \tau_{n_s}$ be the distinct F-algebra embeddings of K into $\overline{K}$. Then*

$$f(t) = \prod_{i=1}^{n_s} (t - \tau_i(\alpha))^{p^e}.$$

It follows that

$$N_{K/F}(\alpha) = (\prod_{i=1}^{n_s} \tau_i(\alpha))^{p^e} \tag{4}$$

and

$$\mathrm{Tr}_{K/F}(\alpha) = p^e \sum_{i=1}^{m} \tau_i(\alpha). \tag{5}$$

PROOF. Put $L = F[\alpha]$. Let $d = [L : F]$, $d_s = [L : F]_s$ and $d_i = [L : F]_i$. Let $\sigma_1, \ldots, \sigma_{d_s}$ be the distinct F-algebra homomorphisms from L into $\overline{F}$. For each $1 \le i \le d_s$, σ_i extends to $\frac{n_s}{d_s}$ F-algebra homomorphisms from K into $\overline{F}$. Let

$$f(t) = (\prod_{i=1}^{d_s} (t - \sigma_i(\alpha)))^{d_i}$$

be the minimal polynomial of α over F, and let $g(t)$ be the characteristic polynomial of $\alpha\bullet$ on K, so by Corollary 6.5 we have

$$g(t) = f(t)^{[K:L]} = (\prod_{i=1}^{d_s} (t - \sigma_i(\alpha))^{d_i \frac{n}{d}} = \left((\prod_{i=1}^{d_s} (t - \sigma_i(\alpha))^{\frac{n_s}{d_s}} \right)^{n_i}$$

$$= \left(\prod_{i=1}^{n_s} (t - \tau_i(\alpha)) \right)^{p^i}.$$

Equations (4) and (5) follow immediately. □

COROLLARY 6.8. *Let $\mathbb{F}_{q^d}/\mathbb{F}_q$ be an extension of finite fields. Then the norm map $N : \mathbb{F}_{q^d}^\times \to \mathbb{F}_q^\times$ is surjective.*

PROOF. Let $\sigma : x \mapsto x^q$, so that $\mathrm{Aut}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle 1, \sigma, \ldots, \sigma^{d-1} \}$. Thus for $x \in \mathbb{F}_{q^d}$,

$$N(x) = \prod_{i=0}^{d-1} \sigma^i(x) = \prod_{i=0}^{d-1} x^{q^i} = x^{\sum_{i=0}^{d-1} q^i} = x^{\frac{q^d-1}{q-1}}.$$

Therefore $\mathrm{Ker}\, N$ consists of all elements of the finite cyclic group $\mathbb{F}_{q^d}^\times$ of order dividing $\frac{q^d-1}{q-1}$, so $\#\,\mathrm{Ker}\, N = \frac{q^d-1}{q-1}$. Since $\mathbb{F}_{q^d}^\times / \mathrm{Ker}\, N \cong N(\mathbb{F}_{q^d}^\times)$, we deduce that $\#N(\mathbb{F}_{q^d}^\times) = q - 1$: N is surjective. □

3. The Trace Form

Let F be a field and V a finite-dimensional F-vector space equipped with a bilinear form, i.e., a function $\langle\ ,\ \rangle : V \times V \to F$ such that for all $v, 1, v_2 \in V$ and $\alpha \in F$,

$$\langle \alpha v_1 + v_2, v_3 \rangle = \alpha \langle v_1, v_3 \rangle + \langle v_2, v_3 \rangle$$

and

$$\langle v_1, \alpha v_2 + v_3 \rangle = \alpha \langle v_1, v_2 \rangle + \langle v_1, v_3 \rangle.$$

Let $V^\vee = \mathrm{Hom}(V, K)$ be the dual space of V. A bilinear form on V induces a linear map $\Phi : V \to V^\vee$, namely

$$\Phi(v) = \langle v,\ \rangle.$$

(Note that a more careful notation would be something like $\Phi_L : v \mapsto \langle v,\ \rangle$, to distinguish it from the *other* obvious map $\Phi_R : v \mapsto \langle\ , v\rangle$. We have $\Phi_L = \Phi_R$ if and only if the bilinear form is **symmetric**, an assumption which we have not (yet) made. But in the general case the two maps are equally good, so let us work with $\Phi = \Phi_L$ for simplicity.) We say that the bilinear form $\langle , \rangle$ is **nondegenerate** if $\Phi : V \to V^\vee$ is an isomorphism. Since Φ is a linear map between two finite-dimensional vector spaces of the same dimension, Φ is an isomorphism if and only if it is injective, i.e., for each $v \in V$, if $\langle v, w \rangle = 0$ for all $w \in V$, then $v = 0$.

Let $\langle \cdot, \cdot \rangle$ be a bilinear form on V, and fix a K-basis $e_1, \ldots, e_n$ of V. We define the **Gram matrix** M of the bilinear form as $M(i, j) = \langle e_i, e_j \rangle$. We use the basis $e_1, \ldots, e_n$ to identify V with F^n. Then for all $v, w \in V$, we have

$$\langle v, w \rangle = v^T M w.$$

We claim that the nondegeneracy of the form is equivalent to the nonsingularity of the Gram matrix M. If M is singular, so is M^T, so there is $0 \neq v$ such that $v^T M = (Mv)^T = 0$, and thus $\langle v, w \rangle = 0$ for all $w \in V$. Conversely, if M is nonsingular, then for all $0 \neq v \in V$, $v^T M$ is nonzero, so it has at least one nonzero component i, so $v^T M e_i = \langle v, e_i \rangle \neq 0$. (This argument also makes clear that Φ_L is an isomorphism if and only if Φ_R is an isomorphism.)

Let $f_1, \ldots, f_n$ be a second F-basis of V. Then there is a unique matrix $P \in \mathrm{GL}_n(F)$ such that $Pe_i = f_i$ for all $1 \leq i \leq n$. Let us now write M_e for the old Gram matrix to emphasize that it is with respect to the old basis $e_1, \ldots, e_n$, which may view as the standard basis for F^n. We can define a Gram matrix M_f with respect to this new basis as well: its (i, j) entry is

$$M_f(i, j) = \langle f_i, f_j \rangle = \langle Pe_i, Pe_j \rangle = (Pe_i)^T M_e (Pe_j) = e_i^T P^T M_e P e_j = (P^T M_e P)(i, j).$$

That is, we have that $M_f = P^T M_e P$, from which it follows that

$$\det M_f = (\det P)^2 \det M_e.$$

We may therefore define the **discriminant** δ_V of the bilinear space $(V, \langle \cdot, \cdot \rangle)$ as the square class of the determinant of any Gram matrix, i.e., the class of $\det M_e$ in $F/F^{\times 2}$, since as we just showed this class is independent of the choice of basis for V.

Our fixed basis $(e_1, \ldots, e_n)$ induces a **dual basis** $(e_1^\vee, \ldots, e_n^\vee)$, characterized by $e_i^\vee(e_j) = \delta_{i,j}$ (Kronecker delta) for all $1 \leq i, j \leq n$. Thus, given a nondegenerate bilinear form $\langle\ ,\ \rangle$ on V, we may pull back the dual basis $(e_1^\vee, \ldots, e_n^\vee)$ under Φ^{-1} to

get a basis $(e^1, \ldots, e^n)$ of V with the characteristic property $\langle e_i, e^j \rangle = \delta_{i,j}$. Conversely, if a basis $(e^1, \ldots, e^n)$ of V exists which is dual to the given basis $(e_1, \ldots, e_n)$ in the above sense, then the bilinear form is easily seen to be nondegenerate. In summary:

PROPOSITION 6.9. *Let V be an n-dimensional vector space over a field K, let $\langle , \rangle$ be a bilinear form on V, and let $(e_1, \ldots, e_n)$ be any K-basis of V. Then the following are equivalent:*

(i) *The induced map $\Phi = \Phi_L : V \to V^\vee$ given by $v \mapsto \langle v, \rangle$ is an isomorphism.*
(ii) *The induced map $\Phi_R : V \to V^\vee$ given by $v \mapsto \langle , v \rangle$ is an isomorphism.*
(iii) *The Gram matrix $M(i,j) = \langle e_i, e_j \rangle$ is nonsingular.*
(iv) *There exists a basis $(e^1, \ldots, e^n)$ of V such that $\langle e_i, e^j \rangle = \delta_{i,j}$.*

Thus a bilinear form is nondegenerate if and only if its discriminant is nonzero.

Let K/F be a finite degree field extension. Define the **trace form** $T : K \times K \to F$, $T(x,y) := \mathrm{Tr}(x \bullet y \bullet)$. The bilinearity of T follows immediately from the linearity of the trace map. Note that T is also **symmetric** in the sense that $T(x,y) = T(y,x)$ for all $x, y \in K$. (It follows for instance that if F does not have characteristic 2, then T can be diagonalized.) The **discriminant** $\delta_{K/F}$ of K/F is the discriminant of the trace form T: thus it is an element of $F/F^{\times 2}$.

EXAMPLE 6.10. *(Trace form of a quadratic extension) Let K/F be a quadratic field extension.*

a) *Suppose that F does* not *have characteristic 2, so we may write $K = F(\sqrt{D})$. We wish to explicitly compute the trace form. A natural choice of F-basis for K is $(1, \sqrt{D})$. The Gram matrix is then*

$$M = \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{D}) \\ \mathrm{Tr}(\sqrt{D}) & \mathrm{Tr}(D) \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2D \end{bmatrix}.$$

Thus the discriminant of K/F is $D \pmod{F^{\times 2}}$.

b) *Now suppose that F has characteristic 2. It may still be that $K = F(\sqrt{D})$ for some $D \in F^\times$: this holds if and only if K/F is inseparable. In this case the trace map and the Gram matrix are both zero, as promised by Theorem 6.12, hence the discriminant is 0. Suppose then that K/F is separable. By Exercise 2.15, there is $a_0 \in F$ such that $K \cong F[t]/(t^2 + t + a_0)$. The classes of 1 and t give an F-basis for K. With respect to this basis, for any $A, B \in F$, the matrix representation for multiplication by $\alpha = A + Bt$ on K is $\begin{bmatrix} A & Ba_0 \\ B & A+B \end{bmatrix}$, so the trace of α is $A + (A+B) = B$. It follows that the Gram matrix for the trace form is*

$$M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}.$$

Thus the discriminant of K/F is $1 \pmod{F^{\times 2}}$.

Thus: away from characteristic 2, quadratic extensions are classified by their discriminant, while in characteristic 2, the discriminant precisely distinguishes between separable and inseparable quadratic extensions.

EXERCISE 6.1. *Let F be a field* not *of characteristic 3, and let K/F be a cubic extension. By Exercise 2.13, there are $a_0, a_1 \in F$ such that $K \cong F[t]/(t^3+a_1t+a_0)$.*[1] *We take as an F-basis for K the classes of $1, t, t^2$.*

a) *Show that the Gram matrix for the trace form is*

$$M = \begin{bmatrix} 3 & 0 & -2a_1 \\ 0 & -2a_1 & -3a_0 \\ -2a_1 & -3a_0 & 2a_1^2 \end{bmatrix}.$$

b) *Deduce: the discriminant of K/F is the class of $-4a_1^3 - 27a_0^2$ in $F^\times/F^{\times 2}$. In particular, in characteristic 2 we always have $\delta_{K/F} = 1 \in F^{\times 2}$.*

c) *A **pure cubic extension** is a cubic extension of the form $F[a^{1/3}]$. Show: the discriminant of a pure cubic extension is $-3 \pmod{F^{\times 2}}$.*

The definition of a pure cubic extension makes sense in all characteristics. In characteristic 3, a cubic extension is pure cubic if and only if it is inseparable. (This has an immediate generalization from 3 to any prime p.) The following result, taken from a paper of Kang [**Ka00**], shows that in characteristic different from 2 the converse of Exercise 6.1 holds – pure cubic extensions are characterized by their discriminant – and characterizes pure cubic extensions in characteristic 2.

THEOREM 6.11. *Let F be a field of characteristic not 3. Let $a_0, a_1 \in F^\times$, and suppose that $f = t^3 + a_1x + a_0 = 0$ is irreducible in F, so that if α is a root of f in $\overline{F}$, then $K \coloneqq F(\alpha)$ is a cubic extension of F.*

a) *Suppose $\mathrm{char}(F) \neq 2$. Then K/F is a pure cubic extension if and only if $\delta_{K/F} = -3 \pmod{F^{\times 2}}$.*

b) *Suppose $\mathrm{char}(F) = 2$. Then K/F is a pure cubic extension if and only if there is $w \in F$ such that $\frac{a_1^3}{a_0^2} = w^2 + w$.*

PROOF. Step 1: Suppose that there is $\beta \in K \setminus F$ with $\beta^3 = c \in F$, so $K = F(\beta)$ is a pure cubic extension. Then $1, \beta, \beta^2$ is an F-basis for K. We may write $\alpha = e + f\beta + g\beta^2$ with $e, f, g \in F$. Then the matrix representation of $\alpha\cdot$ on K with respect to this basis is

$$\begin{bmatrix} e & cg & cf \\ f & e & cg \\ g & f & e \end{bmatrix}.$$

This matrix has characteristic polynomial

$$\chi(t) = t^3 - 3cfgt - (cf^3 + c^2g^3).$$

But $\chi(\alpha) = 0$ and f is the minimal polynomial for α, so we have $\chi = f$: that is,

$$3cfg = -a_1 \text{ and } cf^3 + c^2g^3 = -a_0,$$

so $c, f, g \in F^\times$. Then:

$$-9f^2ga_0 = 9f^2g(cf^3 + c^2g^3) = 9cf^5g + 9c^2f^2g^4 = -3a_1f^4 + a_1^2g^2,$$

which may be rewritten as

$$\left(\frac{g}{f^2}\right)^2 a_1^2 - 3a_1 + 9a_0\left(\frac{g}{f^2}\right) = 0.$$

[1]This is the only place in this exercise that we use that F does not have characteristic 3. So if F has characteristic 3 and the cubic extension K/F happens to be of the above form, the exercise still applies.

Taking $\epsilon \coloneqq \frac{g}{f^2}$, we find that ϵ is a root of the quadratic

$$a_1^2 t^2 + 9a_0 t - 3a_1 = 0. \tag{6}$$

In characteristic different from 2, this means that the discriminant of the quadratic is a square in F, so we get

$$81a_0^2 + 12a_1^3 = -3(-4a_1^3 - 27a_0^2) = -3\delta_{K/F} \in F^{\times 2}.$$

In characteristic 2, multiplying the quadratic by $\frac{a_1^2}{a_0^2}$, we find that ϵ is also a root of

$$(a_1^2/a_0^2)t^2 + (a_1^2/a_0)t + a_1^3/a_0^2 = 0,$$

so $w \coloneqq \frac{a_1^2}{a_0^2}\epsilon$ is an element of F such that $\frac{a_1^3}{a_0^2} = w^2 + w$.

Step 2: Suppose that either the characteristic is not 2 and that $\delta_{K/F} = -3 \in F/F^{\times 2}$ or that the characteristic is 2 and there is $w \in F$ with $\frac{a_1^3}{a_0^2} = w^2 + w$. Then the quadratic (6) has a root $\epsilon \in F^\times$. Put

$$c \coloneqq \frac{-a_1}{3\epsilon},$$

let $\beta \in \overline{F}$ be such that $\beta^3 = c$, and put

$$\gamma \coloneqq \beta + \epsilon\beta^2.$$

One can calculate that $\gamma^3 + a_1\gamma + a_0 = 0$, hence $F(\beta) = F(\alpha)$. □

Exercise 6.2. *In the setting of Step 2 of the above proof, show that indeed* $\gamma^3 + a_1\gamma + a_0 = 0$.

The first question to ask about a bilinear form is whether it is nondegenerate. Here is the answer for the trace form:

Theorem 6.12. *Let K/F be a field extension of finite degree n. The following are equivalent:*

(i) *We have $\delta_{K/F} \neq 0$, i.e., the trace form is nondegenerate.*
(ii) *There is $x \in K$ such that $\mathrm{Tr}(x) \neq 0$.*
(iii) *The trace function $\mathrm{Tr} : K \to F$ is surjective.*
(iv) *The extension K/F is separable.*

Proof. The implications (i) $\implies$ (ii) $\implies$ (iii) are left to the reader.
(iii) $\implies$ (iv): we argue by contraposition. If K/F is not separable, then $\mathrm{char}(F) = p > 0$, $[K : F]_i = p^e$ is divisible by p, and thus (5) shows that the trace function is identically zero.
(iv) $\implies$ (i): By the Primitive Element Corollary, we have $K = F[\alpha]$ for some $\alpha \in K$. Then $(1, \alpha, \ldots, \alpha^{n-1})$ is an F-basis of K. Let $x \in K$. By Proposition 6.9, it is enough to show that the Gram matrix $M(i,j) = \mathrm{Tr}(\alpha^{i-1}\alpha^{j-1}) = \mathrm{Tr}(\alpha^{i+j-2})$ is nonsingular. To see this, let $\alpha_1, \ldots, \alpha_n$ be the distinct F-conjugates of α in $\overline{K}$. Then $\mathrm{Tr}(\alpha) = \sum_{i=1}^n \alpha_i$, so that for any $N \in \mathbb{N}$, $\mathrm{Tr}(\alpha^N) = \sum_{i=1}^n \alpha_i^N$. Now we introduce the Vandermonde matrix $V = V(\alpha_1, \ldots, \alpha_n)$: $V(i,j) = \alpha_j^{i-1}$. Why? Well, we compute that the (i,j) entry of VV^T is $\sum_{k=1}^n \alpha_k^{i-1}\alpha_k^{j-1} = M(i,j)$. Therefore

$$\det M = \det VV^T = (\det V)^2 = (\prod_{i>j} \alpha_i - \alpha_j)^2 \neq 0.$$ □

For a degree n field extension K/F, Theorem 6.12 tells us everything about $\delta_{K/F}$ when K/F is inseparable: namely, $\delta_{K/F} = 0$. But when K/F is separable, the proof of Theorem 6.12 gives us a useful formula for $\delta_{K/F}$: as above, let $\alpha \in K$ be a primitive element for K/F, and let $\alpha_1 = \alpha, \ldots, \alpha_n$ be the conjugates of α. Then

$$\delta_{K/F} = (\prod_{i>j} \alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j) \pmod{F^{\times 2}}. \tag{7}$$

In concrete situations where all the conjugates of α are explicitly known, it is more direct to compute $\delta_{K/F}$ using (7) than the definition (although in the examples to follow, we will proceed directly from the definition in order to build some familiarity with it). There are also many theoretical uses. One interesting aspect of (7) is that it is in general not obvious that the right hand side lies in F, although it must if K/F is a normal extension. In general, let L be the normal closure of K/F. We define the **semi-discriminant**

$$\mathbf{s}(\alpha) := \prod_{i>j} (\alpha_i - \alpha_j) \in L.$$

Because this definition uses an ordering of the conjugates, in fact $\mathbf{s}(\alpha)$ is well-defined only up to a sign. We notice of course that

$$\mathbf{s}(\alpha)^2 = \delta_{K/F} \in F.$$

Thus:

PROPOSITION 6.13. *Let K/F be a field extension of* odd *degree n that is normal and separable. Then $\delta_{K/F} \in F^{\times 2}$.*

PROOF. Because K/F is normal, in the above discussion we have $L = K$, so K contains a square root of $\delta_{K/F}$. Now $[F(\sqrt{\delta_{K/F}}) : F]$ divides 2 and $[K : F] = n$, which is odd, so $[F(\sqrt{\delta_{K/F}}) : F] = 1$ and thus $\delta_{K/F}$ is a square in F. □

4. Discriminants and Resultants

For any field F and any monic polynomial $f \in F[t]$ of positive degree, we factor $f := (t - \alpha_1) \cdots (t - \alpha_n)$ over an algebraic closure $\overline{F}$ and define

$$\delta(f) := \prod_{i>j} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Now it is immediate that $\delta(f) \neq 0$ if and only if f is separable, so we may restrict to the case of separable polynomials. At first glance, we can only say that the coefficients of f lie in some finite degree separable, normal extension L/F, but as soon as we study Galois theory (i.e., very soon!) it will become clear that the coefficients must therefore lie in F, because every automorphism σ of L that pointwise fixes F permutes the conjugates α_i and thus pointwise fixes the coefficients of F. So indeed we have $\delta(f) \in F$ in every case. And again we can define a semi-discriminant (up to sign) $\mathbf{s}(f)$, which in general lies in some quadratic extension of F.

EXERCISE 6.3. *Let R be an integrally closed[2] domain with fraction field F, and let $f \in R[t]$ be monic. Viewing $f \in K[t]$, we have $\delta(f) \in K$. Show: $\delta(f) \in R$.*

EXERCISE 6.4. *(Stickelberger) Let $f \in \mathbb{Z}[t]$. We will show: $\delta(f) \equiv 0, 1 \pmod 4$.*

[2]This hypothesis can be removed using the Fundamental Theorem on Symmetric Polynomials (cf. Exercise 8.46).

a) *Show: we may assume that f is separable.*
b) *Let K be a splitting field of $f \in \mathbb{Q}[t]$, and let $\mathbb{Z}_K$ be the integral closure of $\mathbb{Z}$ in K. Since f is monic and separable, there are distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}_K$ such that $f = \prod_{i=1}^n (t - \alpha_i)$. Define*

$$P := \prod_{1 \le i < j \le n} (\alpha_j + \alpha_i) \in \mathbb{Z}_K$$

and

$$E := \Delta(f) - P^2.$$

Show: $P, E \in \mathbb{Z}$. (This uses a ltitle Galois theory, as above.)
c) *Show: $E \equiv 0 \pmod{4\mathbb{Z}_K}$, and deduce: $\Delta(f) \equiv P^2 \pmod 4$, so $\Delta(f) \equiv 0, 1 \pmod 4$.*

LEMMA 6.14. *Let $f \in F[t]$ be a monic polynomial of degree $n \in \mathbb{Z}^+$ that factors in an algebraic closure as $\prod_{i=1}^n (t - \alpha_i)$. Then:*

$$\delta(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n f'(\alpha_i).$$

PROOF. We have

$$f' = \sum_{1 \le i \le n} \prod_{j \ne i} (t - \alpha_j),$$

so for all $1 \le i \le n$ we have

$$f'(\alpha_i) = \prod_{j \ne i} (\alpha_i - \alpha_j)$$

and thus

$$\prod_{i=1}^n f'(\alpha_i) = \prod_{1 \le i \ne j \le n} (\alpha_i - \alpha_j) = (-1)^{\frac{n(n-1)}{2}} \delta(f). \qquad \square$$

EXERCISE 6.5. *Let $f \in F[t]$ be an irreducible polynomial, and let α be a root of f in an algebraic closure of F. Show:*

$$\delta(f) = (-1)^{\frac{n(n-1)}{2}} N_{F(\alpha)/F}(f'(\alpha)).$$

In practice, for a degree n polynomial $f \in F[t]$, we want formulas for $\delta(f)$ in terms of the *coefficients* of f, not in terms of the roots. There are several ways to do this, each ultimately giving $\delta(f)$ as the determinant of an $n \times n$ matrix with entries F-linear combinations of the coefficients of f, so giving $\delta(f)$ as a polynomial in the coefficients of f.[3] One approach is via the **resultant**: for a field F and polynomials $f, g \in F[t]$ of positive degrees d and e such that

$$f = a \prod_{i=1}^d (t - \alpha_i) \text{ and } g = b \prod_{i=1}^e (t - \beta_j) \in \overline{F}[t],$$

[3]If we did not require f to be monic, the discriminant would still be defined and then it would be a *homogeneous* polynomial of degree n: for instance, the discriminant of $at^2 + bt + c$ is $b^2 - 4ac$. However, for many purposes – including all of ours throughout this text – we will only need to consider discriminants of monic polynomials, and as we will soon see, we should take all available avenues in order to keep the formulas for the disriminant to be as simple as possible.

we define

$$\mathrm{Res}(f,g) \coloneqq a^e b^d \prod_{1\le i\le d,\ 1\le j\le e} (\alpha_i - \beta_j) \in F(\alpha_1,\dots,\alpha_d,\beta_1,\dots,\beta_e).$$

REMARK 6.1. *We are really only interested in discriminants and resultants of monic polynomials, so for a while it is going to look like we made our life a little harder by definining resultants for arbitrary polynomials. Eventually we will give a certain approach to computing resultants by successive lowering the degrees but which may convert monic polynomials to non-monic polynomials.*

Suppose that f and g are separable. Because the expression defining $\mathrm{Res}(f,g)$ is a symmetric function of the β_j's, Galois theory will show that $\mathrm{Res}(f,g) \in F(\alpha_1,\dots,\alpha_d)$, and then, because the expression is a symmetric function of the α_i's, that $\mathrm{Res}(f,g) \in F$. Without the separability hypothesis, the Fundamental Theorem on Symmetric Polynomials will show this as well.

EXERCISE 6.6. *Let $f,g \in F[t]$ be as above.*

a) *Show:*

$$\mathrm{Res}(f,g) = a^e \prod_{1\le i\le d} g(\alpha_i) = (-1)^{de} b^d \prod_{1\le j\le e} f(\beta_j). \tag{8}$$

b) *Show: the formulas in part a) make sense when $f = a$ is or $g = b$ is a nonzero constant, and we get*

$$\mathrm{Res}(a,g) = a^e \text{ and } \mathrm{Res}(f,b) = b^d.$$

We define $\mathrm{Res}(f,g) = 0$ if at least one of f and g is 0. Thus we have defined $\mathrm{Res}(f,g) \in F$ for all $f,g \in F[t]$ in such a way that $\mathrm{Res}(f,g) = 0$ if and only if f and g share a root in an algebraic closure of F if and only if (cf. Lemma 4.1) f and g are not coprime in $F[t]$.

Combining Lemma 6.14 and (8) we get: for a monic $f \in F[t]$ of degree n,

$$\delta(f) = (-1)^{\frac{n(n-1)}{2}} \mathrm{Res}(f,f'). \tag{9}$$

EXERCISE 6.7. *Let F be a field.*

a) *Let $f,g \in F[t]$. Show:*

$$\delta(fg) = \delta(f)\delta(g)\,\mathrm{Res}(f,g)^2.$$

b) *Let $f,g \in F[t]$ be separable polynomials. Show:*

$$\delta(fg) \equiv \delta(f)\delta(g) \pmod{F^{\times 2}}.$$

c) *Show: if $f \in F[t]$ and $c \in F$, then then*

$$\delta((t-c)f) = \delta(f)f(c)^2.$$

Now let R be any commutative ring. For polynomials

$$f = a_0 t^d + a_1 t^{d-1} + \ldots + a_d \text{ and } g = b_0 t^e + \ldots + b_e \in R[t],$$

we define the resultant $\mathrm{Res}(f,g) \in R$ as the determinant of the **Sylvester matrix**:

$$\mathrm{Res}(f,g) \coloneqq \begin{vmatrix} a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ a_1 & a_0 & \cdots & 0 & b_1 & b_0 & \cdots & 0 \\ a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_d & a_{d-1} & \cdots & \vdots & b_e & b_{e-1} & \cdots & \vdots \\ 0 & a_d & \ddots & \vdots & 0 & b_e & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_{d-1} & \vdots & \vdots & \ddots & b_{e-1} \\ 0 & 0 & \cdots & a_d & 0 & 0 & \cdots & b_e \end{vmatrix}.$$

When R is a field, we now have two definitions of $\mathrm{Res}(f,g)$, but they define the same element of R: see e.g. [**vdW**, §5.9].

Using a computer algebra system to compute determinants of Sylvester matrices, one can derive "universal" formulas for discriminants of low-degree polynomials. Below we give the cases of monic polynomials of degree up to four as exercises. As will be seen, starting in degree 4 the formmulas are complicated enough so as to make theoretical use of them look unappealing.

EXERCISE 6.8. *Let F be a field.*

a) *Let $f \coloneqq t^2 + a_1 t + a_0 \in F[t]$. Show: $\delta(f) = a_1^2 - 4a_0$.*

b) *Let $f \coloneqq t^3 + a_2 t^2 + a_1 t + a_0 \in F[t]$. Show:*

$$\delta(f) = a_1^2 a_2^2 - 4a_0 a_2^2 - 4a_1^3 + 18 a_0 a_1 a_2 - 27 a_0^2.$$

In particular, if $a_2 = 0$ ("depressed cubic"), then

$$\delta(f) = -4a_1^3 - 27a_0^2.$$

c) *Let $f \coloneqq t^4 + a_3 t^3 + a_2 t^2 + a_1 t + a_0$. Show:*

$$\begin{aligned} \delta(f) &= a_1^2 a_2^2 a_3^2 - 4a_1^3 a_3^3 - 4a_1^2 a_2^3 + 18 a_1^3 a_2 a_3 - 27 a_1^4 + 256 a_0^3 \\ &+ a_0(-4a_2^3 a_3^2 + 18 a_1 a_2 a_3^3 + 16 a_2^4 - 80 a_1 a_2^2 a_3 a_4 - 6 a_1^2 a_3^2 a_4 + 144 a_1^2 a_2) \\ &+ a_0^2(-27 a_3^4 + 144 a_2 a_3^2 - 128 a_2^2 - 192 a_1 a_3). \end{aligned}$$

In particular, if $a_3 = 0$ ("depressed quartic"), then

$$\delta(f) = -27a_1^4 - 4a_1^2 a_2^3 + 144 a_0 a_1^2 a_2 + 16 a_0 a_2^4 + 256 a_0^3 - 128 a_0^2 a_2^2.$$

EXERCISE 6.9. *$f \in \mathbb{R}[t]$ be a monic polynomial of degree $n \geq 1$.*

a) *Suppose $n = 3$. Show: f has 3, 2 or 1 real roots according to whether its discriminant $\delta(f)$ is positive, zero or negative.*

b) *Suppose that f is separable. Let r be the number of real roots of f, and let $s = \frac{n-r}{2}$ be the number of complex-conjugate pairs of non-real roots of f (equivalently, the number of irreducible quadratic factors of f). Show: $\delta(f) > 0$ if and only if s is even.*

Above we saw that for extensions K/F of degree 2 and 3 in characteristic 2, the discriminant $\delta_{K/F}$ is (the class in $F/F^{\times 2}$ of) 0 if the extension is inseparable and is 1 if the extension is separable: that is, it is confirming Theorem 6.12 but not giving us any additional information. In fact, this is always true:

EXERCISE 6.10. *Let F be a field of characteristic 2, and let $f \in F[t]$ be a monic, separable polynomial of positive degree. Show: $\delta(f) \in F^{\times 2}$.*

Following Swan [**Sw62**], we give a method for computing discriminants using resultants and the Euclidean algorithm.

LEMMA 6.15. *Let F be a field, and let $f, g \in F[t]$ be nonzero polynomials, of degrees d and e, with leading coefficients a and b respectively. Let $c \in F$.*

a) *We have* $\mathrm{Res}(f,g) = (-1)^{de}\mathrm{Res}(g,f)$.
b) *For $f_1, f_2, g_1, g_2 \in F[t]$ nonzero polynomials, we have*

$$\mathrm{Res}(f_1 f_2, g) = \mathrm{Res}(f_1, g)\mathrm{Res}(f_2, g) \text{ and } \mathrm{Res}(f, g_1 g_2) = \mathrm{Res}(f, g_1)\mathrm{Res}(f, g_2).$$

c) *We have* $\mathrm{Res}(f, b) = b^d = \mathrm{Res}(b, f)$.
d) *We have* $\mathrm{Res}(f(t+c), g(t+c)) = \mathrm{Res}(f, g)$.
e) *We have* $\mathrm{Res}(f, t-c) = (-1)^d f(c)$.
f) *If $g = qf + r$, then* $\mathrm{Res}(f,g) = a^{e-\deg r}\mathrm{Res}(f,r)$.

EXERCISE 6.11. *Prove Lemma 6.15 (without using Sylvester determinants).*

Let R be a commutating ring, and let $f, g \in R$. Defining $\mathrm{Res}(f,g)$ as the above Sylvester determinant has one important theoretical advantage: it makes clear that viewing the coefficients of f and g as variables, the resultant $\mathrm{Res}(f,g)$ is given as a polynomial function of these variables, with coefficients in $\mathbb{Z}$. This has the following consequence, which is as useful as it is trivial:

EXERCISE 6.12. *Let $\alpha : R \to S$ be a homomorphism of commutative rings, and let $f, g \in R[t]$. There is an induced homomorphism from $R[t]$ to $S[t]$ – apply α to each coefficient – which we continue to denote by α. Show:*

$$\mathrm{Res}(\alpha(f), \alpha(g)) = \alpha(\mathrm{Res}(f,g)).$$

Let R be a commutative ring and let

$$f = a_0 t^d + a_1 t^{d-1} + \ldots + a_d \text{and } g = b_0 t^e + \ldots + b_e \in R[t]$$

be arbitrary polynomials of degrees d and e. There is a unique homomorphism

$$\alpha : \mathbb{Z}[s_0, \ldots, s_d, t_0, \ldots, t_e] \to R$$

such that $\alpha(s_i) = a_i$ for all $0 \leq i \leq d$ and $\alpha(t_j) = b_j$ for all $0 \leq j \leq d$. We define **generic polynomials**

$$F = s_0 t^d + s_1 t^{d-1} + \ldots + s_d \text{and } g = t_0 t^e + \ldots + t_e \in R[t];$$

then $\alpha(F) = f$ and $\alpha(G) = g$. Then, by Exercise 6.12, any polynomial identity satisfied by $\mathrm{Res}(F,G)$ – which can be proved by working in the fraction field $\mathbb{Q}(s_0, \ldots, s_d, t_0, \ldots, t_e)$ of the domain $\mathbb{Z}[s_0, \ldots, s_d, t_1, \ldots, t_e]$ induces an analogous identity for $\mathrm{Res}(f,g)$. For instance, the fact that $\mathrm{Res}(F,G) = (-1)^{de}\mathrm{Res}(G,F)$ for the generic polynomials F, G implies that $\mathrm{Res}(f,g) = (-1)^{de}\mathrm{Res}(g,f)$ for all polynomials over a commutative ring R. Similarly for polynomial identities involving more than two polynomials: e.g. parts a) and c) of Exercise 6.7 hold for $f, g \in R[t]$ because of this, and all of Lemma 6.15 holds for $f, g \in R[t]$ because of this.

EXERCISE 6.13. *Let R be a commutative ring, and let $f \in R[t]$. Show*

$$\mathrm{Res}(f, f') = \mathrm{Res}(f', f)$$

by reducing to the case in which R is a field of characteristic 0.

For any commutative ring R, there can be at most one function $\mathcal{R} : R[t] \times R[t] \to R$ satisfying parts a) through e) of Lemma 6.15, so these properties imply part f), though it seems easier to prove part f) by reducing to the case of a field and using roots in an algebraic closure. In fact part f) will be our main computational tool.

As a first application, it is now easy to compute the discriminant of a binomial:

PROPOSITION 6.16. *Let $n \in \mathbb{Z}^+$, let F be a field, and let $b \in F$. Then*

$$\delta(t^n + b) = (-1)^{\frac{n(n-1)}{2}} n^n b^{n-1}.$$

PROOF. Let $f \coloneqq t^n + b$. Then using Lemma 6.15 we get

$$\begin{aligned}\delta(f) &= (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(f, f') = (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(t^n + b, nt^{n-1})) \\ &= (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(t^n + b), n) \operatorname{Res}(t^n + b), t)^{n-1} \\ &= (-1)^{\frac{n(n-1)}{2}} n^n ((-1)^n b)^{n-1} = (-1)^{\frac{n(n-1)}{2} + n(n-1)} n^n b^{n-1} \\ &= (-1)^{\frac{n(n-1)}{2}} n^n b^{n-1},\end{aligned}$$

since $n(n-1)$ is even. □

THEOREM 6.17. *Let $p > 2$ be a prime number, and let*

$$\Phi_p \coloneqq \frac{t^p - 1}{t - 1} = t^{p-1} + t^{p-2} + \ldots + t + 1 \in \mathbb{Q}[t]$$

*be the **pth cyclotomic polynomial**. We have*

$$\delta(\Phi_p) = (-1)^{\frac{p-1}{2}} p^{p-2}.$$

PROOF. By Proposition 6.16 and Exercise 6.7 – and since p is odd – we have

$$\begin{aligned}(-1)^{\frac{p-1}{2}} p^p &= (-1)^{\frac{p(p-1)}{2}} (-1)^{p-1} p^p = \delta(x^p - 1) \\ &= \delta(\Phi_p)\delta(t-1) \operatorname{Res}(\Phi_p, t-1)^2 = \delta(\Phi_p) \operatorname{Res}(\Phi_p, t-1)^2.\end{aligned}$$

By (8), we have

$$\operatorname{Res}(\Phi_p, t-1) = (-1)^{p-1} \Phi_p(1) = (-1)^{p-1} p.$$

Thus

$$\delta(\Phi_p) = \frac{(-1)^{\frac{p-1}{2}} p^p}{((-1)^{p-1} p)^2} = (-1)^{\frac{p-1}{2}} p^{p-2}.$$ □

For $N \in \mathbb{Z}^+$, the **Nth cyclotomic polynomial** $\Phi_N \in \mathbb{C}[t]$ is the separable polyomial with roots the primitive Nth roots of unity. It has degree $\varphi(N)$. Since every Nth root of unity in $\mathbb{C}$ is a primitive dth root of unity for a unique $d \mid N$, we have

$$t^N - 1 = \prod_{d \mid N} \Phi_d. \tag{10}$$

Cyclotomic polynomials will be studied in detail in §8.1, and we will show that $\Phi_N \in \mathbb{Q}[t]$ is irreducible. Since every Nth root of unity is a power of any primitive Nth root of unity, it follows that if ζ_N is a primitive Nth root of unity, then $\mathbb{Q}(\zeta_n)$ is a normal extension of $\mathbb{Q}$ of degree $\varphi(N)$, called the **Nth cyclotomic field**.

For a prime power p^n with $n \geq 2$, we have

$$t^{p^n} - 1 = \Phi_{p^n}(t) \cdot (t^{p^{n-1}} - 1).$$

Using this, Proposition 6.16 and Exercise 6.7, we see that to evaluate $\delta(\Phi_{p^n})$ it suffices to evaluate $\mathrm{Res}(t^{p^{n-1}}-1, \Phi_{p^n})$, which wil be easy once we know one further property of Φ_{p^n}: we compute $\delta(\Phi_{p^n})$ in Exercise 8.9. When N is divisible by more than one prime, to use this method to compute $\delta(\Phi_N)$ we would need to know $\mathrm{Res}(\Phi_a, \Phi_b)$ for certain divisors a, b of N. This can certainly be done – see [**Ap70**] – but is not the optimal way to compute these discriminants. Indeed, a standard argument in algebraic number theory computes $\delta(\Phi_N)$ in terms of $\delta(\Phi_{p^n})$ for the prime power divisors p^n of N.

Because $\Phi_N \in \mathbb{Q}[t]$ is reducible, it follows that the discriminant of the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is the class of $\delta(\Phi_N)$ in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Let us denote this class by $\overline{\delta}(\Phi_N)$. This is much easier to compute than $\delta(\Phi_N)$ itself, because Exercise 6.7 shows that for polynomials $f_1, \ldots, f_n \in F[t]$ such that $f_1 \cdots f_n$ is separable, we simply have

$$\overline{\delta}(f_1 \cdots f_n) = \prod_{i=1}^n \overline{\delta}(f_i).$$

Then, because we know discriminants of binomials, (10) allows for an inductive computation of $\overline{\delta}(\Phi_N)$ for any $N \in \mathbb{Z}^+$. Here is one instance of this:

EXERCISE 6.14. *Let p_1, p_2 be distinct odd primes.*

a) *Show:* $\overline{\delta}(t^{p_1p_2}-1) = (-1)^{\frac{p_1p_2-1}{2}} p_1p_2$.

b) *Deduce:* $\overline{\delta}(\Phi_{p_1p_2}) = 1 \pmod{\mathbb{Q}^{\times 2}}$.

Following Swan[4] [**Sw62**], we will now compute the discriminant of any *trinomial*. First we compute the resultant of two binomials:

LEMMA 6.18. *Let $r, s \in \mathbb{Z}^+$, and put $d \coloneqq \gcd(r,s)$, $r_1 \coloneqq \frac{r}{d}$ and $r_2 \coloneqq \frac{s}{d}$. Let F be a field, and let $a, b \in F$. Then*

$$\mathrm{Res}(t^r - a, t^s - b) = (-1)^{rs+s}(a^{s_1} - b^{r_1})^d.$$

PROOF. This is a polynomial identity that can be established generically. In particular we can work in a field of characteristic 0 in which a and b are nonzero.

Put $f \coloneqq t^r - a$ and $g \coloneqq t^s - b$.

Step 1: Suppose the result holds for a pair (r,s) for all $a, b \in F$. Then it holds for the pair (s,r) for all $a, b \in F$: since $s + d \equiv rs + r \pmod 2$ we have

$$\mathrm{Res}(g,f) = (-1)^{rs}\,\mathrm{Res}(t^r - a, t^s - b) = (-1)^{s+d}(b^{r_1} - a^{s_1})^d$$
$$= (-1)^{rs+r}(b^{r_1} - a^{s_1})^d.$$

Step 2: We go by induction on $\max(r,s)$. The base case $r = s = 1$ is easy:

$$\mathrm{Res}(t-a, t-b) = (a-b) = (-1)^{1\cdot 1+1}(a^1 - b^1)^1.$$

So we may assume that $\max(r,s) \geq 2$ and that the result holds for pairs r', s' with $\max(r',s') < \max(r,s)$. After Step 1 we may assume $r \leq s$. Since

$$t^s - b = t^{s-r}(t^r - a) + at^{s-r} - b),$$

Lemma 6.15 gives

$$\mathrm{Res}(t^r - a, t^s - b) = \mathrm{Res}(t^r - a, at^{s-r} - b)$$

[4]Discriminants and resultants were a major topic in algebra from (at least) 1850-1900. One cannot really believe that this formula was first derived in 1962. However the method of is extremely elegant and useful.

$$= \operatorname{Res}(t^r - a, a) \operatorname{Res}(t^r - a), t^{s-r} - \frac{b}{a}) = a^r \operatorname{Res}(t^r - a, t^{s-r} - \frac{b}{a}).$$

We have $\gcd(r, s-r) = \gcd(r,s) = d$ and $s - r = (s_1 - r_1)d$, so by induction,

$$\operatorname{Res}(t^r - a, t^s - b) = a^r (-1)^{r(s-r)+s-r} \left(\frac{a^{s_1}}{a^{r_1}} - \frac{b^{r_1}}{a^{r_1}} \right)^d$$

$$= (-1)^{rs+s} (a^{s_1} - b^{r_1})^d. \qquad \square$$

THEOREM 6.19. *(Swan) Let $n, k \in \mathbb{Z}^+$ with $n \geq k$. Put $d \coloneqq \gcd(n,k)$, and write $n = n_1 d$ and $k = k_1 d$ with $k_1, n_1 \in \mathbb{Z}^+$. Let F be a field, and let $a, b \in F$. Then we have:*

$$\delta(t^n + at^k + b) =$$

$$(-1)^{\frac{n(n-1)}{2}} b^{k-1} \left(n^{n_1} b^{n_1 - k_1} + (-1)^{n_1+1} (n-k)^{n_1-k_1} k^{k_1} a^{n_1} \right)^d.$$

PROOF. Let $f \coloneqq t^n + at^k + b$. Again we may work generically and thus assume That F has characteristic 0 and that $a, b \in F^\times$.

We have

$$\delta(f) = (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(f, f')$$

$$= (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(f, nt^{n-1} + kat^{k-1})$$

$$= (-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(f, t^{n-k} + \frac{ka}{n}) \operatorname{Res}(f, n) \operatorname{Res}(f, t)^{k-1}$$

$$= (-1)^{\frac{n(n-1)}{2}} n^n (-1)^{n(k-1)} b^{k-1} \operatorname{Res}(f, t^{n-k} + \frac{ka}{n})$$

$$= (-1)^{\frac{n(n-1)}{2}} (-1)^{n(k-1)} (-1)^{n(n-k)} n^n b^{k-1} \operatorname{Res}(t^{n-k} + \frac{ka}{n}, f)$$

$$= (-1)^{\frac{n(n-1)}{2}} n^n b^{k-1} \operatorname{Res}(t^{n-k} + \frac{ka}{n}, f).$$

Since

$$t^b + at^k + b = t^k (t^{n-k} + \frac{ka}{n}) + (a - \frac{ka}{n}) t^k + b,$$

we have

$$\operatorname{Res}(t^{n-k} + \frac{ka}{n}, f) = \operatorname{Res}(t^{n-k} + \frac{ka}{n}, (a - \frac{ka}{n}) t^k + b)$$

Put

$$\alpha \coloneqq \frac{b}{a - \frac{ka}{n}}.$$

We have $\gcd(n, n-k) = \gcd(n,k) = d$ and $n - k = (n_1 - k_1)d$. Using Lemmas 6.15 and 6.18 we get

$$\operatorname{Res}(t^{n-k} + \frac{ka}{n}, (a - \frac{ka}{n}) t^k + b) = \operatorname{Res}(t^{n-k} + \frac{ka}{n}, a - \frac{ka}{n}) \operatorname{Res}(t^{n-k} + \frac{ka}{n}, t^k + \alpha)$$

$$= \left(a - \frac{ka}{n} \right)^{n-k} (-1)^{(n-k)k+k} \left(\left(\frac{ka}{n} \right)^{k_1} - \alpha^{n_1 - k_1} \right)^d.$$

Thus we have evaluated $\delta(f)$. We leave it to the reader to check that this simplifies to the formula claimed in the statement. $\square$

For later use, we record the simpler form the above result takes when $k = 1$:

$$\delta(t^n + at + b) = (-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (-1)^{n-1} (n-1)^{n-1} a^n \right). \tag{11}$$

Part II

Algebraic Extensions II: Galois Theory

CHAPTER 7

Galois Extensions

1. Introduction

In this chapter we cover the crown jewel of the theory of algebraic field extensions: Galois extensions and the Galois correspondence. This correspondence brings finite (and profinite) group theory to bear on field theory in an absolutely crucial way.

1.1. Lattices of Subfields and subgroups. As was pointed out by Kaplansky [**Kap95**, §3], some formal aspects of the Galois correspondence make sense in the context of *any* extension of fields. Namely, if K/F is a field extension, we define $\mathrm{Aut}(K/F)$ to be the set of F-algebra automorphisms of K: that is, the set of field automorphisms $\sigma : K \to K$ such that $\sigma(x) = x$ for all $x \in F$. It is immediate that $\mathrm{Aut}(K/F)$ is a group under composition.

Let $(X, \leq)$ be a partially ordered set, and let $x, y \in X$. A **supremum**, or **join**, for x and y is an element $z \in X$ such that $x, y \leq z$ and for any element $w \in X$ with $x, y \leq w$, we have $z \leq w$. Dually, an **infimum**, or **meet**, for x and y is an element $z \in X$ with that $z \leq x, y$ and for any element $w \in X$ with $w \leq x, y$, we have $w \leq z$. It is immediate from the definition that x and y can have at most one supremum and at most one infimum. When it exists, we denote the supremum of x and y by $x \vee y$, and when it exists, we denote the infimum of x and y by $x \wedge y$. In a totally ordered set, every pair of elements has a supremum – the larger of the two – and every pair of elements has an infimum – the smaller of the two. In general, suprema and infima need not exist: at the extreme, if on a set X we take the partial ordering of equality, then no pair of distinct elements has either a supremum or an infimum. A partially ordered set is called **directed** if every pair of elements has a supremum, and a partially ordered set is called a **lattice** if every pair of elements has a supremum and and infimum. We can similarly define suprema and infima for arbitary subsets Y of X. Note that, somewhat trickily, $\sup \varnothing$ is a **bottom element** of X, i.e., an element x with $x \leq y$ for all $y \in X$; and dually $\inf \varnothing$ is a **top element** of X, i.e., an element x with $y \leq x$ for all $\in X$. A **complete lattice** is a partially ordered set in which every subset Y has a supremum $\bigvee Y$ and an infimum $\bigwedge Y$. A finite lattice is complete if and only if it has top and bottom elements.

Let K/F be a field extension. We will define two associated lattices, one of subfields and one of subgroups. First, we let $\mathcal{L}(K/F)$ be the set of subextensions L of K/F, partially ordered under inclusion. This is a lattice: for subextensions L_1, L_2, the supremum $L_1 \vee L_2$ is the compositum $L_1 L_2$ – in other words the subfield generated by L_1 and L_2 – and the infimum $L_1 \wedge L_2$ is the intersection $L_1 \cap L_2$. In fact $\mathcal{L}(K/F)$ is a complete lattice: the top element is K and the bottom element is F, while if $\{L_i\}_{i \in I}$ is any set of subextensions of K/F, we have $\bigvee_i L_i$ is the subfield generated

by all the L_i's, while $\bigwedge_{i\in I} L_i = \bigcap_{i\in I} L_i$. Note that here and in the sequel we denote the pairwise supremum by L_1L_2 but for indexed sets it is convenient to use the $\bigvee$ notation because $\prod$ would create confusion with the Cartesian product.

Let $G \coloneqq \mathrm{Aut}(K/F)$. We define a second lattice $\mathcal{L}(G)$, which is the set of subgroups H of G, partially ordered under inclusion. Very similarly to the above one sees that for any group G, the set of subgroups of G, partially ordered by inclusion, forms a complete lattice, in which the top and bottom elements are G and $\{e\}$, the supremum $\bigvee_{i\in I} H_i$ of a nonempty family of subgroups is the subgroup they generate and the infimum $\bigwedge_{i\in I} H_i$ of a nonempty family of subgroups is their intersection $\bigcap_{i\in I} H_i$.

For a field extension K/F with $G \coloneqq \mathrm{Aut}(K/F)$, there are natural maps from each of the lattices $\mathcal{L}(K/F)$ and $\mathcal{L}(G)$ to the other. Namely, we define

$$\mathcal{H} : \mathcal{L}(K/F) \to \mathcal{L}(G),\ L \mapsto \mathrm{Aut}(K/L).$$

Notice that $\mathrm{Aut}(K/L)$ is the group of automorphisms of K that fix L pointwise; since L contains F, this is a subgroup of $\mathrm{Aut}(K/F)$, the group of automorphisms of K that fix L pointwise.

In the other direction, for any field K and any subgroup G of $\mathrm{Aut}(K)$, we define the **fixed field** or **invariant field**

$$K^G \coloneqq \{x \in K \mid \forall \sigma \in G, \sigma(x) = x.\}$$

EXERCISE 7.1. *Show that indeed K^G is a subfield of K.*

So for a field extension K/F with $G \coloneqq \mathrm{Aut}(K/F)$, we may define a map

$$\mathcal{L} : \mathcal{L}(G) \to \mathcal{L}(K/F),\ H \mapsto K^H.$$

Let $(X, \leq)$ and $(Y, \leq)$ be partially ordered sets. A map $f : X \to Y$ is called **isotone** if for all $x_1, x_2 \in X$, if $x_1 \leq x_2$ then $f(x_1) \leq f(X_2)$. A map $f : X \to Y$ is an **order isomorphism** if it is isotone and there is an isotone map $g : Y \to X$ such that $g \circ f = 1_X$ and $f \circ g = 1_Y$. Equivalently, an order isomorphism is an isotone bijection whose inverse is also isotone.

EXERCISE 7.2. *Let $(X, \leq)$ and $(Y, \leq)$ be partially ordered sets, and let $f : X \to Y$ be an isotone bijection, with inverse function $g : Y \to X$.*

a) *Suppose that $(X, \leq)$ is totally ordered. Show: $g : Y \to X$ is necessarily isotone.*
b) *Give an example in which g is not isotone.*

A map $f : X \to Y$ between partially ordered sets is **antitone** if for all $x_1, x_2 \in X$, if $x_1 \leq x_2$ then $f(x_2) \leq f(x_1)$. A map $f : X \to Y$ is an **order anti-isomorphism** if it is antitone and there is an antione map $g : Y \to X$ such that $g \circ f =!_X$ and $f \circ g = 1_Y$. We observe that the composition of two isotone maps is isotone, as is the compostion of two antitone maps, while the composition of an isotone map and an antitone map (in either direction) is antitone.

Coming back to our field extension K/F with $G = \mathrm{Aut}(K/F)$, we observe that both of the maps

$$\mathcal{H} : \mathcal{L}(K/F) \to \mathcal{L}(G) \text{ by } L \mapsto \mathrm{Aut}(K/L)$$

and

$$\mathcal{L} : \mathcal{L}(G) \to \mathcal{L}(K/F) \text{ by } H \mapsto K^H$$

are antitone. First, for subextensions $L_1 \subseteq L_2$ of K/F we have

$$\mathrm{Aut}(K/L_2) \subseteq \mathrm{Aut}(K/L_1) :$$

indeed, if an automorphism of K fixes every element of L_2, then it fixes every element of the subfield L_1. Second, for subgroups $H_1 \subseteq H_2 \subseteq G$, we have

$$K^{H_2} \subseteq K^{H_1} :$$

indeed, if an element of x is fixed by every element of H_2, then it is fixed by every element of the subgroup H_1.

It follows from the above remarks that both of the compositions

$$\mathcal{L} \circ \mathcal{H} : \mathcal{L}(K/F) \to \mathcal{L}(G)$$

and

$$\mathcal{H} \circ \mathcal{L} : \mathcal{L}(G) \to \mathcal{L}(K/F)$$

are isotone. More explicitly, if $L_1 \subseteq L_2$ are subextensions of K/F, then

$$K^{\mathrm{Aut}(K/L_1)} \subseteq K^{\mathrm{Aut}(K/L_2)},$$

while if $H_1 \subseteq H_2$ are subgroups of G, then

$$\mathrm{Aut}(K/K^{H_1}) \subseteq \mathrm{Aut}(K/K^{H_2}).$$

We also have the following containments:

$$\forall L \in \mathcal{L}(K/F),\ L \subseteq K^{\mathrm{Aut}(K/L)} \tag{12}$$

and

$$\forall H \in \mathcal{L}(G),\ H \subseteq \mathrm{Aut}(K/K^H). \tag{13}$$

Though they may not be immediately obvious, there is a startling lack of content here: (12) says that every element of L is fixed by every automorphism of K that fixes every element of L, and (13) says that every element of H fixes every element of K that is fixed by every element of H!

There is one tiny piece of content here, which we will state now and then prove in the (quite optional) next subsection. For $L \in \mathcal{L}(K/F)$, we define the **closure of** L as We call a subextension L of K/F **closed** if it is of the form $C(L')$ for some subextension L' of K/F, and we call a subgroup H of G **closed** if it is of the form $C(H')$ for some subgroup H' of G. Then:

PROPOSITION 7.1. *Let K/F be a field extension, with $G \coloneqq \mathrm{Aut}(K/F)$.*

a) *For all $L \in \mathcal{L}(K/F)$, we have $C(C(L)) = C(L)$, and for all $H \in \mathcal{L}(G)$, we have $C(C(H)) = C(H)$. It follows that $L \in \mathcal{L}(K/F)$ is closed if and only if $L = C(L)$ and that $H \in \mathcal{L}(G)$ is closed if and only if $H = C(H)$.*

b) *We have $\mathcal{H}(\mathcal{L}(K/F)) = \mathcal{C}(G)$ and $\mathcal{L}(\mathcal{L}(G) = \mathcal{C}(L/K)$.*

c) *The restrictions*

$$\mathcal{H}|_{\mathcal{C}(K/F)} : \mathcal{C}(K/F) \to \mathcal{C}(G)$$

and

$$\mathcal{L}|_{\mathcal{C}(G)} : \mathcal{C}(G) \to \mathcal{C}(L/K)$$

of $\mathcal{H}$ and $\mathcal{L}$ to the subsets of closed subfields and closed subgroups are mutually inverse order anti-isomorphisms.

In other words, the sublattice of closed subextensions is anti-isomorphic to the sublattice of closed subgroups. The issue with this is that we don't know which subfields and subgroups are closed. If it happens that they all are, then we get a nice conclusion:

COROLLARY 7.2. *Let K/F be a field extension, and let $G := \mathrm{Aut}(K/F)$. The following are equivalent:*

(i) *For all subextensions L of K/F, we have $K^{\mathrm{Aut}(K/L)} = L$, and for all subgroups H of G, we have $\mathrm{Aut}(K/K^H) = H$.*
(ii) *The maps $L \mapsto \mathrm{Aut}(K/L)$ and $H \mapsto K^H$ are mutually inverse order anti-isomorphisms from the lattice $\mathcal{L}(K/F)$ of subextensions of K/F to the lattice $\mathcal{L}(G)$ of subgroups of G.*

PROOF. Condition (i) means that every subextension L of K/F is closed and that every subgroup H of G is closed. When this holds Proposition 7.1c) gives (ii).

If condition (i) fails, there iseither a subextension L of K/F that is not closed or a subgroup H of G that is not closed. The closed subextensions of K/F are precisely those that lie in the image of the map $\mathcal{L} : H \mapsto K^H$, so if some subextension is not closed, then $\mathcal{L} : \mathcal{L}(G) \to \mathcal{L}(K/F)$ is not surjective. Similarly, the closed subgroups of G are precisely those that lie in the image of the map $\mathcal{H} : L \mapsto \mathrm{Aut}(K/L)$, so if some subgroup is not closed, then $\mathcal{H} : \mathcal{L}(K/H) \to \mathcal{L}(G)$ is not surjective. □

EXAMPLE 7.3. *Let $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ and $G := \mathrm{Aut}(K/F)$. The conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$ and $\zeta_3^2\sqrt[3]{2}$, where ζ_3 is a primitive cube root of unity. We may view K as a subfield of $\mathbb{R}$, and since neither $\zeta_3\sqrt[3]{2}$ nor $\zeta_3^2\sqrt[3]{2}$ lies in $\mathbb{R}$, certainly neither of these latter two conjugates lies in K. Since $\sigma \in G$ is determined by its action on $\sqrt[3]{2}$ and neither of the other conjugates of $\sqrt[3]{2}$ lies in K, we must have $\sigma = e$: in other words, G is the trivial group. Thus the only subgroup H of G is $\{e\}\}$, so the only subfield of K of the form K^H is K itself. In this case, the bijection of Proposition 7.1c) just takes $\{K\}$ to $\{\{e\}\}$.*

The same holds for any field extension K/F with $\mathrm{Aut}(K/F) = \{e\}$.

Thus the above formalism has the *potential* to give a useful bijective correspondence, but depending upon the nature of K/F it may give nothing nontrivial. Two of the main results of this chapter are as follows. First, suppose that K/F is a finite degree field extension. Then we will give several equivalent criteria for the conditions of Corollary 7.2 to hold, one of which is that K/F be normal and separable, and another is that F is closed: $K^{\mathrm{Aut}(K/F)} = F$. Thus for a finite degree normal, separable extension K/F, we get the classical Galois correspondence: the lattices of subextensions of K/F and subgroups of $G = \mathrm{Aut}(K/F)$ are anti-isomorphic. Second, suppose that K/F is an algebraic extension of infinite degree. Then we will show that every subextension L of K/F is closed if and only if K/F is normal and separable if and only if F is closed. In this case it turns out that not every subgroup of $G = \mathrm{Aut}(K/F)$ is closed, but we will give a useful description of the closed subgroups: namely, we will endow G with a certain topology, called the **Krull topology**, that makes G into a totally disconnected compact Hausdorff topological group. Then the closure operation $H \mapsto C(H)$ defined above on subgroups is precisely the closure with respect to the Krull topology, so we get an anti-isomorphism between the lattice of subextensions $\mathcal{L}(K/F)$ and the lattice of closed subgroups of the topological group G.

1.2. Galois Connections.

Let $(X, \leq)$ and $(Y, \leq)$ be partially ordered sets. An **(antitone) Galois connection from X to Y** is a pair of maps $\Phi : X \to Y$ and $\Psi : Y \to X$ such that:

(GC1) The maps Φ and Ψ are antitone; and
(GC2) For all $x \in X$ and $y \in Y$, we have $x \leq \Psi(y)$ if and only if $y \leq \Phi(x)$.

We observe that (Φ, Ψ) is a Galois connection from X to Y if and only if (Ψ, Φ) is a Galois connection from Y to X.

LEMMA 7.4. *For a field extension K/F with $G = \mathrm{Aut}(K/F)$, let $\mathcal{L}(K/F)$ be the lattice of subextensions L of K/F and $\mathcal{L}(G)$ the lattice of subgroups of G. Put*

$$\mathcal{H} : \mathcal{L}(K/F) \to \mathcal{L}(G),\ L \mapsto \mathrm{Aut}(K/L)$$

and

$$\mathcal{L} : \mathcal{L}(G) \to \mathcal{L}(K/F),\ H \mapsto L^H.$$

Then $(\mathcal{H}, \mathcal{L})$ is a Galois connection from $\mathcal{L}(K/F)$ to $\mathcal{L}(G)$.

PROOF. We know that the maps $\mathcal{H}$ and $\mathcal{L}$ are antitone. Let $L \in \mathcal{L}(K/F)$ and $H \in \mathcal{L}(G)$. Then $L \subseteq \mathcal{L}(H)$ if and only if $L \subseteq K^H$ if and only if $\sigma(x) = x$ for all $\sigma \in H$ and all $x \in L$ if and only if $H \subseteq \mathrm{Aut}(K/L)$ if and only if $H \leq \mathcal{H}(L)$. □

If $(X, \leq)$ is a partially ordered set, a **closure operator on X** is a map $C : X \to X$ such that all of the following hold:

(C1) C is an isotone map: $x_1 \leq x_2 \implies C(x_1) \leq C(x_2)$.
(C2) For all $x \in X$, $x \leq C(x)$.
(C3) For all $x \in X$, $C(C(x)) = x$.

PROPOSITION 7.5. *Let (Φ, Ψ) be a Galois connection from $(X, \leq)$ to $(Y, \leq)$. Then the mapping $\Psi \circ \Phi$ is a closure operator on X and the mapping $\Phi \circ \Psi$ is a closure operator on Y. For a closure operator C on a partially ordered set $(X, \leq)$, we call $C(x)$ the **closure of x** and we say that x is **closed** if $x = C(x)$.*

PROOF. By the symmetry between Φ and Ψ, it is enough to show tha $\Psi \circ \Phi$ is a closure operator on X. Being the composition of two antitone maps, it is an isotone map: (C1). For $x \in X$, since $\Phi(x) \geq \Phi(x)$, (GC2) implies $x \leq \Psi(\Phi(x))$: (C2). Applying (C2) to $\Psi(\Phi(x))$ gives

$$\Psi(\Phi(x)) \leq \Psi(\Phi(\Psi(\Phi(x)))).$$

Applying (GC2) to $\Psi(\Phi(x)) \leq \Psi(\Phi(x))$ we get

$$\Phi(\Psi(\Phi(x))) \geq \Phi(x),$$

and applying Ψ gives

$$\Psi(\Phi(\Psi(\Phi(x)))) \leq \Psi(\Phi(x)),$$

so we get (C3):

$$\Psi(\Phi(\Psi(\Phi(x)))) = \Psi(\Phi(x)).$$ □

COROLLARY 7.6. *Φ and Ψ satisfying the following **tridempotence properties**:*

a) *For all $x \in X$, we have $\Phi(\Psi(\Phi(x))) = \Phi(x)$.*
b) *For all $y \in Y$, we have $\Psi(\Phi(\Psi(x))) = \Psi(y)$.*

PROOF. By the symmetry between Φ and Ψ, it is enough to prove part a). Since $\Phi \circ \Psi$ is a closure operator, we have $\Phi(\Psi(\Phi(x))) \geq \Phi(x)$, and since $\Psi \circ \Phi$ is a closure operator, we have $\Psi(\Phi(x)) \geq x$ and thus $\Phi(\Psi(\Phi(x))) \leq \Phi(x)$. So $\Phi(\Psi(\Phi(x))) = \Phi(x)$. □

Now we have the main result on Galois Connections (which, we hope the reader sees, has virtually no content):

THEOREM 7.7. *Let (Φ, Ψ) be a Galois connection from the partially ordered set $(X, \leq)$ to the partially ordered set $(Y, \leq)$. Put*

$$\overline{X} := \Psi(\Phi(X)) \text{ and } \overline{Y} := \Phi(\Psi(Y).$$

a) *The set of closed elements for the closure operator $\Psi \circ \Phi$ on X is $\overline{X}$, and the set of closed elements for the closure operator $\Phi \circ \Psi$ on Y is $\overline{Y}$.*
b) *We have $\Phi(X) \subseteq \overline{Y}$ and $\Psi(Y) \subseteq \overline{X}$.*
c) *$\Phi|_{\overline{X}} : \overline{X} \to \overline{Y}$ and $\Phi|_{\overline{Y}} : \overline{Y} \to \overline{X}$ are mutually inverse order anti-isomorphisms.*

PROOF. a) For any closure operator C on a partially ordered set X, we have that $C(X)$ is the subset of closed elements: for all $x \in X$, $C(C(x)) = C(x)$, so $C(x)$ is closed, and if x is closed, then $x = C(x) \in C(X)$.
b) For all $x \in X$, $\Phi(x) = \Phi(\Psi(\Phi(x))) = C(\Phi(x)) \in \overline{Y}$. The symmetry between Φ and Ψ implies that $\Psi(Y) \subseteq \overline{X}$.
c) Since $x \in \overline{X}$ if and only if $x = \Psi(\Phi(x))$ and $y \in \overline{Y}$ if and only if $y = \Phi(\Psi(y))$, this is immediate. □

We say a Galois connection (Φ, Ψ) is **perfect** if every element of X is closed and every element of Y is closed. Thus Theorem 7.7 implies that a perfect Galois connection from X to Y gives a pair of mutually inverse order anti-isomorphisms from X to Y. We will see in the next section (without however needing to use this formalism) that if K/F is finite degree, normal and separable, then the Galois connection of Lemma 7.4 is perfect, giving the Galois correspondence between subextensions of K/F and subgroups of $\mathrm{Aut}(K/F)$.

In fact, it is a theorem of Barbilian–Krull [**Bar51**], [**Kr53**] (and derived *much* later, but independently, by the present author) that for a field extension K/F, if the Galois connection of Lemma 7.4 is perfect, then L/K must be finite degree, normal and separable. However, the next best thing is for this Galois connection to be **semi-perfect** in the sense that every subextension L of K/F is closed – that is, $L = K^{\mathrm{Aut}(L/K)}$. Then we get a Galois correspondence between the subfield lattice $\mathcal{L}(K/F)$ and the lattice of closed subgroups of $G = \mathrm{Aut}(K/F)$. Following Barbilian, we call such an extension a **Dedekind extension**. Later in this chapter we will show that if K/F is algebraic, normal and separable then it is a Dedekind extension *and* we will give a useful description of the closure operation on subgroups of $\mathrm{Aut}(K/F)$ in terms an associated topology. In Part II, we will exhibit one further class of Dedekind extensions that was also known to Barbilian–Krull: it suffices for K to be algebraically closed of characteristic 0. It is unknown whether there are any further Dedekind extensions.

EXERCISE 7.3. *Let $(X, \leq)$ and $(Y, \leq)$ be posets with top elements $\top_X$, $\top_Y$ and bottom elements $\bot_X$, $\bot_Y$. Let (Φ, Ψ) be a Galois connection from X to Y.*

a) *Show:* $\top_X \in \overline{X}$.
b) *Show:* $\bot_X \in \overline{X}$ *if and only if* $\Psi(\top_Y) = \bot_X$.

EXERCISE 7.4. *Let G be a group acting effectively on a nonempty set X. Let $\mathcal{L}(G)$ be the lattice of subgroups of G, and let $\mathcal{L}(X)$ be the lattice of subsets of X. We define maps*

$$\mathcal{H} : \mathcal{L}(X) \to \mathcal{L}(G),\ Y \mapsto H_Y := \{g \in G \mid g(y) = y \text{ for all } y \in Y\}$$

and

$$\mathcal{Y} : \mathcal{L}(G) \to \mathcal{L}(X),\ H \mapsto X^H := \{x \in X \mid g(x) = x \text{ for all } x \in H\}.$$

a) *Show: $(\mathcal{H}, \mathcal{Y})$ is a Galois connection from $\mathcal{L}(X)$ to $\mathcal{L}(G)$. We will denote the associated closure operators by $Y \mapsto \overline{Y}$ and $H \mapsto \overline{H}$.*
b) *Show: the bottom element of $\mathcal{L}(X)$ is $\varnothing$ and that $\overline{\varnothing}$ is the set of elements of X fixed by every element of G. Also show: the bottom element of $\mathcal{L}(G)$ is $\{e\}$, which is closed.*
c) *Suppose that G acts freely on X: that is, for all $g \in G \setminus \{e\}$ and all $x \in X$, $g(x) \neq x$. Show: for every nontrivial subgroup H of G, we have $\overline{H} = G$. Deduce: if G has a nontrivial element of finite order, then there is no topological group structure on G that realizes the closure operator $H\overline{H}$ on subgroups of G. What if $G = \mathbb{Z}$?*
d) *Let G be a group. Show: there is an effective G-set X with respect to which every subgroup of G is closed.*
(Hint: this holds if and only if every subgroup H of G is the subgroup of elements pointwise fixing some subset Y of X. But we can build X so that for each subgroup H, this holds for some subset $Y_H = \{y_H\}$ of X.}})

2. Finite Galois Extensions and the Finite Galois Correspondence

THEOREM 7.8. *If K/F is a finite degree field extension,* $\mathrm{Aut}(K/F)$ *is a finite group of cardinality at most* $[K : F]$.

PROOF. First recall that the set of F-algebra embeddings σ of K into an algebraic closure $\overline{F}$ is finite, so in particular the subset of such with $\sigma(K) = K$ is finite. This holds because $K = F(\alpha_1, \ldots, \alpha_n)$, and an embedding σ is determined by sending each α_i to one of the at most $d_i = [F[\alpha_i] : F]$ roots of the minimal polynomial of α_i over F in $\overline{F}$. Therefore the set of such embeddings has cardinality at most $d_1 \cdots d_n$. Note that when $K = F[\alpha]$ is simple this is exactly the bound we want, so that e.g. if K/F is separable we are already done.

Now for the general case. Let $\mathrm{Aut}(K/F) = \{\sigma_1, \ldots, \sigma_N\}$ and suppose, for a contradiction, that $N > m = [K : F]$. Let $\alpha_1, \ldots, \alpha_m$ be an F-basis for K, and consider the $N \times m$ matrix A whose (i, j) entry is $\sigma_i(\alpha_j)$. This matrix has rank at most $m < N$, so that its rows are K-linearly dependent: there exist $c_1, \ldots, c_N \in K$, not all 0, such that for all $1 \leq j \leq m$ we have

$$\sum_i c_i \sigma_i(\alpha_j) = 0.$$

For each $x \in K^\times$, there exist $a_1, \ldots, a_m$ in F such that $x = \sum_j a_j \alpha_j$. Then

$$\sum_i c_i \sigma_i(x) = \sum_i c_i \sigma_i(\sum_j a_j \alpha_j) = \sum_i c_i (a_j \sum_j \sigma_j(\alpha_j))$$

$$= \sum_j a_j (\sum_i c_i \sigma_i(\alpha_j)) = 0.$$

But taking $M = K^\times$ all the automorphisms σ_i give characters $M \to K^\times$ hence are K-linearly independent. Therefore in the last equation we must have $c_i = 0$ for all i, a contradiction. □

PROPOSITION 7.9 (Artin). *Let K be a field and G a finite group of automorphisms of K, of cardinality n. Then: $[K : F] = n$ and $\mathrm{Aut}(K/K^G) = G$.*

PROOF. Step 1: We show that K/K^G has finite degree.[1]

Let $\alpha \in K$, and let $S = \sigma_1, \ldots, \sigma_r$ be a maximal subset of G such that the elements $\sigma_i(\alpha)$ are distinct in K. It follows that for all $\tau \in G$, the r-tuple $v = (\tau\sigma_1\alpha, \ldots, \tau\sigma_r\alpha)$ differs from $w = (\sigma_1\alpha, \ldots, \sigma_r\alpha)$ by a permutation: indeed, since τ is injective, the components of w are all distinct, and if they were not simply a reordering of the components of v, this would contradict the maximality of S. Therefore α is a root of the polynomial

$$f(t) = \prod_{i=1}^{t} (t - \sigma_i\alpha),$$

a polynomial with coefficients in K^G. Moreover, $f(t)$ is separable, and thus K/K^G is separable. Corollary 5.4 applies to show that K/K^G has finite degree, indeed degree equal to the maximal degree $[K^G(\alpha) : K^G]$ of an element $\alpha \in K$.
Step 2: Above, for each α we constructed a polynomial satisfied by α of degree $r \leq n$, it follows that $[K^G : K] \leq n$. On the other hand, by Theorem 7.8 we have $n = \#G \leq \#\,\mathrm{Aut}(K/K^G) \leq [K^G : K]$. We conclude $[K : K^G] = n$ and $G = \mathrm{Aut}(K/K^G)$. □

We say that a finite degree field extension K/F is **Galois** if $K^{\mathrm{Aut}(K/F)} = F$, and we call $\mathrm{Aut}(K/F)$ the **Galois group** of K/F. Proposition 7.9 then asserts that if G is any finite group of automorphisms of a field K, then K/K^G is Galois with Galois group G: $K^{\mathrm{Aut}(K/K^G)} = K^G$. Notice that the containment $K^{\mathrm{Aut}(K/F)} \supseteq F$ is tautological, so what stops K/F from being Galois is precisely that the fixed field $K^{\mathrm{Aut}(K/F)}$ strictly contains F. For instance this occurs when $[K : F] > 1$ but $\mathrm{Aut}(K/F) = \{1\}$ is the trivial group.

EXAMPLE 7.10. *Suppose that F is a field of characteristic different from 3, and let $a \in F \setminus F^3$. The polynomial $f := t^3 - a \in F[t]$ has degree 3 and no root in F so is irreducible: let $K := F[t]/(f)$ be the corresponding cubic field extension, so $K = F(\alpha)$, where $\alpha^3 = a$. If $\sigma \in \mathrm{Aut}(K/F)$, then σ is determined by its action on α Let $\zeta := \frac{\sigma(\alpha)}{\alpha}$. Then*

$$\zeta^3 = \left(\frac{\sigma(\alpha)}{\alpha}\right)^3 = \frac{\sigma(\alpha^3)}{\alpha^3} = \frac{\sigma(a)}{a} = 1,$$

so $\zeta \in K$ is a cube root of unity. If ζ did not lie in F, then since $\zeta^2 + \zeta + 1 = 0$, we would have that $F(\zeta)/F$ is a quadratic subextension of the cubic extension K/F, which is impossible. So $\zeta \in F$.

We deduce: if F has no primitive cube root of unity – e.g. if F is a subfield of $\mathbb{R}$ – then $\mathrm{Aut}(K/F) = \{1\}$, so K/F is not *Galois.*

[1] In many standard treatments of finite Galois theory, the finiteness of K/K^G is an additional assumption. Our source for this stronger version is Lang's *Algebra*.

The next result shows that finite Galois extensions can be characterized in several other useful ways.

THEOREM 7.11 (Omnibus Theorem for Finite Galois Extensions). *Let K/F be a finite degree extension. The following are equivalent:*

(i) $K^{\mathrm{Aut}(K/F)} = F$ *("K/F is Galois.")*
(ii) $\#\,\mathrm{Aut}(K/F) = [K:F]$.
(iii) *K/F is normal and separable.*
(iv) *K/F is the splitting field of a separable, irreducible polynomial.*

PROOF. Let $G = \mathrm{Aut}(K/F)$.
(i) $\implies$ (ii) by Proposition 7.9.
(ii) $\implies$ (i): we have $F \subset K^G \subset K$, and $[K:K^G] = \#G = [K:F]$, so $K^G = F$.
(ii) $\iff$ (iii): Let $\mathrm{Hom}_F(K, \overline{F})$ be the set of F-algebra embeddings of K into $\overline{F}$. We have a natural injection

$$\iota : \mathrm{Aut}(K/F) \hookrightarrow \mathrm{Hom}_F(K, \overline{F})$$

by composing each automorphism of K with the inclusion $K \hookrightarrow \overline{F}$. We know that $\#\,\mathrm{Hom}_F(K, \overline{F}) = [K:F]_s$, the separable degree of K/F, which is equal to $[K:F]$ if and only if K/F is separable. Moreover the map ι is a bijection if and only if K/F is normal. It follows that $\#\,\mathrm{Aut}(K/F) = [K:F]$ if and only if K/F is normal and separable. (iv) $\iff$ (ii): We know that the number of embeddings of K into $\overline{F}$ is equal to the separable degree of K/F and that this equals $[K:F]$ if and only if K/F is separable; moreover, every F-algebra embedding $s : K \to \overline{F}$ has $s(K) = K$ – i.e., gives an automorphism of K if and only if K/F is normal. (iii) $\iff$ (iv): if K/F is separable, then the Primitive Element Corollary gives $K \cong F[t]/(f)$ for some irreducible, separable polynomial f. Since K/F is normal, f splits in K and therefore K/F is the splitting field of the separable polynomial f. The converse is essentially the same: since K/F is a splitting field, it is normal; since it is obtained by adjoining roots of separable polynomials, it is separable. □

EXERCISE 7.5. *Let F be a field, and for $1 \leq i \leq n$, let K_i/F be a finite degree extension (all inside an algebraic closure $\overline{F}$).*

a) *Show: if each K_i/F is Galois, then $(K_1 \cdots K_n)/F$ is Galois.*
b) *Show by example that (if $n \geq 2$, clearly) we may have that no K_i/F is GAlois but $(K_1 \cdots K_n)/F$ is Galois.*

EXERCISE 7.6. *Let F be a field, let $\sigma \in \mathrm{Aut}(F)$, and let C_σ be the cyclic subgroup of $\mathrm{Aut}(F)$ generated by σ. Put*

$$F^\sigma := \{x \in F \mid \sigma(x) = x\}.$$

Show: $F^{C_\sigma} = F^\sigma$.

Let p be a prime number, and let F be a field of characteristic p, with algebraic closure $\overline{F}$. Let $a, n \in \mathbb{Z}^+$, and put $q := p^a$. In §5.5 we showed that $\overline{F}$ contains a unique field of order q^n, which we denote by $\mathbb{F}_{q^n}$. In particular, we have a degree n field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. This extension is Galois: it is the splitting field of the separable polynomial $t^{q^n} - t \in \mathbb{F}_q[t]$.

We define the **q-Frobenius map**

$$\mathfrak{f}_q : F \to F \text{ by } x \mapsto x^q.$$

This is a field homomorphism. It is a field automorphism if and only if F is perfect. In particular, we have $\mathfrak{f}_q \in \mathrm{Aut}(\mathbb{F}_{q^n})$: for one thing, finite fields are perfect; and for another, an injective map from a finite set to itself must be surjective. Since elements $x \in \mathbb{F}_q$ are characterized by the property $x^q = x$, we have

$$F^{\mathfrak{f}_q} = F \cap \mathbb{F}_q.$$

It follows that $\mathfrak{f}_q \in \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. We claim that this automorphism has order n and thus generates the Galois group of $\mathbb{F}_{q^n}/\mathbb{F}_q$. Indeed, for $k \in \mathbb{Z}^+$, we have

$$\mathfrak{f}_q^k = \mathfrak{f}_{q^k}.$$

So $\mathfrak{f}_q^n = \mathfrak{f}_{q^n} = 1_{\mathbb{F}_q^n}$, while if $1 \leq k < n$, then

$$\mathbb{F}_{q^n}^{\mathfrak{f}_q^k} = \mathbb{F}_{q^n}^{\mathfrak{f}_{q^k}} = \mathbb{F}_{q^n} \cap \mathbb{F}_{q^k} \subseteq \mathbb{F}_{q^k} \subsetneq \mathbb{F}_{q^n},$$

so $\mathfrak{f}_q^k \neq 1$ in $\mathrm{Aut}(\mathbb{F}_q^n)$. Let us put $G \coloneqq \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, a cyclic group of order n.

Let L be a subextension of $\mathbb{F}_{q^n}/\mathbb{F}_q$. Then L is of course again a finite field. Since L is an $\mathbb{F}_q$-vector space, its order is a power of q: $L = \mathbb{F}_{q^d}$ for some $d \in \mathbb{Z}^+$. Since $\mathbb{F}_{q^n}$ is an L-vector space, q^n is a power of q^d: thus $d \mid n$. Conversely, for every $d \mid n$, the finite field $\mathbb{F}_{q^d}$ in $\overline{F}$ is a subextension of $\mathbb{F}_{q^n}/\mathbb{F}_q$. Thus the subextensions of $\mathbb{F}_{q^n}/\mathbb{F}_q$ are precisely $\mathbb{F}_{q^d}$ for $d \mid n$. For every such d, the subgroup

$$H_{n/d} \coloneqq \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_{q^d})$$

of G is generated by $\mathfrak{f}_{q^d}$ and has order $\frac{n}{d}$. These are all the subgroups of G. So:

$$L \mapsto \mathrm{Aut}(\mathbb{F}_{q^n}/L)$$

is a bijection from the set of subextensions of $\mathbb{F}_{q^n}/\mathbb{F}_q$ to the set of subgroups of $\mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. For a subextension $L = \mathbb{F}_{q^d}$ of $\mathbb{F}_{q^n}/\mathbb{F}_q$, we have that the *degree* $[L : \mathbb{F}_q] = [\mathbb{F}_{q^d} : \mathbb{F}_q]$ is equal to d, while the *index* $[G : \mathrm{Aut}(\mathbb{F}_{q^n}/L)] = [G : H_{n/d}]$ is equal to d. Because for two subextensions L_1, L_2 of $\mathbb{F}_{q^n}/\mathbb{F}_q$ we have $L_1 \subseteq L_2$ if and only if $[L_1 : \mathbb{F}_q] \mid [L_2 : \mathbb{F}_q]$, and for two subgroups H_1 and H_2 of G we have $H_1 \subseteq H_2$ if and only if $\#H_1 \mid \#H_2$, it follows that our bijection from subextensions to subgroups of the Galois group is antitone, or inclusion-reversing. This is an important special case of the Galois correspondence, coming up soon.

COROLLARY 7.12. *Let K/F be a finite degree field extension.*

a) *The extension K is a subextension of a finite Galois extension L/F if and only if K/F is separable.*
b) *If K/F is separable, any algebraic closure $\overline{F}$ of K contains a unique minimal extension M of K such that M/F is Galois, namely the normal closure of K/F in $\overline{F}$.*

PROOF. Since Galois extensions are separable and subextensions of separable extensions are separable, for K/F to be contained in a finite Galois extension it is clearly necessary for it to be separable. If so, then the normal closure M of K/F, being a compositum of the separable extensions $s(K)$ as s ranges over the finite set of distinct F-algebra embeddings of K into $\overline{F}$ is separable and normal, hence Galois. M/K is even the minimal extension of K which is normal over F, so certainly it is the minimal such Galois extension. □

In view of Corollary 7.12, it is reasonable to call the normal closure of a finite degree separable field extension the **Galois closure**.

THEOREM 7.13 (Natural Irrationalities). *Let K/F be a finite Galois extension, and let L/F be any field extension such that K and L can be viewed as subfields of a common field. Then:*

a) *The field extension KL/L is Galois.*
b) *The restriction map $r : \mathrm{Aut}(KL/L) \to \mathrm{Aut}(K/K \cap L)$ is an isomorphism.*
c) *We have $[KL : L] = [K : K \cap L]$.*

PROOF. a) This is the assertion that finite Galois extensions have the *base change meta-property*. But all of the following properties have the base-change meta property: being of finite degree, normality and separability. Alternately, since K/F is finite Galois, it is the splitting field of the separable polynomial $f \in F[x]$. Then KL/L is the splitting field of the polynomial $f \in L[x]$, which remains separable.
b) Let $\sigma \in \mathrm{Aut}(KL/L)$, and let $r(\sigma)$ denote the restriction of σ to K. Since σ fixes L pointwise and $F \subset L$, also σ fixes F pointwise. So for all $x \in K$, $r(\sigma)(x)$ is an F-conjugate of x; since K/F is normal, this implies $r(\sigma)(x) \in K$ and thus $r(\sigma) \in \mathrm{Aut}(K/F)$. Indeed, because σ pointwise fixes L, $r(\sigma)$ pointwise fixes $K \cap L$ and $r(\sigma) \in \mathrm{Aut}(K/K \cap L)$. This defines a map

$$r : \mathrm{Aut}(KL/L) \to \mathrm{Aut}(K/K \cap L).$$

That r is a group homomorphism is immediate. Moreover, the kernel of r consists of the set of automorphisms α of KL that pointwise fix both K and L and thus also pointwise fix KL: r is injective. Finally we must show that α is surjective. Its image is a subgroup of $\mathrm{Aut}(K/K \cap L)$, which by the Galois correspondence is therefore of the form $\mathrm{Aut}(K/E)$ for some $K \cap L \subset E \subset K$. Now observe that E is pointwise fixed by every $\alpha \in \mathrm{Aut}(KL/L)$, so hence $E \subset (KL)^{\mathrm{Aut}(KL/L)} = L$. It follows that $E \subset K \cap L$ and thus $E = K \cap L$ and α is surjective.
c) By part b) we have

$$[KL : L] = \#\,\mathrm{Aut}(KL/L) = \#\,\mathrm{Aut}(K/K \cap L) = [K : K \cap L]. \qquad \square$$

The name "Natural Irrationalities" of this result is standard, though opaque. It comes from the fact that this is a generalization and abstraction of an argument Abel made to complete Ruffini's proof of the insolvability of the quintic, but we will have neither need or occasion to examine this here. But it is fortunate that – unlike most results in field theory – Theorem 7.13 has a striking name, because it is an extremely useful result so it is nice to be able to refer to it by name.

EXERCISE 7.7. *Let p be a prime number, let $a \in \mathbb{Z}^+$, let $q = p^a$, and let $\mathbb{F}_q$ be "the" finite field of order q. Recall that inside an algebraic closure $\overline{\mathbb{F}_q}$, for all $n \in \mathbb{Z}^+$, there is a unique degree n extension $\mathbb{F}_{q^n}/\mathbb{F}_q$.*

a) *Let F be a field of characteristic p, and define $\mathfrak{f}_q : F \to F$ by $x \mapsto x^q$. Show: $\mathfrak{f}_q \in \mathrm{Aut}(F)$ if and only if F is perfect.*
b) *Let F be a perfect field containing $\mathbb{F}_q$, so $\mathfrak{f}_q \in \mathrm{Aut}(F/\mathbb{F}_q)$. Show: $\mathfrak{f}_q$ has finite order if and only if F is finite, in which case its order is $[F : \mathbb{F}_q]$.*
c) *Deduce: if $\mathbb{F}_{q^n}/\mathbb{F}_q$ is an extension of finite fields, then $\mathrm{Aut}(\mathbb{F}_q^n/\mathbb{F}_q)$ is cyclic of order n, generated by $\mathfrak{f}_q$.*

Now we come to a result that we consider the *Fundamental Theorem* in this subject, the main part of which is that for a finite Galois extension K/F, we have mutually inverse inclusion-reversing correspondences from subextensions of K/F to subgroups of $\mathrm{Aut}(K/F)$. As important as this is, we will see that it follows in a

completely formal way from the results we have already established: there is absolutely no new field-theoretic content here. We include also a treatment of how the Galois correspondence behaves under "conjugation," for which we will want some simple group-theoretic facts that we state as an exercise.

EXERCISE 7.8. *Let G be a group acting on a nonempty set X; then also G acts on the set 2^X of subsets of X. For $x \in X$, we define*

$$\mathrm{Stab}_x \coloneqq \{g \in G \mid gx = x\},$$

a subgroup of G. For a nonempty subset $Y \subseteq X$, we put

$$\mathrm{Fix}_Y \coloneqq \bigcap_{y \in Y} \mathrm{Stab}_y \subseteq G$$

and we put $\mathrm{Fix}_\varnothing \coloneqq G$.

a) *Let $g \in G$ and $x \in X$. Show:*

$$\mathrm{Stab}_{gx} = g \,\mathrm{Stab}_x\, g^{-1}.$$

b) *Let $g \in G$ and let $Y \subseteq X$. Show:*

$$\mathrm{Fix}_{gY} = g \,\mathrm{Fix}_Y\, g^{-1}.$$

THEOREM 7.14 (Fundamental Theorem of Finite Galois Theory). *Let K/F be a finite Galois extension, and put $G \coloneqq \mathrm{Aut}(K/F)$. Let $\mathcal{L}(K/F)$ denote the set of subextensions L of K/F, and let $\mathcal{L}(G)$ denote the set of subgroups of G, partially ordered under inclusion in both cases.*

a) *The maps*

$$L \in \mathcal{L}(K/F) \mapsto \mathrm{Aut}(K/L)$$

and

$$H \in \mathcal{L}(G) \mapsto K^H$$

are mutually inverse antitone bijections from $\mathcal{L}(K/F)$ to $\mathcal{L}(G)$.

b) *Let $L \in \mathcal{L}(K/F)$, and put $H \coloneqq \mathrm{Aut}(K/L)$. Let*

$$G_L \coloneqq \{\sigma \in G \mid \sigma(L) = L\}.$$

Then G_L is the normalizer $N_G(H)$ of H in G.

c) *For $i = 1, 2$, let $L_i \in \mathcal{L}(K/F)$, and put $H_i \coloneqq \mathrm{Aut}(K/L_i)$. Then for all $\sigma \in G$, we have*

$$\sigma(L_1) = L_2 \iff H_2 = \sigma H_1 \sigma^{-1}.$$

In particular, L_1 and L_2 are conjugate subfields of K/F – i.e., there is $\sigma \in G$ such that $\sigma(L_1) = L_2$ – if and only if H_1 and H_2 are conjugate subgroups of G.

d) *For $L \in \mathcal{L}(K/F)$, the extension L/F is Galois if and only if the subgroup $H \coloneqq \mathrm{Aut}(K/L)$ is normal in G, in which case $\mathrm{Aut}(L/F)$ is canonically isomorphic to the quotient group G/H.*

PROOF. a) That the maps $L \mapsto \mathrm{Aut}(K/K)$ and $H \mapsto K^H$ are antitone is essentially tautologous. Indeed, if $F \subseteq L_1 \subseteq L_2 \subseteq K$ and $\sigma \in \mathrm{Aut}(K/L_2)$, then σ pointwise fixes every element of L_2, hence it pointwise fixes every element of L_1, hence $\sigma \in \mathrm{Aut}(K/L_1)$, and thus $\mathrm{Aut}(K/L_2) \subseteq \mathrm{Aut}(K/L_1)$. Similarly, if $H_1 \subseteq H_2 \subseteq G$ and $x \in K^{H_2}$, then $\sigma(x) = x$ for all $\sigma \in H_2$, hence $\sigma(x) = x$ for all $\sigma \in H_1$, and thus $x \in K^{H_1}$.

Let $L \in \mathcal{L}(K/F)$. It is tautologous that $L \subseteq K^{\mathrm{Aut}(K/L)}$: every element of L is pointwise fixed by every element of G that pointwise fixes every element of L! The content here lies in the opposite containment, which again has already been established: since K/F is Galois, it is the splitting field of a separable polynomial $f \in F[t]$, which remains separable as a polynomial in $L[t]$, and its splitting field is still K: thus K/L is Galois. So $L = K^{\mathrm{Aut}(K/L)}$ by Theorem 7.11.

Let $H \in \mathcal{L}(G)$. Once again it is tautologous that $H \subseteq \mathrm{Aut}(K/K^H)$: every element of H pointwise fixes every element of K that is pointwise fixed by every element of H! Again the content lies in the opposite containment and has already been established: by Proposition 7.9, we have $\mathrm{Aut}(K/K^H) = H$.

b) Let $L \in \mathcal{L}(K/F)$ and $H = \mathrm{Aut}(K/L)$. Let $\sigma \in N_G(H)$. Then for all $\rho \in H$, we have $\sigma^{-1}\rho\sigma \in H$, so for all $x \in L$ we have $(\sigma^{-1}\rho\sigma)(x) = x$, hence $\rho(\sigma(x)) = \sigma(x)$, so $\sigma(x) \in K^H = L$. Thus $\sigma(L) \subseteq L$, and since also $\sigma^{-1} \in N_G(H)$, we have $\sigma(L) = L$. Conversely, let $\sigma \in G$ be such that $\sigma(L) = L$, let $\rho \in H$, and let $x \in L$. Then $\sigma(x) \in L$, so $\rho\sigma(x) = \sigma(x)$, so $(\sigma^{-1}\rho\sigma)(x) = x$. Thus $\sigma^{-1}\rho\sigma \in H$, so $\sigma \in N_G(H)$.

c) Let $L \in \mathcal{L}(K/F)$. With regard to the natural action of G on subsets of K, in the notation of Exercise 7.8 we have $\mathrm{Aut}(K/L) = \mathrm{Fix}_L$. The result then follows by applying Exercise 7.8b).

d) Let $L \in \mathcal{L}(K/F)$, and put $H \coloneqq \mathrm{Aut}(K/L)$. That L/F is Galois if and only if H is normal follows from *either* part b) or part c). Indeed, on the one hand L/F is normal if and only if $G_L = G$, but since $G_L = N_G(H)$, this holds if and only if H is normal in G. On the other hand, L/F is normal if and only if it is the only subfield of K/F that is conjugate to L under the action of G, but by part c) the G-conjugates of L are the subgroups conjugate to H, so this holds if and only if H is normal in G. In this case, restricting automorphisms from L to K defines a group homomorphism $q : \mathrm{Aut}(K/F) \to \mathrm{Aut}(L/F)$. The map q is surjective: if $\overline{F}$ is an algebraic closure of F containing L, then by Corollary 3.11 every $\sigma \in \mathrm{Aut}(L/F)$ extends to an automorphism over $\overline{F}$, which then restricts to an automorphism of K since K/F is normal. The kernel of q is the set of all $\sigma \in G$ that pointwise fix L – i.e., it is H – so q induces an isomorphism from G/H to $\mathrm{Aut}(L/F)$. □

Corollary 7.15. *Let K/F be a finite Galois extension, and let L be a subextension of K/F. Put*

$$G \coloneqq \mathrm{Aut}(K/F) \text{ and } H \coloneqq \mathrm{Aut}(K/L).$$

Then we have a natural isomorphism

$$\mathrm{Aut}(L/F) = N_G(H)/H.$$

Exercise 7.9. *Prove Corollary 7.15. (Hint: use Theorem 7.14b).)*

Remark 7.1. *In the notation of Theorem 7.14, the set $\mathcal{L}(K/F)$ has a left G-action. We may endow $\mathcal{L}(G)$ with the left G-action given by $g \bullet H \coloneqq gHg^{-1}$. Then parts a) and c) of Theorem 7.14 imply that*

$$\mathrm{Aut}(K/\cdot) : \mathcal{L}(K/F) \to \mathcal{L}(G)$$

is an isomorphism of left G-sets.

A finite degree field extension K/F is **abelian** if it is Galois and $\mathrm{Aut}(K/F)$ is commutative; it is **cyclic** if is Galois and $\mathrm{Aut}(K/F)$ is cyclic.

Exercise 7.10.

a) *Let K/F be a finite degree abelian extension. Show: every subextension L of K/F is also abelian (in particular, Galois).*
b) *Repeat part a) with "abelian" replaced by "cyclic."*
c) *Is there a finite Galois extension K/F that is* not *abelian such that every subextension L is Galois over F?*
(One aspect of this question concerns finite group theory; the other concerns the existence of certain Galois extensions. This latter question will be answered more generally in the next section.)

As mentioned in Chapter 5, the Galois Correspondence enables us to deduce the Primitive Element Corollary (5.3) from Primitive Element I. Actually, as pointed out by Weintraub [**We21**], we can use the Galois correspondence together with Proposition 5.13 to deduce the Primitive Element Corollary: let K/F be a finite degree separable field extension. If F is finite, then $K^\times$ has a generator, which is a generator for K/F, so we may assume that F is infinite. Again, passing to the normal closure of K/F and applying the Galois Correspondence, we see that K/F has only finitely many proper subextensions $\{L_i\}_{i=1}^n$ By Proposition 5.13, there is $\alpha \in K \setminus \bigcup_{i=1}^n L_i$, and thus $K = F(\alpha)$.

More quantitatively:

PROPOSITION 7.16. *Let K/F be a field extension of finite degree n. Then there are at most $2^{n!-1}$ subextensions of K/F that are separable over F.*

PROOF. If F_s be the separable closure of F in K, then $[F_s : F] \mid [K : F] = n$ and every separable subextension L of K/F is contained in F_s. Let M be the normal closure of F_s/F, so M/F is Galois, and by Proposition 3.19 we have $[M : F] \leq n!$. Let $G := \mathrm{Aut}(M/F)$, so $\#G = [M : F] \leq n!$. The set of separable subextensions of F_s/F is a subset of the set of separable extensions of M/F, which is in bijection with the set of subgroups of G, so there are no more separable subextensions of L/F than subgroups of G. In turn, there are no more subgroups of G than subsets of G containing $\{e\}$, of which there are at most $2^{n!-1}$. □

If K/F is monogenic of degree n, Proposition 7.16 is however much worse than Corollary 5.6, which says that there are no more than 2^{n-1} subextensions. The issue of course is that in the proof of Proposition 7.16 we are passing to the Galois closure and counting subextensions there, which takes us from n to $n!$. If we restrict attention to finite Galois extensions, we can do better.

PROPOSITION 7.17. *Let K/F be a finite Galois extension of degree n. Then there are at most $n^{\lfloor \log_2(n) \rfloor}$ subextensions of K/F.*

PROOF. By the Galois Correspondence, it is equivalent to give an upper bound on the number of subgroups of a group G of order n. If H is a nontrivial group of order at most $N \in \mathbb{Z}^+$, choose a nonidentity element h_1 of H, then an element $h_2 \in H \setminus \langle h_1 \rangle$, then an element $h_3 \in H \setminus \langle h_1, h_2 \rangle$, and so forth, putting $H_i := \langle h_1, \ldots, h_i \rangle$. Then we get a finite sequence of subgroups $H_0 := \{e\} \subsetneq H_1 \subsetneq \ldots \subsetneq H_k = G$. Since for all $0 \leq i \leq k-1$ we have $\#H_{i+1} \geq 2\#H_i$, it follows that

$$2^k \leq \#H_k = \#G \leq N,$$

so $k \leq \lfloor \log_2(N) \rfloor$. Thus every subgroup of G can be generated by at most $\lfloor \log_2(n) \rfloor$ elements, so the number of subgroups of G is at most $n^{\lfloor \log_2(n) \rfloor}$. □

EXERCISE 7.11.

a) *Let G be a group, and let $\mathcal{L}(G)$ be the set of subgroups of G, partially ordered by inclusion. Show: $\mathcal{L}(G)$ is a complete lattice, in which for a set $\{H_i\}_{iinI}$ of subgroups, its infimum is $\bigcap_{i\in I} H_i$ (we define $\bigcap_\varnothing = G$) and its supremum is $\langle H_i \mid i \in I\rangle$, the least subgroup containing each H_i. Show also: $\mathcal{L}(G)$ is finite if and only if G is finite.*

b) *Let K/F be any field extension, and let $\mathcal{L}(K/F)$ be the set of subextensions L of K/F, partially ordered by inclusion. Show: $\mathcal{L}(K/F)$ is complete lattice, in which for a set $\{L_i\}_{i\in I}$ of subextensions, its infimum is $\bigcap_{i\in I} L_i$ (the empty intersection being K) and its supremum is the subfield generated by each L_i and by F (so $\bigvee_\varnothing = F$).*

If $(X, \leq)$ and $(Y, \leq)$ are partially ordered sets, an **anti-isomorphism** $f : X \to Y$ is an antitone map that admits an antitone inverse $g : Y \to X$. An anti-isomorphism induces an isomorphism from X to the order dual $Y^\vee$ in which $y_1 \leq^\vee y_2$ if and only if $y_2 \leq y_1$. Passing from a partially ordered set X to its order dual $X^\vee$ converts suprema to infima and vice versa, so X is a lattice if and only if $X^\vee$ is a lattice, and X is a lattice if and only if $X^\vee$ is a complete lattice. So if $f : X \to Y$ is an anti-isomorphism of lattices, then for all $x_1, x_2 \in X$ we have

$$f(x_1 \vee x_2) = f(x_1) \wedge f(x_2) \text{ and } f(x_1 \wedge x_2) = f(x_1) \vee f(x_2).$$

The same property generalized from two-element subsets of X to arbitrary subsets of X holds if X is a complete lattice.

The point is that if K/F is a finite Galois extension, then Theorem 7.14 gives an anti-isomorphism from the complete lattice $\mathcal{L}(K/F)$ to the complete lattice $\mathcal{L}(G)$ (because the second lattice is finite, so is the first, so here "complete" just means that we have top and bottom elements).

For a subgroup H of a group G, we define the **normal core** $\mathrm{Core}(H) \coloneqq \bigcap_{g\in G} g^{-1}Hg$, which is the largest subgroup of H that is normal in G. Conjugate subgroups have the same normal core. A subgroup H is **corefree** if $\mathrm{Core}(H) = \{e\}$. That this is not a completely standard concept seems unfortunate, because it is fundamental in the study of group actions: consider the action of G on the (left, though it doesn't really matter) coset space G/H by $g \cdot xH \coloneqq gxH$. Let K be the set of all $g \in G$ that act as the identity on G/H; in other terms, K is the kernel of the associated homomorphism $G \to \mathrm{Sym}(G/H)$, so it is a normal subgroup of G that is contained in H. Indeed, for $x \in G$ we have $x \in K$ if and only if for all $g \in G$, $xgH = gH$ if and only if for all $g \in G$, $g^{-1}xgH = H$ if and only if for all $g \in G$, $g^{-1}xg \in H$ if and only if for all $g \in G$, $x \in g^{-1}Hg$ if and only if $x \in \mathrm{Core}(H)$, so $K = \mathrm{Core}(H)$. Thus a transitive group action is faithful if and only if each of its point stabilizers is corefree if and only if any one of its point stabilizers is corefree.

The above argument also gives us, for any subgroup H of a group G, an injective homomorphism $G/\mathrm{Core}(H) \hookrightarrow \mathrm{Sym}(G/H)$. We deduce:

PROPOSITION 7.18. *Let H be a subgroup of a group G, with finite index n. Then $[G : \mathrm{Core}(H)] \mid n!$.*

Now back to the Galois theory:

COROLLARY 7.19. *Let K/F be a finite Galois extension. Let $L, L_1, , \ldots, L_n$ be subextensions of K/F; put $H := \mathrm{Aut}(K/L)$ and for $1 \leq i \leq n$, put $H_i := \mathrm{Aut}(K/L_i)$.*

a) *We have*

$$L_1 \cdots L_n = K^{\bigcap_{i=1}^n H_i}$$

and

$$\bigcap_{i=1}^n = K^{\langle H_1, \ldots, H_n \rangle}.$$

b) *Let M be the normal closure of L/F. Then $M = K^{\mathrm{Core}(H)}$.*

PROOF. a) This is immediate from the above discussion.
b) The normal closure M of L/F is $\prod_{\sigma \in G} \sigma(L)$, the compositum of all the conjugates of L. The result now follows from part a) and Theorem 7.14c). □

This gives us what we need to strengthen Proposition 3.19:

THEOREM 7.20. *Let K/F be a field extension of finite degree n, with normal closure L.*

a) *If F has characteristic 0, then $[L : F] \mid n!$.*
b) *If F has characteristic $p > 0$ and K/F has separable degree m and inseparable degree p^a, so $n = m \cdot p^a$. Then $[L : F] \mid m!p^a \mid n!$.*

PROOF. Step 1: We suppose that K/F is separable, so L is its Galois closure. Let $G := \mathrm{Aut}(L/F)$, so by the Galois Correspondence there is an index n subgroup H of G with $K = L^H$. By Corollary 7.19 we have $L = L^{\mathrm{Core}(H)}$, so $\mathrm{Core}(H) = \{e\}$. Applying Proposition 7.18, we get

$$[L : F] = \#G = [G : \mathrm{Core}(H)] \mid [G : H]! = n!.$$

Step 2: If F has characteristic 0 then K/F is separable, and we are done after Step 1. So we may assume that F has characteristic $p > 0$. Let F_s be the separable closure of F in K, so $[F_s : F] = m$. Because K/F_s is purely inseparable, we may choose $\alpha_1, \ldots, \alpha_a \in K$ such that $\alpha_1^p \in F_s$; for all $2 \leq i \leq a$ we have $\alpha_i^p \in F_s(\alpha_1, \ldots, \alpha_{i-1})$; and $K = F_s(\alpha_1, \ldots, \alpha_a)$. Let M be the Galois closure of F_s/F, so Step 1 gives $[M : F] \mid m!$. Then $M(\alpha_1, \ldots, \alpha_a)$ contains K, is contained in L, and is purely inseparable over M, so M is the separable closure of F in $M(\alpha_1, \ldots, \alpha_a)$. By Corollary 4.31, $M(\alpha_1, \ldots, \alpha_a)/F$ is normal, so $M(\alpha_1, \ldots, \alpha_n) = L$. Moreover, each of $[M(\alpha_1) : M]$ and $[M(\alpha_1, \ldots, \alpha_i) : M(\alpha_1, \ldots, \alpha_{i-1})]$ (for $2 \leq i \leq a$) divides p, so

$$[L : F] = [M(\alpha_1, \ldots, \alpha_a) : F]$$

$$= [M : F][M(\alpha_1) : M][M(\alpha_1, \alpha_2) : M(\alpha_1)] \cdots [M(\alpha_1, \ldots, \alpha_a) : M(\alpha_1, \ldots, \alpha_{a-1})],$$

which divides $m!p^a$. Since $n = m!p^a$, we have $m!p^a \mid m!(p^a)! \mid (mp^a)! = n!$. □

Let F be a field with algebraic closure $\overline{F}$. Let K_1 and K_2 be two finite Galois subextensions of $\overline{F}/F$; for $i = 1, 2$ put $G_i := \mathrm{Aut}(K_i/F)$. Consider the field

$$K := K_1 K_2,$$

which is a finite degree extension of F. Exercise 3.12 implies that K/F is normal, while Corollary 4.13 implies that K/F is separable, so K/F is Galois. Or perhaps more simply: for $i = 1, 2$, K_i/F is the splitting field of a separable polynomial $f_i \in F[t]$. Let f be the squarefree part of $f_1 f_2$: i.e., if a monic irreducible factor

occurs in both f_1 and f_2, we take it only once in f. Then K is the splitting field of the separable polynomial $f \in F[t]$, so K/F is finite Galois. Let $G := \mathrm{Aut}(K/F)$. It is natural to ask how the groups G_1, G_2 and G are related.

For $i = 1, 2$, because K_i/F is normal, the natural restriction map gives a surjective group homomorphism $r_i : G \to G_i$, and this defines a homomorphism

$$r : G \to G_1 \times G_2,\ \sigma \mapsto (r_1(\sigma), r_2(\sigma)).$$

The map r is injective: indeed, an element σ in the kernel of r would pointwise fix both K_1 and K_2, hence it pointwise fixes the subfield they generate, which is K. This does not determine G but already gives some useful information: let $\mathcal{C}$ be a class of finite subgroups, such that membership in $\mathcal{C}$ depends only on the isomorphism class of the group. We say that a finite degree field extension K/F is $\mathcal{G}$-**Galois** if it is Galois and $\mathrm{Aut}(K/F) \cong \mathcal{C}$. Then if $\mathcal{C}$ is closed under finite direct products and passage to subgroups, then the compositum of two $\mathcal{C}$-Galois extensions is a $\mathcal{C}$-Galois extension. This holds for the following classes of finite groups: cyclic groups, commutative groups, nilpotent groups (which we will not mention in this text except in passing parenthetical remarks) and solvable groups (which we will cover in detail later on, starting from the definition).

Let us return to our embedding $r : G \hookrightarrow G_1 \times G_2$. The extension $K_1 \cap K_2/F$ is normal by Proposition 3.18 and separable by Corollary 4.13, so it is Galois: let $Q := \mathrm{Aut}(K_1 \cap K_2/F)$. For $i = 1, 2$, we have natural quotient maps $\pi_i : G_i \to Q$ and $\pi : G \to Q$. Elements of $G_1 \times G_2$ that lie in the image $r(G)$ are pairs (σ_1, σ_2) coming from restricting the same automorphism of F_1F_2, so σ_1 and σ_2 must restrict to the same automorphism of $F_1 \cap F_2$. This shows that $r(G)$ lies in the subgroup $\mathcal{G}$ of $G_1 \times G_2$ consisting of elements (σ_1, σ_2) such that $\pi_1(\sigma_1) = \pi_2(\sigma_2)$. Let $\Delta(Q) = \{(q, q) \in Q \times Q \mid q \in Q\}$ be the diagonal in $Q \times Q$. Then we have a quotient map $(q_1, q_2) : G_1 \times G_2 \to Q \times Q$ and

$$\mathcal{G} = (\pi_1, \pi_2)^{-1}(\Delta(Q)),$$

so

$$[G_1 \times G_2 : \mathcal{G}] = [Q \times Q : \Delta(Q)] = \#Q.$$

By Natural Irrationalities, we have

$$\#G = [K : K_1][K_1 : F] = [K_2 : K_1 \cap K_2][K_1 : F] = \frac{[K_1 : F][K_2 : F]}{[K_1 \cap K_2 : F]}$$

$$= \frac{\#G_1 \cdot \#G_2}{\#Q} = \#\mathcal{G}.$$

It follows that $r(G) = \mathcal{G}$. In particular, we have $G \cong G_1 \times G_2$ if and only if $K_1 \cap K_2 = F$, a property called **linear disjointness** that we will study extensively in Chapter 11.

In general, given surjective group homomorphisms $\pi_1 : G_1 \to Q$ and $\pi_2 : G_2 \to Q$, the **fiber product** $G_1 \times_Q G_2$ is the subgroup $\{(g_1, g_2) \in G_1 \times G_2 \mid \pi_1(g_1) = \pi_2(g_2)\}$ of $G_1 \times G_2$. With this terminology, we have proved:

THEOREM 7.21. *Let $K_1, K_2/F$ be finite Galois extensions inside a common algebraic closure. Then K_1K_2/F is Galois, and* $\mathrm{Aut}(K_1K_2/F)$ *is the* fiber product

of the homomorphisms $\pi_1 : \mathrm{Aut}(K_1/F) \to \mathrm{Aut}(K_1 \cap K_2/F)$ *and* $\pi_2 : \mathrm{Aut}(K_2/F) \to \mathrm{Aut}(K_1 \cap K_2/F)$.

REMARK 7.2. *In an earlier draft, I had Theorem 7.21 as an exercise, which also claimed that* $r(G)$ *is normal in* $G_1 \times G_2$ *with the quotient group being isomorphic to* Q. *But the above discussion shows that* $r(G) = \mathcal{G}$ *is normal in* $G_1 \times G_2$ *if and only if* $\Delta(Q)$ *is normal in* $Q \times Q$. *It is easy to see that for any group* Q, *we have that* $\Delta(Q)$ *is normal in* $Q \times Q$ *if and only if* Q *is commutative. So...that was wrong.*

One of the things that makes Theorem 7.21 a bit counterintuitive is that normally when doing Galois theory, every finite group we write down is the Galois group of some relevant extension, but here, when $K_1 \cap K_2 \subsetneq F$, *the group* $G_1 \times G_2$ *is* not *the Galois group of anything in sight.*

EXERCISE 7.12. *Let* G_1, G_2 *be finite groups, and* K/F *be a finite Galois extension such that* $\mathrm{Aut}(K/F) \cong G_1 \times G_2$. *Show: for* $i = 1, 2$ *there is a Galois subextension* K_i/F *of* K/F *with* $\mathrm{Aut}(K_i/F) \cong G_i$ *such that* $K_1 K_2 = K$.

3. The Fundamental Theorem of Algebra

One of the more surprising applications of Galois theory is to give a snappy proof of the Fundamental Theorem of Algebra: i.e., that $\mathbb{C}$ is algebraically closed. Of course this result is not so well named, because $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ is defined in terms of $\mathbb{R}$, and much of the point of $\mathbb{R}$ is that it is both an algebraic and topological object, defined as the *completion* of $\mathbb{Q}$ in any of several senses (one of which is pursued in the final chapter in this text). So it seems impossible to give a *purely algebraic proof* of the Fundamental Theorem of Algebra. The next best thing for an algebraist is to give a purely algebraic result whose hypotheses are known properties of $\mathbb{R}$ and $\mathbb{C}$ to conclude that $\mathbb{C}$ is algebraically closed. The earliest argument of this type was given by Gauss. It was Artin who first gave an appealing argument using Galois theory and also Sylow theory. We will now give one version of a result of this type.

FACT 1.

a) *Every odd degree polynomial* $f \in \mathbb{R}[t]$ *has a root in* $\mathbb{R}$. *Indeed, this is a famous consequence of the Intermediate Value Theorem together with the fact that* $\lim_{x \to \pm\infty} f(x) = \pm\infty$ *or* $\mp\infty$.

b) *Every quadratic polynomial* $g \in \mathbb{C}[t]$ *has a root in* $\mathbb{C}$. *Indeed, the Intermediate Value Theorem implies that every* $r \in \mathbb{R}^{\geq 0}$ *has a positive real* n*th root* $r^{1/n}$ *for any* $n \in \mathbb{Z}^+$, *so writing* $z \in \mathbb{C}$ *in polar form* $re^{i\theta}$, *we get that* $r^{1/n} e^{i\theta/n}$ *is an* n*th root of* z. *Then the quadratic formula shows that we can solve quadratic equations over* $\mathbb{C}$.

The following result immediately combines with Fact 1 to prove that $\mathbb{C}$ is algebraically closed:

THEOREM 7.22. *Let* K/F *be a finite degree field extension. Suppose that:*

(i) *Every odd degree polynomial* $f \in F[t]$ *has a root in* F.

(ii) *Every quadratic polynomial* $g \in K[t]$ *has a root in* K.

Then K *is algebraically closed.*

PROOF. Step 1: We show that K is perfect. For this we may assume it has characteristic $p > 0$. If p is odd, then by (i) for all $x \in F$, the polynomial $t^p - x \in F[t]$ has a root in F, i.e., $x \in F^p$. So F is perfect, and then by Corollary 4.32 also

K is perfect. If $p = 2$ the same argument shows that K is perfect.
Step 2: Seeking a contradiction, we suppose that K is *not* algebraically closed. Since it is perfect, it therefore admits a proper finite degree separable extension L/K; let M be the Galois closure of M/F (note: *not* of M/K!). Let $G := \mathrm{Aut}(M/F)$, and let H_2 be a Sylow 2-subgroup of G, so M^{H_2}/F is separable of odd degree $[G : H_2]$. By the Primitive Element Corollary, there is then an irreducible polynomial in $F[t]$ of degree $[G : H_2]$, which by (i) implies that $[G : H_2] = 1$, i.e., $G = H_2$ is a 2-group. Then $H := \mathrm{Aut}(M/K)$ is a subgroup of G – nontrivial, since $M \supsetneq L \supsetneq K$ – hence also a 2-group. As we will prove in the next chapter, any nontrivial finite p-group has a subgroup of index p,[2] so H admits an index 2 subgroup H'. But then $M^{H'}/K$ is a quadratic extension, contradicting (i). □

REMARK 7.3. *There are some variations on this theme:*

a) *One can strengthen Theorem 7.22 by replacing "K/F has finite degree" with "K/F is algebraic." This requires the Galois theory of algebraic extensions and the existence of Sylow pro-p-subgroups of profinite groups.*
b) *In Theorem 7.22, the prime 2 is playing a distinguished role. In fact, for any prime p, if in condition (i) we replace "odd" with "prime to p ", in condition (ii) we replace "quadratic" with "degree p" and use the Sylow p-subgroup of G, the proof works verbatim. However, this is a rather uncharming generalization, since it seems to lack any specific application.*

In Fact 1, we showed that $\mathbb{C}$ has no quadratic extension using the fact that every positive real number has a real square root. This suggests a line of generalization that proceeds by considering *orderings* on a field. As we will see in Chapter 14, this was done by Artin–Schreier. Their main result, Theorem 14.18, gives several criteria on a field F for $F(\sqrt{-1})$ to be algebraically closed, one of which is that it admits an ordering (compatible with the field axioms) in which every positive element is a square and every odd degree polynomial in $F[t]$ has a root in F. Another – quite remarkable – condition is that F is not algebraically closed and there is $N \in \mathbb{Z}^+$ such that if K/F is a finite Galois extension then $[K : F] \leq N$. The proof of this Grand Artin–Schreier Theorem will be quite intricate.

Another variant on the above result is due to Shipman [**Sh07**]:

THEOREM 7.23 (Shipman). *Let F be a field such that every polynomial $f \in F[t]$ of prime degree has a root in F. Then F is algebraically closed.*

In the proof we will make use a of (well-known, elementary) result that we now discuss. A **numerical semigroup** M is a submonoid of $(\mathbb{N}, +)$: that is, M contains 0 and is closed under addition. The numerical semigroup $\{0\}$ is **trivial**; the others are **nontrivial**. A subset $S \subseteq \mathbb{N}$ generates a numerical semigroup $\langle S \rangle_{\mathbb{N}}$: it is, one the one hand, the intersection of all numerical semigroups containing S, and on the other hand, the set of all finite $\mathbb{N}$-linear combinations of elements of S (we regard 0 as being a linear combination of the 0-element subset of S.) Such an S also generates a subgroup $(\mathbb{Z}, +)$ – equivalently, an ideal of the ring $\mathbb{Z}$: on the one hand, it is the intersection of all subgroups of $\mathbb{Z}$ containing S, and on the other

[2]What we will prove is that a nontrivial finite p-group has a *normal* subgroup of index p, and in fact a finite group of order p^n has normal sugroups of order p^k for all $0 \leq k \leq n$, but we don't need this.

hand, the set of all finite $\mathbb{Z}$-linear combinations of elements of S. The assertion that $\mathbb{Z}$ is a principal ideal domain is equivalent to the fact $\langle S\rangle_{\mathbb{Z}} = \langle \gcd(S)\rangle_{\mathbb{Z}}$, where $\gcd(S)$ is the largest positive integer that divides every element of S. A numerical semigroup M is called **primitive** if $\langle M\rangle_{\mathbb{Z}} = \mathbb{Z}$: equivalently, if there is no prime number dividing every element of M.

PROPOSITION 7.24. *Let M be a nontrivial numerical semigroup; let $d \coloneqq \gcd(M)$.*

a) *There is $N \in \mathbb{Z}^+$ such that for all $n \geq N$, $nd \in M$.*
b) *M is primitive if and only if it is cofinite: $\mathbb{N} \setminus M$ is finite.*
c) *M is finitely generated: there is finite subset $S \subseteq M$ such that $M = \langle S\rangle_{\mathbb{N}}$.*

PROOF. Step 0: We observe that parts a) and b) are equivalent: indeed, if a) holds and M is primitive, then M is cofinite in $\gcd(M)\mathbb{N} = \mathbb{N}$, while if M is cofinite in $\mathbb{N}$ then it contains two consecutive natural numbers and thus $\gcd(M) = 1$, so b) holds. If b) holds, then

$$\overline{M} \coloneqq \left\{ \frac{x}{\gcd(M)} \mid x \in M \right\}$$

is primitive, so $\overline{M}$ is cofinite, so $M = \gcd(M)\overline{M}$ is cofinite in $\gcd(M)\mathbb{N}$.
Step 1: We will prove parts a) and b) when M is finitely generated by induction on the cardinality of a finite generating set S. The case $\#S = 1$ is trivial: if $S = \{d\}$, then $M = d\mathbb{N} = \gcd(M)\mathbb{N}$. We will also need $n = 2$ as a base case: after Step 0 we may assume that $M = \langle a, b\rangle_{\mathbb{N}}$ for coprime positive integers a and b. Since a and b are coprime, for $0 \leq i \leq b-1$ the integers ia are all distinct modulo b and thus give a system of representatives for the congruence classes modulo b. Every element of M is of the form $xa + yb$ for $x, y \in \mathbb{N}$, and this element lies in the class of ia modulo b if and only if $x \equiv i \pmod{b}$. It follows that the least element of class $ia \pmod{b}$ lying in M is ia, and then adding a positive multiple of b we see that every larger integer that congruence class is also an element of M. Thus M contains all but finitely many non-negative integers lying in each of the finitely many congruence classes modulo b, so M is cofinite in $\mathbb{N}$. We don't need it, but we can't help but point out that this argument shows us that the largest element of $\mathbb{N} \setminus M$ is $(b-1)a - b = ab - a - b$.

Now suppose that $n \geq 3$, assume that parts a) and b) hold for all numerical monoids generated by fewer than n elements, and let $M = \langle S\rangle_{\mathbb{N}}$ with $S = \{x_1, \ldots, x_n\}$ and $\gcd(x_1, \ldots, x_n) = 1$. Put

$$M' \coloneqq \langle x_1, \ldots, x_{n-1}\rangle \text{ and } d' \coloneqq \gcd(x_1, \ldots, x_{d-1}).$$

By induction, M' contains all sufficiently large elements of $d'\mathbb{N}$, so it contains an element of the form md' with $\gcd(d', x_n) = 1$. Since $\gcd(x_1, \ldots, x_n) = 1$, we have $\gcd(d', x_n) = 1$ and thus $\gcd(md', x_n) = 1$. Thus M contains $\langle md', x_n\rangle$, which is cofinite in $\mathbb{N}$, so M is cofinite in M.
Step 2: Let $M = \langle S\rangle_{\mathbb{N}}$ be a numerical monoid. For afinite subset T of S with $\gcd(T) > \gcd(S)$, we may add an element to T to reduce the gcd, so by well-ordering of $\mathbb{N}$ there is a finite subset T of S with $\gcd(T) = \gcd(S)$. By Step 1, $\langle T\rangle_{\mathbb{N}}$ is cofinite in $\gcd(S)\mathbb{N}$, while $M \subseteq \langle M\rangle_{\mathbb{Z}} \cap \mathbb{N} = \gcd(S)\mathbb{N}$, so $\langle T\rangle_{\mathbb{N}}$ is cofinite in S. Thus by adding to T all the elements of $M \setminus \langle T\rangle_{\mathbb{N}}$, we get a finite set of generators of M. This proves part c) and completes the proofs of parts a) and b). □

Now we give the proof of Shipman's Theorem.

PROOF. Let F be a field such that every polynomial in $F[t]$ of prime degree has a root in F. Seeking a contradiction, we assume that some positive degree polynomial in $F[t]$ has no root in F.
Step 1: As above, if F has characteristic $p > 0$, then for all $x \in F$ the polynomial $t^p - x \in F[t]$ has a root in F, so $F = F^p$ and F is perfect.
Step 2: Here is the key new idea: we claim there is a prime ℓ such that every positive degree polynomial $f \in F[t]$ without a root in F has degree divisible by ℓ. Indeed, suppose not: then some polynomial $f \in F[t]$ of degree $d \geq 1$ has no root in F; let the primes dividing d be $p_1, \ldots, p_n$. By assumption, there are polynomials $g_1, \ldots, g_n \in F[t]$ such that $d_i := \deg(g_i)$ is coprime to p_i. Then $M := \langle d, d_1, \ldots, d_n \rangle$ is a primitive numerical semigroup, so by Proposition 7.24 M is cofinite; thus there are $a, a_1, \ldots, a_n \in \mathbb{N}$ such that $p := ad + a_1 d_1 + \ldots + a_n d_n$ is prime. Thus $f^a g_1^{d_1} \cdots g_n^{d_n}$ has prime degree p but has no root in F: contradiction.
Step 3: By Step 1 and our assumption that F is not algebraically closed, there is a nontrivial finite Galois extension K/F. Let $G := \mathrm{Aut}(K/F)$, and let H_ℓ be a Sylow ℓ-subgroup of G. Then K^{H_ℓ}/F is a separable extension of degree $[G : H_\ell]$, so by the Primitive Element Corollary there is an irreducible polynomial $f \in F[t]$ of degree $[G : H_\ell]$. Since this is prime to ℓ, f must have a root in F, meaning $\deg(f) = 1$ and $G = H_\ell$ is an ℓ-group. As above, G has a normal subgroup H' of index ℓ, and then $K^{H'}/F$ is a separable extension of degree ℓ. Applying the Primitive Element Corollary again, we get an irreducible polynomial $f \in F[t]$ of prime degree ℓ: contradiction. □

The following exercises give a sense in which Shipman's Theorem is best possible.

Let p be a prime number. Let us say that a field F has property I_p if every irreducible polynomial in $F[t]$ has degree a power of p.

EXERCISE 7.13. *Suppose F has property I_p. Show: every polynomial in $F[t]$ of degree prime to p has a root in F.*

By Exercise 7.13, in a field F with property I_p that is not algebraically closed, every polynomial $f \in F[t]$ of prime degree $\ell \neq p$ has a root in F.

EXERCISE 7.14. *Suppose that F is separably closed but not algebraically closed (e.g. for any field k of characteristic p, take the separable closure of $k(t)$) of characteristic $p > 0$. Show: F is imperfect – hence not algebraicaly closed– and has property I_p.*

EXERCISE 7.15. *Let F be a field with algebraic closure $\overline{F}$. We say that F is a **perfect $\hat{\mathbb{Z}}$-field** if for all $n \in \mathbb{Z}^+$, there is a unique subextension F_n of $\overline{F}/F$ with $[F_n : F] = n$, and moreover each F_n/F is finite Galois.*

a) *Show: a perfect $\hat{\mathbb{Z}}$-field is perfect. (Thank goodness.)*
b) *(To be done after algebraic Galois extensions are studied.) Show: a perfect $\hat{\mathbb{Z}}$-field is precisely a perfect field K with $\mathrm{Aut}(\overline{F}/F) \cong \hat{\mathbb{Z}}$.*
c) *Show: a finite field is a perfect $\hat{\mathbb{Z}}$-field.*
d) *(For those who know about valuations and complete fields) Show: the Laurent series field $\mathbb{C}((t))$ is a perfect $\hat{\mathbb{Z}}$-field. (Cf. Example 8.31.)*
e) *Let F be a perfect $\hat{Z}$-field, and let p be a prime. Let $S_p(F)$ denote the union of $\bigcup F_n$ as n ranges over all positive integers that are coprime to*

p. Show: $S_p(F)$ is a perfect field satisfying property I_p such that for all $k \in \mathbb{Z}^+$ there is an irreducible polynomial $f \in F[t]$ of degree p^k.

This last exercise shows:

COROLLARY 7.25. *Let ℓ be a prime, and let p be either 0 or a prime. There is a perfect field F of characteristic p such that every polynomial $f \in F[t]$ of degree a prime different from ℓ has a root in F, but F for all $k \in \mathbb{Z}^+$ there is an irreducible polynomial $f_k \in F[t]$ of degree ℓ^k. In particular, F is not algebraically closed.*

I confess that I found the exposition in [**Sh07**] somewhat hard to follow. The proofs of some of the results other than the one given above seem faulty.[3] A much cleaner exposition of Theorem 7.23 was given by M. Aliabadi [**Al18**]. The main maneuver (Step 2) of the proof of Theorem 7.23 is clever (when I saw the statement, I tried to prove it myself for a while and did not succeed) but also in a way disappointing. In retrospect I was trying to prove a stronger result, which I will state as a question:

QUESTION 7.26. *Let F be a field such that every polynomial $f \in F[t]$ of prime degree is irreducible. Must F be algebraically closed?*

4. The Inverse Galois Problem

Let G be a finite group, and let F be a field. We say that **G occurs as a Galois group over F** if there is a finite degree Galois extension K/F with $\mathrm{Aut}(K/F) \cong G$.

The following striking result is remarkably easy to prove.

THEOREM 7.27. *Every finite group occurs as a Galois group over some field.*

PROOF. Step 1: Let $n \in \mathbb{Z}^+$, let k be any field, and let $K := k(t_1, \ldots, t_n)$ be the rational function field over k in the indeterminates $k_1, \ldots, k_n$. Then the symmetric group S_n naturally and effectively acts by automorphisms of K just by permutation of variables: $\sigma \in S_n$ maps t_i to $t_{\sigma(i)}$. By Proposition 7.9 and the remarks after its proof, the extension K/K^{S_n} is finite Galois with $\mathrm{Aut}(K/K^{S_n}) = S_n$.
Step 2: Let G be a finite group of order n. Without changing the isomorphism class of G we may assume that its underlying set is $\{1, \ldots, n\}$. Recall the **(left) Cayley map** $C : G \hookrightarrow S_n$, in which we map $g \in G$ to the bijection $g\cdot : h \mapsto gh$. Then C is an injective group homomorphism.[4] Then with $K = k(t_1, \ldots, t_n)$ as in Step 1, we have that $K/K^{C(G)}$ is a Galois extension with automorphism group $C(G) \cong G$. □

The catch in Theorem 7.27 is that the field F over which we realize G as a Galois group itself depends upon G in a rather complicated way. The case of symmetric groups is well understood: later on we will show that $k(t_1, \ldots, t_n)^{S_n} = k(s_1, \ldots, s_n)$, where for $1 \leq k \leq n$, $s_k(t_1, \ldots, t_n)$ is the **kth elementary symmetric function**: that is, we sum over all $\binom{n}{k}$ monomials of degree k in which each indeterminate t_i appears at most once. We will also show that these elementary symmetric functions

[3] Corollary 7.25 without the control on the characteristic is [**Sh07**, Thm. 3]. In the proof, he claims that the field F obtained by adjoining to $\mathbb{Q}$ all algebraic numbers whose minimal polynomial has degree prime to ℓ has no subextension with finite degree ℓ over $\mathbb{Q}$. This is false, because the compositum K_1K_2/F of two finite degree separable extensions K_1/F, K_2/F each of degree prime to ℓ must itself have degree prime to ℓ if both K_1 and K_2 are normal over F, but not generally otherwise.

[4] Treat this as an exercise if you haven't seen it before.

are algebraically independent (a concept that we will study in much more detail starting in Chapter 10): they satisfy no nonzero polynomial relation. This implies that K^{S_n} is itself a rational function field in n indeterminates, i.e., it is abstractly isomorphic to K. From this it follows easily that over a rational function field $k(t_1, \ldots, t_n, \ldots)$ in a countably infinite set of indeterminates, every finite symmetric group S_n occurs as a Galois group.

If now G is a subgroup of S_n, then G occurs as a Galois group over $k(t_1, \ldots, t_n)^G$, making it natural to ask whether this field is again isomorphic to $k(t_1, \ldots, t_n)$. This question was first raised by Emmy Noether and is called **Noether's Problem**. It lies miles deeper than anything we've mentioned in this text so far, lying in the subject of algebraic geometry (more specifically, when a unirational algebraic variety must be rational). In short, while it is certainly possible for $k(t_1, \ldots, t_n)^G$ to be a rational function field – e.g. when $G = S_n$ and in some other cases as well – it is much more likely that it isn't a rational function field.

For a field F, the **Inverse Galois Problem over F** is to determine which finite groups occur as Galois groups over F.

EXERCISE 7.16. *Let G be a finite group.*

a) *Show: G occurs over $\mathbb{R}$ if and only if $\#G \leq 2$.*
b) *Show: G occurs over $\mathbb{F}_q$ if and only if G is cyclic.*
c) *(For those who know about p-adic fields) Let $F/\mathbb{Q}_p$ be a finite degree field extension. Show: if G occurs over F, then G is solvable.*[5] *Show however that not every finite* commutative *group occurs over F.*

However, for a very large class of fields F, it is not known how to exclude any finite group as occurring as a Galois group over F, in which case the Inverse Galois Problem in practice takes on the form: prove (or disprove!) that *every* finite group occurs over F. For instance, this version of the Inverse Galois Problem is an open problem over $\mathbb{Q}$, over every number field, and over every field that is infinite and finitely generated over its prime subfield. Later, in Corollary 8.12 we will show that every finite *commutative* group occurs over $\mathbb{Q}$. To be sure, this result lies at the advanced undergraduate level. A much more serious result is Shafarevich's Theorem that every finite solvable group occurs over $\mathbb{Q}$ [**Sh54**]. (Shafarevich's original proof contains a mistake with respect to the prime 2. Various authors have explained how to fix it, including Shafarevich himself. We recommend the exposition of Schmidt–Wingberg [**SW98**].)

After solvable groups, it is natural to try to show that all finite simple groups occur over $\mathbb{Q}$, and then one can try to use this to show that every finite group over $\mathbb{Q}$. However, each of these steps remains mostly open. Just to say a few words about the first part: of the 26 sporadic simple groups, all are known to occur over $\mathbb{Q}$ except perhaps the Matthieu group M_{23}. For instance, that the Fischer–Griess "monster group" occurs over $\mathbb{Q}$ was shown by J.G. Thompson [**Th84**]. Hilbert showed that all the alternating groups A_n occur over $\mathbb{Q}$. The next infinite family of finite simple groups is $\mathrm{PSL}_2(\mathbb{F}_q)$ for a prime power q. For a long time people showed that $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs over $\mathbb{Q}$ for various conditions on the prime p (this includes work of Shih, Malle, Matzat and the present author), and then finally Zywina [**Zy15**] showed that $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs over $\mathbb{Q}$ for all primes p. At the time

[5]Solvable groups are covered from scratch in Chapter 9.

of this writing (July 2025), there is no $a \geq 2$ for which we know that $\mathrm{PSL}_2(\mathbb{F}_{p^a})$ occurs over $\mathbb{Q}$ for all primes p.

It follows from some basic results in topology and Riemann surface theory that every finite group occurs over $\mathbb{C}(t)$. Very roughly speaking: for $r \in \mathbb{Z}^+$, let $P_r(\mathbb{P}^1)$ denote a Riemann sphere with (any) $r+1$ points removed. The fundamental group of $P_r(\mathbb{P}^1)$ is a free group F_r on r generators, so every finite group G is a homomorphic image of F_r for all sufficiently large r. By covering space theory, there is a Galois covering $\pi : Y \to P_r(\mathbb{P}^1)$ with Y a connected topological surface and deck transformation group G. The covering map π can be used to endow Y with a holomorphic atlas, making it a noncompact connected Riemann surface. Then one version of *Riemann's Existence Theorem* asserts that there is a unique extension of π to a finite degree map $\overline{\pi} : \overline{Y} \to \mathbb{P}^1$ of compact Riemann surfaces. This makes the meromorphic funtion field $\mathbb{C}(\overline{Y})$ a finite Galois extension of $\mathbb{C}(\mathbb{P}^1) \cong \mathbb{C}(t)$ $\mathrm{Aut}(\mathbb{C}(Y)/\mathbb{C}(\mathbb{P}^1)) \cong G$.

We say that a finite group G **occurs regularly over a field** k if there is a finite Galois extension $K/k(t)$ with $\mathrm{Aut}(K/k(t)) \cong G$ that is moreover **regular** (see §11.6). For any field k, it is conjectured that every finite group occurs regularly over k (regularity is automatic if k is algebraically closed, so above we sketched the proof that every finite group occurs regularly over $\mathbb{C}$): this is called the **Regular Inverse Galois Problem** over k. Hilbert proved that if k is a number field, every regular finite Galois extension $K/k(t)$ induces a finite Galois extension l/k with $\mathrm{Aut}(l/k) \cong \mathrm{Aut}(K/k(t))$. Thus the Regular Inverse Galois Problem over $\mathbb{Q}$ implies the Inverse Galois Problem over $\mathbb{Q}$. Closely related to this is the fact that if Noether's problem has a positive solution for $G \subseteq S_n$, then G occurs regularly over k. Thus if Noether's Problem always had an affirmative solution, then every group would occur as a Galois group over $\mathbb{Q}$ (and over every number field). Although this turns out not to be the case, this is perhaps the "best swing" that has ever been taken at the Inverse Galois Problem over $\mathbb{Q}$.

EXERCISE 7.17. *Let K/F be a purely inseparable algebraic extension. Show: every finite group that occurs over F also occurs over K.*

EXERCISE 7.18. *Let F be a field such that every finite group occurs over F.*

a) *Show: every finite group G occurs infinitely many times over F: that is, inside $\overline{F}$, there is an infinite sequence $\{K_n\}_{n=1}^{\infty}$ of distinct finite Galois extensions of F such that $\mathrm{Aut}(K_n/F) \cong G$ for all $n \in \mathbb{Z}^+$.*

b) *Let K/F be a finite degree extension. Show: every finite group occurs as a Galois group over K.*

5. The Normal Basis Theorem

Let K/F be a finite degree field extension. Then a basis $\alpha_1, \ldots, \alpha_n$ of K as an F-vector space is a **normal basis** if all of its elements lie in the same $\mathrm{Aut}(K/F)$-orbit, i.e., if for all $1 \leq i \leq n$ there is $\sigma \in \mathrm{Aut}(K/F)$ such that $\alpha_i = \sigma\alpha_1$. We say that $\alpha \in K$ **induces a normal basis** if the G-orbit on α gives an F-basis for K. Thus a normal basis is induced by any of its elements.

EXERCISE 7.19. *Let K/F be a degree n field extension.*

a) *Suppose $\alpha_1, \ldots, \alpha_n$ is a normal basis for K/F. Show: K/F is Galois and its Galois group G acts simply transitively on $\alpha_1, \ldots, \alpha_n$.*
b) *Suppose K/F is Galois with Galois group G. Show: $\alpha \in K$ is a primitive element for K/F if and only if the G-orbit on α has size n.*

EXERCISE 7.20. *Let F be a field of characteristic different from 2, and let $K = F(\sqrt{d})$ be a quadratic extension. Let $G = \mathrm{Aut}(K/F)$. Let $\alpha = a + b\sqrt{d}$ with $a, b \in F$ be an arbitrary element of K.*

a) *Show: G fixes α if and only if $b = 0$.*
b) *Show: if $a = 0$ and $b \neq 0$, then the G-orbit on α has size $2 = \#G$, but α does* not *induce a normal basis.*
c) *Show: if $a, b \neq 0$, then α induces a normal basis.*

The previous exercises should serve to clarify the relationship between normal bases and primitive elements: every element of a normal basis is a primitive element, but the converse is not generally true: e.g. $\sqrt{2}$ is a primitive element for $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ despite $\sqrt{2}, -\sqrt{2}$ not being a normal basis.

The main result of this section is the converse of Exercise 7.19: every finite Galois extension admits a normal basis. A lot of literature has been written on this result. Our treatment follows [**CW50**] and [**We**, §3.6]. It is certainly not the shortest treatment available, but it proceeds by establishing several preliminary results which are of some interest in their own right.

Every known proof of the existence of normal bases must negotiate a fundamental dichotomy between finite fields and infinite fields. This dichotomy comes up several times in field theory, algebra and algebraic geometry (another good example of a theorem for which the finite field case must be taken separately is the **Noether Normalization Theorem**), but often without much fanfare our explanation. To our mind at least, the source of the trouble is the different behavior of the evaluation map on polynomials over finite domains versus infinite integal domains. (A geometer might point to the fact that for any $n \in \mathbb{Z}^+$, a field K is infinite if and only if the K-rational points of affine n-space over K are Zariski dense, but in fact this comes down to the same algebraic observation.)

LEMMA 7.28. *Let $R \subset S$ be an extension of domains and $n \in \mathbb{Z}^+$. The following are equivalent:*

(i) *For all $f \in S[t_1, \ldots, t_n]$, $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in R^n \implies f = 0$.*
(ii) *R is infinite.*

PROOF. (i) $\implies$ (ii): We prove the contrapositive. Note that any finite domain is a field, so suppose $R = \mathbb{F}_q$. Let $f(t) = t_1^q - t_1$. Then for all $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$, $f(a) = a_1^q - a_1 = 0$.
(ii) $\implies$ (i): We go by induction on n.
BASE CASE ($n = 1$): suppose $f \in S[t]$ is a polynomial which is not the zero polynomial. Then it has degree $d \geq 0$ and by the Root-Factor Theorem has at most d roots in the fraction field of R, hence *a fortori* at most d roots in R. But $\#R \geq \aleph_0 > d$, so there is $a_1 \in R$ with $f(a_1) = 0$.
INDUCTION STEP: Suppose $n > 1$ and that every polynomial in $n - 1$ variables with S-coefficients which is not the zero polynomial has a R-rational root.

Let $f(t_1, \ldots, t_{n-1}, z) \in S[t_1, \ldots, t_{n-1}, z]$. Put $S' = S[t_1, \ldots, t_{n-1}]$, so f may be identified with a nonzero polynomial $g(z) \in S'[z]$. Applying the Base Case, there is $A \in R'$ such that $0 \neq g(A) \in R'$. Now $g(A)$ is a nonzero element of $S' = S[t_1, \ldots, t_{n-1}]$, so by induction there exist $a_1, \ldots, a_{n-1} \in R$ such that $g(A(a_1, \ldots, a_{n-1})) \neq 0$. Putting $a_n = A(a_1, \ldots, a_{n-1})$ we have

$$f(a_1, \ldots, a_{n-1}, a_n) = g(A(a_1, \ldots, a_{n-1})) \neq 0. \qquad \square$$

PROPOSITION 7.29. *Let K/F be a finite Galois extension with cyclic Galois group. Then K/F admits a normal basis.*

PROOF. Let K/F be cyclic of degree n with $\mathrm{Aut}(K/F) = \langle \alpha \rangle$. We may endow K with the structure of an $F[t]$-module extending its F-module structure by putting $t \cdot x = \sigma(x)$ for all $x \in K$. Then $t^n - 1$ annihilates K; moreover, by linear independence of characters, no smaller degree polynomial does so. It follows that as an $F[t]$-module, K is isomorphic to $F[t]/(t^n - 1)$. Thus there is $\alpha \in K$ such that $\mathrm{ann}(\alpha) = (t^n - 1)$ – take, e.g., the preimage of 1 $(\mathrm{mod}\ t^n - 1)$ under an isomorphism – so the elements $\alpha, \sigma\alpha, \sigma^2\alpha, \ldots, \sigma^{n-1}\alpha$ are F-linearly independent and thus give a normal basis. $\square$

LEMMA 7.30. *Let K/F be a degree n Galois extension, and write $\mathrm{Aut}(K/F) = \{\sigma_i\}_{i=1}^n$. For $\alpha_1, \ldots, \alpha_n \in K$, the following are equivalent:*

(i) *$\alpha_1, \ldots, \alpha_n$ is an F-basis of K.*

(ii) *The matrix $A \in M_n(K)$ with $A_{ij} = \sigma_i \alpha_j$ is nonsingular.*

PROOF. (i) $\implies$ (ii) follows almost immediately from the (K-)linear independence of the characters $\sigma_1, \ldots, \sigma_n$: details are left to the reader.

(ii) $\implies$ (i): We argue by contraposition: suppose $\alpha_1, \ldots, \alpha_n$ is *not* an F-basis for K, so there exist $a_1, \ldots, a_n \in F$, not all zero, with $a_1\alpha_1 + \ldots + a_n\alpha_n = 0$. Then for all i we have

$$\sum_{j=1}^n a_j A_{ij} = \sum_{j=1}^n a_j \sigma_i \alpha_j = \sigma_i(\sum_{j=1}^n a_i \alpha_j) = 0,$$

which shows that the columns of the matrix A are linearly dependent. $\square$

By linear independence of characters, for any field extension K/F, any finite set of automorphisms $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}(K/F)$ is K-linearly independent. If K/F is a Galois extension **and F is infinite**, we have the following significantly stronger independence result.

THEOREM 7.31. *Let K/F be a finite Galois extension of infinite fields. Suppose $f \in K[t_1, \ldots, t_n]$ is a polynomial such that for all $\alpha \in K$, we have $f(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) = 0$. Then $f = 0$.*

PROOF. As a matter of notation, for an n-tuple $(x_1, \ldots, x_n) \in K^n$, we will denote by $(x_1, \ldots, x_n)^\bullet$ the corresponding column vector, i.e., element of $M_{n,1}(K)$. If it brings no confusion, we will suppress indices by writing $x^\bullet$ for $(x_1, \ldots, x_n)^\bullet$.

Let $\alpha_1, \ldots, \alpha_n$ be a basis for K/F. Define $A \in M_n(K)$ by $A_{ij} = \sigma_i \alpha_j$. By Lemma 7.30, A is nonsingular. Now let $c = (c_1, \ldots, c_n) \in F^n$ and put

$$\alpha = \sum_{j=1}^n c_j \alpha_j.$$

Then for all $1 \leq i \leq n$,

$$\sigma_i(\alpha) = \sum_{j=1}^{n} A_{ij} c_j,$$

so

$$\sigma(\alpha)^\bullet = Ac^\bullet.$$

Seeking a contradiction, we suppose that for all $\sigma \in K$, $f(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) = 0$. By the above, this can be reexpressed as

$$0 = f(\sigma(\alpha)^\bullet) = f(Ac^\bullet)$$

for all $c \in F^n$. Thus the polynomial

$$g(t) = g(t_1, \ldots, t_n) = f(At^\bullet) \in K[t_1, \ldots, t_n]$$

vanishes at every $c \in F^n$, so by Lemma 7.28, $g = 0$. So $f(t) = g(A^{-1}t^\bullet) = 0$. □

EXERCISE 7.21. *Show: the conclusion of Theorem 7.31 fails to hold for all extensions $\mathbb{F}_{q^n}/\mathbb{F}_q$ with $n \geq 2$.*

THEOREM 7.32. *(Normal Basis Theorem) Let K/F be a finite Galois extension of degree n. Then there is $\alpha \in K$ such that the set $\{\sigma(\alpha)\}_{\sigma \in \mathrm{Gal}(K/F)}$ is a basis of K as an F-vector space.*

PROOF. By Proposition 7.29 we may assume that F, and hence also K, is infinite. Write out the elements of $\mathrm{Aut}(K/F)$ as $1 = \sigma_1, \sigma_2, \ldots, \sigma_n$. Let $t_1, \ldots, t_n$ be independent indeterminates, and consider the matrix B with $B_{ij} = t_k$, where $\sigma_i \sigma_j = \sigma_k$. In this matrix each t_i appears exactly once in each row and column, so the specialization $t_1 = 1$, $t_i = 0$ for all $i > 1$ gives rise to a permutation matrix with determinant ± 1. It follows that $d(t_1, \ldots, t_n) = \det B$ is a nonzero element of the polynomial ring $K[t_1, \ldots, t_n]$. Applying Theorem 7.31, there is $\alpha \in K$ such that $d(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) \neq 0$.

For $1 \leq j \leq n$, put $\alpha_j = \sigma_j(\alpha)$. Then the matrix A with $A_{ij} = \sigma_i \alpha_j = \sigma_i \sigma_j \alpha = \sigma_k \alpha$ nonsingular, so by Lemma 7.30 $\sigma_1 \alpha, \ldots, \sigma_j \alpha$ is an F-basis of K. □

We want to end by mentioning an interpretation of the Normal Basis Theorem in the foundations of Galois cohomology. Let K/F be a finite degree field extension, and put $G \coloneqq \mathrm{Aut}(K/F)$. Then G acts on K by F-linear automorphisms, so K is naturally a module over the group ring $F[G]$. For those who are comfortable with the terminology, it is straightforward to see that $\alpha \in K$ induces a normal basis for K/F if and only if α is a generator for K as an $F[G]$-module. Thus the Normal Basis Theorem takes the equivalent form: K/F is Galois if and only if K is free of rank 1 as an $F[G]$-module.

6. Hilbert's Theorem 90

Let G be a group, and let M be a G-module, i.e., commutative group on which G acts $\mathbb{Z}$-linearly: that is, we are given a homomorphism $G \to \mathrm{Aut}_{\mathbb{Z}}(M)$. Let $Z^1(G, M)$ be the set of all maps $f : G \to M$ which satisfy the **cocycle condition**:

$$\forall \sigma, \tau \in G,\ f(\sigma\tau) = f(\sigma) + \sigma(f(\tau)).$$

Let $B^1(G, M)$ be the set of maps $f : G \to M$ such that there is $a \in M$ with $f(\sigma) = \sigma(a) - a$ for all $\sigma \in G$.

EXERCISE 7.22.

a) *Show:* $Z^1(G,M)$ *and* $B^1(G,M)$ *are commutative groups under pointwise addition.*
b) *Show:* $B^1(G,M) \subseteq Z^1(G,M)$.

We may therefore define

$$H^1(G,M) = Z^1(G,M)/B^1(G,M),$$

the **first cohomology group of G with coefficients in M**.

EXERCISE 7.23. *Suppose that* G *acts trivially on* M. *Show that* $H^1(G,M) = \mathrm{Hom}(G,M)$, *the group of all homomorphisms from* G *to* M.

Now observe that if K/F is a field extension and $G = \mathrm{Aut}(K/F)$, then both K (as an additive group) and $K^\times$ (as a multiplicative group) are G-modules.

THEOREM 7.33. *Let* K/F *be a finite Galois extension, with Galois group* $G = \mathrm{Aut}(K/F)$. *Then:*
a) *We have* $H^1(G,K) = 0$.
b) *We have* $H^1(G,K^\times) = 0$.

PROOF. a) Let $f : G \to K$ be a 1-cocycle. Since K/F is separable of finite degree, by Theorem 6.12 there is $c \in K$ with $\mathrm{Tr}_{K/F}(c) = 1$. Put

$$b = \sum_{\sigma \in G} f(\sigma)\sigma(c),$$

so

$$\tau(b) = \sum_{\sigma \in G} \tau(f(\sigma))(\tau\sigma)(c)$$

$$= \sum_{\sigma \in G} \left(f(\tau\sigma) - f(\tau)\right)(\tau\sigma)(c) = \sum_{\sigma \in G} f(\tau\sigma)(\tau\sigma)(c) - \sum_{\sigma \in G} f(\tau)(\tau\sigma)(c)$$

$$= b - f(\tau) \cdot \tau\left(\sum_{\sigma \in G} \sigma(c)\right) = b - f(\tau).$$

Thus $f(\tau) = b - \tau(b)$ for all $\tau \in G$, so $f \in B^1(G,K)$.
b) Let $f : G \to K^\times$ be a 1-cocycle. By independence of characters, there is $c \in K$ such that $\sum_{\sigma \in G} f(\sigma)\sigma(c) \neq 0$; fix such a c and put $b = \sum_{\sigma \in G} f(\sigma)\sigma(c)$. Then

$$\tau(b) = \sum_{\sigma \in G} \tau(f(\sigma))(\tau\sigma)(c),$$

so

$$f(\tau)\tau(b) = \sum_{\sigma \in G} f(\tau)\tau(f(\sigma)) \cdot (\tau\sigma)(c) = \sum_{\sigma \in G} f(\tau\sigma) \cdot (\tau\sigma)(c) = b,$$

i.e., $f(\tau) = b/\tau(b)$. So $f \in B^1(G,K^\times)$. □

The following is a basic result from group cohomology.

THEOREM 7.34. *Let* $n \in \mathbb{Z}^+$, *and let* $G = \langle \sigma \mid \sigma^n = 1 \rangle$ *be a finite cyclic group. For any* G*-module* M, *we have*

$$H^1(G,M) \cong \{x \in M \mid (1 + \sigma + \ldots + \sigma^{n-1})(x) = 0\}/\{\sigma x - x \mid x \in M\}.$$

Combining Theorems 7.33 and 7.34 we immediately deduce the following famous result of D. Hilbert, the 90th theorem in his *Zahlbericht*. However, because our focus here is on field-theoretic methods, we will not give a proof of Theorem 7.34 but rather a purely field-theoretic proof of Hilbert's Satz 90.

THEOREM 7.35. *(Hilbert's Satz 90) Let K/F be a finite Galois extension with cyclic Galois group $G = \langle \sigma \mid \sigma^n = 1 \rangle$.*

a) *For $c \in K$, the following are equivalent:*
   (i) $\mathrm{Tr}_{K/F}(c) = 0$.
   (ii) *There is $a \in K$ such that $c = a - \sigma(a)$.*

b) *For $c \in K$, the following are equivalent:*
   (i) $N_{K/F}(c) = 1$.
   (ii) *There is $a \in K^\times$ such that $c = \frac{a}{\sigma(a)}$.*

PROOF. Step 1: Because Galois conjugate elements have the same norm and trace, in both parts a) and b) the implications (ii) $\implies$ (i) are immediate.
Step 2: Let $c \in K$ be such that $\mathrm{Tr}_{K/F}(c) = 0$. Since K/F is separable, by Theorem 6.12 there is $b \in K$ with $\mathrm{Tr}_{K/F}(b) = 1$.[6]

Put

$$a = cb + (c + \sigma(c))\sigma(b) + \ldots + (c + \sigma(c) + \ldots + \sigma^{n-2}(c))\sigma^{n-2}(b).$$

Then

$$\sigma(a) = \sigma(c)\sigma(b) + (\sigma(c) + \sigma^2(c))\sigma^2(b) + \ldots + (\sigma(c) + \ldots + \sigma^{n-1}(c))\sigma^{n-1}(b).$$

Since $\mathrm{Tr}_{K/F}(c) = c + \sigma(c) + \ldots + \sigma^{n-1}(c) = 0$, we have

$$a - \sigma(a) = cb + c\sigma(b) + \ldots + c\sigma^{n-1}b = c\,\mathrm{Tr}_{K/F}(b) = c.$$

Step 3: Let $c \in K$ be such that $N_{K/F}(c) = 1$. By Dedekind's linear independence of characters, there is $b \in K$ with

$$a = b + c\sigma(b) + c\sigma(c)\sigma^2(b) + \ldots + c\sigma(c)\cdots\sigma^{n-2}(c)\sigma^{n-1}(b) \neq 0.$$

Then

$$c\sigma(a) = c\sigma(b) + c\sigma(c)\sigma^2(b) + \ldots + c\sigma(c)\cdots\sigma^{n-1}(c)b = a,$$

so

$$c = \frac{a}{\sigma(a)}.$$ □

We will use Theorem 7.35 later on in our study of cyclic extensions.

EXERCISE 7.24. *(Elkies) A **Pythagorean triple** is an ordered triple (x, y, z) of integers such that $x^2 + y^2 = z^2$. In this exercise we will use Theorem 7.35b) to determine all Pythagorean triples. Clearly the unique Pythagorean triple with $z = 0$ is $(0, 0, 0)$, so we may assume that $z \neq 0$. Let $F := \mathbb{Q}$, $K := \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$, let σ be the nontrivial element of $\mathrm{Aut}(K/F)$, and put*

$$w := \frac{x + iy}{z} \in K.$$

a) *Show: We have $N_{K/F}(w) = 1$, and deduce from Hilbert's Satz 90 that there is $c \in K$ such that $\frac{c}{\sigma(c)} = w$.*

b) *Show: there is $d = m + in \in \mathbb{Z}[i]$ such that $\frac{d}{\sigma(d)} = w$.*

c) *Calculate:*

$$\frac{x + iy}{z} = w = \frac{d}{\sigma(d)} = \frac{(m^2 - n^2) + i(2mn)}{m^2 + n^2}.$$

[6]Alternately, since K/F is Galois, we have $\mathrm{Tr}_{K/F}(x) = x + \sigma(x) + \ldots + \sigma^{n-1}(x)$. It follows from Dedekind's linear independence of characters that $\mathrm{Tr}_{K/F}$ is not identically zero, and since it is an F-linear functional it must then be surjective.

d) *Deduce: there is* $\alpha \in \mathbb{Q}^\times$ *such that* $\alpha(x,y,z) = (m^2-n^2, 2mn, m^2+n^2)$. *This classifies Pythagorean triples up to scaling.*

e) *A Pythagorean triple* (x,y,z) *is* ***primitive*** *if* $\gcd(x,y,z) = 1$. *Every Pythagorean triple is a primitive Pythagorean triple scaled by* $\alpha \in \mathbb{Z}^+$.

(i) *Show: if* (x,y,z) *is a primitive Pythagorean triple, then* x *and* y *have opposite parity (i.e., one is even and the other is odd). Since also* (y,x,z) *is a primitive Pythagorean triple, we may assume without loss of generality that* x *is odd.*

(ii) *Show: every primitive Pythagorean triple* (x,y,z) *with* x *odd is of the form* $(m^2-n^2, 2mn, m^2+n^2)$ *for coprime* $m, n \in \mathbb{Z}$ *of opposite parity.*

EXERCISE 7.25. *Explore various generalizations of Exercise 7.24, for instance:*

a) *(Elkies) Consider rational and integer solutions to* $q(x,y,z) = ax^2+bxy+cxz+dy^2+eyz+fz^2 = 0$.

b) *Consider Pythagorean triples* (x,y,z) *with* $x^2+y^2=z^2$ *over a field other than* $\mathbb{Q}$.

7. Algebraic Galois Extensions

In this section we extend the notion of "Galois extensions" from finite degree extensions to all algebraic extensions. In so doing we find ourselves in a common situation in modern mathematics: for a finite degree field extension K/F, we gave a definition of what it means to be Galois – namely (i) $K^{\mathrm{Aut}(K/F)} = F$ – but in Theorem 7.11 we found that this condition is equivalent to several other conditions: (ii) being normal and separable, (iii) being the splitting field of an irreducible, separable polynomial, and (iv) having $\#\,\mathrm{Aut}(K/F) = [K:F]$. Now we wish to extend the notion of Galois to infinite degree algebraic extensions, and the questions are: which of the conditions are meaningful in this more general context; which of them remain equivalent; and if they are not all equivalent, which should we take as the definition of "Galois"?

The condition $K^{\mathrm{Aut}(K/F)} = F$ makes sense for *any* field extension K/F, though we must understand that in general $\mathrm{Aut}(K/F)$ may be infinite, whereas as we will see shortly, if G is an infinite group of automorphisms of a field K, then we need not have $\mathrm{Aut}(K/K^G) = G$.

The condition (ii) K/F is normal and separable makes sense immediately, because we defined normality and separability for all algebraic extensions. See in particular Theorem 3.15, which gives equivalent conditions for an algebraic field extension to be normal, one of which is that K/F is the splitting field of a *set* of polynomials $\mathcal{S} \subseteq F[t]$ (and clearly we can require the elements of $\mathcal{S}$ to be irreducible). Similarly, Theorem 4.14 gives equivalent conditions for an algebraic field extension K/F to be separable, one of which is that K is obtained from F by adjoining roots of separable polynomials. Condition (iii) makes sense for algebraic field extensions, but clearly the extension obtained by adjoining the roots of a single polynomial has finite degree. In light of the discussion about condition (ii), it is clear how to modify condition (iii) for algebraic extensions: namely, we require K/F to be the splitting field of a set of irreducible separable polynomials (or equivalently, of a set of separable polynomials): it is then clear that (ii) $\iff$ (iii).

Indeed, we can now show that conditions (i), (ii) and (iii) are equivalent, and we define an algebraic extension to be Galois if it satisfies any one of them.

THEOREM 7.36. *For an algebraic field extension K/F, the following are equivalent:*

(i) $K^{\mathrm{Aut}(K/F)} = F$.
(ii) *K/F is normal and separable.*
(iii) *K/F is the splitting field of a set (possibly infinite) of separable polynomials.*

If K/F satisfies these equivalent conditions, we say that it is a ***Galois extension****.*

PROOF. (i) $\implies$ (ii): Let $\alpha \in K$. For all $\sigma \in \mathrm{Aut}(K/F)$, the element $\sigma(\alpha)$ is a conjugate of α, i.e., a root of the minimal polynomial of α over F. Let $\alpha = \alpha_1, \alpha_2, \alpha_n$ be the distinct elements of the set $\{\sigma(\alpha) \mid \sigma \in \mathrm{Aut}(K/F)\}$. Put

$$f \coloneqq \prod_{i=1}^{n}(t - \alpha_i) \in K[t].$$

If $\sigma \in \mathrm{Aut}(K/F)$ then σ permutes the α_i's hence fixes each coefficient of f, so $f \in K^{\mathrm{Aut}(K/F)}[t] = F[t]$. By construction f is separable and splits in K. It follows that K/F is normal and separable.
(ii) $\implies$ (i): Let $\alpha \in K \setminus F$. Then the minimal polynomial P for α over K splits in K and has at least one other distinct root β. There is a unique F-algebra embedding $\sigma : F[\alpha] \to K$ that sends α to β; as usual, we can extend σ to an automorphism of $\overline{F}$ and then the restriction of σ to K is an automorphism of K (since K is normal) for which $\sigma(\alpha) \neq \alpha$. Therefore $K^{\mathrm{Aut}(K/F)} = F$.
(ii) $\iff$ (iii): This equivalence was established above. □

Let us now revisit the abstraction of §7.1 in the somewhat less trivial present framework: $X = K = F^{\mathrm{sep}}$, $G = \mathrm{Aut}(K/F)$. Then the maps $L \mapsto \mathrm{Gal}(K/L)$ and $H \mapsto K^H$ give a bijective correspondence between **closed** subextensions L of K/F and **closed** subgroups H of G. The key fact is the following

LEMMA 7.37. *Let L/F be an algebraic Galois extension, and let K be a subextension that is also Galois over F. Then the natural map*

$$\mathrm{Aut}(L/F) \to \mathrm{Aut}(K/F)$$

obtained by restricting automorphisms of L to the normal extension K is surjective.

PROOF. Let $\sigma \in \mathrm{Aut}(K/F)$, and let $\overline{F}$ be an algebraic closure of F containing L. We may regard σ as giving an F-algebra embedding $K \hookrightarrow \overline{F}$, which by the Magic Mapping Theorem extends to an element $\tilde{\sigma} \in \mathrm{Aut}(\overline{F}/F)$. Since L/F is normal, we have $\tilde{\sigma}(K) = K$. □

EXAMPLE 7.38. *Let p be a prime number, le $\mathbb{F}_p$ be the field of order p, and let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$. The extension $\overline{\mathbb{F}_p}/\mathbb{F}_p$ is Galois, because it is normal and separable (note that the same holds $\overline{F}/F$ if and only if F is perfect). In §5.5 we saw that $\overline{\mathbb{F}_p} = \bigcup_{n\geq 1} \mathbb{F}_{p^n}$. Now is the time to rewrite the union as a direct limit:*

$$\overline{\mathbb{F}_p} = \varinjlim_n \mathbb{F}_{p^n}.$$

For $n \in \mathbb{Z}^+$, we know that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a degree n Galois extension, with $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ generated by the Frobenius map $\mathfrak{f} : x \mapsto x^p$. Thus we have a canonical isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ obtained by mapping 1 to $\mathfrak{f}$. Let us use this isomorphism to identify these groups.

For positive integers $m \mid n$, we have $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, which gives rise to a surjective group homomorphism

$$\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) \twoheadrightarrow \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p),$$

which via the above identification we may write as a surjective homomorphism

$$q_{n,m} : \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}. \tag{14}$$

Indeed, because the canonical generator of the first group is the Frobenius map acting on $\mathbb{F}_{p^n}$, which restricts to the Frobenius map acting on $\mathbb{F}_{p^m}$, which is the canonical generator of the second group, the map $q_{n,m}$ in (14) is the usual quotient map.
Now let $\sigma \in \mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$. For $n \in \mathbb{Z}^+$, we have a restriction map

$$r_n : \mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \twoheadrightarrow \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$$

that is surjective by Lemma 7.37. If $m \mid n$, then $q_{n,m} \circ r_n$ is just restricting to $\mathbb{F}_{p^n}$ and then to $\mathbb{F}_{p^m}$, so we have

$$r_m = q_{n,m} \circ r_n.$$

By the universal property of inverse limits, this gives us a homomorphism

$$\hat{r} : \mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \to \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}.$$

We claim that $\hat{r}$ is an isomorphism.
Injectivity of $\hat{r}$: if σ lies in the kernel of $\hat{r}$, then for all $n \in \mathbb{Z}^+$ we have $r_n(\sigma) = 0$, which means that σ fixes every element of $\mathbb{F}_{p^n}$. Since this holds for all n, we get that σ pointwise fixes every element of $\overline{\mathbb{F}_p}$, so $\sigma = 1$.
Surjectivity of $\hat{r}$: an element of $\hat{\mathbb{Z}}$ is a sequence $\{\sigma_n\}$ with $\sigma_n \in \mathbb{Z}/n\mathbb{Z}$ such that for all $m \mid n$ we have that $\sigma_n \pmod m = \sigma_m$. We can then define $\sigma \in \mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ as follows: if $x \in \mathbb{F}_{p^n}$, then $\sigma(x) := \sigma_n(x)$. The point is that the compatibility condition on the σ_n's makes this well-defined, and it is straightforward to check that this gives a field automorphism.

Thus we have shown that

$$\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}},$$

where by equality we mean the canonical isomorphism we have constructed. We observe that the group $\hat{\mathbb{Z}}$ has continuum cardinality: for instance, if $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, then we have $\hat{\mathbb{Z}} = \prod \mathbb{Z}_p$, where the product is indexed by the prime numbers. Each group $\mathbb{Z}_p$ has continuum cardinality: now our indexing set is $\mathbb{Z}^+$ under its usual, total, ordering, so to determine an element of $\mathbb{Z}_p$ we start with an element of $\mathbb{Z}/p\mathbb{Z}$ – p choices – then lift to an element of $\mathbb{Z}/p^2\mathbb{Z}$ – p choices – and so forth. We get a bijection of $\mathbb{Z}_p$ with $(\mathbb{Z}/p\mathbb{Z})^{\aleph_0}$, which has cardinality $\mathfrak{c} = 2^{\aleph_0}$, so

$$\#\hat{\mathbb{Z}} = \#\prod_p \mathbb{Z}_p = \mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \times \aleph_0} = 2^{\aleph_0} = \mathfrak{c}.$$

On the other hand, $\overline{\mathbb{F}_p}$ is a countable infinite $\mathbb{F}_p$-vector space, so $[\overline{\mathbb{F}_p} : \mathbb{F}_p] = \aleph_0$. Thus for this Galois extension K/F with $K = \overline{\mathbb{F}_p}$ and $F = \mathbb{F}_p$, we have

$$[K : F] = \aleph_0 < \mathfrak{c} = \#\,\mathrm{Aut}(K/F).$$

Thus the cardinal analogue of condition (iv) of Theorem 7.11 does not *hold here.*

The integers $\mathbb{Z}$ form a subgroup of $\hat{\mathbb{Z}}$: to $N \in \mathbb{Z}$ we attach the compatible sequence $\{\mathbb{N} \pmod n\}$. Under the canonical isomorphism from $\mathrm{Aut}(\overline{\mathbb{F}_p}/\mathbb{F}_p) = \hat{\mathbb{Z}}$, the element 1 corresponds to the Frobenius automorphism $x \mapsto x^p$ on $\overline{\mathbb{F}_p}$. Because $\overline{\mathbb{F}_p}/\mathbb{F}_p$ is Galois, we have

$$\overline{\mathbb{F}_p}^{\hat{\mathbb{Z}}} = \mathbb{F}_p.$$

On the other hand, for any perfect field F of characteristic p, the fixed field of the Frobenius automorphism $x \mapsto x^p$ is $\mathbb{F}_p$, hence also

$$\overline{\mathbb{F}_p}^{\mathbb{Z}} = \mathbb{F}_p.$$

This shows that the most naive generalization of the finite Galois correspondence to algebraic Galois extensions cannot hold, since we have a Galois extension K/F and two different subgroups of $\mathrm{Aut}(K/F)$ with the same fixed field.

A partially ordered set $(X, \leq)$ is **directed** if for all $x, y \in X$ there is $z \in X$ with $x, y \leq z$. Any totally ordered set is directed, as is any lattice. A partially ordered set $(X, \leq)$ is **anti-directed** if for all $x, y \in X$ there is $z \in X$ with $z \leq x, y$.

A large part of Example 7.38 applies to any algebraic Galois extension K/F:

LEMMA 7.39. *Let K/F be an algebraic Galois extension. Let I be the set of subextensions F_i of L/F such that F_i/F is finite Galois, partially ordered by inclusion. Then:*

a) *The partially ordered set I is directed.*
b) *We have $K = \varinjlim_{i \in I} F_i$. That is, K is the direct limit of its finite Galois subextensions.*
c) *We have a canonical automorphism $\mathrm{Aut}(K/F) = \varprojlim_{i \in I} \mathrm{Aut}(F_i/F)$. That is, the F-algebra automorphism group of K is the inverse limit of the F-algebra automorphism groups of its finite Galois subextensions.*

EXERCISE 7.26. *Prove Lemma 7.39.*

PROPOSITION 7.40. *Let K/F be an algebraic Galois extension, and put $G := \mathrm{Aut}(K/F)$. Let $\mathcal{L}(K/F)$ denote the set of subextensions L of K/F, and let $\mathcal{L}(G)$ denote the set of subgroups of G, partially ordered under inclusion in both cases.*

a) *Let $L \in \mathcal{L}(K/F)$, and put $H := \mathrm{Aut}(K/L)$. Let*

$$G_L := \{\sigma \in G \mid \sigma(L) = L\}.$$

Then G_L is the normalizer $N_G(H)$ of H in G.
b) *For $i = 1, 2$, let $L_i \in \mathcal{L}(K/F)$, and put $H_i := \mathrm{Aut}(K/L_i)$. Then for all $\sigma \in G$, we have*

$$\sigma(L_1) = L_2 \iff H_2 = \sigma H_1 \sigma^{-1}.$$

In particular, L_1 and L_2 are conjugate subfields of K/F – i.e., there is $\sigma \in G$ such that $\sigma(L_1) = L_2$ – if and only if H_1 and H_2 are conjugate subgroups of G.
c) *For $L \in \mathcal{L}(K/F)$, the extension L/F is Galois if and only if the subgroup $H := \mathrm{Aut}(K/L)$ is normal in G, in which case $\mathrm{Aut}(L/F)$ is canonically isomorphic to the quotient group G/H.*

PROOF. The statements of Proposition 7.40 are precisely the statements of parts b), c) and d) of Theorem 7.14 except that the hypothesis that K/F is finite Galois has been weakened to being algebraic Galois. As we ask the reader to check, the proofs of these last three parts of Theorem 7.14 simply do not use the hypothesis that K/F has finite degree, so they work verbatim to show the current result.[7] □

PROPOSITION 7.41. *Let K/F be an algebraic Galois extension, and let L be a subextension of K/F of finite degree over F.*

a) *The extension L/F is Galois if and only if $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Aut}(K/F)$, in which case we have a canonical isomorphism*

$$\mathrm{Aut}(K/F)/\mathrm{Aut}(K/L) \xrightarrow{\sim} \mathrm{Aut}(L/F). \tag{15}$$

b) *We have*

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

PROOF. Part a) simply records an important case of Proposition 7.40.
b) When L/F is normal, the result is immediate from (15). In general, let M be the Galois closure of the finite degree separable extension L/F. Since $\mathrm{Aut}(K/M)$ has finite index in $\mathrm{Aut}(K/F)$ and $\mathrm{Aut}(K/L)$ contains $\mathrm{Aut}(K/M)$, also $\mathrm{Aut}(K/K)$ has finite index in $\mathrm{Aut}(K/F)$. Moreover M/F and M/L are finite Galois, so

$$[L : F] = \frac{[M : F]}{[M : L]} = \frac{[\mathrm{Aut}(K/F) : \mathrm{Aut}(K/M)]}{[\mathrm{Aut}(K/L) : \mathrm{Aut}(K/M)]} = [\mathrm{Aut}(K/F) : \mathrm{Aut}(K/L)]. \quad \square$$

COROLLARY 7.42. *Let K/F be an algebraic Galois extension. The correspondence $L \mapsto \mathrm{Aut}(K/L)$ is an antitone injection from the set of finite degree subextensions of K/F to the set of finite index subgroups of $G := \mathrm{Aut}(K/F)$.*

PROOF. The antitone part of the assertion is immediate: indeed, for *any* field extensions $F \subseteq L_1 \subseteq L_2 \subseteq K$, we clearly have $\mathrm{Aut}(K/L_2) \subseteq \mathrm{Aut}(K/L_1)$. It remains to show that if L_1 and L_2 are finite degree subextensions of the algebraic Galois extension K/F such that $\mathrm{Aut}(K/L_1) = \mathrm{Aut}(K/L_2)$, then $L_! = L_2$. Let $\sigma \in \mathrm{Aut}(K/L_1)$. Since also $\sigma \in \mathrm{Aut}(K/L_2)$, we have $\sigma \in \mathrm{Aut}(K/L_1L_2)$, hence $\mathrm{Aut}(K/L_1) \subseteq \mathrm{Aut}(K/L_1L_2)$; since we certainly also have $\mathrm{Aut}(K/L_1L_2) \subseteq \mathrm{Aut}(K/L_1)$, we find that

$$\mathrm{Aut}(K/L_1) = \mathrm{Aut}(K/L_1L_2).$$

Applying Proposition 7.41b), we get

$$[L_1 : F] = [L_1L_2 : F],$$

hence $L_2 \subseteq L_1$. Interchanging L_1 and L_2 in this argument gives: $L_1 = L_2$. □

8. Interlude on Profinite Groups

8.1. Profinite Structures. Roughly speaking, a group G is "profinite" if it is an inverse limit of $\varprojlim G_i$ of finite groups. The culprit in the previous sentence is the word "is": if we interpret "is" as *equal* then we have defined a class of groups that is not isomorphism-invariant: this is never a best practice. If we interpret "is" as *isomorphic to* then we are actually doing something subtly wrong, thuogh it will

[7] This seems to suggest that while the name "Fundamental Theorem of Galois Theory" has been applied to all of Theorem 7.14, in truth it is part a) that is fundamental, while the other parts are more "formal". Our treatment of infinite Galois extensions will bear out this suggestion.

take a little while to explain wrong. Instead, we define a **profinite structure** on a group G to a family $\{H_i\}_{i \in I}$ of finite index normal subgroups H_i of G, directed under reverse inclusion, such that the induced homomorphism $\iota : G \to \varprojlim G/H_i$ is an isomorphism. As motivation for this definition, let K/F be an algebraic Galois extension. Then Lemma 7.39 shows that if $\{F_i\}_{i \in I}$ is the family of all finite Galois subextensions of K/F, then $\{\mathrm{Aut}(K/F_i)\}_{i \in I}$ is a profinite structure on $\mathrm{Aut}(K/F)$.

Given a profinite structure $\{H_i\}_{i \in I}$ on a group G, we will endow G with a natural topology that makes it into a compact Hausdorff topological group. Indeed it suffices to endow $\varprojlim G/H_i$ with such a topology, and then we "transport it" to G via ι: a subset U of G is open if and only if $\iota(U)$ is open in $\varprojlim G/H_i$.

Especially, for an algebraic Galois extension K/F, Lemma 7.39 gives us a canonical isomorphism $\mathrm{Aut}(K/F) \xrightarrow{\sim} \varprojlim \mathrm{Aut}(F_i)/F)$, where F_i ranges over finite Galois subextensions of K/F. This profinite structure on $\mathrm{Aut}(K/F)$ endows it with a topology, the **Krull topology**, in which a neighborhood base at e is given by

$$\{\mathrm{Aut}(K/F_i) \mid \ F_i/F \text{ is a finite degree normal subextension of } K/F\}.$$

As we saw in Example 7.38, for infinite degree algebraic Galois extensions K/F, multiple subgroups of $\mathrm{Aut}(K/F)$ can have the same fixed field. (In fact, as we will see later, this for for *every* algebraic Galois extension of infinite degree.) The Krull topology will repair this, giving an antitone bijection between subextensions L of K/F and **closed** subgroups of $\mathrm{Aut}(K/F)$.

Let I be a directed set, and let $\{G_i\}_{i \in I}$ be an inverse system of groups with surjective transition maps $q_{j,i} : G_j \to G_i$. We endow each G_i with the discrete topology and then endow the Cartesian product $\prod_{i \in I} G_i$ with the product topology. This is a product of totally disconnected Hausdorff spaces, hence is totally disconnected Hausdorff: indeed, let X be a connected (nonempty!) subset of $\prod_{i \in I} G_i$, and for $i \in I$, let $\pi_i : \prod_{i \in I} G_i \to G_i$ be projection onto the ith factor. Then $\pi_i(X)$ is a nonempty connected subset of a totally disconnected space, so must be a singleton set $\{x_i\}$, which implies that $X = \{(x_i)_{i \in I}\}$.

Exercise 7.27. *With notation as above, show that the inverse limit $\varprojlim G_i$ is closed in the Cartesian product $\prod_{i \in I} G_i$.*

Exercise 7.28. *Let G be a topological group, and let H be a subgroup of G.*

a) *If H is an open, show that H is also closed.*
b) *Suppose that G is compact and H is closed. Show: H is open if and only if $[G : H]$ is finite.*
c) *Suppose that H is open and that $\tilde{H}$ is a subgroup containing H. Show: $\tilde{H}$ is open.*

Exercise 7.29. *Let G be a topological group, let X be a set, and let $\cdot : G \times X \to X$ be an action.*

a) *Endow X with the discrete topology. Show: the action is continuous if and only if for all $x \in X$, the stabilizer Stab_x is an open subgroup of X.*
b) *Let K/F be an algebraic Galois extension. Let $G := \mathrm{Aut}(K/F)$, endowed with the Krull topology. Endow K with the discrete topology. Show: the natural action of G on K is continuous.*

Now suppose that each G_i is finite. Then each G_i is compact Hausdorff, hence the product space $\prod_{i\in I} G_i$ is compact Hausdorff by Tychonoff's Theorem, and by Exercise 7.27 the closed subspace $\varprojlim G_i$ is compact Hausdorff and, being a subspace of a totally disconnected space, is also totally disconnected. Thus a profinite structure on a group G endows G with the structure of a totally disconnected compact Hausdorff topological group. Rather remarkably, the converse is true: if G is a totally disconnected compact Hausdorff topological group, then the family of open normal subgroups of G is a profinite structure of G that induces the given topology on G. More precisely we have the following result:

THEOREM 7.43. *For a Hausdorff topological group G, the following are equivalent:*

(i) *G is isomorphic as a topological group to an inverse limit of finite discrete groups.*
(ii) *G is totally disconnected and compact.*
(iii) *The identity element e of G admits a neighborhood basis of the form $\{H_i\}_{i\in I}$ with each H_i an open normal subgroup of finite index.*
(iv) *The identity element e of G admits a basis of the form $\{H_i\}_{i\in I}$ with each H_i an open normal subgroup of finite index and G is isomorphic as a topological group to $\varprojlim G/H_i$.*

PROOF. This is [**RS**, Thm. 2.1.3]. □

This finally leads us to the correct definition of a **profinite group**: this is a *topological group G* that is totally disconnected and compact Hausdorff. Thus the topology on any profinite group G comes from a profinite struture on G, and the topology induced by a profinite structure on an abstract group G makes G into a profinite group. For a profinite group G, the family of all open normal subgroups of G is the unique maximal profinite structure on G that induces the given topology on G; more generally, two profinite structures $\{H_i\}_{i\in I}$ and $\{K_j\}_{j\in J}$ on the same abstract group G induce the same profinite topology on G if and only if each is *cofinal* in the other under reverse inclusion: for all $i \in I$ there is $j \in J$ such that $K_j \subseteq H_i$ and for all $j \in J$ there is $i \in I$ such that $H_i \subseteq K_j$.

For a topological group $G = \varprojlim G_i$ and $i \in I$, and let $\pi_i : G \to G_i$ be the projection map. By [**RS**, Prop. 1.1.0], π_i is surjective, so its kernel U_i is a normal subgroup that is closed of finite index, hence open. The subgroups U_i form a neighborhood basis of the identity e of G. Indeed, a base for e in $\prod_{i\in I} G_i$ consists of subsets of the form $\prod_{j\in J}\{e_j\} \times \prod_{i\in I\setminus J} G_i$ as J ranges over finite subsets of I. Intersecting with G, we get a base of i consisting of finite intersections $U^J := \bigcap_{j\in J} U_j$ of the subgroups U_i. However, because I is directed we can choose $i \in I$ such that $i \geq j$ for all $j \in J$ and then $U_i \subseteq U^J$. It follows that a subgroup H of G is open if and only if it contains U_i for some $i \in I$.

THEOREM 7.44. *Let H be a closed subgroup of a profinite group G. Let $\{X_i\}_{i\in I}$ be a nonempty family of nonempty closed subsets of G that is anti-directed under inclusion (that is, for all $i, j \in I$, there is $k \in I$ such that $X_k \subseteq X_i \cap X_j$).*

a) *Then*

$$\bigcap_{i\in I} HX_i = H\left(\bigcap_{i\in I} X_i\right). \tag{16}$$

b) *The closed subgroup H is the intersection of all open subgroups of G that contain it. It H is moreover normal, then it is the intersection of all open normal subgroups of G that contain it.*

c) *As N ranges over all open normal subgroups of G, we have $H = \bigcap_N HN$.*

PROOF. a) A finite nonempty antidirected set has a minimum, so if I is finite there is some $i \in I$ such that $X_i \subseteq X_j$ for all $j \in I$ and then both sides of (16) are HX_i. In the general case the containment $\bigcap_{i\in I} HX_i \supseteq H\left(\bigcap_{i\in I} X_i\right)$ is clear, so let $x \in \bigcap_{i\in I} HX_i$, and let $\{J_t\}_{t\in T}$ be the set of all finite subsets J_t of I such that $\{X_j \mid j \in J_t\}$ is anti-directed. So for each $t \in T$, we have

$$x \in \bigcap_{j\in J_t} HX_j = H\left(\bigcap_{j\in J_t} X_j\right),$$

hence $Hx \cap \left(\bigcap_{j\in J_t} X_j\right)$ is a nonempty closed subset of the compact space G. The finite intersection property for closed subsets of a compact space gives

$$Hx \cap \left(\bigcap_{i\in I} X_i\right) = \bigcap_{t\in T} (Hx \cap \left(\bigcap_{j\in J_t} X_j\right) \neq \varnothing,$$

so $x \in H\left(\bigcap_{i\in I} X_i\right)$.

b) Let $\{X_i\}_{i\in I}$ be the family of all open normal subgroups of G; this is a family of closed subsets that is closed under pairwise intersections hence is anti-directed under inclusion, and we have $\bigcap_{i\in I} X_i = \{e\}$, so applying part a) gives

$$H = \bigcap_{i\in I} HX_i.$$

Since each HX_i is an open subgroup, this shows that H is the intersection of the open subgroups that contain it. If moreover H is normal then so is each HX_i, so H is the intersection of the open normal subgroups that contain it.

c) By part b), it is enough to show: for every open subgroup U containing H, there is an open normal subgroup N such that $HN \subseteq U$. The normal core $\mathrm{Core}(U)$ is an intersection of finitely many conjugates of U, so is an open normal subgroup of G contained in U. Thus $H\,\mathrm{Core}(U) \subseteq U$. □

EXERCISE 7.30. *Let H be a subgroup of a profinite group G. Show: the closure $\overline{H}$ of H in G is the intersection of all open subgroups of G that contain H.*

EXERCISE 7.31. *Let N be a closed normal subgroup of a profinite group G. Show: the natural map $G/N \to \varprojlim G/U$ – where we range over open normal subgroups of G containing N – is an isomorphism of topological groups. Thus G/N is a profinite group.*

8.2. The Waterhouse–Milne Theorem. We now give a generalization of Artin's key result (Proposition 7.9) that for a finite group G of automorphisms of a field K, we have that K/K^G is finite Galois with Galois group G. As we mentioned in Example 7.38 above, a naive generalization of this to infinite groups fails: we may have $\mathrm{Aut}(K/K^G) \supsetneq G$ (and moreover we may have that K/K^G is transcendental; more on this once we study transcendental extensions in earnest). It turns out, not for the first time, that the statement can be repaired via topology:

THEOREM 7.45 (Waterhouse–Milne). *Let G be a compact Hausdorff topological group acting effectively by automorphisms on a field K, and assume that the action is continuous when K is given the discrete topology. Then:*

a) *The extension K/K^G is an algebraic Galois extension.*
b) *The inclusion map map $G \hookrightarrow Aut(K/K^G)$ is an isomorphism of topological groups.*

PROOF. Let $x \in K$. By Exercise 7.29, the stabilizer H_x of x in G is open, hence has finite index since G is compact, and thus the G-orbit on x is finite by the Orbit-Stabilizer Theorem. The conjugates of H_x in G are precisely the stabilizers of the points in the G-orbit of x, so they are finite in number, and thus the normal core $\mathrm{Core}(H_x)$ is an open subgroup of G. Let $X \subseteq K$ be any finite G-stable subset. The subgroup

$$N_X := \mathrm{Aut}(K/K^G(X))$$

is the kernel of the G-action on $K^G(X)$, so is a normal subgroup of G. Because

$$N_X \supseteq \bigcap_{x \in X} \mathrm{Core}(H_x)$$

an the latter is an open subgroup, it follows that N_X is an open normal subgroup of G. Thus the finite group G/N_X acts on $K^G(X)$ and we have

$$(K^G(X))^{G/N_X} = K^G.$$

By Proposition 7.9, the extension $K^G(X)/K^G$ is finite Galois with Galois group G/N_X. Thus the extension $K = \varinjlim_X K^G(X)$ is a direct limit of finite Galois extensions, hence is an algebraic Galois extension, with

$$\mathrm{Aut}(K/K^G) = \varprojlim_X G/N_X.$$

Viewed as a subgroup of $\varprojlim_X G/N_X$, the group G is on the one hand dense and on the other hand, being a compact subset of a Hausdorff space, closed, hence $G = \varprojlim_X G/N_X$. Moreover the map $G \to \varprojlim_X G/N_X$ is a continuous bijection from a compact space into a Hausdorff space, so it is a closed map, hence a homeomorphism. □

EXERCISE 7.32. *Let G be a profinite group. Show: the following are equivalent:*

(i) *The topology on G is induced by a countable profinite structure.*
(ii) *Either G is finite or G is homeomorphic to the Cantor set.*
(iii) *G is metrizable.*
(iv) *G is second countable.*
(v) *G is separable.*
(vi) *G is first countable.*

A profinite group satisfying these equivalent conditions is called ***countably based****.*

EXERCISE 7.33. *Let K/F be an algebraic Galois extension, with F a countable field.*

a) *Show: K is also a countable field.*
b) *Show: the profinite group $\mathrm{Aut}(K/F)$ is countably based.*

8.3. Profinite orders, profinite indices and profinite Sylow theory. Let G be a profinite group. Like any compact space, G is discrete if and only if it is finite. In this case the topology places no limitations on $\#G$, and of course there are finite groups of cardinality n for all $n \in \mathbb{Z}^+$. The situation is quite different when G is infinite. Then G cannot have any isolated points: indeed because G acts transitively on iself by homeomorphisms, if G had one isolated point then all of its points would be isolate and thus G would be discrete. Now:

LEMMA 7.46. *Let X be a nonempty compact Hausdorff space without isolated points. Then $\#X \geq \mathfrak{c} = 2^{\aleph_0}$.*

PROOF. Compact Hausdorff spaces are normal. Since X is nonempty and without isolated points, it must have points $y_0 \neq y_1$. Since X is Hausdorff, there are disjoint open subsets V_0 and V_1 with $x_i \in V_i$ for $i \in \{0,1\}$. Since normal spaces are regular, for $i \in \{0,1\}$ there is an open set U_i such that $y_i \in U_i \subseteq \overline{U_i} \subseteq V_i$. Each U_i is nonempty open in the Hausdorff space X, so it is inifnite; moreover none of its points are isolated.

We repeat the above argument with U_0 and U_1 in place of X, getting nonempty open subsets $U_{i,0}, U_{i,1} \subseteq U_i$ with disjoint closures. And so forth: we generate an infinite rooted binary tree of nonempty open subsets of X, with X as the root, and 2^n subsets $U_{i_1,\ldots,i_n}$ with pairwise disjoint closures at level n. Paths in this tree correspond to infinite sequences $x = \{x_n\}$ with $x_n \in \{0,1\}$ for all $n \in \mathbb{Z}^+$. Because X is compact, for each such x we have $\bigcap_{n=1}^{\infty} \overline{U_{x_1,\ldots,x_n}} \neq \varnothing$, so we may choose a point $P_x \in \overline{U_{x_1,\ldots,x_n}}$. If $x \neq x'$, then let n be the least index such that $x_n \neq x'_n$; then one of $P_x, P_{x'}$ lies in $\overline{U_{x_1,\ldots,x_{n-1},0}}$ and the other lies in $\overline{U_{x_1,\ldots,x_{n-1},1}}$, so $P_x \neq P_{x'}$. Thus $x \mapsto P_x$ defines an injection $2^{\aleph_0} \hookrightarrow X$. □

It follows that an infinite compact Hausdorff group has at least continuum cardinality. In fact, a much stronger result is known: by [**HSTT**, Ch. 1], if G is an infinite compact Hausdorff group, then there is a cardinal κ such that $\#G = 2^{\kappa}$. Conversely, for any cardinal κ, the group $(\mathbb{Z}/2\mathbb{Z})^{\kappa}$ is profinite and has cardinality 2^{κ}, so we deduce an infinite cardinal is the cardinality of a profinite group if and only if it is of the form 2^{κ} for some $\kappa \geq \aleph_0$.

EXERCISE 7.34. *Let G be an infinite, countably based profinite group. Show: $\#G = \mathfrak{c}$.*

COROLLARY 7.47. *Let G be an infinite compact Hausdorff topological group. Then G has a subgroup that is* not *closed.*

PROOF. Lemma 7.46 gives that G is uncountable. Choose a countably infinite subset S of G and let H be the subgroup it generates. Since there are only countably many words in the elements of S and their inverses, H is countably infinite. If H were a closed subgroup of G, it would also be a compact Hausdorff topological group and thus be uncountable, so H is not closed in G. □

EXERCISE 7.35. *Let G be an infinite profinite group. Show: the following infinite cardinals are all equal:*

(i) *The number of open normal subgroups of G.*
(ii) *The minimum cardinality of a neighborhood base for G at e.*
(iii) *The minimum cardinality of a base for the topology of G.*

We denote this common quantity by $\omega(G)$. Thus $\omega(G) = \aleph_0$ if and only if G is (infinite and) countably based.

By [**HR**, Thm. 9.15], if G is an infinite profinite group, then G is homeomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(G)}$. This recovers the assertion of Exercise 7.32 that an infinite countably based profinite group is homeomorphic to the Cantor set. Moreover, the assertion that two profinite groups are homeomorphic if and only if they have the same cardinality is equivalent to the Generalized Continuum Hypothesis (GCH): for all cardinals $\kappa_1 < \kappa_2$, we have $2^{\kappa_1} < 2^{\kappa_2}$. Thus the Krull topology is not very useful in distinguishing profinite groups from one another.

In fact there is a different invariant of a profinite group G, the **profinite order**, that is a much closer analogue to the order of a finite group. Whereas the order of a finite group is a natural number and the order of an infinite profinite group is an infinite cardinal number, the profinite order of an infinite profinite group is an infinite *supernatural number*, a concept due to Steinitz that we now define.

Unique factorization of positive integers into prime powers is equivalent to the statement that the multiplicative monoid $(\mathbb{Z}^+, \cdot)$ is isomorphic to the infinite direct sum $\bigoplus_{i=1}^{\infty}(\mathbb{N}, +)$. We arrive at the supernatural numbers by expanding the monoid $\bigoplus_{i=1}^{\infty}(\mathbb{N}, +)$ in two ways: first, we replace each factor of $(\mathbb{N}, +)$ with $\mathbb{N}^* := (\mathbb{N}, +) \cup \{\infty\}$, where ∞ is just a formal symbol that is not an element of $\mathbb{N}$. We extend the monoid structure by making ∞ an absorbing element: that is, for all $n \leq \infty$, $n + \infty = \infty + n = \infty$. Second, we replace the direct sum by a direct product, thus:

$$\mathbb{S} := \prod_{i=1}^{\infty} \mathbb{N}^*.$$

For a supernatural number n, we still think of the ith coordinate x_i as giving the exponent to which the nth prime p_i appears in the prime factorization of n, but now by our twofold expansion: (i) a prime may appear with infinite exponent rather than having non-negative integer exponent and (ii) we drop the restriction that the exponent must be zero for all but finitely many primes.

What kind of structure does the set $\mathbb{S}$ of supernatural numbers have? It is a commutative monoid under componentwise multiplication: if $x = \prod p_n^{x_n}$ and $y = \prod p_n^{y_n}$, then $xy := p_n^{x_n + y_n}$. As for any commutative monoid, we may define a divisibility relation: $x \mid y$ if there is z such $xz = y$. Because the monoid $\mathbb{S}$ is **reduced** – that is, for all $x, y \in \mathbb{S}$, if $xy = 1$, then $x = y = 1$ – the divisiblity relation is a partial ordering on $\mathbb{S}$. This induced partial ordering makes $\mathbb{S}$ into a lattice: given two supernatual numbers x and y, their supremum under divisibility is their **least common multiple**, defined as

$$\operatorname{lcm}(x, y) = \prod p^{\max x_n, y_n},$$

and their infimum under divisibility is their **greatest common divisor**, defined as

$$\gcd(x, y) = \prod p^{\min x_n, y}.$$

Indeed $\mathbb{S}$ is not just a lattice but a complete lattice: we can take the gcd and lcm of any set of supernatural numbers. For instance

$$\operatorname{lcm}(2, 2^2, 2^3, \ldots, 2^n, \ldots) = 2^\infty.$$

This is true because $\mathbb{N}^*$ is (unlike $\mathbb{N}$) a complete lattice and the direct product of complete lattices is a complete lattice.

If S is any set of supernatural numbers, we can define the product of the elements of S as the supremum of products of the elements in finite subsets of S. (In particular, $\prod \varnothing = 1$.)

Now if G is a profinite group, we define its **profinite order**

$$|G| \coloneqq \operatorname{lcm}\{\#G/N \mid N \text{ is an open normal subgroup of } G\}.$$

Example 7.48.

a) *If G is a finite group, then we are taking the* lcm *of a finite set of numbers, one of which is $\#G$ and the others are divisors of $\#G$, so*

$$|G| = \#G.$$

b) *For a prime p, the open sugroups of $\mathbb{Z}_p$ are precisely $p^n\mathbb{Z}_p$ for $n \in \mathbb{Z}^+$, all of which are normal, and $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. Thus we have*

$$|\mathbb{Z}_p| = \operatorname{lcm}(1, p, p^2, \ldots, p^n) = p^\infty.$$

c) *The open subgroups of $\hat{\mathbb{Z}}$ are $N\hat{\mathbb{Z}}$ for $N \in \mathbb{Z}^+$, all of which are normal, and $\hat{\mathbb{Z}}/N\hat{\mathbb{Z}} \cong \mathbb{Z}/N\mathbb{Z}$. Thus we have*

$$|\hat{\mathbb{Z}}| = \prod_p p^\infty.$$

Exercise 7.36.

a) *Let $\{G_i\}_{i\in I}$ be an indexed family of profinite groups. Show:*

$$|\prod_{i\in I} G_i| = \prod\{|G_i| \mid i \in I\}.$$

b) *Let $x \in \mathbb{S}$. Show: there is a countably based profinite group G with $|G| = x$.*

Exercise 7.37. *Let G be a profinite group, and let p be a prime. Show: the following are equivalent:*

(i) *G is isomorphic as a topological group to an inverse limit of finite, discrete p-groups.*
(ii) *Every open normal subgroup N of G has index a power of p.*
(iii) *Every open subgroup U of G has index a power of p.*
(iv) *We have $|G| \mid p^\infty$.*

A profinite group satisfying these equivalent conditions is called a ***pro-p-group****.*

Let H be a closed subgroup of a profinite group G. We define the **profinite index**

$$|G : H| \coloneqq \operatorname{lcm}\{[G : U] \mid \ U \text{ is an open subgroup of } G \text{ containing } H\}.$$

EXERCISE 7.38. *The definition that we gave for the profinite index of a closed subgroup makes sense for* any *subgroup H of a profinite group. Show: if H is a subgroup of a profinite group G, then $|G : H| = |G : \overline{H}|$.*

EXERCISE 7.39.

a) *Let $\varphi : G \to G'$ be an isomorphism of profinite groups, and let H be a closed subgroup of G. Show: $|G : H| = |G' : \varphi(H)|$.*
b) *Deduce: if H is a subgroup of a profinite group G, then for all $g \in G$ we have $|G : H| = |G : g^{-1}Hg|$.*

PROPOSITION 7.49. *Let H be a closed subgroup of a profinite group G.*

a) *The index $|G : H|$ is $\operatorname{lcm}\{[G : NH]\}$ as N ranges over open normal subgroups of G.*
b) *If H is normal, then $|G : H| = |G/H|$.*
c) *In particular, we have $|G : \{e\}| = |G|$.*

PROOF. a) If N is an open normal subgroup of G, then NH is an open subgroup of G containing H. Conversely, if U is an open subgroup of G containing H, then its normal core $\operatorname{Core}(U)$ is an open normal subgroup of G such that $\operatorname{Core}(U)H \subseteq U$, so $[G : U] \mid [G : N(U)H]$. Thus as N ranges over open normal subgroups of G, the set of indices $[G : NH]$ is a cofinal subset of the set of indices $[G : U]$ as U ranges over all open normal subgroups of G containing H, so $|G : H] = \operatorname{lcm}\{[G : NH] \mid N$ is an open normal subgroup of $G\}$.
b) If H is normal, then for every open normal subgroup U of G we have that NU is an open normal subgroup of G, so part a) tells us that $|G : H]$ is the lcm of $\#G/U$ as U ranges over open normal subgroups of G containing H, which is $|G/N|$.
c) Take $N := \{e\}$ in part a). □

THEOREM 7.50. *(Profinite Lagrange Theorem) Let G be a profinite group and let H, H_1, H_2 be closed subgroups of G with $H_1 \subseteq H_2$.*

a) *We have $|G : H_1| = |G : H_2||H_2 : H_1|$.*
b) *We have $|G| = |H||G : H|$.*

PROOF. a) If N is an open normal subgroup of G, then $N \cap H_2$ is an open normal subgroup of H_2, and we have

$$[G : NH_1] = [G : NH_2][NH_2 : NH_1] = [G : NH_2][H_2 : (N \cap H_2)H_1],$$

so $|G : H_1] \mid |G : H_2||H_2 : H_1|$. Conversely, let N_1 be an open normal subgroup of G and let N_2 be an open normal subgroup of H_2. Then N_2 is the intersection with H_2 of an open subset U of G containing $\{e\}$, so U contains an open normal subgroup M of G, and thus $M \cap H_2 \subseteq N_2$. Then also $N := M \cap N_1$ is an open normal subgroup of G, and

$$[G : N_1H_2][H_2 : N_2H_1] \mid [G : NH_2][H_2 : (N \cap H_2)H_1] = [G : NH_1],$$

so $|G : H_2||H_2 : H_1| \mid |G : H_1|$.
b) Apply part a) with $H_1 := \{e\}$ and $H_2 := H$. □

Now we come to the definition that is the point of this subsection. Let G be a profinite group, and let p be a prime. A **Sylow pro-p-subgroup** of G is a closed pro-p-subgroup H of G such that $\gcd(|G : H|, p) = 1$. A Sylow pro$-p$-subgroup is a maximal pro-p-subgroup: indeed, if H is a Sylow pro-p-subgroup and K is a pro-p-subgroup with $H \subsetneq K$,then $|K| = |H||K : H|$, so $|K : H| \mid |K| \mid p^\infty$, but also

$|K : H| \mid |G : H|$ so $p \nmid |K : H|$, an thus $|K : H| = 1$, so $H = K$. We will shortly show that conversely, maximal pro-p-subgroups are Sylow pro-p-subgroups.

LEMMA 7.51. *Let G be a profinite group, and let $\{H_i\}_{i \in I}$ be a family of closed subgroups of G that is directed under reverse inclusion: for all $i, j \in I$, there is $k \in I$ such that $H_k \subseteq H_i \cap H_j$. Let $H \coloneqq \bigcap_{i \in I} H_i$. Then:*

$$|G : H| = \operatorname{lcm}\{|G : H_i| \mid i \in I\}.$$

PROOF. For $i \in I$, we have $H \subseteq H_i$, so $|G : H_i| \mid |G : H|$ by Theorem 7.50a), and thus $\operatorname{lcm}_{i \in I} |G : H_i| \mid |G : H|$. Conversely, let U be an open subgroup containing H, so $\bigcap_{i \in I}(H_i \cap (G \setminus U)) = \varnothing$. Since each $H \cap (G \setminus U)$ is closed, by compactness there are $i_1, \ldots, i_n \in I$ such that $\bigcap_{j=1}^{r}(H_{i_j} \cap (G \setminus U)) = \varnothing$. By hypothesis, we may choose $k \in I$ such that $H_k \subseteq \bigcap_{j=1}^{r} H_{i_j}$, and then $H_k \subseteq U$, so $|G : U| \mid |G : H_k| \mid \operatorname{lcm}_{i \in I} |G : H_i|$. Thus $|G : H| \mid \operatorname{lcm}_{i \in I} |G : H_i|$.

□

THEOREM 7.52 (Profinite Sylow Theorem). *Let G be a profinite group, and let p be a prime number. Then:*

a) *G has a Sylow pro-p-subgroup.*
b) *Any two Sylow pro-p-subgroups are conjugate in G.*
c) *If H is a closed pro-p-subgroup of G, then H is contained in some Sylow pro-p-subgroup.*

PROOF. In this proof we will make use of the following parts of the Sylow theory of finite groups: every finite group admits a Sylow p-subgroup, and in a finite group G, if H is a p-subgroup and P is a Sylow p-subgroup, then some conjugate of H is contained in P.

a) Let I be the set of closed subgroups of G of index prime to p, partially ordered by reverse inclusion. If $\mathcal{C}$ is any chain in I, then Lemma 7.51 implies that $\bigcap_{H \in \mathcal{C}} H$ is an element of I that is an upper bound for $\mathcal{C}$, so by Zorn's Lemma there is a minimal element $H \in I$. We claim that H is a Sylow p-subgroup: for this, we need to show that H is a pro-p-group. Assume not: then there is a finite index normal subgroup N of H such that the finite group H/N is not a p-group, and let H'/N be a Sylow p-subgroup of H/N,so $H' \subsetneq H$. By Theorem 7.50, we have

$$|G : H'| = |G : H||H : H'|,$$

which shows that H' is a proper closed subgroup of H of index prime to p, contradicting the minimality of H. Thus H is a Sylow pro-p-subgroup of G.

b), c) Since Sylow pro-p-subgroups are maximal and every conjugate of a Sylow pro-p-subgroup is a Sylow pro-p-subgroup, to prove both parts it is enough to show: if H is a closed pro-p-subgroup of G and P is a Sylow pro-p-subgroup of G, then there is $g \in G$ such that $g^{-1}Hg \subseteq P$.

Let N be an open normal subgroup of G. Then $N \cap P$ is an open normal subgroup of P and $NP/N \cong P/(N \cap P)$, so NP/N is a finite p-group; similarly, NT/N is a p-subgroup of the finite group G/N. Moreover $[G : NP] \mid |G : P|$, so NP/N is a Sylow p-subgroup of G/N. By the Sylow Theorem for finite groups, some conjugate of NT/N is contained in NP/N, so the set

$$R(N) \coloneqq \{g \in G \mid g^{-1}NTg \subseteq NP\}$$

is nonempty. Since $R(N)$ is a union of cosets of the finite index open subgroup N, it is open and closed. If M is another open normal subgroup of G with $M \subseteq N$, then $R(M) \subseteq R(N)$, so if $N_1, \ldots, n_r$ are open normal subgroups of G, we have

$$\bigcap_{i=1}^{r} R(N_i) \supseteq R(\bigcap_{i=1}^{r} N_i) \supsetneq \varnothing.$$

Thus as N ranges over open normal subgroups of G, $\{R(N)\}$ is a family of closed subsets of the compact group G satisfying the finite intersection condition, so there is $g \in G$ with $g \in \bigcap_N R(N)$. Then for every open normal subgroup N of G we have $g^{-1}Tg \subseteq NP$, so

$$g^{-1}Tg \subseteq \bigcap_N NP = P.$$

□

EXERCISE 7.40. *Let G be a commutative profinite group.*

a) *For each prime p, show: G has a unique Sylow pro-p-subgroup G_p.*
b) *Show: G is isomorphic (as a topological group) to $\prod_p G_p$.*

An important consequence is: if G is a profinite group and p is a prime number, then G admits an infinite closed pro-p-subgroup if and only if $p^\infty \mid |G|$.

9. The Algebraic Galois Correspondence

THEOREM 7.53 (Fundamental Theorem of Algebraic Galois Theory). *Let K/F be an algebraic Galois extension, and put $G := \mathrm{Aut}(K/F)$, endowed with the Krull topology. Let $\mathcal{L}(K/F)$ denote the set of subextensions of K/F, and let $\mathcal{L}(G)$ denote the set of subgroups of G, partially ordered by inclusion in both cases. Let $\mathcal{L}_c(G)$ denote the set of closed subgroups of G.*

a) *A subgroup of G is open if and only if it is of the form $\mathrm{Aut}(K/L)$ for a finite degree subextension L of K/F. A subgroup of G is closed if and only if it is of the form $\mathrm{Aut}(K/L)$ for a subextension L of K/F.*
b) *The maps*
$$L \in \mathcal{L}(K/F) \mapsto \mathrm{Aut}(K/L)$$
and
$$H \in \mathcal{L}(G) \mapsto K^H$$
are mutually antitone bijections from $\mathcal{L}(L/F)$ to $\mathcal{L}_c(G)$.
c) *Let H be a subgroup of G, with closure $\overline{H}$. Then*
$$K^H = K^{\overline{H}}$$
and
$$\mathrm{Aut}(K/K^H) = \overline{H}.$$

PROOF. a) By definition of the Krull topology, a neighborhood base for the identity in G is given by the subgroups $\mathrm{Aut}(K/L)$ for a subextension L/F that is finite Galois. Thus a subgroup H of G is open if and only if it contains some such subgroup $\mathrm{Aut}(K/L)$. By Proposition 7.40, we have an isomorphism of topological groups $r : G/\mathrm{Aut}(K/L) \to \mathrm{Aut}(L/F)$, so the subgroups of G containing $\mathrm{Aut}(K/L)$ are in bijection with subgroups of $\mathrm{Aut}(L/F)$, which by the finite Galois correspondence are all of the form $\mathrm{Aut}(L/L')$ for a subextension L' of L/F. For such an L', we have $r^{-1}(\mathrm{Aut}(L/L')) = \mathrm{Aut}(K/L')$.

Let L be a subextension of K/F. Then $L = \varinjlim L_i$ is the direct limit of its finite degree subextensions. It follows that

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

is an intersection of open subgroups of G, hence is a closed subgroup of G. Conversely, if H is a closed subgroup of G, let $\{U_i\}_{i\in I}$ be the family of open subgroups of G containing H; this family is closed under finite intersections hence anti-directed under inclusion. By part a), for all $i \in I$ there is a finite degree subextension F_i of K/F such that $U_i = \mathrm{Aut}(K/F_i)$, and then Theorem 7.44b) gives

$$H = \bigcap_{i\in I} \mathrm{Aut}(K/F_i) = \mathrm{Aut}(K/\bigvee_{i\in I} F_i).$$

b) Again it is immediate that the maps $L \mapsto \mathrm{Aut}(K/L)$ and $H \mapsto K^H$ are antitone and that

$$L \subseteq K^{\mathrm{Aut}(K/L)} \text{ and } H \subseteq \mathrm{Aut}(K/K^H).$$

Because K/L is normal and separable, Theorem 7.36 implies $L^{\mathrm{Aut}(K/L)} = L$.
Now let H be a closed subgroup of G, so H is again a profinite group. Then Theorem 7.45 gives

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

c) Since $H \subseteq \overline{H}$, we clearly have $K^{\overline{H}} \subseteq K^H$. To show the reverse inclusion, let $x \in K \setminus K^{\overline{H}}$, and let L be a finite Galois subextension of $K/K^{\overline{H}}$ containing x. There is $\tilde{\sigma} \in \overline{H}$ such that $\tilde{\sigma}(x) \neq x$, and $\tilde{\sigma}$ restricts to an automorphism $\sigma \in \mathrm{Aut}(L/K^{\overline{H}})$ such that $\sigma(x) \neq x$. Let

$$q : \overline{H} \to \mathrm{Aut}(L/K^{\overline{H}})$$

be the quotient map. It is continuous and $\mathrm{Aut}(L/K^{\overline{H}})$ is discrete, so $q^{-1}(\sigma)$ is open in $\overline{H}$. Since H is dense in $\overline{H}$, we have that $H \cap q^{-1}(\sigma)$ is nonempty, meaning there is $h \in H$ such that $q(h) = \sigma$. It follows that $q(x) = \sigma(x) \neq x$, so $x \notin K^H$. Thus we have $K^H = K^{\overline{H}}$.

Finally, using part b) we have

$$\mathrm{Aut}(K/K^H) = \mathrm{Aut}(K/K^{\overline{H}}) = \overline{H}. \qquad \square$$

The following result shows some set-theoretic pathologies that arise in the Galois correspondence for any algebraic Galois extension of infinite degree: first, whereas for a finite degree field extension K/F we have $\#Aut(K/F) \leq [K : F]$, with equality if and only if K/F is Galois, for any infinite algebraic Galois extension we have $[K : F] < \#\,\mathrm{Aut}(K/F)$. Second we show that in any infinite degree algebraic Galois extension K/F there is a proper subgroup H of G such that $K^H = F = K^G$.

Corollary 7.54 (Excess Cardinality). *Let K/F be an algebraic Galois extension of infinite degree, let $G \coloneqq \mathrm{Aut}(K/F)$, and let $\omega(G)$ be the number of open normal subgroups of G.*

a) *We have $[K : F] \leq \omega(G) < 2^{\omega(G)} = \#G$.*
b) *There is a proper subgroup H of G such that $K^H = F$.*

Proof. We observe that $\omega(G)$ is also the number of finite Galois subextensions of K/F. Also we recall from above that G is homeomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(G)}$.
a) For each finite Galois subextension L of K/F, let S_L be an F-basis for L/F,

and let $S \coloneqq \bigcup_L S_L$. If $x \in K$, then x lies in some finite Galois subextension L/F – namely, the normal closure of $F(x)/F$ – so x lies in the F-span $\langle S \rangle_F$ of S. It follows that $\langle S \rangle_F = K$. Since S is an indexed union of finite sets where the index set has infinite cardinality $\omega(G)$, we have $\#S \leq \omega(G)$. Thus K has a spanning set of cardinality at mosst $\omega(G)$, so its dimension $[K : F]$ as an F-vector space is at most $\omega(G)$. The inequality $\omega(G) < 2^{\omega(G)}$ is Cantor's Theorem, and since G is homeomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(G)}$, we have $\#G = 2^{\omega(G)}$.
b) Since $\bigoplus_{i \in \omega(G)} \mathbb{Z}/2\mathbb{Z}$ is a dense subset of $(\mathbb{Z}/2\mathbb{Z})^{\omega(G)}$ of cardinality $\omega(G)$, the homeomorphic space G also has a dense subset X of cardinality $\omega(G)$. Let H be the subgroup generated by X, so H is a dense subgroup of G of cardinality $\omega(G)$, whereas G itself has cardinality $2^{\omega(G)} > \omega(G)$, so H is a dense proper subgroup of G. By Theorem 7.53c), we have $K^H = K^{\overline{H}} = K^G = F$. □

EXERCISE 7.41. *Maintain the hypotheses of Corollary 7.54. Show: the set of subgroups H of G with $K^H = F$ has cardinality greater than $\omega(G)$.*

EXERCISE 7.42. *State and prove a generalization of Theorem 7.13 (Natural Irrationalities) in which K/F is an algebraic Galois extension.*

10. The Leptin–Waterhouse Theorem

We will now prove that every profinite group is isomorphic, as a topological group, to the automorphism group of some algebraic Galois extension endowed with the Krull topology, or much shorter and sweeter: every profinite group is a Galois group. This result has been independently derived several times: for instance by Poizat [**Po74**] and Waterhouse [**Wa74**]. In fact, for what (very) little it is worth, I discovered this result and its proof in 1999 as a second year graduate student: it was in fact one of the very first research-level results that I had proved, and I remember showing it to a couple of friends but not knowing the literature well enough to be able to find any precedence: at the time, I was not even sure anyone else would be interested.

We will give Waterhouse's proof, which is a lovely application of Theorem 7.45.

THEOREM 7.55 (Leptin–Waterhouse). *Every profinite group is a Galois group. More precisely, let $G = \varprojlim G_i$ be a profinite group. Then there is an algebraic Galois extension K/F and an isomorphism of topological groups $G \xrightarrow{\sim} \mathrm{Aut}(K/F)$.*

PROOF. The group G is a closed subgroup of the direct product $\mathcal{G} \coloneqq \prod_{i \in I} G_i$, which is itself a profinite topological group under the profinite structure given by the system of finite index normal subgroups

$$\mathcal{G}^J \coloneqq \prod_{i \in I \setminus J} G_i \times \prod_{i \in J} \{e_i\}$$

as J ranges over finite subsets of I. It suffices to find a Galois extension K/F with $\mathrm{Aut}(K/F) \cong \mathcal{G}$, for then $\mathrm{Aut}(K/K^G) = G$.

Let k be any field; for $i \in I$, let $t_{i,1}, \ldots, t_{i,\#G_i}$ be a set of indeterminates, and fix a simply transitive action of the finite group G_i on the set $\{t_{i,1}, \ldots, t_{i,\#G_i}\}$. Let

$$K \coloneqq k(\{t_{i,j} \mid i \in I, 1 \leq j \leq \#G_i\})$$

be a rational function field. For all $i \in I$, there is a natural action of G_i on K by permuting the indeterminates $t_{i,1}, \ldots, t_{i,\#G_i}$. For all $i \neq j$, the G_i-action and the G_j-action commmute, hence there is an induced action of $\mathcal{G}$. In this action the stabilizers are open subgroups: indeed, for any one $x \in K$, the set J of indices i such that some $t_{i,j}$ appears in either the numerator or denominator of x is finite, hence the stabilizer of x contains the open subgroup $\mathcal{G}^J$ so is itself an open subgroup. Equivalently, when K is given the discrete topology, the $\mathcal{G}$-action on K is continuous, so by Theorem 7.45 if we take $F \coloneqq K^{\mathcal{G}}$, we have $\mathrm{Aut}(K/F) = \mathcal{G}$. □

By Cayley's Theorem, we could also have reduced to the case of $\mathcal{G} \coloneqq \prod_{i \in I} S_{n_i}$ a product of finite symmetric groups, which acts more naturally on a suitable rational function field. We leave it to the reader to decide which version is preferable.

Remark 7.4. *Waterhouse's statement of Theorem 7.45 from* [**Wa74**, Thm. 1] *requires G to be a profinite group. By only assuming that it is a compact Hausdorff topological group (but later concluding that it must be profinite) we are following Milne* [**Mi**, Prop. 7.10]. *Let me also mention that in this work Milne attributes the Leptin–Waterhouse Theorem to J.T. Tate. Tate was the PhD advisor of both Milne (1968 PhD) and Waterhouse (1968 PhD) and was famous for not loving to write things down, so it is not implausible that Tate could have had a hand in the results of this section, but I have no further information about it.*

11. Non-Open Finite Index Subgroups of Profinite Groups

Let K/F be an algebraic Galois extension. When $[K : F]$ is infinite, the main new wrinkle in the Galois correspondence beyond the finite case is that subextensions L of K/F get mapped to *closed* subgroups of $G \coloneqq \mathrm{Aut}(K/F)$ and in particular finite degree subextensions K of K/F get mapped to *open* subgroups of G.

Suppose that $[K : F]$ is infinite. Then K/F admits subextensions of arbitrarily large finite degree, so G has infinitely many open subgroups and is thus infinite. Like any infinite compact Hausdorff topological group, G is uncountably infinite, because it admits a Haar measure with unit mass. It is then easy to see that there are subgroups of G that are not closed: indeed, if G is an infinite group, let X be a countably infinite subset; then the subgroup $\langle X \rangle$ generated by X is also countably infinite, so cannot be a closed subgroup of the compact group G. Here is a much more interesting question:

Question 7.56. *Let G be an infinite profinite group. Is every finite index subgroup of G open?*

The answer depends on the group G.

Exercise 7.43.

a) *Consider $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$, a profinite ring of characteristic 0. Show: for all $n \in \mathbb{Z}^+$, the unique index n subgroup of $\mathbb{Z}_p$ is $p^n\mathbb{Z}_p$, which is open. Show moreover that every nontrivial closed subgroup of $\mathbb{Z}_p$ is open. Deduce: the set of closed subgroups of $\mathbb{Z}_p$ is countably infinite.*

b) *Consider $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$, a profinite ring of characteristic 0. Show: for all $n \in \mathbb{Z}^+$, the unique index n subgroup of $\hat{\mathbb{Z}}$ is $n\hat{\mathbb{Z}}$, which is open.*

c) *By part b), the set of open subgroups of $\hat{\mathbb{Z}}$ is countably infinite. Show: the set of closed subgroups of $\hat{\mathbb{Z}}$ has cardinality $\mathfrak{c} = 2^{\aleph_0}$.*

Now we consider the profinite group $G := \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$. By Leptin–Waterhouse, this is a Galois group. In the next chapter, we will show that G is isomorphic to $\mathrm{Aut}(\mathbb{Q}_{(2)}/\mathbb{Q})$, where $\mathbb{Q}_{(2)}$ is the compositum of all quadratic extensions of $\mathbb{Q}$. By definition of the profinite topology on G, every open subgroup contains $G^J := \prod_{i \notin J} \mathbb{Z}/2\mathbb{Z} \times \prod_{i \in J} \{0\}$ for a finite subset $J \subseteq \mathbb{Z}^+$. Since there are only countably many such subsets J and for each J there are only finitely many subgroups of G containing G^J, the set of open subgroups of G is countably infinite. For all $n \in \mathbb{Z}^+$, $G^{\{n\}}\}$ is the kernel of $\pi_n : G \to \mathbb{Z}/2\mathbb{Z}$, which is an open index 2 subgroup, so the set of open index 2 subgroups of G is countably infinite.[8] However we claim that there are uncountably many index 2 subgroups. Indeed, for every surjective homomorphism of abstract groups $\varphi : G \to \mathbb{Z}/2\mathbb{Z}$, the kernel of φ is an index 2 subgroup; and conversely if H is an index 2 subgroup of G then composing the quotient map $q : G \to G/H$ with the unique isomorphism $G/H \to \mathbb{Z}/2\mathbb{Z}$ gives a surjective homomorphism. Thus index 2 subgroups of G are in bijection with nonzero elements of the $\mathbb{F}_2$-dual vector space $G^\vee$ of G. Any infinite dimensional vector space over a field has a dual space of larger infinite dimension. In this case: the dimension of G is an $\mathbb{F}_2$-vector space is $\mathfrak{c} = 2^{\aleph_0}$, so there is an $\mathbb{F}_2$-basis $\mathcal{B}$ for G of size $\mathfrak{c}$. Surjective linear map $\varphi : G \to \mathbb{F}_2$ correspond to maps $\mathcal{B} \to \mathbb{F}_2$ that are not identically 0, so the number of such maps is $2^{\#\mathcal{B}} = 2^{2^{\aleph_0}}$.

EXERCISE 7.44. *Let H be an index 2 subgroup of $\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$, given as the kernel of a surjective $\mathbb{F}_2$-linear functional $\varphi : G \to \mathbb{Z}/2\mathbb{Z}$. Show: H is open if and only if φ is continuous. Show that the topology on G is induced by the metric on G in which the distance between two distinct elments x, y of G is 2^{-n} if $x_i = y_i$ for all $0 \leq i < n$ and $x_n \neq y_n$. Use this metric to show that if $\varphi : G \to \mathbb{Z}/2\mathbb{Z}$ is continuous, then the kerrnel of φ contains G^J for some finite subset J of $\mathbb{Z}^+$.*

A profinite group G is **strongly complete** if every finite index subgroup of G is open. Thus e.g. $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$ are strongly complete, while $\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ is not.

PROPOSITION 7.57. *Let G be a strongly complete profinite group, and let N be a closed normal subgroup. Then G/N is a strongly complete profinite group.*

PROOF. Let $q : G \to G/N$ be the quotient map, a continuous surjection. We show the contrapositive: suppose that G/N is *not* strongly complete, so it admits a finite index subgroup H that is not open. Then $q^{-1}(H)$ is a finite index subgroup of G, so if $q^{-1}(H)$ were open in G, then it would be closed and thus compact, hence its continuous image $q(q^{-1}(H)) = H$ would be compact hence closed in the Hausdorff space G/N, hence H would be closed of finite index in G/N, hence open, which is not the case. So $q^{-1}(H)$ is a finite index subgroup of G that is not open, hence G is *not* strongly complete. □

EXERCISE 7.45. *Let F be a field, and let $F_{(2)}$ be the compositum of all separable quadratic extensions of F inside an algebraic closure $\overline{F}$ of F.*

a) *Show: the following are equivalent:*
   (i) *$[F_{(2)} : F]$ is infinite.*

[8]But we did not exhibit all of them: for instance, the subgroup of elements such that the sum of the first 17 coordinates is equal to 0 is another open index 2 subgroup.

(ii) *For all $n \in \mathbb{Z}^+$, the group $(\mathbb{Z}/\mathbb{Z})^n$ is a Galois group over F.*
(iii) *There is an algebraic Galois extension K/F with $\mathrm{Aut}(K/F)$ isomorphic (as a topological group) to $\prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$.*

b) *Suppose that F satisfies the equivalent conditions of part a), and let K/F be a finite degree extension. Show: K also satisfies the equivalent conditions of part a).*

We deduce:

COROLLARY 7.58. *Let F be a field not of characteristic 2, and let $F_{(2)}$ be the compositum of all quadratic field extensions of F inside an algebraic closure $\overline{F}$. If $[F_{(2)} : F]$ is infinite, then the absolute Galois group $\mathfrak{g}_F := \mathrm{Aut}(F^{\mathrm{sep}}/F)$ is not strongly complete.*

PROOF. By Exercise 7.45, there is a closed normal subgroup N of $\mathfrak{g}_F$ such that $\mathfrak{g}_F/N \cong \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$. Our above discussion and Proposition 7.57 implies that $\mathfrak{g}_F$ is not strongly complete. □

Let F be a field not of characteristic 2. Then quadratic extensions of F inside an algebraic closure $\overline{F}$ are all separable and are in bijection with square classes $F^\times/F^{\times 2}$, the conditions of Exercise **??**a) are also equivalent to $F^\times/F^{\times 2}$ being infinite. Certainly this holds for $\mathbb{Q}$ and hence by Exercise 7.45b) also for any number field F.

EXERCISE 7.46. *Let k be a field, and let $F := k(t)$.*

a) *Show: there are infinitely many monic irreducible polynomials $f \in k[t]$.*
b) *Show: the group $F^\times/F^{\times 2}$ is infinite. (Hint: $k[t]$ is a PID.)*
c) *Deduce: if k does not have characteristic 2, then the equivalent conditions of Exercise 7.45a) hold for F, and thus the absolute Galois group $\mathfrak{g}_F$ of F is* not *strongly complete.*

As we will see in the following chapter, if F has characteristic 2, then $\wp(F) := \{x^2 + x \mid x \in F\}$ is a subgroup of $(F, +)$ and separable quadratic extensions are in bijection with order 2 subgroups of the quotient group $F/\wp(F)$, so the conditions of Exercise 7.45a) are equivalent to $F/\wp(F)$ being infinite. By Exercise 8.34, these conditions hold for $F = k(t)$ where k is any field of characteristic 2.

A **global field** is a field that is a finite degree extension either $\mathbb{Q}$ or of $\mathbb{F}_p(t)$ for some prime p. Thus we have shown:

COROLLARY 7.59. *The absolute Galois group of a global field is* not *strongly complete.*

EXERCISE 7.47. *Let $\hat{\mathbb{Z}}^\times$ be the unit group of the ring $\hat{\mathbb{Z}}$.*

a) *Show: $\hat{\mathbb{Z}}^\times = \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times$ is a profinite group.*
b) *Show: $\hat{\mathbb{Z}}^\times$ is* not *strongly complete.*

On the other hand, perhaps the deepest result in all of profinite group theory enlarges our supply of strongly complete profinite groups. A profinite group G is **topologically finitely generated** if it admits a finite set X such that the least closed subgroup containing X is all of G: we say that X is a set of **topological generators** for X. Equivalently, G is topologically finitely generated if and only if

it contains a finitely generated dense subgroup. For instance the groups $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$ are topologically finitely generated and even **topologically cyclic**: in each case, the single element 1 is a topological generator.

THEOREM 7.60 (Nikolov–Segal). *Every topologically finitely generated profinite group is strongly complete.*

PROOF. See [**NS07**]. □

We close this chapter by revisiting the subtle issue arising in the definition of a profinite group: why is it wrong to define a profinite group as an abstract group that is *isomorphic* to an inverse limit $\varprojlim G_i$ of finite discrete groups? If G is a group and $\iota : G \to \varprojlim G_i$ is an isomorphism to an inverse limit of finite groups, endowed with its canonical topology, then we topologize G by transporting the topology via ι: $U \subseteq G$ is open if and only if $\iota(U)$ is open. However, if $\iota' : G \to \varprojlim G_i'$ is another isomorphism to an inverse limit of finite groups, endowed with its canonical topology, then if we topologize G by transport of structure via ι', then we might get a different topology on G.

To address this, we call a profinite group (G, τ)**profinitely rigid** if τ is the only topology on G that makes it into a profinite group and **weakly rigid** if for every profinite topology τ' on G, the topological groups (G, τ) and (G, τ') are isomorphic. For instance, the profinite group admits discontinuous automorphisms, so is not rigid; it is weakly rigid if and only if the Continuum Hypothesis holds. We claim that a strongly complete profinite group (G, τ) is rigid: indeed, any profinite topology τ' on G other than τ must be strictly coarser – $\tau' \subsetneq \tau$ and then $1_G : (G, \tau) \to (G, \tau')$ is a continuous bijection from a compact space to a Hausdorff space, so is a homeomorphism: contradiction. Thus Theorem 7.60 implies that every topologically finitely generated profinite group is profinitely rigid.

If X is a set, (Y, τ_Y) is a topological space and $f : X \to Y$ is a bijection, put

$$f^*(\tau_Y) \coloneqq \{f^{-1}(V) \mid V \in \tau_Y\};$$

this is the topology we get on X via transport of structure. If now τ is a topology on X, then f is continuous if and only if $f^*(\tau_Y) \subseteq \tau_X$, and if moreover τ_X and τ_Y are compact Hausdorff topologies, then as above we get that f is continuous if and only if $f^*(\tau_Y) = \tau_X$. It follows that if (G, τ) is a profinite group admitting a discontinuous group automorphism α, then $\alpha^*(\tau)$ and τ are distinct profinite topologies on G, so (G, τ) is not profinitely rigid.

Now let $G \coloneqq \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$, endowed with its canonical profinite topology. Since $\bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ is a countable dense subset of G, any topological group automorphism $\alpha : G \to G$ is determined by its restriction to $\bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$, so the group $\mathrm{Aut}_c(G)$ of topological group automorphisms has cardinality at most $(\#G)^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \times \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$. However $\mathrm{Aut}(G)$ is the set of $\mathbb{F}_2$-linear automorphisms G, which is an $\mathbb{F}_2$-vector space of dimension $\mathfrak{c}$. Fix an $\mathbb{F}_2$-basis $\mathcal{B}$ for G. Then every bijection $f : \mathcal{B} \to \mathcal{B}$ extends to a unique $\mathbb{F}_2$-linear automorphism of G, and the number of bijections on $\mathcal{B}$ is $2^{\#\mathcal{B}} = 2^{\mathfrak{c}}$, so $\#\operatorname{Aut} G \geq 2^{\mathfrak{c}}$. Thus G admits *many* discontinuous automorphisms, so G is not profinitely rigid. It turns out that G is weakly rigid if and only if the Continuum Hypothesis holds.

The first examples of profinite groups that were not weakly rigid were given rather recently by Kiehlmann. In [**Ki13**], Kiehlmann classifies countably based (cf. Exercise 7.32) commutative profinite groups up to both topological group isomorphism and abstract isomorphism. There is an immediate reduction to the case of pro-p-groups (inverse limits of finite p-groups), so we restrict attention to this case. A commutative pro-p-group G is said to have **bounded torsion** if there is some $a \in \mathbb{Z}^+$ such that $p^a x = 0$ for all $x \in G$ and **unbounded torsion** otherwise. Kiehlmann shows that two countably based commutative profinite groups with bounded torsion are topologically isomorphic if and only if they are abstractly isomorphic. On the other hand, if G is a countably based commutative pro-p-group with unbounded torsion, then Kiehlmann shows that there are uncountably many pairwise nonisomorphic profinite groups that are abstractly isomorphic to G. For instance, for a prime number p, the groups

$$G_1 := \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \text{ and } G_2 := G_1 \times \mathbb{Z}_p$$

are abstractly isomorphic but not topologically isomorphic.

CHAPTER 8

Solvable Extensions

1. Cyclotomic Extensions

1.1. Basics. Let K be a field. An element $x \in K^\times$ is a **root of unity** if there is $n \in \mathbb{Z}^+$ such that $x^n = 1$; equivalently, x lies in the torsion subgroup $K^\times[\text{tors}]$ of $K^\times$. We put

$$\mu_n(K) \coloneqq \{x \in K \mid x^n = 1\},$$

and

$$\mu(K) \coloneqq \bigcup_{n \geq 1} \mu_n(K).$$

Thus $\mu_n(K)$ and $\mu(K)$ are subgroups of $K^\times$ and $\mu(K) = K^\times[\text{tors}]$.

LEMMA 8.1. *For a field K and $n \in \mathbb{Z}^+$, we have $\#\mu_n(K) \leq n$.*

PROOF. The elements of $\mu_n(K)$ are the roots of the polynomial $t^n - 1$ over K, and a nonzero polynomial over a field cannot have more roots than its degree. □

LEMMA 8.2. *A finite subgroup of the multiplicative group of a field is cyclic.*

PROOF. Let F be a field, let G be a finite subgroup of $F^\times$, and put $n \coloneqq \#G$. Lagrange's Theorem gives $x^n = 1$ for all $x \in G$, so G is a subgroup of the group

$$\mu_n(F) \coloneqq \{x \in F \mid x^n = 1\},$$

so it suffices to show that $\mu_n(F)$ is cyclic. By Lemma 8.2, the group $\mu_n(F)$ is finite. We use the **Cyclicity Criterion** [**Cl-NT**, Thm. B.9]: a finite group G is cyclic if and only if for all $d \in \mathbb{Z}^+$ there are at most d element of order n in G. This holds in $\mu_n(F)$ since the polynomial $t^d - 1$ can have no more than d roots. □

EXAMPLE 8.3. *Fix $n \in \mathbb{Z}$. For $0 \leq k < n$, the elements $e^{\frac{2\pi k i}{n}}$ are distinct nth roots of unity in $\mathbb{C}$. So $\#\mu_n(\mathbb{C}) = n$.*

EXERCISE 8.1. *Let K be an ordered field. Show that $\mu(K) = \{\pm 1\}$.*

An element of $K^\times$ of exact order n is called a **primitive nth root of unity**.

PROPOSITION 8.4. *Let K be an algebraically closed field. For $n \in \mathbb{Z}^+$, the following are equivalent:*

(i) $\operatorname{char} K \nmid n$.
(ii) $\#\mu_n(K) = n$.
(iii) *K admits a primitive nth root of unity.*
(iv) *K admits precisely $\varphi(n)$ primitive nth roots of unity.*

PROOF. (i) $\iff$ (ii): Let $f(t) = t^n - 1$. Then $f'(t) = nt^{n-1}$. Thus $\operatorname{char} K \nmid n \iff \gcd(f, f') = 1 \iff t^n - 1$ has n distinct roots $\iff \#\mu_n(K) = n$.
(ii) $\iff$ (iii): By Lemma 8.2, $\mu_n(K)$ is a finite, cyclic n-torsion commutative group. Thus it has order n if and only if it has an element of order n.
(ii) $\implies$ (iv): (ii) holds $\iff$ $\mu_n(K)$ is cyclic of order n, in which case it has precisely $\varphi(n)$ generators.
(iv) $\implies$ (iii): Since for all $n \in \mathbb{Z}^+$, $\varphi(n) \geq 1$, this is clear. □

EXERCISE 8.2.

a) *Let K be an algebraically closed field of characteristic zero. Show that $\mu(K) \cong \varinjlim \mathbb{Z}/n\mathbb{Z}$.*

b) *Let K be an algebraically closed field of characteristic $p \geq 0$. Show that*

$$\mu(K) \cong \varinjlim_{n \in \mathbb{Z}^+,\ p \nmid n} \mathbb{Z}/n\mathbb{Z}.$$

EXERCISE 8.3. *Show that for any field K, $\mu(K^{\mathrm{sep}}) = \mu(\overline{K})$.*

Henceforth we only consider μ_n for $\operatorname{char} K \nmid n$.

For a field K, we denote by K^{cyc} the field obtained by adjoining to K all roots of unity in a fixed algebraic closure $\overline{K}$. Then K^{cyc} is the splitting field of the set $\{t^n - 1\}_{\operatorname{char} K \nmid n}$ of separable polynomials, so is an algebraic Galois extension, the **maximal cyclotomic extension of K**. For $n \in \mathbb{Z}^+$ with $\operatorname{char} K \nmid n$, let $K(\mu_n)$ be the splitting field of the separable polynomial $t^n - 1$, the **nth cyclotomic extension**. Thus

$$K^{\mathrm{cyc}} = \varinjlim K(\mu_n).$$

For a field K, it is traditional to denote by ζ_n a primitive nth root of unity in K^{sep}. When $K = \mathbb{C}$, the standard choice is $\zeta_n = e^{\frac{2\pi i}{n}}$. There is an advantage to this choice: for all $m \mid n$, we have the compatibility relation

$$\zeta_n^{\frac{n}{m}} = \zeta_m. \tag{17}$$

EXERCISE 8.4. *Let K be any algebraically closed field.*

a) *Show that one may choose, for all $n \in \mathbb{Z}^+$ with $\operatorname{char} K \nmid n$, a primitive nth root of unity ζ_n such that the compatibility relation (17) holds.*

b) *In how many ways is it possible to do this?*
(Suggestion: express your answer as an inverse limit of finite sets.)

PROPOSITION 8.5. *Let K be a field and $N \in \mathbb{Z}^+$ with $\operatorname{char} K \nmid N$.*

a) *We have $K(\mu_N) = K(\zeta_N)$.*

b) *There is a canonical injective group homomorphism $a_N : \operatorname{Aut}(K(\zeta_N)/K) \hookrightarrow (\mathbb{Z}/N\mathbb{Z})^\times$.*

c) *The map a_N is an isomorphism if and only if $\Phi_N(t) \in K[t]$ is irreducible.*

PROOF. a) In other words, the assertion is that by adjoining any one primitive root of unity, we get the splitting field of the polynomial $t^N - 1$. Since every Nth root of unity is a power of ζ_N, this is clear.
b) For $\sigma \in \operatorname{Aut}(K(\zeta_N)/K)$, $\sigma(\zeta_N)$ is a primitive nth root of unity: any automorphism of a field preserves the order of elements of the multiplicative group of that field. Thus $\sigma(\zeta_N) = \zeta_N^{a_N(\sigma)}$ for a unique $a_N(\sigma) \in (\mathbb{Z}/N\mathbb{Z})^\times$. It is immediate that

$\sigma \mapsto a_N(\sigma)$ is a group homomorphism. If $a_N(\sigma) = 1$, then $\sigma(\zeta_N) = \zeta_N$, so σ fixes $K(\zeta_N)$ and is thus trivial.
c) By part a), the map a_N is an isomorphism if and only if $\#\operatorname{Aut}(K(\zeta_N)/K) = \#(\mathbb{Z}/N\mathbb{Z})^\times = \varphi(N)$, and since $K(\zeta_N)/K$ is finite Galois, this holds if and only if $[K(\zeta_N) : K] = \varphi(N)$. If $f \in K[t]$ is the minimal polynomial of ζ_N, then f is irreducible, $f \mid \Phi_N$ and $[K(\zeta_N) : K] = \deg(f)$, so $[K(\zeta_N) : K] = \varphi(N)$ if and only if $f = \Phi_N$ if and only if Φ_N is irreducible. □

EXERCISE 8.5. *Let K be a field, with separable closure K^{sep}, and let $\mathfrak{g}_K := \operatorname{Aut}(K^{\mathrm{sep}}/K)$.*

a) *In order to define a_N we chose a primitive Nth root of unity $\zeta_N \in K^{\mathrm{sep}}$. Show that the homomorphism a_N is in fact independent of this choice.*

b) *Suppose that $M \mid N$. Show that we have a commutative diagram*

$$\begin{array}{ccc} \operatorname{Aut}(K(\zeta_N)/K) & \stackrel{a_N}{\to} & (\mathbb{Z}/N\mathbb{Z})^\times \\ \downarrow & & \downarrow \\ \operatorname{Aut}(K(\zeta_M)/K) & \stackrel{a_M}{\to} & (\mathbb{Z}/M\mathbb{Z})^\times, \end{array}$$

where the map $(\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/M\mathbb{Z})^\times$ is the induced map on units of the quotient map $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/M\mathbb{Z}$.

c) *Deduce that there is an injection*

$$a : \operatorname{Aut}(K^{\mathrm{cyc}}/K) \hookrightarrow \varprojlim_{N \in \mathbb{Z}^+, \operatorname{char} K \nmid N} (\mathbb{Z}/N\mathbb{Z})^\times.$$

Precomposing with the quotient map $\mathfrak{g}_K \to \operatorname{Aut}(K^{\mathrm{cyc}}/K)$, we get a homomorphism

$$\chi_N : \mathfrak{g}_K \to (\mathbb{Z}/N\mathbb{Z})^\times,$$

*the **modulo N cyclotomic character**. For any prime $\ell \neq \operatorname{char} K$, there is an injection*

$$\operatorname{Aut}(\varinjlim K(\mu_{\ell^n})/K) \to \mathbb{Z}_\ell^\times,$$

and precomposing with $\mathfrak{g}_K \to \operatorname{Aut}(K^{\mathrm{cyc}}/K)$ we get a homomorphism

$$\chi_\ell : \mathfrak{g}_K \to \mathbb{Z}_\ell^\times,$$

*called the ℓ-**adic cyclotomic character**. When $\operatorname{char} K = 0$, there is an injection*

$$\operatorname{Aut}(K^{\mathrm{cyc}}/K) \hookrightarrow \hat{\mathbb{Z}}^\times,$$

and precomposing with $\mathfrak{g}_K \to \operatorname{Aut}(K^{\mathrm{cyc}}/K)$ we get a homomorphism

$$\chi_\ell : \mathfrak{g}_K \to \hat{\mathbb{Z}}^\times,$$

*the **adelic cyclotomic character**.*

1.2. Cyclotomic Polynomials. For $n \in \mathbb{Z}^+$, let $\Phi_n(t)$ be the unique monic polynomial with roots the primitive nth roots of unity in $\mathbb{C}$.[1]

PROPOSITION 8.6.

a) *For all $n \in \mathbb{Z}^+$, we have*

$$\prod_{d \mid n} \Phi_d(t) = t^n - 1. \tag{18}$$

[1]The use of $\mathbb{C}$ here is somewhere between tradition and psychology: any algebraically closed field of characteristic zero – e.g. $\overline{\mathbb{Q}}$ – would serve as well.

b) *For all $n \in \mathbb{Z}^+$, we have $\Phi_n(t) \in \mathbb{Z}[t]$.*
c) *For all $n \in \mathbb{Z}^+$, we have*

$$\Phi_n(t) = \prod_{d|n} (t^d - 1)^{\mu(\frac{n}{d})}. \tag{19}$$

PROOF. a) Both sides of (18) are monic polynomials with $\mathbb{C}$ coefficients whose roots are precisely the nth roots of unity in $\mathbb{C}$. So they are equal.
b) By strong induction on n. The base case is clear: $\Phi_1(t) = t - 1$. Now suppose $n > 1$ and that $\Phi_d(t) \in \mathbb{Z}[t]$ for all proper divisors d of n. Then

$$Q(t) \coloneqq \prod_{d|n,\ d \neq n} \Phi_d(t) \in \mathbb{Z}[t]$$

is a monic polynomial and $Q(t)\Phi_n(t) = t^n - 1$. Now imagine actually performing polynomial long division of $t^n - 1$ by $Q(t)$ to get $\Phi_n(t)$: since $t^n - 1, \Phi_n(t) \in \mathbb{Z}[t]$ are monic, the quotient $\Phi_n(t)$ has $\mathbb{Z}$-coefficients.
c) This follows from part a) by the Möbius Inversion Formula applied in the commutative group $\mathbb{Q}(t)^\times$.[2] □

THEOREM 8.7. *Let $n \in \mathbb{Z}^+$ and let K be a field of characteristic $p \nmid n$. Regard $\Phi_n(t) \in \mathbb{F}_p[t] \subset K[t]$. Then $\Phi_n(t)$ is a separable polynomial, and its roots in $\overline{K}$ are precisely the primitive nth roots of unity.*

PROOF. Since $n \neq 0$ in K, we have $\gcd(t^n - 1, (t^n - 1)') = 1$, so $t^n - 1$ is separable and thus so is $\Phi_n(t)$ by Proposition 4.2b). It is clear that the $\varphi(n)$ roots of $\Phi_n(t)$ in $\overline{K}$ are nth roots of unity; that they are the $\varphi(n)$ *primitive* nth roots of unity follows by an easy induction argument. □

EXERCISE 8.6. *Let p be a prime number, and let $a \in \mathbb{Z}^+$.*
a) *Show: $\Phi_p(t) = 1 + t + \ldots + t^{p-1}$.*
b) *Show: $\Phi_{2p}(t) = 1 - t + \ldots + (-t)^{p-1}$.*
c) *Show: $\Phi_{p^a}(t) = \Phi_p(t^{p^{a-1}})$.*

EXERCISE 8.7. *For $N \in \mathbb{Z}^+$, let $r(N) \coloneqq \prod_{p|N} p$. Show:*

$$\Phi_N(t) = \Phi_{r(N)}(t^{\frac{N}{r(N)}}).$$

EXERCISE 8.8. *Let $N \in \mathbb{Z}^+$.*
a) *Show: for all $N \geq 2$, the constant coefficient of $\Phi_N(t)$ is 1.*
b) *Show: for all $N \neq 2$, the product of the primitive Nth roots of unity in $\mathbb{C}$ is 1.*
c) *Show:*

$$\Phi_N(1) = \begin{cases} 0 & \text{if } N = 1 \\ p & \text{if } N = p^a \text{ for a prime } p \text{ and } a \in \mathbb{Z}^+ \\ 1 & \text{otherwise.} \end{cases}$$

(Hint: for all $N \geq 2$, $\prod_{d|N, d>1} \Phi_d = 1 + t + \ldots + t^{N-1}$.)

EXERCISE 8.9. *Recall that in Theorem 6.17 we showed that for all $p > 2$, $\delta(\Phi_p) = (-1)^{\frac{p-1}{2}} p^{p-2}$. (Also $\delta(\Phi_2) = 1$.) We will compute $\delta(\Phi_{p^n})$ for all $n \geq 2$.*

[2] In fact we don't need this in what follows – it is just a pretty formula.

a) *Let $n \in \mathbb{Z}^{\geq 2}$. Show:*

$$t^{p^n} - 1 = (t^{p^{n-1}} - 1)\Phi_{p^n}.$$

Using Exercise 6.7, deduce:

$$\delta(\Phi_{p^n}) = \frac{\delta(t^{p^n} - 1)}{\delta(t^{p^{n-1}} - 1)\operatorname{Res}(t^{p^{n-1}} - 1, \Phi_{p^n})^2}. \tag{20}$$

b) *Let $\zeta_1, \ldots, \zeta_{p^{n-1}}$ be the p^{n-1}th roots of unity in $\mathbb{C}$. Show: for all $1 \leq i \leq p^{n-1}$, we have $\Phi_{p^n}(\zeta_i) = p$. Deduce:*

$$\operatorname{Res}(t^{p^{n-1}} - 1, \Phi_{p^n}) = p^{p^{n-1}}. \tag{21}$$

c) *Use (20), (21) and Proposition 6.16 to compute $\delta(\Phi_{p^n})$. You should get the following answer:*
- *If p is odd, then*

$$\delta(\Phi_{p^n}) = (-1)^{\frac{\varphi(p^n)}{2}} p^{n\varphi(p^n) - p^{n-1}}.$$

- $\delta(\Phi_{2^2}) = -4$.
- *For $n \geq 3$, $\delta(\Phi_{2^n}) = 2^{(n-1)2^{n-1}}$.*

THEOREM 8.8. *(Gauss–Kronecker) For all $n \in \mathbb{Z}^+$, $\Phi_n(t) \in \mathbb{Q}[t]$ is irreducible.*

PROOF. Since $\Phi_n(t) \in \mathbb{Z}[t]$ is monic and $\mathbb{Z}$ is a UFD, by Gauss's Lemma it is equivalent to show that Φ_n is irreducible in $\mathbb{Z}[t]$. We may write $\Phi_n(t) = f(t)g(t)$ with $f, g \in \mathbb{Z}[t]$ monic and f irreducible, and the goal is to show that $f = \Phi_n$.
Step 1: Let α be a root of $f(t) \in \overline{\mathbb{Q}}$ (hence a primitive nth root of unity) and let p be a prime number not dividing n. We CLAIM that α^p is also a root of $f(t)$.
PROOF OF CLAIM: Suppose not; then, since $p \nmid n$, α^p is a primitive nth root of unity, so α^p is a root of g. Thus α is a root of $h(t^p)$. Since f is monic irreducible and $f(\alpha) = 0$, f is the minimal polynomial for α, so there is $h \in \mathbb{Z}[t]$ with $f(t)h(t) = g(t^p)$. Now apply the homomorphism $\mathbb{Z}[t] \to \mathbb{Z}/p\mathbb{Z}[t]$, $f \mapsto \overline{f}$ and use Proposition 4.5: we get

$$\overline{g}^p = \overline{fh}.$$

Let $\overline{q}$ be an irreducible factor of $\overline{f}$. Then $\overline{q} \mid \overline{f} \mid \overline{g^p}$, so $\overline{q} \mid \overline{g}$. It follows that

$$\overline{q}^2 \mid \overline{f}\,\overline{g} = \overline{\Phi_n}.$$

This shows that $\overline{\Phi_n}$ is not separable, contradicting Theorem 8.7.
Step 2: Let β be any root of $\Phi_n(t)$ in $\overline{\mathbb{Q}}$. Then β and α are both primitive nth roots of unity, so that there is a sequence of (not necessarily distinct) prime numbers $p_1, \ldots, p_r$ with $\gcd(p_1, \ldots, p_r, n) = 1$ and $\alpha^{p_1 \cdots p_r} = \beta$. Applying Step 1 successively to $\alpha, \alpha^{p_1}, \ldots, \alpha^{p_1 \cdots p_{n-1}}$ we find that β is also a root of $f(t)$. Thus f has as its roots *all* primitive nth roots of unity, i.e., $f = \Phi_n$, and Φ_n is irreducible. □

1.3. Some Applications. Let K be a field of characteristic not dividing n, and let ζ_n be a primitive nth root of unity in $\overline{K}$. Then $K(\zeta_n)/K$ is the splitting field of the separable polynomial $\Phi_n \in K[t]$, so we may regard $G := \operatorname{Aut}(K(\zeta_n)/K)$ as a subgroup of $S_{\varphi(n)}$, where the $\varphi(n)$ roots being permuted are precisely the primitive nth roots of unity, which we may identify with $(\mathbb{Z}/n\mathbb{Z})^\times$ by writing each primitive nth root of unity as a power of ζ_n. As we know, for $\sigma \in G$, if $\sigma(\zeta_n) = \zeta_n^{a_n}$, then $\sigma(\zeta) = \zeta^{a_n}$ for all primitive nth roots of unity ζ. This identifies $(\mathbb{Z}/n\mathbb{Z})^\times$ as

a subgroup of $S_{\varphi(n)}$ via the Cayley map that lets any group act on itself (say, on the left) via permutations. So we find that

$$G \subseteq (\mathbb{Z}/n\mathbb{Z})^\times \subseteq S_{\varphi(n)}.$$

When $K = \mathbb{Q}$, the polynomial Φ_n is irreducible, so this gives an example of an irreducible separable polynomial whose Galois group is *much* smaller than the full symmetric group:

COROLLARY 8.9. *Let $n \in \mathbb{Z}^+$. The extension $\mathbb{Q}(\mu_n)/\mathbb{Q}$ is Galois, with Galois group canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.*

EXERCISE 8.10. *Let $n \in \mathbb{Z}^{\geq 3}$. Put $\zeta_n := e^{2\pi i/n}$, so*

$$2\cos\left(\frac{2\pi}{n}\right) = \zeta_n + \zeta_n^{-1}.$$

Put $\mathbb{Q}(\mu_n)^+ := \mathbb{Q}\left(2\cos(\frac{2\pi}{n})\right)$.

a) *Let c be complex conjugation, acting as an automorphism of $\mathbb{Q}(\mu_n)$. Show: under the canonical isomorphism $\mathrm{Aut}(\mathbb{Q}(\mu_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, c corresponds to $-1 \pmod n$.*

b) *Show: $\mathbb{Q}(\mu_n)^{\langle c\rangle} = \mathbb{Q}(\mu_n)^+$.*
(Hint: ζ_n satisfies a quadratic polynomial with coefficients in $\mathbb{Q}(\mu_n)^+$.

c) *Deduce: $\mathrm{Aut}(\mathbb{Q}(\mu_n)^+/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$, and thus it is an abelian extension of $\mathbb{Q}$ of degree $\begin{cases} 1 & n \in \{1,2\} \\ \frac{\varphi(n)}{2} & n \geq 3 \end{cases}$.*

*For reasons that I hope this exercise makes clear, $\mathbb{Q}(\mu_n)^+$ is often called the **real subfield of the nth cyclotomic field**.*

EXERCISE 8.11. *Let $\mathbb{F}_q$ be a finite field, and let $n \in \mathbb{Z}^+$ with $\gcd(n,q) = 1$, so $\overline{\mathbb{F}_q}$ has a primitive nth root of unity ζ_n. Put $G := \mathrm{Aut}(\mathbb{F}_q(\zeta_n)/\mathbb{F}_q)$.*

a) *Show: $G = \langle q \pmod n\rangle$ is cyclic. We denote the order of G by $\mathbf{o}_n(q)$.*

b) *Show: $G = \{1\}$ if and only if $q \equiv 1 \pmod n$.*

c) *Show: $\Phi_n \in \mathbb{F}_q[t]$ is irreducible if and only if $\mathbf{o}_n(q) = \varphi(n)$. Deduce: if Φ_n is irreducible for* any *prime power q, then $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic – that is, $n \in \{1,2,4\}$ or is p^k or $2p^k$ for an odd prime number p and $k \in \mathbb{Z}^+$.*

d) *Suppose $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. Show: there are infinitely many prime numbers p such that $\Phi_n \in \mathbb{F}_p[t]$ is irreducible.*

e) *Show: $\Phi_n \in \mathbb{F}_q[t]$ is the product of $\frac{\varphi(n)}{\mathbf{o}_n(q)}$ distinct monic irreducible polynomials, each having degree $\mathbf{o}_n(q)$.*

EXERCISE 8.12. *Let $m, n \in \mathbb{Z}^+$ with $m \mid n$.*

a) *Show: $\mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_n)$ if and only if $m = n$ or (m is odd and $n = 2m$).*

b) *Show:*

$$\mathbb{Q}(\mu_m, \mu_n) = \mathbb{Q}(\mu_{\mathrm{lcm}(m,n)}). \tag{22}$$

$$\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{\gcd(m,n)}). \tag{23}$$

The next exercise gives results that are usually proved by elementary number theory, but can also be proved using the field theory we've just developed.

EXERCISE 8.13.

a) *Let $m, n \in \mathbb{Z}^+$ with $m \mid n$. Show: $\varphi(m) \mid \varphi(n)$.*
b) *Let $n \in \mathbb{Z}^{\geq 3}$. Show: $\varphi(n)$ is even.*
(Hint: n is divisible either by 4 or by some odd prime.)

THEOREM 8.10. *Let $n \in \mathbb{Z}^+$. There are infinitely many primes p with $p \equiv 1 \pmod{n}$.*

PROOF. We may assume $n \geq 2$. Let S be a finite set (possibly empty) of primes $p \equiv 1 \pmod{n}$, and let $q = \prod_{p \in S} p$. For sufficiently large $k \in \mathbb{Z}$, we have

$$N = \Phi_n(knq) > 1.$$

Since the constant term of Φ_n is 1, for any prime $p \mid knq$, $N \equiv 1 \pmod{p}$. Since $N > 1$, there is a prime p with $\Phi_n(knq) = N \equiv 0 \pmod{p}$, so $p \nmid knq$: in particular $p \notin S$. By Theorem 8.7, $knq \in \mathbb{F}_p$ is a primitive nth root of unity. By Lagrange's Theorem, $n \mid p - 1$. We've produced a prime $p \notin S$ with $p \equiv 1 \pmod{n}$. □

LEMMA 8.11. *Let G be a finite commutative group. Then there are $k, n \in \mathbb{Z}^+$ and a surjective homomorphism of groups $(\mathbb{Z}/n\mathbb{Z})^k \to G$.*

EXERCISE 8.14. *Prove Lemma 8.11.*

COROLLARY 8.12. *Every finite* commutative *group occurs as a Galois group over $\mathbb{Q}$.*

PROOF. Let G be a finite commutative group.
Step 1: By Lemma 8.11, G is a quotient of $(\mathbb{Z}/n\mathbb{Z})^k$ for some $k, n \in \mathbb{Z}^+$. Since any group which is a quotient of a finite Galois group over a field K is also a finite Galois group over that field, it suffices to treat the case $G = (\mathbb{Z}/n\mathbb{Z})^k$.
Step 2: By Theorem 8.10, there are prime numbers $p_1, \ldots, p_k$ such that $n \mid (p_i - 1)$ for $1 \leq i \leq k$. The group $(\mathbb{Z}/p_i\mathbb{Z})^\times$ is cyclic of order $\varphi(p_i) = p_i - 1$, so there is a surjection $q_i : (\mathbb{Z}/p_i\mathbb{Z})^\times \to \mathbb{Z}/n\mathbb{Z}$. Let

$$q = (q_1, \ldots, q_k) : \prod_{i=1}^k (\mathbb{Z}/p_i\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^k,$$

a surjective group homomorphism. Put $N = p_1 \cdots p_k$. Since the p_i's are distinct, by the Chinese Remainder Theorem there is an isomorphism

$$\mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \prod_{i=1}^k \mathbb{Z}/p_i\mathbb{Z}$$

and thus, passing to unit groups, an isomorphism

$$\Phi : (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\sim} \prod_{i=1}^k (\mathbb{Z}/p_i\mathbb{Z})^\times.$$

Thus we get a surjective map

$$\mathrm{Aut}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\Phi} \prod_{i=1}^k (\mathbb{Z}/p_i\mathbb{Z})^\times \xrightarrow{q} (\mathbb{Z}/n\mathbb{Z})^k.$$

By Galois Theory, there is a subextension L of $\mathbb{Q}(\mu_N)/\mathbb{Q}$ with $\mathrm{Aut}(L/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^k$. □

EXERCISE 8.15. *Show: for any number field K and any finite commutative group G, there is a Galois extension L/K with $\mathrm{Aut}(L/K) \cong G$.*

EXERCISE 8.16. *Let $n \in \mathbb{Z}^+$. Let $K/\mathbb{Q}$ be a finite Galois extension. We may view K as a subfield of $\mathbb{C}$: since $K/\mathbb{Q}$ is normal, any two embeddings $K \hookrightarrow \mathbb{C}$ have the same image. Thus it makes sense to ask whether K is a subfield of $\mathbb{R}$.*

a) *(Parker: [**Pa74**]) Show: for all $n \in \mathbb{Z}^+$, there is a finite Galois extension $K/\mathbb{Q}$ with $K \subseteq \mathbb{R}$ such that $\mathrm{Aut}(K/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z}$.*
b) *Show: for any finite commutative group G, there is a finite Galois extension $K/\mathbb{Q}$ with $\mathrm{Aut}(K/\mathbb{Q}) \cong G$ such that $K \subseteq \mathbb{R}$.*
c) *Let G be a finite group of odd order. Suppose that $K/\mathbb{Q}$ is Galois and $\mathrm{Aut}(K/\mathbb{Q}) \cong G$. Show: $K \subseteq \mathbb{R}$.*
d) *Dirichlet's Theorem on primes in arithmetic progresssions states that for any $a, N \in \mathbb{Z}^+$ with $\gcd(a, N) = 1$, there are infinitely many primes $p \equiv a \pmod N$. Thus Theorem 8.10 is the $a = 1$ case of this (which is* much *easier to prove than the general case). Use Dirichlet's Theorem to prove: for every finite commutative group G of even order, there is a Galois extension $K/\mathbb{Q}$ with $\mathrm{Aut}(K/\mathbb{Q}) \cong G$ such that K is* not *contained in $\mathbb{R}$.*[3]

THEOREM 8.13. *Let p be an odd number. Then the unique quadratic subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$ is*

$$\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ -\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

PROOF. Step 1: The Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is $\mathbb{Z}/p\mathbb{Z}^\times = \mathbb{F}_p^\times$, which is cyclic by Lemma 8.2, hence has a unique index 2 subgroup. By the Galois correspondence, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has a unique quadratic subextension, say $\mathbb{Q}(\sqrt{d})$.

Step 2: So it suffices to show that $\sqrt{(-1)^{\frac{p-1}{2}}p} \in \mathbb{Q}(\zeta_p)$. Gauss proved this using the Legendre symbol and quadratic Gauss sums [**Cl-NT**, Thm. 4.18]. We will give a purely field-theoretic argument, following Weintraub [**We**, pp. 109-111].

By Corollary 8.9, $\mathrm{Aut}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}^\times = \mathbb{F}_p^\times$ is cyclic of even order $p-1$, so $[\mathbb{F}_p^\times : \mathbb{F}_p^{\times 2}] = 2$. If r is a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$, then every $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ is of the form r^k for a unique $k \in \mathbb{Z}/p\mathbb{Z}$. It follows that the elements of $\mathbb{F}_p^{\times 2}$ are precisely r^2, r^4, r^{p-1}. Moreover, we have $r^{\frac{p-1}{2}} = -1$ – indeed, $r^{\frac{p-1}{2}}$ squares to 1 and cannot be -1 since r generates $\mathbb{F}_p^\times$ – and it follows that $-1 \in \mathbb{F}_p^{\times 2}$ if and only if $p \equiv 1 \pmod 4$.

We observe that the elements $\gamma \in \mathbb{Q}(\zeta_p)$ such that $\mathbb{Q}(\gamma)$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ are characterized by $\sigma(\gamma) \neq \gamma$ and $\sigma^2(\gamma) = \gamma$. Thus if we can find such a γ and compute its minimal polynomial, then the discriminant of that quadratic polynomial is the desired d. Indeed, if we put

$$\alpha := \zeta_p^{r^2} + \zeta_p^{r^4} + \ldots + \zeta_p^{r^{p-1}} = \sum_{i=1}^{\frac{p-1}{2}} \zeta_p^{r^{2i}}$$

[3]When G is cyclic, this is also claimed in [**Pa74**], but he does not prove it, and it seems to me that one wants Dirichlet's Theorem to make the argument work.

and

$$\beta := \zeta_p^r + \zeta_p^{r^3} + \ldots + \zeta_p^{r^{p-2}} = \sum_{i=1}^{\frac{p-1}{2}} \zeta_p^{r^{2i-1}},$$

then we have $\sigma(\alpha) = \beta$ and $\sigma(\beta) = \alpha$, so $\sigma^2(\alpha) = \alpha$ and $\sigma^2(\beta) = \beta$: that is, α and β are two conjugate generators of $\mathbb{Q}(\sqrt{d})$. The minimal polynomial of either one is

$$(t-\alpha)(t-\beta) = t^2 - (\alpha+\beta)t + (\alpha\beta),$$

and we have $\alpha + \beta = \sum_{i=1}^{p-1} \zeta_p^{r^i} = \sum_{j=1}^{p-1} \zeta_p^j = -1$, since

$$\Phi_p(\zeta_p) = 1 + \zeta_p + \ldots + \zeta_p^{p-1} = 0.$$

So it remains to compute

$$\alpha\beta = \sum_{u \in \mathbb{F}_p^{\times 2}, v \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}} \zeta_p^{u+v} \in \mathbb{Q}. \tag{24}$$

In Exercise 8.17 you are asked to show: if $\gamma \in \mathbb{Q}(\zeta_p)$, we may write $\gamma = \sum_{i=1}^{p-1} a_i \zeta_p^i$ for unique $a_1, \ldots, a_{p-1} \in \mathbb{Q}$, and then we have $\gamma \in \mathbb{Q}$ if and only if $a_1 = \ldots = a_{p-1}$, in which case $\gamma = \frac{-\sum_{i=1}^{p-1} a_i}{p-1}$. Because of this, as we will soon see, in order to compute the right hand side of (24) we only need to determine the number of pairs (u, v) with $u + v = 0$.

Case 1: Suppose $p \equiv 1 \pmod 4$, so as above $-1 \in \mathbb{F}_p^{\times 2}$. Then $\zeta_p^{u+v} = 1$ if and only if $v = -u$ in $\mathbb{F}_p$, but since u and -1 are squares in $\mathbb{F}_p$, so is $-u$, whereas v is not. So in this case we never have $\zeta_p^{u+v} = 1$, so $\sum_{u \in \mathbb{F}_p^{\times 2}, v \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}} \zeta_p^{u+v}$ is a rational number of the form $a_1\zeta_p + \ldots + a_{p-1}\zeta_p^{p-1}$ with $a_1 + \ldots + a_{p-1}$ equal to the number of terms in the sum, hence to $\frac{p-1}{2} \cdot \frac{p-1}{2} = \frac{(p-1)^2}{4}$. By Exercise 8.17c), we find that

$$\alpha\beta = \frac{-\frac{(p-1)^2}{4}}{p-1} = \frac{-(p-1)}{4}.$$

Thus the minimal polynomial of α is

$$t^2 + t + \frac{-(p-1)}{4} = 0,$$

which has discriminant $d = 1^2 - 4 \cdot \frac{-(p-1)}{4} = p$.

Case 2: Suppose $p \equiv 3 \pmod 4$, so as above $-1 \notin \mathbb{F}_p^{\times 2}$. Then, for each $u \in \mathbb{F}_p^{\times 2}$, we have $-u \notin \mathbb{F}_p^{\times 2}$, which means that precisely $\frac{p-1}{2}$ terms in the right hand side of (24) evaluate to 1. The remaining part of the sum is therefore still a rational number of the form $\sum_{i=1}^{p-1} a_i \zeta_p^i$ with $a_i \in \mathbb{Q}$ such that $\sum_{i=1}^{p-1}$ is equal to $\frac{(p-1)^2}{4} - \frac{p-1}{2}$ (the number of remaining terms of the sum), so by Exercise 8.17c) we find

$$\alpha\beta = \frac{p-1}{2} + \frac{-1}{p-1} \cdot \left(\frac{(p-1)^2}{4} - \frac{p-1}{2} \right) = \frac{p-1}{4} + \frac{1}{2}.$$

Thus the minimal polynomial of α is

$$f^2 + t + \frac{p-1}{4} + \frac{1}{2},$$

which has discriminant $d = 1^2 - 4 \cdot (\frac{p-1}{4} + \frac{1}{2}) = -p$. □

EXERCISE 8.17. *Let $p > 2$ be a prime number.*

a) *Let $\gamma \in \mathbb{Q}(\zeta_p)$. Show: there are unique $a_1, \ldots, a_{p-1} \in \mathbb{Q}$ such that*

$$\gamma = \sum_{i=1}^{p-1} a_i \zeta_p^i. \tag{25}$$

b) *With respect to (25), show that the following are equivalent:*
   (i) *We have $\gamma \in \mathbb{Q}$.*
   (ii) *We have $a_1 = \ldots = a_{p-1}$.*

c) *Suppose that the equivalent conditions of part b) hold. Show:*

$$\gamma = \frac{-\sum_{i=1}^{p-1} a_i}{p-1}.$$

EXERCISE 8.18.

a) *Show $\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ and that it has precisely three quadratic subfields: $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$.*

b) *By Corollary 8.9, we may identify $\mathrm{Aut}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ with $(\mathbb{Z}/8\mathbb{Z})^\times$. Show: the fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ are, respectively, $\mathbb{Q}(\zeta_8)^{H_i}$ with H_1 the subgroup generated by $5 \pmod 8$, H_2 the subgroup generated by $7 \pmod 8$ and H_3 the subgroup generated by $3 \pmod 8$.*

EXERCISE 8.19. *Let $d \in \mathbb{Q}^\times \setminus \mathbb{Q}^{\times 2}$. Show: there is some $n \in \mathbb{Z}^+$ such that $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_n)$.*

Exercise 8.19 is the first nontrivial case of the celebrated **Kronecker–Weber Theorem**, which asserts that every finite abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{Z}^+$.

In elementary number theory [**Cl-NT**, Thm. 1.25], one learns that for a prime $p > 2$ and a positive integer a, the group $(\mathbb{Z}/p^a\mathbb{Z})^\times$ is cyclic, while for $a \geq 3$, the group $(\mathbb{Z}/2^a\mathbb{Z})^\times$ is isomorphic to $C_2 \times C_{2^{a-2}}$, where C_d denotes a cyclic group of order d. You may make use of these group-theoretic results in the following exercise.

EXERCISE 8.20. *Let $n \in \mathbb{Z}^{\geq 3}$, and write $n = 2^a p_1^{a_1} \cdots p_r^{a_r}$ for prime numbers $2 < p_1 < \ldots < p_r$, $a \in \mathbb{N}$ and $a_1, \ldots, a_r \in \mathbb{Z}^+$.*

a) *Suppose $a \leq 1$. Show: $\mathbb{Q}(\zeta_n)$ has precisely $2^r - 1$ quadratic subfields, and find them all explicitly.*

b) *Suppose $a = 2$. Show: $\mathbb{Q}(\zeta_n)$ has precisely $2^{r+1} - 1$ quadratic subfields, and find them all explicitly.*

c) *Suppose $a \geq 3$. Show: $\mathbb{Q}(\zeta_n)$ has precisely $2^{r+2} - 1$ quadratic subfields, and find them all explicitly.*

One can solve Exercise 8.20 without using the above group-theoretic results. To give a taste, let us show that for $a \geq 3$, the quadratic subfields of $\mathbb{Q}(\zeta_{2^a})$ are precisely $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. For $a = 3$, this is Exercise 8.18, which can be done by a simple direct computation. Suppose that for some $a \geq 4$ the field $\mathbb{Q}(\zeta_{2^a})$ had a fourth quadratic subfield $\mathbb{Q}(\sqrt{d})$; we may assume that d is a nonsquare, squarefree integer. Because $\mathbb{Q}(\zeta_{2^a})$ would then also contain square roots of $-d$, $2d$ and $-2d$, it would then contain square roots of both e and $-e$ for some positive odd integer e. Writing $e = p_1 \cdots p_r$ for a product of distinct odd primes, we have that for all i, one of $\sqrt{p_i}$, $\sqrt{-p_i}$ lies in $\mathbb{Q}(\zeta_{p_i})$ and thus one of $\sqrt{e}$, $\sqrt{-e}$ lies in $\mathbb{Q}(\zeta_e)$. This means

that $\mathbb{Q}(\zeta_e)$ and $\mathbb{Q}(\zeta_{2^a})$ have a common quadratic subfield, contradicting Exercise 8.12b). If you like, try solving Exercise 8.20 using similar arguments.

2. Kummer Theory

2.1. Cyclic Extensions. A finite degree field extension K/F is **cyclic** if $\mathrm{Aut}(K/F)$ is a cyclic group of order $[K : F]$. In particular a cyclic extension is necessarily Galois. By a **generator** of a cyclic extension L/K, we mean an element σ which generates $\mathrm{Aut}(L/K)$. (Of course σ is not unique if $n > 2$.)

EXAMPLE 8.14. *A quadratic extension K/F is cyclic if and only if it is separable. Thus if F does not have characteristic 2 then every quadratic extension K/F is cyclic, and moreover – as the quadratic formula holds here – is of the form $F(\sqrt{a})$ for some $a \in F \setminus F^2$.*

Let F be a field of characteristic 0. Since adjunction of square roots of elements of F yields cyclic extensions, it is natural to try to construct cyclic extensions of degree n by adjunction of nth roots. This is a good idea, but it works only under certain restrictions.

EXAMPLE 8.15. *We revisit Example 3.16. For $n \geq 3$, let $p_n(t) = t^n - 2$, and let $F_n = \mathbb{Q}[t]/(p_n(t))$. We may embed $\mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$, and then, since p_n has a unique root $\sqrt[n]{2}$ in $\mathbb{R}$, and in such a way we view $F_n \hookrightarrow \mathbb{R}$. If ζ_n is a primitive nth root of unity, then the conjugates of $\sqrt[n]{2}$ over $\mathbb{Q}$ are $\zeta_n^i \sqrt[n]{2}$ for $0 \leq i < n$. The only conjugate that lies in $\mathbb{R}$, let alone F_n, is $\sqrt[n]{2}$, so $F_n/\mathbb{Q}$ is not normal (so certainly not cyclic). The splitting field of $F_n/\mathbb{Q}$ is*

$$K_n := \mathbb{Q}(\zeta_n, \sqrt[n]{2}).$$

Because the subgroup $\mathrm{Aut}(K_n/F_n)$ of $\mathrm{Aut}(K_n/\mathbb{Q})$ is not normal, the group $\mathrm{Aut}(K_n/\mathbb{Q})$ is not commutative, hence certainly not cyclic.

Now let $n = 3$. Then the polynomial $p_3(t)$ remains irreducible over $\mathbb{Q}(\zeta_3)$: indeed, every irreducible cubic polynomial remains irreducible over a quadratic field extension, so $K_3/\mathbb{Q}(\zeta_3)$ is Galois of degree 3, hence cyclic. A generator for its automorphism group is the automorphism that sends $\sqrt[3]{2}$ to $\zeta_3 \sqrt[3]{2}$. We also compute in this way that the automorphism group $\mathrm{Aut}(K_3/\mathbb{Q})$ is noncommutative of order 6 and thus, as a permutation group on the conjugates $\sqrt[3]{2}, \zeta_3 \sqrt[3]{2}, \zeta_3^2 \sqrt[3]{2}$, is the full symmetric group S_3. Indeed, it has order $[K_3 : \mathbb{Q}(\zeta_3)][\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 6$ and is noncommutative since the order 2 subgroup $\mathrm{Aut}(K_3/F_3)$ is not normal.

PROPOSITION 8.16. *Let K be a field of characteristic $p \geq 0$, let $n \in \mathbb{Z}^+$, and let $a \in K$ be such that the polynomial $f(t) = t^n - a$ is irreducible in $K[t]$. Let $L := K[t]/(f(t)) = K(\sqrt[n]{a})$. The following are equivalent:*

(i) *The extension L/K is cyclic.*
(ii) *The field K contains a primitive nth root of unity. (In particular, $p \nmid n$).*

PROOF. We have $f'(t) = nt^{n-1}$, so by the Derivative Criterion, L/K is separable if and only if $p \nmid n$. It follows that if $p \mid n$ then *neither* (i) nor (ii) holds, so we may assume henceforth that $p \nmid n$. In this case the roots of $f(t)$ in a splitting field are of the form $\zeta_n^i \sqrt[n]{a}$, where ζ_n is a primitive nth root of unity.
(i) $\implies$ (ii): In particular, $\frac{\zeta_n \sqrt[n]{a}}{\sqrt[n]{a}} = \zeta_n$ lies in any splitting field for f, so if L/K is normal then ζ_n lies in L.

(ii) $\implies$ (i): The above discussion shows that if K contains a primitive nth root of unity – say ζ_n – then L/K is normal and separable, thus Galois.

It remains to show that the group $\mathrm{Aut}(L/K)$ is cyclic. For this, observe that there is a unique $\sigma \in \mathrm{Aut}(L/K)$ such that $\sigma(\sqrt[n]{a}) = \zeta_n \sqrt[n]{a}$: such an automorphism exists because the automorphism group of a Galois extension $K[t]/(f)/K$ acts transitively on the roots of f, and it is unique because $L = K(\sqrt[n]{a})$. For any $i \in \mathbb{Z}^+$, $\sigma^i : \sqrt[n]{a} \mapsto \zeta_n^i \sqrt[n]{a}$, and thus the order of σ is

$$\langle \sigma \rangle = n = [L : K] = \#\,\mathrm{Aut}(L/K). \qquad \square$$

There is an important converse to Proposition 8.16. To prove it, we need first the following result, which despite its innocuous appearance is actually quite famous.

LEMMA 8.17. *Let K be a field, $\zeta_n \in K$ a primitive nth root of unity. Let L/K be a cyclic extension of degree n, with generator σ. There is $\alpha \in L$ such that $\zeta_n = \frac{\sigma(\alpha)}{\alpha}$.*

PROOF. Equivalently, we need to show that ζ_n is an eigenvalue for the K-linear endomorphism $\sigma : L \to L$. Since σ has order n, by Dedekind's Theorem the transformations $1, \sigma, \ldots, \sigma^{n-1}$ are all K-linearly independent, and therefore the minimal polynomial of σ is indeed $p(t) = t^n - 1$. Thus ζ_n is a root of the minimal polynomial for σ and therefore also a root of its characteristic polynomial. $\square$

THEOREM 8.18. *Let $n \in \mathbb{Z}^+$, and let K be a field containing a primitive nth root of unity ζ_n. Let L/K be cyclic of degree n with generator σ.*

a) *There is $a \in K$ such that $\sigma(\sqrt[n]{a}) = \zeta_n \sqrt[n]{a}$ and $L = K(\sqrt[n]{a})$.*
b) *If $b \in K$ is such that $\sigma(\sqrt[n]{b}) = \zeta_n \sqrt[n]{b}$ and $L = K(\sqrt[n]{b})$, then $\frac{a}{b} \in K^n$.*

PROOF. a) By Lemma 8.17, there is $\alpha \in L$ such that $\sigma(\alpha) = \zeta_n \alpha$. Thus for all $i \in \mathbb{Z}^+$ $\sigma(\alpha^i) = \zeta_n^i \alpha$. In particular $a = \alpha^n \in K$, and the subgroup of $\mathrm{Aut}(L/K)$ fixing $K(\alpha)$ pointwise is the identity. It follows that $L = K(\alpha) = K(\sqrt[n]{a})$.
b) We have $\sigma(\sqrt[n]{\frac{a}{b}}) = \sqrt[n]{\frac{a}{b}}$, so $\frac{\sqrt[n]{a}}{\sqrt[n]{b}} = u \in K$. Take nth powers: $\frac{a}{b} = u^n \in K^n$. $\square$

PROPOSITION 8.19. *Let K be a field containing a primitive nth root of unity ζ_n, and let L/K be a field extension such that $L = K(\alpha)$ and $\alpha^n = a \in K$.*

a) *L/K is a cyclic extension.*
b) *The degree $m = [L : K]$ is equal to the order of the image of a in $K^\times/K^{\times n}$.*
c) *The minimal polynomial of α over K is $t^m - \alpha^m$.*

PROOF. a) Since K contains a primitive nth root of unity, in characteristic $p > 0$ we must have $p \nmid n$, so the polynomial $f = t^n - a \in K[t]$ is separable. Therefore the splitting field of f is a finite Galois extension of K. But the roots of f are $\{\zeta_n^i \alpha \mid 0 \le i < n\}$ and since $\zeta_n \in K$, all of these roots lie in L. This shows that L is the splitting field of the separable polynomial f, so L/K is Galois.

For all $\sigma \in \mathrm{Aut}(L/K)$, there is a unique $a(\sigma) \in \mathbb{Z}/n\mathbb{Z}$ such that $\sigma(\alpha) = \zeta_n^{a(\sigma)} \alpha$, so $\sigma \mapsto a(\sigma)$ defines a map

$$a : \mathrm{Aut}(L/K) \to \mathbb{Z}/n\mathbb{Z}.$$

We claim a is an injective group homomorphism. For $\sigma, \tau \in \mathrm{Aut}(L/K)$ we have

$$(\sigma\tau)(\alpha) = \sigma(\zeta_n^{a(\tau)} \alpha) = \zeta_n^{a(\tau)} \sigma(\alpha) = \zeta_n^{a(\tau)} \zeta_n^{a(\sigma)} \alpha = \zeta_n^{a(\sigma)+a(\tau)} \alpha,$$

which shows that $a(\sigma\tau) = a(\sigma) + a(\tau)$. Moreover we have $a(\sigma) = 0$ if and only if $\sigma(\alpha) = \alpha$ if and only if $\sigma = 1$, since α generates L/K. It follows that $\mathrm{Aut}(L/K)$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$ hence is cyclic of order M for some $M \mid n$.
b) If a has order m in $K^\times/K^{\times n}$, there is $b \in K^\times$ such that $a^m = b^n$. Then

$$(\alpha^m)^n = (\alpha^n)^m = a^m = b^n,$$

so there is an nth root of unity ζ such that $\alpha^m = \zeta b$. Since K contains a primitive nth root of unity, this shows that $\alpha^m \in K$. It therefore follows that for all $\sigma \in \mathrm{Aut}(L/K)$ we have $ma(\sigma) = 0 \in \mathbb{Z}/n\mathbb{Z}$ and thus $M \mid m$. Conversely, the L/K conjugates of α are $\{\sigma(\alpha) \mid \sigma \in \mathrm{Aut}(L/K)\}$, so the minimal polynomial of α is

$$\prod_{\zeta \in \mu_M} (t - \zeta\alpha) = t^M - \alpha^M,$$

so $\alpha^M \in K$ and thus $a^M = \alpha^{Mn} \in K^{\times n}$, so $m \mid M$. It follows that

$$m = M = \#\,\mathrm{Aut}(L/K) = [L : K].$$

c) Indeed, we just saw that we may take $b = \alpha^m$. □

PROPOSITION 8.20. *Let K be a field containing a primitive nth root of unity, and let $L = K(\sqrt[n]{a})$ for $a \in K$. Then any subextension M of L/K is of the form $K(\sqrt[d]{a})$ for some divisor d of n.*

PROOF. Let m tbe the order of a in $K^\times/K^{\times n}$. By Proposition 8.19m the extension L/K is cyclic of degree m. Let σ be a generator of $\mathrm{Aut}(L/K)$, and put $\zeta := \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$. Since for all $d \in \mathbb{Z}^+$ we have $\sigma^d(\sqrt[n]{a}) = \zeta^d \sqrt[n]{a}$, we have that ζ is a primitive mth root of unity. Since $G := \mathrm{Aut}(L/K)$ is cyclic of order m, for all $d \mid m$ there is a unique subgroup $H_d := \langle \sigma^d \rangle$ of order $\frac{m}{d}$ and these are the only subgroups of G. In particular, if $d_0(m)$ denotes the number of positive divisors of m, then $d_0(m)$ is the number of subgroups of G and thus, by Galois theory, also the number of subextensions of L/K.

For $d \mid m$ and $i \in \mathbb{Z}^+$, we have that σ^i fixes $K(\sqrt[d]{a})$ pointwise if and only if

$$\sqrt[d]{a} = (\sqrt[n]{a})^{n/d} = \sigma^i((\sqrt[n]{a})^{n/d}) = \zeta^{in/d}\sqrt[d]{a}$$

if and only if $m \mid \frac{in}{d}$. The least $i \in \mathbb{Z}^+$ that satisfies this condition is $\gcd(\frac{n}{d}, m)$, so

$$\mathrm{Aut}(L/K(\sqrt[d]{a})) = H_{\gcd(\frac{n}{d},m)}.$$

As d ranges over all divisors of n, the values of $\gcd(\frac{n}{d}, m)$ are precisely all the divisors of m, so the set $\{K(\sqrt[d]{a}) \mid d \mid n\}$ consists of $d_0(m)$ different subextensions of L/K, which by the above, means they account for all the subextensions. □

If K is a field of characteristic not dividing n but not containing a primitive nth root of unity, there is in general no simple description of the degree n cyclic extensions of K. A lot of work has been done on special cases: for instance **global class field theory** gives a kind of description of all abelian extensions of a number field or function field in one variable over a finite field. Cyclic extensions have a distinguished role to play in this theory (e.g. via the **Hasse Norm Theorem**), but restricting class field theory to the cyclic case does not make it easier.

2.2. The Kummer Pairing. Let F be a field containing a primitive nth root of unity, and let B be a subgroup of $F^\times$ containing $F^{\times n}$. We denote by F_B the compositum of all fields $F(a^{1/n})$ for $a \in B$. This is a possibly infinite compositum of cyclic extensions of exponent dividing n, so it is Galois, with Galois group $G \coloneqq \mathrm{Aut}(F_B/F)$ an inverse limit of cyclic groups of exponent dividing n.

Let $a \in B$, let $\alpha \in \overline{F}$ be an nth root of a, and let $\sigma \in G$. Then $\sigma(\alpha) = \zeta_{\sigma,a}\alpha$, where $\zeta_{\sigma,a} \in \mu_n$ is an nth root of unity. Suppose that we took a different nth root α' of a, so there is an nth root of unity z such that $\alpha' = z\alpha$. Then

$$\frac{\sigma(\alpha')}{\alpha'} = \frac{\sigma(z\alpha)}{z\alpha} = \frac{\sigma(z)}{z}\frac{\sigma(\alpha)}{\alpha} = \zeta_{\sigma,a},$$

since $\mu_n \subseteq F$. Thus we get a well-defined pairing

$$\langle \cdot, \cdot \rangle : G \times B \to \mu_n,\ \langle \sigma, a \rangle \coloneqq \zeta_{\sigma,a},$$

which we call the **Kummer pairing**. If $\sigma_1, \sigma_2 \in G$ and $a \in B$, then

$$\zeta_{\sigma_1\sigma_2,a} = \langle \sigma_1\sigma_2, a \rangle = \frac{(\sigma_1\sigma_2)(\alpha)}{\alpha} = \frac{\sigma_1(\zeta_{\sigma_2,\alpha}\alpha)}{a} = \frac{\zeta_{\sigma_1,a}\zeta_{\sigma_2,a}\alpha}{\alpha} = \zeta_{\sigma_1,a}\zeta_{\sigma_2,a}.$$

Simlarly, applying σ^{-1} to $\sigma(\alpha) = \zeta_{\sigma,a}\alpha$ we find

$$\langle \sigma^{-1}, a \rangle = \langle \sigma, a \rangle^{-1}.$$

Thus, for each $a \in B$, the map $\langle \cdot, b \rangle : G \to \mu_n$ is a group homomorphism. Now let $\sigma \in G$ and $a_1, a_2 \in B$, and choose α_1, α_2 such that $\alpha_1^n = a_1$ and $\alpha_2^n = a_2$. Then

$$\sigma(\alpha_1\alpha_2) = \sigma(\alpha_1)\sigma(\alpha_2) = \zeta_{\sigma,a_1}\zeta_{\sigma,a_2}\alpha_1\alpha_2,$$

so

$$\langle \sigma, a_1a_2 \rangle = \langle \sigma, a_1 \rangle \langle \sigma, a_2 \rangle.$$

Also $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \zeta_{\sigma,a}^{-1}\alpha_1$, so

$$\langle \sigma, a^{-1} \rangle = \langle \sigma, a \rangle^{-1}.$$

Thus, for each fixed $\sigma \in B$, the map $\langle \sigma, \cdot \rangle : B \to \mu_n$ is a group homomorphism. We summarize this as: the Kummer pairing is *bilinear*. For an addiively written commutative group A and $n \in \mathbb{Z}^+$, we put

$$A[n] \coloneqq \{a \in A \mid na = 0\},$$

the **n-torsion subgroup** of A.

LEMMA 8.21. *Let A, B, C be additively written commutative groups, with C finite cyclic of order n. Let $\langle \cdot, \cdot \rangle : A \times A' \to C$ be a bilinear map, with left kernel*

$$K_A \coloneqq \{a \in A \mid\ \forall b \in B, \langle a, b \rangle = 0\}$$

and right kernel

$$K_B \coloneqq \{b \in B \mid\ \forall a \in A, \langle a, b \rangle = 0\}.$$

a) *We have $A/K_A = A/K_A[n]$ and $B/K_B = B/K_B[n]$.*
b) *If one of A/K_A and B/K_B is finite, then so is the other, and the pairing induces an isomorphism from each to the dual group of the other.*

PROOF. It virtually immediate to see that (for any bilinear pairing), we get an induced injection

$$\iota : A/K_A \hookrightarrow \mathrm{Hom}(B/K_B, C)$$

via $a + K_A \mapsto (b + K_B \mapsto \langle a, b \rangle)$.
a) Let $a \in A$. Then for all $b \in B$ we have $\langle na, b \rangle = n\langle a, b \rangle = 0$, so $na \in K_B$, and

thus $A/K_A = A/K_A[n]$. In exactly the same way we see that $B/K_B = B/K_B[n]$.
b) Up to replacing the pairing with its transpose $\langle b, a\rangle^T := \langle a, b\rangle$, we may assume that B/K_B is finite and show that A/K_A is finite. But indeed, if B/K_B and C are both finite, so is $\mathrm{Hom}(B/K_B, C)$, and the injection ι shows that also A/K_A is finite. Since A/K_A and B/K_B are n-torsion, we have $\mathrm{Hom}(A/K_A, C) = (A/K_A)^\vee$ and $\mathrm{Hom}(B/K_B, C) = (B/K_B)^\vee$. Thus ι may be viewed as an injection

$$\psi : A/K_A \hookrightarrow (B/K_B)^\vee,$$

and by switching A and B we also get an injection

$$\psi^T : B/K_B \hookrightarrow (A/K_A)^\vee.$$

Because for a finite commutative group G we have $\#G^\vee = \#G$, from the last two injections we deduce

$$\#A/K_A \leq \#B/BK_B \leq \#A/K_A,$$

so $\#A/K_A = \#B/K_B$. Thus ψ and ψ^T are isomorphisms, completing the proof. □

THEOREM 8.22. *Let $n \in \mathbb{Z}^+$, let F be a field containing a primitive nth root of unity, let B be a subgroup of $F^\times/F^{\times n}$, let F_B/F be the Galois extension obtained by adjoining nth roots of all elements of B, and let $G := \mathrm{Aut}(F_B/F)$. With regard to the Kummer pairing*

$$\langle \cdot, \cdot \rangle : G \times B \to \mu_n$$

defined above, we have:

a) *The left kernel of the pairing is trivial: that is, if $\sigma \in G \setminus \{1\}$, then there is $b \in B$ with $\langle \sigma, b\rangle \neq 1$.*
b) *The right kernel of the pairing is $F^{\times n}$: that is, for $b \in B$, we have $\langle \sigma, b\rangle = 1$ for all $\sigma \in G$ if and only if $b \in F^{\times n}$.*
c) *We have that G is finite if and only if $B/F^{\times n}$ is finite, in which case B is isomorphic to the character group $G^\vee$ of G. In particular, we have*

$$[F_B : F] = \#B. \tag{26}$$

PROOF. a) Let $\sigma \in G$. If for $a \in B$ we have $\langle \sigma, a\rangle = 1$, then if α is an nth root of a, we have $\sigma(\alpha) = \alpha$. So if this holds for all $a \in B$, we have that σ pointwise fixes every element of F_B, hence $\sigma = 1$.
b) Let $a \in B$. If for $\sigma \in G$ we have $\langle \sigma, a\rangle = 1$, then if α is an nth root of a, we have $\sigma(\alpha) = \alpha$. If this holds for all $\sigma \in G$, then $\alpha \in F_B^G = F$, so $a \in F^{\times n}$. Similarly, if $a \in F^{\times n}$, then it has an nth root $\alpha \in F$, hence $\sigma(\alpha) = \alpha$ for all $\sigma \in G$.
c) After establishing a) and b), this part is immediate from Lemma 8.21. □

THEOREM 8.23. *Let $n \in \mathbb{Z}^+$, and let F be a field containing a primitive nth root of unity. For a subgroup B of $F^\times/F^{\times n}$, let F_B/F be the Galois extension obtained by adjoining to F the nth roots of all elements of B. Then the map $B \mapsto F_B$ is an isotone bijection from the set of subgroups of $F^\times/F^{\times n}$ to the set of algebraic Galois extensions that are abelian of exponent dividing n.*

PROOF. Step 1: Let B_1 and B_2 be subgroups of $F^\times/F^{\times n}$. It is clear that if $B_1 \subseteq B_2$ then $F_{B_1} \subseteq F_{B_2}$: thus, the map is isotone. We will show that conversely, if $F_{B_1} \subseteq F_{B_2}$, then $B_1 \subseteq B_2$.

Let $b \in B_1$. Then $F(b^{1/n}) \subseteq F_{B_2}$, so there is a (finitely generated, hence) finite subgroup B_2' of B_2 such that $b^{1/n} \in F_{B_2'}$. It suffices to show that $b \in B_2'$. Put

$$B_3 \coloneqq \langle B_2', b \rangle.$$

Then $F_{B_2'} = F_{B_3}$, so by (28) we have

$$\#B_2' = [F_{B_2'} : F] = [F_{B_3} : F] = \#B_3,$$

and since $B_2' \subseteq B_3$, this gives $B_2' = B_3$, i.e., $b \in B_2'$, as desired.
Step 2: If B_1 and B_2 are two subgroups of $F^\times/F^{\times n}$ such that $F_{B_1} = F_{B_2}$, then Step 1 implies that $B_1 \subseteq B_2$ and $B_2 \subseteq B_1$ and thus $B_1 = B_2$. Thus the map $B \mapsto F_B$ is an isotone injection from the set of subgroups of $F^\times/F^{\times n}$ to the set of algebraic Galois extensions of F that are abelian of exponent dividing n. To complete the proof, let K/F be an algebraic Galois extension that is abelian of exponent dividing n. We need to show that $K = F_B$ for some $B \subseteq F^\times/F^{\times n}$. If $B = \varinjlim B_i$ is a direct limit of subgroups of $F^\times/F^{\times n}$, then it is clear that $F_B = \varinjlim F_{B_i}$, so because every algebraic Galois extension is the direct limit of its finite degree subextensions, we may assume that K/F has finite degree. The finite commutative group $G \coloneqq \mathrm{Aut}(K/F)$ of exponent dividing n can be written as $\prod_{i=1}^d C_i$ where each C_i is a cyclic group. For $1 \leq i \leq d$, put $K_i \coloneqq K^{\prod_{j \neq i} C_j}$, so $K = K_1 \cdots K_d$ and $\mathrm{Aut}(K_i/F) \cong C_i$ is cyclic of exponent $e_i \mid n$. By Theorem 8.18, K_i/F is obtained by adjoining an e_ith root of an element a_i of F, hence also by adjoining an nth root of $b_i = a_i^{n/e_i}$. Thus, taking $B = \langle b_1, \ldots, b_d \rangle$ in $F^\times/F^{\times n}$, we get that $K = F_B$, completing the proof. □

Exercise 8.21. *Let $n \in \mathbb{Z}^+$, let F be a field containing a primitive nth root of unity, and let B be a subgroup of $F^\times/F^{\times n}$. By Theorem 8.22c), when B is finite, we have that B is naturally isomorphic to the character group of $\mathrm{Aut}(F_B/F)$. In the general case, we view B as a locally compact abelian torsion group by giving it the discrete topology.*

a) *Show: B is naturally isomorphic to the Pontrjagin dual of the profinite group $\mathrm{Aut}(F_B/F)$.*
b) *The group B is an n-torsion commutative group. By a theorem of Baer (that applies to every n-torsion commutative group), B is isomorphic to a group of the form $\bigoplus_{i \in I} C_{n_i}$, where I is an index set, each n_i is a positive integer dividing n, and C_{n_i} is a cyclic group of order n_i. Deduce: $\mathrm{Aut}(F_B/B) \cong \prod_{i \in I} C_{n_i}$.*

2.3. The maximal abelian extension of exponent dividing n. Fix $n \in \mathbb{Z}^+$, and let F be a field with algebraic closure $\overline{F}$. For any family $\{F_i/F\}_{i \in I}$ of subextensions of $\overline{F}/F$ in which each F_i is abelian of exponent dividing n, also the compositum $\bigvee_{i \in I} F_i$ is abelian of exponent n. It follows that inside $\overline{F}$ there is a unique *maximal* abelian extension of exponent dividing n, which we will denote here by $F_{(n)}/F$. If F contains a primitive nth root of unity, then by Exercise 8.21 we have that $\mathrm{Aut}(F_{(n)}/F)$ is naturally isomorphic to the Pontrjagin dual of the group $F^\times/F^{\times n}$ of nth power classes. More precisely, by Exercise 8.21, there is a set I and positive integers $n_i \mid n$ such that

$$\mathrm{Aut}(F_{(n)}/F) \cong \prod_{i \in I} C_{n_i},$$

where C_{n_i} is a cyclic group of order n_i.

In the case that $n = \ell$ is a prime number, an ℓ-torsion commutative group B has the canonical structure of an $\mathbb{F}_\ell$-vector space and thus is isomorphic to $\bigoplus_{i \in I} \mathbb{F}_\ell$ (a special case of Baer's Theorem cited in Exercise 8.21) and thus the Pontrajgin dual B^* of B is isomorphic to $\prod_{i \in I} \mathbb{F}_\ell$. Thus for a field F containing a primitive ℓth root of unity, we have the notion of an $\mathbb{F}_\ell$-basis for the $F^\times/F^{\times \ell}$, which we can take as the index set I above.

PROPOSITION 8.24.

a) *An $\mathbb{F}_2$-basis for $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is given by $\{-1, p \mid$ p is a prime number$\}$.*
b) *We have $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \cong \bigoplus_{i=1}^\infty \mathbb{Z}/2\mathbb{Z}$.*
c) *The maximal abelian extension of $\mathbb{Q}$ of exponent 2 is*

$$\mathbb{Q}_{(2)} = \mathbb{Q}(\sqrt{-1}, \sqrt{p} \mid \text{ } p \text{ is a prime number}),$$

and we have

$$\mathrm{Aut}(\mathbb{Q}_{(2)}/\mathbb{Q}) \cong \prod_{i=1}^\infty \mathbb{Z}/2\mathbb{Z}.$$

PROOF. a) Since every nonzero rational number x is of the form $(-1)^\epsilon \prod_{p \text{ prime}} p^{a_p}$ with $a_p \in \mathbb{Z}$ and $a_p = 0$ for all but finitely many p, x is equal to a square times ± 1 times a product of distinct primes. This shows that -1 and the prime numbers span $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Clearly we cannot write -1 as a square times a product of primes since the latter is positive, and we cannot write a prime number p as plus or minus a square $\frac{a^2}{b^2}$ times a product of primes other than p, because after multiplying both sides by p^2, on the set left we have an integer that is precisely divisible by an odd power of p and on the right we have an integer that is precisely divisible by an even power of p, contradicting unique factorization. This shows that -1 together with the prime numbers forms an $\mathbb{F}_2$-linearly independent subset of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.
As discussed above, parts b) and c) follow immediately from part a). □

EXERCISE 8.22. *Let F be any number field. Show:* $\mathrm{Aut}(F_{(2)}/F) \cong \prod_{i=1}^\infty \mathbb{Z}/2\mathbb{Z}$.

3. The equation $t^n - a = 0$

Let F be a field, and let $a \in F^\times$. In this section we analyze the structure of the splitting field of a polynomial $t^n - a = 0$ *without* assuming that the ground field contains a primitive nth root of unity. We closely follow [**La**, §VI.9]. By making the substitution $t \mapsto \alpha t$ for $\alpha \in F^\times$, we see that the answer depends only on the class of $a \in F^\times/F^{\times n}$.

The first question is when $t^n - a \in F[t]$ is irreducible. This is an interesting phenomenon: nth roots are of course ubiquitous in mathematics, and someone with enough "real world experience" will likely have a certain (at least subconscious) conjecture on this. The most obvious conjectures turn out to be incorrect, but they can be fixed to give a clean necessary and sufficient criterion for irreducibility.

Let us first mention one important initial foray: if $F = \mathbb{Q}$, then an element of $\mathbb{Q}^\times/\mathbb{Q}^{\times n}$ has a unique representive by a nonzero integer a that is (nth power)-free,i.e., is not divisible by p^n for any prime p. Then Eisenstein's Criterion tells us:

if for some prime p we have that $p \mid n$ but $p^2 \nmid n$, then $x^n - a$ is irreducible (in $\mathbb{Z}[t]$ and in $\mathbb{Q}[t]$). In particular, for all $n \in \mathbb{Z}^{\geq 2}$ and all primes p, the polynomial $t^n \pm p \in \mathbb{Q}[t]$ is irreducible. So over $\mathbb{Q}$ we are left with the case of nonzero integers a with the property that for all primes p, $p \mid a \implies p^2 \mid a$. (Such numbers are sometimes called "squarefull" or "powerful.") When $n = 2, 3$, the polynomial $t^n - a$ is reducible if and only if it has a root in F if and only if $a \in F^{\times n}$. However, already for $n = 4$ we see that, even over $\mathbb{Q}$, $t^n - a$ may have no rational root but still be reducible: namely, if $a \in \mathbb{Z}$ is not a square, then a^2 is not a fourth power, but

$$t^4 - a^2 = (t^2 + a)(t^2 - a)$$

is reducible. More generally, if n is properly divisible by a prime number p, then for all $a \in F^\times$ we have that $t^n - a^p = (t^{n/p})^p - a^p$ is reducible – it has $t^{n/p} - a$ as a factor, while it has a rational root if and only if $a \in F^{\times \frac{n}{p}}$.

This brings us to the following plausible conjecture: suppose that for all primes $p \mid n$, $a \notin F^{\times p}$. Now must $t^n - a$ be irreducible? Unfortunately not!

EXAMPLE 8.25. *In $\mathbb{Q}[t]$, we have*

$$t^4 + 4 = (t^2 + 2t + 2)(t^2 - 2t + 2).$$

Here we have $n = 4$, so it is divisible precisely by the prime $p = 2$, and $a = -4$, which is not *a square in $\mathbb{Q}$, but the polynomial $t^4 + 4$ is reducible anyway.*

Slightly more generally, if F is a field and $b \in F$, then

$$t^4 + 4b^4 = (t^2 + 2bt + 2b^2)(t^2 - 2bt + 2b^2), \tag{27}$$

even though $-4b^4$ need not be a square in F.

Example 8.25 looks discouraging, but it turns out that it is essentially the only thing wrong with our plausible conjecture. Here is the complete answer:

EXERCISE 8.23. *Let a be an element of a field F, and let $m \mid n$ be positive integers. Show: if $t^n - a \in F[t]$ is irreducible, then also $t^m - a \in F[t]$ is irreducible.*

THEOREM 8.26. *Let $n \geq 2$, let F be a field, and let $a \in F^\times$. The following are equivalent:*

(i) *The polynomial $f(t) := t^n - a \in F[t]$ is irreducible.*
(ii) *Both of the following hold:*
- *For all prime numbers $p \mid n$, we have $a \notin F^p$; and*
- *If $4 \mid n$, then $a \notin -4F^4$.*

PROOF. $\neg$ (ii) $\implies$ $\neg$ (i): If for some prime $p \mid n$ we have that $a = b^p$, then writing $n = dm$ for some $m \in \mathbb{Z}^+$, we have

$$f = (t^m)^p - b^p = (t^m - b)((t^m)^{p-1} + \ldots + b^{p-1})$$

is reducible. Now suppose that $4 \mid n$ and that there is $b \in F$ with $a = -4b^4$. Then $t^4 - a$ is reducible by (27), so by Exercise 8.23, also $t^n - a$ is reducible.
(ii) $\implies$ (i): We begin by establishing several special cases.
Step 1: Suppose that $n = p^e$ is a prime power, $a \in F \setminus F^p$ and p is the characteristic of F. This case is covered by Lemma 4.6.
Step 2: Suppose that $n = p$ is a prime that is *not* the characteristic of F and that $a \in F \setminus F^p$. We will show that $t^p - a \in F[t]$ is irreducible. Assume not: then there

is a root α of $t^p - a$ in $\overline{F}$ with $[F(\alpha) : F] = d < p$. Let N denote the norm map from $F(\alpha)$ to F. Since $\alpha^p = a$, we have

$$N(\alpha)^p = N(a) = a^d.$$

Since p is prime, we have $\gcd(d, p) = 1$, and thus there are $x, y \in \mathbb{Z}$ such that $xd + yp = 1$, so

$$a = a^{xd}a^{up} = (N(\alpha)^x a^u)^p \in F^p,$$

a contradiction.

Step 3: Suppose that $e \in \mathbb{Z}^+$, p is an *odd* prime that is not the characteristic of F and $a \in F \setminus F^p$. We will show that $t^{p^e} - a \in F[t]$ is irreducible by induction on e, the $e = 1$ case having been Step 2. Seeking a contradiction, suppose that $\alpha \in F(\alpha)^p$: thus, there is $\beta \in F(\alpha)$ with $\beta^p = \alpha$. Again letting N denote the norm from $F(\alpha)$ to F. Because the minimal polynomial of α is $t^p - a$, we have $N(\alpha) = (-1)^p a$; since p is odd, we get:

$$a = (-1)^p N(\alpha) = (-N(\beta))^p \in F^p,$$

a contradiction. Now we write

$$t^p - a = \prod_{i=1}^{p} (t - \alpha_i),$$

with $\alpha_1, \ldots, \alpha_p \in \overline{F}$ and $\alpha_1 = \alpha$. Substituting $t^{p^{e-1}}$ for t, we have

$$t^{p^e} - a = \prod_{i=1}^{p} (t^{p^{e-1}} - \alpha_i),$$

and let $A \in \overline{F}$ be a root of $t^{p^{e-1}} - \alpha \in F(\alpha)[t]$. By induction, we have

$$[F(\alpha, A) : F] = [F(\alpha, A) : F(\alpha)][F(\alpha) : F] = p^e.$$

Since A is a root of $t^{p^e} - a$, it follows that $t^{p^e} - a \in F[t]$ is irreducible.

Step 4: Now suppose that we are in the setup of Step 3 except that $p = 2$. Then the above argument will work provided that we can show $\alpha \notin F(\alpha)^2$. Assuming for the sake of a contradiction that $\alpha \in F(\alpha)^2$, as in Step 3 we find that $-a \in F^2$, but now in order to derive a contradiction we need to use the additional hypothesis $a \notin -4F^4$ of condition (ii) of the statement. Since $-a = b \in F^2$ and $a \notin F^2$, we have $i = \sqrt{-1} \notin F$. So in $F(i)$ we have

$$t^{2^e} - a = t^{2^e} + b^2 = (t^{2^{e-1}} + ib)(t^{2^{e-1}} - ib).$$

We will show that $t^{2^{e-1}} + ib \in F(i)[t]$ is irreducible; then so is $t^{2^{e-1}} - ib \in F(i)[t]$, and by uniqueness of factorization in univariate polynomial rings and the fact that $i \notin F$, this implies that $t^{2^e} - a \in F[t]$ is irreducible. By induction on e it suffices to show that ib is neither a square nor minus a fourth power in $F(i)$, but since $i \in F(i)^2$, it suffices to show that $ib \notin F(i)^2$. We do so quite honestly: suppose there are $c, d \in F$ such that

$$ib = (c + di)^2 = (c^2 - d^2) + 2cdi.$$

Then $d = \pm c$ and $ib = \pm 2c^2 i$; squaring, we get

$$a = -b^2 = -4c^4,$$

a contradiction.

Step 5: Finally we treat the general case of $t^n - a$, where a satisfies condition (ii) of

the statement. We go by induction on n, and we may assume assume that $n = p^e m$ for a prime $p > 2$ and $\gcd(m, p) = 1$. Much as above, if we write

$$t^m - a = \prod_{i=1}^{m} (t - \alpha_i)$$

with $\alpha_1, \ldots, a_m \in \overline{F}$ and put $\alpha = \alpha_1$, then

$$t^n - a = \prod_{i=1}^{m} (t^{p^e} - \alpha_i.)$$

By induction, we may assume that $t^m - a \in F[t]$ is irreducible. We CLAIM that $\alpha \notin F(\alpha)^p$. Assuming the claim, by the previous steps we know that if $t^{p^e} - \alpha \in F(\alpha)[t]$ is irreducible, so if $A \in \overline{F}$ is a root of this polynomial, then

$$[F(\alpha, A) : F] = [F(\alpha, A) : F(\alpha)][F(\alpha) : F] = p^e m = n,$$

and since A is a root of $t^n - a$, it follows that $t^n - a \in F[t]$ is irreducible.

We finish anticlimactically: if there is $\beta \in F(\alpha)$ with $\beta^p = \alpha$, then

$$a = (-1)^m N(\alpha) = ((-1)^m N(\beta))^p,$$

so $a \in F^p$, a contradiction. □

The following is an immediate consequence.

COROLLARY 8.27. *Let p be a prime number, F a field, and $a \in F \setminus F^p$.*

a) *If p is odd or $p = \mathrm{char}(K) = 2$, then $t^p - a$ is irreducible if and only if $t^{p^n} - a$ is irreducible for all $n \geq 1$.*
b) *If $p = 2 \neq \mathrm{char}(K)$, then $t^4 - a$ is irreducible if and only if $t^{2^n} - a$ is irreducible for all $n \geq 2$.*

Here is a less precise but easier to remember consequence of Theorem 8.26

EXERCISE 8.24. *Let F be a field, let $n \in \mathbb{Z}^+$, and let $a \in F^\times$. Suppose that for all primes $p \mid n$ we have that neither a nor $-a$ lies in $F^{\times p}$. Show: $t^n - a \in F[t]$ is irreducible.*

Let F be a field. Let n be a positive integer that is not divisible by the characteristic of F, let $a \in F^\times$, and let K be the splitting field of the separable polynomial $f := t^n - a$. We address the following question: what is the Galois group $G := \mathrm{Aut}(K/F)$ of f? Let α be a root of f in K, so $K = F(\alpha, \zeta_n)$. Then an element $\sigma \in G$ is determined by its action on α and ζ_n, and we have

$$\sigma(\alpha) = \zeta^{b(\sigma)}\alpha,\ b(\sigma) \in \mathbb{Z}/n\mathbb{Z},$$

$$\sigma(\zeta_n) = \zeta_n^{d(\sigma)},\ d(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Consider the group

$$G(n) := \left\{ \begin{bmatrix} 1 & 0 \\ b & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \right\}.$$

The identity

$$\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & d^{-1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ bd & 1 \end{bmatrix}.$$

shows that the subgroup

$$N = \left\{ \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \right\}$$

is normal. It also cyclic of order n, and it follows easily that

$$G(n) \cong \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times,$$

with the homomorphism given by the canonical isomorphism

$$\varphi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}\, \mathbb{Z}/n\mathbb{Z}.$$

A straightforward computation shows that the commutator subgroup of $G(n)$ is contained in N; since $G(n)/N \cong (\mathbb{Z}/n\mathbb{Z})^\times$ is commutative, N must be the commutator subgroup of $G(n)$. The map $\sigma \mapsto d(\sigma)$ is precisely the modulo n cyclotomic character χ_n, so $\zeta_n \in F \iff G \subseteq N$. In general, let $X_n \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ be the image of the cyclotomic character, viewed as a subgroup of diagonal matrices $\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}$ as above. Then

$$G \subseteq G_\chi(n) \coloneqq \mathbb{Z}/n\mathbb{Z} \rtimes X_n,$$

so it is natural to ask under what conditions we have $G = G_\chi(n)$.

PROPOSITION 8.28. *With hypotheses and notation as above, the following are equivalent:*

(i) $G = G_\chi(n)$.
(ii) *The polynomial $t^n - a$ remains irreducible in $F(\zeta_n)$.*
(iii) *We have $F(\sqrt[n]{a}) \cap F(\zeta_n) = F$.*

PROOF. We have $\#G_\chi(n) = n \cdot \#X_n$ and

$$\#G = [K : F] = [F(\sqrt[n]{a}, \zeta_n) : F]$$
$$= [F(\sqrt[n]{a}, \zeta_n) : F(\zeta_n)][F(\zeta_n) : F] = [F(\sqrt[n]{a}, \zeta_n) : F(\zeta_n)]\#X_n,$$

so

$$G = G_\chi(n) \iff [F(\sqrt[n]{a}, \zeta_n) : F(\zeta_n)] = n.$$

By Proposition 8.19, the degree $[F(\sqrt[n]{a}, \zeta_n) : F(\zeta_n)]$ is equal to the order of a in $F(\zeta_n)^\times / F(\zeta_n)^{\times n}$, which is n if and only if $t^n - a \in F(\zeta_n)[t]$ is irreducible: this shows (i) $\iff$ (ii).
We also have

$$\#G = [F(\sqrt[n]{a}, \zeta_n) : F(\sqrt[n]{a})][F(\sqrt[n]{a}) : F] = n[F(\sqrt[n]{a}, \zeta_n) : F(\sqrt[n]{a})],$$

so $G = G_\chi(n)$ if and only if $[F(\sqrt[n]{a}, \zeta_n) : F(\sqrt[n]{a})] = \#X_n$. Since $F(\zeta_n)/F$ is Galois, by Natural Irrationalities we have

$$[F(\sqrt[n]{a}, \zeta_n) : F(\sqrt[n]{a})] = [F(\zeta_n) : F(\zeta_n) \cap F(\sqrt[n]{a})]$$

and the latter quantity is $\#X_n$ if and only if $F(\zeta_n) \cap F(\sqrt[n]{a}) = F$. □

Here is one case where it is easy to see that the conditions of Proposition 8.28 hold:[4]

PROPOSITION 8.29. *Suppose $t^n - a$ is irreducible and* $\gcd(n, \varphi(n)) = 1$. *Then*

$$G = G_\chi(n) = \mathbb{Z}/n\mathbb{Z} \rtimes X_n.$$

EXERCISE 8.25. *Prove Proposition 8.29.*

[4]Cases of this show up frequently on University of Georgia's PhD level qualifying exams.

The following is a more substantial contribution:

THEOREM 8.30. *Let n be an* odd *positive integer not divisible by the characteristic of F, and suppose that $[F(\zeta_n) : F] = \varphi(n)$: equivalently, the mod n cyclotomic character is surjective. Let $a \in F$ be such that $a \in F \setminus F^p$ for all primes $p \nmid n$. Let K be the splitting field of $t^n - a$ over F, and let $G := \mathrm{Aut}(K/F)$ be its Galois group. Then $G = G(n)$, and the commutator subgroup of G is $\mathrm{Aut}(K/F(\zeta_n))$.*

PROOF. Since n is odd, by Theorem 8.26 the polynomial $t^n - a$ is irreducible in F. Let $\alpha \in K$ be a root, so $[F(\alpha) : F] = n$.
Step 1: Suppose $n = p$ is prime. Since $\gcd(p, \varphi(p)) = \gcd(p, p-1) = 1$, Proposition 8.29 applies to give $G = G(n)$. The commutator subgroup is N, which is precisely the set of automorphisms that pointwise fix ζ_n, so the commutator subgroup is $\mathrm{Aut}(K/F(\zeta_n))$. (This latter argument holds in the general case.)
Step 2: Now suppose that n is composite; we may write $n = pm$ with p prime. Since the mod n cyclotomic character is surjective and $m \mid n$, also the mod m cyclotomic character is surjective. Put $\beta := \alpha^p$, so of course β is a root of $t^m - a$, and by induction the result applies to $t^m - a$. In particular we have

$$n = pm = [F(\alpha) : F] = [F(\alpha) : F(\beta)][F(\beta) : F],$$

so $[F(\alpha) : F(\beta)] = p$. This implies that $t^p - \beta$ is irreducible over $F(\beta)$: otherwise, the minimal polynomial of α over $F(\beta)$ would have degree less than p, contradiction. Consider the subfield

$$L := F(\alpha) \cap F(\beta, \zeta_n) \subset K.$$

Certainly $F(\beta) \subset L$. On the other hand, $L/F(\beta)$ is an abelian extension. On the other hand, L is also the splitting field of $t^p - \beta$ over $F(\beta)$, so by Step 1, the maximal abelian subextension of $K/F(\beta)$ is $F(\beta, \zeta_p)$, and thus

$$L \subset F(\alpha) \cap F(\beta, \zeta_p) = F(\beta) :$$

if it were any larger, then $F(\alpha)$ would contain a nontrivial subextension of $F(\zeta_p)/F$, contradicting $[F(\zeta_n) : F] = \varphi(n)$. Thus

$$[F(\alpha, \zeta_n) : F(\beta, \zeta_n)] = p :$$

if not, then these fields would be equal and thus

$$F(\beta) \subseteq F(\alpha) \subseteq F(\beta, \zeta_n),$$

so $F(\alpha)/F(\beta)$ would be abelian, again contradicting Step 1. An argument identical to the above but using induction instead of Step 1 shows that

$$F(\zeta_n) \cap F(\beta) = F$$

and then using Natural Irrationalities we get

$$[F(\beta, \zeta_n) : F(\beta)] = [F(\zeta_n) : F] = \varphi_n.$$

It follows that

$$[K : F] = [K : F(\beta, \zeta_n)][F(\beta, \zeta_n) : F(\zeta_n)][F(\zeta_n) : F] = n\varphi(n) = \#G(n),$$

so $\mathrm{Aut}(K/F) = G_n$. The conclusion on commutator subgroups follows. □

EXERCISE 8.26.

a) *Let $a \in \mathbb{Z}^+$, and let $f_a(t) := x^4 + a^2 \in \mathbb{Q}[t]$. Show: f_a is irreducible if and only if $2a \notin \mathbb{Q}^{\times 2}$.*

b) *Suppose that f_a is irreducible. Show: the splitting field of f_a is $\mathbb{Q}(\sqrt{2a}, \sqrt{-1})$, which is Galois over $\mathbb{Q}$ with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus the conclusion of Theorem 8.30 does not hold here: $[K : F] = \frac{n\varphi(n)}{2}$, not $n\varphi(n)$.*

Later, in Corollary 9.18, we will show that if $x^4 + b \in \mathbb{Q}[t]$ is irreducible and $-b \notin \mathbb{Q}^{\times 2}$, then the Galois group of the splitting field of $x^4 + b$ is $G(4) \cong D_4$.

EXERCISE 8.27. *Let $n \in \mathbb{Z}^{\geq 6}$ be even.*

a) *Show: the cyclotomic field $\mathbb{Q}(\zeta_n)$ has a quadratic subfield different from $\mathbb{Q}(\sqrt{-1})$, hence of the form $\mathbb{Q}(\sqrt{a})$ for a squarefree integer $a \neq \pm 1$.*
b) *Show: the polynomial $g_a := t^n - a \in \mathbb{Q}[t]$ is irreducible but becomes reducible over $\mathbb{Q}(\zeta_n)[t]$.*
c) *Let $K/\mathbb{Q}$ be the splitting field of g_a, and let $G := \mathrm{Aut}(K/\mathbb{Q})$. Show: G is a proper subgroup of $G(n)$.*

These exercisess exploited the fact (a consequence of Proposition 8.28) that if $n \in \mathbb{Z}^+$ is even, $a \in \mathbb{Q}^\times$ is such that $x^n - a \in \mathbb{Q}[t]$ is irreducible and $\sqrt{a} \in \mathbb{Q}(\zeta_n)$, then the Galois group G of the splitting field of $x^n - a$ is a proper subgroup of $G_\chi(n) = G(n)$. Remarkably, the converse is true: when n is even, we have $G = G(n)$ if and only if $\sqrt{a} \notin \mathbb{Q}(\zeta_n)$. This was shown by Jacobson–Vélez in [**JV90**]. This we can check whether $G = G(n)$ by knowing the quadratic subfields of $\mathbb{Q}(\zeta_n)$: cf. Exercise 8.20. Under the same hypotheses, Jacobson–Vélez show there is $s \in \mathbb{N}$ such that

$$\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt[2^s]{a})$$

and for this s we have

$$[G(n) : G] = 2^s.$$

They go on to compute the group G in every case when $F = \mathbb{Q}$.

EXAMPLE 8.31. *Let F be a field of characteristic 0, let $a \in F^\times$ be such that for all $n \in \mathbb{Z}^+$ the polyomial $t^n - a \in F[t]$ is irreducible: as above, for this it is necessary that for all primes p we have $a \notin F^{\times p}$, and if this holds and moreover neither a nor $-a$ lies in $F^{\times 2}$, then $t^n - a$ is irreducible for all $n \in \mathbb{Z}^+$. For $n \in \mathbb{Z}^+$, let K_n/F be the splitting field of $t^n - a$, and let $K = \bigcup_{n \in \mathbb{Z}^+} K_n$. Viewing $\mathbb{Z}^+$ as being directed under the divisibility relation, we have that $K = \varinjlim_n K_n$ is an algebraic Galois extension that is the direct limit of the finite Galois extensions, so if $G_n := \mathrm{Aut}(K_n/K)$, then $G := \mathrm{Aut}(K/F) = \varprojlim_n G_n$. Since each G_n is a subgroup of $\mathbb{Z}/n\mathbb{Z} \rtimes X_n = \mathbb{Z}/n\mathbb{Z} \rtimes \chi_n(\mathfrak{g}_F)$, we have that G is a closed subgroup of $\hat{\mathbb{Z}} \rtimes \chi(\mathfrak{g}_F)$, which is itself a closed subgroup of $\hat{\mathbb{Z}} \rtimes \chi(\mathfrak{g}_F)$.*
• *We have that $\chi(\mathfrak{g}_F) = \{e\}$ if and only if $F \supseteq \mathbb{Q}^{\mathrm{cyc}}$, i.e., if and only if $F \supseteq \mu_n$ for all $n \in \mathbb{Z}^+$. In this case $G \cong \hat{\mathbb{Z}}$. This holds for instance when $F = \mathbb{C}((t))$ is the field of Laurent series over $\mathbb{C}$ (the fraction field of the domain $\mathbb{C}[[t]]$) of formal power series over $\mathbb{C}$) and $a := t$. Indeed, for $n \in \mathbb{Z}^+$, the element t has order n in $F^\times/F^{\times n}$, which by Kummer Theory implies that $x^n - t \in F[x]$ is irreducible. Thus*

$$\mathrm{Aut}(\mathbb{C}((t))(\{t^{1/n}\}_{n \in \mathbb{Z}^+})/\mathbb{C}((t))) \cong \hat{\mathbb{Z}}.$$

This becomes more interesting if we augment it with the following two claims, whose proofs come from valuation theory:
(i) For all $n \in \mathbb{Z}^+$, we have $\mathbb{C}((t))(t^{1/n}) = \mathbb{C}((t^{1/n}))$.
It is clear that the left hand side is contained in the right, but the converse is less obvious, since formal Laurent series are infinite sums. One can show this by noting

that the formal Laurent series field $\mathbb{C}((t))$ *is* complete *for the norm* $||x|| \coloneqq 2^{-}v(x)$*, where* $v(0) \coloneqq \infty$ *and for* $x = \sum_{n \geq N} a_n t^n$ *with* $a_N \neq 0$*, we put* $v(x) \coloneqq N$*. Then* $K_n = C((t))(t^{1/n})$ *is a finite degree extension of a complete normed field, and thus the norm extends uniquely to a norm* $|| \cdot ||_n$ *on* K_n*, which is also complete* [**Cl-NTII**, Thm. 1.43]*. The field* $\mathbb{C}((t^{1/n}))$ *is complete for a norm extending the norm on* $\mathbb{C}((t))$ *– it is essentially the same norm as on* $\mathbb{C}((t))$*, except now the map* v *takes values in* $1/n\mathbb{Z} \cup \{\infty\}$ *, which restricts to a norm on* K_n *extending the norm on* $\mathbb{C}((t))$*, which must be the norm* $|| \cdot ||_n$ *above. Thus* $\mathbb{C}((t^{1/n}))/K_n$ *is an extension of complete normed fields, but it is clear that* K_n *is dense in* $\mathbb{C}((t^{1/n}))$*: for* $x \in \mathbb{C}((t^{1/n}))$*, the (finite!) partial sums of* x *lie in* K_n *and converge to* x*. So we must have* $K_n = \mathbb{C}(t^{1/n}))$*. Here we did not use that the coefficients of the Laurent series were complex numbers: for any field* k*, we have* $k((t))(t^{1/n}) = k((t^{1/n}))$*.*
(ii) The ***Puiseux series field*** $K = \bigcup_n \mathbb{C}((t^{1/n}))$ *is algebraically closed. This follows from the structure theory of complete normed fields* [**Cl-NTII**, Thm. 2.66]*. Putting these two facts together, we get that* $K = \mathbb{C}((t))(\{t^{1/n}\}_{n \in \mathbb{Z}^+})$ *is the algebraic closure of the field* $\mathbb{C}((t))$ *of Laurent series, and thus the absolute Galois group* $\mathfrak{g}_{\mathbb{C}((t))}$ *of* $\mathbb{C}((t))$ *is isomorphic to* $\hat{\mathbb{Z}}$*. This is a rare example where we can construct the algebraic closure of a field explicitly. In a sense that we will explore carefully later in this chapter, the algebraic closure of* $\mathbb{C}((t))$ *is "solvable by radicals."*
• *Let us now take* $F \coloneqq \mathbb{R}((t))$ *and* $a \in t$*. Because* $x^n - t$ *is irreducible in* $\mathbb{C}((t))$ *for all* $n \in \mathbb{Z}^+$*, certainly it is irreducible in* $\mathbb{R}((t))$*. This time the image of the cyclotomic character is* $\chi(\mathfrak{g}_F) = \{\pm 1\}$ *(because complex conjugaton acts on* μ_n *by inversion) We claim that in this case, for all* $n \in \mathbb{Z}^{\geq 3}$ *we have* $G_n \cong \mathbb{Z}/n\mathbb{Z} \rtimes \{\pm 1\}$ *is the dihedral group* D_n *of order* $2n$*, so*

$$G \cong \hat{\mathbb{Z}} \rtimes \{\pm 1\}$$

is the profinite dihedral group. Indeed: for $n \geq 3$ *the extension* $F(t^{1/n})/F$ *has degree* n *and is not normal, because* $F(t^{1/n}) \cong \mathbb{R}((t^{1/n}))$ *does not contain a primitive* n*th root of unity, so we have*

$$F(t^{1/n}) \subsetneq K_n \subseteq \mathbb{C}((t))(t^{1/n}) = F(t^{1/n}, \sqrt{-1}),$$

so $[K_n : F] = 2n$ *and* $G_n = \mathbb{Z}/n\mathbb{Z} \rtimes \{\pm 1\}$*. Because* $K = \bigcup_n \mathbb{R}((t))(t^{1/n}, \zeta_n) = \bigcup_n \mathbb{C}((t^{1/n}))$ *is algebraically closed, this shows that the absolute Galois group of* $\mathbb{R}((t))$ *is isomorphic to the profinite dihedral group* $\hat{\mathbb{Z}} \rtimes \{\pm 1\}$*. Again this means that the algebraic closure of* $\mathbb{R}((t))$ *is solvable by radicals, and again this is the exception rather than the rule.*

EXERCISE 8.28. *Let* $x \in \mathbb{S}$ *be a supernatural number such that: if* $2^2 \mid x$ *then* $2^\infty \mid x$*, and for all primes* $p > 2$*, if* $p \mid x$*, then* $p^\infty \mid x$*. Show: there is an algebraic extension* $K/\mathbb{R}((t))$ *such that* $|\mathfrak{g}_K| = x$*.*

4. Artin–Schreier Theory

Let p be a prime number, and let F be a field of characteristic p. Our goal is to study extensions K/F that are cyclic of degree p. In this regard the Kummer Theory of §9.2 breaks down completely: if $\zeta \in F$ is such that $\zeta^p = 1$, then since are in characterstic p we have

$$0 = \zeta^p - 1 = (\zeta - 1)^p,$$

so $\zeta = 1$. It follows that the only p-power root of unity in characteristic p is 1. This definitively kills the Kummer-theoretic approach to cyclic extensions of §9.2.

Happily, there is something to take its place. We consider the map

$$\wp : F \to F,\ x \mapsto x^p - x.$$

This map is *not* a field homomorphism. However, for all $x, y \in F$ we have

$$\wp(x+y) = (x+y)^p - (x+y) = x^p + y^p - x - y = \wp(x) + \wp(y),$$

so it is an endomorphism of the additive group $(F, +)$ of F. Its kernel is $\{x \in F \mid x^p - x = 0\}$, which is the prime subfield $\mathbb{F}_p$. (The existence of a nontrivial kernel shows that $\wp$ is not a field homomorphism.) Borrowing somewhat geometric language, we call the $\wp$ the **Artin–Schreier isogeny**.

THEOREM 8.32. *Let F be a field of characteristic $p > 0$, and let $a \in F$.*

a) *The following are equivalent:*
   (i) *The polynomial $f_a := t^p - t - a \in F[t]$ is irreducible.*
   (ii) *We have $a \notin \wp(F)$: that is, there is no $\alpha \in F$ such that $\alpha^p - \alpha = a$.*

b) *When the equivalent conditions hold, the splitting field K/F of f_a is a cyclic Galois extension of degree p.*

PROOF. a) (i) $\implies$ (ii): An irreducible polynomial of degree $p > 1$ has no rational roots.
(ii) $\implies$ (i): Suppose that f_a has no root in F and let $\alpha \in \overline{F}$ be a root of f. Since $\wp$ is an additive group homomorphism with kernel $\mathbb{F}_p$, for all $i \in \mathbb{F}_p$ we have

$$f_a(\alpha + i) = \wp(\alpha + i) - a = \wp(\alpha) + \wp(i) - a = \wp(\alpha) - a = f_a(\alpha) = 0.$$

This shows that the roots of f_a in $\overline{K}$ are the p distinct elements

$$\alpha_i := \alpha + (i-1),\ 1 \le i \le p.$$

It follows that for all $1 \le i \le p$ we have $F(\alpha) = F(\alpha_i)$. Notice that f_a is separable, hence a product of distinct irreducible factors. Let $p_1 \in F[t]$ be the minimal polynomial of α_1. We want to show that $p_1 = f_a$, i.e., that every α_i is a root of p_1. If not, $1 \le i_2 \le p$ be least such that α_{i_2} is not a root of p_2. If $f_a \neq p_1 p_2$, let $1 \le i_3 \le p$ be least such that α_{i_3} is not a root of $p_1 p_2$, and so forth. Eventually we get $f_a = p_1 \cdots p_r$. But for all $1 \le j \le r$, the degree of p_j is $[F(\alpha_{i_j}) : F] = [F(\alpha) : F]$. So all these degrees are equal and their product is p; since f_a has no root in F, none of the degrees is 1, so it must be that $r = 1$ and $f = p_1$ is irreducible.
b) If f_a is irreducible, then it follows from our proof of part a) that if $\alpha \in \overline{F}$ is any root of f_a then $F(\alpha)$ is the splitting field of f_a, so it is a Galois extension of prime degree p, so it is cyclic. □

EXERCISE 8.29. *Let $a \in F \setminus \wp(F)$, let $\alpha \in \overline{K}$ be a root of f_a, and let $K = F(\alpha)$. Show: there is a unique $\sigma \in \mathrm{Aut}(K/F)$ such that $\sigma(\alpha) = \alpha + 1$, so $\mathrm{Aut}(K/F) = \langle \sigma \rangle$.*

Let $a \in F \setminus \wp(F)$. It follows from Theorem 8.32 that $t_a = t^p - t - a \in F[t]$ is irreducible and that for any two elements $\alpha, \beta \in \overline{F}$ such that $\wp(\alpha) = \wp(\beta) = a$ we have that $F(\alpha) = F(\beta)$ is the splitting field for f_a. Because of this we write $F(\wp^{-1}(a))$ for this common field: although $\wp^{-1}(a)$ consists of p different elements, they each generate the same field. Conversely, every cyclic field extension of degree p in characteristic p is generated by an "Artin–Schreier root":

THEOREM 8.33. *Let F be a field of characteristic p, and let K/F be cyclic of degree p. Then there is $a \in F \setminus \wp(F)$ such that $K = F(\wp^{-1}(a))$.*

PROOF. Let σ be a generator of the cyclic group $\mathrm{Aut}(K/F)$. Since $\mathrm{Tr}_{K/F}(-1) = -p = 0$, by Theorem 7.35 there is $\alpha \in K$ such that $-1 = \alpha - \sigma(\alpha)$, or equivalently

$$\sigma(\alpha) = \alpha + 1.$$

It follows that $\alpha \notin F$ and since K/F has degree p we must have $K = F(\alpha)$. Put

$$a \coloneqq \wp(\alpha) = \alpha^p - \alpha.$$

Then

$$\sigma(a) = \sigma(\alpha)^p - \sigma(\alpha) = (\alpha+1)^p - (\alpha+1) = \alpha^p - \alpha = a,$$

so $a \in F$ and $K = F(\wp^{-1}(a))$. □

EXAMPLE 8.34. *For a prime power $q = p^k$, we consider "the" finite field $\mathbb{F}_q$. For $a \in \mathbb{F}_q^\times$, as above consider $f_a \coloneqq t^p - t - a$. Theorem 8.32 tells us that f_a is irreducible if and only if it has no root in $\mathbb{F}_q$. For all $x \in \mathbb{F}_p$, we have $f_a(x) = x^p - x - a = -a \neq 0$, so if $q = p$ this shows that f_a is irreducible. But because $x^p = x$ is the charateristic property of elements of $\mathbb{F}_p$, this argument will not work when $q > p$. Rather, we consider the Artin–Schreier isogeny $\wp : \mathbb{F}_q \to \mathbb{F}_q$ by $x \mapsto x^p - x$. As mentioned above, $\wp$ is an endomorphism of the additive group $(\mathbb{F}_q, +)$, and as just mentioned, its kernel is precisely $(\mathbb{F}_p, +)$. It follows that its image $\wp(\mathbb{F}_q)$ is an additive subgroup of order p^{k-1}, and it follows that*

$$\mathbb{F}_q/\wp(\mathbb{F}_q) \cong (\mathbb{Z}/p\mathbb{Z}, +).$$

So we may choose $a \in \mathbb{F}_q \setminus \wp(\mathbb{F}_q)$, in which case f_a is irreducible, and for any $\alpha \in \overline{\mathbb{F}_q}$ with $f_a(\alpha) = 0$, we have that $\mathbb{F}_q(\alpha)/\mathbb{F}_q$ is an abelian extension of degree p.

Of course we already knew not only that $\mathbb{F}_q$ has a degree p abelian extension, but that (within $\overline{\mathbb{F}_q}$) it has a unique *degree p abelian extension. So we should be able to see that if we choose $a, b \in \mathbb{F}_q \setminus \wp(\mathbb{F}_q)$ and $\alpha, \beta \in \overline{\mathbb{F}_q}$ such that*

$$\wp(\alpha) = \alpha^p - \alpha = a, \ \ \wp(\beta) = \beta^p - \beta = b,$$

then $\mathbb{F}_q(\alpha) = \mathbb{F}_q(\beta)$. They key is that by our above computation, a and b generate the same subgroup of $\mathbb{F}_q/\wp(\mathbb{F}_q)$: indeed, they both generate this cyclic group of order p. So there is $1 \leq n < p$ and $z \in \mathbb{F}_q$ such that $na - b = z^p - z$. It follows that

$$\wp(n\alpha - \beta) = n\wp(\alpha) - \wp(\beta) = na - b = \wp(z^p - z),$$

so there is $i \in \mathbb{F}_p$ such that

$$n\alpha - \beta = z^p - z + i \in \mathbb{F}_q,$$

and it follows that

$$\mathbb{F}_q(\alpha) = \mathbb{F}_q(\beta).$$

The argument made at the end of Example 8.34 works more generally: if F is a field of characteristic $p > 0$ and $a, b \in F$ lie in the same nonzero coset of $\wp(F)$, then taking $\alpha, \beta \in \overline{F}$ with $\wp(\alpha) = a$ and $\wp(\beta) = b$, we have $F(\alpha) = F(\beta)$. Remarkably, the converse of this also holds, as we will now show.

EXAMPLE 8.35. *Let k be a field of characteristic $p > 0$, let $F \coloneqq k(t)$ and let $a \in k[y]$ be a polynomial of degree $d \geq 1$. Suppose there is $x \in F$ such that $x^p - x = a$. Then x is integral over $k[t]$ and $k[t]$ is integrally closed, so we must have $x \in k[t]$. Let x have degree D, which clearly must be positive. Then the degree of x^p is pD, which is larger than the degree of x, so the degree of $x^p - x$ is pD. Since $x^p - x$, this means that $d = pD$, i.e., d is a multiple of p. This shows that if the degree of a is* not *divisible by p, then by Theorem 8.32 the polynomial $x^p - x - a \in F[x]$ is irreducible and $F(\wp^{-1}(a))/F$ is cyclic of degree p.*

EXERCISE 8.30. *Let k be a field of characteristic $p > 0$, and Let $K \coloneqq k((t))$ be the field of formal Laurent series over k.*

a) *For $f \in k((t))^\times$, we may uniquely write $f = \sum_{n \geq N} a_n t^n$ with $a_N \neq 0$, and we put $\operatorname{ord}(f) \coloneqq N$. We put $\operatorname{ord}(0) \coloneqq \infty$. Show: for $f, g \in k((t))$, we have*
$$\operatorname{ord}(f+g) \geq \min \operatorname{ord}(f), \operatorname{ord}(g)$$
and
$$\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g).$$
b) *Let $f \in k((t))$ be such that $\operatorname{ord}(f)$ is negative and not divisible p. Show: $f \notin \wp(K)$.*
c) *For every positive integer n that is not divisible by p, put $f_n \coloneqq t^{-n}$. Show: if $n_1 \neq n_2$, then f_{n_1} and f_{n_2} generate distinct subgroups of $K/\wp(K)$.*

4.1. The Artin–Schreier Pairing. Again, F is a field of characteristic $p > 0$. For a subgroup B of $F/\wp(F)$, we put
$$F_B \coloneqq F(\wp^{-1}(B))$$
be the extension of F obtained by adjoining Artin-Schreier roots of elements of B. Then F_B is a compositum of cyclic extensions of exponent p, hence it is an abelian extension of exponent dividing p,[5] possibly of infinite degree. Let $G \coloneqq \operatorname{Aut}(F_B/F)$; we will view G as a multiplicative group. Let $a \in b$, let $\alpha \in \wp^{-1}(a)$ be an Artin–Schreier root of a, and let $\sigma \in G$. Then $\sigma(\alpha)$ is a root of the polynomial $t^p - t - a$, hence (by the proof of Theorem 8.32) of the form $\alpha + i_{\sigma,a}$ for some $i_{\sigma,a} \in \mathbb{Z}/p\mathbb{Z}$. Suppose we took a different Artin-Schreier root $\alpha' \in \wp^{-1}(a)$. Then $\alpha' = \alpha + j$ for some $j \in \mathbb{Z}/p\mathbb{Z}$, so
$$\sigma(\alpha') - \alpha' = \sigma(\alpha + j) - (\alpha + j) = \sigma(\alpha) - \alpha = i_{\sigma,a}.$$
Thus we get a well-defined pairing
$$\langle \cdot, \cdot \rangle : G \times B \to \mathbb{Z}/p\mathbb{Z}, \ \langle \sigma, b \rangle \mapsto i_{\sigma,b},$$
called the **Artin–Schreier pairing**.

EXERCISE 8.31. *With notation as above, show that the Artin–Schreier pairing $\langle \cdot, \cdot \rangle : G \times B \to \mathbb{Z}/p\mathbb{Z}$ is bilinear. That is:*

a) *Show: for all $\sigma_1, \sigma_2, \sigma \in G$ and $b \in B$ we have*
$$\langle \sigma_1 \sigma_2, b \rangle = \langle \sigma_1, b \rangle + \langle \sigma_2, b \rangle$$
and
$$\langle \sigma^{-1}, b \rangle = -\langle \sigma, b \rangle.$$

[5]More precisely, F_B/F has exponent p unless $F_B = F$. We will shortly see that this occurs if and only if $B = \{0\}$.

b) *Show: for all* $\sigma \in G$ *and* $b_1, b_2 \in B$ *we have*

$$\langle \sigma, b_1 b_2 \rangle = \langle \sigma, b_1 \rangle + \langle \sigma, b_2 \rangle$$

and

$$\langle \sigma, -b \rangle = -\langle \sigma, b \rangle.$$

The following results are such close analogues of Theorem 8.22 that its proof may be left as an exercise.

THEOREM 8.36. *Let* F *be a field of characteristic* $p > 0$*, let* B *be a subgroup of* $F/\wp(F)$*, let* F_B/F *be the Galois extension obtained by adjoining Artin–Schreier roots of all elements of* B*, and let* $G \coloneqq \mathrm{Aut}(F_B/F)$*. With regard to the pairing*

$$\langle \cdot, \cdot \rangle : G \times B \to \mathbb{Z}/p\mathbb{Z}.$$

defined above, we have:

a) *The left and right kernels of the pairing are trivial.*
b) *We have that* G *is finite if and only if* B *is finite, in which case* B *is isomorphic to the character group* $G^\vee$ *of* G*. In particular, we have*

$$[F_B : F] = \#B. \tag{28}$$

THEOREM 8.37. *Maintain the notation of Theorem 8.37. The mapping* $B \mapsto F_B$ *is an isotone bijection between the set of subgroups of* $F/\wp(F)$ *and the set of algebraic Galois extensions of* F *of exponent dividing* p*.*

EXERCISE 8.32.

a) *Prove Theorem 8.36.*
b) *Prove Theorem 8.37.*

EXERCISE 8.33. *Let* F *be a field of characteristic* $p > 0$*, let* B *be a subgroup of* $F/\wp(F)$*, let* F_B/F *be the extension obtained by adjoining Artin–Schreier roots of the elements of* B*, and let* $G \coloneqq \mathrm{Aut}(F_B/F)$*. By Theorem 8.36, when* B *is finite,it is naturally isomorphic to the character group of* G*. In the general case, we view* B *as a locally compact abelian torsion group by giving it the discrete topology. Show:* B *is naturally isomorphic to the Pontrjagin dual of the profinite group* G*.*

EXERCISE 8.34. *Let* k *be a field of characteristic* $p > 0$*, and let* $K \coloneqq k(t)$*.*

a) *Show:* $K/\wp(K)$ *is infinite.*
b) *Let* $F_{(p)}/F$ *be the maximal abelian extension of* F *of exponent dividing* p*. Show:* $F_{(p)}/F$ *has infinite degree.*

EXERCISE 8.35. *Let* $\mathbb{F}_q$ *be a finite field, and let* $F \coloneqq \mathbb{F}_q((t))$ *be the Laurent series field.*

a) *Show:* $F/\wp(F)$ *is countably infinite.*
b) *Let* $K \coloneqq F_{F/\wp(F)}$*, so* K/F *is the maximal abelian extension of exponent* p*, and let* $G \coloneqq \mathrm{Aut}(K/F)$*. Show: as topological groups, we have*

$$G \cong \prod_{n=1}^{\infty} (\mathbb{Z}/p\mathbb{Z}, +).$$

5. Interlude on Finite Solvable Groups

Let G be a group. A **subnormal sequences** in G is a finite sequence

$$G_0 = \{1\} \subsetneq G_1 \subsetneq \ldots \subsetneq G_N = G$$

in which for all $0 \leq i \leq N-1$, we have that G_i is a proper, normal subgroup of G_{i+1}. The **length** of the sequence is N: thus the length is the number of inclusions, which is one less than the number of groups in the sequence. Given two subnormal sequences in G, we say that the second series **refines** the first if the second contains all of the subgroups in the first: this is a partial ordering on the set of all normal sequences in G. A **Jordan–Hölder sequence** is a subnormal sequence that is *maximal*, i.e., admits no proper refinement. A subnormal sequence $\{G_i\}_{i=0}^N$ in G is maximal if and only if for all $0 \leq i \leq N-1$ we have that G_i is a maximal normal subgroup of G_{i+1} if and only if for all $0 \leq i \leq N-1$, the quotient group G_{i+1}/G_i is a simple group. For $1 \leq i \leq N$, we put $S_i \coloneqq G_i/G_{i-1}$, and we refer to the elements of the associated sequence $(S_1, \ldots, S_N)$ as the **Jordan–Hölder factors**.

For a positive integer N with prime factorization $p_1^{a_1} \cdots p_r^{a_r}$, we put $\Omega(N) \coloneqq \sum_{i=1}^r a_i$, i.e., the number of prime factors of N counted with multiplicity. (We put $\Omega(1) \coloneqq 0$.) The length of a normal sequence in a finite group G is at most $\Omega(\#G)$, so G admits a Jordan–Hölder sequence. (An infinite group may or may not admit a Jordan–Hölder sequence; here we are only concerned with finite groups.) By convention, the trivial group has no Jordan–Hölder factors.

THEOREM 8.38 (Jordan–Hölder). *Let G be a group that admits a Jordan–Hölder sequence, and let $\{H_i\}_{i=0}^{N_1}$ and $\{K_i\}_{i=0}^{N_2}$ be two subnormal sequences in G.*

a) *We have $N_1 = N_2$: any two Jordan–Hölder sequences in G have the same length. Let us write $N = N_1 = N_2$. We call N the **length** $\ell(G)$ of G.*

b) *Let $(S_1, \ldots, S_N)$ be the Jordan-Hölder factors of the sequence $\{H_i\}$ – thus $S_i = H_i/H_{i-1}$ – and let $(T_1, \ldots, T_N)$ be the Jordan–Hölder factors of the sequence $\{K_i\}$ – thus $T_i = K_i/K_{i-1}$. Then there is a bijection $\sigma : \{1, \ldots, N\} \to \{1, \ldots, N\}$ such that for all $1 \leq i \leq N$, the simple groups H_i and K_i are isomorphic.*

Thus Theorem 8.38 associates to any finite group G a finite sequence of simple groups that is well-determined up to permutation. A slightly different way of looking at this is to consider the Jordan-Hölder factors to be a *finite multiset* of isomorphism classes of finite simple groups: i.e., each finite simple group occurs with finite multiplicity (possibly 0) and the sum of all the multiplicities is the length $\ell(G)$. This gives a sense in which finite simple groups are the building blocks for all finite groups. However, given such a set $(S_1, \ldots, S_N)$ of building blocks we can in general build multiple finite groups out of them: more precisely, nonisomorphic groups can have the same multiset of Jordan–Hölder factors, the simplest example being C_{p^2} and $C_p \times C_p$, where C_n denotes a cyclic group of order n.

A finite group G is **solvable** if all of its Jordan–Hölder factors are commutative, in which case they must all have prime order. Otherwise put, finite solvable groups are the finite groups G with $\ell(G) = \Omega(\#G)$.

EXERCISE 8.36. *Show: a finite group G is solvable if and only if it admits a subnormal sequence $\{G_i\}_{i=0}^n$ (*not *necessarily maximal) such that G_i/G_{i-1} is commutative for all $1 \leq i \leq n$.*

(In fact, admitting a subnormal sequence with commutative successive quotients is the *definition* of solvability for an arbitrary group G, but we only need the finite case here.) In particular, a finite commutative group is solvable. However, the converse does not hold. Indeed, most finite p-groups are not commutative, but:

PROPOSITION 8.39. *Finite p-groups are solvable.*

PROOF. Let G be a finite p-group. Then G acts on itself by conjugation, and the orbits are the conjugacy classes in G. Thus each conjugacy class $C(g)$ in G is isomorphic as a G-set to $G/\operatorname{Stab}(g)$, which shows that each nontrivial conjugacy class has size a power of p. Since the sum of the sizes of the conjugacy classes is $\#G$, which is also a power of p, it follows that the number of trivial conjugacy classes must be divisible by p. Since $C(1) = \{1\}$ is a trivial conjugacy class, there must be at least one more trivial conjugacy class, i.e., the center $Z(G)$ of G is nontrivial. From this it follows that a finite p-group is simple if and only if it has order p.

Again, let G be a finite p-group. Then every Jordan–Hölder factor of G is a finite, simple p-group, hence by the above argument is isomorphic to C_p. Thus G is solvable. □

EXAMPLE 8.40.

a) *Consider the symmetric group S_3. Since A_3 has order 3, $[S_3 : A_3] = 2$ and index 2 subgroups are normal, it is immediate that*

$$\{1\} \subsetneq A_3 \subsetneq S_3$$

is a Jordan–Hölder sequence in S_3. Thus the Jordan–Hölder factors of S_3 are (C_2, C_3) and S_3 is solvable but not commutative.

b) *Consider the symmetric group S_4. We define the* ***Klein 4-group***

$$V := \{e,\ (12)(34),\ (13)(24),\ (14)(23)\},$$

which is a subgroup of A_4. Because two elements in a symmetric group S_n are conjugate if and only if they have the same cycle type and the nontrivial elements of V are all the elements of S_4 of cycle type $(2,2)$, we have that V is a normal subgroup of S_4, hence certainly it is normal in A_4. Again, index 2 subgroups are normal, so it is now clear that

$$\{1\} \subsetneq \{(12)(34)\} \subsetneq V \subsetneq A_4 \subsetneq S_4$$

is a Jordan–Hölder sequence in S_4, with composition factors (C_2, C_2, C_2, C_3), so S_4 is solvable but not commutative.

THEOREM 8.41. *Let $N \in \mathbb{Z}^{\geq 5}$.*

a) *The alternating group A_N is a finite simple group.*

b) *The* unique *Jordan–Hölder sequence in S_N is $\{1\} \subsetneq A_N \subsetneq S_N$.*

PROOF. For part a), see e.g. [**La**, Thm. I.5.5]. b) First we claim that A_N is the unique index 2 subgroup of S_N. Indeed, let H be any index 2 subgroup of S_N. Then H is normal and is determined as the kernel of a surjective homomorphism $q : S_N \to C_2$. Since the elements τ of S_N of cycle type (12) – i.e., the **transpositions** – form a conjugacy class and a set of generators for S_N, we must have $q(\tau) \neq 1$ for all such τ (because q must take the same value on all τ, and if this value were 1 then q would be trivial). Thus H contains every product of an even number of transpositions, so H contains A_N and thus $H = A_N$.

Now because $\{1\} \subseteq A_N \subsetneq S_N$ is a Jordan–Hölder sequence in S_N, we know

that G has length 2 and composition factors A_N and C_2. So a nontrivial, proper normal subgroup of G that is not A_N has order 2, hence is generated by an order 2 element lying in the center of S_N, but this is absurd: every cycle type other than $(1, 1, \ldots, 1)$ occurs with more than one element, so the center of S_N is trivial. □

EXERCISE 8.37. *Show: the conclusion of Theorem 8.41b) also holds for $N \in \{2, 3\}$ but not for $N = 4$.*

We will now give an alternate characterization of solvability for finite groups using the "derived sequence." Recall that for elements x and y in a group G, we define the **commutator**

$$[x, y] \coloneqq xyx^{-1}y^{-1}.$$

The first thing to say is that x and y commute if and only if $[x, y] = 1$, so all commutators are trivial in G if and only if G is commutative. Writing x^g for $g^{-1}xg$, one immediately checks that for all $x, y, g \in G$, we have

$$[y, x]^{-1} = [x, y]$$

and

$$[x^g, y^g] = [x, y]^g.$$

We define the **commutator subgroup** (or **derived subgroup**) G' to be the subgroup generated by all commutators $[x, y]$ for $x, y \in G$. In general, the product of commutators is not a commutator, but the above identities show that the set of all finite products of commutators is closed under taking inverses and under conjugation, which in particular shows that G' is a *normal subgroup* of G. The quotient map $G \to G/G'$ is universal for homomorphisms from G into a commutative group H, and in particular for any normal subgroup N of G we have that the quotient G/N is commutative if and only if N contains G'.
Now we continue the process: we define $G^{(0)} = G$ and for $n \in \mathbb{Z}^{\geq 0}$,

$$G^{(n+1)} \coloneqq (G^{(n)})'.$$

Thus

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(n)} \supseteq \ldots$$

is a decreasing sequence of normal subgroup of G, called the **derived sequence**. If G is finite (again, the case of interest to us here) then at some point we must have $G^{(n)} = G^{(n+1)}$, and that point the derived sequence stabilizes.

THEOREM 8.42. *A finite group G is solvable if and only if $G^{(n)} = \{1\}$ for some $n \in \mathbb{Z}^+$.*

PROOF. Let $n \in \mathbb{N}$ be minimal such that $G^{(n)} = \{1\}$; if $n \leq 1$ then G is commutative, hence solvable, so we may and shall assume that $n \geq 2$. Then

$$\{1\} = G^{(n)} \subsetneq G^{(n-1)} \subsetneq G^{(1)} \subsetneq G^{(0)} = G$$

is a normal sequence with commutative successive quotients, so G is solvable.

Conversely, suppose that G is solvable, and let $\{G_i\}_{i=0}^N$ be a subnormal sequence with commutative successive quotients. Because G_0/G_1 is commutative, we must have $G' \subseteq G_1$. Now let $n \in \mathbb{Z}^+$ and inductively suppose that $G^{(n)} \subseteq G_n$. Again, beacuse G_n/G_{n+1} is commutative, we must have $G^{(n+1)} = (G^n)' \subseteq G_n' \subseteq G_{n+1}$. It follows by induction that $G^{(n)} \subseteq G_n$ for all n, and thus $G^{(N)} = \{1\}$. □

THEOREM 8.43. *Let H be a normal subgroup of a finite group G. The following are equivalent:*

(i)) *The group G is solvable.*

(ii)) *Both of the groups H and G/H are solvable.*

PROOF. If $\{H_i\}_{i=0}^{N_1}$ is a Jordan–Hölder squence for H and $\{K_i\}_{i=0}^{N_2}$ is a Jordan–Hölder sequence for G/H, then viewing each K_i as a subgroup of G containing H, we may splice these sequences together:

$$\{1\} = H_0 \subsetneq \ldots \subsetneq H_{N_1-1} \subsetneq H \subsetneq K_1 \subsetneq \ldots \subsetneq G$$

to get a Jordan–Hölder sequence for G. This shows that the multiset of Jordan–Hölder factors of G is "multiunion" of the multisets of Jordan–Hölder factors of H and of G/H – in other words, for each isomorphism class of finite simple group S, we add the multiplicities to which S occurs in H and in G/H to get the multiplicity to which it occurs in G. Now it is clear that all the Jordan–Hölder factors of G are prime order cyclic if and only if the same holds for the Jordan–Hölder factors of both H and of G/H. □

Notice that if a finite group G is commutative and H is a normal subgroup of G, then both H and G/H are commutative. However the converse is not true. (Moreover, in between commutative and solvable lies the class of finite nilpotent groups – among other things, these are the finite groups for which every Sylow subgroup is normal – and the same remark holds here.) The group S_3 gives a specific counterexample. But more to the point, solvable groups are the smallest class of finite groups containing all finite commutative groups and closed under taking extensions (i.e., if H and G/H belong to the class, then so does G).

6. Solvability by Radicals in Characteristic 0

Throughout this section we restrict to fields F of characteristic 0. All field extensions of F will be algebraic, lying inside a fixed algebraic closure $\overline{F}$ of F.

A **simple radical extension** is an extension $F(\alpha)/F$, where α satisfies a polynomial $f \in F[t]$ of the form $t^n - a$ for some $n \in \mathbb{Z}^+$ and some $a \in F$.

EXERCISE 8.38. *Show: the class of simple radical field extensions (in characteristic 0) satisfies the base-change meta-property (DC2) of §3.4.*[6]

Let K/F be a finite degree field extension. A **radical chain** for K/F is a finite sequence of the form $(\alpha_1, n_1, \ldots, \alpha_k, n_k)$ where $\alpha_1, \ldots, \alpha_k$ are elements of K, $n_1, \ldots, n_k$ are positive integers, and for all $0 \leq i \leq k-1$, we have that[7]

$$\alpha_{k+1}^{n_{k+1}} \in F(\alpha_1, \ldots, \alpha_k).$$

The **index set** of a radical chain is $\{n_1, \ldots, n_k\}$.

Thus a finite degree field extension K/F admits a radical chain if and only if it admits a sequence of subfields

$$F = L_0 \subsetneq L_1 \subsetneq \ldots \subsetneq L_{n-1} \subsetneq L_n = F \tag{29}$$

[6]We will see later that this class does *not* satisfy either meta-property (DC1) or (DC3).

[7]Here and hereafter, when we write $F(\alpha_1, \ldots, \alpha_0)$, we mean F.

such that for all $0 \leq i \leq n-1$, the extension L_{i+1}/L_i is a simple radical extension, and we call this tower of field extensions a **radical tower**. We say that K/F is a **radical extension** if it admits a radical chain (equivalently, a radical tower).

EXERCISE 8.39. *Let K/F be a radical extension. Show: K/F admits a radical chain whose index set consists of prime numbers.*

It is immediate from the definition that the class of radical extensions of characteristic 0 fields satisfies *half* of the tower meta-property: if K/F and L/K are radical extensions, then so is L/F. We will see later that if $F \subseteq K \subseteq L$ are finite degree field extensions with L/F radical, then K/F need not be radical (but L/K must be, a special case of the base-change meta-property). But as we saw in §3.4, this is all we need to deduce that if K_1, K_2 are radical extensions of F, then so is K_1K_2/F: K_1K_2/K_1 and K_1/F are radical, hence K_1K_2/F is radical.

EXERCISE 8.40. *Let F be a field of characteristic 0, with algebraic closure $\overline{F}$, and let $\sigma \in \mathrm{Aut}(\overline{F})$. Let K/F be a finite degree subextension of $\overline{F}/F$.*

a) *Show: if K/F is a simple radical extension, then so is $\sigma(K)/\sigma(F)$.*
b) *Show: if K/F is a radical extension, then so is $\sigma(K)/\sigma(F)$.*

Let F be a field, and let $\alpha \in \overline{F}$. We say that α is **solvable by radicals** if α is contained in a radical extension of F. We say that an algebraic extension K/F is **solvable by radicals** if every element of K is solvable by radicals.

EXERCISE 8.41. *We work throughout with fields of characteristic 0.*

a) *Show: the finite degree extensions that are solvable by radicals form a distinguished class.*
b) *Show: algebraic field extensions that are solvable by radicals form a distinguished class.*

LEMMA 8.44. *Let K/F be a radical field extension, and let $(\alpha_1, n_1, \ldots, \alpha_k, n_k)$ be a radical chain for K/F. Let L be the normal closure of K/F. Then L/F admits a radical chain with index set $\{n_1, \ldots, n_k\}$.*

PROOF. Let $\mathrm{Aut}(L/F) = \{\sigma_1, \ldots, \sigma_r\}$. Then $K = F(\alpha_1, \ldots, \alpha_k)$, so

$$L = F(\sigma_1(\alpha_1), \ldots, \sigma_r(\alpha_1), \sigma_1(\alpha_2), \ldots, \sigma_r(\alpha_2), \ldots, \sigma_1(\alpha_k), \ldots, \sigma_r(\alpha_k).$$

It follows that

$$(\sigma_1(\alpha_1), n_1, \ldots, \sigma_r(\alpha_1), n_1, \sigma_1(\alpha_2), n_2, \ldots, \sigma_r(\alpha_2), n_2, \ldots,$$
$$\sigma_1(\alpha_k), n_k, \ldots, \sigma_r(\alpha_k), n_k)$$

is a radical chain for L/F, since for all $1 \leq i \leq r$ and $1 \leq j \leq k-1$ we have

$$\sigma_i(\alpha_j)^{n_j} = \sigma_i(\alpha_j^{n_j}) \in \sigma_i(F(\alpha_1, \ldots, \alpha_{i-1})) = F(\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_{j-1})). \qquad \square$$

Now we can state and prove a very famous theorem of young Évariste Galois:

THEOREM 8.45 (Galois). *Let F be a field of characteristic 0, let K/F be a finite degree field extension, let L be the normal closure of K/F, and put $G \coloneqq \mathrm{Aut}(L/F)$. The following are equivalent:*

(i) *The extension K/F is solvable by radicals.*
(iii) *The finite group G is solvable.*

PROOF. (i) $\implies$ (ii): Suppose that K/F is solvable by radicals, so it is contained in a radical extension K_1/F. Let L_1 be the normal closure of K_1/F. Then $L \subseteq L_1$, which by Lemma 8.44 is also a radical extension. Since $G = \mathrm{Aut}(L/F)$ is a quotient of $\mathrm{Aut}(L_1/F)$ and quotients of solvable groups are solvable, it is no loss of generality to assume that $K_1 = K$ and $L_1 = L$, or in other words that K/F is itself a radical extension. Choose a radical chain for L/F with radical tower

$$F = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_k = L \tag{30}$$

and index set $\{n_1, \ldots, n_k\}$, and put $N = \mathrm{lcm}(n_1, \ldots, n_k)$. Let ζ_N be a primitive Nth root of unity. Then $L(\zeta_N)/F(\zeta_N)$ is Galois, and we may lift the radical chain from F to $F(\zeta_N)$, getting a radical tower

$$F(\zeta_N) = F_0(\zeta_N) \subseteq \ldots \subseteq F_k(\zeta_N) = L(\zeta_N) \tag{31}$$

with index set $\{n_1, \ldots, n_k\}$. If $L(\zeta_N) = F(\zeta_N)$, then L is contained in an abelian extension of F, and we're done. Otherwise, we may remove repetitions in the tower (31), possibly shrinking the index set: still every index divides N. By Proposition 8.16, for $0 \leq i \leq k-1$, the extension $F_{i+1}(\zeta_N)/F_i(\zeta_N)$ is cyclic. For $0 \leq i \leq k$, put $H_i \coloneqq \mathrm{Aut}(L(\zeta_N)/F_{k-i}(\zeta_N))$. Then

$$\{e\} = H_0 \subsetneq H_1 \subsetneq \ldots \subsetneq H_k = \mathrm{Aut}(L(\zeta_N)/F(\zeta_N))$$

is a subnormal series of $H_k = \mathrm{Aut}(L(\zeta_N)/F(\zeta_N))$ with cyclic successive quotients, so $\mathrm{Aut}(L(\zeta_N)/F(\zeta_N))$ is a solvable group. Finally, $\mathrm{Aut}(L(\zeta_N)/F(\zeta_N))$ is a normal subgroup of $\tilde{G} = \mathrm{Aut}(L(\zeta_N)/F)$ whose quotient, $\mathrm{Aut}(F(\zeta_N)/F)$ is abelian, which shows that $\tilde{G}$ is a solvable group, hence so is its quotient $G = \mathrm{Aut}(L/F)$.
(ii) $\implies$ (i): Suppose that $G = \mathrm{Aut}(L/F)$ is solvable. Let N be the product of all primes p dividing $\#G$. Suppose we can show that $L(\zeta_N)/F(\zeta_N)$ is solvable by radicals. Then there is a radical extension $F'/F(\zeta_N)$ containing $L(\zeta_N)$. But also $F(\zeta_N)/F$ is a simple radical extension, hence F'/F is a radical extension containing L, so L/F is solvable by radicals.

Put $H \coloneqq \mathrm{Aut}(L(\zeta_N)/F(\zeta_N))$; this is a subgroup of $\mathrm{Aut}(L(\zeta_N)/F)$, which as above is solvable because $\mathrm{Aut}(L/F)$ is solvable and $\mathrm{Aut}(L(\zeta_N)/L)$ is commutative. Let $\{H_i\}_{i=0}^k$ be a Jordan–Hölder sequence for H; putting $F_i \coloneqq L(\zeta_N)^{H_{k-i}}$, we get a tower of field extensions

$$F(\zeta_N) = F_0 \subsetneq F_1 \subsetneq \ldots \subseteq F_r = L(\zeta_N.)$$

Then for all $0 \leq i \leq k-1$, $H_i = \mathrm{Aut}(F_{i+1}/F_i)$ is cylic of order a prime divisor of N, so by Theorem 8.18 each F_{i+1}/F_i is a simple radical extension, and thus $L(\zeta_N)/F(\zeta_N)$ is (radical, hence) solvable by radicals, completing the proof. □

Theorem 8.45 tells us that for a finite degree field extension K/F in characteristic 0, every element of K can be built out of finitely many elements of F using field operations and the extraction of roots if and only if the Galois group of the normal closure of K/F is solvable. In light of this, we abbreviate "solvable by radicals" to **solvable** in this situation.

EXERCISE 8.42. *A profinite group G is **pro-solvable** if it is an inverse limit of finite, discrete groups. Let F be a field of characteristic 0, let K/F be an algebraic field extension, with normal closure L, and let $G \coloneqq \mathrm{Aut}(L/F)$, a profinite group when endowed with the Krull topology. Show that the following are equivalent:*

(i) *The extension K/F is solvable by radicals: that is, every $\alpha \in K$ lies in a (finite degree!) radical extension F'/F.*
(ii) *The group G is pro-solvable.*

EXERCISE 8.43. *Let F be a field of characteristic 0. Show that the following are equivalent:*

(i) *There is no proper finite Galois extension K/F with solvable Galois group.*
(ii) *There is no proper Galois extension K/F with pro-solvable Galois group.*
(iii) *For all $n \geq 2$, the map $x \mapsto x^n$ on F is surjective.*
(iv) *For all primes p, the map $x \mapsto x^p$ on F is surjective.*

*A field satisfying these equivalent conditions is said to be **solvably closed**.*

The following exercise shows that solvability is faithfully preserved by solvable lifts.

EXERCISE 8.44. *Let F be a field of characteristic 0, and let $K, L/F$ be finite degree field extensions. Suppose that K/F is solvable. Show: KL/K is solvable if and only if L/F is solvable.*

EXERCISE 8.45. *State and prove a version of the previous exercise for algebraic extensions.*

We now turn to the subject of "radical formulas." For any field F and any separable degree n polynomial $f \in F[t]$, let K/F be the splitting field of f; then the **Galois group of f** is $G \coloneqq \mathrm{Aut}(K/F)$. After ordering the roots of f in K as $\alpha_1, \ldots, \alpha_n$, we may view G as a subgroup of S_n, since every $\sigma \in G$ determines, and is determined by, a permutation of $\alpha_1, \ldots, \alpha_n$. Let us suppose moreover that F has characteristic 0. Then Galois's Theorem tells us that there are radical expressions for each of $\alpha_1, \ldots, \alpha_n$ if and only if G is a solvable group.

As the results of this section were derived for fields of characteristic 0, let us now make that assumption again. Then we have derived a remarkable transition between the cases $n \leq 4$ and $n \geq 5$. If $n \leq 4$, then G is a subgroup of the solvable group S_n so is itself solvable. Thus for *every polynomial* f of degree at most 4 there are radical expressions for the roots of f. In particular, consider the **generic polynomial of degree n**

$$f = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in \mathbb{Q}(a_0, \ldots, a_{n-1});$$

that is, the coefficients of f are independent indeterminates. Then if $n \leq 4$ we have a radical expression for the roots of f in terms of the coefficients $a_0, \ldots, a_{n-1}$.

When $n = 2$, this is extremely familiar: the roots of $t^2 + a_1 t + a_0$ are

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}.$$

Suppose now that $n = 3$ or 4. We have shown, in a sense, the existence of cubic and quartic formulas: given any *particular* irreducible cubic or quartic polynomial f over any field F, there are radical expressions for each of the roots of f. But in the quadratic case, away from characteristic 2 we had one formula that worked for all polynomials at once. As will prove just below, if we view $a_0, \ldots, a_{n-1}$ as independent indeterminates over $\mathbb{Q}$, then the polynomial

$$f = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in \mathbb{Q}(a_0, \ldots, a_{n-1}[t]$$

has Galois group S_n, which since $n = 3$ or 4 means that it is solvable by radicals. The hope is that this "generic formula" will yield a formula for any particular polynomial over a field K of characteristic 0 just by specializing $a_0, \ldots, a_{n-1}$ to be elements of K. The issue here is that the generic formula may have indeterminates in the denominator, which means that for certain "exceptionally chosen" values of $a_0, \ldots, a_{n-1} \in K$, we may be dividing by 0 and thus not get a valid formula. Without entering into the details of the cubic and quartic formulas – as we do not wish to do here – let us say that this does happen, but these degenerate cases can be handled much more easily. For instance, one standard version of the "generic cubic formula" remains valid for all cubics $t^3 + a_1 t + a_0 = 0$ (to which any cubic away from characteristic 3 can be reduced) with $a_1 \neq 0$; but if $a_1 = 0$, then clearly the roots are the three cube roots of $-a_0$.

Now suppose that $n \geq 5$. In §8.3 we observed that for any field k and $n \in \mathbb{Z}^+$, the symmetric group S_n acts by field automorphisms on $k(t_1, \ldots, t_n)$ just by permutation of variables, so $k(t_1, \ldots, t_n)/k(t_1, \ldots, t_n)^{S_n}$ is a finite Galois extension with Galois group S_n. Let us now return to this and establish a little more. For $1 \leq k \leq n$, let $s_k = s_k(t_1, \ldots, t_)) \in k[t_1, \ldots, t_n]$be the kth elementary symmetric polynomial: it is the sum over all $\binom{n}{k}$ degree k monomials in $k[t_1, \ldots, t_n]$ in which no variable appears more than once. For instance, when $n = 4$ we have

$$s_1 = t_1 + t_2 + t_3 + t_4,\ s_2 = t_1t_2 + t_1t_3 + t_1t_4 + t_2t_3 + t_2t_4 + t_3t_4,$$

$$s_3 = t_1t_2t_3 + t_1t_2t_4 + t_1t_3t_4 + t_1t_2t_3,\ s_4 = t_1t_2t_3t_4.$$

Let us note also that clearly the S_n action on the rational function field $k(t_1, \ldots, t_n)$ restricts to an S_n action by ring automorphisms on the polynomial ring $k[t_1, \ldots, t_n]$. For any group G acting by automorphisms on a commutative ring R, we may define the **invariant subring**

$$R^G := \{x \in R \mid \forall \sigma \in G, \sigma(x) = x\}.$$

As the name suggests, each symmetric polynomial s_k lies in the invariant subring $k[t_1, \ldots, t_n]^{S_n}$: this is true (e.g.) because S_n permutes the k element subsets of $\{1, \ldots, n\}$. One of the oldest algebraic results is that the elementary symmetric polynomials generated the invariant subring: that is, every S_n-invariant polynomial in the variables $t_1, \ldots, t_n$ is itself a polynomial, with coefficients in k, in the elementary symmetric polynomials $s_1, \ldots, s_n$. This is part of our next result.

THEOREM 8.46. *Let k be a field, let $n \in \mathbb{Z}^+$, and let $K := k(t_1, \ldots, t_n)$ be a rational function field. For $1 \leq k \leq r$, let $s_k \in k[t_1, \ldots, t_n]$ be the kth elementary symmetric polynomial. Put $F := K^{S_n}$.*

a) *We have $F = k(s_1, \ldots, s_n)$.*
b) *The elements $s_1, \ldots, s_n$ of F are algebraically independent, so as abstract fields, we have $F \cong K$.*
c) *We have $k[t_1, \ldots, t_n]^{S_n} = k[s_1, \ldots, s_n]$.*

PROOF. a) Put $f := (t - t_1) \cdots (t - t_n) \in K[t]$. Then just by multiplying out f, we find:

$$f = t^n - s_1t^{n-1} + s_2t^{n-2} - \ldots + (-1)^{n-1}s_{n-1}t + (-1)^n s_n \in k(s_1, \ldots, s_n)[t].$$

Now, the splitting field of the polynomial $f \in k(s_1, \ldots, s_n)[t]$ is manifestly $k(t_1, \ldots, t_n)$, so $k(t_1, \ldots, t_n)/k(s_1, \ldots, s_n)$ is a finite Galois extension. Because it is the splitting

field of a degree n polynomial, the degree of this extension is at most $n!$. On the other hand, permutation of variables gives a faithful S_n-action on $k(t_1, \ldots, t_n)$ that fixes $k(s_1, \ldots, s_n)$ pointwise, so we must have

$$\mathrm{Aut}(k(t_1, \ldots, t_n)/k(s_1, \ldots, s_n)) = S_n.$$

It follows that

$$F = K^{S_n} = k(t_1, \ldots, t_n)^{\mathrm{Aut}(k(t_1,\ldots,t_n)/k(s_1,\ldots,s_n))} = k(s_1, \ldots, s_n).$$

b) Here we need to borrow a bit from the theory of transcendental field extensions, covered in Chapter 10 (so the reader may prefer to come back to this part later). In the tower of field extensions $k \subset k(s_1, \ldots, s_n) \subset k(t_1, \ldots, t_n)$, the latter extension has finite degree, so the transcendence degree of $k(s_1, \ldots, s_n)/k$ is equal to the transcendence degree of $k(t_1, \ldots, t_n)/k$, which is k. If the set $t_1, \ldots, t_n$ were not algebraically independent, then for some i the extension $k(t_1, \ldots, t_n)/k(t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n)$ would be algebraic and thus the transcendence degree of $k(t_1, \ldots, t_n)/k$ would be at most $n - 1$, a contradiction.

c) Our argument essentially follows one of Gauss from 1815. First, let $f \in k[t_1, \ldots, t_n]$. We may write $f = \sum_{i=0}^d f_i$ for $f_i \in [t_1, \ldots, t_n]$ homogeneous of degree i, and then for all $\sigma \in S_n$, also $\sigma(f_i)$ is homogeneous of degree i. It follows that $f \in k[t_1, \ldots, t_n]^{S_n}$ if and only if $f_i \in k[t_1, \ldots, t_n]^{S_n}$ for all i. Thus it suffices to show that any nonzero *homogeneous* $f \in k[t_1, \ldots, t_n]^{S_n}$ lies in $k[s_1, \ldots, s_n]$.

We endow the set of monomials in $k[t_1, \ldots, t_n]$ with the *lexicographic order*: that is for distinct monomials $m_a = t_1^{a_1} \cdots t_n^{a_n}$ and $m_b = t_1^{b_1} \cdots t_n^{b_n}$, we put $m_a \prec m_b$ if for the least i such that $a_i \neq b_i$ we have $a_i < b_i$. This gives a well-ordering on monomials (or equivalently, on $\mathbb{N}^N$). This gives every nonzero element of $k[t_1, \ldots, t_n]$ a *leading term*, corresponding to the largest monomial.

Coming back to our nonzero homogeneous symmetric $f \in k[t_1, \ldots, t_n]^{S_n}$, say of degree $d \geq 1$, by symmetry its leading term is of the form $c_1 t_1^{a_1} \cdots t_n^{a_n}$ for $a_1 \geq \ldots \geq a_n$. Let

$$g_1 := c_1 s_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_n^{a_n}.$$

Then g_1 is also symmetric, homogeneous of degree d and with the same leading term as f_1. So $f_2 := f - g_1$ is symmetric, homogeneous of degree d with a smaller leading term, say $c_2 t_1^{b_1} \cdots t_n^{b_n}$. So: put

$$g_2 := c_2 s_1^{b_1 - b_2} s_2^{b_2 - b_3} \cdots s_n^{b_n}.$$

Then $f_3 := f_2 - g_2 = f - g_1 - g_2$ is still symmetric, homogeneous of degree d with yet smaller leading term, and so forth. Clearly this process must terminate at some point – on the one hand, our ordering $\prec$ on monomials is a well-ordering; but even simpler, all of our monomials have the same degree d, of which there are only finitely many. Thus there is $N \in \mathbb{Z}^+$ and $h_1, \ldots, h_N \in k[s_1, \ldots, s_n]$ such that $f = g_1 + \ldots + g_N$. Clearly then $f \in k[s_1, \ldots, s_n]$, completing the proof. □

EXERCISE 8.46. *This exercise concerns the proof of Theorem 8.46c).*

a) *Show that the polynomials g_1 and f have the same leading term.*

b) *Confirm that the proof works to show: for any commutative ring R,*

$$R[t_1, \ldots, t_n]^{S_n} = R[s_1, \ldots, s_n].$$

This is the ***Fundamental Theorem on Symmetric Polynomials****.*

Theorem 8.46 implies that the polynomial $(t-t_1)\cdots(t-t_n) \in k(t_1,\ldots,t_n)[t]$ is a **generic polynomial over k**: its coefficients are algebraically independent. Thus we find that the generic polynomial over any field k has Galois group S_n. Applying Galois's Theorem, we get:

THEOREM 8.47 (Abel-Ruffini). *Let k be a field. For $n \geq 5$, the generic polynomial of degree n is not solvable by radicals.*

We now return to constructible numbers. We will complete the proof of the Gauss–Wantzel Theorem on constructibility of the regular n-gon, but first we will give a strikingly clean Galois-theoretic characterization of constructible numbers:

THEOREM 8.48. *For an algebraic number $\alpha \in \mathbb{C}$, the following are equivalent:*

(i) *α is constructible.*
(ii) *The Galois group of the minimal polynomial of α is a 2-group.*

PROOF. Let L be the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$, and let $G \coloneqq \mathrm{Aut}(L/\mathbb{Q})$.
(i) $\implies$ (ii): By Theorem 2.9, the algebraic number α is constructible if and only if it is "solvable by quadratics over $\mathbb{Q}$": that is, if and only if $\mathbb{Q}(\alpha)$ is contained in an extension K_1/F given by a radical chain with index set $\{2\}$. By Lemma 8.44, the normal closure L_1 of $K_1/\mathbb{Q}$ is also given by a radical chain with index set $\{2\}$, so every nontrivial quadratic extension in the corresponding radical tower is quadratic. Thus $\mathrm{Aut}(L_1/\mathbb{Q})$ is a 2-group, hence so is its quotient $\mathrm{Aut}(L/Q)$.
(ii) $\implies$ (i): If G is a 2-group, then by Proposition 8.39 it admits a Jordan–Hölder sequence whose successive quotients are cyclic of order 2, which corresponds by Galois theory to a tower of quadratic extensions

$$\mathbb{Q} = F_0 \subsetneq F_1 \subsetneq \ldots F_k = L.$$

Thus $\alpha \in L$ is constructible. □

Theorem 8.48 explains our earlier remark that just because the minimal polynomial of an algebraic number α has degree a power of 2 does not mean that α is constructible. For instance, if $f \in \mathbb{Q}[t]$ is an irreducible quartic with Galois group S_4 (as is the case for "most" irreducible quartics in $\mathbb{Q}[t]$ in a sense that we will unfortunately not discuss here), then none of the roots of f are constructible numbers.

EXERCISE 8.47. *Complete the proof of Theorem 2.12 by showing that if n is a power of 2 times a product of distinct Fermat primes, then $e^{\frac{2\pi i}{n}}$ is constructible.*

We may view theorem 8.48 as the special case of Theorem 8.45 in which $F = \mathbb{Q}$ and we are considering solvability by radical chains with index set $\{2\}$. If we revisit the proof of Theorem 8.45 in this context, we find that it simplifies: we no longer need to adjoin any roots of unity. This suggests the following generalization:

EXERCISE 8.48. *Let $\mathcal{P}$ be a nonempty set of prime numbers. A finite group is a $\mathcal{P}$-**group** if $p \mid \#G$ implies $p \in \mathcal{P}$. We say a finite degree field extension K/F in characteristic 0 is **solvable by $\mathcal{P}$-radicals** if K is contained in an extension L/F admitting a radical chain whose index set is a subset of $\mathcal{P}$.*

a) *Suppose that for all $p \in \mathcal{P}$, F contains a primitive pth root of unity. Show: a finite degree extension K/F is solvable by $\mathcal{P}$-radicals if and only if its Galois group is a solvable $\mathcal{P}$-group.*[8]
b) *Give counterexamples to show that the hypothesis on primitive roots of unity is necessary.*

After soaring these heights, let us come back to engage with some earthly problems. We defined radical extensions so as to be able to define extensions that are solvable by radicals. Other than showing that radical extensions are closed under passage to finite towers (well, this is by definition), under taking lifts, composita and normal closures, we did not show anything about them. In fact their properties can be quite delicate as compared to the class of solvable exensions. For one thing, while it is easy to use the definition of a simple radical or radical extension to give examples of them, it is annoyingly difficult to show that a finite degree field extension is *not* simple radical or radical, except in the presence of sufficient roots of unity.

Since we are in characteristic 0, all quadratic extensions are radical extensions. What about cubic extensions? Notice that in any prime degree, a radical extension must be simple radical. At first glance, it may seem that we have answered this question already in Theorem 6.11: a cubic extension K/F should be radical if and only if its discriminant $\delta_{K/F} = -3 \pmod{F^{\times 2}}$. But actually this is only half clear: this result characterizes *pure cubic extensions* – i.e., cubic K/F of the form $K = F(a^{1/3})$ for some $a \in F$. Certainly a pure cubic extension is a simple radical extension. However, for the converse, how do we know that a cubic extension that is not pure cannot nevertheless be of the form $F(a^{1/n})$ for some $n \geq 4$? The following results, taken from work of Isaacs–Moulton [**IM98**], will help us explore this:

PROPOSITION 8.49. *Let F be a field, let $n \in \mathbb{Z}^+$, and let K/F be a field extension of the form $K = F(\alpha)$, where $\alpha^n \in F$. Put $d := [K : F]$. Then:*

a) *Let $f \in F[t]$ be the minimal polynomial of α. Then every root of f in $\overline{F}$ has the form $\zeta\alpha$, where $\zeta^n = 1$.*
b) *There is an nth root of unity $\epsilon \in K$ such that $\epsilon\alpha^d \in F$. In particular, if $\mu_n(K) = \mu_n(F)$, then $\alpha^d \in F$.*

PROOF. a) Put $a := \alpha^n \in F$, so α is a root of $t^n - a \in F[t]$. Thus the minimal polynomial f of α divides $t^n - a$, so every root of f in $\overline{F}$ is a root of $t^n - a$, hence of the form $\zeta\alpha$ for an nth root of unity ζ.
b) Since every root of f is an nth root of unity times α, the product of all the roots of f (with multiplicities) is of the form $\epsilon\alpha^d$ for an nth root of unity ϵ. But the product of all the roots of f is $(-1)^d$ times the constant coefficient of f, which is an element of F: that is, $\epsilon\alpha^d \in F$. The last statement of part b) follows immediately: if $\mu_n(K) = \mu_n(F)$, then $\epsilon \in F$, so $\alpha^d \in F$. □

COROLLARY 8.50. *Let d be an* odd *positive integer, and let $K/\mathbb{Q}$ be a degree d simple radical extension of $\mathbb{Q}$. Then there $\alpha \in K$ such that $\alpha^d \in \mathbb{Q}$ and $K = \mathbb{Q}(\alpha)$.*

PROOF. By definition of a simple radical extension, there is $\alpha \in K$ and $n \in \mathbb{Z}^+$ such that $\alpha^n \in \mathbb{Q}$ and $K = \mathbb{Q}(\alpha)$. For a field F, let $\mu(F)$ denote the group of all

[8]By Proposition 8.39, if $\#\mathcal{P} = 1$, then every $\mathcal{P}$-group is solvable. This remains true if $\#\mathcal{P} = 2$, a celebrated theorem of Burnside. Clearly it need not hold for $\#\mathcal{P} = 3$, as A_5 is a noncommutative, simple $\{2, 3, 5\}$-group.

roots of unity in F. It suffices to show that $\mu(K) = \mu(\mathbb{Q}) = \{\pm 1\}$, for then we have $\mu_n(K) = \mu_n(\mathbb{Q})$, and Proposition 8.49b) applies to show that $\alpha^d \in \mathbb{Q}$.

Suppose to the contrary that K contains a primitive nth root of unity ζ_n for some $n \geq 3$. Then

$$\varphi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] \mid [F : \mathbb{Q}] = d.$$

But d is odd and (by Exercise 8.13b)) $\varphi(n)$ is even, a contradiction. □

COROLLARY 8.51. *Let $d \in \mathbb{Z}^{\geq 3}$, and let K/F be a degree d field extension such that $K = F(\alpha)$ such that $\alpha^n \in F$ for some $n \in \mathbb{Z}^+$.*

a) *If K/F is Galois, then $\#\mu_n(K) \geq d$.*
b) *If K/F is not Galois and d is prime, then $\alpha^d \in F$.*

PROOF. a) Suppose that K/F is Galois. Let $f \in F[t]$ be the minimal polynomial of α. It has degree d, so being normal and separable, it has d distinct roots in K. By Proposition 8.49a), each of these roots is an nth root of unity times α, so K has at least d different roots of unity.
b) By Proposition 8.49b), there is a root of unity ϵ such that $\epsilon\alpha^d \in F$. If $\epsilon \notin F$, then $F(\epsilon)/F$ is a proper Galois subextension of the prime degree non-Galois extension K/F, which is a contradiction. So $\epsilon \in F$ and thus $\alpha^d \in F$. □

However:

EXAMPLE 8.52. *By Theorem 8.13, the unique quadratic subfield of $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ is $F := \mathbb{Q}(\sqrt{-7}) \neq \mathbb{Q}(\sqrt{-3})$. Thus $\mathbb{Q}(\zeta_7)/F$ is a Galois simple radical extension of degree 3. If it were a pure cubic extension, then on the one hand its discriminant would have to be $-3 \pmod{F^{\times 2}}$, but on the other hand being a Galois cubic extension, its discriminant would have to be $1 \pmod{F^{\times 2}}$, and as we have just said, -3 is* not *a square in F. Thus we have a radical cubic extension that is* not *obtainable by adjoining a cube root.*

Thus in order to know whether an extension is simple radical or radical, it helps enormously to know which roots of unity it contains. In the abstract setting ("let K/F be a degree n extension") this may be difficult. It is much easier if one is looking at particular fields, especially number fields:

EXERCISE 8.49. *Let d_1, d_2 be nonzero rational numbers that are distinct and nontrivial in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, and put $F := \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Evidently $F/\mathbb{Q}$ is a radical extension, but is it a simple radical extension?*

a) *Show:* $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is not *a simple radical extension.*
b) *Show:* $\mathbb{Q}(\sqrt{2}, \sqrt{-2})/\mathbb{Q}$ is *a simple radical extension.*
c) *Discuss the general case.*

Let us end this section by noting that the cause of the above complications is that in our definition of simple radical equation $F(\alpha)/F$, we do not require the polynomial $t^n - \alpha^n \in F$ to be irreducible. (By Theorem 8.26, when $4 \nmid n$ this is equivalent to requiring that α^n not be a pth power in F for any $p \mid n$, with a slight complication when $4 \mid n$.) Let us say that $F(\alpha)/F$ is **simple irreducible radical** when $t^n - \alpha^n$ is irreducible. The point is that for a simple irreducible radical extension K/F, we have "$n = d$," where $d = [K : F]$. Then we define an **irreducible radical extension** to be given by a finite tower of simple irreducible radical extensions and an extension to be **solvable by irreducible radicals** if it is contained some

irreducible radical extension.

Example 8.52 gives a simple radical extension that is not irreducible radical. But:

PROPOSITION 8.53. *Let K/F be a finite degree extension in characteristic 0. Then K/F is solvable by radicals if and only if it is solvable by irreducible radicals.*

PROOF. For $n \in \mathbb{Z}^+$, let ζ_n be any primitive nth roof of unity in $\overline{F}$.

Clearly being solvable by irreducible radicals implies being solvable by radicals. Conversely, since every finite degree extension K/F that is solvable by radicals has solvable Galois group, the proof of Theorem 8.45 shows for K/F to be solvable by irreducible radicals, it will suffice if for all $n \geq 3$, the cyclotomic extension $F(\zeta_n)/F$ is solvable by irreducible radicals. We show this by induction on n, the base case $n = 3$ being clear, as $F(\zeta_3)/F$ has degree at most 2. So suppose $n > 3$ and that for all $1 \leq k < n$ there is an irreducible radical extension of F containing ζ_k.
Case 1: Suppose $n = p$ is prime. Then

$$[F(\zeta_p) : F] \mid p - 1 = 2 \cdot \frac{p-1}{2}.$$

By Theorem 8.13a), the extension $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has a unique quadratic subextension $\mathbb{Q}(\sqrt{N_p})$. (Part b) of this theorem tells us what N_p is, but this is not needed here.) We can start our irreducible radical tower of F with $F(\sqrt{N_p})$. Then $F(\zeta_p)/F(\sqrt{N_p})$ is abelian of degree dividing $\frac{p-1}{2}$, so it decomposes as a tower of cyclic extensions of prime degrees $\ell_i < p$. By induction, there is an irreducible radical tower containing each ζ_{ℓ_i}, and then the lifted tower to $F(\sqrt{N_p}, \{\zeta_{\ell_i}\})$ has each step trivial or a prime degree ℓ_i abelian extension of a field containing an ℓ_ith root of unity, so is a simple irreducible radical extension.
Case 2: Suppose $n = p^a$ is a prime power with $a \geq 2$. By induction, there is an irreducible radical tower K/F containing $\zeta_{p^{a-1}}$. The extension $K(\zeta_{p^a})/K(\zeta_{p^{a-1}})$ is abelian of degree dividing $[\mathbb{Q}(\zeta_{p^a}) : \mathbb{Q}(\zeta_{p^{a-1}})] = p$, and $\zeta_p \in K$, so this extension is either trivial or irreducible simple radical.
Case 3: If $n = p_1^{a_1} \cdots p_r^{a_r}$ with $r \geq 2$, then $F(\zeta_n) = F(\zeta_{p_1^{a_1}}) \cdots F(\zeta_{p_r^{a_r}})$, so the result follows from Case 2. □

EXERCISE 8.50. *Let F be a field of characteristic neither 2 nor 3, let $f \in F[t]$ be an irreducible cubic polynomial, and let K/F be an irreducible radical extension in which f splits. Show: K contains a primitive cube root of unity.*

Example 8.52 shows that Exercise 8.50 would be false for radical extensions instead of irreducible radical extensions.

Exercise 8.50 is taken from [**Ma64**] and is closely related to the *casus irreducibilis* in the classical study of cubic equations. It implies that for an irreducible cubic polynomial f defined over a subfield of $\mathbb{R}$, any formula for the roots of f using only square roots and cube roots must involve $\sqrt{-3}$, hence such a formula cannot be attained over the real numbers. For a subfield F of $\mathbb{R}$ and $\alpha \in \mathbb{R}$, we say that α is **solvable by real radicals over F** if there is a field K with $F(\alpha) \subseteq K \subseteq \mathbb{R}$ with K/F a radical extension. This turns out to be a much more restrictive condition:

THEOREM 8.54 (Isaacs). *Let $f \in \mathbb{Q}[t]$ be an irreducible polynomial that splits over $\mathbb{R}$. If f has any root α that is solvable by real radicals over $\mathbb{Q}$, then the degree*

of f is a power of 2 and the Galois group of f is a 2-group. In particular, all the roots of f are constructible numbers.

PROOF. See [**Is85**]. □

7. Solvability by Radicals in Characteristic p

Let p be a prime number. In this section, all of our fields have characteristic p, and our task is to modify the results of the previous section, in particular to arrive at an analogue of Galois's Theorem 8.45. This is certainly possible...but indeed in more than one way, and we have some choices to make.

Suppose first that we only want to consider finite degree *separable* extensions. In this case, we need to modify our definition of a simple radical extension: indeed, let F be a field of characteristic p, let $\alpha \in F$ and let $\beta \in \overline{F}$ be such that $\beta^p = \alpha$. Then β satisfies the polynomial $t^p - \beta = 0$, so by Lemma 4.6, either $\alpha = \gamma^p$ for some $\gamma \in F$, and then $\beta = \gamma \in F$ – or $t^p - \alpha$ is irreducible, and thus $F(\beta)/F$ is inseparable. More generally, if $n \in \mathbb{Z}^+$ and $\alpha \in F$ and $\beta \in \overline{F}$ is such that $\beta^{np} = \alpha$, then the extension $F(\beta)/F$ can be decomposed as a tower

$$F \subseteq F(\beta^p) \subseteq F(\beta),$$

and by the above, $F(\beta)/F(\beta^p)$ is only separable if it is trivial, so in characteristic p a separable extension obtained by adjoining an nth root is also obtained by adjoining an mth root for some $p \nmid m$. It would seem that this gives us a definition of a "separable simple radical extension", namely an extension of the form $F(\alpha)/F$ where there is a positive integer n with $p \nmid n$ such that $\alpha^n \in F$. We could then define "separable radical chain," "separable radical tower," "separable radical extension" and "solvable by separable radicals" in terms of our definition of separable simple radical extensions.

With these definitions, the proof of (i) $\implies$ (ii) in Theorem 8.45 runs verbatim to show that if K/F is a finite degree extension that is solvable by separable radicals according to the above definition, then if L is the Galois closure of K/F and $G = \mathrm{Aut}(L/F)$, then G is a solvable group. However, the proof of the converse implication breaks down: if G is solvable, then its order may be divisible by p, and then the proof gives us a subextension F_{i+1}/F_i that is cyclic of degree p, and such extensions are never given by adjoining a pth root. For a specific example, let ζ_5 be a primitive 5th root of unity in characteristic 2. Then the extension $\mathbb{F}_2(\zeta_5)/\mathbb{F}_2$ is obtained by adjoining a 5th root so is a simple radical extension of the kind considered above. Its degree is the least f such that $5 \mid 2^f - 1$, which is 4, and it is a cyclic Galois extension.

This motivates us to modify our above definition: for a field F of characteristic p, a **separable simple radical extension** is an extension that is *either* of the form $F(a^{1/n})/F$ for $a \in F$ and $p \nmid n$ is of the form $F(\rho^{-1}(a))$ for some $a \in F$. Again, Artin–Schreier theory tells us that nontrivial extensions of the latter type are precisely the cyclic degree p extensions of F. Then we define **separable radical chain**, **separable radical extension** and **solvable by separable radicals** in terms of separable simple radical extensions as above, and the proof of Theorem 8.45 is easily modified to show:

THEOREM 8.55. *Let F be a field of characteristic $p > 0$, let K/F be a separable finite degree field extension, let L be the Galois closure of K/F, and put $G := \mathrm{Aut}(L/F)$. The following are equivalent:*

(i) *The extension K/F is solvable by separable radicals.*
(ii) *The finite group G is solvable.*

EXERCISE 8.51. *Prove Theorem 8.55.*

But our first definition is still interesting: let us call a field extension $F(a^{1/n})/F$ with $p \nmid n$ a **classical separable simple radical extension**. Based on this definition, we can define a **classical separable radical extension** and an extension that is **solvable by classical separable radicals**. The following exercise shows that the presence of roots of unity in $\overline{F}$ that do not lie in F is the obstruction to giving a clean characterization of the class of extensions that are solvable by classical separable radicals.

EXERCISE 8.52. *Let F be a field of characteristic p, and let K/F be a finite degree separable extension with Galois closure L and Galois group $G := \mathrm{Aut}(L/F)$.*

a) *Suppose G is solvable and of order not divisible by p. Show: K/F is solvable by classical separable radicals.*
b) *Suppose K/F is solvable by classical separable radicals. Show: G is solvable.*
c) *Suppose F contains an algebraic closure of $\mathbb{F}_p$. Show: K/F is solvable by classical separable radicals if and only if G is solvable of order prime to p.*

Finally we drop the separability hypothesis. For a field F of characteristic $p > 0$, a **simple radical extension** is an extension that is *either* of the form $F(a^{1/n})/F$ for $a \in F$ and $n \in \mathbb{Z}^+$ (the point is that now $p \mid n$ *is* allowed) or is of the form $F(\rho^{-1}(a))$ for some $a \in F$. Using this definition we define **radical extension** and **extension that is solvable by radicals** in the usual way.

LEMMA 8.56. *Let F be a field of characteristic $p > 0$, let K/F be a radical extension, and let L be the normal closure of K/F. Then L/F is a radical extension.*

EXERCISE 8.53. *Prove Lemma 8.56.*

EXERCISE 8.54. *We work throughout with fields of characteristic $p > 0$.*

a) *Show: finite degree extensions that are solvable by radicals form a distinguished class.*
b) *Show: algebraic field extensions that are solvable by radicals form a distinguished class.*

Let K/F be a finite degree algebraic extension. By Proposition 4.8 and Theorem 4.17, K/F is a radical extension: indeed it admits a radical chain with index set $\{p\}$. Since a normal algebraic extension is the compositum of its separable and purely inseparable parts, we are led to the following result:

THEOREM 8.57. *Let F be a field of characteristic $p > 0$, let K/F be a finite degree extension, let L be the normal closure, and let $G := \mathrm{Aut}(L/F)$ be the pseudo-Galois group of K/F. The following are equivalent:*

(i) *The extension K/F is solvable by radicals.*
(ii) *The group G is solvable.*

PROOF. As in Theorem 4.26, let F_s be the separable closure of F in L and let F_i be the purely inseparable closure of F in L. By Corollaries 4.27 and 4.31, we have that F_s/F is Galois and $L = F_sF_i$.
(i) $\implies$ (ii): Suppose that K/F is solvable by radicals. Lemma 8.56 implies that also L/F is solvable by radicals. Since subextensions of extensions that are solvable by radicals are also solvable by radicals, we have that F_s/F is a Galois extension that is solvable by radicals, which as discussed above, means that F_s/F is solvable by separable radicals, and thus by Theorem 8.55 we have that $\mathrm{Aut}(F_s/F)$ is solvable. By Exercise 9.1, the restriction map $Aut(L/F) \to \mathrm{Aut}(F_s/F)$ is an isomorphism, thus $G = \mathrm{Aut}(L/F)$ is solvable.
(ii) $\implies$ (i): The argument is quite similar to the previous implication. Suppose that $G = \mathrm{Aut}(L/F)$ is solvable. A subextension of an extension that is solvable by radicals is also solvable by radicals, so it suffices (and indeed is equivalent, by Lemma 8.56) to show that L/F is solvable by radicals. Still G is isomorphic to $\mathrm{Aut}(F_s/F)$, so F_s/F is solvable by radicals by Theorem 8.55. As mentioned above, since F_i/F is purely inseparable, it is solvable by radicals, and thus $(L = F_sF_i)/F$ is solvable by radicals by Exercise 8.54. □

Except for their characteristic hypotheses, Theorems 8.45 and 8.57 are identically worded, so we could state them together as: let K/F be a finite degree field extension with normal closure L. Then K/F is solvable by radicals if and only if $\mathrm{Aut}(L/F)$ is a solvable group. However this enunciation is hiding two differences that occur in positive characteristic: first our definition of solvable by radicals includes Artin–Schreier extensions, and second, $\mathrm{Aut}(L/F)$ is in general a pseudo-Galois group rather than a Galois group. So we prefer to keep the results separate.

CHAPTER 9

Classical Galois Theory

1. The Galois Group of a Polynomial

We now give a different perspective on Galois groups: more concrete but also richer.

EXERCISE 9.1. *Let K/F be a finite degree field extension, with normal closure L, let $G := \mathrm{Aut}(L/F)$, and let F_s be the maximal separable subextension of L/F.*

a) *Show: F_s/F is finite Galois, and the natural restriction map $G \to \mathrm{Aut}(F_s/F)$ is an isomorphism.*

b) *Show: K/F is separable if and only if $\#G = [L : F]$.*

c) *Show: if K/F is separable, then K/F is Galois if and only if*

$$\#G = [K : F].$$

In the setup of Exercise 9.1, we refer to $G = \mathrm{Aut}(L/F)$ as the **pseudo-Galois group** of K/F, and when K/F is separable, we refer to G as the **Galois group** of K/F. Thus if K/F is inseparable, its pseudo-Galois group is the Galois group of the maximal separable subextension F_s of the normal closure L/F. However, we will almost exclusively deal with Galois groups and not pseudo-Galois groups.

Suppose K/F is a finite degree separable extension – say $[K : F] = d$ – with normal closure L. There is a more concrete take on the Galois group $G = \mathrm{Aut}(L/F)$ that can be extremely useful. By the Primitive Element Corollary we have $K \cong F[t]/(f)$ for a monic irreducible polynomial $f \in F[t]$, and then L is the splitting field of f, so there are distinct $\alpha_1, \ldots, \alpha_d \in L$ such that

$$f = \prod_{i=1}^{n} (t - \alpha_i) \in L[t].$$

Since $f \in F[t]$, for $\sigma \in G = \mathrm{Aut}(L/F)$, for all $1 \leq i \leq d$ we have $f(\sigma(\alpha_i)) = \sigma f(\alpha_i) = \sigma(0)) = 0$, and thus $\sigma(\alpha_i) = \alpha_j$ for some j. That is, G acts on the set $\{\alpha_1, \ldots, \alpha_d\}$ of roots of f, which gives us a homomorphism

$$\Phi : G \to S_d.$$

Because $L = F(\alpha_1, \ldots, \alpha_d)$, this action is *faithful*: in other words, the homomorphism Φ is injective. Thus we may view the Galois group G as a subgroup of S_d. There is one crucial property that the permutation group G must satisfy:

PROPOSITION 9.1. *With notation as above, the Galois group G is a **transitive** subgroup of S_d: that is, for all $1 \leq i, j \leq d$, there is $\sigma \in G$ such that $\sigma(\alpha_i) = \alpha_j$.*

PROOF. The statement is equivalent to G having a single orbit on the set $\{\alpha_1, \ldots, \alpha_d\}$. In general, suppose the distinct orbits of G on this set are $G\alpha_{i_1}, \ldots, G\alpha_{i_r}$ for some $1 \leq r \leq d$. We wish to show that $r = 1$. For $1 \leq i \leq r$, let $g_i \in L[t]$

be the monic separable polynomial whose distinct roots are all the roots of f that lie in the same G-orbit as α_{i_1}. Then we have $f = \prod_{i=1}^r g_i$, and moreover, for all $\sigma \in G$, $\sigma g_i = g_i$. The latter means that for each $1 \leq i \leq r$, each coefficient of g_I is an element of L that is pointwise fixed by every $\sigma \in G$, so each coefficient of g_i lies in F and thus $g_i \in F$. Thus the factorization $f = \prod_{i=1}^f g_i$ actually takes place in $F[t]$, which contradicts the irreducibility of f unless $r = 1$. □

For a field F and a monic separable polynomial $f \in F[t]$ of positive degree, we define the **Galois group of f** to be the Galois group of L/F, where L is the splitting field of f. This recovers the previous situation if f is irreducible. In general, a small modification of the previous argument shows:

PROPOSITION 9.2. *Let F be a field, let $f \in F[t]$ be a separable monic polynomial of degree $d \geq 1$ with splitting field L. Write*

$$f = \prod_{i=1}^d (t - \alpha_i) \in L[t],$$

and let $G \coloneqq \mathrm{Aut}(L/F)$. Then:

a) *There is a natural, faithful action of G on $\{\alpha_1, \ldots, \alpha_d\}$ and thus an injective group homomorphism*

$$\Phi : G \hookrightarrow S_d.$$

b) *The orbits of G on S_d are naturally in bijection with the irreducible factors of $f \in F[t]$. In particular, the G-action is transitive if and only if f is irreducible over F.*

EXERCISE 9.2. *Prove Proposition 9.2.*

In order to regard the Galois group of a monic separable polynomial $f \in F[t]$ as a permutation group, we had to choose an ordering of its roots in some splitting field. Choosing a different ordering of the roots amounts to conjugating the permutation group by an element of S_d. Thus, to be precise, in the notation of Proposition 9.2 it is the *conjugacy class* of the group $\Phi(G)$ in S_d that is well-defined by f and not $\Phi(G)$ itself. (This remark is ubiquitous when working with permutation groups.)

Now if we look back at the proof of Theorem 7.27, we see that it actually shows more: not only is every finite group G a Galois group, but for every *permutation group* $G \subseteq S_n$, there is a field F, a monic separable polynomial $f \in F[t]$ and an ordering of the roots of f in a splitting field such that the Galois group of f is the subgroup G of S_n. It follows that, as we vary over all ground fields, the possible Galois groups of irreducible separable polynomials of degree d are precisely the transitive subgroups of S_d.

PROPOSITION 9.3. *Let F be a field, and let $f \in F[t]$ be a monic separable polynomial of degree $d \geq 1$ that factors as $\prod_{i=1}^d (t - \alpha_i)$ in the splitting field L. Let $G \coloneqq \mathrm{Aut}(L/F)$ be the Galois group of G. For $1 \leq i \leq d$, let H_i be the stabilizer of α_i in G.*

a) *For $1 \leq i \leq d$, we have $F(\alpha_i) = L^{H_i}$.*
b) *If α_i and α_j lie in the same G-orbit, then the subgroups H_i and H_j are conjugate.*
c) *Suppose f is irreducible. Then the following are equivalent:*

(i) *The subgroup H_1 is trivial.*
(ii) *We have $F(\alpha_1) = L$.*
(iii) *The extension $F(\alpha_1)/F$ is Galois.*

PROOF. a) An element $\sigma \in G = \mathrm{Aut}(L/F)$ fixes $F(\alpha_i)$ pointwise if and only if $\sigma(\alpha_i) = \alpha_i$.
b) In general, when a group G acts on a set X and there is $g \in G$ and $x_1, x_2 \in X$ such that $gx_1 = x_2$, then $\mathrm{Stab}_{x_2} = g\,\mathrm{Stab}_{x_1}\, g^{-1}$. Part b) is a case of this.
c) Since by part a) we have $F(\alpha_1) = L^{H_1}$, by the Galois correspondence we have that H_1 is trivial if and only if $F(\alpha_1) = L$, showing the equivalence of (i) and (ii). Since L/F is Galois, certainly (ii) $\implies$ (iii). Finally, if $F(\alpha_1)/F$ is Galois, then it is normal, so for all $1 \leq i \leq d$ we have $\alpha_i \in F(\alpha_1)$, so $F(\alpha_1) = L$, which as above implies that H_1 is trivial. □

EXAMPLE 9.4.

a) *Let $f = (t - \alpha_1)(t - \alpha_2) \in F[t]$ be an irreducible, separable quadratic polynomial. The only transitive subgroup of $S_2 \cong C_2$ is S_2 itself. Thus the Galois group of f must be cyclic of order 2.*
b) *Let $f = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3) \in F[t]$ be an irreducible separable cubic, with splitting field L. The transitive subgroups of S_3 are S_3 itself and the subgroup A_3 of even permutations, which is cyclic of order 3.*
c) *Let $f = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3)(t - \alpha_4) \in F[t]$ be an irreducible separable quartic, with splitting field L. Let G be the Galois group of f, viewed as a transitive subgroup of S_4. We have that $F(\alpha_1)/F$ is Galois if and only if $\#G = 4$. The transitive subgroups of S_4 are as follows:*
• *Any subgroup generated by a 4-cycle. There are $\frac{4\cdot 3\cdot 2}{4} = 6$ 4-cycles in S_4, generating 3 different cyclic subgroups of S_4, all conjugate to each other:*

$$C_{4,1} := \langle (1234) \rangle,\ C_{4,2} := \langle (1243) \rangle,\ C_{4,3} := \langle (1324) \rangle.$$

In this case $F(\alpha_1)/F$ is Galois.
• *The Klein 4-group*

$$V_4 := \{e, (12)(34), (13)(24), (14)(23)\},$$

which is normal in S_4 and abstractly isomorphic to $C_2 \times C_2$. In this case $F(\alpha_1)/F$ is Galois.
• *The Sylow Theorems imply that S_4 has a unique conjugacy class of subgroups of order 8 and that there are either 1 or 3 such subgroups, with the former occurring if and only if there is a normal subgroup of order 8. On the other hand, the subgroup*

$$D_{4,1} := \langle (1234), (13) \rangle,$$

which is isomorphic to the dihedral group D_4 of order 8. This group has two elements of order 4, (1234) and its inverse (1432). Thus

$$D_{4,2} := \langle (1324), (12) \rangle$$

and

$$D_{4,3} := \langle (1243), (14) \rangle$$

are distinct, but conjugate, dihedral groups. So none of these subgroups are normal. Because these groups contain a 4-cycle, they are transitive. In this case $F(\alpha_1)/F$ is not Galois.

- *The alternating group A_4 of order 12 contains V_4, so is transitive. In this case $F(\alpha_1)/F$ is not Galois.*
- *The symmetric group S_4 itself. In this case $F(\alpha_1)/F$ is not Galois.*

EXERCISE 9.3.

a) *Show: there is a non-transitive subgroup G of S_4 that is abstractly isomorphic to the Klein group V_4 but not conjugate to it. Show that there are precisely 3 such groups, all conjugate.*
b) *Show: there is a transitive subgroup of S_6 that is abstractly isomorphic to S_5 but not conjugate to a point stabilizer Stab_i for $1 \leq i \leq 6$. (One approach to this is to show that $\mathrm{PGL}_2(\mathbb{F}_5)$ is isomorphic to S_5.)*
c) *Show: there are subgroups G_1 and G_2 of S_6 such that:*
   - *Each of G_1 and G_2 is transitive;*
   - *$G_1 \cong S_4 \cong G_2$; and*
   - *G_1 and G_2 are* not *conjugate in S_6.*

EXERCISE 9.4.

a) *Confirm that the transitive subgroups of S_4 are as claimed in Example 9.4. (Suggestions: if G is a transitive subgroup of S_4, then by Orbit-Stabilizer and Lagrange, we have $\#G \in \{4, 8, 12, 24\}$. Clearly the unique subgroup of order 24 is S_4. A subgroup of order 12 has index 2 hence is normal, which helps to show that A_4 is the only subgroup of order 12. Example 9.4 handles the case of order 8. For groups of order 4 you can use the fact that every p-subgroup of a finite group is contained in a Sylow p-subgroup to reduce to looking at subgroups of $D_{4,i}$ for $1 \leq i \leq 3$.)*
b) *Show that the transitive subgroups of S_5 are as follows:*
   - *There are 24 5-cycles that generate 6 diferent cyclic subgroups $C_{5,i}$ for $1 \leq i \leq 6$, all conjugate to each other.*
   - *There are 6 dihedral groups $D_{5,i}$ of order 10, all conjugate to*

$$D_{5,1} \coloneqq \langle (12345), (25)(34) \rangle;$$

   for $2 \leq i \leq 6$, $D_{5,i}$ is obtained by a conjugation that takes (12345) to a generator of the cyclic subgroup $C_{5,i}$.
   - *There are 6 groups $\mathrm{AL}_{5,i}$ for $1 \leq i \leq 6$. We may take*

$$\mathrm{AL}_{5,1} \coloneqq \langle (12345), (2354) \rangle);$$

   for $2 \leq i \leq 6$, $F_{5,i}$ is obtained by a conjugation that takes (12345) to a generator of $C_{5,i}$. Each of these groups has order 20 and is abstractly isomorphic to the group $\mathrm{AGL}_1(\mathbb{F}_5)$ of invertible affine linear maps $x \mapsto ax + b$ on $\mathbb{F}_5$ for $a \in \mathbb{F}_5^\times$ and $b \in \mathbb{F}_5$, which is the semidirect product $\mathbb{F}_5 \rtimes \mathbb{F}_5^\times$.
   - *The alternating group A_5.*
   - *The symmetric group S_5.*

EXERCISE 9.5. *Show: for $1 \leq i \leq 6$, the unique index 2 subgroup of $\mathrm{AL}_{5,i}$ is $D_{5,i}$.*

EXERCISE 9.6. *Let p be a prime number. Show: a subgroup G of S_p is transitive if and only if G contains a p-cycle.*

EXERCISE 9.7. *Let F be a field, let $n \in \mathbb{Z}^+$, and let $f \in F[t]$ be a separable polynomial of degree n with Galois group S_n. Let α be a root of f in an algebraic closure. Show: the group* $\mathrm{Aut}(F(\alpha)/F)$ *is trivial.*

2. The Inverse Galois Problem for Permutation Groups

Thinking of Galois groups as permutation groups gives a potential enrichment of the Inverse Galois Problem. Namely, let F be a field, let $n \in \mathbb{Z}^+$, let G be a finite group, and let $\iota : G \hookrightarrow S_n$ be a group embedding such that $\iota(G)$ is a transitive subgroup of S_n. In practice we rarely use ι explicitly but rather speak of a **degree n permutation representation of G**. Let G_1 and G_2 be two finite groups. We say that two pairs $\iota_1 : G_1 \hookrightarrow S_{n_1}$ and $\iota_2 : G_2 \hookrightarrow S_{n_2}$ are **equivalent** if $n_1 = n_2 = n$, say, and the subgroups $\iota_1(G_1)$ and $\iota_2(G_2)$ of S_n are conjugate.

We say that (G, ι) **occurs as a Galois permutation group over F** if there is an irreducible separable degree n polynomial $f \in F[t]$ with Galois group conjugate to $\iota(G)$. We could then define the **Inverse Galois Problem for Permutation Groups (IGPPG)** over a field F to be the question whether every transitive permutation group (G, ι) occurs as a Galois permutation group over F. But as we will see, for a given finite group G, if G occurs as a Galois group over F, every transitive permutation representation (G, ι) occurs as as a Galois permutation group over F.

To see why, we review some basic theory of permutation groups. For a subgroup H of a group G, we define the **Cayley-Schreier representation** to be the action of G on its left coset space G/H given by $g \bullet xH = gxH$. This representation is transitive, the stabilizer of the coset H is the subgroup H, so (like any transitive action) the other point stabilizers are precisely the conjugates of H. Therefore the kernel of the action is the normal core $\mathrm{Core}(H)$ of H, so the action is faithful if and only if H is corefree. Conversely, if G acts transitively on a nonempty set X such that the stabilizer of some $p \in X$ is H, then the X is equivalent as a G-set to G/H under the mapping $xH \mapsto xp$. In particular, two Cayley-Schreier representations G/H_1 and G/H_2 are equivalent if and only if H_1 and H_2 are conjugate subgroups of G. Thus inequivalent transitive permutation representations (G, ι) of a finite group G are naturally in bijection with conjugacy classes of corefree subgroups H of G. A special case of the Cayley-Schreier representation is when $H = \{e\}$: then G acts on itself by $g\bullet : x \mapsto gx$. This action is **simply transitive**, and conversely any simply transitive G-action on a set is equivalent to the Cayley action.[1]

EXERCISE 9.8. *Let G be a finite group of order n. Show: every degree n transitive permutation representation of G is equivalent to the Cayley representation.*

EXERCISE 9.9. *Let G be a finite group, and let $\iota : G \hookrightarrow S_n$ be a group embedding with image a transitive subgroup of S_n. Show:*

$$n \mid \#G \mid n!.$$

Exercise 9.9 shows that for a finite group G, the set of degrees of transitive permutation representations of G is finite. Since S_n has only finitely many conjugacy

[1]More precisely we have defined the *left* Cayley-Schreier representation and the *left* Cayley representation. But the right Cayley-Schreier representation – i.e., the action of G on right cosets $\{Hx\}_{x \in G}$ is also transitive and the stabilizer of the coset H is the subgroup H, so it is equivalent to the left Cayley-Schreier representation.

classes of subgroups, it follows that a given finite group G can have only finitely many inequivalent transitive permutation representations. However, this number can certainly be arbitrarily large, as we will shortly see.

If G is commutative then any faithful, transitive action of G on a nonempty finite set is equivalent to the Cayley representation: indeed, since the action is transitive, for any $x \in X$, the action is equivalent to the action of G on G/Stab_x. As we saw above, the kernel of this action is the normal core $\operatorname{Core}(\operatorname{Stab}_x)$, but since G is commutative every subgroup is normal, so the action is faithful if and only if $\operatorname{Core}(\operatorname{Stab}_x)$ is trivial if and only if Stab_x is trivial, if and only if the the action is simply transitive.[2]

The smallest noncommutative group is S_3. If S_3 is a transitive subgroup of S_n, then we need $6 \mid n!$ and $n \mid 6$, so $n \in \{3, 6\}$. But of course S_3 does have a degree 3 permutation representation – it comes to us that way! – and a degree 6 representation, the Cayley representation. Becaause a degree 3 representation is determined by its stabilizer being an order 2 subgroup of S_3 and all order 2 subgroups of S_3 are conjugate, the degree 3 representation is unique up to (permutation group) isomorphism. These two representations are two different ways of looking at the same Galois-theoretic situation: a degree 3 representation of S_3 as a Galois permutation group is an irreducible, separable cubic $f_3 \in F[t]$ with Galois group S_3. If L is the splitting field of f_3, then the Galois extension L/F has a primitive element, whose sextic minimal polynomial $f_6 \in F[t]$ realizes the degree 6 representation of S_3 as a Galois permutation group. Conversely, given a Galois extension L/F with $\operatorname{Aut}(L/F) = S_3$, let $K \coloneqq L^{\langle (12) \rangle}$. Then K/F is a separable cubic extension which by Corollary 7.19 has normal closure $L^{\operatorname{Core}\langle (12) \rangle} = L^{\{e\}} = L$, so the minimal polynomial f_3 of a primitive element for K/F realizes the degree 3 representation of S_3.

If G is a finite simple group (e.g. A_n for $n \geq 5$), then every proper subgroup of G is corefree, so the equivalence classes of transitive permutation representations of G are in bijection with conjugacy classes of proper subgroups of G. Or if $G = S_n$ for $n \geq 5$ then every proper subgroup of S_n except for A_n is corefree. In particular, for $n \geq 5$ every element of S_n generates a corefree subgroup, so there are at least as many conjugacy classes of corefree subgroups in S_n as there are conjugacy classes of elements in S_n, namely $P(n)$, the number of cycle types of elements of n. This is quite an underestimate, but it certainly shows that a finite group may have arbitrarily many inequivalent permutation representations.

Now we are in a position to demonstrate our claim on the equivalence of IGG and IGGPG for a given finite group G. Suppose that F is a field and G occurs as a Galois group over F: thus there is a finite Galois extension L/F with $G \cong \operatorname{Aut}(L/F)$. Let f be the minimal polynomial of a primitive element for L/F, so f has degree $\#G$, and thus by Exercise 9.8 viewing G as the Galois group of f gives the Cayley representation of G. Now let $\iota : G \hookrightarrow S_n$ be any group embedding with transitive image. Let $H \coloneqq \{\sigma \in G \mid \iota(\sigma)(1) = 1\}$, so H is a corefree subgroup of G of index

[2]This extends to finite groups for which every subgroup is normal, but these are rare: the noncommutative such groups are precisely the direct products of the quaternion group Q_8 with a finite commutative group A with no elements of order 4.

n. Put $K \coloneqq L^H$. Again by Corollary 7.19, the normal closure of K is L, so taking the minimal polynomial f of a primitive element α for K/F, we get that f has Galois group G, and because H is the stabilizer of α in G, the representation of G on the roots of f in L is equivalent to ι.

3. The Role of the Discriminant

Let $n \in \mathbb{Z}^{\geq 2}$, let k be a field, and let $K \coloneqq k(t_1, \ldots, t_n)$ be a rational function field in n variables. For $1 \leq i \leq n$, let $s_k(t_1, \ldots, t_n)$ be the kth elementary symmetric function, and let $F \coloneqq k(s_1, \ldots, s_n)$, so by Theorem 8.46, we have that K/F is finite Galois with $\mathrm{Aut}(K/F) = S_n$ acting by permutations on $\{t_1, \ldots, t_n\}$. By the Galois Corrspondence, the subextensions of K/F are all of the form K^H for some subgroup H of S_n. It is interesting to ask for explicit generators for these subfields.

One easy case: for $1 \leq i \leq n$, let H_i be the stabilizer of t_i, so the H_i's are conjugate subgroups of S_n and each H_i is isomorphic to S_{n-1}. Then $K^{H_i} = F(t_i)$: indeed, the containment $F(t_i) \subseteq K^{H_i}$ is clear, and conversely, since S_n is the Galois group of the polynomial $f(t) \coloneqq \prod_{i=1}^n (t - t_i) \in F[t]$ and S_n is transitive, f is irreducible, so $[F(t_i)] : F] = \deg f = n$, while $[K^{H_i} : F] = \frac{[K:F]}{[K^{H_i}:K]} = \frac{\#G}{\#H_i} = n$ by the Orbit-Stabilizer Theorem, so $F(t_i) = K^{H_i}$. The same argument works to show:

Exercise 9.10. *Let F be a field, let $f \in F[t]$ be irreducible and separable of degree $n \geq 1$; suppose f factors in an algebraic closure of F as $f = \prod_{i=1}^n (t - \alpha_i)$. Let K/F be the splitting field of f, let G be the Galois group of f, and for $1 \leq i \leq n$, let H_i be the stabilizer of α_i in G. Show:*

$$\forall 1 \leq i \leq n,\ K^{H_i} = F(\alpha_i).$$

The case $n = 2$ is trivial: then K/F is a quadratic extension, so there are certainly no proper, nontrivial subextensions. When $n = 3$, there are precisely four nontrivial proper subgroups of S_3: three of them are the point stabilizers H_1, H_2, H_3 of the elements t_1, t_2, t_3, and the other one is A_3. Because $[S_3 : A_3] = 2$, we have that K^{A_3}/F is a spearable quadratic extension. Can we give an explicit generator?

Yes. In fact we will answer the more general question: for any $n \in \mathbb{Z}^{\geq 3}$ we have $[S_n : A_n] = 2$, so K^{A_n}/F is a quadratic extension, and we will find an explicit generator for it over F. We have a nice structure theory for separable quadratic extensions, or rather two nice structure theories, one for characteristic different from 2 and one for characteristic 2. Suppose first that k (hence also F and K) does *not* have characteristic 2. Then every quadratic extension of F is of the form $F(\sqrt{d})$ for some $d \in F^\times \setminus F^{\times 2}$. Moreover, let $\sigma \in S_n$. Then $\sigma(\sqrt{d}) = \pm\sqrt{d}$, but more precisely σ fixes $\sqrt{d}$ if and only if $\sigma \in A_n$, so we find that

$$\sigma(\sqrt{d}) = \mathrm{sgn}(\sigma)\sqrt{d}, \tag{32}$$

where $\mathrm{sgn}(\sigma) \in \{\pm 1\}$ denotes the sign of the permutation σ. Conversely, for any $d \in F^\times \setminus F^{\times 2}$ such that $\sqrt{d} \in K$ and (32) holds for d, we have $K^{A_n} = F(\sqrt{d})$.

This may remind us of something we've done before. Indeed, with $f = \prod_{i=1}^n (t - t_i) \in F[t]$ as above, we may take

$$d = \delta(f) = \prod_{i>j} (t_i - t_j)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (t_i - t_j) \tag{33}$$

to be the discriminant and thus may take $\sqrt{d}$ to be the semi-discriminant

$$\mathbf{s}(f) = \prod_{i>j}(t_i - t_j) \in K.$$

Let us check that this works: first, the second expression for $\delta(f)$ in (33) shows that it invariant under S_n hence lies in $F^\times$. Let $\sigma \in G$. Then $\sigma(t_i - t_j) = t_{\sigma(i)} - t_{\sigma(j)}$, which is one of the factors of $\mathbf{s}(f)$ if and only if $\sigma(i) > \sigma(j)$ and is otherwise -1 times one of the factors of $\mathbf{s}(f)$. The total number of factors of -1 is (by definition) the number of **inversions** of the permutation σ, and a permutation is even if and only if it has an even number of inversions. (One can see this by observing (i) for all $1 \leq k \leq n-1$, the transposition $\tau_k = (k\ k+1)$ has just a single inversion $(k, k+1)$; (ii) multiplying $\sigma \in S_n$ by τ_k either decreases or increases the number of permutations by 1 according to whether $(k, +1)$ is or is not an inversion of σ; and (iii) every element of S_n can be written as a product of the τ_k's.) Thus all $\sigma \in S_n$ we have

$$\sigma(\mathbf{s}(f)) = \operatorname{sgn}(\sigma)\mathbf{s}(f).$$

Thus

$$k(t_1, \ldots, t_n)^{A_n} = k(s_1, \ldots, s_n, \mathbf{s}(f)) = k(s_1, \ldots, s_n, \sqrt{\delta(f)}).$$

Contemplation of the "generic" polynomial $f = \prod_{i=1}^n (t-t)i)$ was just for motivation purposes; a similar result holds for any monic separable polynomial to give a crtierion for when its Galois group G is contained in A_n. (Since A_n is normal in S_n, whether G is contained in A_n depends only on the conjugacy class of G.)

THEOREM 9.5. *Let F be a field not of characteristic 2, and let $f \in F[t]$ be a monic separable polynomial of degree n. Let L be the splitting field of f, and let G be the Galois group of f.*

a) *We have $\sqrt{\delta(f)} \in L$.*
b) *We have $G \subseteq A_n$ if and only if $\delta(f) \in F^{\times 2}$.*
c) *We have $L^{A_n \cap G} = F(\sqrt{\delta(f)})$.*

EXERCISE 9.11. *Prove Theorem 9.5.*

EXAMPLE 9.6. *Let $p > 2$ be a prime number, and let $\Phi_p \in \mathbb{Q}[t]$ be the pth cylclotomic polynomial, with splitting field $L := \mathbb{Q}(\zeta_p)$, the pth cyclotomic field. By Corollary 8.9, the Galois group of Φ_p is $G = (\mathbb{Z}/p\mathbb{Z})^\times$, which is cyclic of order $p-1$. Since $p-1$ is even, no $(p-1)$-cycle is an element of A_{p-1}, we have that $\mathbb{Q}(\zeta_p)^{A_{p-1} \cap G} = \mathbb{Q}(\sqrt{\delta(\Phi_p)})$ is a quadratic extension of $\mathbb{Q}$, indeed the unique quadratic subxtension of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ because G is cyclic. By Theorem 6.17 we have (since $p-2$ is odd)*

$$\mathbb{Q}(\sqrt{\delta(\Phi_p)}) = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p^{p-2}}) = \mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p}).$$

This gives a second proof of Theorem 8.13.

Because the transitive subgroups of S_3 are $A_3 = C_3$ and S_3, Theorem 9.5 gives a nice way to determine the Galois group of an irreducible, separable cubic polynomial.

COROLLARY 9.7. *Let F be a field not of characteristic 2, and let $f = t^3 + at_2^2 + bt + c \in F[t]$ be an irreducible, separable cubic polynomial. Let G be the Galois group of F. Let*

$$\delta(f) = a^2b^2 - 4a^2c - 4b^3 + 18abc - 27c^2 \in F^\times$$

be the discriminant of f.

a) *If $\delta(f) \notin F^{\times 2}$, then $G = S_3$.*
b) *If $\delta(f) \in F^{\times 2}$, then $G = C_3$.*

EXERCISE 9.12.

a) *Let $f_1 := t^3 - 1701t + 5103 \in \mathbb{Q}[t]$. Show: f_1 is separable and has Galois group C_3.*
b) *Let $f_2 := t^3 + t + 1 \in \mathbb{Q}[t]$. Show: f_2 is separable and has Galois group S_3.*

EXERCISE 9.13. *Let F be a field not of characteristic 2, let $c \in F^\times$ be such that $-c \notin F^{\times 3}$, so $:= t^3 + c \in F[t]$ is irreducible by Theorem 8.26. Let G be the Galois group of f. Show: $G = C_3$ if and only if $-3 \in F$ if and only if F contains a primitive cube root of unity, and otherwise $G = S_3$.*

PROPOSITION 9.8. *Let F be a field of characteristic different from 2, and let $f \in F[t]$ be monic and separable of degree $n \in \mathbb{Z}^+$, with irreducible factorization $f = \prod_{i=1}^n g_i$. Suppose that the Galois group G of f is cyclic. Then $\delta(f) \in F^{\times 2}$ if and only if $n + r$ is even.*

PROOF. Let σ be a generator of G. Let S be the set of roots of f in an algebraic closure of F. By Proposition 9.2b), two roots lie in the same G-orbit if and only if they are both roots of g_i for some i. It follows that σ cyclically permutes the roots of each g_i, so the cycle type of σ is $(\deg g_1, \ldots, \deg g_r)$, and thus

$$\operatorname{sgn}(\sigma) = (-1)^{\sum_{i=1}^r ((\deg g_i)-1)} = (-1)^{n-r} = (-1)^{n+r}.$$

Combining this with Theorem 9.5 completes the proof. □

For a field F, we define the **Möbius function** $\mu : F[t] \to \{0, \pm 1\}$ as follows: $\mu(f) := 0$ if and only if $f = 0$ or f is not separable, while if f is separable and has r monic irreducible factors, then $\mu(f) := (-1)^r$.

EXERCISE 9.14. *Let q be an odd prime power.*

a) *Let $f \in \mathbb{R}[t]$ be a separable polynomial with s complex conjugate pairs of nonreal roots. Exercise 6.9b) was to show that $\delta(f) > 0$ if and only if s is even. Show this again using Proposition 9.8.*
b) *(Stickelberger) Let $f \in \mathbb{F}_q[t]$ be separable of positive degree. Show $\delta(f) \in \mathbb{F}_q^{\times 2}$ if and only if $\deg(f) \equiv \mu(f) \pmod 2$.*
c) *Let q be an odd prime power, and let $f \in \mathbb{F}_q[t]$ be a separable polynomial. Show: $\delta_{\mathbb{F}_{q^n}/\mathbb{F}_q} \in \mathbb{F}_q^\times$ if and only if n is odd.*

For a field F and a nonzero $f \in F[t]$, we denote by $\omega(f)$ the number of distinct monic irreducible divisors of f and by $\Omega(f)$ the number of monic irreducible factors of f counting multiplicities, so $\omega(f) = \Omega(f)$ if and only if f is separable.

The next exercise gives Swan's proof of quadratic reciprocity [**Sw62**].

EXERCISE 9.15. *Let p and q be distinct odd primes.*

a) *Consider $t^p - 1 \in \mathbb{F}_q[t]$. Show: $\delta(t^p - 1) \equiv (-1)^{\frac{p-1}{2}} p \pmod{\mathbb{F}_q^{\times 2}}$.*
b) *Let $\mathbf{o}_p(q)$ be the order of q in the group $\mathbb{F}_p^\times$. Use Exercise 8.11e) to show:*

$$\omega(t^p - 1) = 1 + \frac{p-1}{\mathbf{o}_p(q)}.$$

c) *Let L be an odd prime power, let $x \in \mathbb{F}_L^\times$ ("the" finite field of order L), and let $\mathbf{o}_L(x)$ be the order of x in the group $\mathbb{F}_L^\times$. Show: $x \in \mathbb{F}_L^{\times 2}$ if and only if $\frac{L-1}{\mathbf{o}_L(x)}$ is even. Deduce: $-1 \in \mathbb{F}_L^{\times 2}$ if and only if $L \equiv 1 \pmod 4$.*

d) *Suppose that $(-1)^{\frac{p-1}{2}}p$ is a square in $\mathbb{F}_q$. Use Exercise 9.14b) to show that $\frac{p-1}{\mathbf{o}_p(q)}$ is even, and deduce that q is a square in $\mathbb{F}_p$.*

e) *Suppose that $(-1)^{\frac{p-1}{2}}p$ is not a square in $\mathbb{F}_q$. Use Exercise 9.14b) to show that $\frac{p-1}{\mathbf{o}_p(q)}$ is odd, and deduce that q is not a square in $\mathbb{F}_p$.*

f) *Deduce the **Quadratic Reciprocity Law**: if at least one of p and q is $1 \pmod 4$, then p is a square modulo q if and only if q is a square modulo p, while if $p \equiv q \equiv 3 \pmod 4$, then p is a square modulo q if and only if q is* not *a square modulo p.*

EXERCISE 9.16. *Let $f \in \mathbb{Z}[t]$ be monic and such that the mod 2 reduction $f_2 \in \mathbb{F}_2[t]$ is separable, so by Exercise 6.4 we have $\delta(f) \equiv 1, 5 \pmod 8$. Stickelberger showed: if $\delta(f) \equiv 1 \pmod 8$, then $\mu(f) \equiv \deg(f) \pmod 2$, while if $\delta(f) \equiv 5 \pmod 8$, then $\mu(f) \not\equiv \deg(f) \pmod 2$. An elementary proof was given by Carlitz* [**Ca53**]. *Following Swan* [**Sw62**], *we will use this result to prove the **Second Supplement** to quadratic reciprocity. Let $p > 2$ be prime.*

a) *View $t^p - 1 \in \mathbb{Z}[t]$. Show: if $p \equiv \pm 1 \pmod 8$ then $\delta(t^p - 1) \equiv 1 \pmod 8$; and if $p \equiv \pm 3 \pmod 8$, then $\delta(t^p - 1) \equiv 5 \pmod 8$.*

b) *View $t^p - 1 \in \mathbb{F}_2[t]$. Show: $\omega(t^p - 1) = 1 + \frac{p-1}{\mathbf{o}_p(2)}$.*

c) *Use Stickelberger's Theorem to show: $2 \in \mathbb{F}_p^{\times 2}$ if and only if $p \equiv \pm 1 \pmod 8$.*

Now we turn to the case in which F has characteristic 2. In this case the semidiscriminant of a separable polynomial $f = \prod_{i=1}^n (t - \alpha_i)$ with Galois group G is

$$\mathbf{s}(f) = \prod_{i>j} (\alpha_i - \alpha_j) = \prod_{i>j} (\alpha_i + \alpha_j).$$

In this expression the factors are indexed by 2-element subsets of $\{\alpha_1, \ldots, \alpha_n\}$ hence are permuted by G, so $\mathbf{s}(f)$ is *always* G-invariant, hence (as we observed in Chapter 6) $\mathbf{s}(f) \in F^\times$ hence $\delta(f) \in F^{\times 2}$. Thus whereas outside of characteristic 2, the discriminant $\delta(f)$ of a polynomial $f \in F[t]$ plays two key roles – (i) $\delta(f) \neq 0$ if and only if f is separable, and if these conditions hold then (ii) $\delta(f) \in F^{\times 2}$ if and only if the Galois group of f is contained in A_n – in characteristic 2 the discriminant plays only the first role. So we will supplement with another expression in the roots of f called the **Berlekamp discriminant**.

Let us motivate this by coming back to the case of $F = k(s_1, \ldots, s_n)$, $K = k(t_1, \ldots, n)$ and the generic polynomial $f := \prod_{i=1}^n (t - t_i) \in k(s_1, \ldots, s_n)$ where k has characteristic 2. Now, since K^{A_n}/F is a separable quadratic extension in characteristic 2, by Artin-Schreier theory (and indeed already by Exercise 2.15), there is $b \in F$ such that $K^{A_n} = F(\wp^{-1}(b))$, i.e., is obtained by adjoining a root β of the polynomial $t^2 + t + b = 0$. The other root of this polynomial is $\beta + 1$, so now we are looking for an element $\beta \in K$ such that

$$\forall \sigma \in A_n, \sigma(\beta) = \beta \text{ and } \forall \sigma \in S_n \setminus A_n,\ \sigma(\beta) = \beta + 1.$$

Let us start with the simple case $n = 2$ and look for an element $\beta \in k(t_1, t_2)$ such that interchanging t_1 and t_2 carries β to $\beta + 1$. In this case, a bit of honest searching

will lead us eventually to $\beta := \frac{t_1}{t_1+t_2}$, whose Galois conjugate is $\beta' = \frac{t_2}{t_1+t_2} = 1-\beta = \beta+1$ since we are in characteristic 2. The minimal polynomial of β is

$$(t-\beta)(t-\beta') = t^2 + t + \frac{t_1 t_2}{(t_1+t_2)^2}.$$

If now F is any field of characteristic 2 and $f := t^2 + at + b \in F[t]$ is any separable, irreducible quadratic polynomial, with roots α_1 and α_2 in an algebraic closure, then the same calculations show that if $\beta := \frac{\alpha_1}{\alpha_1+\alpha_2}$ and $\beta' := \frac{\alpha_2}{\alpha_1+\alpha_2}$, then the minimal polynomial of β is $t^2+t+\frac{\alpha_1\alpha_2}{(\alpha_1+\alpha_2)^2} = t^2+t+\frac{c}{b^2} = \frac{c}{\delta(f)}$, and thus $K = F(\wp^{-1}(\frac{c}{\delta(f)}))$.

All of the above serves to motivate the following definition. Let R be a domain with fraction field F, and let $f \in R[t]$ be a monic polynomial of degree $n \in \mathbb{Z}^+$. We say that n is separable if it is separable when regarded as a polynomial in $F[t]$, and we factor it over an algebraic closure of F as $\prod_{i=1}^n (t-\alpha_i)$. We suppose moreover that for all $i \neq j$, $\alpha_i \neq -\alpha_j$ – notice that when R has characteristic 2 this is just the separability of f. For $1 \leq i \neq j \leq k$, we put

$$\beta_{i,j} := \frac{\alpha_i}{\alpha_i + \alpha_j} \in \overline{F},$$

and we define the **Berlekamp semi-discriminant**

$$\mathbf{s}_2(f) := \beta := \sum_{i<j} \beta_{i,j} \in \overline{F}$$

and the **Berlekamp discriminant**

$$\delta_2(f) := \sum_{i<j} \frac{\alpha_i \alpha_j}{\alpha_i^2 + \alpha_j^2} \in \overline{F}.$$

If G is the Galois group of $f \in F[t]$, it is immediate that elements of G permute the terms of $\delta_2(f)$, so $\delta_2(f) \in F$. In order for the Berlekamp semi-discriminant to have the desired relationship to the Berlekamp discriminant, we need to be in characteristic 2: suppose that $R = F$ is a field of characteristic 2, and let G be the Galois group of f. Then for $\sigma \in S_n$, we have that $\sigma(\beta_{i,j}) = \beta_{\sigma(i),\sigma(j)}$, which is one of the terms of β if and only if (i,j) is not an inversion for σ, while if (i,j) is an inversion for σ, it is 1 plus one of the terms of β. Keeping in mind that F has characteristic 2, we find:

- For all $\sigma \in A_n$, $\sigma(\mathbf{s}_2(f)) = \mathbf{s}_2(f)$; and
- For all $\sigma \in S_n \setminus A_n$, $\sigma(\mathbf{s}_2(f)) = 1 + \mathbf{s}_2(f)$.

LEMMA 9.9. *Let F be a field of characteristic 2, and let $f \in F[t]$ be a separable polynomial of positive degree. The roots of the polynomial*

$$t^2 + t + \delta_2(f) \in F[t]$$

are $\mathbf{s}_2(f)$ and $\mathbf{s}_2(f)+1$.

EXERCISE 9.17. *Prove Lemma 9.9.*

Thus, in close analogy to what happens in characteristic different from 2, we have

$$k(t_1,\dots,t_n)^{A_n} = k(s_1,\dots,s_n,\mathbf{s}_2(f)) = k(s_1,\dots,s_n,\wp^{-1}(\delta_2(f)).$$

And again this adapts readily to give a result for any monic separable polynomial in characteristic 2:

THEOREM 9.10. *Let F be a field of characteristic 2, and let $f \in F[t]$ be a monic separable polynomial of degree n. Let L be the splitting field of f, and let G be the Galois group of f.*

a) *We have $\wp^{-1}(\delta_2(f)) \in L$.*
b) *We have $G \subseteq A_n$ if and only if $\delta_2(f) \in \wp(F)$.*
c) *We have $L^{A_n \cap G} = F(\wp^{-1}(\delta_2(f)))$.*

EXERCISE 9.18. *Prove Theorem 9.10.*

By convention, if F has characteristic 2 and $f = t + a \in F[t]$ is a monic linear polynomial, we put $\delta_2(f) := 0$.

EXERCISE 9.19. *Let F be a field of characteristic 2, and let $f, g \in F[t]$ be monic polynomials of positive degree. Show:*

$$\delta_2(fg) \equiv \delta_2(f) + \delta_2(g) \pmod{\wp(F)}.$$

Just as for the usual discriminant, in order to apply Theorem 9.10 in concrete cases we need an expression for the Berlekamp disciminant $\delta_2(f)$ in terms of the coefficients rather than the roots of f. Again this can be done in several ways, and we will settle for brute force. We may write

$$\delta_2(f) = \frac{\psi_n(\alpha_1, \ldots, \alpha_n)}{D^+(\alpha_1, \ldots, \alpha_n)},$$

where $\psi_n, D_n^+ \in \mathbb{Z}[t_1, \ldots, t_n]$ are polynomials with $D_n^+ = \prod_{i<j}(t_i^2 + t_j^2)$. In fact, though we will not use it, we have

$$\psi_n = \sum_{i<j} t_i t_j \prod_{i'<j' | (i',j') \neq (i,j)} (t_{i'}^2 + t_{j'}^2).$$

Since the denominator D^+ is an S_n-invariant polynomial and the fraction $\delta_2(f)$ is S_n-invariant, also the numerator ψ_n is S_n-invariant. For any commutative ring R, the proof of Theorem 8.46 gives an algorithm to write an S_n-invariant polynomial $f \in R[t_1, \ldots, t_n]$ as a polynomial in $R[s_1, \ldots, s_n]$ where $s_k(t_1, \ldots, t_n)$ is the kth elementary symmetric polynomial, and thus if we write

$$\prod -i = 1^n(t - \alpha_i) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0,$$

then $s_k(\alpha_1, \ldots, \alpha_n) = (-1)^k a_k$. In fact, because we only use the Berlekamp discriminant in characteristic 2, we can view ψ_n and D_n^+ as polynomials in $\mathbb{F}_2[t_1, \ldots, t_n]$, in which case $S_k(\alpha_1, \ldots, \alpha_n) = a_k$ and $D_n^+ = \delta(f)$ is the usual discriminant.[3]

Implenting this algorithm by hand quickly becomes tedious, but computer algebra packages handle this easily. We used MAGMA to compute the following:

PROPOSITION 9.11. *Let F be a field, of characteristic 2, and let $f \in F[t]$ be a monic separable polynomial of degree n.*

a) *If $n = 2$ and $f = t^2 + at + b$, then $\delta_2(f) = \frac{b}{a^2}$.*
b) *If $n = 3$ and $f = t^3 + at^2 + bt + c$, then $\delta_2(f) = \frac{a^3c + abc + b^3 + c^2}{(ab+c)^2}$.*
c) *If $n = 4$ and $f = t^4 + at^3 + bt^2 + ct + d$, then*

$$\delta_2(f) = \frac{a^4d^2 + a^3bcd + a^3c^3 + a^2b^3d + abc^3 + b^3c^2 + c^4}{(a^2d + abc + c^2)^2}.$$

[3]Lifting to characteristic 0 is used in another method of computing $\delta_2(f)$: see [**Ca14**, §2.2].

PROOF. For instance, the MAGMA commands we used to compute part c) are:

```
F<a,b,c,d> := RationalFunctionField(FiniteField(2),4);
R <a,b,c,d> := PolynomialRing(FiniteField(2),4);
f := (a*b)/(a^2+b^2) + (a*c)/(a^2+c^2) + (b*c)/(b^2+c^2) +
(a*d)/(a^2+d^2) + (b*d)/(b^2+d^2) + (c*d)/(c^2+d^2);
P := R ! Numerator(f);
D := R ! Denominator(f);
IsSymmetric(P,R);
IsSymmetric(D,R);
```

The output is:

```
true a^4*d^2 + a^3*b*c*d + a^3*c^3 + a^2*b^3*d + a*b*c^3 + b^3*c^2 + c^4
true a^4*d^2 + a^2*b^2*c^2 + c^4
```

□

EXERCISE 9.20. *Let k be a field, let $F := F(s)$ (rational function field), and let $p \in F[s]$ have positive degree. Show: $f := t^3 + pt + p \in F[t]$ is irreducible.*
(Hint: by Gauss's Lemma it is equivalent to show that $f \in (F[s])[t]$ is irreducible. To see this, apply Eisenstein's Criterion with $\mathfrak{p}$ equal to the ideal generated by some irreducible factor of p.)

EXAMPLE 9.12. *Let k be a field of characteristic 2, and put $F := k(s)$, the rational function field in the indeterminate s. Let $p \in k[s]$ be a polynomial of positive degree d, and put*

$$f := t^3 + pt + p \in F[t].$$

Then $\delta(f) = p^2 \neq 0$, so f is separable. Moreover f is irreducible by Exercise 9.20, so its Galois group is either S_3 or A_3. We have

$$\delta_2(f) = \frac{p^3 + p^2}{p^2} = p + 1.$$

a) *If p has odd degree then so does $\delta_2(f)$, and then by Example 8.35 we have $\delta_2(f) \notin \wp(F)$, so the Galois group of f is S_3. Thus for instance the Galois group of $t^3 + st + s$ is S_3.*
b) *If $p = s^2 + s + 1$, then $\delta_2(f) = s^2 + s \in \wp(F)$, so f has Galois group C_3.*
c) *If $p = s^2$, then $\delta_2(f) = s^2 + 1$. Suppose that there is $x \in F$ such that $x^2 + x = s^2 + 1$. Then x is integral over the UFD $k[s]$, hence $x \in k[s]$. Since $\deg(x^2 + x) = 2 \deg x$ and $\deg(s^2 + 1) = 2$, we must have $x = as + b$ for $a, b \in k$. Then $x^2 + x = a^2 s^2 + as + b^2 + b \neq s^2 + 1$. So the Galois group of f is S_3.*

In §8.5 we saw: aside from the alternating groups A_n, the only nontrivial proper normal subgroup of S_n is V_4 inside S_4. Determining the V_4-invariants is easy:

PROPOSITION 9.13. *Let k be any field, let $K = k(t_1, t_2, t_3, t_4)$, and put*

$$\beta_1 := t_1 t_2 + t_3 t_4, \ \beta_2 := t_1 t_3 + t_2 t_4, \ \beta_3 := t_1 t_4 + t_2 t_3.$$

Then

$$K^{V_4} = k(s_1, s_2, s_3, s_4, \beta_1, \beta_2, \beta_3).$$

PROOF. Put $F \coloneqq k(s_1, s_2, s_3, s_4)$. We have $\mathrm{Aut}(K/F) = S_4$, acting on $\{t_1, t_2, t_3, t_4\}$ by permuting the indices. It is immediate to see that each of the elements e, $(12)(34)$, $(13)(24)$, $(14)(23)$ of V_4 fixes each of β_1, β_2, and β_3, so $F(\beta_1, \beta_2, \beta_3) \subseteq K^{V_4}$. Moreover S_4 acts on $\{\beta_1, \beta_2, \beta_3\}$– this is equivalent to the natural S_4-action on partitions of $\{1, 2, 3, 4\}$ into two 2-element subsets – so the polynomial $g \coloneqq (t - \beta_1)(t - \beta_2)(t - \beta_3)$ lies in $F[t]$ and $F(\beta_1, \beta_2, \beta_3)$ is the splitting field of g, hence $F(\beta_1, \beta_2, \beta_3)/F$ is a Galois extension, with Galois group a quotient of S_4. The permutation (12) fixes β_1 and interchanges β_2 and β_3, while the permutation (132) carries $\beta_1 \mapsto \beta_2 \mapsto \beta_3 \mapsto \beta_1$. It follows that $\mathrm{Aut}(F(\beta_1, \beta_2, \beta_3)/F) \cong S_3$, so

$$[F(\beta_1, \beta_2, \beta_3) : F] = 6 = \frac{24}{4} = \frac{[K : F]}{[K : K^{V_4}]} = [K^{V_4} : K].$$

Thus $F(\beta_1, \beta_2, \beta_3) = K^{V_4}$. □

The proof works for any separable irredcible quartic with Galois group S_4. In the next section, we will show that for any separable irreducible quartic $f = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)(t-\alpha_4) \in F[t]$ with splitting field L/F and Galois group G, we have

$$L^{V_4 \cap G} = F(\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_2\alpha_4, \alpha_1\alpha_4 + \alpha_2\alpha_3).$$

In fact, this observation, together with the results on discriminants from the present section, will enable us to determine G explicitly in terms of the coefficients of f.

4. The Galois Group of a Quartic

In this section we give a complete discussion of Galois groups of irreducible, separable quartic polynomials. This is quite a standard topic in texts on field and Galois theory *outside of characteristic* 2. However, the usual treatment adapts nicely to characteristic 2 using the Berlekamp discriminant. This must be well-known to many experts, but I have not seen it in print. In [**Co-CQ**], Conrad gives a treatment of Galois groups of cubics and of quartics in arbitrary characteristic that proceeds a bit differently: his basic idea is that in the context of the generic polynomial $\prod_{i=1}^n (t - t_i)$, by summing over the A_n-orbit of an "asymmtric monomial" – for $n = 3$ he takes $t_1^2 t_2$, and for $n = 4$ he takes $t_1^3 t_2^2 t_3$ – one gets a primitive element for the quadratic extension $k(t_1, \ldots, t_n)^{A_n}/k(s_1, \ldots, s_n)$ that is independent of the characteristic of k.

4.1. The Kappe–Warren Theorem. Let F be a field, and let $f \in F[t]$ be an irreducible, separable quartic (degree 4) polynomial. Let L/F be the splitting field of F inside an algebraic closure $\overline{F}$ and let $G \coloneqq \mathrm{Aut}(L/F)$ be its Galois group. As we saw in Example 9.4, there are up to conjugacy in S_4 five possibilities for G: it could be the cyclic group C_4, the Klein group V_4, the dihedral group D_4, the alternating group A_4 or the symmetric group S_4. In this section we will explain how to determine G in terms of the coefficients of f.

From the previous section, we have a criterion for $G \subseteq A_4$: when F does not have characteristic 2, this holds if and only if $\delta(f) \in F^{\times 2}$, while if F has characteristic 2, this holds if and only if $\delta_2(F) \in \wp(F)$. Since $\#D_4 \nmid \#A_4$, clearly D_4 does not embed in A_4. Looking back at the explicit descriptions of C_4 and V_4 as subgroups of S_4 and recalling that a k-cycle lies in A_n if and only if k is odd, we see that V_4 is a subgroup of A_4 and C_4 is not. Thus, if $\delta(f) \notin F^{\times 2}$, our task is to determine from f whether G is C_4, D_4 or S_4, while if $\delta(f) \in F^{\times 2}$, we must

determine from f whether G is V_4 or A_4.

Here is a key piece of (very!) classical algebra: if

$$f = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)(t-\alpha_4) \in L[t],$$

then we define

$$\beta_1 := \alpha_1\alpha_2 + \alpha_3\alpha_4,$$
$$\beta_2 := \alpha_1\alpha_3 + \alpha_2\alpha_4,$$
$$\beta_3 := \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

and

$$g := (t-\beta_1)(t-\beta_2)(t-\beta_3) \in L[t].$$

Let $\sigma \in G$. Then σ permutes $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, hence it permutes the set of partitions of $\{1,2,3,4\}$ into two parts each of size 2, hence it permutes $\beta_1, \beta_2, \beta_3$. Thus in fact we have $g \in L^G[t] = F[t]$. The polynomial g is the **resolvent cubic** of F.

EXERCISE 9.21. *Let F be a field, and let $f = t^4 + at^3 + bt^2 + ct + d \in F[t]$ be an irreducible separable polynomial. Show: the resolvent cubic of f is*

$$g := t^3 - bt^2 + (ac - 4d)t + (4bd - a^2d - c^2).$$

EXERCISE 9.22. *Maintain the above notation.*

a) *Show:*
$$\beta_1 - \beta_2 = -(\alpha_4 - \alpha_1)(\alpha_3 - \alpha_2),$$
$$\beta_1 - \beta_3 = -(\alpha_3 - \alpha_1)(\alpha_4 - \alpha_2),$$
$$\beta_2 - \beta_3 = -(\alpha_2 - \alpha_1)(\alpha_4 - \alpha_3).$$
b) *Deduce: $\delta(f) = \delta(g)$. In particular, g is separable.*
c) *Suppose F has characteristic 2. Show: $\delta_2(f) = \delta_2(g)$.*

LEMMA 9.14. *With notation as above, let $\sigma \in G \setminus \{e\}$.*

a) *If σ has cycle type $(2,2)$, then G fixes each of β_1, β_2 and β_3.*
b) *If σ has cycle type $(2,1,1)$ or (4), then σ fixes exactly one root of g and interchanges the other two.*
c) *If σ has cycle type (3), then σ cyclically permutes the roots of g.*

EXERCISE 9.23. *Prove Lemma 9.14.*

Let $M := F(\beta_1, \beta_2, \beta_3)$ be the splitting field of g, so M/F is a Galois extension of degree 1, 2, 3 or 6.

We recall that the transitive subgroups of S_4 are C_4 (three different subgroups, all conjugate), D_4 (three different subgroups, all conjugate), V_4, A_4 and S_4.

• Suppose $G = S_4$. Then in characteristic different from 2, we have $\delta(f) = \delta(g) \notin F^{\times 2}$, while in characteristic 2 we have $\delta_2(f) = \delta_2(g) \notin \wp(F)$. Lemma 9.14 implies that $\mathrm{Aut}(M/F) \cong S_3$. Exactly as in the proof of Proposition 9.13 we see that $M = L^{G \cap V_4} = L^{V_4}$. Conversely, if this discriminant / Berlekamp discriminant condition holds and g is irreducible, then G is not contained in A_4 and $3 \mid [M:F] \mid [L:F] = \#G$, so $G = S_4$.

• Suppose $G = A_4$. Then in characteristic different from 2, we have $\delta(f) = \delta(g) \in$

$F^{\times 2}$, while in characteristic 2 we have $\delta_2(f) = \delta_2(g) \in \wp(F)$. Lemma 9.14 implies that $\mathrm{Aut}(M/F) \cong C_3$. We have $M \subseteq L^{G \cap V_4} = L^{V_4}$ and $[L^{V_4} : F] = \frac{[L:F]}{[L:L^{V_4}]} = \frac{12}{4} = 3 = [M : F]$, so $M = L^{G \cap V_4}$. Conversely, if this discriminant / Berlekamp discriminant condition holds and g is irreducible, then G is contained in A_4 and has order divisible by 3 so $G = A_4$.

• Suppose $G = V_4$. Then in characteristic different from 2, we have $\delta(f) = \delta(g) \in F^{\times 2}$, while in characteristic 2 we have $\delta_2(f) = \delta_2(g) \in \wp(F)$. Lemma 9.14 implies that $M = F$: equivalently, g splits in F. Conversely, if this discriminant / Berlekamp discriminant condition holds and g splits in F, then Lemma 9.14 implies that $G = V_4$. We have $L^{G \cap V_4} = L^G = F = M$.

• Suppose G is isomorphic to C_4. Then G is not contained in A_4, so in characteristic different from 2 we have $\delta(f) = \delta(g) \notin F^{\times 2}$, while in characteristic 2 we have $\delta_2(f) = \delta_2(g) \notin \wp(F)$. Lemma 9.14 implies that g has a unique root in F, which by relabelling the roots of f we may assume is β_1. Thus M/F is a quadratic extension, the unique quadratic subextension of L/F. Then $G \cap V_4$ has order 2, so $L^{G \cap V_4} = M$.

• Suppose G is isomorphic to D_4. Then G is not contained in A_4, so in characteristic different from 2 we have $\delta(f) = \delta(g) \notin F^{\times 2}$, while in characteristic 2 we have $\delta_2(f) = \delta_2(g) \notin \wp(F)$. The polynomial g cannot be irreducible, because then by our above analysis we would have $G = S_4$, and then Lemma 9.14 implies that M/F is a quadratic extension. We have $M \subseteq L^{G \cap V_4}$ and $[L^{G \cap V_4} : F] = [L^{V_4} : F] = \frac{[L:F]}{[L:L^{V_4}]} = \frac{8}{4} = 2 = [M : F]$, so $L^{G \cap V_4} = M$.

We are not quite done: if the discriminant / Berlekamp discriminant of f generates a quadratic subextension of L/F and $[M : F] = 2$, then we have yet to distinguish between $G \cong C_4$ and $G \cong D_4$.

First we give the "classical" criterion to distinguish between C_4 and D_4. If $G \cong C_4$, then $L = K$, so the splitting field of f is a quadratic extension of M, and thus $f \in M[t]$ is reducible. Now suppose that $G \cong D_4$. We claim that in this case $f \in M[t]$ is irreducible. Because $f \in F[t]$ is an irreducible quartic, it cannot have any roots in the quadratic extension M, so the only other possibility is that f factors in $M[t]$ as a product of two irreducible quadratics, so each root of f generates a quadratic extension of M, and in particular $M \subseteq K$. We have $M = L^{V_4}$, so by the Galois Correspondence we have $K = L^H$ for an order 2 subgroup H of V_4. The order 2 subgroups of V_4 are those generated by the elements (12)(34), (13)(24) and (14)(23), but none of these elements fix any of the roots of f: contradiction.

Thus we have distinguished between the Galois groups C_4 and D_4, in a way that was standard up until relatively recently (it is what is done in [**Ja1**] for instance). But this condition is not as practical as one might like. However, a more "elementary test" was given in a note of Kappe–Warren [**KW89**]. We will give their criterion now and then later on in the section we will give a nice application of it that is also done in their paper.

We are in the case where the resolvent cubic g has a unique root in F; reordering $\alpha_2, \alpha_3, \alpha_4$ if necessary, we may assume that this root is $\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4$. We now consider the polynomial

$$h := (t^2 - \beta_1 t + d)(t^2 + at + (b - \beta_1)) \in F[t].$$

Since $(\alpha_1\alpha_2) + (\alpha_3\alpha) = \beta_1$ and $(\alpha_1\alpha_2)(\alpha_3\alpha_4) = d$, the roots of $t^2 - \beta_1 t + d$ are $\alpha_1\alpha_2$ and $\alpha_3\alpha_4$. Similarly, since $(\alpha_1 + \alpha_2) + (\alpha_3 + \alpha_4) = -a$ and

$$(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4$$

$$= (\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4) - (\alpha_1\alpha_2 + \alpha_3\alpha_4) = b - \beta_1,$$

the roots of $t^2 + at + (b - \beta_1)$ are $\alpha_1 + \alpha_2$ and $\alpha_3 + \alpha_4$.

• If $G = C_4$, then h splits in M: indeed, each root of h either lies in F or some quadratic subextension of L/F, but M is the unique quadratic subextension of L/F.

• If $G = D_4$, we claim h does not split in M: if it did, then $t^2 - (\alpha_1 + \alpha_2)t + \alpha_1\alpha_2 \in M[t]$ is a quadratic polynomial with α_1 as a root, so $[M(\alpha_1) : M] \leq 2$ and thus $[M(\alpha_1) : F] \leq 4$. But $M(\alpha_1)$ contains $F(\alpha_1) = K$ and $[K : F] = 4$, so $M(\alpha_1) = K$ and thus M is contained in K, which we saw above is not the case.

This is the "elementary test" given by Kappe–Warren: we distinguish between $G \cong C_4$ and $G \cong D_4$ by whether the polyomial h built from the unique F-rational root of the resolvent cubic splits in the splitting field M of the resolvent cubic. When the characteristic is different from 2, we can touch it up a bit to make it even easier to apply.

By Exercise **??**b), we have $M = F(\delta(f))$. Next we claim that neither of $\delta(t^2 - \beta_1 t + d)$ or $\delta(t^2 + at + (b - \beta_1))$ can be a nonzero square in F, or in other words, if either of these quadratic polynomials has an F-rational root, then it has a repeated F-rational root. To see this: the roots of $t^2 - \beta_1 t + d$ are $\alpha_1\alpha_2$ and $\alpha_3\alpha_4$. Suppose that $\alpha_1\alpha_2 \in F$. Because G is isomorphic to either C_4 or D_4, G contains a 4-cycle σ, and then $\sigma(\{1, 2\}) = \{i, j\} \neq \{1, 2\}$ and $\alpha_1\alpha_2 = \sigma(\alpha_1\alpha_2) = \alpha_i\alpha_j$. If $i = 1$, then we have $\alpha_1\alpha_2 = \alpha_1\alpha_j$ and thus $\alpha_2 = \alpha_j$, contradiction. In a similar way we get a contradiction unless $\{i, j\} = \{3, 4\}$, in which case we have $\alpha_1\alpha_2 = \sigma(\alpha_1\alpha_2) = \alpha_3\alpha_4$. Since the roots of $t^2 + at + (b - \beta_1)$ are $\alpha_1 + \alpha_2$ and $\alpha_3 + \alpha_4$, the same argument works to show that $\alpha_1 + \alpha_2 \in F$ implies $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$. We have

$$\delta(t^2 - \beta_1 t + d) = \beta_1^2 - 4d \text{ and } \delta(t^2 + at + (b - \beta_1)) = a^2 - 4b + 4\beta_1.$$

If $\delta(t^2 - \beta_1 t + d) = 0$, then this factor splits in F so certainly splits in M. If $\delta(t^2 - \beta_1 t + d) \neq 0$ then it is not a square in F, so the splitting field of $t^2 - \beta_1 t + d$ is $F(\sqrt{\beta_1^2 - 4d})$. This quadratic extension is contained in $M = F(\sqrt{\delta(f)})$ if and only if $F(\sqrt{\beta_1^2 - 4d}) = F(\sqrt{\delta(f)})$, which holds if and only if $\beta_1^2 - 4d \equiv \delta(f) \pmod{F^{\times 2}} \iff (\beta_1^2 - 4d)\delta(f) \in F^{\times 2}$. Thus overall we find that $t^2 - \beta_1 t + d$ splits in M if and only if $(\beta_1^2 - 4d)\delta(f)$ is a square in F. The same argument shows that $t^2 + at + (b - \beta_1)$ splits in M if and only if $(a^2 - 4b + 4\beta_1)\delta(f)$ is a square in F.

We have proven the following results, which we will state separately in characteristic different from 2 and in characteristic 2.

THEOREM 9.15. *Let f be a field of characteristic different from 2, and let $f = t^4 + at^3 + bt^2 + ct + d \in F[t]$ be an irreducible (hence separable, because the characteristic is not 2) quartic polynomial, with resolvent cubic g. Let G be the Galois group of f, and let M/F be the splitting field of g. If g has a unique F-rational root r, we put*

$$h \coloneqq (t^2 - rx + d)(t^2 + ax + (b - r)) \in F[t].$$

a) *$G = S_4$ if and only if $\delta(f) \notin F^{\times 2}$ and $g \in F[t]$ has no F-rational root.*
b) *$G = A_4$ if and only if $\delta(f) \in F^{\times 2}$ and $g \in F[t]$ has no F-rational root.*
c) *$G = V_4$ if and only if $g \in F[t]$ splits.*
d) *The following are equivalent:*
   (i) *We have $G \cong C_4$.*
   (ii) *We have $[M : F] = 2$ and f is reducible as a polynomial in $M[t]$.*
   (iii) *The resolvent cubic g has a unique root in F and h splits as a polynomial in $M[t]$.*
   (iv) *Both $(r^2 - 4d)\delta(f)$ and $(a^2 - 4b + 4r)\delta(f)$ are squares in F.*
e) *The following are equivalent:*
   (i) *We have $G \cong D_4$.*
   (ii) *We have $[M : F] = 2$ and f is irreducible as a polynomial in $M[t]$.*
   (iii) *The resolvent cubic g has a unique root in F and h does not split as a polynomial in $M[t]$.*
   (iv) *One of $(r^2 - 4d)\delta(f)$ and $(a^2 - 4b + 4r)\delta(f)$ is not a square in F.*

THEOREM 9.16. *Let f be a field of characteristic 2, and let $f = t^4 + at^3 + bt^2 + ct + d \in F[t]$ be an irreducible, separable quartic polynomial, with resolvent cubic g. Let G be the Galois group of f, and let M/F be the splitting field of g. If g has a unique F-rational root r, we put*

$$h \coloneqq (t^2 - rx + d)(t^2 + ax + (b - r)) \in F[t].$$

a) *We have $G = S_4$ if and only if $\delta_2(f) \notin \wp(F)$ and $g \in F[t]$ has no F-rational root.*
b) *We have $G = A_4$ if and only if $\delta_2(f) \in \wp(F)$ and $g \in F[t]$ has no F-rational root.*
c) *We have $G = V_4$ if and only if $g \in F[t]$ splits.*
d) *The following are equivalent:*
   (i) *We have $G \cong C_4$.*
   (ii) *We have $[M : F] = 2$ and f is reducible as a polynomial in $M[t]$.*
   (iii) *The resolvent cubic g has a unique root in F and h splits as a polynomial in $M[t]$.*
e) *The following are equivalent:*
   (i) *We have $G \cong D_4$.*
   (ii) *We have $[M : F] = 2$ and f is irreducible as a polynomial in $M[t]$.*
   (iii) *The resolvent cubic g has a unique root in F and h does not split as a polynomial in $M[t]$.*

The following exercise shows that every transitive subgroup of S_4 occurs as the Galois group of a quartic polynomial $f \in \mathbb{Q}[t]$.

EXERCISE 9.24. *In each part, you are given a quartic polynomial $f_i \in \mathbb{Q}[t]$. Your task is to first show that f_i is irreducible and then show that its Galois group is as indicated.*

a) *Show:* $f_1 := t^4 + t + 1$ *has Galois group* S_4.
b) *Show:* $f_2 := t^4 + 8t + 12$ *has Galois group* A_4.
c) *Show:* $f_3 := t^4 - 2$ *has Galois group* D_4.
d) *Show:* $f_4 := t^4 - 4t^3 + 59t^2 - 110t + 107$ *has Galois group* C_4.
e) *show:* $f_5 := t^4 + 1$ *has Galois group* V_4.

EXERCISE 9.25. *(K. Conrad) Let* k *be a field of characteristic* 2. *Let* $F := k(s)$, *and let* $f := t^4 + st + s \in F[t]$.

a) *Show:* f *is irreducible and separable.*
b) *Suppose* k *contains a primitive cube root of unity (e.g.* $k = \mathbb{F}_4$*). Show: the Galois group of* f *is* A_4.
c) *Suppose* k *does not contain a primitive cube root of unity (e.g.* $k = \mathbb{F}_2$*). Show: the Galois group of* f *is* S_4.

4.2. Intermediate Subfields. Let K/F be a separable quartic extension. What are the intermediate fields, i.e., the subextensions M of K/F? As for any finite degree separable extension, this can be answered using $G := \mathrm{Aut}(L/F)$, where L is the normal closure of K/F. Let α_1 be a primitive element for K/F, and let f be the minimal polynomial for α_1 over f, so $f = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)(t-\alpha_4) \in L[t]$. Let H be the stabilizer of α_1. Then $K = L^H$, so by the Galois correspondence, subextensions of K/F are in antitone bijection with subgroups of G containing H. By Orbit-Stabilizer, we have $[G : H] = 4$.

• Suppose that H acts transitively on $\{\alpha_2, \alpha_3, \alpha_4\}$, and suppose there is a subgroup H' with $H \subsetneq H' \subseteq G$. Then every element of $H' \setminus H$ moves α_1, so H' is transitive. By Orbit-Stabilizer, $[H'H] = 4$, so $H' = G$. Thus in this case there are no subfields M with $F \subsetneq M \subseteq K$. This happens when $G = S_4$, in which case $H = \mathrm{Sym}(\alpha_2, \alpha_3, \alpha_4) \cong S_3$ and when $G = A_4$, in which case H is generated by the permutation (234). (Clearly the same argument works when $G = S_n$ for any n; as we will see later, the conclusion still holds for $G = A_n$ for all $n \geq 3$.)

• If $G = V_4$ or $G \cong C_4$, then $K = L$ and the action is simply transitive: $H_1 = \{e\}$. Thus subfields $K \subsetneq M \subsetneq F$ correspond to proper nontrivial subgroups of G. When $G = V_4$, there are 2 such subgroups, each of index 2, so there are two quadratic subfields M. When $G = C_4$, there is one such subgroup, of index 2, so there is a unique quadratic subfield M.

• Suppose $G = D_4$. By Example 9.4, G contains a 2-cycle, which stabilizes two different roots. Since all the point stabilizers are conjugate, H_1 also contains a 2-cycle, hence must be generated by a 2-cycle, since it has index 4 hence order 2. We leave it to the reader to show that in the copy $D_{4,1} = \langle (1234), (13) \rangle$, the point stabilizer of 1 is the subgroup generated by (24), and the unique subgroup H' with $H \subsetneq H' \subsetneq D_{4,1}$ is $\langle (13), (24) \rangle$. So K/F has a unique quadratic subfield.

EXERCISE 9.26. *Let* F *be a field of characteristic different from* 2, *and let* K/F *be a quartic field extension. Show that the following are equivalent:*

(i)) *There is a subextension* M *with* $F \subsetneq M \subsetneq K$.
(ii) *The extension* K/F *admits a primitive element* α *with minimal polynomial of the form* $t^4 + bt^2 + d$.

We will now use Theorem 9.15 to compute the Galois group G of an irreducible polynomial of the form $t^4 + bt^2 + d \in F[t]$, where F is a field of characteristic

different from 2. In this case, the resolvent cubic is

$$g = t^3 - bt^2 - 4dt + 4bd = (t-b)(t^2 - 4d).$$

Thus g is reducible, which by Theorem 9.15 rules out $G = S_4$ or $G = A_4$. (We knew this already: by Exercise 9.26, K/F has a quadratic subfield, ruling out A_4 and S_4 by the above discussion.) Theorem 9.15 gives: $G = V_4$ if and only if g splits if and only if $d \in F^{\times 2}$. Suppose $d \notin F^{\times 2}$, so b is the unique root of g in F, the splitting field M of g is $F(\sqrt{d})$ and we have

$$h = (t^2 - bx + d)t^2.$$

So by Theorem 9.15, we have $G = C_4$ if and only if $(b^2 - 4d)d \in F^{\times 2}$. Thus:

THEOREM 9.17. *Let F be a field not of characteristic 2, and let $f := t^4 + bt^2 + d \in F[t]$ be irreducible, with Galois group G. Then:*

a) *If $d \in F^{\times 2}$, then $G \cong V_4$, the Klein 4-group.*
b) *If $d \notin F^{\times 2}$ and $d(b^2 - 4d) \in F^{\times 2}$, then $G \cong C_4$ is cyclic of order 4.*
c) *Otherwise, $G \cong D_4$ is dihedral of order 8.*

EXERCISE 9.27. *(Kappe–Warren) Let F be a field of characteristic different from 2, with algebraic closure $\overline{F}$. Let $b, d \in F$, and put $f := t^4 + bt^2 + d \in F[t]$.*

a) *Show: there are $\alpha, \beta \in \overline{F}$ such that $f = (t-\alpha)(t+\alpha)(t-\beta)(t+\beta) \in \overline{F}[t]$.*
b) *Show that the following are equivalent:*
   (i) *$f \in F[t]$ is irreducible.*
   (ii) *None of α^2, $\alpha + \beta$, $\alpha - \beta$ lie in F.*
   (iii) *None of $b^2 - 4d$, $-b + 2\sqrt{d}$ and $-b - 2\sqrt{d}$ lie in F^2.*
c) *Let p, q be distinct odd primes. Show: $t^4 + pt^2 + q \in \mathbb{Q}[t]$ is irreducible and has Galois group D_4.*

EXERCISE 9.28. *(Conrad) Let F be a field of characteristic different from 2, and let $a \in F$, $b \in F$ and $d \in F^\times \setminus F^{\times 2}$. Put*

$$K := F(\sqrt{a + b\sqrt{d}}),$$

and assume that $[K : F] = 4$. Let G be the Galois group of K/F (i.e., $G = \mathrm{Aut}(L/F)$, where L is the normal closure of K/F).

a) *Show: If f is the minimal polynomial for $\sqrt{a + b\sqrt{d}}$, then $\delta(f) \equiv a^2 - db^2 \pmod{F^{\times 2}}$. Deduce: $a^2 - db^2 \neq 0$.*
b) *Suppose $a^2 - db^2 \in F^{\times 2}$. Show: $G \cong V_4$, and thus K/F is Galois.*
c) *Suppose $a^2 - db^2 \notin F^{\times 2}$ and $d(a^2 - db^2) \in F^{\times 2}$. Show: $G \cong C_4$, and thus K/F is Galois.*
d) *Suppose $a^2 - db^2 \notin F^{\times 2}$ and $d(a^2 - db^2) \notin F^{\times 2}$. Show: $G \cong D_4$, and thus K/F is not Galois.*

EXERCISE 9.29. *Let F be a field of characteristic different from 2, and let $K = F(\sqrt{D})$ be a quadratic extension of F.*

a) *Suppose F contains a primitive 4th roof of unity. Show: there is a cyclic quartic extension L/F containing K as a subfield.*
b) *Show: the following are equivalent:*
   (i) *There is a cyclic quartic extension L/F containing K as a subfield.*
   (ii) *There are $x, y \in F$ such that $D = x^2 + y^2$.*

COROLLARY 9.18. *Let F be a field of characteristic different from 2 and* not *containing a primitive 4th root of unity. Let $d \in F^\times$ be such that $-d \notin F^{\times 2}$ and $\frac{d}{4} \notin F^{\times 4}$, so by Theorem 8.26 the polynomial $t^4 + d \in F[t]$ is irreducible. Let G be the Galois group of f.*

a) *If $d \in F^{\times 2}$, then $G \cong V_4$.*
b) *If $d \notin F^{\times 2}$, then $G \cong D_4$.*

EXERCISE 9.30. *Prove Corollary 9.18.*

It is of some interest to try to realize various Galois groups by polynomials of as simple form as possible. In Exercise 9.24 above we realized both V_4 and D_4 as Galois groups over $\mathbb{Q}$ using polynomials of the form $t^4 + d$; by Corollary 9.18, these are the only two Galois groups that are possible with this polynomials of this especially simple form. However, comparing Exercises 9.24 and 9.26, we see that there is a polynomial of the form $t^4 + bt^2 + d$ with Galois group C_4. Let us find one explicitly.

EXAMPLE 9.19. *We know an irreducible polynomial $f \in \mathbb{Q}[t]$ with Galois group C_4: namely $\Phi_5 = t^4 + t^3 + t^2 + t + 1 = 0$. This is not of the desired form, but we can find a different primitive element for the field $\mathbb{Q}(\zeta_5)$ whose minimal polynomial does have this form. Namely, from Theorem 8.13 we know that $\mathbb{Q}(\zeta_5)$ is a quadratic extension of $\mathbb{Q}(\sqrt{5})$, so $\mathbb{Q}(\zeta_5)$ has a primitive element of the form $\sqrt{r + s\sqrt{5}}$ for some $r, s \in \mathbb{Q}$, so if $t^2 + at + b$ is the minimal polynomial for $r + s\sqrt{5}$, then the polynomial $t^4 + at^2 + b$ has Galois group C_4.*

Explicitly: let $\zeta_5 := e^{2\pi i/5}$. Complex conjugation is an order two field automorphism of $\mathbb{Q}(\zeta_5)$, so its fixed field is a real quadratic field F. Clearly $\alpha := \zeta_5 + \zeta_5^{-1} = \zeta_5 + \overline{\zeta_5}$ lies F. Since $(t - \zeta_5)(t - \zeta_5^{-1}) = t^2 - \alpha t + 1 \in F[t]$, it follows that $F = \mathbb{Q}(\alpha)$. Since α is twice the real part of $e^{2\pi 5}$, we have $\alpha = 2\cos(2\pi/5)$, which in Exercise 9.31 you are asked to show is $\frac{\sqrt{5}-1}{2}$. Thus the discriminant of the quadratic equation $t^2 - \alpha t + 1$ is $\alpha^2 - 4 = \frac{-5}{2} + \frac{-1}{2}\sqrt{5}$, we find that $\mathbb{Q}(\zeta_5) = \mathbb{Q}(\sqrt{\frac{-5}{2} + \frac{-1}{2}\sqrt{5}})$. The minimal polynomial of $\frac{-5}{2} + \frac{-1}{2}\sqrt{5}$ is $t^2 + 5t + 5$, and therefore the splitting field of $t^4 + 5t^2 + 5$ is $\mathbb{Q}(\zeta_5)$, with Galois group C_4.

EXERCISE 9.31. *Show:* $\cos(2\pi/5) = \frac{\sqrt{5}-1}{4}$.
(Suggestion: one approach is to use $\cos(4\pi/5) = \cos(6\pi/5)$ *and the double and triple angle formulas to get a reducible cubic equation with* $\cos(2\pi/5)$ *as a root.)*

5. The Galois Group of a Quintic

We recall that the transitive subgroups of S_5 are: six order five cyclic groups $C_{5,i}$ for $1 \leq i \leq 6$, all conjugate; six order ten dihedral groups $D_{5,i}$ for $1 \leq 6$, all conjugate; six order twenty groups AL_i for $1 \leq i \leq 6$, each isomorphic to $\mathrm{AGL}_1(\mathbb{F}_5)$ and all conjugate; A_6 and S_6. For all $1 \leq i \leq 6$ we have $C_{5,i} \subseteq D_{5,i} \subseteq \mathrm{AL}_i \subseteq S_5$ and $D_{5,i} \subseteq A_5$ (and no containment relations among these groups not implied by these).

EXERCISE 9.32. *Let F be a field not of characteristic 2 and not containing a primitve fourth root of unity. Let $f \in F[t]$ be a separable quintic with Galois group $\mathrm{AGL}_1(\mathbb{F}_5)$. Show: $\delta(f)$ is not a square in F, but it is a sum of two squares in F.*

Let F be a field, and let $f \in F[t]$ be a separable polynomial of degree $n \geq 2$, let L/F be the splitting field of f, let G be the Galois group of f, and write

$f = \prod_{i=1}^n (t - \alpha_i) \in L[t]$. We define

$$S^{(2)}(f) := \prod_{1 \leq i < j \leq n} (t - (\alpha_i + \alpha_j)) \in L[t],$$

a polynomial of degree $\binom{n}{2}$. Then G permutes the roots of $S^{(2)}(f)$, so $S^{(2)}(f) \in F[t]$.

EXERCISE 9.33. *Let F be a field, and let $f := t^6 + dt + e \in F$ be a separable polynomial. Show:*

$$S^{(2)}(f) = t^{10} - 3d^6 - 11et^5 - 4d^2t^2 + 4det - e^2.$$

The following result is a mild generalization of [**JY82**, Lemma II.1.1], wherein they attribute the proof to G.A. Elliott.

LEMMA 9.20. *Let F be a field, and let p be prime number. Let $f \in F[t]$ be irreducible of degree p (hence also separable). Suppose that the cyclotomic polyomial $\Phi_p(t) \in F[t]$ is irreducible. Then $S^{(2)}(f) \in F[t]$ is separable.*

PROOF. If $p = 2$, then $S^{(2)}(f)$ is linear and the conclusion is clear, so we may assume $p \geq 3$. The irreducibility of $\Phi_p(t)$ implies that F does *not* have characteristic p, since in characteristic p we have $\Phi_p = \frac{t^p-1}{t-1} = (t-1)^{p-1}$.

Let L/F be the splitting field of f, and factor $f \in L[t]$ as $\prod_{i=1}^p (t - \alpha_i)$. Let V be the F-subspace of L spanned by $\alpha_1, \ldots, \alpha_p$. Let G be the Galois group of f. Since G is a transitive subgroup of S_p and p is prime, we have that G contains a p-cycle, and by reordering the α_i's we may assume that $\sigma := (12 \cdots p) \in G$. The automorphism σ of L restricts to a F-linear automorphism of V. Let $\overline{F}$ be an algebraic closure of F, let $\overline{V} := V \otimes_F \overline{F}$, and let $\overline{\sigma} = \sigma \otimes 1$ be the unique extension of σ to an $\overline{F}$-linear automorphism of $\overline{V}$. Since $\overline{\sigma}^p = 1$ and the characteristic is not p, the minimal polynomial of $\overline{\sigma}$ has distinct eigenvalues, so $\overline{\sigma}$ can be diagonalized with corresponding eigenvalues pth roots of unity. Thus, if $t := \dim_F V$, then there is an $\overline{F}$-basis $e_1, \ldots, e_t$ for $\overline{V}$ and pth roots of unity $\zeta_1, \ldots, \zeta_t$ such that

$$\forall 1 \leq i \leq t,\ \overline{\sigma}(v_i) = \zeta_i v_i.$$

there are unique $a_1, \ldots, a_t \in \overline{F}$ such that

$$\alpha_1 = \sum_{i=1}^t a_i v_i.$$

Since $\overline{\sigma}(\alpha_1) = \alpha_2 \neq 1$, there is $1 \leq I \leq t$ such that $a_I \neq 0$ and $\zeta_I \neq 1$. It follows that there is a primitive pth root of unity so that – with respect to the basis $v_1, \ldots, v_t$ – the set of Ith coordinates of the vectors $\alpha_1, \ldots, \alpha_p$ is $\{c_I \zeta^j \mid 0 \leq j \leq p-1\}$. Thus if there are $0 \leq i_1, j_1, i_2, j_2 \leq p-1$ with $i_1 \neq j_1$, $i_2 \neq j_2$ and $\{i_1, j_1\} \neq \{i_2, j_2\}$ such that $\alpha_{i_1} + \alpha_{j_1} = \alpha_{i_2} + \alpha_{j_2}$, then projecting onto the Ith coordinate shows that there are $1 \leq i_1, j_1, i_2, j_2 \leq p-1$ with $i_1 \neq j_1$, $i_2 \neq j_2$ and $\{i_1, j_1\} \neq \{i_2, j_2\}$ such that $\zeta^{i_1} + \zeta^{j_1} = \zeta^{i_2} + \zeta^{j_2}$, so ζ would be a root of the nonzero polynomial $t^{i_1} + t^{j_1} - t^{i_2} - t^{j_2} \in F[t]$, hence is also a root of $t^{i_1-1} + t^{j_1-1} - t^{i_2-1} - t^{j_2-1}$, which has degree at most $p-2$. However, the hypothesis on the irreducibility of $\Phi_p \in F[t]$ means that Φ_p, of degree $p-1$, is the minimal polynomial of ζ, a contradiction. □

The following result is a direct consequence of Lemma 9.20 and Theorem 8.8:

COROLLARY 9.21. *If $f \in \mathbb{Q}[t]$ is irreducible of prime degree p, then $S^{(2)}(f) \in \mathbb{Q}[t]$ is separable.*

LEMMA 9.22. *Suppose F is a field of characteristic different from 2. Let $f \in F[t]$ be separable of degree $n \geq 3$, and suppose that $S^{(2)}(f)$ is separable. Then f and $S^{(2)}(f)$ have the same splitting field.*

PROOF. It is immediate that the splitting field of $S^{(2)}(f)$ is contained in the splitting field of f. Conversely, let $1 \leq i \leq n$, and choose $1 \leq j, k \leq n$ such that i, j, k are all distinct. Then

$$\alpha_i = \frac{(\alpha_i + \alpha_j) + (\alpha_i + \alpha_k) - (\alpha_j + \alpha_k)}{2},$$

so the splitting field of f is contained in the spliting field of $S^{(2)}(f)$. □

Let G be a group acting on a nonempty set X, and let k be an integer with $1 \leq k \leq \#X$. The action is **k-homogeneous** if the induced action on the set of k-element subsets of X is transitive. Clearly 1-homogeneous is the same as transitive. Immediately from the definition we have that a k-transitive action is k-homogeneous. It is natural to ask about the converse. If X is finite and $k \leq \frac{\#X}{2}$, then it turns out that a k-homogeneous action must be $(k-1)$-transitive. If $k \geq 5$, it must be k-transitive, but if $2 \leq k \leq 4$ there are some highly limited exceptions: when $k = 2$ there is one infinite family of exceptions, all involving group actions on a set of size a prime power $q \equiv 3 \pmod 4$. When $k = 3$ there is a simlar infinite family of exceptions plus exactly three more exceptions, and when $k = 4$ there are precisely three exceptions. For all this, see [**DM**, Thm. 9.4B].

For transitive subgroups of S_5, we already know that S_5 is 5-transitive, A_5 is 3-transitive and $\mathrm{AGL}_1(\mathbb{F}_5)$ is 2-transitive. The subgroup D_5 is not 2-homogeneous: indeed D_5 acts isometrically on the vertices of a regular 5-gon, hence preserves distances between pairs of distinct points. Thus a pair of adjacent vertices cannot lie in the same D_5-orbit as a pair of non-adjacent vertices. The subgroup C_5 of D_5 is therefore not 2-homogeneous as well. In particular, a subgroup of S_5 is 2-homogeneous if and only if it is 2-transitive.

The relevance of this is the following:

LEMMA 9.23. *Let F be a field, let $f \in F[t]$ be separable of degree $n \geq 3$, and suppose that $S^{(2)}(f)$ is separable. Then $S^{(2)}(f) \in F[t]$ is irreducible if and only if G (viewed as a permutation group on the roots of f) is 2-homogeneous.*

PROOF. Indeed, separability of R_2 means that the G-action on roots of $S^{(2)}(f)$ is equivalent to the G-action on 2-element subsets of the roots of f, so $S^{(2)}(f)$ is irreducible if and only if the former action is transitive if and only if the latter action is 2-homogeneous. □

We come back to the generic case: let k be a field, $K = k(t_1, \ldots, t_5)$ and $F = k(s_1, \ldots, s_5)$, and consider the element

$$\theta_1 := t_1^2 t_2 t_5 + t_1^2 t_3 t_4 + t_2^2 t_1 t_3 + t_2^2 t_4 t^5 + t_3^2 t_1 t_5 +$$
$$t_3^2 t_2 t_4 + t_4^2 t_1 t_2 + t_4^3 t_3 t_5 + t_5^2 t_1 t_4 + t_5^2 t_2 t_3 \in K.$$

One computes that its stabilizer is $\mathrm{AL}_{5,1} := \langle (12345), (2354) \rangle$, which has index 6 in S_5. Put $\sigma := (12345)$. Its Galois conjugates are

$$\theta_1,\ \theta_2 := (12)\theta_1,\ \theta_3 := \sigma\theta_2,\ \theta_4 := \sigma\theta_3,\ \theta_5 := \sigma\theta_4,\ \theta_6 := \sigma\theta_5.$$

It follows that the stabilizers of the θ_i's are precisely the six conjugates of $\mathrm{AL}_{5,1}$ in S_5 and thus are precisely the maximal solvable transitive subgroups of S_5. We also observe that since no $\mathrm{AL}_{5,1}$ is contained in A_5, then $\mathrm{AL}_{5,1} \cap A_5$ has index at least 6 in A_5, hence A_5 acts transitively on $\{\theta_1, \ldots, \theta_6\}$.

We may define a **sextic resolvent polynomial**

$$R_6(f) \coloneqq (t-\theta_1)(t-\theta_2)(t-\theta_3)(t-\theta_4)(t-\theta_5)(t-\theta_6) \in F[t].$$

Using a computer algebra package to express symmetric functions in the t_i's as polynomials in the s_i's we can explicitly write down a formula for $R_6(f)$ in terms of the coefficients of f. In [**Du91**], Dummit writes down such a formula for when f is a depressed quintic (i.e., with the coefficient of t_4 set equal to 0, to which any quintic can be reduced away from characteristic 5): this formula occupies 14 lines. In the case

$$f = t^5 + dt + e,$$

it simplifies to

$$R_6(f) = t^6 + 8dt^5 + 40d^2t^4 + 160d^3t^3 + 400d^4t^2 + (512d^5 - 3125e^4)t + (256d^6 - 9375de^4).$$

LEMMA 9.24. *Let F be a field not of characteristic 5, and let $f \in F[t]$ be an irreducible, separable quintic. Then $R_6(f)$ is separable.*

PROOF. Let G be the Galois group of f. By Orbit-Stabilizer, G contains a 5-cycle, and we may order the roots of f so that $\sigma \coloneqq (12345) \in G$. Above we ordered the roots of $R_6(f)$ such that σ fixes θ_1 and maps $\theta_2 \mapsto \theta_3 \mapsto \theta_4 \mapsto \theta_5 \mapsto \theta_6 \mapsto \theta_2$. Thus σ induces a five-cycle on the roots of $R_6(f)$ other than θ_1. If all of $\theta_2, \ldots, \theta_6$ are distinct, then since σ fixes θ_1 they must all be distinct from θ_1 and thus $R_6(f)$ is separable. If two of $\theta_2, \ldots, \theta_6$ are equal, then because 5 is prime we must have $\theta_2 = \theta_3 = \theta_4 = \theta_5 = \theta_6$. Seeking a contradiction, we assume this. Then:

$$0 = (\alpha_5 - \alpha_3)(\alpha_1 - \alpha_4)(\theta_2 - \theta_3) - (\alpha_5 - \alpha_1)(\alpha_3 - \alpha_4)(\theta_6 - \theta_4)$$

$$= (\alpha_1 - 2\alpha_2 + \alpha_3)(\alpha_1 - \alpha_4)(\alpha_4 - \alpha_3)(\alpha_1 - \alpha_5)(\alpha_3 - \alpha_5)(\alpha_4 - \alpha_5),$$

which since f is separable implies $\alpha_1 - 2\alpha_2 + \alpha_3 = 0$. Applying σ repeatedly to this linear equation we get $\alpha_2 - 2\alpha_3 + \alpha_4 = 0, \ldots, \alpha_5 - 2\alpha_1 + \alpha_2 = 0$.

Clearly the solution space of this linear system contains the line ℓ in which $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = \alpha_5$, so these are the only solutions if and only if the coefficient matrix has rank 4. The rank of a matrix with entries in a field F depends only on its reduced row echelon form so is invariant under extensions of F. Moreover the coefficients of the matrix are intgers hence lie in the prime subfield of F, so whether the solution space is the line ℓ depends only on the characteristic of F. When F has characteristic 0 we may work over the real numbers: placing $\alpha_1, \ldots, \alpha_5$ as the vertices of a regular pentagon, the linear system is saying that the value at each vertex is the average of the values at the adjacent vertices. Choosing the vertex with maximum value, this means that the two vertices adjacent to the maximum vertex also share the same maximum value, and then moving around the circle we get that the values at all the vertices are equal. Notice that this argument did use that we had five equations: it works for all $n \geq 3$ with an $n \times n$ matix whose first row is $(1, -2, 1, 0, \ldots, 0)$ and whose remaining $n-1$ rows are the cyclic permutations of the first row.

In general, we compute that each of the 4×4 minors of the matrix

$$M := \begin{bmatrix} 1 & -2 & 1 & 0 & 0 \\ 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 1 & -2 & 1 \\ 1 & 0 & 0 & 1 & -2 \\ -2 & 1 & 0 & 0 & 1 \end{bmatrix} \in M_5(\mathbb{Z})$$

is ± 5. Since the rank of a matrix is the largest i such that there is a nonvanishing $i \times i$ minor, this shows that viewed as a matrix in a field F, the matrix M has rank 4 if and only if the characteristic of F is not 5.

We are done, but let's say a bit more about what's going on here: M and its transpose M^T are **circulant matrices**, namely $n \times n$ matrices whose rows are cyclic permutations of the first row. For a circulant matrix C defined over a field F, if its first column is $(a_0, a_1, \ldots, a_{n-1})$, then we have [**In56**, Prop. 1.1]

$$\operatorname{rank}(C) = n - \deg(\gcd(a_{n-1}t^{n-1} + \ldots + a_1 t + a_0, t^n - 1)).$$

For $n \geq 3$, let M_n be the circulant matrix with first row $(1, -2, 1, 0, \ldots, 0)$. Then M_n^T is circulant with first column $(1, -2, 1, 0, \ldots, 0)$, so

$$\operatorname{rank}(M_n) = \operatorname{rank}(M_n^T) = n - \deg(\gcd((t-1)^2, t^n - 1)).$$

If the characteristic of F does not divide n, then this gcd is $t - 1$, so M has rank $n - 1$; otherwise this gcd is $(t-1)^2$, so the rank is $n - 2$. □

Remark 9.1. *Unlike cubic resolvent of a quartic polynomial, in general the separability of a quintic polynomial f is* not *sufficient to ensure the separability of the sextic resolvent $R_6(f)$. For example, over any field F of characteristic different from 5, the polynomial $f := t^5 + t^5 + t^4 + t^3 + t^2 + t = t \cdot \Phi_5(t)$ is separable, but $R_6(f) = (t+1)^2(t^4 + 4t^3 + 16t^2 + 49t + 61)$.*

Theorem 9.25. *(Dummit) Let F be a field not of characteristic 5, and let $f \in F[t]$ be an irreducible quintic with Galois group G.*

a) *If G is solvable, then $R_6(f)$ factors as a linear polynomial times an irreducible quintic.*
b) *If G is not solvable, then $R_6(f)$ is irreducible.*

Proof. Since $R_6(f)$ is separable and the splitting field of $R_6(f)$ is a subfield of the splitting field of f, the action of G on the roots of $R_6(f)$ determines a homomorphism $G \hookrightarrow S_6$, whose image $\overline{G}$ is the Galois group of $R_6(f)$. Since G is a transitive subgroup of S_5, by Orbit-Stabilizer G contains a 5-cycle, and by relabelling the roots of f we may assume that $\sigma := (12345) \in G$.
a) Suppose that G is solvable. Then G is contained in a subgroup $\mathrm{AL}_{5,i}$ for some i. The group $\mathrm{AGL}_1(\mathbb{F}_5)$ has $(\mathbb{F}_5, +)$ as a normal Sylow 5-subgroup, hence a unique subgroup of order 5, so the subgroups $\mathrm{AL}_{5,i}$ are indexed by the 6 order 5 subgroups of S_5 and thus G is contained in $\mathrm{AL}_{5,1} = \langle (12345), (2354) \rangle$. Thus G fixes θ_1, hence so does $\overline{G}$, so $\theta_1 \in F$. Because σ cyclically permutes $\theta_2, \theta_3, \theta_4, \theta_5, \theta_6$, so does the image of σ in $\overline{G}$, hence $\prod_{i=2}^{6}(t - \theta_i) \in F[t]$ is an irreducible quintic.
b) Suppose that G is not solvable. Then G contains A_5, which we saw above acts transitively on the roots of $R_6(f)$, hence $\overline{G}$ acts transitively on the roots of $R_6(f)$ and $R_6(f)$ is irreducible. □

We deduce the following result that is *almost* a complete determination of the Galois group of an irreducible quintic over a class of fields F including $F = \mathbb{Q}$:

COROLLARY 9.26. *Let F be a field such that $\Phi_5 \in F[t]$ is irreducible. (In particular, F cannot have characteristic 5.) Let $f \in F[t]$ be an irreducible quintic polynomial. Let G be the Galois group of f.*

a) *Suppose that $S^{(2)}(f) \in F[t]$ is irreducible and $R_6(f) \in F[t]$ has no F-rational root. If F does not have characteristic 2, suppose moreover that $\delta(f) \notin F^{\times 2}$, while if F has characteristic 2, suppose moreover that $\delta_2(f) \notin \wp(F)$. Then $G = S_5$.*
b) *Suppose that $S^{(2)}(f) \in F[t]$ is irreducible and $R_6(f) \in F[t]$ has no F-rational root. If F does not have characteristic 2, suppose moreover that $\delta(f) \in F^{\times 2}$, while if F has characteristic 2, suppose moreover that $\delta_2(f) \in \wp(F)$. Then $G = A_5$.*
c) *Suppose that $S^{(2)}(f) \in F[t]$ is irreducible and $R_6(f) \in F[t]$ has an F-rational root. Then $G \cong \mathrm{AGL}_1(\mathbb{F}_5)$.*
d) *The following are equivalent:*
   (i) *The $S^{(2)}(f) \in F[t]$ is reducible.*
   (ii) *The polynomial $R_6(f)$ has an F-rational root; if f does not have characteristic 2 then $\delta(f) \in F^{\times 2}$; and if F has characteristic 2 then $\delta_2(f) \in \wp(F)$.*
   (iii) *The Galois group G is isomorphic to C_5 or D_5.*

PROOF. We have shown that $S^{(2)}(f)$ is irreducible if and only if G is S_5 or A_5 or is isomorphic to $\mathrm{AGL}_1(\mathbb{F}_5)$. We have also shown that $R_6(f)$ has an F-rational root if and only if G is isomorphic to C_5, D_5 or $\mathrm{AGL}_1(\mathbb{F}_5)$. Finally, $\delta(f)$ is a square / $\delta_2(f) \in \wp(F)$ holds if and only if G is a subgroup of A_5 if and only if G is A_5 or is isomorphic to C_5 or D_5. Every case follows immediately from this. □

Our situation is eerily familiar from the quartic case: our resolvent and discriminant conditions allow us to characterize three of the five possible Galois groups, but they do not allow us to tell whether the Galois group is cyclic or dihedral. When $F = \mathbb{Q}$, Dummit in [**Du91**] completes the analysis in a way that is somewhat similar to what Kappe–Warren did in the quartic case: when the Galois group is either C_5 or D_5, from the unique rational root θ of $R_6(t)$, Dummit constructs a product of two quadratics $h(t) \coloneqq Q_1(t)Q_2(t) \in \mathbb{Q}[t]$ such that the Galois group is C_5 if and only if h splits in $\mathbb{Q}[t]$. The bad news is that the formulas for the coefficients of h are *very* complicated: indeed, working with the depressed quintic $t^5+bt^3+ct^2+dt+e \in \mathbb{Q}[t]$, in the appendix to his paper he writes down the necessary formulas. The appendix is 45 pages! So we are not going to give Dummit's criterion here (which is a bit of a shame because some interesting mathematics is used to derive it). Though Dummit works exclusively over $\mathbb{Q}$, I believe his argument should work verbatim over a field of characteristic different from 2 in which $\Phi_5(t)$ is irreducible, and it may be possible to include the characteristic 2 case using Berlekamp discriminants.

Because we have not yet seen a quintic polynomial with Galois group D_5, we will derive a *sufficient* condition for the Galois group of an irreducible quintic $f \in \mathbb{Q}[t]$ to have Galois group D_5.

THEOREM 9.27. *Let $f \in \mathbb{Q}[t]$ be an irreducible polynomial of odd degree $n \in \mathbb{Z}^+$, with Galois group G.*

a) *If $\#G = n$, then f splits in $\mathbb{R}[t]$.*
b) *Thus if f does not split in $\mathbb{R}$ and f satisfies the equivalent condition of Corollary 9.26d), then the Galois group of f is isomorphic to D_5.*

PROOF. a) We will give two proofs.
FIRST PROOF: Since $\#G = n = \deg(f)$, the splitting field of f is $K := \mathbb{Q}[t]/(f)$. Since f has odd degree, it has a real root, and thus there is a field embedding $K \hookrightarrow \mathbb{R}$. Because $K/\mathbb{Q}$ is normal, every field embedding $\sigma : \mathbb{Q} \hookrightarrow \mathbb{C}$ has $\sigma(K) \subseteq K \subseteq \mathbb{R}$, so all roots of f are real.
SECOND PROOF: We go by contraposition: if f does not split in $\mathbb{R}[t]$ then f has a pair of non-real complex conjugate roots α and $\overline{\alpha}$. This means that complex conjugation acts nontrivially on the splitting field L of f, so $2 \mid [L : \mathbb{Q}] = \#G$, so G does not have order n.
b) This follows immediately from part a) and Corollary 9.26d). □

The following exercise shows that all five transitive subgroups of S_5 occur as Galois groups over $\mathbb{Q}$.

EXERCISE 9.34.

a) *Let $f_1 := t^5 - t + 1 \in \mathbb{Q}[t]$. Show: f_1 is irreducible. Then use Corollary 9.26 to show that f has Galois group S_5.*
b) *Let $f_2 := t^5 + 20t + 16 \in \mathbb{Q}[t]$. Show: f_2 is irreducible. Then use Corollary 9.26 to show that f has Galois group A_5.*
c) *Let $f_3 := t^5 - 2$. Use Theorem 8.26 to show that f_3 is irreducible. Use Proposition 8.29 to show that it has Galois group isomorphic to $\mathrm{AGL}_1(\mathbb{F}_5)$, then confirm this using Corollary 9.26.*
d) *Let $f_4 := t^5 - 5t + 12$. Show: f_4 is irreducible. Use calculus to show that f_4 has exactly one real root. Then use Theorem 9.27 to show that f has Galois group isomorphic to D_5.*
e) *Let $f_5 := t^5 + t^4 - 4t^3 - 3t^2 + 3t + 1$. Show: f_5 is the minimal polynomial of $2\cos(\frac{2\pi}{11})$. Deduce: the Galois group of f_5 is isomorphic to C_5.*

In §10 we will show that the converse of Theorem 9.27 need not hold: an irreducible quintic $f \in \mathbb{Q}[t]$ can have five real roots and still have Galois group D_5.

6. S_p as a Galois group over $\mathbb{Q}$

In this section we will show that S_p occurs as a Galois group over $\mathbb{Q}$ for all primes p. We already know this for $p = 2, 3, 5$, so it suffices to treat $p \geq 7$. In fact our present method will work for all $p \geq 5$.

LEMMA 9.28. *Let p be a prime number. In the symmetric group S_p, let σ be any p-cycle and let τ be any transposition (i.e., of the same cycle type as (12)). Then the subgroup generated by σ and τ is all of S_n.*

PROOF. Step 1: The conclusion is not changed by simultaneously conjugating σ and τ, so we may assume that $\tau = (12)$. Some power of σ^i of σ maps 1 to 2; because p is prime, this power must still be a p-cycle. Of course we have $\langle \sigma^i, \tau \rangle \subseteq \langle \sigma, \tau \rangle$, so it suffices to show that the former subgroup is all of S_p. Thus we may assume that $\sigma = (12i_3 \dots i_p)$, and then after reordering the elements $3, 4, \dots, p$ (the point being that τ only moves 1 and 2), we may assume that $\sigma = (12 \dots p)$.

Step 2: Now we will show that for any $n \in \mathbb{Z}^+$, if $\sigma = (12\ldots n$ and $\tau = (12)$, then $\langle \sigma, \tau \rangle = S_n$. Indeed, let $2 \leq i \leq n-2$, and observe that

$$\sigma^i(12)\sigma^{-i} = (i+1\ i+2).$$

Thus the subgroup generated by σ and τ contains all transpositions of consecutive elements, hence the subgroup it generates is all of S_n. □

EXERCISE 9.35. *Let $n \in \mathbb{Z}^{\geq 2}$, let $\tau = (12)$, and let $\sigma \in S_n$ be an n-cycle. There is a unique $1 \leq i < n$ such that σ^i maps 1 to 2. Show: $\langle \sigma, \tau \rangle = S_n$ if and only if $\gcd(i, n) = 1$.*

PROPOSITION 9.29. *Let p be a prime number, let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p with exactly two nonreal roots, and let $L/\mathbb{Q}$ be the splitting field of f. Then $\mathrm{Aut}(L/\mathbb{Q}) \cong S_p$.*

PROOF. We write $f = \prod_{i=1}^p (t - \alpha_i) \in L[t]$ and regard G as a subgroup of S_p. Let $K := \mathbb{Q}(\alpha_1)$, so $[K : \mathbb{Q}] = p$. It follows that $p \mid [L : \mathbb{Q}] = \#G$. By Cauchy's Theorem, there is a p-cycle σ in G. Let τ be complex conjugation. Since the complex conjugate of an algebraic number is again an algebraic number (with the same minimal polynomial) and $L/\mathbb{Q}$ is normal, the automorphism τ restricts to give an order two element of G. By the hypothesis on the number of nonreal roots, τ must be a transposition, and now Lemma 9.28 shows that $G = S_p$. □

EXERCISE 9.36. *Let*

$$f := (t^2+2)t(t-2)(t+2)(t-4)(t+4) + 2 = t^7 - 18t^5 + 24t^3 + 128t + 2 \in \mathbb{Q}[t].$$

Use Eisenstein's Criterion and Proposition 9.29 to show that f is irreducible and has Galois group S_7.

The idea of Exercise 9.36 is that for a given prime p, finding a polynomial that satisfies the hypotheses of Theorem 9.29 is not especially hard. But to do this systematically for all primes $p \geq 5$ at once requires some care. First we recall a classical result.

THEOREM 9.30 (Continuity of Roots). *Let $n \in \mathbb{Z}^+$. For $f = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$ and $g = t^n + b_{n-1}t^{n-1} + \ldots + b_1 + b_0$ in $\mathbb{C}[t]$, we put*

$$d(f, g) := \max_{0 \leq i \leq n-1} |a_i - b_i|.$$

For all $\epsilon > 0$, there is $\delta > 0$ such that if $d(f, g) < \delta$, there are $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, beta_n \in \mathbb{C}$ such that

$$f = (t - \alpha_1)\cdots(t - \alpha_n),\ g = (t - \beta_1)\cdots(t - \beta_n)$$

and $|\alpha_i - \beta_i| < \epsilon$ for all $1 \leq i \leq n$.

PROOF. See e.g. [**Br10**, Thm. 0]. □

EXERCISE 9.37. *Maintain the notation of Theorem 9.30 and let $f \in \mathbb{R}[t]$ be a polynomial of degree $n \geq 1$ with no repeated* real *roots. Show: there is $\delta = \delta(f) > 0$ such that if $g \in \mathbb{R}[t]$ is a degree n polynomial with $d(f, g) < \epsilon$, then g has the same number of real roots as f.*

EXERCISE 9.38. *Let $f : \mathbb{R} \to \mathbb{R}$ be continuously differentiable such that:*

(i) *f and f' have finitely many roots: $f^{-1}(\{0\})$ and $(f')^{-1}(\{0\})$ are finite;*
(ii) *f has simple roots: there is no $x \in \mathbb{R}$ such that $f(x) = f'(x) = 0$; and*

(iii) $\lim_{|x|\to\infty} |f(x)| = \infty$.

If there is no root of f', put $C \coloneqq \infty$; otherwise, put

$$C \coloneqq \max_{x\in\mathbb{R}|f'(x)=0} |f(x)| > 0.$$

Show: if $c \in \mathbb{R}$ is such that $|c| < C$, then $\#f^{-1}(0) = \#f^{-1}(c)$.

Now we will use construct, for all primes $p \geq 5$, a degree p polynomial $f \in \mathbb{Q}[t]$ satisfying the hypotheses of Proposition 9.29 and thus having Galois group S_p. This construction is taken from Milne's field theory notes [**Mi**], in which it is attributed to Martin Ward; it is a simplified version of an older construction.

Choose even positive integers m and $n_1 < n_2 < \ldots < n_{p-2}$, and put

$$g \coloneqq (t^2 + m)(t - n_1)\cdots(t - n_{p-2}) \in \mathbb{Q}[t].$$

Then g is a separable polynomial of degree p with exactly two nonreal roots. By either Exercise 9.37 or 9.38, for any real number δ of sufficiently small absolute value, the polynomial $f + \delta$ also has exactly two nonreal roots. We will take δ to be of the form $\frac{-2}{n}$ for a sufficiently large odd positive integer n, and put

$$f \coloneqq g - \frac{2}{n} \in \mathbb{Q}[t].$$

Now write

$$nf = nt^p + a_{n-1}t^{p-1} + \ldots + a_1 t + a_0 \in \mathbb{Z}[t].$$

This polynomial is Eisenstein at 2: the leading coefficient n is odd, for $1 \leq i \leq p-1$, the coefficient a_i is even, and $a_0 \equiv 2 \pmod 4$. So this polynomial is irreduible over $\mathbb{Z}[t]$, hence by Gauss's Lemma f is irreducible over $\mathbb{Q}[t]$. By Proposition 9.29, the splitting field of f over $\mathbb{Q}$ is Galois with automorphism group S_p.

7. Solvability in Prime Degree

Let F be a field, and let $f \in F[t]$ be an irreducible separable polynomial of degree n, with splitting field K and Galois group G. Galois himself made a deep and beautiful study of when G is solvable.

The simplest case is when $n = p$ is a prime number so G is a transitive subgroup of the symmetric group S_p. In this case Galois showed that G is solvable if and only if K is generated over F by any two distinct roots of f. He also showed that there is a single subgroup $\mathrm{AGL}_1(\mathbb{F}_p)$ of S_p (which we will define shortly) such that a transitive subgroup G of S_p is solvable if and only if it is conjugate to a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p)$.

When n is composite, there is a dichotomy in the study of subgroups of S_n: such subgroups can be either **primitive** or **imprimitive**. (When $n = p$ is prime, every transitive subgroup is primitive.) When $n = p^2$ is the square of a prime and G is imprimitive, then there is again a single subgroup $\mathrm{AGL}_1(\mathbb{F}_p)\wr\mathrm{AGL}_1(\mathbb{F}_p)$ of S_{p^2} such that G is solvable if and only if it is conjugate to a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p)\wr\mathrm{AGL}_1(\mathbb{F}_p)$. In the primitive case, there are three such subgroups M_1, M_2, M_3 of S_{p^2} such that G is solvable if and only if it is conjugate to a subgroup of M_i for some $1 \leq i \leq 3$. Finally, if G is a primitive solvable subgroup of S_n, then it turns out that $n = p^a$ is a prime power, so up to conjugacy we may view S_n as the group of bijections on the set $\mathbb{F}_p^a$, and Galois showed that up to conjugacy, G contains the additive

subgroup $\mathbb{F}_p^a$ and is contained in a group $\mathrm{AGL}_a(\mathbb{F}_p)$. When $a = 1$, this recovers the first result mentioned above. However, for $a \geq 2$, the group $\mathrm{AGL}_a(\mathbb{F}_p)$ is usually not solvable: the only exceptions are $\mathrm{AGL}_2(\mathbb{F}_2)$ and $\mathrm{AGL}_2(\mathbb{F}_3)$.

For a commutative ring R, we denote by $\mathrm{AGL}_1(R)$ the group of invertible affine linear maps on R, i.e., functions from R to R of the form $x \mapsto ax + b$ for $a \in R^\times$ and $b \in R$.

Exercise 9.39. *Let F be a commutative ring.*

a) *Show:* $\mathrm{AGL}_1(R)$ *is naturally isomorphic to the subgroup of* $\mathrm{GL}_2(R)$ *consisting of matrices of the form* $\left[\begin{array}{cc} a & b \\ 0 & 1 \end{array}\right]$ *with* $a \in R^\times$ *and* $b \in R$.

b) *Show:* $\mathrm{AGL}_1(\mathbb{Z}/n\mathbb{Z})$ *is isomorphic to the group $G(n)$ from §9.3.*

c) *Show:* $\mathrm{AGL}_1(R)$ *acts transitively on R.*

d) *Show:* $\mathrm{AGL}_1(R) = (R, +) \rtimes (R^\times, \cdot)$. *($R^\times$ acts on R via multiplication.)*

e) *Deduce: if R is finite, then* $\mathrm{AGL}_1(R)$ *is a finite solvable group.*

Let F be a field, and let $F \in F[t]$ be a separable polynomial of prime degree p. The group $\mathrm{AGL}_1(\mathbb{F}_p)$ has a natural faithful action on $\mathbb{F}_p$, which by Cayley's Theorem allows us to view it as a subgroup of S_p. As usual, this is well-defined up to conjugacy, but if we use the bijection from $\{1, \ldots, p\}$ to $\mathbb{F}_p$ given by $i \mapsto i \pmod p$ then this nails down $\mathrm{AGL}_1(\mathbb{F}_p)$ as a specific subgroup of S_p.

Let $\theta := (12 \ldots p) \in S_p$. This is the permutation obtained from the translation $x \mapsto x + 1$, hence is an element of $\mathrm{AGL}_1(\mathbb{F}_p)$.

Lemma 9.31.

a) *The normalizer of $\langle\theta\rangle$ in S_p is* $\mathrm{AGL}_1(\mathbb{F}_p)$.

b) *Let $\tau \in S_p$ be such that $\tau\theta\tau^{-1} \in \mathrm{AGL}_1(\mathbb{F}_p)$. Then $\tau \in \mathrm{AGL}_1(\mathbb{F}_p)$.*

Proof. a) Since $\theta \in \mathrm{AGL}_1(\mathbb{F}_p)$, clearly $\mathrm{AGL}_1(\mathbb{F}_p)$ is contained in the normalizer of $\langle\theta\rangle$. Conversely, let $\tau \in S_p$ lie in the normalizer of $\langle\theta\rangle$: thus there is some $1 \leq \ell \leq p-1$ such that $\tau\theta = \theta^\ell\tau$, which means:

$$\forall i \in \mathbb{F}_p,\ \tau(i+1) - \tau(i) = \ell. \tag{34}$$

We do not disturb whether τ lies in $\mathrm{AGL}_1(\mathbb{F}_p)$ by adjusting by an element of the subgroup $(\mathbb{F}_p, +)$, so we may assume that $\tau(0) = 0$, and then (34) implies that $\tau(i) = \ell i$ for all $i \in \mathbb{F}_p$, so $\tau \in \mathbb{F}_p^\times \subseteq \mathrm{AGL}_1(\mathbb{F}_p)$.
b) Let $\tau \in S_p$ be such that $\tau\theta\tau^{-1} \in \mathrm{AGL}_1(\mathbb{F}_p)$. Since $\#\,\mathrm{AGL}_1(\mathbb{F}_p) = p(p-1)$ and $\langle\theta\rangle = \mathbb{F}_p$ is normal in $\mathrm{AGL}_1(\mathbb{F}_p)$, by Sylow theory $\langle\theta\rangle$ is the unique subgroup of $\mathrm{AGL}_1(\mathbb{F}_p)$ of order p. Thus $\tau\theta\tau^{-1} \in \langle\theta\rangle$, so τ lies in the normalizer of $\langle\theta\rangle$, which by part a) is $\mathrm{AGL}_1(\mathbb{F}_p)$. □

Lemma 9.32. *Let H be a finite index normal subgroup of a group G, and let $g \in G$ be an element of finite order n. If n and $[G : N]$ are coprime, then $g \in N$.*

Proof. Let $q : G \to G/N$ be the quotient map. Then $e = q(g^n) = q(g)^n$, but also by Lagrange's Theorem we have $q(g)^{\#G/N} = q(g)^{[G:N]}$. Since there are $a, b \in \mathbb{Z}$ such that $an + b[G : N] = 1$, it follows that $q(g) = 1$: that is, $g \in N$. □

Let $G \subseteq S_n$ be a transitive subgroup. We say that G is a **Frobenius permutation group** if no nonidentity element of G fixes more than one element of $\{1, \ldots, n\}$.

We say that G is a **strict Frobenius permutation group** if moreover G is not simply transitive, i.e., some point stabilizer is nontrivial. If G is a finite group acting faithfully on a finite set X, then G determines a subgroup of $S_{\#X}$ up to conjugacy. We will say that G is a Frobenius permutation group (resp. a strict Frobenius permutation group) if the associated subgroup of $S_{\#X}$ is a Frobenius permutation group (resp. a strict Frobenius permutation group).

EXERCISE 9.40. *Let G be a finite group.*

a) *We say that G is a **Frobenius group** if for some $n \in \mathbb{Z}^+$ there is an injective group homomorphism $\iota : G \hookrightarrow S_n$ such that the subgroup $\iota(G)$ of S_n is a Frobenius permutation group. Show: every finite group is a Frobenius group.*

b) *We say that G is a **strict Frobenius group** if for some $n \in \mathbb{Z}^+$ there is an injective group homomorphism $\iota : G \hookrightarrow S_n$ such that the subgroup $\iota(G)$ of S_n is a strict Frobenius permutation group. Show: G is a strict Frobenius group if and only if there is a nontrivial, proper subgroup H of G such that for all $g \in G \setminus H$ we have that $H \cap gHg^{-1} = \{e\}$.*
(Hint: consider the action of G on the set G/H of left H-cosets.)

LEMMA 9.33. *Let $(R, \mathfrak{m})$ be a finite local commutative ring.*

a) *The group $\mathrm{AGL}_1(R)$ acts faithfully and transitively on the finite set R.*

b) *The following are equivalent:*
   (i) *R is a field.*
   (ii) *The group $\mathrm{AGL}_1(R)$ is a Frobenius permutation group.*

PROOF. a) The action of $\mathrm{AGL}_1(R)$ on R is faithful by definition, and the subgroup $(R, +)$ of $\mathrm{AGL}_1(R)$ acts simply transitively on R, so the larger group $\mathrm{AGL}_1(R)$ acts transitively.
b) (i) $\implies$ (ii) Suppose $R = \mathbb{F}_q$ is a finite field, and let $g = ax + b \in \mathrm{AGL}_1(R)$ with $a \in \mathbb{F}_q^\times$ and $b \in \mathbb{F}_q$. Suppose there are distinct elements $x \neq y$ of $\mathbb{F}_q$ such that $g(x) = x$ and $g(y) = y$. Then

$$ax + b = g(x) = x \text{and } ay + b = g(y) = y,$$

so

$$(1 - a)x = b = (1 - a)y.$$

If $1 - a \neq 0$ in the field $\mathbb{F}_q$, then dividing by it would yield $x = y$, a contradiction. So $1 - a = 0$, i.e., $a = 1$. Then $x = ax + b = x + b$, so $b = 0$. It follows that g is the identity element of $\mathrm{AGL}_1(\mathbb{F}_q)$.
(ii) $\implies$ (i): We go by contraposition: suppose that R is not a field; equivalently, the maximal ideal $\mathfrak{m}$ of R is nonzero. Let $x \in \mathfrak{m}$ be a nonzero element. Like every nonunit element of a finite commutative ring, x is a zero-divisor: there is a nonzero element y of R such that $xy = 0$. Since R is local, we have $1 + x \in R^\times \subseteq \mathrm{AGL}_1(R)$. Then $1 + x$ fixes 0 (clearly) and also y: $(1 + x)y = y + xy = y$. □

EXERCISE 9.41.

a) *Let R be a commutative ring. Show: the action of $\mathrm{AGL}_1(R)$ on R is simply transitive if and only if the unit group $R^\times$ is trivial.*

b) *Show: for all prime powers $q > 2$, $\mathrm{AGL}_1(\mathbb{F}_q)$ is a strict Frobenius permutation group, while $\mathrm{AGL}_1(\mathbb{F}_2)$ is not.*

EXERCISE 9.42. *Let R be a finite ring that is* not *a field. Show that the following are equivalent:*

(i) $\mathrm{AGL}_1(R)$ *is a Frobenius permutation group.*
(ii) R *is isomorphic to* $\prod_{i=1}^r \mathbb{F}_2$ *for some* $r \in \mathbb{N}$.

THEOREM 9.34 (Galois). *Let F be a field, let $f \in F[t]$ be irreducible and separable of prime degree p, with Galois group G. The following are equivalent:*

(i) *The group G is solvable.*
(ii) *For every pair α, β of distinct roots of F, the splitting field of f is $F(\alpha, \beta)$.*
(iii) *For some pair α, β of distinct roots of F, the splitting field of f is $F(\alpha, \beta)$.*
(iv) *G is conjugate to a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p)$.*

PROOF. (i) $\implies$ (iv): Since f is irreducible, the permutation group $G \subseteq S_p$ is transitive, so applying the Orbit-Stabilizer Theorem and then Cauchy's Theorem we get that G has an element of order p, which in S_p must be a p-cycle. Adjusting G within its conjugacy class we may assume that $\theta = (12\dots p) \in G$. Because G is solvable, we have a tower of subgroups

$$\{e\} = G_0 \subsetneq G_1 \subsetneq \dots \subsetneq G_n = G$$

such that for all $0 \leq i \leq n-1$, the index $[G_{i+1} : G_]$ is a prime number. Let $i \geq 1$ be minimal such that $\theta \in G_i$. Let ℓ be the prime number such that $[G_i : G_{i-1}] = \ell$. By Lemma 9.32, we must have $\ell = p$. Next we claim that $i = 1$: assume not. Then G_{i-1} is nontrivial, so there is $\tau \in G_{i-1}$ and $j \neq k \in F_p$ such that $\tau(j) = k$. Then the element $\rho := \tau\theta^{j-k}$ of G_i fixes k, so ρ is a product of cycles of length less than p, hence (since p is prime) the order of ρ is prime to p. Applying Lemma 9.32 again we find that $\rho \in G_{i-1}$, hence $\theta^{j-k} \in G_{i-1}$, hence (again, since θ has prime order p) $\theta \in G_{i-1}$, a contradiction.

Thus we have $G_1 = \langle\theta\rangle \subseteq \mathrm{AGL}_1(\mathbb{F}_p)$. Let $1 \leq j \leq n$ be maximal such that $G_j \subseteq \mathrm{AGL}_1(\mathbb{F}_p)$. Seeking a contradiction, we suppose that $j < n$. Let $\tau \in G_{j+1}$. Then $\tau\theta\tau^{-1} \in \mathrm{AGL}_1(\mathbb{F}_p) \subseteq G_j$, so Lemma 9.32 gives $\tau \in \mathrm{AGL}_1(\mathbb{F}_p)$. It follows that $\mathrm{AGL}_1(\mathbb{F}_p) \subseteq G_{j+1}$: contradiction. Thus $G_n = G \subseteq \mathrm{AGL}_1(\mathbb{F}_p)$, as desired.
(iv) $\implies$ (i): By assumption, G is isomorphic to a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p)$, which by Exercise 9.39e) is solvable, hence G is solvable.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (iv): Again, because G is a transitive subgroup of S_p, after conjugating G we may assume that $\theta \in G$. Since f, is irreducible, we have $[F(\alpha) : F] = \deg f = p$. Let g be the minimal polynomial of β over $F(\alpha)$, and let $m := \deg(g)$. Since $g \mid \frac{f}{t-\alpha}$, we have $m \leq p-1$. Thus

$$[F(\alpha, \beta) : F] = pm.$$

It follows that $\langle\theta\rangle$ is a Sylow p-subgroup of G. By Sylow Theory, the number n_p of Sylow p-subgroups of G satisfies $n_p \mid m$ and $n_p \equiv 1 \pmod p$; since $m < p$, it follows that $n_p = 1$, hence $\langle\theta\rangle$ is normal in G. Lemma 9.31a) gives $G \subseteq \mathrm{AGL}_1(\mathbb{F}_p)$.
(iv) $\implies$ (ii): We may assume that G is a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p)$. Let K be the splitting field of f, and let $\alpha \neq \beta$ be any distinct roots of f in K. We want to show $K = F(\alpha, \beta)$; by the Galois Correspondence, this holds if and only if: for all $\sigma \in G = \mathrm{Aut}(K/F)$, if σ fixes both α and β, then $\sigma = e$. In other words, $K = F(\alpha, \beta)$ if and only if $G \subseteq S_p$ is a Frobenius permutation group. But G is a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p)$, which is a Frobenius permutation group by Lemma

9.33, and every transitive subgroup of a Frobenius permutation group is itself a Frobenius permutation group. □

8. Primitive and Imprimitive Permutation Groups

Let G be a group acting faithfully on a nonempty set X. Then G also naturally acts on the set 2^X of all subsets of X: for $g \in G$ and $Y \subseteq X$, we put $gY \coloneqq \{gy \mid y \in Y\}$.[4] So also G acts on the set 2^{2^X} of families of subsets of X. A **partition** of X is an element $\mathcal{P} \in 2^{2^X}$ such that $\varnothing \notin \mathcal{P}$, the union of the elements of $\mathcal{P}$ is X and the elements of $\mathcal{P}$ are pairwise disjoint. We say that $\mathcal{P}$ is **uniform** if for all $Y_1, Y_2 \in \mathcal{P}$ we have $\#Y_1 = \#Y_2$. If $g \in G$ and $\mathcal{P}$ is a partition of X, then also $g\mathcal{P}$ is a partition of X, so G acts on the set $\mathcal{P}(X)$ of partitions of X. For $g \in G$ and $\mathcal{P} \in \mathcal{P}(X)$, we say that **g fixes $\mathcal{P}$ pointwise** if for all $Y \in \mathcal{P}$ we have $gY = Y$. We say that **g stabilizes** $\mathcal{P}$ if $g\mathcal{P} = \mathcal{P}$, or in other words, if g permutes the elements of $\mathcal{P}$. We let $\mathrm{Fix}_{\mathcal{P}}$ be the set of elements of g that fix $\mathcal{P}$ pointwise and we let $\mathrm{Stab}_{\mathcal{P}}$ be the set of elements of g that stabilize $\mathcal{P}$. For a set Y, we let $\mathrm{Sym}(Y)$ be the set of bijections from Y to Y, which is a group under composition. The elements of $\mathrm{Stab}_{\mathcal{P}}$ act on the set $\mathcal{P}$, giving a homomorphism

$$\rho : \mathrm{Stab}_{\mathcal{P}} \to \mathrm{Sym}_{\mathcal{P}} .$$

The kernel of ρ is $\mathrm{Fix}_{\mathcal{P}}$, so $\mathrm{Fix}_{\mathcal{P}}$ is a normal subgroup of $\mathrm{Stab}_{\mathcal{P}}$. The map ρ is surjective if and only if $\mathcal{P}$ is uniform. It will shortly become clear why this is the case of interest to us.

Given a bijection $\varphi : X \to X'$, we can "transport" the G-action to X': for $x' \in X'$ and $g \in G$, we put

$$gx' \coloneqq \varphi(g\varphi^{-1}(x)).$$

For a uniform partition $\mathcal{P}$ of X, there is a set

$$X' \coloneqq X_1 \times \mathcal{P}$$

and a bijection

$$\varphi : X \to X'$$

such that for all $Y \in \mathcal{P}$ we have $\varphi(Y) = X_1 \times \{Y\}$. We may therefore view G as a subgroup of $\mathrm{Sym}_{X'}$. The elements of $\mathrm{Fix}_{\mathcal{P}} \subseteq G$ are the elements of $\mathrm{Sym}_{X'}$ that stabilize each "horizontal line" $X_1 \times \{Y\}$, giving an isomorphism from $\mathrm{Fix}_{\mathcal{P}}$ to $\mathrm{Sym}_{X_1}^{\mathcal{P}}$, and the elements of $\mathrm{Stab}_{\mathcal{P}} \subseteq G$ are the elements of $\mathrm{Sym}_{X'}$ that map each horizontal line $X_1 \times \{Y_1\}$ to a horizontal line $X_1 \times \{Y_2\}$. We may also view $\mathrm{Sym}_{\mathcal{P}}$ as a subgroup of $\mathrm{Sym}_{X'}$: for $\sigma \in \mathrm{Sym}_{\mathcal{P}}$, σ acts on the element (x', Y) of X' by $(x', \sigma(Y))$. These elements map horizontal lines to horizontal lines, so we may view $\mathrm{Sym}_{\mathcal{P}}$ as a subgroup of $\mathrm{Stab}_{\mathcal{P}}$.

Proposition 9.35. *With notation as above, we have*

$$\mathrm{Stab}_{\mathcal{P}} = \mathrm{Fix}_{\mathcal{P}} \rtimes \mathrm{Sym}_{\mathcal{P}} \cong \mathrm{Sym}_{X_1}^{\mathcal{P}} \rtimes \mathrm{Sym}_{\mathcal{P}} .$$

Proof. First proof: We have already seen that $\mathrm{Fix}_{\mathcal{P}}$ is normal in $\mathrm{Stab}_{\mathcal{P}}$, so it suffices to show that the subgroups $\mathrm{Fix}_{\mathcal{P}}$ and $\mathrm{Sym}_{\mathcal{P}}$ of $\mathrm{Stab}_{\mathcal{P}}$ are disjoint and generate $\mathrm{Stab}_{\mathcal{P}}$. Any element $g \in \mathrm{Fix}_{\mathcal{P}} \cap \mathrm{Sym}_{\mathcal{P}}$ acts on any element (x_1, Y) of X' by fixing both the first and second coordinates, so $g = e$. If $g \in \mathrm{Stab}_{\mathcal{P}}$, then g

[4] This action appears, for instance, in one of the standard proofs of the Sylow Theorems.

induces a bijection on $\mathcal{P}$, hence an element $h \in \mathrm{Sym}_{\mathcal{P}}$. Then $h^{-1}g \in \mathrm{Fix}_{\mathcal{P}}$.

Second proof: we have a short exact sequence of groups

$$1 \to \mathrm{Fix}_{\mathcal{P}} \to \mathrm{Stab}_{\mathcal{P}} \xrightarrow{\rho} \mathrm{Sym}_{\mathcal{P}} \to 1,$$

so we must show that this sequence splits, i.e., that the map ρ has a **section** $\iota : \mathrm{Sym}_{\mathcal{P}} \to \mathrm{Stab}_{\mathcal{P}}$ – a homomorphism such that $\rho \circ \iota = 1_{\mathrm{Sym}_{\mathcal{P}}}$. But the whole point of replacing X with the Cartesian product $X' \times \mathcal{P}$ is that this gives a canonical section, the one $\sigma(x', Y) = (x', \sigma(Y))$ defined above. □

Let $\mathcal{P}$ be a uniform partition on $\{1, \ldots, n\}$: thus there are $n_1, n_2 \in \mathbb{Z}^+$ with $n_1 n_2 = n$ such that each $Y \in \mathcal{P}$ has size n_1 and there are n_2 elements of $\mathcal{P}$. As above, we choose a bijection $\{1, \ldots, n\} \to \{1, \ldots, n_1\} \times \{1, \ldots, n_2\}$. This identifies the subgroup $\mathrm{Stab}_{\mathcal{P}}$ of S_n with

$$S_1^{n_2} \rtimes S_{n_2},$$

where the action of S_{n_2} on $S_1^{n_2}$ is by permuting the factors in the product. By definition, this subgroup of $S_{n_1 n_2}$ is the **wreath product**

$$S_{n_1} \wr S_{n_2}.$$

Slightly more generally, if G_1 is a subgroup of S_{n_1} and G_2 is a subgroup of S_{n_2}, then $G_1^{n_2} \rtimes G_2$ is a subgroup of $S_1^{n_2} \rtimes S_{n_2}$ that we denote by

$$G_1 \wr G_2.$$

Having come this far, for any group G_1, a set $\mathcal{P}$, and a subgroup G_2 of $\mathrm{Sym}_{\mathcal{P}}$, we have a natural action of G_2 on $G_1^{\mathcal{P}}$ so can define

$$G_1 \wr G_2 := G_1^{\mathcal{P}} \rtimes G_2.$$

We have

$$\#(G_1 \wr G_2) = (\#G_1)^{\#\mathcal{P}} \times \#G_2,$$

so in particular

$$\#(S_{n_1} \wr S_{n_2}) = (n_1!)^{n_2} \cdot n_2!$$

A partition $\mathcal{P}$ of $\{1, \ldots, n\}$ is called **trivial** if $\#\mathcal{P} \in \{1, n\}$; otherwise it is called **nontrivial**. Nontrivial partitions exist if and only $n \geq 3$.

EXERCISE 9.43. *Let $\mathcal{P}$ be a partition of $\{1, \ldots, n\}$. Show:* $\mathrm{Stab}_{\mathcal{P}}$ *is a proper subgroup of S_n if and only if $\mathcal{P}$ is nontrivial.*

EXERCISE 9.44. *Let $\mathcal{P}$ be a partition of $\{1, \ldots, n\}$. Show:* $\mathrm{Stab}_{\mathcal{P}}$ *is a transitive subgroup of S_n if and only if $\mathcal{P}$ is uniform.*

EXERCISE 9.45. *Let $n \in \mathbb{Z}^+$, and let $\mathcal{P}_1$ and $\mathcal{P}_2$ be uniform partitions of $\{1, \ldots, n\}$. Show: $\mathcal{P}_1$ and $\mathcal{P}_2$ are conjugate under the action of S_n if and only if $\#\mathcal{P}_1 = \#\mathcal{P}_2$.*

EXERCISE 9.46. *Let $n \in \mathbb{Z}^{\geq 3}$.*

a) *Let G be a subgroup of S_n. Show: G is transitive if and only if it is* not *contained in* $\mathrm{Fix}_{\mathcal{P}}$ *for any nontrivial partition $\mathcal{P}$ of $\{1, \ldots, n\}$.*

b) *Let G be a transitive subgroup of S_n, and let $\mathcal{P}$ be a partition of $\{1, \ldots, n\}$ such that $G \subseteq \mathrm{Stab}_{\mathcal{P}}$. Show: the action of G on $\mathcal{P}$ is transitive. Deduce: $\mathcal{P}$ is uniform.*

A subgroup G of S_n is called **imprimitive** if it is a subgroup of $\mathrm{Stab}_{\mathcal{P}}$ for some nontrivial partition of $\mathcal{P}$; otherwise it is called **primitive**.

EXERCISE 9.47. *Let $G \subseteq S_n$ be a permutation group. A **block** is a subset B of S_n such that for all $g \in G$, we have $g(B) = B$ or $g(B) \cap B = \varnothing$. We say a block B is **nontrivial** if $1 < \#B < n$.*

a) *Show: nontrivial blocks exist if and only if G is imprimitive.*
b) *Deduce: primitive permutation groups are transitive.*

If p is prime, then every uniform partition of $\{1, \ldots, n\}$ is trivial, so every subgroup of S_p is primitive.

For a permutation group $G \subseteq S_n$, a **block** is a nonempty subset B of $\{1, \ldots, n\}$ such that for all $g \in G$, if we have $g(B) = B$ or $g(B) \cap B = \varnothing$. Every subset of $\{1, \ldots, n\}$ of cardinality 1 or n is a block for G; we call these blocks **trivial** and other blocks **nontrivial**. Now assume that G is moreover transitive; then the G-orbit $\mathcal{P}_B \coloneqq \{\sigma B \mid \sigma \in G\}$ of a block B is a uniform partition of $\{1, \ldots, n\}$ that is nontrivial if and only if B is nontrivial. Clearly we have $G \subseteq \mathrm{Stab}_{\mathcal{P}_B}$, so if G has a nontrivial block then it is imprimitive. Conversely, every element of a partition stabilized by G is a block for G, so if G is nontrivial then it admits a nontrivial block.

Here is another take on primitive versus imprimitive transitive permutation groups. Let G be a transitive subgroup of $\{1, \ldots, n\}$, and for $1 \leq i \leq n$, let G_i be the stabilizer of $\{i\}$. Then the Orbit-Stabilizer Theorem gives an isomorphism of G-sets from $\{1, \ldots, n\}$ to the coset space G/G_i. The groups $G_1, \ldots, G_n$ form a full conjugacy class of subgroups and the faithfulnes of the action is equivalent to $\bigcap_{i=1}^n G_i = \{e\}$, meaning that each G_i is **corefree**: the largest normal subgroup of G_i is $\{e\}$.

THEOREM 9.36. *Let G be a transitive subgroup of S_n, and for $i \in \{1, \ldots, n\}$ let G_i be the stabilizer of i. The following are equivalent:*

(i) *G is a primitive permutation group.*
(ii) *G_i is a maximal subgroup of G.*

PROOF. Step 1: We claim that there is a natural isotone bijective correspondence between blocks B for G containing i and subgroups of G containing G_i: namely, we map a block B containing i to the subgroup Stab_B, and we map a subgroup H containing G_i to the block $B_H \coloneqq \{hi \mid h \in H\}$. Here is a detailed proof:
• Let $B \subseteq \{1, \ldots, n\}$ be a block for G that contains i, and let $\mathcal{P} = \mathcal{P}_B$ be the corresponding partition stabilized by G. Then $G_i \subseteq \mathrm{Stab}_B$: indeed, let $g \in G_i \subseteq G \subseteq \mathrm{Stab}_{\mathcal{P}}$. Then g stabilizes the partition of which B is an element and carries the element i of B to itself, hence $g(B) = B$. If we have blocks $i \in B_1 \subseteq B_2$ and $g \in G$ such that $g(B_1) = B_1$, then $g(i) \in B_1 \subseteq B_2$, so $g(B_2) = B_2$.
• Let H be a subgroup of G containing G_i, and consider

$$B_H \coloneqq \{hi \mid h \in H\}.$$

Clearly $i \in B_H$; we claim that B_H is a block for G. Indeed, let $\sigma \in G$, and suppose that $B \cap \sigma(B) \neq \varnothing$. Then there are $h_1, h_2 \in H$ such that $h_1 i = \sigma h_2 i$, so $h_1^{-1} \sigma h_2 \in G_i \subseteq H$, so $\sigma \in H$. Since B is H-invariant, it follows that $\sigma(B) = B$. It is immediate that if $G_i \subseteq H_1 \subseteq H_2$ then $B_{H_1} \subseteq B_{H_2}$.
For a block B containing i, we have that B_{Stab_B} consists of elements hi for $h \in \mathrm{Stab}_B$, hence $hi \in B$, and thus $B_{\mathrm{Stab}_B} \subseteq B$. We know that $i \in B_{\mathrm{Stab}_B}$; for

$j \in B \setminus \{i\}$, by transitivity of G there is $g \in G$ such that $gi = j$. Because g stabilizes the partition $\mathcal{P}_B$ and maps the element i of B to the element j of B, we must have $g(B) = B$, so $g \in \mathrm{Stab}_B$ and $j \in B_{\mathrm{Stab}_B}$. This shows $B_{\mathrm{Stab}_B} = B$.
Let H be a subgroup of G containing G_i. Since B_H is H-invariant, we have $H \subseteq \mathrm{Stab}_{B_H}$. Conversely, let $g \in \mathrm{Stab}_{B_H}$. Then there is $h \in H$ such that $gi = hi$, since $h^{-1}g \in G_i \subseteq H$, so $g \in H$.
Step 2: G_i is maximal if and only if there are precisely two subgroups of G containing G_i. G is primitive if and only if there are precisely two blocks for G containing i. Thus the equivalence of (i) and (ii) follows from Step 1. □

EXERCISE 9.48. *For $n \geq 3$ let D_n be the dihedral group of order $2n$, viewed as a subgroup of S_n via its action by isometries on the regular n-gon.*

a) *Let $n = n_1 n_2$. Show D_n is conjugate to a subgroup of $S_{n_1} \wr S_{n_2}$ (and thus also a subgroup of $S_{n_2} \wr S_{n_1}$).*
b) *Show: D_n is primitive if and only if n is prime.*

Theorem 9.36 has an important field-theoretic consequence:

COROLLARY 9.37. *Let $n \in \mathbb{Z}^{\geq 2}$, let F be a field, and let $f \in F[t]$ be irreducible and separable, of degree n. We factor f in an algebraic closure $\overline{F}$ as*

$$f = (t - \alpha_1) \cdots (t - \alpha_n).$$

Let G be the Galois group of f and let $K \coloneqq F(\alpha_1)$. The following are equivalent:

(i) *There is no subfield F' with $F \subsetneq F' \subsetneq K$.*
(ii) *The permutation group G is primitive.*

PROOF. Let L be the splitting field of f, so L is the normal closure of K/F and $\mathrm{Aut}(L/F) = G$. The subgroup of elements of G fixing α_1 may be viewed as the point stabilizer G_1 inside G. We have $K = L^{G_1}$, so by the Galois correspondence subextensions F' of K/F are in antitone bijection with subgroups of G containing G_1. By Theorem 9.36, we have that G is primitive if and only if G_1 is maximal, completing the proof. □

EXERCISE 9.49. *Maintain the notation of Corollary 9.37, and suppose moreover that K/F is* not *Galois.*

a) *Suppose that the equivalent conditions of Corollary 9.37 hold. Show: $\mathrm{Aut}(K/F) = \{e\}$.*
b) *Show by example that it is possible for the equivalent conditions of Corollary 9.37* not *to hold – i.e., that there is an intermediate subextension $F \subsetneq F' \subsetneq K$ – and still have $\mathrm{Aut}(K/F) = \{e\}$.*
(Suggestion: try a degree 9 extension $K/\mathbb{Q}$.)

Now we'll see that S_n-extensions and A_n-extensions have no intermediate subfields.

It is clear that S_n itself is a primitive subgroup of S_n: we may assume $n \geq 4$, and if $\mathcal{P}$ is a nontrivial uniform partition of $\{1, \ldots, n\}$, let $B \in \mathcal{P}$. We may choose $i \neq j \in B$ and $\sigma \in S_n$ such that $\sigma(i) = j$ and $\sigma(j) \notin B$. Then $\sigma \notin \mathrm{Stab}_{\mathcal{P}}$. By Theorem 9.36, the point stabilizers in S_n are maximal subgroups of S_n. We can see this directly: since point stabilizers are conjugate, it suffices to show that the stabilizer G_n of n is maximal. Let H be a subgroup of S_n properly containing G_n, and let $\sigma \in H \setminus G_n$. The orbits of G_n on $\{1, \ldots, n\}$ are $\{1, \ldots, n-1\}$ and $\{n\}$, but

σ maps n to some element of $\{1, \ldots, n-1\}$, so H acts transitively on $\{1, \ldots, n\}$. By Orbit-Stabilizer, $\#H = n \cdot (n-1)! = \#S_n$, so $H = S_n$.

EXERCISE 9.50. *Let $n \in \mathbb{Z}^{\geq 3}$.*

a) *Let $G \subseteq S_n$ be a simple, transitive subgroup. Show: G is primitive.*
b) *Deduce: if $n \geq 5$, the alternating group A_n is primitive.*
c) *Show: A_3 and A_4 are primitive.*
d) *Let F be a field, and let $f \in F[t]$ be irreducible separable of degree n with Galois group A_n. Let α be a root of f in an algebraic closure. Show: there is no field F' with $F \subsetneq F' \subseteq F(\alpha)$.*

Corollary 9.37 makes a fundamental connection between the Galois closure of a finite degree field separable extension K/F admitting a nontrivial proper subextension and wreath products. This seems underdeveloped in the literature. A very recent work of Barquero-Sanchez–Calvo-Monge makes this connection much more explicitly: see [**BSCM25**, Thm. 1.1]. We do not treat these results here.

EXAMPLE 9.38. *Up to S_4-conjugacy, the unique nontrivial uniform partition of $\{1,2,3,4\}$ is*

$$\mathcal{P} = \{\{1,2\},\{3,4\}\},$$

so every element of $\mathcal{P}$ has size $n_1 = 2$ and there are $n_2 = 2$ elements of $\mathcal{P}$. It follows from the above that $\mathrm{Stab}_{\mathcal{P}} \cong S_2 \wr S_2$ has size $2^2 \cdot 2 = 8$ and its normal subgroup $\mathrm{Fix}_{\mathcal{P}}$ has index 2 in $\mathrm{Stab}_{\mathcal{P}}$ hence size 4. Explicitly, we have

$$\mathrm{Fix}_{\mathcal{P}} = \{e, (12), (34), (12)(34)\}$$

is isomorphic but not conjugate to the Klein group V_4 in S_4.

In Example 9.4 we observed that there are 3 order 8 subgroups $D_{4,1}, D_{4,2}, D_{4,3}$ of S_4, all dihedral groups, forming a single conjugacy class. We did not mention it at the time, but all three subgroups contain $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$. Indeed we can see that every element of V_4 stabilizes $\mathcal{P}$. In particular, if choose the bijection $\{1,2,3,4\} \to \{1,2\} \times \{1,2\}$

$$1 \mapsto (1,1),\ 2 \mapsto (2,1),\ 3 \mapsto (1,2),\ 4 \mapsto (2,2),$$

then the element $(13)(24)$ corresponds to the nontrivial element of S_2 under the section $\iota : S_2 \hookrightarrow S_2 \wr S_2$ constructed above. We may think of a chest with two drawers, and each drawer having two slots, labelled 1 and 2, with a ball in each slot. Then the element $(13)(24)$ corresponds to swapping the two drawers, without disturbing the positions of the balls in each drawer.

For our choice of $\mathcal{P}$, we have

$$\mathrm{Stab}_{\mathcal{P}} = D_{4,2} = \langle (1324), (12) \rangle.$$

The other two groups $D_{4,1}$ and $D_{4,3}$ are the stabilizer groups of the other two nontivial uniform partitions of $\{1,2,3,4\}$.

It follows from Example 9.38 that $V_4 \subseteq S_4$ is imprimitive. The following exercise generalizes this to finite commutative subgroups of S_n for composite n.

EXERCISE 9.51. *Let $n \in \mathbb{Z}^{\geq 2}$, and let $G \subseteq S_n$ be a subgroup.*

a) *Suppose G is commutative and transitive. Show: G is simply transitive. (Hint: the point stabilizers are conjugate, but G is commutative.)*
b) *Show: every group of order n occurs as a simply transitive subgroup of S_n, uniquely up to conjugacy.*

c) *Suppose G is simply transitive and primitive. Show: n is prime. (Hint: if n is composite, then G has a nontrivial proper subgroup.)*
d) *Conclude: if G is commutative and primitive, then n is prime.*

EXERCISE 9.52. *Let G_1 be a finite group, and let $G_2 \subseteq S_n$. Show: the wreath product $G_1 \wr G_2$ is solvable if and only if G_1 and G_2 are both solvable.*

EXERCISE 9.53. *Let $n \in \mathbb{Z}^{\geq 2}$. Show: the following are equivalent:*
(i) *Every imprimitive subgroup of S_n is solvable.*
(ii) *n is a prime number, or $n \in \{4, 6, 8, 9\}$.*

9. Solvability in Degree p^2

EXERCISE 9.54. *Let p be a prime number, and let C_p be a cyclic subgroup of S_p (it is unique up to conjugacy). Show: $C_p \wr C_p$ is a Sylow p-subgroup of S_{p^2}.*

EXAMPLE 9.39. *As we know, the transitive subgroups of S_4 are A_4, S_4, V_4 and (conjugate to) C_4 or D_4. Which of these subgroups are primitive? In fact we already know: clearly S_4 is primitive; by Exercise 9.50 A_4 is primitive; by Exercise 9.51 the commutative groups V_4 and C_4 are imprimitive, while by Exericse 9.48, the group D_4 is primitive. In our work on Galois groups of quartics, we saw that V_4 and C_4 are (up to conjugacy, in the case of C_4) contained in D_4. As subgroups of S_4 we have that D_4, $S_2 \wr S_2$ and $\mathrm{AGL}_1(\mathbb{F}_2) \wr \mathrm{AGL}_1(\mathbb{F}_2)$ are all conjugate subgroups. Since every subgroup of S_4 is solvable, this is the $p = 2$ case of the following result.*

THEOREM 9.40. *Let p be a prime number, and let $G \subseteq S_{p^2}$ be transitive and imprimitive. The following are equivalent:*
(i) *G is solvable.*
(ii) *G conjugate to a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p) \wr \mathrm{AGL}_1(\mathbb{F}_p)$.*

PROOF. (i) $\implies$ (ii) Let G be a transitive, imprimitive, solvable subgroup of S_{p^2}. Since the only nontrivial factorization of p^2 is $p^2 = p \cdot p$, it follows that G is conjugate to a subgroup of $S_p \wr S_p$. Let $q : S_p \wr S_p \to S_p$ be the quotient by the normal subgroup S_p^p, and put $G' := q(G)$. Then G' is also transitive: indeed there is a uniform partition $\mathcal{P} = \{Y_1, \ldots, Y_p\}$ of $\{1, \ldots, p^2\}$ with $\#\mathcal{P} = p$ such that $G \subseteq \mathrm{Fix}_{\mathcal{P}}$, and because G is transitive it must transitively permute the elements of $\mathcal{P}$. Being a quotient of the solvable group G, the group $G' \subseteq S_p$ is also solvable, so by Theorem 9.34 we find that up to conjugacy G' is a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p)$, which means that there is an element γ of $\iota(S_p)$ such that

$$\gamma G \gamma^{-1} \subseteq S_p \wr \mathrm{AGL}_1(\mathbb{F}_p). \tag{35}$$

For $1 \leq i \leq p$, let $G_i := \{g \in G \mid g(Y_i) = Y_i\}$. Thus G_i acts on Y_i, which has size p, giving a group homomorphism $\rho_i : G_i \to S_p$ (well-defined up to conjugacy); we put $G_i' := \rho_i(G)$. Again G_i' is solvable, and again the transitivity of G implies the transitivity of G_i': indeed, write the elements of Y_i as $y_{i,1}, \ldots, y_{i,p}$, and let $1 \leq j_1 \neq j_2 \leq p$. Since G is transitive, there is $g \in G$ such that $g y_{i,j_1} = y_{i,j_2}$. Because g preserves the partition $\mathcal{P}$, it maps every element of Y_i to some element $Y_{i'}$ of $\mathcal{P}$. But also it maps the element y_{i,j_1} of Y_i to an element Y_{i,j_2} of Y_i, so it must be that $g(Y_i) = Y_i$: that is, $g \in G_i$. By Theorem 9.34 (and its proof), there is $\delta_i \in S_p$ such that

$$\theta := (12 \cdots p) \in \delta_i G_i' \delta_i^{-1} \subseteq \mathrm{AGL}_1(\mathbb{F}_p).$$

Then the element $\delta := (\delta_1, \ldots, \delta_p) \in S_p^p$ has the property that after conjugating G by δ, we have

$$\forall 1 \leq i \leq p, \theta \in G_i' \subseteq \mathrm{AGL}_1(\mathbb{F}_p). \tag{36}$$

Because $\rho(\delta) = e$, after this conjugation we still have $G \subseteq S_p \wr \mathrm{AGL}_1(\mathbb{F}_p) = S_p^p \rtimes \mathrm{AGL}_1(\mathbb{F}_p)$. For $g \in G$, we may write $g = (\mu_1, \ldots, \mu_p)\tau$ with each $\mu_i \in S_p$ and $\tau \in \mathrm{AGL}_1(\mathbb{F}_p)$. Let $1 \leq j \leq p$. Applying (36) with $i := \tau(j)$, we find $h = (\nu_1, \ldots, \nu_p)\rho \in G$ with $\rho(i) = i$ and $\nu_i = \theta$. Now put

$$\gamma := g^{-1}hg.$$

We claim that

$$\gamma = (\lambda_1, \ldots, \lambda_p)\tau^{-1}\rho\tau. \tag{37}$$

for $\lambda_1, \ldots, \lambda_p \in S_p$ such that $\lambda_j = \mu_j^{-1}\theta\mu_j$. You are asked to confirm this in Exercise 9.55. Since $(\tau^{-1}\rho\tau)(j) = \tau^{-1}\rho(i) = \tau^{-1}(i) = j$, we have that $\gamma \in G_j$, so

$$\mu_j^{-1}\theta\mu_j = \lambda_j \in G_j' \subseteq \mathrm{AGL}_1(\mathbb{F}_p).$$

Lemma 9.31b) implies that $\mu_j \in \mathrm{AGL}_1(\mathbb{F}_p)$. Since this holds for all $1 \leq j \leq p$, it follows that $g \in \mathrm{AGL}_1(\mathbb{F}_p) \wr \mathrm{AGL}_1(\mathbb{F}_p)$, as desired.
(ii) $\implies$ (i): The group $\mathrm{AGL}_1(\mathbb{F}_p) = \mathbb{F}_p \rtimes \mathbb{F}_p^\times$ is a semi-direct product of finite commutative groups, hence is solvable. Exercise 9.52 implies that $\mathrm{AGL}_1(\mathbb{F}_p) \wr \mathrm{AGL}_1(\mathbb{F}_p)$ is solvable, hence G, being isomorphic to a subgroup of $\mathrm{AGL}_1(\mathbb{F}_p) \wr \mathrm{AGL}_1(\mathbb{F}_p)$, is also solvable. □

EXERCISE 9.55. *Let H, N be groups, and let $\varphi : H \to \mathrm{Aut}\, N$ be a group homomorphism, and put*

$$G := N \rtimes H.$$

Recall that elements of G may be viewed as ordered pairs (n, h) with $n \in N$ and $h \in H$, with a group law that is "twisted by φ:

$$\forall (n_1, h_1), (n_2, h_2) \in G,\ (n_1, h_1) \cdot (n_2, h_2) := (n_1\varphi_{h_1}(n_2), h_1h_2)$$

and

$$\forall (n, h) \in G,\ (n, h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1}).$$

a) *Let G_1 be a group, let $n \in \mathbb{Z}^+$, and let G_2 be a subgroup of S_n. The wreath product $G_1 \wr G_2$ is the semidirect product $G_1^n \rtimes G_2$, where $\varphi : G_2 \to G_1^n$ acts by permuting the factors. We write the elements of $G_1 \wr G_2$ as $\sigma = (g_1, \ldots, g_n; \tau)$ with $g_i \in G_1$ and $\tau \in G_2$. Show:*

$$\sigma^{-1} = (g_{\tau^{-1}(1)}, \ldots, g_{\tau^{-1}(n)}; \tau^{-1}).$$

Let $\sigma' = (g_1', \ldots, g_n'; \tau')$ be another element of $G_1 \wr G_2$. Show:

$$\sigma\sigma' = (g_{\tau'(1)}g_1', \ldots, g_{\tau'(n)}g_n'; \tau\tau').$$

b) *Prove (37).*

10. Galois's Theorem on Solvable Permutation Groups

If a group G acts on nonempty sets $X_1, \ldots, X_k$, then it also acts "diagonally" on the Cartesian product $\mathcal{X} := \prod_{i=1}^k X_i$ by

$$g \cdot (x_1, \ldots, x_k) := (gx_1, \ldots, gx_k).$$

If G acts faithfully on X_i for all $1 \leq i \leq k$, then G acts effectively on $\mathcal{X}$.[5] If G acts transitively on $\mathcal{X}$, then G acts transitively on X_i for all $1 \leq i \leq k$. However, the converse need not hold. In particular, suppose that for a G-action on a set X, we take $X_i := X$ for all $1 \leq i \leq k$. Then, if k and $\#X$ are at least 2, then G never asks transitively on $\mathcal{X} = X^k$: the diagonal $\Delta := \{(x, \ldots, x) \in X^K \mid x \in X\}$ is a proper, nonempty G-stable subset. Another G-stable subset of X^k is the set

$$\mathcal{P}_k(X) := \{(x_1, \ldots, x_k) \mid x_1, \ldots, x_k \text{ are all distinct}\}.$$

We observe that $\mathcal{P}_k(X)$ is nonempty if and only if $k \leq \#X$. When this holds, we say that the G-action on X is **k-transitive** if the G-action on $\mathcal{P}_k(X)$ is transitive. Thus 1-transitive is the same as transitive; instead of 2-transitive we will say **doubly transitive**. We say that the G-action on X is **simply k-transitive** if the action on $\mathcal{P}_k(X)$ is simply transitive.

This terminology applies in particular to subgroups G of S_n, with their natural action on $\{1, \ldots, n\}$.

EXERCISE 9.56. *Suppose that a group G acts k-transitively on a set X. Show: for all $1 \leq \ell < k$, also G acts ℓ-transitively on X.*

EXAMPLE 9.41. *The natural action of S_n on $\{1, \ldots, n\}$ is n-transitive. Conversely, if a group G acts effectively on a set X of cardinality n and the action is n-transitive, then by Orbit-Stabilizer we have $\#G \geq \#\mathcal{P}_n(X) = n!$, so we must have $G = \operatorname{Sym} X$. It follows that for a permutation group $G \subseteq S_n$, if G is n-transitive, then $G = S_n$. We also have $\#\mathcal{P}_{n-1}(X) = n!$, so an $n-1$ -transitive permutation group $G \subseteq S_n$ must also be S_n.*

We claim that for all $n \geq 3$, the alternating group A_n is $n-2$-transitive. We must show that for any injection $\iota : \{1, \ldots, n-2\} \to \{1, \ldots, n\}$, there is $\sigma \in A_n$ such that $\sigma|_{\{1,\ldots,n-2\}} = \iota$. But there are precisely two elements $\sigma_1, \sigma_2 \in S_n$ that extend ι, and $\sigma_2 = \sigma_1\tau$, where τ is the transposition of the two elements not in the image of ι. Thus precisely one of σ_1 and σ_2 lies in A_n.

EXERCISE 9.57. *Let F be a field. Show: the natural action of $\mathrm{AGL}_1(F)$ on F is simply 2-transitive.*

The following basic result gives an inductive approach to k-transitivity of group actions.

PROPOSITION 9.42. *Let G be a group acting transitively on a set X, and let $k \in \mathbb{Z}$ with $2 \leq k \leq \#X$. Let $x \in X$, and let G_x be the stabilizer of x. The following are equivalent:*

(i) *G acts k-transitively on X.*
(ii) *G_x acts $(k-1)$-transitively on $X \setminus \{x\}$.*

[5]The converse is not true: for the G-action to be effective on X, it is sufficient but not necessary for the G-action on *some* X_i to be effective.

PROOF. (i) $\implies$ (ii): Suppose that G acts k-transitively on X, and let $\mathbf{x}' \coloneqq (\mathbf{x_1}, \ldots, \mathbf{x_{k-1}})$ and $\mathbf{y}' \coloneqq (\mathbf{y_1}, \ldots, \mathbf{y_{k-1}})$ be elements of $\mathcal{P}_{k-1}(X \setminus \{x\})$. Then $\mathbf{x} \coloneqq (\mathbf{x_1}, \ldots, \mathbf{x_{k-1}}, \mathbf{x})$ and $\mathbf{y} \coloneqq (\mathbf{y_1}, \ldots, \mathbf{y_{k-1}}, \mathbf{x})$ are elements of $\mathcal{P}_k(X)$, so by hypothesis there is $g \in G$ such that $g\mathbf{x} = \mathbf{y}$, which implies that $g(x) = x$ – so $g \in G_x$ – and $g\mathbf{x}' = \mathbf{y}'$.
(ii) $\implies$ (i): Suppose that G_x acts $(k-1)$-transitively on $X \setminus \{x\}$, choose distinct elements $x_1, \ldots, x_{k-1}$ of $X \setminus \{x\}$, and put $\mathbf{x} \coloneqq (\mathbf{x_1}, \ldots, \mathbf{x_{k-1}}, \mathbf{x})$. Then for G to act k-transitively on X, it suffices to show that for any $\mathbf{y} \coloneqq (\mathbf{y_1}, \ldots, \mathbf{y_k}) \in \mathcal{P}_{\mathbf{k}}(\mathbf{X})$ there is $g \in G$ such that $g\mathbf{x} = \mathbf{y}$. Since G is transitive, there is $\sigma \in G$ such that $\sigma x = y_k$. Thus $\sigma^{-1} y_k = x$, and since $\mathbf{y} \in \mathcal{P}_{\mathbf{k}}(\mathbf{X})$, it follows that for all $1 \leq i \leq k-1$ we have $\sigma^{-1}(y_i) \neq x$. Our hypothesis now implies that there is $h \in G_x$ such that $h(x_1, \ldots, x_{k-1}) = (\sigma^{-1}y_1, \ldots, \sigma^{-1}y_{k-1})$, and since $\sigma^{-1}y_k = x$, it follows that

$$h\mathbf{x} = (\sigma^{-1}y_1, \ldots, \sigma^{-1}y_{k-1}, x) = \sigma^{-1}\mathbf{y}.$$

Thus $\sigma h \in G$ and $\sigma h \mathbf{x} = \mathbf{y}$. □

For a commutative ring R and $n \in \mathbb{Z}^+$, we define the **affine general linear group** $\mathrm{AGL}_n(R)$ to consist of all bijective functions $f : R^n \to \mathbb{R}^n$ of the form $f_{A,b}(x) \coloneqq Ax + b$, where $A \in \mathrm{GL}_n(R)$ is an invertible R-linear map and $b \in R^n$. Thus $\mathrm{AGL}_n(R)$ acts effectively on R^n. Then $\mathrm{GL}_n(R)$ embeds as a subgroup of $\mathrm{AGL}_n(R)$ via $A \mapsto f_{A,0}$. Similarly, the additive group $(R^n, +)$ of R embeds as a subgroup of $\mathrm{AGL}_n(R)$ via $b \mapsto f_{1,b}$. Clearly $(R^n, +)$ and $\mathrm{GL}_n(R)$ are disjoint subgroups of $\mathrm{AGL}_n(R)$ that generate $\mathrm{AGL}_n(R)$.

EXERCISE 9.58. *Let R be a commutative ring, and let $n \in \mathbb{Z}^+$.*

a) *With notation as above, let $A \in \mathrm{GL}_n(R)$ and $b \in R^n$. Show:*

$$f_{A,0}^{-1} f_{0,b} f_{A,0} = f_{1,A^{-1}(b)}.$$

b) *Deduce:*

$$\mathrm{AGL}_n(R) = (R^n, +) \rtimes \mathrm{GL}_n(R).$$

PROPOSITION 9.43. *Let R be a commutative ring, let $n \in \mathbb{Z}^+$, and let $k \in \mathbb{Z}^{\geq 2}$.*

a) *The following are equivalent:*
   (i) $\mathrm{AGL}_n(R)$ *acts k-transitively on R^n.*
   (ii) $\mathrm{GL}_n(R)$ *acts $(k-1)$-transitively on $R^n \setminus \{0\}$.*

b) *The following are equivalent:*
   (i) $\mathrm{AGL}_n(R)$ *acts doubly transitively on R^n.*
   (ii) *R is a field.*

c) *The following are equivalent:*
   (i) $\mathrm{AGL}_n(R)$ *acts 3-transitively on R^n.*
   (ii) *Either ($n = 1$ and $R \cong \mathbb{F}_3$), or ($n \geq 2$ and $R \cong \mathbb{F}_2$).*

d) *The following are equivalent:*
   (i) $\mathrm{AGL}_n(R)$ *acts 4-transitively on R^n.*
   (ii) *We have $n = 2$ and $R \cong \mathbb{F}_2$.*

PROOF. a) The stabilizer of 0 in $\mathrm{AGL}_n(R)$ is $\mathrm{GL}_n(R)$, so this is immediate from Proposition 9.42a).
b) First suppose that R is a field. Then $\mathrm{GL}_n(R)$ acts simply transitively on the set of ordered R-bases of R^n, and every nonzero vector in R^n is the first element of some ordered R-basis, so $\mathrm{GL}_n(R)$ acts transitively on the set of nonzero vectors in R^n. By part a) this implies that $\mathrm{AGL}_n(R)$ acts doubly transitively on R^n.

Now suppose that R is not a field, so there is a nonzero proper ideal I of R. By part a), our task is to show that $\mathrm{GL}_n(R)$ does not act transitively on the set of nonzero vectors in R^n. The set of vectors in the $\mathrm{GL}_n(R)$-orbit of the first standard basis basis vector $e_1 = (1, 0, \ldots, 0)$ are the set of vectors v that appear as the first column of some matrix $A \in \mathrm{GL}_n(R)$. Because R is not a field, it has a nonzero proper ideal I; let $x \in I \setminus \{0\}$. The vector $(x, \ldots, x)$ is nonzero but cannot appear as the first column of a matrix in $\mathrm{GL}_n(R)$, because any matrix with first column $(x, \ldots, x)$ has determinant divisible by x, hence lying in I, hence not a unit in R. Thus e_1 and $(x, \ldots, x)$ do not lie in the same $\mathrm{GL}_n(R)$-orbit on $R^n \setminus \{0\}$.
c) Suppose $\mathrm{AGL}_n(R)$ acts 3-transitively on R^n. By parts a) and b), R is a field and $\mathrm{GL}_n(R)$ acts 2-transitively on $R^n \setminus \{0\}$. Suppose first that $n = 1$. In this case, to consider double transitivity we need R not to be isomorphic to $\mathbb{F}_2$, because otherwise $R^n \setminus \{0\}$ has only a single element. Assuming this, in this case $\mathrm{GL}_n(R) = R \setminus \{0\}$ acts simply transitively on $R \setminus \{0\}$. When $R \cong \mathbb{F}_3$, then because $R \setminus \{0\}$ has size 2, transitivity and double transitivitiy are equivalent, so the action is indeed doubly transitive. Otherwise $\#R \geq 4$, so we may choose distinct elements α and β in $R \setminus \{0, 1\}$ and then there is no $u \in R^\times$ that maps $(1, \alpha) \in \mathcal{P}_2(R^\times)$ to $(1, \beta) \in \mathcal{P}_\in(R^\times)$ because $u \cdot 1 = 1$ forces $u = 1$, so then $u\alpha \neq \beta$. Now suppose that $n \geq 2$. If R is not isomorphic to $\mathbb{F}_2$, we may choose $\alpha \in R \setminus \{0, 1\}$. Then $(e_1, \alpha e_1)$ and (e_1, e_2) are both elements of $\mathcal{P}_2(R^n \setminus \{0\})$ but there is no $A \in \mathrm{GL}_n(R)$ such that $A(e_1) = e_1$ and $A(\alpha e_1) = e_2$, because if $A(e_1) = e_1$ then $A(\alpha e_1) = \alpha A(e_) = \alpha e_1 \neq e_2$.

We saw above that $\mathrm{AGL}_1(\mathbb{F}_3)$ acts doubly transitively on $\mathbb{F}_3$. Finally, we will show that for all $n \geq 2$, the group $\mathrm{GL}_n(\mathbb{F}_2)$ acts doubly transitively on nonzero elements of $\mathbb{F}_2^n$, which by part a) shows that $\mathrm{AGL}_n(\mathbb{F}_2)$ acts triply transitively on $\mathbb{F}_2^n$, completing the proof. The key observation is that in $\mathbb{F}_2^n$ any two distinct nonzero vectors v_1 and v_2 are $\mathbb{F}_2$-linearly independent, so since $\mathrm{GL}_n(F_2)$ acts simply transitively on ordered bases, it acts doubly transitively on nonzero vectors.
d) By part c), $\mathrm{AGL}_2(\mathbb{F}_2)$ acts 3-transitively on $\mathbb{F}_2^2$, which has size 4, so 3-transitivity and 4-transitivity are equivalent. It does not make sense to speak of 4-transitivity of $\mathrm{AGL}_1(\mathbb{F}_3)$ acting on the three element set $\mathbb{F}_3$, so by parts a) and c) it suffices to show that for all $n \geq 3$ the action of $\mathrm{GL}_n(\mathbb{F}_2)$ on $\mathbb{F}_2^n$ is not 3-transitive. For this, we observe that $(e_1, e_2, e_1 + e_2)$ and (e_1, e_2, e_3) are two elements of $\mathcal{P}_3(\mathbb{F}_2^n \setminus \{0\})$ and if $A \in \mathrm{GL}_n(\mathbb{F}_2)$ satisfies $Ae_1 = e_1$ and $Ae_2 = e_2$, then $A(e_1 + e_2) = e_1 + e_2 \neq e_3$. □

For a commutative ring R and $n \in \mathbb{Z}^+$, the set of $n \times n$ invertible scalar matrices – i.e., diagonal matrices in which each diagonal entry is equal to a fixed element $\alpha \in R^\times$ form a normal subgroup of $\mathrm{GL}_n(R)$. We denote the quotient by $\mathrm{PGL}_n(R)$, the **projective general linear group**.

Exercise 9.59. *Let F be a field. On the set $F^2 \setminus \{0\}$ we define an equivalence relation: for all $\alpha \in F^\times$, we put $(x_1, x_2) \sim (\alpha x_1, x_2)$. We define the **projective line** $\mathbb{P}^1(F)$ to be the set of equivalence classes under this equivalence relation.*

a) *We may map $\iota : F \hookrightarrow \mathbb{P}^1(F)$ by mapping $x \in F$ to the $\sim$-equivalence class of $(x, 1)$. Show: the map ι is an embedding, and $\mathbb{P}^1(F) \setminus \iota(F)$ consists of a single element, the $\sim$-equivalence class of $(1, 0)$. We denote this element of $P^1(F)$ by ∞.*
b) *Show: in the natural action of $\mathrm{GL}_2(F)$ on $F^2 \setminus \{(0, 0)\}$, the scalar matrices act trivially, so we get an action of $\mathrm{PGL}_2(F)$ on $\mathbb{P}^1$. Show: this action is effective and transitive.*

c) *Show: the action of* $\mathrm{PGL}_2(F)$ *on* $\mathbb{P}^1(F)$ *can be expressed in terms of* ***linear fractional transformations*** $x \mapsto \frac{ax+b}{cx+d}$.

d) *Let* G_∞ *be the stabilizer of* ∞ *in the action of* $\mathrm{PGL}_2(F)$ *on* $\mathbb{P}^1(F)$. *Show:* G_∞ *consists of elements of* $\mathrm{PGL}_2(F)$ *all of whose preimages in* $\mathrm{GL}_2(F)$ *are upper triangular. Show: there is a group isomorphism* $\rho : \mathrm{AGL}_1(F) \to G_\infty$ *such that if we pull back the* G_∞*-action on* F *to* $\mathrm{AGL}_1(F)$ *via* ρ, *we get the standard* $\mathrm{AGL}_1(F)$*-action on* F. *Deduce from Proposition 9.42 that* $\mathrm{PGL}_2(F)$ *acts 3-transitively on* $\mathbb{P}^1(F)$.

PROPOSITION 9.44. *Let* $G \subseteq S_n$ *be a doubly transitive permutation group. Then* G *is primitive.*

PROOF. Let B be a subset of $\{1, \ldots, n\}$ of size $1 < k < n$. Choose distinct elements $i, j \in B$ and $k \in \{1, \ldots, n\} \setminus B$. Since G is doubly transitive, there is $\sigma \in G$ such that $\sigma(i) = j$ and $\sigma(j) = k$. Then $\sigma(B)$ has nonempty intersection with B but is not equal to B, so B is not a block for G. Thus G is primitive. □

For a group G, a **minimal normal subgroup** N is a nontrivial normal subgroup of G that is minimal among all *nontrivial* normal subgroups. Thus the trivial group has no minimal normal subgroups.

EXERCISE 9.60. *Let* G *be a nontrivial group.*

a) *Show:* G *is a minimal normal subgroup of* G *if and only if* G *is simple.*

b) *Show: if* G *is finite, then* G *has at least one minimal subgroup.*

c) *Suppose* G *is finite commutative. Show: the minimal normal subgroups of* G *are precisely the subgroups of prime order. Deduce that a finite group may have arbitrarily (finitely!) many isomorphism classes of minimal normal subgroups.*

d) *Show: an infinite cyclic group has no minimal normal subgroup.*

EXERCISE 9.61. *Let* $\mathbb{F}_q$ *be a finite field, and let* $n \in \mathbb{Z}^+$. *Show:* $(\mathbb{F}_q^n, +)$ *is a minimal normal subgroup of* $\mathrm{AGL}_n(\mathbb{F}_q)$.

The **socle** $\mathrm{soc}(G)$ of a nontrivial finite group G is the subgroup generated by all minimal normal subgroups.

The following result is not hard to prove, but I find it quite surprising.

THEOREM 9.45. *Let* G *be a nontrivial finite group.*

a) *Suppose* K *is a minimal normal subgroup of* G *and* L *is any normal subgroup of* G. *Then either* $K \subseteq L$ *or* $\langle K, L \rangle = K \times L$.

b) *There are minimal normal subgroups* $K_1, \ldots, K_m$ *of* G *such that*

$$\mathrm{soc}(G) = \prod_{i=1}^{m} K_i.$$

c) *If* K *is a minimal normal subgroup of* G, *then there are simple subgroups* $T_1, \ldots, T_k$ *of* G, *all conjugate to each other, such that* $K = \prod_{i=1}^{m} T_i$.

PROOF. a) We may assume that K is not contained in L. Then $K \cap L$ is normal in G and proper in the minimal normal subgroup K, so $K \cap L = \{e\}$. Since K and L are both normal, the subgroup they generate is then the direct product $K \times L$.
b) Since G is finite and nontrivial, the set of minimal normal subgroups of G

is finite and nonempty; let us write them out as $K_1, \ldots, K_n$. If $n = 1$, then clearly $\mathrm{soc}(G) = K_1$ and we're done, so we may assume that $n \geq 2$. For any subset $I \subseteq \{1, \ldots, n\}$, the subgroup $\langle K_i \mid i \in I \rangle$ is normal. Since K_1 and K_2 are both minimal normal subgroups, neither contains the other, so by part a) we have $\langle K_1, K_2 \rangle = K_1 \times K_3$. If $n = 2$, we're done, so suppose $n \geq 3$. Then again by part a), we have that $\langle K_1, K_2, K_3 \rangle$ is either $K_1 \times K_2$ – this happens if and only if $K_1 \times K_2$ contains K_3 – or is $K_1 \times K_2 \times K_3$. Continuing in this manner, we arrive at the desired result.

c) Let K be a minimal normal subgroup of G, and let T be a minimal normal subgroup of K. Then for all $g \in G$, the subgroup $T^g := g^{-1}Tg$ is also a minimal normal subgroup of K. We can choose a subset $T_1, \ldots, T_m$ of these conjugates that is maximal with respect to the property that the subgroup L that they generate is $\prod_{i=1}^m T_i$. Then as in part b) we see that L contains all conjugates of T hence is normal (since it has a set of generators that is closed under conjugation) in G. Since $\{e\} \subsetneq L \subseteq K$ and K is minimal normal, we have $L = K$. Finally, let $1 \leq i \leq m$. Then for any normal subgroup N_i of T_i, under the group embedding $T_i \hookrightarrow \prod_{i=1}^m T_i = K$, N_i is a normal subgroup of K, so in order for T_i to be minimal normal it must be simple. □

COROLLARY 9.46. *Let G be a finite solvable group, and let N be a minimal normal subgroup of G. Then there is a prime number p and $n \in \mathbb{Z}^+$ such that $N \cong (\mathbb{F}_p, +)^n$.*

EXERCISE 9.62. *Prove Corollary 9.46.*

LEMMA 9.47. *Let $G \subseteq S_n$ be primitive, and let N be a nontrivial normal subgroup of G. Then N is transitive.*

PROOF. Let $i \in \{1, \ldots, n\}$, and let $\sigma \in G$. Since N is normal in G, we have

$$\sigma N i = \sigma N \sigma^{-1} \sigma i = N \sigma i,$$

showing that G stabilizes the partition of $\{1, \ldots, n\}$ into N-orbits. Since G is primitive and N is nontrivial, that forces this partition to have a single element: thus N is transitive. □

THEOREM 9.48 (Galois). *Let $G \subseteq S_n$ be a primitive solvable permutation group. Then $n = p^a$ is a prime power, and for some conjugate G' of G we have*

$$\mathbb{F}_p^a \subseteq G' \subseteq \mathrm{AGL}_a(\mathbb{F}_p) \subseteq S_{p^a}.$$

PROOF. Let N be a minimal normal subgroup of G. By Lemma 9.47, N is transitive, and by Exercise 9.46 we have that $N \cong \mathbb{F}_p^a$ for some $a \in \mathbb{Z}^+$. In particular N is commutative and transitive, so by Exercise 9.51a) we find that N is simply transitive: thus $n = p^a$, and after replacing G by a conjugate G' we may assume that G' is a group of permutations on $\mathbb{F}_p^a$ that contains $(\mathbb{F}_p^a, +)$. We will write the elements as τ_v for $v \in \mathbb{F}_p^a$ to emphasize that they act by translations. It remains to show that $G' \subseteq \mathrm{AGL}_a(\mathbb{F}_p)$.

Let G'_0 be the stabilizer of 0 in G. Since F_p^a is normal in G', for all $v \in \mathbb{F}_p^a$ there is $w \in \mathbb{F}_p^a$ such that $g\tau_v g^{-1} = \tau_w$. Since $g0 = 0$, we find:

$$gv = g\tau_v 0 = \tau_w g0 = \tau_w 0 = w,$$

so

$$\forall g \in G'_0, \forall v \in \mathbb{F}_p^a,\ g\tau_v g^{-1} = \tau_{gv}.$$

For fixed $g \in G_0'$, conjugation by g is a group automorphism of $\mathbb{F}_p^a$, hence the map $v \mapsto gv$ is a group automorphism of $\mathbb{F}_p^a$. Every group automorphism of an $\mathbb{F}_p$-vector space is $\mathbb{F}_p$-linear, so this shows that $g \in \mathrm{GL}_a(\mathbb{F}_p)$. Since $\mathbb{F}_p^a$ acts transitively on itself, for every element g of G' there is $v \in \mathbb{F}_p^a$ such that $\tau_v g \in G_0'$. Thus G' is contained in the subgroup generated by $\mathrm{GL}_a(\mathbb{F}_p)$ and $(\mathbb{F}_p^a, +)$, which is $\mathrm{AGL}_a(\mathbb{F}_p)$. □

EXERCISE 9.63. *Let $G \subseteq S_6$ be a solvable subgroup of S_6. Show: $\#G \leq 54$, and $\#G = 54$ if and only if G is conjugate to $S_3 \wr S_2$.*

Let F be a field, and let G be a subgroup of $\mathrm{GL}_n(F)$. We say that G is **irreducible** if the natural representation of G on F^n is irreducible: that is, there is no nontrivial, proper F-subspace of F^n that is stabilized by G.

The following exercise shows that classifying solvable primitie subgroups of S_{p^n} is equivalent to classifying solvable irreducible subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$.

EXERCISE 9.64. *Let p be a prime number, let $n \in \mathbb{Z}^+$, and let consider a permutation group*

$$\mathbb{F}_p^n \subseteq G \subseteq \mathrm{AGL}_n(\mathbb{F}_p) \subseteq S_{p^n}.$$

Let G_0 be the stabilizer of 0 in G. Notice that G_0 is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$.

a) *Show: G is primitive if and only if G_0 is irreducible.*
b) *Show: G is solvable if and only if G_0 is solvable.*

11. Dedekind's Theorem and S_n as a Galois Group over $\mathbb{Q}$

THEOREM 9.49 (Dedekind). *Let $f \in \mathbb{Z}[t]$ be monic separable of degree $n \geq 2$, with Galois group G. For a prime number p, let $f_p \in \mathbb{Z}/p\mathbb{Z}[t]$ be the polynomial obtained by reducing the coefficients of f modulo p,and assume that f_p is separable (equivalently, p does not divide the discriminant of f). Suppose that f_p factors as $g_1 \cdots g_k$ with $\deg(g_i) = n_i$. Then there is an element $\sigma_p \in G$ of cycle type $(n_1, \ldots, n_k)$.*

PROOF. (Milne) Step 1: Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\overline{\mathbb{Q}}$, and put

$$L := \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \text{ and } A := \mathbb{Z}[\alpha_1, \ldots, \alpha_n].$$

Since $\mathbb{Z}$ is a Noetherian ring and A is a finitely generated $\mathbb{Z}$-module, every $\mathbb{Z}$-submodule of A is also finitely generated, while $\mathbb{Z}[\frac{1}{p}]$ is not finitely generated, so p is not invertible in A and therefore is contained in a maximal ideal $\mathfrak{p}$ of A. The intersection $\mathfrak{p} \cap A$ is a prime ideal of $\mathbb{Z}$ containing p, hence $\mathfrak{p} \cap A = (p)$, and it follows that $A/\mathfrak{p}$ is a finite degree field extension of $\mathbb{F}_p$, say of degree d_p. For $a \in A$, we write $\overline{a}$ for the image of a in $A/\mathfrak{p}$; then $A/\mathfrak{p} = \mathbb{F}_p[\overline{\alpha_1}, \ldots, \overline{\alpha_n}]$ is the splitting field of f_p. Let G_p be the Galois group of f_p, so G_p is cyclic of order d_p, generated by the Frobenius map $\mathfrak{f}_p : x \mapsto x^p$.
Step 2: Let

$$D_{\mathfrak{p}} := \{\sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p}\},$$

so $D_{\mathfrak{p}}$ is a subgroup of G and reduction modulo $\mathfrak{p}$ gives a homomorphism

$$r : D_{\mathfrak{p}} \to G_p.$$

We claim that r is an isomorphism of groups. First, the fact that the roots $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ are distinct means that for $\sigma \in D_{\mathfrak{p}}$, σ is a nontrivial permutation of

the α_i's if and only if $r(\sigma)$ is a nontrivial permutation of the $\overline{\alpha_i}$'s, and thus r is injective. In particular we have $\#D_p \leq \#G_p$.

Let $x \in A$ be such that $A/\mathfrak{p} = \mathbb{F}_p(\overline{x})$. By the Chinese Remainder Theorem, there is $y \in A$ such that $y \equiv x \pmod{\mathfrak{p}}$ and $y \equiv 0 \pmod{\sigma(\mathfrak{p})}$ for all $\sigma \in G \setminus D_{\mathfrak{p}}$. Put

$$g \coloneqq \prod_{\sigma \in G} (t - \sigma(y)).$$

Then $g \in \mathbb{Q}[t]$ by Galois theory, and because each $\sigma(y)$ is integral over $\mathbb{Z}$, also each coefficient of g is integral over $\mathbb{Z}$; since $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, we get $g \in \mathbb{Z}[t]$. Moreover

$$g_p = t^{\#G - \#D_{\mathfrak{p}}} \prod_{\sigma \in D_{\mathfrak{p}}} (t - \overline{\sigma(x)}) \in \mathbb{F}_p[t].$$

Thus the minimal polynomial of $\overline{x}$ over $\mathbb{F}_p$ divides g_p, so

$$\#G_p = [\mathbb{F}_p(\overline{x}) : \mathbb{F}_p] \leq \deg g_p = \#D_{\mathfrak{p}}.$$

It follows that $\#D_{\mathfrak{p}} = \#G_{\mathfrak{p}}$, so r is an injective map between two finite groups of the same size, so r is an isomorphism.

Step 3: By Step 2 there is a unique $\sigma_p \in G$ such that $r(\sigma_p) = \mathfrak{f}_p$. For any ireducible polynomial $g \in \mathbb{F}_p[t]$ of degree d, the Frobenius map $\mathfrak{f}_p$ acts on the roots of g in $\overline{\mathbb{F}_p}$ as a d-cycle. It follows that if the degrees of the irreducible factors of f_p are $n_1, \ldots, n_k$, then σ_p acts on $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ with cycle type $(n_1, \ldots, n_k)$ and thus also σ_p acts on $\alpha_1, \ldots, \alpha_n$ with cycle type $(n_1, \ldots, n_k)$, completing the proof. □

EXERCISE 9.65. *Let R be a Dedekind domain, and let $\mathfrak{p}$ be a maximal ideal of R such that the field $R/\mathfrak{p}$ is finite. State and prove a generalization of Theorem 9.49 with $\mathbb{Z}$ replaced by R and $\mathbb{F}_p$ replaced by $R/\mathfrak{p}$.*

It is remarkably easy to use Theorem 9.49 to show that S_n occurs as a Galois group for all $n \geq 2$. First:

LEMMA 9.50. *Let $n \in \mathbb{Z}^{\geq 2}$, and let $G \subseteq S_n$ be a transitive subgroup containing an $(n-1)$-cycle and a 2-cycle. Then $G = S_n$.*

PROOF. The hypothesis and conclusion are invariant under conjugation of G, so we may assume that G contains the n-cycle $c \coloneqq (12 \cdots n-1)$ and a 2-cycle $\tau = (ij)$. We claim that G must also contain a 2-cycle of the form (kn) for some $1 \leq k \leq n-1$. Since G is transitive, there is $\sigma \in G$ such that $\sigma(i) = n$. Then $\tau' \coloneqq \sigma\tau\sigma^{-1}$ is a 2-cycle that maps n to $\sigma(j) \neq \sigma(i) = n$, so τ' is of the desired form. Now we have

$$\{c^i \tau' c^{-i} \mid 1 \leq i \leq n-1\} = \{(2n), (3n), \ldots, (n-1n)\},$$

and it is easy to see that this set of transpositions generates S_n. □

COROLLARY 9.51. *Let $n \in \mathbb{Z}^{\geq 2}$. Then there is a monic irreducible polynomial $f \in \mathbb{Z}[t]$ of degree n with Galois group S_n.*

PROOF. Given a nonempty finite set S of prime numbers and for each $p \in S$ a monic degree n polynomial $f_p \in \mathbb{F}_p[t]$, by the classical Chinese Remainder Theorem there is a monic degree n polynomial $f \in \mathbb{Z}[t]$ such that for all $p \in S$, the modulo p reduction of f is f_p. Also, by the Primitive Element Theorem and the structure theory of finite fields, for all prime numbers p and $d \in \mathbb{Z}^+$, there is a degree d irreducible monic polynomial in $\mathbb{F}_p[t]$. Choose a prime number $p \geq n-2$ and put

$S := \{2, 3, p\}$. Below we specify monic separable degree n polynomials $f_2 \in \mathbb{Z}/2\mathbb{Z}[t]$, $f_3 \in \mathbb{Z}/3\mathbb{Z}[t]$ and $f_p \in \mathbb{Z}/p\mathbb{Z}[t]$; let $f \in \mathbb{Z}[t]$ be a polynomial reducing modulo 2 to f_2 and reducing modulo p to f_p.
• Let $g_1 \in \mathbb{F}_2[t]$ be monic irreducible of degree n.
• Let $g_1 \in \mathbb{F}_3[t]$ be a monic irreducible polynomial of degree $n-1$; if $n = 2$, w take $g_1 = t - 1$. We put $f_3 := tg_1$, so f_3 is monic separable.
• Let $p \geq n-2$ be a prime number, let $g_1 \in \mathbb{F}_p[t]$ be a monic irreducible quadratic polynomial, and put $f_p := g_1 \cdot \prod_{i=1}^{n-2}(t-i)$, so f_p is monic separable.
Let $G \subseteq S_n$ be the Galois group of f. Applying Theorem 9.49 to the primes 2, 3 and p, we find first that G contains an n-cycle, so it is transitive, then that it contains an $(n-1)$-cycle, and finally that it. Then Lemma 9.50 gives $G = S_n$. □

EXERCISE 9.66. *Show that the proof of Corollary 9.51 can be modified so that the third prime is* 5 *rather than some prime* $p \geq n-2$. *Namely, show that one may take* f_5 *to be the product of an irreducible quadratic and either one or two more irreducible polynomials of odd degrees (and show that this can be done so as to make* f_5 *separable). The point being: if* $\sigma_5 \in G$ *is the element given by Theorem 9.49, then some power of* σ_5 *is a* 2*-cycle.*

EXERCISE 9.67. *Let* F *be a* ***global field****: that is,* F *is a finite degree extension of either* $\mathbb{Q}$ *or* $\mathbb{F}_p(t)$. *Show: for all* $n \geq 2$, S_n *occurs as a Galois group over* F.

We can use Theorem 9.49 to show that A_5 occurs as a Galois group over $\mathbb{Q}$. First:

EXERCISE 9.68.

a) *Let* G *be a noncommutative simple group, and let* H *be a proper subgroup of* G. *Show:* $[G : H] \geq 5$.
(Hint: Since H *is proper and* G *is simple,* G *acts faithfully on* G/H*.)*
b) *Let* H *be a subgroup of* A_5. *Show that the following are equivalent:*
(i) $H = A_5$.
(ii) H *contains elements of orders* 3 *and* 5.
(iii) H *is transitive and contains an element of order* 3.

EXAMPLE 9.52. *We will show that the Galois group* G *of*

$$f := t^5 + 20t + 16 \in \mathbb{Q}[t]$$

is A_5.[6] *In what follows we will make various statements about discriminants and factorization of polynomials. These were all confirmed using the MAGMA computer algebra system.*

• *The discriminant of* f *is* $2^{16} \cdot 5^6 \in \mathbb{Q}^{\times 2}$ *(of course we used a computer algebra system for this), so* G *is a subgroup of* A_5.

• *The image* f_3 *of* f *in* $\mathbb{Z}/3\mathbb{Z}[t]$ *is irreducible. By Gauss's Lemma, this shows that* f *is irreducible, and thus* G *is a transitive subgroup of* A_5 *so by Orbit-Stablizer has order divisible by* 5. *Alternately, Dedekind's Theorem implies that* G *has an element* σ_5 *of order* 5.

• *The image* f_7 *of* f *in* $\mathbb{Z}/7\mathbb{Z}[t]$ *factors into ireducibles as*

$$f_7 = (t+2)(t+3)(t^3 + 2t^2 + 5t + 5),$$

[6]We follow `https://math.stackexchange.com/questions/286944/quintic-polynomial-with-galois-group-a-5`

so by Dedekind's Theorem there is a 3-cycle $\sigma_7 \in G$. By Exercise 9.68b), we conclude: $G = A_5$.

Now we go a little further to show that Exercise 9.68 can be avoided:

- *The image f_{23} of f in $\mathbb{Z}/23\mathbb{Z}$ factors into irreducibles as*

$$f_{23} = (t+17)(t^2+12t+14)(t^2+17t+2),$$

so by Dedekind's Theorem there is $\sigma_{23} \in G$ of cycle type $(2,2)$. Thus G is a subgroup of A_5 of order at least 30, hence G has index 1 or 2 in A_5. Since index 2 subgroups are normal and A_5 is simple, it must be that $G = A_5$.

The cycle types of elements of A_5 are (5), (3, 1), (2, 2, 1) and (1, 1, 1, 1, 1). In Example 9.52 we saw that every nontrivial cycle type corresponds to the factorization of f modulo some prime $p \nmid \delta(f)$. What about the trivial cycle type – in other words, is there a prime p such that $f_p \in \mathbb{Z}/p\mathbb{Z}[t]$ splits? The answer is *yes* although we have to wait a little for it: the smallest such prime is $p = 887$. In fact, by a deep theorem of Cebotarev that lies beyond the scope of this text to properly discuss, it turns out that in the setting of Dedekind's Theorem, for every $\sigma \in G$ there are infinitely many prime numbers p not dividing $\delta(f)$ such that σ_p is conjugate to σ in G. There is moreover an *Effective* version of this result, which means: given a polynomial $f \in \mathbb{Z}[t]$ as in Dedekind's Theorem, one can compute from f a bound $B(f)$ such that for each $\sigma \in G$, there is a prime $p \leq B(f)$ not dividing $\delta(f)$ such that σ is conjugate to σ_p. The upshot of this is that there is an algorithm that takes as input a separable polynomial $f \in \mathbb{Q}[t]$ and returns the cycle types of the elements of its Galois group G.

EXERCISE 9.69.

a) *Let H be a subgroup of A_6 with elements of orders 3, 4 and 5. Show: $H = A_6$.*
(Suggestion: use that up to conjugacy there are two index 6 subgroups of A_6, both isomorphic to A_5.)

b) *Let $f := t^6 + 15t^2 + 18t - 20 \in \mathbb{Q}[t]$. Show: f is irreducible and separable and has Galois group A_6.*

THEOREM 9.53.

a) *Let $n \geq 2$, and let H be a subgroup of S_n. If H contains a 2-cycle and a p-cycle for some prime $p > \frac{n}{2}$, then $H = S_n$.*

b) *Let $n \geq 3$, and let H be a subgroup of S_n. If H contains a 3-cycle and a p-cycle for some prime $p > \frac{n}{2}$, then $H \supseteq A_n$.*

PROOF. See [**Co-SA**, §3]. □

A famous result in analytic number theory called Bertrand's Postulate (but first proved by Chebyshev) states that for all $n \geq 2$ there is a prime number p with $\frac{n}{2} < p \leq n$. Thus for all $n \geq 3$, A_n contains a 3-cycle and a p-cycle for some prime $p > \frac{n}{2}$. Thus for all $n \geq 3$ we get a method for showing that an irreducible, separable degree n polynomial $f \in \mathbb{Q}[t]$ has Galois group S_n: check that its discriminant is a square and then find primes $p_1, p_2 \nmid \delta(f)$ such that f_{p_1} factors into an irreducible cubic times a product of linear polynomials and f_{p_2} factors into an irreducible polynomial of degree p (for some prime p with $\frac{n}{2} < p \leq n$) times a product of linear factors. Then Dedekind's Theorem together with Theorem 9.53 shows that

the Galois group of f is A_n. By the Cebotarev Density Theorem, so long as the Galois group of f is A_n, this method will always succeed.

EXERCISE 9.70. *Let $f := t^7 - 56t + 48$. Show: f is irreducible and separable and has Galois group A_7.*

In fact Hilbert showed [**Hi92**] that A_n occurs as a Galois group over $\mathbb{Q}$ for all $n \geq 2$. His methods are geometric in nature and beyond the scope of this text.

For all $n \leq 11$, complete lists of transitive subgroups (up to conjugacy, as usual) of S_n were computed by Butler-McKay [**BM83**]. For some n it can happen that non-conjugate transitive subgroups of S_n have the same set of cycle types of elements, and then one needs to do more, which very roughly speaking involves looking at actions on both ordered and unordered subsets of the set of roots. But it is indeed the case that there is an algorithm to compute the Galois group of a separable, irreducible polynomial $f \in \mathbb{Q}[t]$ of degre at most 11, and this algorithm has been implemented in MAGMA. In [**SM85**], for all $n \leq 7$ and each transitive subgroup G of S_n, Soicher–McKay exhibit a polynomial $f \in \mathbb{Q}[t]$ with Galois group G.

As of late 2025, the list of transitive subgroups of S_n is known for all $n \leq 31$. It is also known that for all $n \leq 22$, every transitive subgroup G of S_n occurs as a Galois group over $\mathbb{Q}$, and the sole transitive subgroup of S_{23} that is not yet known to occur over $\mathbb{Q}$ is the Matthieu group M_{23}. For the last piece of this result and a description of the literature, see [**vBCEKSV25**], which realizes a single (heretofore recalcitrant) subgroup of S_{17} using modular forms methods.

Dedekind's Theorem provides a superior method to showing that an irreducible quintic $f \in \mathbb{Q}[t]$ has Galois group D_5 than the one provided by Theorem 9.27.

EXAMPLE 9.54. *We revisit the polynomial $f := t^5 - 5t + 12 \in \mathbb{Q}[t]$ from Exercise 9.34d), which has discriminant $(2^6 5^3)^2$. Since $f_7 \in \mathbb{F}_7[t]$ is irreducible, also f is irreducible. Let G be its Galois group. We have*

$$R_6(f) = t^6 - 40t^5 + 1000t^4 - 20000t^3 + 250000t^2 - 66400000t + 976000000,$$

and since $R_6(40) = 0$, G is solvable. By Theorem 9.26, G is isomorphic to C_5 or D_5. Since $f_3 \in \mathbb{F}_3[t] = t(t+1)(t+2)(t^2+1)$, Dedekind's Theorem implies that G contains an element of even order, so $G \cong D_5$.

The following exercise shows that the converse of Theorem 9.27 does not hold: an irreducible quintic $f \in \mathbb{Q}[t]$ can have five real roots and Galois group D_5.

EXERCISE 9.71. *Let $f := t^5 - t^4 - 5t^3 + 4t^2 + 3t - 1 \in \mathbb{Q}[t]$.*

a) *Show: f is irreducible.*
b) *Use calculus to show that f has five real roots.*
c) *Use Corollary 9.26 and Theorem 9.49 to show that the Galois group of f is isomorphic to D_5.*

A number field F is **totally real** if for every embedding $\sigma : F \hookrightarrow \mathbb{C}$ we have $\sigma(F) \subseteq \mathbb{R}$ and is **totally complex** if for *no* embedding $\sigma : F \hookrightarrow \mathbb{C}$ do we have $\sigma(F) \subseteq \mathbb{R}$. A number field of degree $n \geq 3$ need not be either totally real or totally complex; these are just the extremes, but Theorem 9.27a) and its proof amount to showing that if $F/\mathbb{Q}$ is Galois, it must be totally real or totally complex and thus an odd degree Galois extension must be totally real. From the online database

LMFDB, one can see that least for all $n \leq 20$, every even order transitive subgroup G of S_n occurs as both as a Galois group of a degree n polynomial $f \in \mathbb{Q}[t]$ with totally real splitting field and as the Galois group of a degree n polynomial $g \in \mathbb{Q}[t]$ with totally complex splitting field. Based on this, it seems reasonable to conjecture that the Totally Real Inverse Galois Problem should still have an affirmative answer.

According to the Cebotarev Density Theorem, if an irreducible quintic $f \in \mathbb{Q}[t]$ has Galois group D_5, then the method of Example 9.54 will *always* work to prove that its Galois group is D_5. If the irreducible quintic $f \in \mathbb{Q}[t]$ has Galois group C_5, then after checking that $\delta(f) \in \mathbb{Q}^{\times 2}$ and $R_6(f)$ has a root in $\mathbb{Q}$, then as we compute $f_p \in \mathbb{F}_p[t]$ for various primes $p \nmid \delta(f)$, we will never find an irreducible quadratic factor, so we will become increasingly suspicious that the Galois group of f is indeed C_5. This is where the *effective* form of Cebotarev's Theorem comes into play: such a result (and there is such a result!) gives us an explicit bound X in terms of the coefficients of f so that if we compute f_p for all primes $p \leq X$ with $p \nmid \delta(f)$ and never find an irreducible quadratic factor, then we may conclude that the Galois group of f is indeed C_5 and not D_5.

Unconditional forms of the Effective Cebotarev Density Theorem give quite a large bound X. The algorithms used by computer algebra packages such as MAGMA are much more sophisticated. MAGMA indeed has an algorithm to compute the Galois group of irreducible, separable polynomials of *any* degree over number fields and over global function fields (finite degree extensions of $\mathbb{F}_p(t)$). These algorithms are significantly more complicated than what we've described above; they involve computation of many resolvent polynomials, and they make use of Frobenius elements – the elements σ_p that appear in Theorem 9.49. See [**Su15**] for a detailed description of the algorithm that MAGMA actually uses.

Part III

Transcendental Field Extensions

CHAPTER 10

Structure of Transcendental Extensions

1. Rational Function Fields

1.1. The degree of $[k(t) : k(f)]$.

THEOREM 10.1. *Let k be a field, and let $K = k(t)$ be the field of rational functions in one variable over k. Let $f \in k(t) \setminus k$, which we may write as $f = \frac{p(t)}{q(t)}$ with $\gcd(p, q) = 1$. Then:*

a) *We have that f is transcendental over k.*
b) *We have $[K : k(f)] = \max(\deg(p), \deg(q))$.*

PROOF. Put $d := \max \deg p, \deg q$, and consider the polynomial

$$P := p(X) - fq(X) \in k[f][X] \subseteq k(f)[X].$$

Then $\deg P \leq d$. In fact, since $f \notin k$, if $p(X)$ and $q(X)$ have the same degree, the leading terms of $p(X)$ and $fq(X)$ cannot cancel and thus $\deg P = d$. We have

$$P(t) = p(t) - fq(t) = 0,$$

so t satisfies a degree d polynomial equation with coefficients in $k(f)$. This shows that t is algebraic over $k(f)$ of degree at most d. It follows that if f were algebraic over k then t would be algebraic over k, which it certainly is not. This shows part a) and also that $[K : k(f)] \leq d$.

To complete the proof it suffices to show that $P \in k(f)[X]$ is irreducible. Since $P \in k[f][X] = k[f, X] = k[X][f]$ has degree 1 in f, in the polynomial ring $k[f, X]$ the only possible factorization could be into $c(X)\ell(X, f)$, where $c(X) \in k[X]$ and $\ell(X, f)$ has degree 1 in X and thus $c(X) \mid \gcd(P(x), Q(x))$, hence $c(X) \in k^\times$ and the factorization is trivial. So $P \in k[f][X]$ is irreducible. Since $k[X]$ is a UFD, by one version of Gauss's Lemma [**Cl-CA**, Cor. 15.25a)] we have $P \in k(f)[X]$ is irreducible, completing the proof. □

Let L/K be a field extension. We say that **K is algebraically closed in L** if for all $x \in L$, if x is algebraic over K then $x \in K$. Otherwise put, L/K is *not* algebraically closed in L if there is a subextension M of L/K such that M/K is nontrivial algebraic. In particular, if $L \supsetneq K$ and K is algebraically closed in L then L/K is transcendental.

This terminology may be confusing at first, because it is so close to "algebraically closed" and yet means something quite different. There is however some connection:

EXERCISE 10.1. *For a field K, show that the following are equivalent:*

(i) *For every field extension L/K we have that K is algebraically closed in L.*
(ii) *The field K is algebraically closed.*

As an important example, Theorem 10.1a) is precisely the assertion that for every field k we have that k is algebraically closed in $k(t)$. One can easily generalize this as follows:

PROPOSITION 10.2. *Let k be a field, and let $k[\{t_i\}_{i\in I}]$ be the polynomial ring over k in a (possibly infinite) set of indeterminates. Let K be the fraction field of $k[\{t_i\}_{i\in I}]$, a **rational function field**. Then k is algebraically closed in K.*

PROOF. Step 1: Suppose that I is finite, in which case we may as well take $I = \{1, \ldots, n\}$. We will prove that k is algebraically closed in $K = k(t_1, \ldots, t_n)$ by induction on n, the base case $n = 1$ being Theorem 10.1a). Suppose the result holds for rational function fields in $n-1$ variables, and let $x \in K$ be algebraic over k. Certainly then x is algebraic over $k(t_1, \ldots, t_{n-1})$, and since $k(t_1, \ldots, t_n) = k(t_1, \ldots, t_{n-1})(t_n)$, it follows from the base case that $x \in k(t_1, \ldots, t_{n-1}$, and then it follows from the induction hypothesis that $x \in k$.
Step 2: Suppose that I is infinite, and let $x \in K$ be algebraic over k. We have $K = \bigcup_{S\subset T} k(\{t_i \mid i \in S\})$ as S ranges over all finite subsets of T, so x lies in some subfield that is a rational function field in finitely many indeterminates, and thus being algebraic over k we get from Step 1 that x lies in k. □

1.2. $\mathrm{Aut}(K(t)/K)$**.** We now compute the automorphism group $\mathrm{Aut}(K(t)/K)$ of the transcendental extension $K(t)/K$. We will see in particular that this group if infinite if and only if K is infinite, which gives our first example of an infinite automorphism group of a field.

If L/K is a field extension, S is a set of generators for L/K, M/K is another field extension and $\iota_1, \iota_2 : L \hookrightarrow M$ are K-algebra homomorphisms, then $\iota_1 = \iota_2$ if and only if $\iota_1(x) = \iota_2(x)$ for all $x \in S$. It follows that if $\sigma, \tau \in \mathrm{Aut}(K(t)/K)$, then we have $\sigma = \tau$ if and only if $\sigma(t) = \tau(t)$. So the main question is for which $f \in K(t)$ we can extend $t \mapsto f$ to a K-algebra automorphism of $K(t)$. By the universal property of polynomial algebras [**Cl-CA**, Thm. 5.37], for any $f \in K(t)$ there is a unique K-algebra homomorphism $\varphi : K[t] \to K(t)$ such that $\varphi(t) = f$. If $f = a \in K$, then the kernel of φ is $(t-a)$, so φ cannot extend to a homomorphism $K(t) \to K(t)$ – field homomorphisms are injective. If $f \in K(t) \setminus K$, then since K is algebraically closed in $K(t)$, the element f is transcendental. It follows that for $p = a_n t^n + \ldots + a_1 t + a_0 \in \mathrm{Ker}\,\varphi$ then $0 = \varphi(p) = a_n f^n + \ldots + a_1 f + a_0$ and thus $p = 0$ since f is transcendental. So φ is an injective K-algebra homomorphism of domains and thus uniquely extends to a homomorphism on fraction fields

$$\Phi : K(t) \to K(t).$$

The image of Φ is the subfield $k(f)$ of $K(t)$. By Theorem 10.1, if we write $f \in K(t) \setminus K$ as $f = \frac{p}{q}$ with $\gcd(p, q) = 1$, then we have

$$[K(t) : \Phi(K(t))] = [K(t) : K(f)] = \max(\deg(p), \deg(q)).$$

It follows that the field homomorphism $\Phi : K(t) \to K(t)$ is a field automorphism if and only if $\max(\deg(p), \deg(q)) = 1$.

It follows that evaluation at t gives a bijection from $\mathrm{Aut}(K(t)/K)$ to $\{\frac{at+b}{ct+d} \mid a, b, c, d \in K \mid ad - bc \neq 0\}$ – the latter condition is because $ad - bc = 0$ if and only

if $\frac{at+b}{ct+d} \in k$. Thus we can represent each $\sigma \in \mathrm{Aut}(K(t)/K)$ as a matrix

$$M(\sigma) := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(K).$$

Two matrices determine the same automorphism if and only if they are scalar multiples of each other, so if we define $\mathrm{PGL}_2(K)$ as the quotient of $\mathrm{GL}_2(K)$ modulo the (central, hence normal) subgroup $K^\times$ of scalar matrices $\{\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in K^\times\}$ then we get a canonical bijection from $\mathrm{Aut}(K(t)/K)$ to $\mathrm{PGL}_2(K)$. In the following theorem we summarize the above discussion and add one more piece.

THEOREM 10.3. *The map* $\mathrm{Aut}(K(t)/K) \to \mathrm{PGL}_2(K)$ *given by*

$$s \in \mathrm{Aut}(K(t)/K) \mapsto s(t) = \frac{at+b}{ct+d} \mapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix} \pmod{K^\times}$$

is an isomorphism of groups.

EXERCISE 10.2. *Complete the proof of Theorem 10.3 by showing that the above bijection from* $\mathrm{Aut}(K(t)/K)$ *to* $\mathrm{PGL}_2(K)$ *is an isomorphism of groups.*

EXERCISE 10.3. *Let* K *be a field.*

a) *Suppose that* $K \cong \mathbb{F}_q$. *Show:* $\#\,\mathrm{Aut}(K(t)/K) = (q+1)(q^2-q)$.
b) *Suppose that* K *is infinite. Show:* $\#\,\mathrm{Aut}(K(t)/K) = \#K$.

1.3. Lüroth's Theorem.

THEOREM 10.4 (Lüroth's Theorem). *Let* K *be a field, and let* L *be a field such that* $K \subsetneq L \subset K(t)$. *Then there is* $f \in K(t)$ *such that* $L = K(f)$.

PROOF. Let $v \in L \setminus K$. By Theorem 10.1 we know that $K(t)/K(v)$ has finite degree, so $[K(t) : L]$ is finite. Let

$$f(x) := x^n + \ell_{n-1}x^{n-1} + \ldots + \ell_1 x + \ell_0 \in L[x]$$

be the minimal polynomial of t over L. Since t is transcendental over K, there is $0 \le j \le n-1$ such that l_j lies in $L \setminus K$: we fix one such index and call it J. Put

$$u := \ell_J;$$

we will in fact show that $L = K(u)$. Put

$$m := [K(t) : K(u)].$$

Since $K(u) \subset L$ we have $m \ge n$, so to show $L = K(u)$ it suffices to show $n \ge m$.

We may scale the coefficients of f so as to get a primitive polynomial in $K[t][x]$: choose $c_0(t), \ldots, c_{n-1}(t), d(t) \in K[t]$ such that $\gcd(c_0, \ldots, c_{n-1}, d) = 1$ and for all $0 \le j \le n-1$ we have $\ell_j = \frac{c_j}{d}$. In particular we have

$$u = \ell_J = \frac{c_J}{d}.$$

Put

$$M := \max(\deg(c_J), \deg(d)).$$

By Theorem 10.1 we have

$$m = [K(t) : K(u)] \le M.$$

The inequality is because of the possibility that c_J and d are not coprime. Put

$$F(x,t) := d(t)f(x) = d(t)x^n + c_{n-1}(T)x^{n-1} + \ldots + c_0(T) \in K[x,t].$$

Then $F(x,t)$ is primitive as a polynomial in x, has x-degree $\deg_x F = n$ and has t-degree $\deg_t F \geq M \geq m$. Now t is a root of the polynomial $c_J(x) - ud(x) \in L[x]$, so there is $q \in L[x]$ such that

$$c_J(x) - ud(x) = q(x)f(x) \in L[x].$$

Substituting $u = \frac{c_J}{d}$ and clearing denominators, we get

$$c_J(x)d(t) - c_J(t)d(x) = d(t)q(x)f(x) = q(x)F(x,t).$$

Since the left hand side lies in $K[t,x]$ and $F(x,t)$ is primitive in x, Gauss's Lemma implies that

$$q(x) = r(x,t) \in K[x,t]$$

and thus

$$c_J(x)d(t) - c_J(t)d(x) = r(x,t)F(x,t). \tag{38}$$

In (38), the t-degree of the left hand side is at most $\max(\deg(d(t), \deg(c_J(t)) = m$, whereas for the right hand side we have

$$\deg_t(r(x,t)F(x,t))\deg_t(r(x,t)) + \deg_t(F(x,t)) \geq \deg_t(r(x,t)) + M.$$

It follows that $\deg_t(r(x,t)) = 0$, i.e., $r(x,t) = r(x) \in K[x]$. It follows that $rF = c_J(x)d(t) - c_J(t)d(x)$ is primitive in $K[t][x]$, and then the symmetric form of $c_J(x)d(t) - c_J(t)d(x)$ implies that rF is also primitive in $K[x][t]$, which implies that $r \in K$ is constant. We conclude

$$n = \deg_x(F) = \deg_x(rF) = \deg_x(c_J(x)d(t) - c_J(t)d(x)) \geq M \geq m.$$

It follows that $n = M$ and $L = K(u)$. □

It turns out though that Theorem 10.4 is one of the last positive results of its kind. More generally, the **Lüroth Problem** asks: if K is a field, $K(t_1, \ldots, t_n)$ is a rational function field over K and L is a field with $K \subseteq L \subseteq K(t_1, \ldots, t_n)$ such that $K(t_1, \ldots, t_n)/L$ has finite degree, must we have $L \cong K(t_1, \ldots, t_n)$? Theorem 10.4 yields an affirmative answer to the Lüroth Problem for $n = 1$ and all fields K.[1]

For $n \geq 2$ the Lüroth Problem is really one of the most basic (and deep) questions of higher-dimensional birational algebraic geometry. There is only one more case of an affirmative answer: when K is algebraically closed of characteristic 0 (e.g. $K = \mathbb{C}$, the most important field for classical algebraic geometry) Castelnuovo showed that when $n = 2$ the Lüroth Problem again has an affirmative answer: that is, any finite index K-subalgebra of $K(t_1, t_2)$ is again K-isomorphic to $K(t_1, t_2)$. On the other hand, for any prime number p, and any algebraically closed field K of charcteristic p, Zariski gave counterexamples to the Lüroth Problem over K with $n = 2$ [**Za58**]. Moreover there are counterexamples to the Lüroth Problem for $n = 2$ over many non-algebraically closed fields of characteristic 0, including $K = \mathbb{Q}$. For each $n \geq 3$ there are counterexamples to the Lüroth Problem even over $K = \mathbb{C}$, the first such examples being given by Clemens and Griffiths [**CG72**].

These higher dimensional counterexamples to the Lüroth Problem are far beyond our means in these notes. Indeed the methods of pure field theory are not even well equipped to give an example of a finite degree field extension $K/\mathbb{C}(t)$ that is not isomorphic to $\mathbb{C}(t)$, although such examples are given by meromorphic function

[1]When $n = 1$, Theorem 10.1 implies that for any L with $K \subsetneq L \subset K(t)$, then $K(t)/L$ must have finite degree. This is clearly false when $n \geq 2$, hence we impose that hypothesis explicitly.

fields of any compact Riemann surface of genus $g \geq 1$. The situation is highly analogous (and actually more than analogous!) to what one encounters in general topology, where the methods developed are "too general" to provably exhibit a compact, connected topological surface that it not homeomorphic to the 2-sphere– even though the torus presents itself as a very plausible candidate, one needs the methods of a different subject, algebraic topology, to confirm this.

Theorems 10.1 and 10.4 give a good picture of the subfield lattice of $K(t)/K$ for any field K. Namely, this lattice is Noetherian – for any subextension $K \subsetneq L \subset K(t)$ we have $[K(t) : L]$ is finite, so there are no infinite ascending chains. On the other hand, the lattice is not Artinian, as there are infinite descending chains, e.g.

$$K(t) \supsetneq K(t^2) \supsetneq K(t^4) \supsetneq \ldots \supsetneq K(t^{2^n}) \supsetneq \ldots.$$

This observation can be generalized.

EXERCISE 10.4. *Let L/K be a transcendental field extension. Show: the subfield lattice of L/K is not Artinian.*

It turns out that the subfield lattice of a field extension L/K is Noetherian if and only if L/K is finitely generated: this is Exercise 10.12, and at the point at which it is assigned it will be more clear how to show it.

EXERCISE 10.5. *Show: there is an infinite degree algebraic field extension whose subfield lattice is Artinian.*

EXERCISE 10.6. *Combining Exercise 10.3 with Lüroth's Theorem (Theorem 10.4) we deduce the following intriguing consequence: for a finite field $\mathbb{F}_q$, there is a function $f \in \mathbb{F}_q(t)$ such that*

$$\mathbb{F}_q(t)^{\mathrm{Aut}(\mathbb{F}_q(t)/\mathbb{F}_q)} = \mathbb{F}_q(f)$$

and $\mathbb{F}_q(t)/\mathbb{F}_q(f)$ is finite Galois with automorphism group $\mathrm{PGL}_2(\mathbb{F}_q)$. Can you explicitly write down this rational function f?[2]

2. Transcendence Bases and Transcendence Degree

Let K/F be an extension. A finite set $S = \{x_1, \ldots, x_n\} \subset K$ is **algebraically independent** over F if for the only polynomial $P(t_1, \ldots, t_n) \in F[t_1, \ldots, t_n]$ such that $P(x_1, \ldots, x_n) = 0$ is $P = 0$. An arbitrary set $S \subset K$ is **algebraically independent** if all of its finite subsets are algebraically independent. (To be precise, we must impose some ordering on the elements of S in order to substitute them in as values of an n-variable polynomial, but the definition is obviously independent of the chosen ordering.) We say that K/F is **purely transcendental** if it is of the form $F(S)$ for some algebraically independent subset S of K.

PROPOSITION 10.5. *Let K/F be an extension and $S = \{x_i\}$ be an ordered set of elements of K. The following are equivalent:*

(i) *The natural map $\Phi : F[\{t_i\}] \to K$ given by $t_i \mapsto x_i$ is an injection.*
(ii) *The map Φ extends uniquely to an isomorphism $F(\{t_i\}) \to F(S)$.*
(iii) *S is algebraically independent over F.*

[2]This question is answered in [**Ho20**]. In fact for any subgroup $H \subset \mathrm{PGL}_2(\mathbb{F}_q)$, Hou explicitly computes f_H such that $\mathbb{F}_q(t)^H = \mathbb{F}_q(f_H)$.

A subset S of K/F is a **transcendence basis** if it is algebraically independent and $K/F(S)$ is algebraic. In other words, a transcendence basis for K/F effects a decomposition of K/F into a tower $K/F(S)/F$ of a purely transcendental extension followed by an algebraic extension.

EXAMPLE 10.6. *The empty set is – perhaps by definition – always algebraically independent. If K/F is algebraic, then the only algebraically independent subset is the empty set, which is a transcendence basis.*

LEMMA 10.7. *Let K/F be an extension, $S \subset K$ be algebraically independent, and $x \in K$. Then $S \cup \{x\}$ is algebraically independent if and only if x is transcendental over $F(S)$.*

PROOF. f S is an algebraically independent subset and $x \in K$ is transcendental over $F(S)$, then suppose for a contradiction that $S \cup \{x\}$ were dependent: i.e., there is a finite ordered subset $S_n = (x_1, \ldots, x_n)$ of S and a nonzero polynomial $P \in F[t_1, \ldots, t_n, t_{n+1}]$ such that $P(x_1, \ldots, x_n, x) = 0$. But the transcendence of x over $F(S)$ implies that the polynomial $P(x_1, \ldots, x_n, t_{n+1})$ is identically zero, so that the polynomial $Q(t_1, \ldots, t_n) := P(t_1, \ldots, t_n, 0)$ is not identically zero and $Q(x_1, \ldots, x_n) = 0$, contradicting the independence of $(x_1, \ldots, x_n)$. The other direction is even easier. □

COROLLARY 10.8.

a) *An algebraically independent subset S of K is a transcendence basis if and only if it is not properly contained in any other algebraically independent set.*
b) *Every algebraically independent subset of K is contained in a transcendence basis.*

PROOF. Part a) follows immediately from Lemma 10.7: a maximal algebraically independent set S is precisely one for which $K/F(S)$ is algebraic, i.e., a transcendence basis. Moreover the union of a chain of algebraically independent sets is algebraically independent, so part b) follows from part a) by Zorn's Lemma. □

Applying Corollary 10.8 to $S = \emptyset$, we deduce that every field extension K/F admits a transcendence basis.

EXERCISE 10.7. *Let $\{x_i\}_{i \in S}$ be a transcendence basis for the (nonalgebraic) field extension K/F. Let $n_\bullet : S \to \mathbb{Z}^+$ be any function. Show: $\{x_i^{n_i}\}$ is also a transcendence basis.*

The **transcendence degree** of a field extension K/F is the minimum cardinality of a transcendence basis.

The transcendence degree of an extension is related to $\#K$ and $\#F$ as follows:

PROPOSITION 10.9. *Let K/F be a transcendental field extension, with transcendence degree κ. Then*

$$\#K = \max(\#F, \kappa, \aleph_0).$$

PROOF. Since K/F is transcendental, K is infinite. Moreover, κ and $\#F$ are cardinalities of subsets of K, so clearly $\#K \geq \max(\#F, \kappa, \aleph_0)$. Conversely, let S be a transcendence basis; then $F(S)$ has cardinality $\max(\#, \kappa)$ and $K/F(S)$ is algebraic and $F(S)$ is infinite, so $\#K = \#F(S)$. □

3. Applications to Algebraically Closed Fields

THEOREM 10.10 (Automorphism Extension Theorem). *Let K be an extension of F, with K algebraically closed. Then every automorphism of F can be extended to at least one automorphism of K.*

PROOF. Let $\{x_i\}_{i \in S}$ be a transcendence basis for K/F. There is a unique $\sigma \in \operatorname{Aut} F(S)$ that extends ι and fixes each x_i. Since K is the algebraic closure of $F(S)$, by Corollary 3.11 we can further extend σ to an automorphism of K. □

For any field K, let $\mathbb{F}$ be its prime subfield. An **absolute transcendence basis** for K is a transcendence basis for K/F.

COROLLARY 10.11.

a) *Two algebraically closed fields K_1 and K_2 are isomorphic if and only if they have the same characteristic and the same absolute transcendence degree.*
b) *Suppose K_1, K_2 are two algebraically closed fields of the same characteristic and $\#K_1 = \#K_2$ is uncountable. Then $K_1 \cong K_2$.*

PROOF. Evidently any pair of isomorphic fields $K_1 \cong K_2$ have the same characteristic and absolute transcendence degree. If K_1 is algebraically closed with prime subfield $\mathbb{F}$ and transcendence degree κ, then for a set S of indeterminates of cardinality κ, then K_1 is isomorphic to the algebraic closure of $\mathbb{F}(S)$, which shows that the characteristic and the absolute transcendence degree determine the isomorphism class of an algebraically closed field. Proposition **??** implies that the absolute transcendence degree of any uncountable field is equal to its cardinality, and part b) then follows immediately from part a). □

Remark: The fact that any two algebraically closed fields of given cardinality and, say, continuum cardinality, are isomorphic has important applications in model theory: via the Tarski–Vaught test, it shows that the first order theory of algebraically closed fields of a given characteristic is **complete**.

THEOREM 10.12. *Let K/F be an extension of fields, of transcendence degree κ. The following are equivalent:*

(i) *For any field extension K'/F with transcendence degree $\kappa' \leq \kappa$, there is an F-algebra embedding $K' \hookrightarrow K$.*
(ii) *The field K is algebraically closed.*

EXERCISE 10.8. *Prove Theorem 10.12.*

THEOREM 10.13 (Charnow [**Ch70**]). *Let K be an algebraically closed field. The group $\operatorname{Aut}(K)$ of all automorphisms of K has cardinality $2^{\#K}$.*

PROOF. Step 0: Recall that for any infinite cardinal κ, we have

$$2^\kappa \leq \kappa^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa} = 2^\kappa.$$

Thus $2^{\#K}$ is also the cardinality of the set of all functions from K to K, so is the largest conceivable value of $\#\operatorname{Aut}(K)$.
Step 1: We must check the result for $\overline{\mathbb{F}_p}$ and $\overline{\mathbb{Q}}$. In the former case we have identified the automorphism group as $\hat{\mathbb{Z}}$, which indeed has cardinality $c = 2^{\aleph_0} = 2^{\#\overline{\mathbb{F}_p}}$. In the latter case we can by no means "identify" $\operatorname{Aut}(\overline{\mathbb{Q}})$, but to see that it has continuum

cardinality it suffices, by the automorphism extension theorem, to exhibit a simpler Galois extension $K/\mathbb{Q}$ which has continuum cardinality. Indeed one can take K to be quadratic closure of $\mathbb{Q}$, i.e., the compositum of all quadratic field extensions of $\mathbb{Q}$. The automorphism group here is $(\mathbb{Z}/2\mathbb{Z})^{\aleph_0} = c$.
Step 2: By the automorphism extension theorem, the cardinality of the automorphism group of any algebraically closed field is at least that of the continuum, which by Step 0 gives the answer for all countable fields, i.e., for all fields of countable absolute transcendence degree.
Step 3: Otherwise K is uncountable so there is an absolute transcendence basis S with $\#S = \#K$. Now the natural action of $\mathrm{Sym}(S)$ on S gives rise to an injection $\mathrm{Sym}(S) \hookrightarrow \mathrm{Aut}(\mathbb{F}(S))$, i.e., by permutation of indeterminates. By the automorphism extension theorem, this shows that $\#\mathrm{Aut}(K) \geq \#\mathrm{Sym}(S) = 2^{\#S}$. □

Corollary 10.14. *Let K/F be a field extension, with K algebraically closed. Then $K^{\mathrm{Aut}(K/F)}$ is the purely inseparable closure of F in K. In particular, we have $K^{\mathrm{Aut}(K/F)} = F$ if and only if F is perfect.*

Proof. If x lies in the purely inseparable closure of F in K, then for some $e \in \mathbb{Z}^+$, $x^{p^e} \in F$. Since x has no Galois conjugates, we must have $\sigma(x) = x$ for every $\sigma \in \mathrm{Aut}(K/F)$. Let $\overline{F}$ be the algebraic closure of F in K. By the usual Galois theory we have $\overline{F}^{\mathrm{Aut}(\overline{F}/F)}$ is the purely inseparable closure of F in $\overline{F}$, and by the automorphism extension theorem we conclude that $K^{\mathrm{Aut}(K/F)} \cap \overline{F}$ is the purely inseparable closure of F in K. If $x \in K$ is transcendental over F, then by Corollary 10.8b) there is a transcendence basis $S = (x, \{x_\alpha\})$ containing x. By Exercise 10.12, also $S' = (x^2, \{x_\alpha\})$ is a transcendence basis, so there is an automorphism $F(S) \to F(S')$ sending $x \mapsto x^2$, which, as usual, extends to an F-algebra automorphism σ of K with $\sigma(x) = x^2 \neq x$. □

Let us return to the Galois connection attached to a field extension as discussed at the beginning of Chapter 7: let K/F be a field extension, let $\mathcal{L}(K/F)$ be the lattice of subextensions L of K/F, let $G \coloneqq \mathrm{Aut}(K/F)$, and let $\mathcal{L}(G)$ be the lattice of sugroups of G. Then the maps

$$\mathcal{L} : \mathcal{L}(G) \to \mathcal{L}(K/F),\ H \mapsto L^H$$

and

$$\mathcal{H} : \mathcal{L}(K/F) \to \mathcal{L}(G),\ L \mapsto \mathrm{Aut}(K/L)$$

give an antitone Galois connection, hence an antitone bijection between the sublattices of closed subextensions and closed subgroups. Let us say that K/F is **perfectly Galois** if this Galois connection is perfect: that is, every subextension of K/F and every subgroup of G is cloed, and thus $\mathcal{L}$ and $\mathcal{H}$ are mutually inverse antitone bijections. As mentioned above, it turns out that K/F is perfectly Galois if and only if it is finite Galois. The proof that I know of this uses a bit of arithmetic geometry so cannot be given here, but we saw in Chapter 7 that an algebraic Galois extension of infinite degree is not perfectly Galois. However such an extension is the next best thing: every subextension L of K/F is closed, so the lattice $\mathcal{L}(K/F)$ is in anti-isomorphic to the lattice of closed subgroups of $\mathcal{H}(G)$ (and in this case, we can construe "closed" to mean closed in the Krull topology). Let us call a field extension **Dedekind** if it has this property: equivalently, every subextension L of K/F is of the form K^H for at least one subgroup H of G (and then the closure of any such H is $\mathrm{Aut}(K/L)$). Then Corollary 10.14 gives another class of Dedekind

extensions: K/F is Dedekind if K is algebraically closed of characteristic 0 (since then perfectness is automatic).

We claim that in positive characteristic there are no transcendental Dedekind extensions. Indeed, let F be a field of characteistic $p > 0$, and let K/F be a transcendental field extension, so there is $t \in K$ that is transcendental over F. Seeking a contradiction, suppose that K/F is Dedekind: then $K^{\mathrm{Aut}(K/F(t))} = F(t)$. Since $F(t^p) \subseteq F(t)$, we have an inclusion of subgroups of G: $\mathrm{Aut}(K/F(t))) \subseteq \mathrm{Aut}(K/F(t^p))$. Let $\sigma \in \mathrm{Aut}(K/F(t^p))$. Then σ fixes $F(t^p)$ pointwise, so it pointwise fixes the coefficients of the polynomial $X^p - t^p \in F(f^p)[x]$ and therefore it permutes the roots of this polynomial. But the only root of this polynomial in an algebraic closure of $F(t^p)$ is t, so $\sigma(t) = t$. It follows that $\mathrm{Aut}(K/F(t)) = \mathrm{Aut}(K/F(t^p))$ and thus

$$F(t) = K^{\mathrm{Aut}(K/F(t))} = K^{\mathrm{Aut}(K/F(t^p))} \supsetneq F(t^p),$$

so K/F is not in fact a Dedekind extension.

Exercise 10.9.

a) *Let K/F be a nontrivial purely transcenendental extension, and let K^{sep} be the separable closure of K. Show: $\mathfrak{g}_K := \mathrm{Aut}(K^{\mathrm{sep}}/K)$ is infinite.*

b) *Let F be a field of characteristic 0, let K/F be a transcendental field extension with K algebraically closed, and let T be a transcendence basis for K/F. Show: $K/F(T)$ is an algebraic Galois extension of infinite degree.*

c) *Let K/F be a perfectly Galois extension, and let L be a subextension of K/F. Show: K/L is perfectly Galois.*

d) *Show: if K/F is a transcendental extension of fields of characteristic 0 with K algebraically closed, then K/F is* not *perfectly Galois.*

In fact algebraic Galois extensions, and extensions where the top field is algebraically closed of characteristic 0 are the only known Dedekind extensions.

Another fact which is true about automorphism groups of algebraically closed field extensions K/F is that any bijection φ between algebraically independent subsets I and I' of K extends to an F-automorphism of F. For this it is necessary and sufficient that φ extend to a bijection on transcendence bases $S \supseteq I$, $S' \supseteq I'$. This holds provided that all transcendence bases of K/F have the same cardinality. This brings us to the next section.

4. An Axiomatic Approach to Independence

We wish to prove the following result.

Theorem 10.15. *Let K/F be a field extension. Then any two transcendence bases for K/F have the same cardinality, so that the transcendence degree of K/F is the cardinality of* any *transcendence basis.*

Of course this is strikingly similar to the situation in ordinary linear algebra. We could therefore go back to our linear algebra texts, consult the proof of the cardinality independence of bases in vector spaces, and attempt to mimic it in the present context. This approach will succeed. Of course in order to do this we will have to find some sort of precise analogy between linear independence and algebraic independence. In mathematics, once we determine that situations A and B

are analogous (to the extent that certain proofs can be carried over from one context to the other), do we just dutifully copy down the similar proofs and keep the analogy in the back of our mind in case we need it later? Depending on taste, this is a reasonable approach to take, perhaps more reasonable for the mind which is able to quickly remember what it once knew. As for myself, I would at the same time worry that it would take me some time and energy to recreate the analogy if I hadn't written it down, and I would also be curious whether A and B might be common instances of a more general construction that it might be interesting or useful to know explicitly. So we shall follow the second course here, with apologies to those with different tastes.

Let us begin by placing alongside the analogies between linear independence of a subset S of an F-vector space V and algebraic independence of a subset S of an F-algebra K.

In both contexts we have a set, say X, and a collection of subsets S of X that we are calling **independent**, subject to:

(LI1) The empty set is independent.
(LI2) A set is independent if and only if all its finite subsets are independent.
(LI3) Any subset of an independent set is independent.

Notice that it follows from (LI2) and (LI3) that the union $S = \bigcup_i S_i$ of any chain of independent subsets is independent: if not, there would exist a finite dependent subset S' of S, but S' would have to be a subset of some S_i, contradicting the independence of S_i. Combining this with (LI1) and aplying Zorn's Lemma, we get

(A) Maximal independent sets exist, and every independent set is contained in some maximal independent set.

Could it be that (LI1) through (LI3) imply the following desirable property?

(B) All maximal independent sets have the same cardinality.

Unfortunately this is not the case. Suppose we have a set X which is partitioned into disjoint subsets:

$$X = \coprod_i X_i.$$

Call a subset $S \subset X$ independent if and only if it is contained in X_i for some i. Then (LI1) through (LI3) are satisfied and the maximal independent sets are simply the X_i's, which we are evidently not entitled to conclude have the same cardinality.

So we need another axiom. Consider the following:

(LI4) If S_1 and S_2 are independent subsets of X with $\#S_1 < \#S_2$, then there exists $x \in X \setminus S_1$ such that $S_1 \bigcup \{x\}$ is independent.

A set X equipped with a family of subsets $\{S_i\}$ satisfying axioms (LI1) through (LI4) is called an **independence space**.

In an independence space, if S_1 and S_2 are independent sets with $\#S_1 < \#S_2$, then S_1 is non-maximal. Therefore a maximal independent set has cardinality at least as large as any other independent set, so by symmetry all maximal independent sets have the same cardinality: independence spaces satisfy (B). Conversely, (LI1) through (LI3) and (B) clearly imply (LI4).

In this new language, Theorem 10.15 takes the form

THEOREM 10.16. *If K/F is a field extension, then the collection of algebraically independent subsets of K is an independence space.*

Unfortunately it is not so obvious how to show that the collection of algebraically independent subsets of K satisfies (LI4). So let us try a different approach, in terms of something called spanning sets. We notice that to each subset S of a vector space its linear span $\overline{S}$ gives an abstract closure operator: namely we have

(SO1) = (CL1) $S \subset \overline{S}$
(SO2) = (CL2) $S \subset S' \implies \overline{S} \subset \overline{S'}$
(SO3) = (CL3) $\overline{\overline{S}} = \overline{S}$.

But the linear span satisfies two other properties, the first of which is not surprising in view of what has come before:

(SO4) if $x \in \overline{S}$, there exists a finite subset $S' \subset S$ such that $x \in \overline{S'}$.

Famously, linear span also satisfies the following **Exchange Lemma**:[3]

(SO5) If $y \in \overline{S \cup x}$ and y is *not* in $\overline{S}$, then $x \in \overline{S \cup y}$.

(Proof: If $y \in \overline{S \cup x}$, there exist $s_1, \ldots, s_n \in S$ and scalars $a_1, \ldots, a_n, a$ such that $y = a_1 s_1 + \ldots + a_n s_n + ax$. If y is not in the span of S, then $a \neq 0$, so $x = y - \frac{-a_1}{a} s_1 + \ldots + \frac{-a_n}{a} s_n \in \overline{S \cup y}$.)

Now, suppose K/F is a field extension and S is a subset of K. We will define $\overline{S}$ to be the algebraic closure of $F(S)$ in K. It is immediate that this "algebraic closure" operator satisfies (SO1) through (SO4). Let us check that it also satisfies (SO5): suppose $y \in \overline{S \cup x}$ and y is not in the algebraic closure of S. Then there exists a finite subset $x_1, \ldots, x_n$ of S such that y is algebraic over $F(x_1, \ldots, x_n, x)$: i.e., there exists a polynomial $f(t_1, \ldots, t_n, t_{n+1}, t_{n+2})$ with F-coefficients such that $f(x_1, \ldots, x_n, x, t_{n+2}) \neq 0$ and $f(x_1, \ldots, x_n, x, y) = 0$. Writing

$$f(x_1, \ldots, x_n, t_{n+1}, t_{n+1}) = \sum_{i=0}^{g} A_i(x_1, \ldots, x_n, t_{n+2}) t_{n+1}^i,$$

[3]This is an absolutely prototypical example of a *lemma*: the exchange lemma is the essential kernel of content in the theory of linearly independence, and yet it is itself not very memorable or appealing, so is doomed to be overshadowed by the figurehead theorems that it easily implies.

observe that not all the polynomials $A_i(x_1, \ldots, x_n, t_{n+2})$ can be zero. Since y is not algebraic over $F(S)$, it follows that not all of the elements $A(x_1, \ldots, x_n, y)$ are zero, and therefore $f(x_1, \ldots, x_n, t_{n+1}, t_{n+1}, y) \neq 0$. Since $f(x_1, \ldots, x_n, x, y) = 0$, it follows that x is algebraic over $F(S, y)$ as asserted.

Suppose again that X is any set equipped with a **spanning operator** $S \mapsto \overline{S}$, i.e., an operator satisfying the three closure axioms (CL1) through (CL3) and also (CL4) and (CL5). A subset S of X is a **spanning set** if $\overline{S} = X$. A subset S of X is **independent** if for all $s \in S$, s is not in $\overline{S \setminus s}$. A **basis** is an independent spanning set.

Note that it is immediate to show that the independent sets for a spanning operator satisfy (LI1) through (LI3). In particular, we have (A), that bases exist and any independent set is contained in a basis. Again it is not obvious that (LI4) is satisfied. Rather we will show (B) directly – which is what we really want anyway – and by the above remarks that implies (LI4).

In the following results X is always a set equipped with a spanning operator $S \mapsto \overline{S}$.

PROPOSITION 10.17. *For a subset $S \subseteq X$, the following are equivalent:*

(i) *S is a minimal spanning set of X.*
(ii) *S is a maximal independent set of X.*
(iii) *S is a basis.*

PROOF. (This is the usual thing.) (i) $\implies$ (iii): Suppose S is minimal spanning but not dependent; then by definition there exists $s \in S$ such that $x \in \overline{S \setminus s}$), so that $\overline{S \setminus s}$, being a closed set containing S, also contains the closure of S, i.e., X, and we found a smaller spanning set. (iii) $\implies$ (ii): if S is a basis and $S \cup \{x\}$ is independent then x does not lie in $\overline{S}$ which is absurd since S is a spanning set. (ii) $\implies$ (i) is similar: if S were a maximal independent set but not a spanning set, then there exists $x \in X \setminus \overline{S}$ and then $S \cup \{x\}$ is independent. □

THEOREM 10.18. *Let S be an independent subset of X and T a spanning set. There exists a subset $T' \subset T$ such that $S \cup T'$ is a basis and $S \cap T' = \emptyset$.*

PROOF. Let $\mathcal{I}$ be the collection of all subsets T' of T such that $S \cap T' = \emptyset$ and $S \cup T'$ is indepdendent. Observe that $\emptyset \in \mathcal{I}$, so $\mathcal{I}$ is not itself empty. As usual, $\mathcal{I}$ is closed under unions of increasing chains so by Zorn's Lemma has a maximal element T'. Let $x \in T$, and suppose that x is not in $\overline{S \cup T'}$. Then $T'' := T' \cup \{x\}$ is a strictly larger subset of T such that $S \cup T''$ is still independent, contradicting the maximality of T'. Therefore

$$X = \overline{T} \supset \overline{\overline{S \cup T'}} = \overline{S \cup T'},$$

so $S \cup T'$ is a basis. □

COROLLARY 10.19. *If X admits a finite spanning set, it admits a finite basis.*

PROOF. Apply Theorem 10.18 with $S = \emptyset$. □

THEOREM 10.20. *Any two bases B, B' of X have the same cardinality.*

PROOF. Case 1: Suppose $B = \{x_1, \ldots, x_n\}$ is a finite basis, and let B' be any other basis. Let $m = \#B \cap B'$. If $m = n$ then $B \subset B'$ and by Proposition 10.17 distinct bases are at least incomparable, so $B = B'$. So suppose (WLOG) that $B \cap B' = \{x_1, \ldots, x_m\}$ with $m < n$. The set $B \setminus x_{m+1}$ cannot be a spanning set, whereas B' is, so there exists $y \in B'\overline{B \setminus x_{m+1}}$. The set $B_1 := (B \setminus x_{m+1}) \cup y$ is independent. By the Exchange Lemma (SO5), $x_{m+1} \in \overline{(B_1)}$. Hence $B \subset \overline{B_1}$, and since B is a spanning set, so is B_1. Thus B_1 is a basis. Notice that B_1 has n elements and also $\{x_1, \ldots, x_m, y\} \subset B_1 \cap B'$, so that we have replaced B by another basis of the same cardinality and sharing at least one more element with B'. Repeating this procedure will produce a finite sequence of bases B_2, B_3, each of cardinality n, such that the last basis B_k is contained in, and thus equal to, B'.

Case 2: We may now suppose that B and B' are both infinite. For every $x \in X$, we claim the existence of a subset E_x with the property that $x \in \overline{E_x}$ and for any subset E of B such that $x \in \overline{E}$, $E_x \subset E$. Assuming the claim for the moment, we complete the proof. Consider the subset $S = \bigcup_{x \in B'} E_x$ of B. Since each E_x is finite, $\#S \leq \#B'$. On the other hand, for all $x \in B'$, $x \in \overline{E_x} \subset \overline{S}$, so $B' \subset \overline{S}$ and therefore $\overline{S} \supset \overline{B'} = X$. Therefore S is a spanning subset of the basis B, so $S = B$ and thus $\#B \leq \#B'$. By reversing the roles of B and B' in the argument we conclude $\#B = \#B'$.

It remains to prove the claim on the existence of E_x. In turn we claim that if E' and E'' are two subsets of B such that $x \in \overline{E'} \cap \overline{E''}$ and x is not in the span of any proper subset of E', then $E' \subset E''$; this certainly suffices. Assuming to the contrary that there exists $y \in E' \setminus E''$. Then x is not in the span of $E' \setminus y$ and is in the span of $(E' \setminus y) \cup y$, so by (SO5) y is in the span of $(E' \setminus y) \cup x$. Since x is in the span of E'', we get that y is in the span of $(E' \setminus y) \cup E''$. But this contradicts the fact that the $(E' \setminus y) cup E'' \cup \{y\}$, being a subset of B, is independent. □

Remark: A set X endowed with a spanning operator as above is often called a **finitary matroid**. (The word "finitary" refers to (SO4).) Combinatoricists are especially interested in finite matroids, which includes the class of finite-dimensional vector spaces over finite fields but not that of independent subsets of a field extension (except in the trivial case of an algebraic field extension).

For future reference, for a field extension L/K, we will refer to the matroid with sets the subsets of L, spanning operator $S \mapsto \overline{S}$ the algebraic closure of $K(S)$ in L and (it follows) with independent sets the algebraically independent subsets the **transcendence matroid of L/K**.

We saw above how to go from a finitary matroid to an independence space, namely by decreeing a subset $S \subset X$ to be dependent if there exists $x \in S$ such that $x \in \overline{S \setminus x}$. Conversely, to every independence space we can associate a finitary matroid: define the span $\overline{Y}$ of a subset Y to be the set of $x \in X$ such that $S \cup x$ is dependent. This complete equivalence between concepts of linear independence and spanning seems a bit unexpected, even in the context of vector spaces.

For finite matroids, combinatorialists know at least half a dozen other equivalent

axiomatic systems: e.g. in terms of graphs, circuits, "flat" subspaces and projective geometry. As above, demonstrating the equivalence of any two of these systems is not as easy as one might expect. This phenomenon of multiple nonobviously equivalent axiomatizations has been referred to, especially by G. Rota, as **cryptomorphism**. Of course every twenty-first century student of mathematics has encountered crytomorphism (although it seems that the multiplicity is especially large for finite matroids!). In several essays, Rota saw cryptomorphism as a warning not to take any particular axiomatization of a theory or structure too seriously. This seems fair, but since the different axiomatizations can lead to different and possibly easier proofs, perhaps it should also be viewed as an instance of the inherent richness of mathematical concepts.

5. More on Transcendence Degrees

PROPOSITION 10.21. *Let L/K be a field extension and T a subset of L such that $L = K(T)$. Then* $\mathrm{trdeg}(L/K) \leq \#T$.

PROOF. In the transcendence matroid of L/K, T is a spanning set. According to Theorem 10.18 with $S = \varnothing$, some subset T' of T is a basis for the matroid, i.e., a transcendence basis for L/K. Thus

$$\mathrm{trdeg}(L/K) = \#T' \leq \#T. \qquad \square$$

THEOREM 10.22. *Let $F \subset K \subset L$ be a tower of field extensions.*

a) *If $\{x_i\}_{i\in I}$ is a transcendence basis for K/F and $\{y_j\}_{j\in J}$ is a transcendence basis for L/K, then $\{x_i, y_j\}$ is a transcendence basis for L/F.*
b) *We have* $\mathrm{trdeg}(L/F) = \mathrm{trdeg}(L/K) + \mathrm{trdeg}(K/F)$.

PROOF. a) We first show that $\{x_i, y_j\}$ is an algebraically independent set. Choose any finite subsets of $\{x_i\}$ and $\{y_j\}$: for ease of notation, we rename the elements $x_1, \ldots, x_m, y_1, \ldots, y_n$. Suppose there exists a polynomial $P \in F[t_1, \ldots, t_{m+n}]$ such that $P(x_1, \ldots, x_m, y_1, \ldots, y_n) = 0$. Put

$$Q(t_1, \ldots, t_n) \coloneqq P(x_1, \ldots, x_m, t_1, \ldots, t_n) \in K[t].$$

Then $Q(y_1, \ldots, y_n) = 0$ implies $Q(t_1, \ldots, t_n) = 0$. Each coefficient of this polynomial is a polynomial expression in $x_1, \ldots, x_m$ with F-coefficients, and the algebraic independence of the x_i's implies that each of these coefficients is equal to 0. Thus $P = 0$. Let $K_0 = F(\{x_i\})$, so K/K_0 is algebraic. Let $L_0 = K(\{y_j\}$, so L/L_0 is algebraic. Let $z \in L$. Then z satisfies a polynomial equation with coefficients in L_0. Since K/K_0 is algebraic, z also satisfies a polynomial equation with coefficients in $K_0(\{y_j\}) = F(\{x_i, y_j\})$.
b) By part a), $\{x_i, y_j\}$ is a transcendence basis for L/F, of cardinality $\#I + \#J = \mathrm{trdeg}(K/F) + \mathrm{trdeg}(L/K)$. $\square$

EXERCISE 10.10. *Let K, L be subetensions of a field extension M/F. Suppose K/F has finite degree and L/F is purely transcendental. Show $[LK : L] = [K : F]$. (Suggestion: reduce to the case $K = F[t]/(p(t))$ and $L = F(t)$. For this case, if the polynomial $p(t)$ factors over $F(t)$, then by taking $t = a$ for $a \in F$ we get a factorization over F. One has to be a little careful here in order to avoid values a which make the denominator of one of the rational functions equal to 0.)*[4]

[4]This result will become much more clear following our later discussion of **linear disjointness**. The reader may prefer to defer the exercise until then.

THEOREM 10.23.
For $F \subseteq K \subseteq L$ a tower of field extensions, the following are equivalent:

(i) *Both extensions K/F and L/K are finitely generated.*
(ii) *The extension L/F is finitely generated.*

PROOF. (i) $\implies$ (ii): If $K = F(x_1, \ldots, x_m)$ and $L = K(y_1, \ldots, y_n)$, then $L = F(x_1, \ldots, x_m, y_1, \ldots, y_n)$.
(ii) $\implies$ (i): It is immediate that if L/F is finitely generated then so is L/K for any subextension K of L/F: any finite generating set for L/F is also a finite generating set for L/K. Let $z_1, \ldots, z_e$ be a transcendence basis for K/F. Then $F(z_1, \ldots, z_e)/F$ is finitely generated, so it suffices to show that the algebraic extension $K/F(z_1, \ldots, z_e)$ is finitely generated. Moreover, $L/F(z_1, \ldots, z_e)$ is finitely generated, so it is enough to prove the result with $F(z_1, \ldots, z_e)$ in place of F and thus we may assume that K/F is algebraic.

We are thus reduced to showing: if $L/K(t_1, \ldots, t_n)$ is a finite extension of a rational function field and K/F is an algebraic extension, then L/F finitely generated implies K/F finitely generated – or, equivalently since K/F is algebraic – that K/F is finite. But suppose not: then for all $d \in \mathbb{Z}^+$ there exists a subextension K_d of K/F such that $[K_d : F] \geq d$. By the preceding exercise we have $[K_d(t_1, \ldots, t_n) : F(t_1, \ldots, t_n)] = [K_d : F] \geq n$. Thus $L/F(t_1, \ldots, t_n)$ is an algebraic extension but

$$[L : F(t_1, \ldots, t_n)] \geq [K(t_1, \ldots, t_n) : F(t_1, \ldots, t_n) \geq \aleph_0,$$

so it is algebraic of infinite degree, hence not finitely generated: contradiction! □

EXERCISE 10.11. *Let k be any field. Consider the polynomial ring $R = k[x, y]$: note that it is finitely generated as a k-algebra. Show that there is a k-subalgebra of R which is* not *finitely generated. (Thus Theorem 10.23 exhibits a property of field extensions without analogue in the study of commutative rings.)*

EXERCISE 10.12. *For a field extension L/K, show the following are equivalent:*

(i) *The subfield lattice of L/K is Noetherian: there are no infinite chains*

$$K = F_0 \subsetneq F_1 \subsetneq \ldots F_n \subsetneq \ldots \subset L.$$

(ii) *The extension L/K is finitely generated.*

CHAPTER 11

Linear Disjointness and Separability

1. Definition and First Properties

Let E/F be a field extension, and let R, S be F-subalgebras of E. We say that R and S are **F-linearly disjoint in E** if the canonical map $R \otimes_F S \to E$ is injective. (If the *ambient field* E is understood, we will just say that R, S are F-linearly disjoint, or that they are **linearly disjoint over F**. In fact the dependence on E is often suppressed, for reasons that will be explored soon enough.)

LEMMA 11.1. *Let E/F be a field extension, and let K, L be subextensions of finite degree over F. Then K and L are linearly disjoint over F if and only if $[KL : F] = [K : F][L : F]$.*

PROOF. Since K and L are finite-dimensional over F, the compositum KL is the F-algebra generated by K and L, so the canonical map $\tau : K \otimes_F L \to KL$ is always surjective. Since its source and target are both finite-dimensional F-vector spaces, τ is injective if and only if

$$[K : F][L : F] = \dim_F K \otimes_F L = \dim_F LK. \qquad \square$$

EXERCISE 11.1. *Let K, L be finite degree extensions of a field F of coprime degrees. Show: K, L are F-linearly disjoint.*

LEMMA 11.2. *If R, S are F-linearly disjoint in E, then $R \cap S = F$.*

PROOF. By contraposition: suppose there exists $u \in (R \cap S) \setminus F$. We may then choose F-bases A of R and B of S such that $\{1, u\} \subset A \cap B$. The elements $1 \otimes u$ and $u \otimes 1$ are then F-linearly independent in $R \otimes_F S$ but under $\iota : R \otimes_F S \to E$ they both get mapped to u, so ι is not injective. $\square$

EXERCISE 11.2.

a) *Let $F = \mathbb{Q}$ and $E = \mathbb{C}$. Show: $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}(e^{\frac{2\pi i}{3}}\sqrt[3]{2})$ are not linearly disjoint over F, even though $K \cap L = F$.*

b) *Try to generalize the result of part a), for instance as follows: if K/F is algebraic and* not *normal, then inside any algebraic closure E of K there exists a field extension L/F such that $K \cap L = F$ but K, L are not F-linearly disjoint in E.*

EXERCISE 11.3. *Let R, S be F-subalgebras of E/F. Show that the following are equivalent:*

(i) *R and S are linearly disjoint over F.*

(ii) *For all F-linearly independent subsets $\{a_i\}_{i \in I}$ of R and $\{b_j\}_{j \in J}$ of S, $\{a_i b_j\}_{(i,j) \in I \times J}$ is F-linearly independent in E.*

(iii) *For all $m, n \in \mathbb{Z}^+$, if $a_1, \ldots, a_m$ are F-linearly independent in R and $b_1, \ldots, b_n$ are F-linearly independent in S, then $a_1b_1, \ldots, a_m, b_1, a_2b_1, \ldots, a_mb_n$ are F-linearly independent in E.*

EXERCISE 11.4. *(Linear disjointness is preserved by direct limits) Let R be an F-subalgebra of E/F. Suppose $R = \varinjlim R_i$ is a direct limit of a family $\{R_i\}_{i \in I}$ of F-subalgebras. Show: for any F-subalgebra S of E/F, R and S are linearly disjoint if and only if for all $i \in I$, R_i and S are linearly disjoint.*

EXERCISE 11.5. *Let E/F be a field extension, and let R and S be linearly dsijoint F-subalgebras of E. Let $R' \subseteq R$ and $S' \subseteq S$ be F-subalgebras. Show: R' and S' are linearly disjoint over F.*

LEMMA 11.3. *Two subalgebras R and S of E/F are linearly disjoint over F if and only if the subfields they generate, say K and L, are linearly disjoint over F.*

PROOF. Suppose that R and S are linearly disjoint over F. It is enough to show that if $k_1, \ldots, k_m$ are F-linearly independent elements of K and $l_1, \ldots, l_n$ are F-linearly independent elements of L, then $\{k_il_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$ are F-linearly independent in E. There exist $a, a_1, \ldots, a_m \in R$ such that $k_i = \frac{a_i}{a}$ for all i, and simiarly there exist $b, b_1, \ldots, b_n \in S$ such that $l_j = \frac{b_j}{b}$ for all j. Then if $\alpha_{ij} \in F$ is such that $\sum_{i,j} \alpha_{ij} \frac{a_ib_j}{ab} = 0$, then multiplying by ab gives $\sum_{i,j} \alpha_{ij}a_ib_j = 0$, and by assumption $\alpha_{ij} = 0$ for all i and j.
The converse is immediate from Exercise 11.5. □

Thus it is no loss of generality to speak of linear disjointness of sub*fields* of E/F, but it is often convenient to phrase things in terms of subdomains of these fields.

PROPOSITION 11.4. *Let K, L be subextensions of a field extension E/F. The following are equivalent:*

(i) *K and L are linearly disjoint over F.*
(ii) *Every F-linearly independent subset S of K is L-linearly independent in E.*
(ii′) *Every F-linearly independent subset T of L is K-linearly independent in E.*
(iii) *There is an F-basis A of K which is L-linearly independent as a subset of E.*
(iii′) *There is an F-basis B of L which is K-linearly independent as a subset of E.*

PROOF. (i) $\implies$ (ii): Let A be F-linearly independent in K. Consider any finite subset of elements of A, say $k_1, \ldots, k_n$, and let $\beta_1, \ldots, \beta_n \in L$ be such that

$$\beta_1k_1 + \ldots + \beta_nk_n = 0. \tag{39}$$

Choose an F-basis $\{l_j\}_{j \in J}$ for L, so that there are unique $\alpha_{ij} \in F$ such that for all i, $\beta_i = \sum_j \alpha_{ij}l_j$. Substituting this into (39) gives

$$\sum_{i,j} \alpha_{ij}k_il_j = 0.$$

By Exercise 11.3 this forces $\alpha_{ij} = 0$ for all i, j and thus $\beta_j = 0$ for all k, so the k_i's are L-linearly independent.
(i) $\implies$ (ii′): The above proof works with the roles of K and L reversed.

(ii) $\implies$ (i): By Exercise 11.3, it is enough to fix $m, n \in \mathbb{Z}^+$ let $k_1, \ldots, k_m$ be F-linearly independent elements of K and $l_1, \ldots, l_n$ be F-linearly independent elements of L and show that $\{k_i l_j\}$ are F-linearly independent elements of E. Suppose that $\alpha_{ij} \in F$ are such that $\sum_{i,j} \alpha_{ij} k_i l_j = 0$. But we may rewrite this as

$$(\alpha_{11} l_1 + \ldots + \alpha_{1n} l_n) k_1 + \ldots + (\alpha_{m1} l_1 + \ldots + \alpha_{mn} l_n) k_m = 0.$$

By hypothesis the k_i's are L-linearly independent, so this forces all the coefficients of the above equation to be equal to zero, which in turn, since the l_j's are F-linearly independent, forces all the α_{ij}'s to be zero.
(ii$'$) $\implies$ (i) in the same way.
(ii) $\implies$ (iii) and (ii$'$) $\implies$ (iii$'$) are immediate.
(iii) $\implies$ (ii): Let S be an F-linearly independent subset of K, and complete it to a basis A' of K. Let $\varphi : A' \to A$ be a bijection and Φ the induced F-linear automorphism of K. Suppose that A' is not L-linearly independent, i.e., there exists a finite subset $a_1', \ldots, a_n'$ of A' and $\beta_1, \ldots, \beta_n \in L$, not all zero, such that $\sum_i \beta_i a_i' = 0$. Applying Φ to this relation gives $\sum_i \beta_i a_i = 0$, so that A is not L-linearly independent, contradiction. Thus A' is L-linearly independent independent and *a fortiori* so is its subset S.
(iii$'$) $\implies$ (ii$'$) in the same way. □

REMARK 11.1. *Some sources take condition (ii) of Proposition 11.4 to be the definition of linear disjointness. This has the advantage of not requiring any knowledge of tensor products on the part of the reader. All the other advantages, however, seem to lie with the tensor product definition. For instance, it is clearly symmetric with respect to K and L.*

EXERCISE 11.6. *Let K, L be subfields of E/F, and let R be an F-subalgebra of K with fraction field K. Suppose that there exists a K-basis of R which is L-linearly independent in E. Show that K, L are F-linearly disjoint in E.*

THEOREM 11.5. *Let C/F be a field extension, and let K, L, M be subextensions of C/F with $K \subseteq M$. The following are equivalent:*

(i)) *We have that M and L are linearly disjoint over F.*
(ii) *We have:*
  a) *The fields K and L are linearly disjoint over F, and*
  b) *The fields M and KL are linearly disjoint over K.*

PROOF. We consider the F-algebra maps

$$M \otimes_F L \xrightarrow{\iota} M \otimes_K (K \otimes_F L) \xrightarrow{\varphi_1} M \otimes_K K[L] \xrightarrow{\varphi_2} M[L].$$

The map ι is an isomorphism: this a special case of the "telescoping tensor identity"

$$M \otimes_T (T \otimes_R P) \cong M \otimes_R P$$

valid for a homomorphism $R \to T$ of commutative rings, an R-module P and a T-module M. In this particular case it can be seen as follows: if $\{m_i\}_{i \in I}$ is a K-basis for M and $\{\alpha_j\}_{j \in J}$ is an F-basis for K, then $\{\alpha_j m_i \mid (i,j) \in I \times J\}$ is an F-basis for M, so if $\{l_x\}_{x \in X}$ is an F-basis for L, then $\{(\alpha_j m_i) \otimes l_x \mid (i,j,x) \in I \times J \times X\}$ is an F-basis for $M \otimes_F L$. This maps under ι to $(\alpha_j m_i) \otimes (1 \otimes l_x) = \alpha_j (m_i \otimes (1 \otimes l_x))$, which is an F-basis for $M \otimes_K (K \otimes_F L)$ since $m_i \otimes (1 \otimes l_x)$ is a K-basis for $M \otimes (K \otimes_F L)$. The composition of these maps is the natural multiplication map

$$\varphi : M \otimes_F L \to M[L],$$

so in all cases we have that φ_1, φ_2 and φ are surjective.
(i) $\implies$ (ii): Suppose M and L are linearly disjoint over F: thus φ is an isomorphism. Since we have that $\varphi = \varphi_2 \circ \varphi_1 \circ \iota$, that ι is an isomorphism and that φ_1 and φ_2 surjective, we deduce that $\varphi_2 \circ \varphi_1$ is an isomorphism, hence φ_1 is injective, hence φ_1 is an isomorphism, hence φ_2 is an isomorphism. Because M is a nonzero K-vector space, the injectivity of φ_1 implies the injectivity of $K \otimes_F L \to K[L]$, so K and L are linearly disjoint over F. The injectivity of φ_2 implies that M and $K[L]$ are linearly disjoint over K, which by Lemma 11.3 implies that M and KL are linearly disjoint over F.
(ii) $\implies$ (i): If K and L are linearly disjoint over F, then φ_1 is injective. If M and KL are linearly disjoint over K then by Exercise 11.5 we have that M and $K[L]$ are linearly disjoint over K, so φ_2 is injective. Therefore φ is injective, so M and L are linearly disjoint over F. □

2. Intrinsic Nature of Linear Disjointness

The definiton of linear disjointness is initially hard to process because it involves four different algebras. In fact the dependence of the definition on the "ambient" field E is in many cases rather weak. One easy of instance of this is given in the following exercise.

EXERCISE 11.7. *Let K, L be subextensions of a field extension E/F, and let E'/E be any field extension. Show: K, L are F-linearly disjoint as subfields of E if and only if they are F-linearly disjoint as subfields of E'.*

We now look more deeply into the dependence on the ambient field E, following a MathOverflow discussion led by Andrew Critch. Let F be a field, and let K, L be field extensions of F. We say that K, L are **somewhere linearly disjoint over F** if there exists a field extension E/F and F-algebra embeddings of K and L into E such that K, L are F-linearly disjoint in E. Further, we say that K, L are **everywhere linearly disjoint over F** if for all field extensions E/F and all F-algebra embeddings of K, L into E, K, L are F-linearly disjoint in E.

Certainly we want everywhere linearly disjoint over F to imply somewhere linearly disjoint over F. To see this there is a minor technicality to be disposed of, which is treated in the next exercise.

EXERCISE 11.8.

a) *Let F be a field and K, L be field extensions of F. Show: there is a field extension E and F-algebra embeddings of K and L into E. Show that for instance one may take E to be any algebraically closed field such that* $\operatorname{trdeg}(E/F) \geq \max \operatorname{trdeg}(K/F), \operatorname{trdeg}(L/F)$.
b) *Deduce: if K, L are everywhere linearly disjoint over F then they are somewhere linearly disjoint over F.*

EXERCISE 11.9. *Let F be any field, and put $K = L = F(t)$.*

a) *Take $E = F(t)$ to show that K, L are not everywhere linearly disjoint.*
b) *Take $E = F(a, b)$ (rational function field in two variables) to show that K and L are somewhere linearly disjoint.*

PROPOSITION 11.6. *Let F be a field, and let K and L be field extensions of F. The following are equivalent:*

(i) *The fields K, L are somewhere F-linearly disjoint.*
(ii) *The tensor product $K \otimes_F L$ is a domain.*

PROOF. If $K \otimes_F L$ can be embedded into a field, then it is a domain. Conversely, if $K \otimes_F L$ is a domain, it can be embedded into its fraction field. □

PROPOSITION 11.7. *Let F be a field, and let K and L be field extensions of F. The following are equivalent:*

(i) *The fields K, L are everywhere F-linearly disjoint.*
(ii) *$K \otimes_F L$ is a field.*

PROOF. (i) $\implies$ (ii): In order to show that the (evidently nonzero, since it contains F) ring $R = K \otimes_F L$ is a field, it suffices to show that the only maximal ideal is (0). So let $\mathfrak{m}$ be a maximal ideal of R. Then $E = R/\mathfrak{m}$ is a field extension of K, L and the induced map $K \otimes_F L \to E$ is precisely the quotient map $R \to R/\mathfrak{m}$. Since this map is injective, $\mathfrak{m} = (0)$.
(ii) $\implies$ (i): If $R = K \otimes_F L$ is a field, then every homomorphism into a nonzero ring – and in particular, any F-algebra homomorphism – is injective. □

THEOREM 11.8. *Let K, L be field extensions of F.*

a) *Suppose that K, L are everywhere F-linearly disjoint. Then at least one of K, L is algebraic over F.*
b) *Conversely, suppose that at least one of K, L is algebraic over F. Then K, L are somewhere F-linearly disjoint if and only if they are everywhere F-linearly disjoint.*

PROOF. a) If K and L are transcendental over F, then they admit subextensions $K' = F(a)$, $L' = F(b)$. By Exercise 11.5, it suffices to show that $F(a)$ and $F(b)$ are not everywhere F-linearly disjoint over F. To see this take $E = F(t)$ and map $K' \to E$ by $a \mapsto t$ and $L' \to E$ by $b \mapsto t$ and apply Lemma 11.2.
b) Because every algebraic extension is a direct limit of finite degree extensions, by Exercise 11.4 it is no loss of generality to assume that K/F is finite, and in light of Propositions 11.6 and 11.7, we must show that if $K \otimes_F L$ is a domain then it is a field. But if $\{k_1, \ldots, k_n\}$ is a basis for K/F, then $k_1 \otimes 1, \ldots, k_n \otimes 1$ is a basis for $K \otimes_F L$ over L, so $K \otimes_F L$ is a domain and a finitely generated L-module. Therefore it is a field, by an elementary argument which we have seen before (and which is a special case of the preservation of Krull dimension in an integral extension). □

In conclusion: the notion of F-linear disjointness of two field extensions K, L is *intrinsic* – independent of the embeddings into E – if and only if at least one of K, L is algebraic over F. In most of our applications of linear disjointness this hypothesis will be satisfied, and when it is we may safely omit mention of the ambient field E.

Here is a first result with our new convention in force.

THEOREM 11.9. *Let K/F be purely transcendental and L/F be algebraic. Then K, L are F-linearly disjoint.*

PROOF. By Exercise 11.4 and Lemma 11.3 it is enough to show that for all $n \in \mathbb{Z}^+$, $F[x_1, \ldots, x_n]$, L are F-linearly disjoint. By Corollary 3.4, this holds if and only if $F[x_1, \ldots, x_n] \otimes_F L$ is a domain. It is clear that the F-basis of $F[x_1, \ldots, x_n]$ consisting of monomials remains L-linearly independent in $L[x_1, \ldots, x_n]$ and by

Proposition 11.4 this implies that $F[x_1, \ldots, x_n]$ and L are F-linearly disjoint. In particular, the natural map $F[x_1, \ldots, x_n] \otimes_K L \to L[x_1, \ldots, x_n]$ is an isomorphism of L-algebras. □

THEOREM 11.10. *Let K, L be two field extensions of F with K/F purely transcendental. Then $K \otimes_F L$ is a domain.*

PROOF. The F-algebra $K \otimes_F L$ is the direct limit of the F-algebras $K_i \otimes_F L_i$ as K_i ranges over finitely generated subextensions of K/F and L_i ranges over finitely generated subextensions of L/F. Since the direct limit of domains is a domain, we have reduced to the case in which K and L are finitely generated over F, say $E_2 = F(s_1, \ldots, s_m)$, and $E_1 = F(t_1, \ldots, t_n, x_1, \ldots, x_p)$, where the t_i's are independent indeterminates over F and for all $1 \leq k \leq p$, the field extension $F(t_1, \ldots, t_n, x_1, \ldots, x_k)/F(t_1, \ldots, t_n, x_1, \ldots, x_{k-1})$ has finite degree. Put $K_1 = F(t_1, \ldots, t_n)$. Let E be the algebraic closure of the fraction field of $F[s_1, \ldots, s_m] \otimes_F F[t_1, \ldots, t_n]$. We may embed E_2 and L in E, and then E_2 and K_1 are linearly disjoint over F. Since K_1E_2/K_1 is purely transcendental and E_1/K_1 is algebraic, by Theorem 11.11 K_1E_2 and E_1 are linearly disjoint over K_1. By Theorem 11.5, the fields E_1 and E_2 are linearly disjoint over F, hence $E_1 \otimes_F E_2$ is a domain. □

3. Separability

LEMMA 11.11. *Let K/F be a degree n separable field extension of characteristic $p > 0$, and let $a_1, \ldots, a_n$ be an F-basis for K. Then for all $e \in \mathbb{Z}^+$, $a_1^{p^e}, \ldots, a_n^{p^e}$ is also an F-basis for K.*

PROOF. An evident inductive argument reduces us to the $e = 1$ case.

For all $1 \leq i \leq n$, a_i is both separable and purely inseparable over $F(a_1^p, \ldots, a_n^p)$, and thus $a_i \in F(a_1^p, \ldots, a_n^p)$. It follows that $F(a_1^p, \ldots, a_n^p) = K$. Now let V be the F-subspace spanned by $a_1^p, \ldots, a_n^p$. For all $1 \leq i, j \leq n$, there are $\alpha_1, \ldots, \alpha_k \in F$ such that

$$a_i a_j = \sum_k \alpha_k a_k.$$

Raising both sides to the pth power gives

$$a_i^p a_j^p = \sum_k \alpha_k^p a_k^p \in V.$$

It follows that V is a finite dimensional F-subalgebra of the field K, so V is a field. Since V contains a_i^p for all $1 \leq i \leq n$, we have $V = K$. Thus the n-element spanning set $a_1^p, \ldots, a_n^p$ of $V = K$ is an F-basis. □

PROPOSITION 11.12. *Let K/F be a separable algebraic extension. Then K and $F^{p^{-\infty}}$ are F-linearly disjoint.*

PROOF. Since $F^{p^{-\infty}} = \varinjlim F^{p^{-e}}$, applying Exercise 11.4 twice, we may assume that K/F has finite degree and show that for all $e \in \mathbb{Z}^+$, the extensions K and $F^{p^{-e}}$ are linearly disjoint over F. By Proposition 11.4, for this, it is enough to show that any F-basis $a_1, \ldots, a_n$ for K remains $F^{p^{-e}}$-linearly independent. Equivalently, we must show that for any F-basis $a_1, \ldots, a_n$ of K, then $a_1^{p^e}, \ldots, a_n^{p^e}$ are F-linearly independent, which is Lemma 11.11. □

The natural question to ask at this point is: can an inseparable extension K/F be linearly disjoint from $F^{p^{-\infty}}$? It follows from what we already know about separable extensions that the answer is *no* if K/F is inseparable and normal, for then by Corllary 4.27 it contains a nontrivial purely inseparable subextension and thus $F \subsetneq K \cap F^{p^{-1}} \subset K \cap F^{p^{-\infty}}$. In fact, as we are about to see, among algebraic field extensions K/F, being linearly disjoint from $F^{p^{-\infty}}$ characterizes separable extensions. But actually we can go further, with the following definitions.

A **separating transcendence basis** for a field extension K/F is an algebraically independent subset S of K such that $K/F(S)$ is separable algebraic.

It is clear that separating transcendence bases need not exist, e.g. an inseparable algebraic extension will not admit a separating transcendence basis. On the other hand, it is clear that separable algebraic extensions and purely transcendental extensions both admit separating transcendence bases: as with being linearly disjoint from the perfect closure, this is something that these apparently very different classes of extensions have in common.

We say that a field extension K/F is **separably generated** if it admits a separating transcendence basis.

EXERCISE 11.10. *Give an example of a separably generated field extension admitting a transcendence basis that* is not *a separating transcendence basis.*

An arbitrary field extension K/F is **separable** if every finitely generated subextension admits a separating transcendence basis.

And now the main theorem on separable extensions.

THEOREM 11.13. *(Mac Lane) Let F be a field of characteristic $p > 0$, and let E/F be a field extension. The following are equivalent:*

(i) *The extension E/F is separable: every finitely generated subextension is separably generated.*
(ii) *The extensions E and $F^{p^{-\infty}}$ are F-linearly disjoint.*
(iii) *The extensions E and $F^{p^{-1}}$ are F-linearly disjoint.*

PROOF. (i) $\implies$ (ii): Since every field extension is the direct limit of its finite generated subextensions, by Exercise LD2 we may assume that E/F is finitely generated and thus separably generated, so let B be a transcendence basis for E/F such that $E/F(B)$ is separable algebraic. By Proposition 11.12, E and $F(B)^{p^{-\infty}}$ are $F(B)$-linearly disjoint. Since $F(B)^{p^{-\infty}} \supset F^{p^{-\infty}}(B)$, it follows that $F^{p^{-\infty}}(B)$ are $F(B)$-linearly disjoint. Theorem 11.5 implies that E and $F^{p^{-\infty}}$ are F-linearly disjoint.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (i): Suppose that E and $F^{p^{-1}}$ are F-linearly disjoint. We will prove by induction on n that for all $n \in \mathbb{N}$, if $K = F(a_1, \ldots, a_n)$ is a finitely generated subextension of E/F then there exists a subset $S \subset \{a_1, \ldots, a_n\}$ which is a separating transcendence basis for K/F. When $n = 0$, $K = F$ and the result is trivial. The result is also clear if $a_1, \ldots, a_n$ are algebraically independent. Hence we may assume (after relabelling) that there exists $r < n$ such that $a_1, \ldots, a_r$ are a

transcendence basis for K/F. Let $f \in K[t_1, \ldots, t_{r+1}]$ be a polynomial of minimal total degree such that $f(a_1, \ldots, a_{r+1}) = 0$; necessarily f is irreducible.

We CLAIM f is *not* of the form $g(t_1^p, \ldots, t_r^p)$. If it were, there would exist $h \in F^{p^{-1}}[t_1, \ldots, t_{r+1}]$ such that $g(t_1^p, \ldots, t_r^p) = h(t_1, \ldots, t_r)^p$ with $h(a_1, \ldots, a_{r+1}) = 0$. Let $\{m_i\}$ be the monomials occurring in h. Then the elements $m_i(a_1, \ldots, a_{r+1})$ are $F^{p^{-1}}$-linearly dependent, so *by hypothesis* they are F-linearly dependent. This gives a nontrivial polynomial relation in the a_i of degree less than the degree of h, contradiction.

It follows that there is at least one i, $1 \leq i \leq r+1$, such that $f(t_1, \ldots, t_{r+1})$ is not a polynomial in t_i^p. Then a_i is algebraic over $F(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{r+1})$ and thus $\{a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{r+1}\}$ is a transcendence basis for K/F. So

$$F[a_1, \ldots, a_{i-1}, t, a_{i+1}, \ldots, a_{r+1}] \cong F[t_1, \ldots, t_{r+1}],$$

so $f(a_1, \ldots, a_{i-1}, t, a_{i+1}, \ldots, a_{r+1})$ is ireducible in $F[a_1, \ldots, a_{i-1}, t, a_{i+1}, \ldots, a_{r+1}]$, so by Gauss's Lemma it is irreducible in $F(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{r+1})[t]$. Since a_i is a root of $f(a_1, \ldots, a_{i-1}, t, a_{i+1}, \ldots, a_{r+1})$ and this is not a polynomial in t^p, a_i is separable algebraic over $F(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{r+1})$ and hence over $L := F(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$. The induction hypothesis applies to L to give a subset $\{a_{i_1}, \ldots, a_{i_r}\}$ of $\{a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}$ that is a separating transcendence base for L/F. Since a_i is separable algebraic over L, it is separable algebraic over $F(a_{i_1}, \ldots, a_{i_r})$. So $\{a_{i_1}, \ldots, a_{i_r}\}$ is a separating transcendence basis for K/F. $\square$

REMARK 11.2. *By our earlier results on linear disjointness, the conditions in Theorem 11.13 are also equivalent to any of the following ones:*

(iv) $E \otimes_F F^{p^{-1}}$ *is a field.*
(v) $E \otimes_F F^{p^{-1}}$ *is a domain.*
(vi) $E \otimes_F F^{p^{-\infty}}$ *is a field.*
(vii) $E \otimes_F F^{p^{-\infty}}$ *is a domain.*

EXAMPLE 11.14. *(Mac Lane): Let F be any field of characteristic $p > 0$, $F(t)$ a rational function field. Let $E = F(t, t^{p^{-1}}, t^{p^{-2}}, \ldots)$. Then any finitely generated subextension of E/F is isomorphic to $F(t)$ and thus separably generated. But E itself does not admit a separating transcendence basis. Thus E/F is separable but not separably generated.*

EXERCISE 11.11. *Let K/F be a field extension in characteristic $p > 0$. Show that K/F is separable if and only if: for every F-linearly subset $S \subset K$, the set $S^p := \{s^p \mid s \in S\}$ is also F-linearly independent.*

COROLLARY 11.15. *Let $F \subseteq K \subseteq L$ be a tower of field extensions in characteristic $p > 0$.*

a) *If L/F is separable, then K/F is separable.*
b) *If K/F and L/K are separable, then L/F is separable.*
c) *If L/F is separable and K/F is algebraic, then L/K is separable.*

PROOF. a) We use Theorem 11.13 and Remark 11.2: if L/F is separable, then $L \otimes_F F^{p^{-1}}$ is a domain, hence so its its subring $K \otimes_F F^{p^{-1}}$, so K/F is separable.
b) If K/F and L/K are separable, then K and $F^{p^{-1}}$ are linearly disjoint over F and L and $K^{p^{-1}}$ are linearly disjoint over K. Since $F^{1/p}K \subset K^{1/p}$, we get that $F^{1/p}K$ and L are linearly disjoint over F, so L and $F^{1/p}$ are linearly disjoint over

F by Theorem 11.5. Thus L/F is separable.
c) Suppose L/F is separable and K/F is algebraic. Part a) gives that K/F is separable algebraic. Let $K(x_1, \ldots, x_n)$ be a finitely generated subextension of L/K. Then $F(x_1, \ldots, x_n)$ is a finitely generated subextension of the separable extension L/F, so it admits a separating transcendence basis: there are $y_1, \ldots, y_m \in L$ such that $F(x_1, \ldots, x_n)/F(y_1, \ldots, y_m)$ is separable algebraic. Since K/F is separable algebraic, so is $K(x_1, \ldots, x_n)/F(x_1, \ldots, x_n)$, and therefore $K(x_1, \ldots, x_n)/F(t_1, \ldots, t_m)$ is separable algebraic. Thus $t_1, \ldots, t_m$ is a separating transcendence basis for $K(x_1, \ldots, x_n)/F$, so $K(x_1, \ldots, x_n)/F$ is separably generated. □

EXAMPLE 11.16. *Let F be a field of characteristic p, let $L = F(t)$ and let $K = F(t^p)$. Then L/F is separable but L/K is not. This shows that in Corollary 11.15, the hypothesis that K/F be algebraic cannot be removed.*

COROLLARY 11.17. *Let K/F be a field extension.*

a) *If K/F is separably generated, then K/F is separable.*
b) *If K/F is finitely generated, then it is separably generated if and only if it is separable.*
c) *If K/F is finitely generated and separably generated, then every subextension is also separably generated.*

PROOF. a) Suppose K/F is separably generated. Let L be a purely transcendental subextension of K/F such that K/L is separable algebraic. By Theorem 11.11 the fields L and $F^{1/p}$ are linearly disjoint over F, and because K/L is separable and $LF^{1/p}/L$ is purely inseparable, K and $LF^{1/p}$ are linearly disjoint over L. By Theorem 11.5 we have that K and $F^{1/p}$ are linearly disjoint over F, so Theorem 11.13, K/F is separable.
b) Suppose K/F is finitely generated. Then if it is separable then every finitely generated subextension is separably generated...including K/F itself. Conversely, if K/F is separably generated then by part a) (and without the finite generation hypothesis) we know that K/F is separable.
c) This follows from part a) and Corollary 11.15. □

EXERCISE 11.12.

a) *Show: separably generated extensions do* not *satisfy the base change metaproperty (DC2). (Suggestion: let F be a field of characteristic $p > 0$, let $K = F(t^{1/p})$ and $L = F(t)$.)*
b) *Conclude that separably generated extensions – and thus also separable extensions – do not form a distinguished class in the sense of Lang.*
c) *Dis/prove: the compositum of two separably generated extensions is separably generated.*
d) *Dis/prove: the compositum of two separable extensions is separable.*

4. Linear Disjointness and Normality

THEOREM 11.18. *Let F be a field, with algebraic closure $\overline{F}$. Let K_1, K_2 be finite Galois subextensions of $\overline{F}/F$. For $i = 1, 2$, put $G_i := \mathrm{Aut}(K_i/F)$, and put $G := \mathrm{Aut}(K_1K_2/F)$. Let*

$$\sigma : G \hookrightarrow G_1 \times G_2$$

be the natural group homomorphism. The following are equivalent:

(i) *The fields K_1 and K_2 are linearly disjoint over F.*
(ii) *We have $K_1 \cap K_2 = F$.*
(iii) *The map σ is an isomorphism.*
(iv) *We have $G \cong G_1 \times G_2$.*

PROOF. (i) $\implies$ (ii) by Lemma 11.2.
(ii) $\implies$ (iii): Recall Theorem 7.21, which describes the image of the injective map σ as the fiber product of $\pi_1 : G_1 \to \mathrm{Aut}(K_1/K_1 \cap K_2)$ and $\pi_2 : G_2 \to \mathrm{Aut}(K_2/K_1 \cap K_2)$. So if $K_1 \cap K_2 = F$, this fiber product is the entire direct product $G_1 \times G_2$ and thus σ is an isomorphism.
(iii) $\implies$ (iv) is immediate.
(iv) $\implies$ (i): If $G \cong G_1 \times G_2$, then

$$[K_1K_2 : F] = \#G = \#G_1 \cdot \#G_1 = [K_1 : F][K_2 : F],$$

so K_1 and K_2 are linearly disjoint over F by Lemma 11.1. □

Let K_1, K_2 be two finite degree field extensions of F inside $\overline{F}$. Suppose that $K_1 \cap K_2 = F$. We say in Exercise 11.2 that K_1 and K_2 need *not* be linearly disjoint over F, while in Proposition 11.18 we saw that if both are Galois over F then they will be linearly disjoint over F. This raises a question – what if just one of K_1 and K_2 is Galois over F? – that is answered by the next result.

THEOREM 11.19. *Let E/F be a field extension, and let K_1, K_2 be two algebraic subextensions. Suppose that for some $i \in \{1, 2\}$ the extension K_i/F is normal and that for some $j \in \{1, 2\}$ the extension K_j/F is separable. Then K_1 and K_2 are linearly disjoint over F if and only if $K_1 \cap K_2 = F$.*

PROOF. By Lemma 11.3, if K_1 and K_2 are linearly disjoint over F, then $K_1 \cap K_2 = F$. So we may assume that $K_1 \cap K_2 = F$ and prove that K_1 and K_2 are linearly disjoint over F. Applying Exercise 11.4 twice, we reduce to the case in which K_1 and K_2 each have finite degree over F, so linear disjointness is equivalent to $[K_1K_2 : F] = [K_1 : F][K_2 : F]$ by Lemma 11.1.
Step 1: Suppose that K_1/F is both normal and separable: thus it is Galois. By Natural Irrationalities, we have

$$[K_1K_2 : F] = [K_1K_2 : K_2][K_2 : F] = [K_1 : K_1 \cap K_2][K_2 : F] = [K_1 : F][K_2 : F].$$

so

$$[K_1K_2 : F] = [K_1 : F][K_2 : F] \iff K_1 \cap K_2 = F.$$

Step 2: Without loss of generality, we may suppose that K_1/F is normal and that K_2/F is separable. Let F_s and F_i be the separable and inseparable closures of F in K_1, so $K_1 = F_sF_i$ by Corollary 4.27 and F_s/F is Galois by Corollary 4.31. Thus by Step 1 we have that F_s and L are linearly disjoint over F, so by Theorem 11.5 it suffices to show that K_1 and F_sL are linearly disjoint over F_s. Since K_1/F_s is purely inseparable and F_sL/F is separable, this follows from Proposition 11.12. □

EXAMPLE 11.20. *Let p be a prime number, and let k be a field of characteristic p. We revisit Example 4.28, which constructs a degree p^2 extension K of $F := k(x, y)$ (rational function field) that is not balanced: the extension has separable degree p but no nontrivial purely inseparable subextension.*

Because K/F is not separable, by Theorem 11.13 we have that K and $F^{1/p}$ are not linearly disjoint over F. On the other hand $K \cap F^{1/p}$ is contained in K

and purely inseparable over F, so $K \cap F^{1/p} = F$. In general, $F^{1/p}/F$ need not have finite degree, but later (Corollary 12.18) we will see that it does if k is perfect. In general, let $\overline{F}$ be an algebraic closure of F containing K and $F^{1/p}$. Since the map $K \otimes_F F^{1/p} \to \overline{F}$ is not injective, there must be some normal finite degree subextension F' of $F^{1/p}$ such that $K \otimes_F F' \to \overline{F}$ is not injective, hence K and F' are nonintersecting finite degree field extensions of F, one of which is normal, which are not linearly disjoint.

If $p = 2$, the separable closure F_s of F in K is a quadratic over F, hence F_s/F is normal, so K/F is normal by Corollary 4.31. Thus K and F' are nonintersecting finite degree normal extensions of F that are not linearly disjoint.

Unfortunately the last part of Example 11.20 is particular to characteristic 2:

EXERCISE 11.13. *With notation as in Example 11.20, let $p \geq 3$ be a prime number, let F_s be the maximal separable subextension of K/F: it is the field $F[t]/(g)$, with $g := t^p + xt + y \in F[t]$.*

a) *Show: $\delta(g) = \pm x^p \in F^\times$.*

b) *Use Proposition 6.13 and Corollary 4.31 to show that K/F is not normal.*

In fact, for any prime number p, there is a field F of characteristic p and two finite degree purely inseparable (hence normal) field extensions $K_1, K_2/F$ that are nonintersecting but not linearly disjoint. These examples however lie deeper in the study of purely inseparable field extensions than we will be able to go in this text. But in [**Sw68**], Sweedler defines a class of purely inseparable extensions K/F called **modular**, satisfying several equivalent conditions: for finite degree extensions, one condition is being a (finitely iterated) tensor product of monogenic extensions. Another condition is that K^{p^e} and F are linearly disjoint over their intersection for all $e \in \mathbb{Z}^+$. In [**Sw68**, Example 1.1], Sweedler constructs for any prime p a degree p^3 purely inseparable field extension in characteristic p that is not modular. This shows that in any characteristic p, nonintersecting purely inseparable field extensions need not be linearly disjoint.

5. Interlude

For later use we record the following result, whose proof will use methods of commutative algebra rather than field theory.[1]

THEOREM 11.21 (Integrality of Products). *Let k be an algebraically closed field, and for $i = 1, 2$, let R_i be a domain that is finitely generated as a k-algebra. Then $R_1 \otimes_k R_2$ is a domain.*

PROOF. The statement holds trivially if either $R_1 = k$ or $R_2 = k$, so assume that each of R_1 and R_2 have positive transcendence degree over k. Seeking a contradiction, suppose that we have nonzero elements

$$x = \sum_{i=1}^{m} a_i \otimes b_i, \ y = \sum_{j=1}^{n} c_j \otimes d_j \in R_1 \otimes_k R_2$$

such that $xy = 0$. We may assume that each of $b_1, \ldots, b_m$ and $d_1, \ldots, d_n$ are k-linearly independent in R_2, and we may also assume that $a_1 c_1 \neq 0$. Because R_1 is a Hilbert-Jacobson ring [**Cl-CA**, Prop. 11.3], there is a maximal ideal $\mathfrak{m}$ of R_1

[1]The proof comes from `https://stacks.math.columbia.edu/tag/020C`.

such that $a_1c_1 \in R_1 \setminus \mathfrak{m}$. Denote the quotient map $R_1 \to R_1/\mathfrak{m}$ by $a \mapsto \overline{a}$. Because k is algebraically closed, we have $R_1/\mathfrak{m} = k$ [**Cl-CA**, Thm. 11.5]. Then under the homomorphism $R_1 \otimes_k R_2 \to R_1/\mathfrak{m} \otimes_k R_2 = R_2$ the relation $xy = 0$ becomes

$$(\sum_i \overline{a_i} b_i)(\sum_j \overline{c_j} d_j) = 0,$$

which exhibits a product of two nonzero elements in the domain R_2 being zero, a contradiction. □

Although our motivation for proving Theorem 11.21 is field theoretic – it will be used in the proof of Theorem 11.24 giving an important equivalent condition on a class of field extensions – for those with some familiarity with algebraic geometry it is hard not to notice that it is saying precisely that over an algebraically closed field, the product of two integral affine varieties remains integral.

EXERCISE 11.14. *Show that if the conclusion of Theorem 11.21 holds for a field k, then k is algebraically closed.*

6. Regular Extensions

A field extension K/F is **regular** if for all field extensions L/F, the F-algebra $K \otimes_F L$ is a domain.

As an important example, in this new terminology Theorem 11.10 says precisely that purely transcendental extensions are regular.

EXERCISE 11.15. *Show: If K/F is regular and algebraic, then $K = F$.*

LEMMA 11.22. *If K/F is regular, then for all algebraic extensions L/F, we have that $K \otimes_F L$ is a field.*

PROOF. We have by definition that $K \otimes_F L$ is a domain, so by Proposition 11.6 we have that K and L are somewhere linearly disjoint over F. Since L/F is algebraic, Theorem 11.8 gives that K and L are everwhere linearly disjoint over F, and then Proposition 11.7 gives that $K \otimes_F L$ is a field. □

LEMMA 11.23. *Let K and L be commutative F-algebras. If $K \otimes_F L$ is a field, then K and L are fields.*

PROOF. Tensoring $F \hookrightarrow L$ with the (flat, since F is a field) F-module K gives an injection $K \hookrightarrow K \otimes_F L$. This shows that K is a domain. Let $t \in K^\bullet$, and let C be the cokernel of multiplication by t on K. Tensoring the exact sequence

$$0 \to K \xrightarrow{\cdot t} K \to C \to 0$$

with L, we get

$$0 \to K \otimes_F L \xrightarrow{\cdot t \otimes 1} K \otimes_F L \to C \otimes_F L \to 0.$$

Since $K \otimes_F L$ is a field, multiplication by $t \otimes 1$ is an isomorphism, so $C \otimes_F L = 0$, so $C = 0$. This shows that K is a field. Interchanging K and L, the same argument shows that L is a field. □

THEOREM 11.24. *For a field extension K/F, the following are equivalent:*

(i) *We have that K/F is regular.*
(ii) *For every algebraic extension L/F, we have that $K \otimes_F L$ is a field.*

(iii) *For any algebraic closure $\overline{F}$ of F, we have that $K \otimes_F \overline{F}$ is a field.*
(iv) *We have that F is algebraically closed in K and K/F is separable.*

PROOF. (i) $\implies$ (ii): This follows from Lemma 11.22.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (ii): Let L/F be an algebraic field extension. We have by assumption that $K \otimes_F \overline{F} = (K \otimes_F L) \otimes_L \overline{F}$ is a field, so by Lemma 11.23 we deduce that $K \otimes_F L$ is a field.
(ii) $\implies$ (iv): Let L be the algebraic closure of F in K, so by assumption we have that $K \otimes_F L$ is a field. Thus the F-subalgebra $L \otimes_F L$ is a domain, and since L/F is algebraic this implies $L = F$. The separability is automatic in characteristic 0 and in characteristic p we have that $K \otimes_F F^{p^{-1}}$ is a field, so K/F is separable by Theorem 11.13.
(iv) $\implies$ (iii): Let F^{sep} be the maximal separable subextension of $\overline{F}/F$. Then F^{sep}/F is Galois and $F^{\mathrm{sep}} \cap K = F$, so $K \otimes_F F^{\mathrm{sep}}$ is a field. Since K/F is separable, $K \otimes_F F^{\mathrm{sep}}/F^{\mathrm{sep}}$ is separable (indeed one can choose the same separating transcendence basis), hence K is F-linearly disjoint from the maximal purely inseparable extension of F^{sep}, which is $\overline{F}$.
(iii) $\implies$ (i): We must show that $K \otimes_F L$ is a domain for *every* field extension L/F. For this it is harmless to replace L with a larger field extension, so suppose that L is algebraically closed, and let $\overline{F}$ be the algebraic closure of F in L (which is indeed algebraically closed!). By assumption, we have that $K \otimes_F \overline{F}$ is a field, and since

$$K \otimes_F L = f(K \otimes_F \overline{F}) \otimes_{\overline{F}} L,$$

we may replace F by $\overline{F}$ and K by $K \otimes_F \overline{F}$ and thereby assume that F is algebraically closed. In order to show that $K \otimes_F L$ is a domain it is enough to show that for any finitely generated F-subalgebra R_1 and any finitely generated R_2-subalgebra R_2 of L, the ring $R_1 \otimes_F R_2$ is a domain. (This is essentially Exercise 11.4, and at any rate it is not difficult: just write out an arbitrary element of the tensor product to see that it has this form.) This is a nontrivial fact, but fortunately for us we have just proven it: Theorem 11.21. □

COROLLARY 11.25. *For a field F, the following are equivalent:*
(i) *Every field extension K/F is regular.*
(ii) *The field F is algebraically closed.*

EXERCISE 11.16. *Prove Corollary 11.25.*

EXERCISE 11.17. *Let $F \subset K \subset L$ be a tower of field extensions.*
a) *Show: If K/F and L/K are regular, then so is L/F.*
b) *Show: if L/F is regular, then K/F is regular.*
c) *If L/F is regular, must L/K be regular?*

CHAPTER 12

Derivations and Differentials

1. Derivations

1.1. Definitions and First Results. Let R be a commutative ring, and let M be an R-module. A **derivation** of R into M is a map $D : R \to M$ satisfying both of the following:

(D1) For all $x, y \in R$, $D(x + y) = D(x) + D(y)$
(i.e., D is a homomorphism of additive groups),
(D2) For all $x, y \in R$, $D(xy) = xD(y) + D(x)y$ ("product rule").

EXERCISE 12.1. *Let R be a commutative ring, and let M be an R-module. Let $D : R \to M$ be a derivation, let $x \in R$ and let $n \in \mathbb{Z}^+$. Show:*

$$D(x^n) = nx^{n-1}D(x).$$

Suppose we are given a subring k of R. Then a **k-derivation** is a derivation $D : R \to M$ satisfying the additional property

(D3) For all $x \in k$, $D(x) = 0$.

We write $\mathrm{Der}(R, M)$ for the set of all derivations $D : R \to M$ and $\mathrm{Der}_k(R, M)$ for the set of all k-derivations $D : R \to M$. When $M = R$ we speak of "derivations on R" and write $\mathrm{Der}(R)$ for $\mathrm{Der}(R, R)$ and $\mathrm{Der}_k(R)$ for $\mathrm{Der}_k(R, R)$.

EXAMPLE 12.1. *Let k be a commutative ring, and let $R := k[t]$. The usual polynomial derivative $f \mapsto f'$ is a k-derivation on R; we will denote it by ∂. The derivation ∂ is the unique k-derivation D such that $D(t) = 0$.*

If $D \in \mathrm{Der}(R)$ and $n \in \mathbb{Z}^+$, we put $D^n := D \circ D \circ \cdots \circ D$ (n times). We also put $D^0 = 1_R$.

LEMMA 12.2 (Leibniz Rule). *Let R be a commutative ring, $D \in \mathrm{Der}(R)$ and $n \in \mathbb{Z}^+$. For $x, y \in R$, we have*

$$D^n(xy) = \sum_{k=0}^{n} \binom{n}{k} D^{n-k}(x)D^k(y).$$

EXERCISE 12.2. *Prove Lemma 12.2. (Suggestion: use induction.)*

If $D \in \mathrm{Der}(R)$ and $n \in \mathbb{Z}^{\geq 2}$. Then Lemma 12.2 strongly suggests that D^n is in general *not* a derivation. Consider the usual dervative ∂ on $\mathbb{R}[t]$: we have $\partial^n(t^n \cdot t^n) = \frac{(2n)!}{n!}t^n$, while $\partial^n(t^n)t^n + t^n\partial^n(t^n) = 2n!t^n$, and we have $\frac{(2n)!}{n!} > 2n!$ for all $n \geq 2$. However, if R has prime characteristic p, then Lemma 12.2 implies that for $D \in \mathrm{Der}(R)$, also $D^p \in \mathrm{Der}(R)$.

EXERCISE 12.3. *Let $k \subseteq R$ be commutative rings, and let M be an R-module.*

a) *Let $\mathrm{Hom}_k(M,R)$ be the set of all k-module homomorphisms $f : M \to R$. Show: $\mathrm{Der}_k(M,R) \subseteq \mathrm{Hom}_k(M,R)$.*

b) *For $D \in \mathrm{Der}_k(R)$ and $a \in R$, let $aD : R \to R$ be the map $x \mapsto aD(x)$. Show: $aD \in \mathrm{Der}_k(R)$. This gives $\mathrm{Der}_k(R)$ the structure of an R-module.*

c) *For $D_1, D_2 \in \mathrm{Der}_k(R)$, define $[D_1, D_2] : R \to R$ by*

$$x \mapsto D_1(D_2(x)) - D_2(D_1(x)).$$

*Show: $[D_1, D_2] \in \mathrm{Der}_k(R)$. Deduce: this equips $\mathrm{Der}_k(R)$ with the structure of a **Lie algebra over k**.*

EXERCISE 12.4. *Let $D : R \to M$ be a derivation, and let*

$$C \coloneqq \{x \in R \mid D(x) = 0\}.$$

Show: C is the unique maximal subring k of R such that $D \in \mathrm{Der}_k(R,M)$.

EXERCISE 12.5. *For a field k, compute the constant subring of $\partial : k[t] \to k[t]$. (The answer depends on the characteristic of k.)*

EXERCISE 12.6. *Let k be a domain, let $n \in \mathbb{Z}^+$, and let $R = k[t_1, \ldots, t_n]$ be the polynomial ring in n variables over k. Show that for each $1 \leq i \leq n$ there is a unique k-derivation ∂_i on R such that $\partial_i(t_j) = \delta_{ij}$.*

When $k = \mathbb{R}$, it is well known that we may differentiate not only polynomials but also rational functions. This generalizes nicely to our abstract algebraic context.[1]

THEOREM 12.3. *Let R be a domain with fraction field K, and let $D \in \mathrm{Der}(R)$.*

a) *There is a unique extension of D to a derivation on K, given by*

$$D_K\left(\frac{x}{y}\right) = \frac{yD(x) - xD(y)}{y^2}. \tag{40}$$

b) *If D is a k-derivation for some subring k of R with fraction field $f(k)$, then D_K is an $f(k)$-derivation.*

PROOF. a) Our first order of business is to show that D_K is well-defined, i.e., if $x_1, x_2, y_1, y_2 \in R$ are such that $y_1 y_2 \neq 0$ and $x_1 y_2 = x_2 y_1$, then

$$\frac{y_1 D(x_1) - x_1 D(y_1)}{y_1^2} = \frac{y_2 D(x_2) - x_2 D(y_2)}{y_2^2}.$$

We check this by a straightforward if somewhat unenlightening calculation:

$$\begin{aligned} &y_2^2 \left(x_1 D(y_1) - y_1 D(x_1)\right) - \left(y_1^2 (x_2 D(y_2) - y_2 D(x_2)\right) \\ &= y_2^2 x_1 D(y_1) - y_2^2 y_1 D(x_1) - y_1^2 x_2 D(y_2) - y_1^2 y_2 D(x_2) \\ &= (y_2 x_1 d(y_1 y_2) - y_1 y_2 D(x_1 y_2)) - (y_1 x_2 D(y_1 y_2) + y_1 y_2 D(y_1 x_2)) \\ &= (x_1 y_2 - x_2 y_1) D(y_1 y_2) - y_1 y_2 D(x_1 y_2 - x_2 y_1) = 0. \end{aligned}$$

Next we check that D_K is a derivation:

$$D_K\left(\frac{x_1}{y_1}\right) + D_K\left(\frac{x_2}{y_2}\right) = \frac{y_1 D(x_1) - x_1 D(y_1)}{y_1^2} + \frac{y_2 D(x_2) - x_2 D(y_2)}{y_2^2}$$

[1] It actually generalizes a little *more* nicely: rational functions may not be everywhere defined, which is something we don't need to worry about here.

$$= \frac{y_1y_2^2D(x_1) + y_1^2y_2D(x_2) - x_1y_2^2D(y_1) - x_2y_1^2D(y_2)}{y_1^2y_2^2}.$$

On the other hand we have

$$D_K\left(\frac{x_1}{y_1} + \frac{x_2}{y_2}\right) = D_K\left(\frac{x_1y_1 + x_2y_1}{y_1y_2}\right) = \frac{N(x_1, x_2, y_1, y_2)}{y_1^2y_2^2},$$

where

$$N(x_1, x_2, y_1, y_2) = y_1y_2D_K(x_1y_2 + x_2y_1) - x_1y_2D_K(y_1y_2) - x_2y_1D_K(y_1y_2)$$
$$= y_1y_2^2D(x_1) + y_1y_2^2D_K(x_2) + (x_2y_1y_2 - x_1y_2^2 - x_2y_1y_2)D_K(y_1) + (x_1y_1y_2 - x_1y_1y_2 - x_2y_1^2)D_K(y_2)$$
$$= y_1y_2^2D_K(x_1) + y_1^2y_2D_K(x_2) - x_1y_2^2D_K(y_1) - x_2y_1^2D_K(y_2),$$

establishing the additivity of D_K. Similarly we have

$$D_K\left(\frac{x_1}{y_1}\frac{x_2}{y_2}\right) = \frac{y_1y_2D_K(x_1x_2) - x_1x_2D_K(y_1y_2)}{y_1^2y_2^2}$$
$$= \frac{x_2y_1y_2D_K(x_1) + x_1y_1y_2D_K(x_2) - x_1x_2y_2D_K(y_1) - x_1x_2y_1D_K(y_2)}{y_1^2y_2^2},$$

while

$$\frac{x_1}{y_1}D_K\left(\frac{x_2}{y_2}\right) + D_K\left(\frac{x_1}{y_1}\right)\frac{x_2}{y_2}$$
$$= \frac{x_1y_1(y_2D_K(x_2) - x_2D_K(y_2)) + x_2y_2(y_1D_K(x_1) - x_1D_K(y_1))}{y_1^2y_2^2}$$
$$= \frac{x_2y_1y_2D_K(x_1) + x_1y_2y_2D_K(x_2) - x_1x_2y_2D_K(y_1) - x_1x_2y_1D_K(y_2)}{y_1^2y_2^2},$$

establishing the product rule.

Let $\mathcal{D}$ be any derivation on K extending D. For $x, y \in K$ with $y \neq 0$, we have

$$\mathcal{D}(x) = \mathcal{D}\left(\frac{x}{y} \cdot y\right) = \frac{x}{y}\mathcal{D}(y) + y\mathcal{D}\left(\frac{x}{y}\right),$$

so

$$\mathcal{D}\left(\frac{x}{y}\right) = \frac{\mathcal{D}(x)}{y} - \frac{x\mathcal{D}(y)}{y^2} = \frac{y\mathcal{D}(x) - x\mathcal{D}(y)}{y^2} = D_K\left(\frac{x}{y}\right),$$

completing the proof of part a).

b) Since D_K extends D and $D(x) = 0$ for all $x \in k$, certainly $D_K(x) = 0$ for all $x \in k$. Using (40) it follows that for all $x, y \in k$ with $y \neq 0$, $D\left(\frac{x}{y}\right) = 0$. □

PROPOSITION 12.4. *Let L/K be a field extension, and let $D \in \mathrm{Der}_K(L)$. Let $f \in K[t_1, \ldots, t_n]$ and $a = (a_1, \ldots, a_n) \in L^n$. Then*

$$D(f(a)) = \sum_{i=1}^{n} \partial_i f(a_1, \ldots, a_n)D(a_i).$$

EXERCISE 12.7. *Prove Proposition 12.4.*

Let L/K be a field extension, and let S be a subset of L. We say $D \in \mathrm{Der}\, L$ is **S-finite** if $\{x \in S \mid D(x) \neq 0\}$ is finite. The S-finite derivations form an L-subspace of $\mathrm{Der}_K(L)$ that we will denote by $\mathrm{Der}_K^S(L)$. This concept is only interesting if S is infinite: if S is finite, then $\mathrm{Der}_K^S(L) = \mathrm{Der}_K(L)$.

PROPOSITION 12.5. *Let L/K be a field extension, and let S be a set of generators for L/K.*

a) *We have*

$$\dim_L \mathrm{Der}_K^S(L) \leq \#S.$$

b) *If L/K can generated by $n < \aleph_0$ elements, then then* $\dim_L \mathrm{Der}_K(L) \leq n$.

PROOF. Let $L^{(S)}$ be the set of all finitely nonzero functions from S to L. This is an L-vector space with basis canonically in bijection with S: indeed, for $s \in S$, let δ_s be the function which takes the value 1 at s and zero elsewhere. Then $\{\delta_s\}_{s \in S}$ is an L-basis for $L^{(S)}$.
The natural restriction map $\mathrm{Der}_K^S(L) \to L^{(S)}$ is L-linear and injective. The L-linearity is a triviality: the injectivity follows from the fact that every element of L is a rational function in the elements of S with coefficients in K. Since $\dim L^{(S)} = \#S$, part a) follows immediately. Part b) is also immediate from the observation that S-finiteness is a vacuous condition when S itself is a finite set. □

1.2. The Derivation Extension Theorem. Let $L = K(x_1, \ldots, x_n)/K$ be a finitely generated field extension. Let $I(x_1, \ldots, x_n)$ be the ideal of $K[t_1, \ldots, t_n]$ consisting of all polynomials f such that $f(x_1, \ldots, x_n) = 0$. Thus $I(x_1, \ldots, x_n)$ is the kernel of the natural surjective K-algebra map

$$K[t_1, \ldots, t_n] \to K[x_1, \ldots, x_n],\ t_i \mapsto x_i,$$

so $I(x_1, \ldots, x_n)$ is a prime ideal.

EXERCISE 12.8. *Let K be a field, and let $D \in \mathrm{Der}(K)$.*

a) *For a polynomial $f \in K[t_1, \ldots, t_n]$, we denote by f^D the polynomial obtained from f by applying D to each coefficient:*

$$f = \sum_I a_I t_1^{i_1} \cdots t_n^{i_n} \mapsto f^D = \sum_i D(a_I) t_1^{i_1} \cdots t_n^{i_n}.$$

Show: this defines an extension of D to a derivation on $K[t_1, \ldots, t_n]$.

b) *Show: there is a unique derivation $\overline{D}$ on $K(t_1, \ldots, t_n)$ such that $\overline{D}|_K = D$ and $\overline{D}(t_i) = 0$ for all $1 \leq i \leq n$. The restriction of $\overline{D}$ to $K[t_1, \ldots, t_n]$ is the derivation of part a).*

Suppose D is a derivation on K and $\overline{D}$ is a derivation on $K(x_1, \ldots, x_n)$ extending D. Then for all $f \in I(x_1, \ldots, x_n)$ we have

$$0 = \overline{D}(f(x_1, \ldots, x_n)) = \overline{D}(\sum_I a_I x_1^{i_1} \cdots x_n^{i_n}) =$$

$$\sum_I D(a_i) x_1^{i_1} \cdots x_n^{i_n} + \sum_I a_i \left(\sum_{k=1}^n x_1^{i_1} \cdots x_{k-1}^{i_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_n^{i_n} i_k x_k^{i_k - 1} \overline{D}(x_k) \right)$$

$$= f^D(x) + \sum_{i=1}^n (\partial_i f)(x) \overline{D}(x_i).$$

Thus each $f \in I(x_1, \ldots, x_n)$ gives a linear equation satisfied by the values $\overline{D}(x_1), \ldots, \overline{D}(x_n) \in K(x_1, \ldots, x_n)$. The next result – probably the most important one in this section – says that these linear relations give the only constraints in extending D to a derivation on $K(x_1, \ldots, x_n)$.

THEOREM 12.6 (Derivation Extension Theorem). *Let K be a field, let $L = K(x_1, \ldots, x_n)$ be a finitely generated field extension, and let $\{f_j\}_{j \in J}$ be a set of generators for the ideal $I(x_1, \ldots, x_n)$ of $K[t_1, \ldots, t_n]$. Let D be a derivation on K. For $u_1, \ldots, u_n \in L$, the following are equivalent:*

(i) *For all $j \in J$, we have*

$$0 = f_j^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i f_j)(x_1, \ldots, x_n) u_i. \tag{41}$$

(ii) *There is $\overline{D} \in \operatorname{Der} L$ extending D such that $\overline{D}(x_i) = u_i$ for all $1 \leq i \leq n$.*

(iii) *There is a unique $\overline{D} \in \operatorname{Der} L$ extending D such that $\overline{D}(x_i) = u_i$ for all $1 \leq i \leq n$.*

PROOF. Clearly (iii) $\implies$ (ii). (ii) $\implies$ (iii): Since derivations are additive and satisfy the product rule, specifying $\overline{D}$ on K and its values at $x_1, \ldots, x_n$ determines its values on $K[x_1, \ldots, x_n]$, which determines its values on the fraction field $K(x_1, \ldots, x_n)$ by Theorem 12.3. Just above we showed that (ii) $\implies$ (i), so it suffices to show that (i) $\implies$ (ii): suppose (41) holds for all f_j in a set of generators for $I(x_1, \ldots, x_n)$. Then for all $j_1, j_2 \in J$ we have

$$(f_{j_1} + f_{j_2})^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i (f_{j_1} + f_{j_2})(x_1, \ldots, x_n) u_i =$$

$$\left(f_{j_1}^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i f_{j_1}(x_1, \ldots, x_n) u_i \right) + \left(f_{j_2}^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i f_{j_2}(x_1, \ldots, x_n) u_i \right)$$

$$= 0 + 0 = 0.$$

For $j \in J$ and $g \in K[t_1, \ldots, t_n]$, we have

$$(gf_j)^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i (gf_j))(x_1, \ldots, x_n) u_i$$

$$= g(x_1, \ldots, x_n) \left(f_j^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i f_j)(x_1, \ldots, x_n) u_i \right)$$

$$+ f_j(x_1, \ldots, x_n) \left(g^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i g)(x_1, \ldots, x_n) u_i \right)$$

$$= g(x_1, \ldots, x_n) \cdot 0 + 0 \cdot \left(g^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i g)(x_1, \ldots, x_n) u_i \right) = 0.$$

This shows that (41) holds for all $f \in I(x_1, \ldots, x_n)$. Now we define $\overline{D}$ on $K[x_1, \ldots, x_n]$ by putting, for $g \in K[t_1, \ldots, t_n]$,

$$\overline{D}(g(x_1, \ldots, x_n)) \coloneqq g^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i g)(x_1, \ldots, x_n) u_i.$$

The point here is that the same element of $K[x_1, \ldots, x_n]$ can in general by expressed as $g(x_1, \ldots, x_n)$ for several polynomials $g \in K[t_1, \ldots, t_n]$, but any two such polynomials differ by an element of $I(x_1, \ldots, x_n)$, so our calculation just above has checked that if $g_1(x_1, \ldots, x_n) = g_2(x_1, \ldots, x_n)$ then $\overline{D}(g_1(x_1, \ldots, x_n)) = \overline{D}(g_2(x_1, \ldots, x_n))$. The fact that $\overline{D}$ is a derivation now follows from the fact that $g \mapsto g^D$ and $g \mapsto \partial_i g$ are derivations. Thus we have succeeded in extending D to a derivation $\overline{D}$ of

$K[x_1, \ldots, x_n]$. By Theorem 12.3a), there is a unique extension of $\overline{D}$ to a derivation on $K(x_1, \ldots, x_n)$. Finally, for $1 \leq i \leq n$, taking $g = t_i$ gives

$$\overline{D}(x_i) = \overline{D}(g(x_1, \ldots, x_n)) = g^D(x_1, \ldots, x_n) + \sum_{i=1}^{n} (\partial_i g)(x_1, \ldots, x_n) u_i$$

$$= 0 + 0 \cdot u_1 + \ldots + 0 \cdot u_{i-1} + 1 \cdot u_i + 0 \cdot u_{i+1} + \ldots + 0 \cdot u_n = u_i. \qquad \square$$

1.3. The structure of $\mathrm{Der}_K(L)$ for a finitely generated extension L/K. Let L/K be any finitely generated field extension. In this section we will apply Theorem 12.6 to give a good description of the L-vector space $\mathrm{Der}_K(L)$. In particular its dimension is an interesting invariant of the extension L/K and will be computed. What we know so far is that, by Proposition 12.5, $\dim_L \mathrm{Der}_K(L)$ is bounded above by the minimal number of generators of L/K, and we sill soon that equality holds if L/K is purely transcendental. It turns out that in characteristic 0, we always have $\dim_L \mathrm{Der}_K(L) = \mathrm{trdeg}(L/K)$, while in positive characteristic separability issues intervene to make things more interesting.

The easiest application of Theorem 12.6 is when $L = K(t_1, \ldots, t_n)$ is a rational function field. In this case the ideal $I(t_1, \ldots, t_n)$ is the zero ideal, so in this case Theorem 12.6 says that we may extend $D \in \mathrm{Der}(K)$ to a derivation $\overline{D}$ on $K(t_1, \ldots, t_n)$ by freely choosing the values of $\overline{D}(t_1), \ldots, \overline{D}(t_n)$. We have met special cases of this result before: Exercise 12.8 treats the case $\overline{D}(t_i) = 0$ for all i and Exercise 12.6 fixes $1 \leq j \leq n$ and treats the case $\overline{D}(t_i) = \delta(i, j)$ (Kronecker δ). This gives part a) of the following result, and part b) will follow easily.

COROLLARY 12.7. *Let $L = K(t_1, \ldots, t_n)$ be a purely transcendental extension.*

a) *Let $D \in \mathrm{Der}\, K$. For each $1 \leq i \leq n$, there is a unique $D_i \in \mathrm{Der}\, L$ that extends D and such that for all $1 \leq i \leq n$ we have*

$$D_i(t_j) = \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}.$$

b) *For each $1 \leq i \leq n$ there is a unique $\delta_i \in \mathrm{Der}_K(L)$ such that*

$$\delta_i(t_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

The set $\{\delta_1, \ldots, \delta_n\}$ is an L-basis for $\mathrm{Der}_K(L)$, so

$$\dim_L \mathrm{Der}_K(K(t_1, \ldots, t_n)) = n.$$

PROOF. a) This restates Exercise 12.6 and is immediate from Theorem 12.6. b) Applying part a) with $D = 0 \in \mathrm{Der}\, K$ gives the $\delta_1, \ldots, \delta_n$. Let $S = \{t_1, \ldots, t_n\}$. Then the map $\mathrm{Der}_K L \to L^S$ given by restricting any $D \in \mathrm{Der}_K L$ to S is a bijection. This restriction map is L-linear, hence it is an L-vector space isomorphism. $\square$

COROLLARY 12.8. *Let L/K be a separable algebraic extension.*

a) *Every derivation on K extends uniquely to a derivation on L.*
b) *We have $\mathrm{Der}_K(L) = 0$.*

PROOF. a) Step 1: suppose that $[L : K]$ is finite. By the Primitive Element Corollary (Corollary 5.3), we have $L = K[x]$ for some $x \in L$. The minimal polynomial $f \in K[t]$ of x is a generator of the ideal $I(x)$ of $K[t]$. By Theorem 12.6, if D_L extends K to L, then we have $0 = f^D(x) + f'(x)D_L(x)$. Since $K(x)$ is separable, we have $f'(x) = 0$, and thus

$$D_L(x) = \frac{-f^D(x)}{f'(x)}. \tag{42}$$

By Theorem 12.6, there is a unique $D_L \in \mathrm{Der}(L)$ extending D and satisfying (42). Step 2: Suppose that L/K is an infinite degree separable extension. It is therefore the direct limit of its finite separable subextensions L_α. By Step 1, there exists a unique $D_\alpha \in \mathrm{Der}_K(L_\alpha)$ extending D. Because of the uniqueness, it is automatic that these derivations fit together to give a derivation D_L on L: that is, for any $x \in L$, we choose α such that $x \in L_\alpha$ and put $D_L(x) = D_{L_\alpha}(x)$. If $x \in L_\alpha \cap L_\beta$ then the uniqueness forces $D_{L_\alpha}(x) = D_{L_\alpha L_\beta}(x) = D_{L_\beta}(x)$.
b) Let $D \in \mathrm{Der}_K(L)$. Then D extends $0 \in \mathrm{Der}(K)$, as does $0 \in \mathrm{Der}\, L$. By part a), we must have $D = 0$. □

EXERCISE 12.9. *Let $F \subseteq K \subseteq L$ be a tower of fields with L/K separable algebraic, and let M be a subextension of L/K. Show that for any F-derivation D of L such that $D(K) \subseteq K$, we have also $D(M) \subseteq M$.*

EXAMPLE 12.9. *Let K have characteristic $p > 0$, and let L/K be a nontrivial monogenic purely inseparable extension of degree p^a, so there $x \in L$ such that $L = K(x)$ and a is the least positive integer such that $y := x^{p^a} \in K$. Let $D \in \mathrm{Der}(K)$. The ideal $I(x)$ is generated by $f(t) = t^{p^n} - y$. For any $u \in L$ there is at most one extension of D to a derivation on L with $D(x) = u$, and by Theorem 12.6, such an extension exists if and only if*

$$0 = f^D(x) + f'(x)u = -D(y) + 0 \cdot u = -D(y).$$

In other words, if $D(y) \neq 0$, then D does not extend to L, while if $D(y) = 0$, we may extend it to L by arbitrarily prescribing its value at x. Taking $D = 0$, we find that evaluation at x gives an L-vector space isomorphism

$$\mathrm{Der}_K L \xrightarrow{\sim} L.$$

EXERCISE 12.10. *Let $L = K(x)$ be a monogenic inseparable algebraic extension. Show:* $\dim_L \mathrm{Der}_K L = 1$.

LEMMA 12.10. *Let K be a field of characteristic $p > 0$, and let L/K be an algebraic extension that is purely inseparable of exponent at most 1 (that is, $L \subseteq K^{1/p}$.) Let S be a set of generators for L/KS, and let $D \in \mathrm{Der}(K)$. The following are equivalent:*

(i) *D extends to a derivation on L.*
(ii) *For all $x \in S$, we have $D(x^p) = 0$.*

PROOF. (i) $\implies$ (ii): Note first that since L/K is purely inseparable of exponent 1, for all $x \in L$ we have $x^p \in K$, so condition (ii) makes sense. If D extends to a derivation on L, then for all $x \in L$, we have $D(x^p) = px^{p-1}D(x) = 0$.
(ii) $\implies$ (i): Consider the set $\mathcal{S}$ of pairs (M, D_M) such that M is a field with $K \subseteq M \subseteq L$ and $D_M \in \mathrm{Der}(M)$ is such that $D_M|_K = D$. On $\mathcal{S}$ we define the relation $(M, D_M) \preceq (M', D_{M'})$ if $M \subset M'$ and $D_{M'}|_M = D_M$. This makes $\mathcal{S}$ into

a partially ordered set in which the union over any chain is an upper bound, so by Zorn's Lemma the set $\mathcal{S}$ has a maximal element (M, D_M). If $M \neq L$, then there is $x \in L \setminus M$. Then $x^p \in K$ and $D_M(x^p) = D(x^p) = 0$, so by Example 12.9 we may extend D_M to a derivation $D_{M(x)}$ on $M(x)$, contradicting the maximality of (M, D_M). Thus $M = L$ and D_M is the desired extension of D to L. □

COROLLARY 12.11. *Let K be a field of characteristic $p > 0$, and let L/K be a purely inseparable extension of exponent 1, of finite degree p^n. Let $x_1, \ldots, x_n$ be a p-basis for L/K. Then:*

a) *There are unique $D_1, \ldots, D_n \in \mathrm{Der}_K(L)$ such that*

$$\forall 1 \leq i, j \leq n,\ D_i(x_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

b) *We have $\dim_L \mathrm{Der}_K(L) = n$.*

PROOF. a) The uniqueness of the D_i's is immediate from the fact that S is a set of generators for L/K. As for the existence, let $1 \leq i \leq n$. By Example 12.9, the 0-derivation on K extends to a unique derivation D_i on $K(x_i)$ with $D_i(x_i) = 1$. Let $j_1 \neq i$. Since $x_{j_1}^p \in K$, we have $D(x_{j_1}^p) = 0$, so by Example 12.9 D_i extends uniquely to a derivation on $K(x_i, x_{j_1})$ with $D_i(x_{j_1}) = 0$. Writing $\{1, \ldots, n\} \setminus \{i, j_1\} = \{j_2, \ldots, j_{n-1}\}$, the same argument works to extend D_i to $K(x_i, x_{j_1}, x_{j_2})$ and so forth, eventually to $K(x_1 \ldots, x_n) = L$.
b) Since S generates L/K, restriction to S gives an injection of L-vector spaces $E_S : \mathrm{Der}_K(L) \hookrightarrow L^S$. Under E_S the derivations $D_1, \ldots, d_n$ of part a) map to the standard basis vectors of L^S, so E_S is an L-vector space isomorphism. □

PROPOSITION 12.12. *For a finitely generated field extension L/K, the following are equivalent:*

(i) *The extension L/K is separable algebraic.*
(ii) *We have $\mathrm{Der}_K(L) = 0$.*

PROOF. (i) $\implies$ (ii): This is Corollary 12.8.
(ii) $\implies$ (i): If L/K is *not* separably generated (equivalently, is not separable), then there is a subextension F_1 of L/K such that L/F_1 is finite degree inseparable. By decomposing L/F_1 is purely inseparable over separable, one sees that there is a subextension M of L/F_1 such that L/M is purely inseparable monogenic. By Example 12.9 we have

$$(0) \subsetneq \mathrm{Der}_M(L) \subseteq \mathrm{Der}_K(L).$$

Otherwise L/K is separably generated and transcendental; let $x_1, \ldots, x_d$ be a separable transcendence basis, so $L/K(x_1, \ldots, x_d)$ is separable algebraic (in fact of finite degree, though this is not needed). Then $\delta_1 \in \mathrm{Der}_K(L(x_1, \ldots, x_n)) \setminus \{0\}$, and by Corollary 12.8 δ_1 extends (uniquely) to a nonzero element of $\mathrm{Der}_K(L)$. □

The following is an instance of derivations working for us rather than we for them.

COROLLARY 12.13. *Let $L = K(x_1, \ldots, x_n)$ be a finitely generated field extension. Suppose there are $f_1, \ldots, f_n \in I(x_1, \ldots, x_n) \subseteq K[x_1, \ldots, x_n]$ such that the matrix $(\partial_i f_j)(x_1, \ldots, x_n) \in M_n(L)$ is nonsingular. Then L/K is separable algebraic.*

PROOF. Let $D \in \mathrm{Der}_K(L)$. Since $f_j(x) = 0$, we have

$$0 = D(f_j(x)) = f^D(x) + \sum_{i=1}^n (\partial_i f_j)(x) D(x_i) = \sum_{i=1}^n (\partial_i f_j)(x) D(x_i).$$

The assumed nonsingularity of the matrix therefore gives $D(x_1) = \ldots = D(x_n) = 0$, so $D = 0$. By Proposition 12.12, we have that L/K is separable algebraic. □

THEOREM 12.14. *Let L/K be a finitely generated separable field extension.*

a) *If $\{x_1, \ldots, x_n\}$ is a separating transcendence basis for L/K, then there is an L-basis $\{D_i\}_{1 \leq i \leq n}$ for $\mathrm{Der}_K(L)$ such that for all $1 \leq i \leq n$, the restriction of D_i to $K(x_1, \ldots, x_n)$ is ∂_i.*

b) *We have $\dim_L \mathrm{Der}_K(L) = \mathrm{trdeg}(L/K)$.*

PROOF. a) Let $\{x_1, \ldots, x_n\}$ be separating transcendence basis for L/K, and put $M \coloneqq K(x_1, \ldots, x_n)$. Let $\delta_1, \ldots, \delta_n$ be the M-basis for $\mathrm{Der}_K(M)$ of Corollary 12.7. By Corollary 12.8, each δ_i extends uniquely to an element D_i of $\mathrm{Der}_K(L)$. We claim that $\{D_1, \ldots, D_n\}$ is an L-basis for $\mathrm{Der}_K(L)$.

If $D_1, \ldots, D_n$ were L-linearly dependent, then (since each $D_i \neq 0$), for some $2 \leq m \leq n$ we would have elements $a_i \in L$ such that $D_m = \sum_{1 \leq i < m} a_i D_i$. Evaluating this equation at t_m gives $1 = 0$, a contradiction.

Let $D \in \mathrm{Der}_K(L)$, and for $1 \leq i \leq n$, put $a_i \coloneqq D(t_i)$. Then the restriction of $D - \sum_{i=1}^n a_i D_i$ to M is zero, hence $D = \sum_{i=1}^n a_i D_i$ by Corollary 12.8.
b) This is immediate from part a). □

PROPOSITION 12.15. *Let K be a field of characteristic $p > 0$. For L/K a finitely generated field extension and $x \in L$, the following are equivalent:*

(i) *For all $D \in \mathrm{Der}_K(L)$, we have $D(x) = 0$.*

(ii) *We have $x \in KL^p$.*

PROOF. (i) $\implies$ (ii): We show the contrapositive: for $x \in L \setminus KL^p$, we will show that there is $D \in \mathrm{Der}_K(L)$ such that $D(x) \neq 0$. The field extension L/KL^p is inseparable algebraic and finitely generated, hence it is finite of some degree p^a. There is a tower of degree p (hence monogenic) purely inseparable field extensions

$$F_0 = KL^p \subsetneq F_1 = KL^p(x) \subsetneq F_2 \subsetneq F_a = L.$$

By Example 12.9 there is $D \in \mathrm{Der}_{KL^p}(KL^p(x))$ such that $D(x) = 1$. Inductively, having extended D to F_i, we may write $F_{i+1} = F_i(x_{i+1})$, so $x_{i+1}^p \in F_i$. But also $x_{i+1}^p \in KL^p$, so $D(x_{i+1}^p) = 0$. By Example 12.9 again we may extend D to F_{i+1}. Eventually we extend D to $F_a = L$.
(ii) $\implies$ (i): Let $D \in \mathrm{Der}_K(L)$. Then the kernel of the K-linear map D is a subfield of L that contains K (by assumption) and L^p (since $D(x^p) = pD(x)^{p-1} = 0$ in characteristic p), so the kernel contains KL^p. □

Finally we come to the general computation of $\dim_L \mathrm{Der}_K(L)$ that was promised.

THEOREM 12.16. *Let $L = K(x_1, \ldots, x_n)$ be a finitely generated field extension, and put*

$$d \coloneqq \dim_L \mathrm{Der}_K(L).$$

a) *Let m be the minimal cardinality of a set of elements $y_1, \ldots, y_m$ such that $L/K(y_1, \ldots, y_m)$ is separable algebraic. Then $m = t$.*

b) *If K has characteristic $p > 0$ then we have*

$$p^d = [L : KL^p].$$

c) *The extension L/K is separably generated if and only if $d = \mathrm{trdeg}(L/K)$.*

PROOF. a) If $L/K(y_1, \ldots, y_m)$ is separable algebraic, then $D \in \mathrm{Der}_K(L)$ is determined by its values on $y_1, \ldots, y_m$, which shows that $d \leq t$. To complete the proof of part a) we must find elements $y_1, \ldots, y_d$ such that $L/K(y_1, \ldots, y_d)$ is separable algebraic. If K has characteristic 0, then L/K is separable and by Theorem 12.14b) we have $d = \mathrm{trdeg}(L/K)$, so we may take $y_1, \ldots, y_d$ to be any transcendence basis for L/K. So suppose K has characteristic $p > 0$. We have $\mathrm{Der}_K(L) = \mathrm{Der}_{KL^p}(L)$, so $d = \dim_L \mathrm{Der}_{KL^p}(L)$. The extension L/KL^p is finitely generated and $L \subset (KL^p)^{1/p}$, so Corollary 12.11 applies to show that there are elements $y_1, \ldots, y_d$ of L and $D_1, \ldots, D_d \in \mathrm{Der}_K(L)$ such that $D_i(y_j) = \delta(i, j)$ (Kronecker delta). Then $\{D_1, \ldots, D_d\}$ is an L-basis for $\mathrm{Der}_K(L)$, so if $D = \sum_{i=1}^d \alpha_i D_i \in \mathrm{Der}_K(L)$ vanishes on $y_1, \ldots, y_d$, then $D = 0$. This shows that $\mathrm{Der}_{K(y_1,\ldots,y_d)}(L) = 0$, so by Proposition 12.12 we get that $L/K(y_1, \ldots, y_d)$ is separable algebraic.
b) In the proof of part a), we saw that in characteristic $p > 0$ we have $d = \dim_L \mathrm{Der}_{KL^p}(L)$, so Corollary 12.11 gives $[L : KL^p] = p^{\dim_L \mathrm{Der}_{KL^p}(L)} = p^d$.
c) If L/K is separably generated, then Theorem 12.14b) gives $d = \mathrm{trdeg}(L/K)$. Conversely, if $\mathrm{trdeg}(L/K) = m$ and there are $y_1, \ldots, y_m \in L$ such that $L/K(y_1, \ldots, y_m)$ is separable algebraic, then $y_1, \ldots, y_m$ are algebraically independent over K hence yield a separating transcendence basis. Thus L/K is separably generated. □

COROLLARY 12.17. *Let K be a field of characteristic $p > 0$, and let L/K be purely inseparable of finite degree. Then the minimal number of generators for L/K is $\dim_L \mathrm{Der}_K L$.*

PROOF. By Theorem 12.16a), $\dim_L \mathrm{Der}_K L$ is the minimal size of a subset S of L such that $L/K(S)$ is separable algebraic. Since L/K is purely inseparable, the extension $L/K(S)$ is separable algebraic if and only if $K(S) = L$. □

COROLLARY 12.18. *Let K be a perfect field of characteristic $p > 0$, and let L/K be finitely generated of transcendence degree d. Then for all $n \in \mathbb{Z}^+$ we have*

$$[L : L^{p^n}] = p^{dn}.$$

PROOF. Step 1: First suppose that $n = 1$. Since K is perfect, we have that L/K is separably generated and $KL^p = K^pL^p = L^p$. By parts b) and c) of Theorem 12.16 we get $p^d = [L : L^p]$.
Step 2: Applying Step 1 to each extension in the tower

$$L^{p^n} \subseteq L^{p^{n-1}} \subseteq \ldots \subseteq L^p \subseteq L$$

yields the general case. □

1.4. Derivations in Infinitely Generated Field Extensions.

PROPOSITION 12.19. *Let K be a field, let S a set and let $L \coloneqq K(\{t_s\}_{s \in S})$ be a rational function field in a set of indeterminates indexed by S.*

a) *For $s \in S$, there is a unique K-derivation δ_s of L such that $\delta_s(t_s) = 1$ and $\delta_s(t_{s'}) = 0$ for all $s' \neq s$.*
b) *The set $\{\delta_s\}_{s \in S}$ is an L-basis for $\mathrm{Der}_K^S(L)$.*

PROOF. a) For each finite subset W of S that contains s, there is a unique K-derivation D_W on $K_W \coloneqq K(\{t_s \mid s \in W\})$ such that $D_W(t_s) = 1$ and for each $w \in W \setminus \{s\}$ we have $D_W(t_w) = 0$. When $W_1 \subset W_2$, we have $K_{W_1} \subset K_{W_2}$ and $(D_{W_2})|_{K(W_1)} = D_{W_1}$. Since L is the direct limit of the subfields K_W, it follows that there is a unique derivation D on L that extends this compatible family of derivations on the subfields. This derivation satisfies the required properties of δ_s, and it is unique because L is generated by K and the elements t_i for $i \in S$.
b) In Proposition 12.5, we saw that the natural map $r : \mathrm{Der}_K^S(L) \to L^S$ obtained by restricting each derivation to S was injective and L-linear. Under this map r, the derivations δ_s map to an L-basis for L^S. It follows that r is an L-vector space isomorphism and thus $\{\delta_s\}_{s\in S}$ is an L-basis. □

EXERCISE 12.11. *Let K be a field, S an infinite set, and let $L = K(\{t_s \mid s \in S\})$ be the rational function field in a set of indeterminates parameterized by S. Let L^S be the L-vector space of* all *functions from S to L. Show that restriction to S gives an L-isomorphism*

$$\mathrm{Der}_K(L) \xrightarrow{\sim} L^S.$$

Deduce that $\dim_L \mathrm{Der}_K L > \#S$.

THEOREM 12.20. *For a field extension K/F, the following are equivalent:*

(i) *The extension K/F is separable.*
(ii) *Every derivation on F extends to a derivation on K.*

PROOF. (i) $\implies$ (ii): First suppose that F has characteristic 0, so there is a separating transcendence basis $\{x_i\}_{i\in I}$ for K/F. If $D \in \mathrm{Der}\, F$, then for any finite subset $J \subset I$, by Corollary 12.7a) there is a unique extension of D to $F(\{x_i \mid i \in J\})$ such that $D(x_i) = 0$ for all $i \in J$. These derivations piece together to give a unique extension of D to $F(\{x_i \mid i \in I\})$ such that $D(x_i) = 0$ for all $i \in I$. By Corollary 12.8, since $K/F(\{x_i \mid i \in I\})$ is separable algebraic, D extends uniquely to a derivation on K.[2]

Now suppose that F has characteristic $p > 0$. Since K/F is separable, the fields $F^{1/p}$ and K are linearly disjoint over F; applying the pth power map to all these fields, we get that F and K^p are linearly disjoint over F^p. Let $\{u_i\}_{i\in I}$ be a basis for K^p as an F^p-vector space, one of whose elements is 1. Then there are elements $\gamma_{i,j,k} \in F^p$ such that

$$\forall i, j \in I,\ u_i u_j = \sum_k \gamma_{i,j,k} u_k.$$

By linear disjointness, $\{u_i\}_{i\in I}$ is an F-linearly independent subset of K, and its F-span is the ring $F[K^p]$.

Let $D \in \mathrm{Der}(F)$. Every element $x \in F[K^p]$ has a unique expression as a finite sum $\sum_{i\in I} x_i u_i$ with $x_i \in F$. We put

$$\overline{D}(x) \coloneqq \sum_{i\in I} D(x_i) u_i.$$

[2]As should be clear, this argument is valid whenever K/F is separably generated.

The map $\overline{D} : F[K^p] \to K$ is clearly additive. Moreover, for $x = \sum_{i \in I} x_i u_i$, $y = \sum_{i \in I} y_i u_i \in F[K^p]$, then since $D(\gamma_{i,j,k}) = 0$ for all $\gamma_{i,j,k} \in F^p$ we have

$$\overline{D}(xy) = \overline{D}(\sum_{i,j,k} x_i y_j \gamma_{i,j,k} u_k)$$

$$= \sum_{i,j,k} (D(x_i)y_j + s_i D(y_j))\gamma_{i,jk})u_k = x\overline{D}(y) + \overline{D}(x)y.$$

Thus $\overline{D}$ is a derivation on $F[K^p]$, and it extends D since one of the u_i's is 1. By Theorem 12.3 the derivation $\overline{D}$ extends uniquely to FK^p. If $x = \sum_i x_i u_i \in K^p$, then each x_i lies in F^p so $D(x_i) = 0$ and thus $\overline{D}(x) = \sum_i D(x_i)u_i = 0$, so $\overline{D} \in \mathrm{Der}_{K^p}(FK^p)$. Lemma 12.10 now implies that $\overline{D}$ extends to a derivation on K.

(ii) $\implies$ (i): Suppose that every derivation on F extends to a derivation on K. We may of course assume that F and K have characteristic $p > 0$, for in characteristic 0 every field extension is separable. By Exercise 11.11 it suffices to show that if S is an F-linearly independent subset of K, then $S^p = \{x^p \mid x \in S\}$ is also F-linearly independent. Assuming not, let n be the minimal cardinality of an F-linearly dependent subset of S^p. Then there are elements $x_1, \ldots, x_n \in S$ and $a_2, \ldots, a_n \in F^\times$ such that

$$x_1^p + \ldots + a_n x_n^p = 0. \tag{43}$$

Let $D \in \mathrm{Der}(F)$ and extend it to a derivation on K, which we continue to denote by D. Since for all $x \in K$ we have $D(x^p) = 0$, applying D to (43) gives

$$0 = D(1)x_1^p + D(a_2)x_2^p + \ldots + D(a_n)x_n^p = D(a_2)x_2^p + \ldots + D(a_n)x_n^p.$$

By the minimality of n we have $D(a_2) = \ldots = D(a_n) = 0$. Applying Proposition 12.15 with $K = \mathbb{F}_p$ and $L = F$, we get that $a_2, \ldots, a_n \in F^p$, i.e., there are $b_2, \ldots, b_n \in F^\times$ such that $a_i = b_i^p$ for all $2 \leq n$, and then (43) implies that $x_1 + b_2 x_2 + \ldots + b_n x_n = 0$, contradicting the F-linear independence of $x_1, \ldots, x_n$. □

We can now characterize fields F such that $\mathrm{Der}(F) = 0$:

Exercise 12.12. *Let F be a field.*

a) *Suppose that F has characteristic 0. Show: $\mathrm{Der}(F) = 0$ if and only if $F/\mathbb{Q}$ is algebraic.*
b) *Suppose that F has characteristic $p > 0$. Show: $\mathrm{Der}(F) = 0$ if and only if F is perfect.*

The next two exercises explore whether Proposition 12.12 extends to infinitely generated field extensions.

Exercise 12.13. *For a field extension L/K in characteristic 0, show that the following are equivalent:*

(i) *L/K is algebraic.*
(ii) *$\mathrm{Der}_K(L) = 0$.*

Exercise 12.14. *Let p be a prime number.*

a) *Find a field K of characteristic p and an inseparable algebraic field extension L/K such that $\mathrm{Der}_K(L) = 0$.*
b) *Let κ be a cardinal number. Find a field K of characteristic p and a separable extension L/K of transcendence degree κ with $\mathrm{Der}_K(L) = 0$.*

2. Kähler Differentials

Let $B \subset A$ be an extension of commutative rings. We define the **module of Kähler differentials** $\Omega_{A/B}$ to be the quotient of the free A-module $\tilde{A}$ on the set $\{da \mid a \in A\}$ (here we understand that for each $a \in A$ we have a formal symbol da, such that the map $a \mapsto da$ is injective) via the following submodule R of relations:

$$\forall a, b \in A,\ d(a+b) - da - db,$$

$$\forall a, b \in A, d(ab) - (adb + bda),$$

$$\forall \alpha \in B,\ d\alpha.$$

The effect of this is that we get a map

$$d : A \to \Omega_{A/B},\ a \mapsto da.$$

By construction, d is a B-derivation. Moreover it is universal among all B-derivations into an A-moduule M in the following sense.

PROPOSITION 12.21. *If M is an A-module and $D : A \to M$ is a B-derivation, then there is a unique A-module homomorphism $f : \Omega_{A/B} \to M$ such that $D = f \circ d$.*

PROOF. There is a unique A-module homomorphism $\tilde{f} : \tilde{A} \to M$ such that for all $a \in A$, $\tilde{f}(da) = D(a)$. For all $a, b \in A$, we have

$$\tilde{f}(d(a+b)-d(a)-d(b)) = \tilde{f}(d(a+b))-\tilde{f}(d(a))-\tilde{f}(d(b)) = D(a+b)-D(a)-D(b) = 0,$$

$$\tilde{f}(d(ab) - adb - bda) = \tilde{f}(d(ab)) - a\tilde{f}(db) - b\tilde{f}(da) = D(ab) - aD(b) - bD(a) = 0,$$

and for all $\alpha \in B$ we have

$$\tilde{f}(d\alpha) = D(\alpha) = 0.$$

Thus $\tilde{f}$ factors through $f : \Omega_{A/B} \to M$ and has the property that for all $a \in A$, $f(da) = D(a)$, so $D = f \circ d$. Conversely, any such f satisfies $f(da) = D(a)$ for all $a \in A$, and since $\{da\}_{a \in A}$ generate $\Omega_{A/B}$ as an A-module, the map is unique. □

EXERCISE 12.15. *Let $B \subset A$ be a ring extension.*

(i) *If S is a set of generators for B as an A-algebra (that is, every element of B is an A-linear combination of products of elements of S), then $\{ds \mid s \in S\}$ is a set of generators for $\Omega_{A/B}$ as an A-module.*
(ii) *Suppose that A and B are fields and $A = B(S)$. Show that the elements $\{ds \mid s \in S\}$ span $\Omega_{A/B}$ as an A-vector space.*

We can restate Proposition 12.21 as giving a natural A-module isomorphism

$$\mathrm{Der}_B(A, M) = \mathrm{Hom}_A(\Omega_{A/B}, M).$$

In particular, taking $M = A$, we get

$$\mathrm{Der}_B(A) = \mathrm{Hom}_A(\Omega_{A/B}, A) = \Omega_{A/B}^{\vee}. \tag{44}$$

That is, the B-derivations of A are the A-linear functionals on $\Omega_{A/B}$. In particular:

COROLLARY 12.22.

a) *Suppose $\Omega_{A/B}$ is finitely generated and free as an A-module. Then $\mathrm{Der}_B(A)$ is finitely generated and free as an A-module and $\mathrm{rank}\,\mathrm{Der}_B(A) = \mathrm{rank}\,\Omega_{A/B}$.*
b) *Let L/K be a finitely generated field extension. Then*

$$\dim_L \Omega_{L/K} = \dim_L \mathrm{Der}_K(L) < \infty.$$

PROOF. a) This just uses the fact that the dual of a finitely generated free module is a finitely generated free module of the same rank.
b) If $\Omega_{L/K}$ were infinite-dimensional, then so would be its dual space and thus $\mathrm{Der}_K(L)$ would be infinite-dimensional, but the number of generators of L/K is an upper bound on $\dim_L \mathrm{Der}_K(L)$. So $\Omega_{L/K}$ is a finite-dimensional L-vector space, and we may now apply part a). □

We say a ring extension $B \subset A$ is **omega-finite** if $\Omega_{A/B}$ is a finitely generated A-module and **omega-free** if $\Omega_{A/B}$ is a free A-module. Evidently omega-freeness automatic when A is a field. For a field extension L/K, we saw above that omega-finiteness holds if and only if $\mathrm{Der}_K(L)$ is a finite-dimensional L-vector space, hence it holds if L/K is either finitely generated or separably generated and of finite transcendence degree. In this case, we have

$$\Omega_{L/K} \xrightarrow{\iota} \Omega_{L/K}^{\vee\vee} = \mathrm{Der}_K(L)^{\vee},$$

where ι is the natural isomorphism of a finite-dimensional vector space with its second dual space given by evaluating linear functionals on V at points of V. Under this isomorphism, for $\sum_{i=1}^n a_i dx_i \in \Omega_{L/K}$ and $D \in \mathrm{Der}_K(L)$ we have

$$(\sum_{i=1}^n a_i dx_i)(D) = \sum_{i=1}^n a_i D(x_i).$$

Let L/K be an omega-finite field extension. By Exercise 12.15, the elements $\{dx \mid x \in L\}$ span $\Omega_{L/K}$ as an L-vector space. It follows that there is a finite subset S of L such that the map $s \mapsto ds$ is injective and the set $\{ds \mid s \in S\}$ is an L-basis for $\Omega_{L/K}$. We call S a **differential basis for** L/K. By the above considerations, there is then a unique dual basis $\{D_s\}_{s\in S}$ for $\mathrm{Der}_K(L)$ such that for all $s, s' \in S$ we have $D_s(s') = \begin{cases} 1 & \text{if } s = s' \\ 0 & \text{otherwise} \end{cases}$. Let us call $\{D_s\}_{s\in S}$ the **dual differential basis**.

THEOREM 12.23.
Let L/K be a finitely generated field extension, and let $x_1, \ldots, x_n \in L$.

a) *If $\{x_1, \ldots, x_n\}$ is a separating transcendence basis for L/K, then $\{dx_1, \ldots, dx_n\}$ is an L-basis for $\Omega_{L/K}$.*
b) *Suppose that L/K is separable. If $\{dx_1, \ldots, dx_n\}$ is an L-basis for $\Omega_{L/K}$, then $\{x_1, \ldots, x_n\}$ is a separating transcendence basis for L/K.*

PROOF. a) If $x_1, \ldots, x_n$ is a separating transcendence basis for L/K, then for all $1 \leq i \leq n$ there is a unique $D_i \in \mathrm{Der}_K(L)$ such that $D_i(x_j) = \delta(i,j)$ and $D_1, \ldots, D_n$ is an L-basis of $\mathrm{Der}_K(L)$. Since $\mathrm{Der}_K(L) = \Omega_{L/K}^{\vee}$, this basis is the dual basis of a unique L-basis $b_1, \ldots, b_n$ of $\Omega_{L/K}$: that is, for all $1 \leq i, j \leq n$, we have $D_i(b_j) = \delta(i,j)$. We have identified D_i with an L-linear functional ℓ_i on $\Omega_{L/K}$: this functional is the unique one such that for all $x \in L$ we have $\lambda_i(dx) = D_i(x)$. Thus for all $1 \leq i, j, \leq n$ we have $\lambda_i(dx_j) = D_i(x_j) = \delta(i,j)$, and it follows that we have $b_1 = dx_1, \ldots, b_n = dx_n$.
b) Suppose $dx_1, \ldots, dx_n$ is an L-basis for $\Omega_{L/K} = \mathrm{Der}_K(L)^{\vee}$. First of all this gives that $\dim \mathrm{Der}_K(L) = n$, and since L/K is finitely generated and separable, by Theorem 12.14 we get that $\mathrm{trdeg}(L/K) = n$.

Now, let $D \in \mathrm{Der}_K(L)$ be such that for all $1 \leq i \leq n$ we have $0 = dx_i(D) = D(x_i)$. Since the dx_i's span $\mathrm{Der}_K(L)^{\vee}$ this implies $D = 0$, which shows that

$\mathrm{Der}_K(L) = \mathrm{Der}_{K(x_1,\dots,x_n)}(L)$. Using Proposition 12.12 we get that $L/K(x_1,\dots,x_n)$ is separable algebraic, so $x_1,\dots,x_n$ is a separating transcendence basis for L/K. □

EXERCISE 12.16. *Show that Theorem 12.23 holds without the hypothesis that L/K is finitely generated.*

3. Applications to One Variable Function Fields

COROLLARY 12.24. *Let K be a field of characteristic $p > 0$, and let L/K be finitely generated and separable, of transcendence degree 1.*

a) *For $x \in L$, the following are equivalent:*
   (i) *We have that x is a **separating element** for L/K – i.e., $\{x\}$ is a separating transcendence basis for L/K.*
   (ii) *We have $dx \neq 0$.*
   (iii) *We have that $x \notin KL^p$.*
   If K is perfect, the conditions are also equivalent to $x \notin L^p$.
b) *For each separating element x of L/K, there is a unique derivation $\delta_x \in \mathrm{Der}_K(L)$ such that $\delta_x(x) = 1$.*
c) *For elements x, y of L/K with y separating, we have*

$$\delta_y = \delta_y(x)\delta_x.$$

d) *For $y \in K$, $\delta_x(y) \neq 0$ if and only if y is a separating element of L/K.*

PROOF. a) Theorem 12.23 shows (i) $\iff$ (ii). Since $\Omega_{L/K}$ is the L-dual of the one-dimensional L-vector space $\mathrm{Der}_K(L)$, for any $x \in L$ we have $dx = 0$ if and only if $D(x) = 0$ for all $D \in \mathrm{Der}_K(L)$ if and only if $x \in KL^p$ by Proposition 12.15, showing (ii) $\iff$ (iii).
b) Theorem 12.14a) supplies $\delta_x \in \mathrm{Der}_K(L)$ such that $\delta_x(x) = 1$, while Theorem 12.14b) shows that $\dim_L \mathrm{Der}_K(L) = 1$, which implies that this derivation is unique.
c) Since δ_y is nonzero in the one-dimensional vector space $\mathrm{Der}_K(L)$, there is a unique $\alpha \in L^\times$ such that $\delta_y = \alpha\delta_x$. Evaluating at x gives $\alpha = \delta_y(x)$.
d) If y is a separating element of L/K then it follows from part c) that $\delta_x(y) = \frac{1}{\delta_y(x)} \neq 0$. If y is not separating, then by part a) we have $dy = 0$ and thus

$$0 = dy(\delta_x) = \delta_x(y).$$ □

COROLLARY 12.25. *Let k be a perfect field of characteristic $p > 0$, let K/k be finitely generated of transcendence degree 1, and let L/K be an inseparable algebraic field extension. Then $L \supseteq K^{1/p}$.*

PROOF. Let K_s be the maximal separable subextension of L/K. Then all the hypotheses apply to L/K_s in place of L/K, and if we can show that $L \supseteq K_s^{1/p}$ then that suffices, since $K_s^{1/p} \supseteq K^{1/p}$. Because of this we may assume that L/K is a nontrivial purely inseparable extension, and thus there is $\alpha \in L \setminus K$ such that $x = \alpha^p \in K$. We have

$$K \subsetneq K(\alpha) \subseteq K^{1/p},$$

so by Corollary 12.18 we get

$$L \supseteq K(\alpha) = K^{1/p}.$$ □

EXERCISE 12.17. *Let k be a perfect field of characteristic $p > 0$, let K/k be finitely generated of transcendence degree 1, and let L/K be a finite degree extension. Let K_s be the maximal separable subextension of L/K, so $[L : K_s] = p^a$ for some $a \in \mathbb{N}$. Show: $L = K^{p^{-a}}$.*

We have developed field theory to the point where it is essentially algebraic geometry in disguise. For instance, Corollary 12.25 carries all the content of the following fact: if $f : C_1 \to C_2$ is a finite morphism of nice curves defined over a perfect field k of characteristic $p > 0$, then it factors as a Frobenius map $C_1 \to C_1^{p^a}$ followed by a separable morphism $C_1^{p^a} \to C_2$ [**Si**, Cor. II.2.12]. (It also calls attention to the fact that the ground field k should be perfect for this to hold.)

4. p-Bases

Throughout this section we work with fields of a fixed characteristic $p > 0$.

LEMMA 12.26. *Let F be a field of characteristic p, and let $S \subset F$. Let $\overline{S}$ be the set of all F^p-linear combinations of monomials $x_1^{i_1} \cdots x_n^{i_n}$ with $x_1, \ldots, x_n \in S$ and $0 \leq i_1, \ldots, i_n < p$. Then $\overline{S} = F^p(S)$.*

PROOF. We have $F^p(S) = \varinjlim F^p(T)$ as T ranges over finite subsets of S and $\overline{S} = \varinjlim \overline{T}$ as T ranges over all finite subets of S. So it suffices to show that $\overline{S} = F^p(S)$ for all finite subsets $S \subset F$. The inclusion $\overline{S} \subset F^p(S)$ is clear. Conversely, because S is finite and consists of elements algebraic over F^p, we have $F^p(S) = F^p[S]$: that is, each element of $F^p(S)$ is an F^p-linear combination of monomials $x_1^{a_1} \cdots x_n^{a_n}$ with $x_1, \ldots, x_n \in S$ and $a_1, \ldots, a_n \in \mathbb{N}$. For $1 \leq i \leq n$, write $a_i = pb_i + r_i$ with $0 \leq r_i < p$. Then

$$x_1^{a_1} \cdots x_n^{a_n} = (x_1^{b_1} \cdots x_n^{b_n})^p x_1^{r_1} \cdots x_n^{r_n} = \alpha x_1^{r_1} \cdots x_n^{r_n}$$

with $\alpha \in F^p$. This completes the proof. □

A **p-spanning subset** is a subset $S \subset F$ such that $\overline{S} = F$. On the other hand:

LEMMA 12.27. *For a subset $S \subset F$, the following are equivalent:*

(i) *For every finite subset $\{s_1, \ldots, s_n\} \subset S$, the set of monomials $s_1^{i_1} \cdots s_n^{i_n}$ with $0 \leq i_1, \ldots, i_n < p$ is F^p-linearly independent.*
(ii) *For all $s \in S$, we have $s \notin \overline{S \setminus \{s\}}$.*

*A subset satisfying these equivalent conditions is called a **p-independent subset**.*

PROOF. We easily reduce to the case where S is finite. (i) $\implies$ (ii): If (ii) fails, then we may write $S = \{s_1, \ldots, s_n, x\}$ such that $x \in \sum_I s_1^{i_1} \cdots s_n^{i_n}$ for $0 \leq i_1, \ldots, i_n < p$. It is clear that this violates the condition in (i).
(ii) $\implies$ (i): Let $S = \{s_1, \ldots, s_n\}$. A nontrivial F^p-linear dependence relation among the monomials $s_1^{i_1} \cdots s_n^{i_n}$ yields, after reordering the s_i's if necessary, a nonzero polynomial $f \in F^p(s_1, \ldots, s_{n-1})$ of degree less than p satisfied by s_n. This means that s_n is both separable and purely inseparable over $F^p(s_1, \ldots, s_{n-1})$, so $s_n \in F^p(s_1, \ldots, s_{n-1}) = \overline{S \setminus \{s\}}$, a contradiction. □

Probably the reader suspects what is coming next: we claim that for subsets S of F, the mapping $S \mapsto \overline{S} = F^p(S) \subset F$ is a spanning operator in the sense of §11.4. The properties (SO1) through (SO4) hold immediately: in fact, for any subfield A of a field F, the operator $S \subset F \mapsto A(S)$ satisfies these properties. We now check

(SO5) ("Exchange Lemma"): for $x, y \in F$ and $S \subset F$, if $y \in \overline{S \cup \{x\}} \setminus \overline{S}$, we must show that $x \in \overline{S \cup \{y\}}$.

If $y \in \overline{S \cup \{x\}}$ then there are $s_1, \ldots, s_n \in S$ and for all $I = (i_1, \ldots, i_{n+1}) \in \{0, \ldots, p-1\}^{n+1}$ an element $\alpha_I \in F^p$ such that

$$y = \sum_I \alpha_I s_1^{i_1} \cdots s_n^{i_n} x^{i_{n+1}}.$$

Because $y \notin \overline{S}$, there is at least one I with $i_{n+1} \neq 0$ such that $\alpha_I \neq 0$ and this shows that x satisfies a polynomial relation of degree less than p with coefficients in $F^p(S, y)$. In other words, x is separable algebraic over $F^p(S, y)$, but it is also purely inseparable over $F^p(S, y)$, so $x \in F^p(S, y) = \overline{S \cup \{y\}}$.

A **p-basis** for F is a subset $S \subset F$ that is both p-independent and p-spanning. By the abstract theory developed in §11.4, we know: a subset $S \subset F$ is a p-basis if and only if it is a maximal p-independent subset if and only if it is a minimal p-spanning subset. Moreover, every p-independent subset is contained in a p-basis, every p-spanning usbset contains a p-basis, and any two p-bases have the same cardinality, which we call the **p-dimension** $\dim_p F$ of F.

COROLLARY 12.28. *Let F be a field of characteristic $p > 0$.*

a) *The following are equivalent:*
   (i) *The extension F/F^p has finite degree.*
   (ii) *The field F has finite p-dimension.*

b) *When the equivalent conditions of part a) hold, we have $[F : F^p] = p^{\dim_p F}$.*

PROOF. a) The extension F/F^p has finite degree if and only if F has a finite p-spanning set if and only if F has a finite p-basis.
b) If $S = \{s_1, \ldots, s_n\}$ is a p-basis then $\{s_1^{i_1} \cdots s_n^{i_n} \mid 0 \leq i_1, \ldots, i_n < p\}$ is an F^p-basis for F. □

EXERCISE 12.18. *Let F be a field of characteristic $p > 0$ such that $\dim_p(F)$ is infinite. Show: $[F : F^p] = \dim_p(F)$.*

We can use derivations to give a characterization of p-independent subsets:

THEOREM 12.29. *Let F be a field of characteristic $p > 0$, and let S be a subset of F. The following are equivalent:*

(i) *The subset S is p-independent.*
(ii) *For all $x \in S$ there is a $D_x \in \mathrm{Der}_{F^p}(F)$ such that for all $s \in S$ we have*

$$D_x(s) = \begin{cases} 1 & s = x \\ 0 & s \neq x \end{cases}.$$

PROOF. (i) $\implies$ (ii): Suppose that S is p-independent, and let $\mathcal{S}$ be the set of subsets $T \subset S$ such that for all $t \in T$ there is $D_{T,t} \in \mathrm{Der}_{F^p}(F^p(T))$ such that $D_{T,t}(t) = 1$ and $D_{T,t}(t') = 0$ for all $t' \in T \setminus \{t\}$, partially ordered under inclusion. For any chain $\{T_i\}_{i \in I}$ in $\mathcal{S}$, the union $\bigcup_{i \in I} T_i$ is an upper bound: the derivation $D_{T,t}$ is uniquely determined by its properties, so if $t \in T_1 \subset T_2$ then the restriction of $D_{T_2,t}$ to $F^p(T_1)$ is $D_{T_1,t}$. For any $t \in \bigcup_{i \in I} T_i$, the existence and uniquenessf of the derivation $D_{\bigcup_{i \in I} T_i, t}$ follows easily from this. By Zorn's Lemma the set $\mathcal{S}$ has a maximal element T. If $T \subsetneq S$, choose $s \in S \setminus T$; by the p-independence of S we

have $s \notin F^p(T)$ and $s^p \in F^p \subset F^p(T)$, so by Example 12.9, for all $\alpha \in F^P(T \cup \{s\})$, each derivation $D \in \mathrm{Der}_{F^p}(F^p(T))$ admits a unique extension to $F^p(T \cup \{s\})$ such that $D(s) = \alpha$. For all $t \in T$, extending $D_{T,t}$ by $D(s) = 0$ yields the derivation $D_{S,t}$, while extending the 0 derivation on $F^p(T)$ to $F^p(T \cup \{s\})$ by $D(s) = 1$ yields the derivation $D_{S,s}$. This shows that $T \cup \{s\} \in \mathcal{S}$, contradicting the maximality of T. It follows that $T = S$.

$\neg$ (i) $\implies$ $\neg$ (ii): If the subset S is not p-independent, then there is $s \in S$ such that $s \in F^p(S \setminus \{s\})$. It follows that every $D \in \mathrm{Der}_{F^p}(F)$ such that $D(t) = 0$ for all $t \neq s$ also satisfies $D(s) = 0$. □

COROLLARY 12.30. *Let F be a field of characteristic $p > 0$. For $S \subset F$, the following are equivalent:*

(i) *The subset S is a p-basis for F.*
(ii) *The map $s \mapsto ds$ is injective and $\{ds \mid s \in S\}$ is a basis for Ω_{F/F^p}.*

PROOF. (i) $\implies$ (ii): Let S be a p-basis for F.

Since S is a p-spanning subset of F we have $F = F^p(S)$, so by Exercise 12.15 the set $\{ds \mid s \in S\}$ spans Ω_{F/F^p}.

Since S is a p-independent subset, applying Theorem 12.29 gives a family of derivations $\{D_x \mid x \in S\}$ such that for all $y \in S$, we have

$$D_x(y) = \begin{cases} 1 & y = x \\ 0 & y \neq x \end{cases}.$$

Regarding $\mathrm{Der}_{F^p}(F)$ as the F-vector space dual of Ω_{F/F^p}, we have

$$\forall x, y \in S,\ D_x(dy) = D_x(y) = \begin{cases} 1 & y = x \\ 0 & y \neq x \end{cases}.$$

Thus if dx were an F-linear combination of elements dy with $y \in S \setminus \{x\}$, evaluating at D_x gives $1 = 0$, a contradiction. So the dx's are distinct elements and form an F-linearly independent subset of Ω_{F/F^p}.

(ii) $\implies$ (i): Suppose that $x \in S \mapsto dx$ is an injection and that $\{dx \mid x \in S\}$ is an F-basis for Ω_{F/F^p}. Because $\mathrm{Der}_{F/F^p} = \Omega^\vee_{F/F^p}$, there is a unique family of derivations $\{D_x \mid x \in S\}$ such that $D_x \in \mathrm{Der}_{F^p}(F)$ and for all $x, y \in S$ we have $D_x(y) = \begin{cases} 1 & y = x \\ 0 & y \neq x \end{cases}$. Theorem 12.29 implies that S is a p-independent subset. If it were not a p-basis, there would be a strictly larger p-independent subset $\tilde{S} = S \cup \{s\}$, and Theorem 12.29 implies that there is $D_s \in \mathrm{Der}_{F^p}(F)$ such that $D_s(s) = 1$ and $D_s(x) = 0$ for all $x \in S$. But then on the one hand we would have $D_s(ds) = D_s(s) = 1$, and on the other hand, since ds is an F-linear combination of dx for $x \in S$, we would have $D_s(ds) = 0$, a contradiction. □

Corollary 12.30 is an example of how Kähler differentials behave better than derivations in non-omega finite extensions. Indeed, when $\Omega_{K/F}$ is infinite-dimensional as a K-vector space, its dual vector space $\mathrm{Der}_F(K)$ is an infinite vector space of larger dimension. If we choose a **differential basis** for K/F – i.e., a subset S of K such that $s \mapsto ds \in \Omega_{K/F}$ is injective and $\{ds \mid s \in S\}$ is a K-basis for $\Omega_{K/F}$ – then there is a "dual basis" $\{D_s \mid s \in S\}$ of F-derivations of K characterized by the usual

relation $D_x(y) = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases}$ for all $x, y \in S$. However this dual basis is a basis not for $\mathrm{Der}_F(K)$ but for the subspace $\mathrm{Der}_F^S(K)$ of S-finite derivations, a subspace which depends strongly on the choice of S.

EXERCISE 12.19. *An extension of characteristic p fields $F \subseteq K$ is **p-radical** if $K \subset F^{1/p}$: in other words, K is obtained by adjoining pth roots of elements of F. For any p-radical extension K/F and any subset $S \subseteq K$, define $\overline{S} := F(S)$.*

a) *Show that $\overline{S}$ is the F-span of monomials $s_1^{i_1} \cdots s_n^{i_n}$ with $s_1, \ldots, s_n \in S$ and $0 \leq i_1, \ldots, i_n < p$.*

b) *Extend the theory of p-spanning subsets, p-independent subsets and p-bases to p-radical extensions K/F. Show in particular:*

(i) *The extension K/F has a p-basis – a subset S such that $K = F(S)$ and for all $s \in S$, $s \notin F(S \setminus \{s\})$ – and any two p-bases have the same cardinality.*

(ii) *If S is a finite p-basis for K/F, then $[K : F] = p^{\#S}$, while if S is an infinite p-basis for K/F, then $[K : F] = \#S$.*

(iii) *A subset $S \subset F$ is a p-basis if and only if $s \mapsto ds \in \Omega_{K/F}$ is injective and $\{ds \mid s \in S\}$ is an F-basis for $\Omega_{K/F}$.*

(iv) *For $x \in F$, we have $dx = 0 \in \Omega_{K/F}$ if and only if $x \in F$.*

5. Faith's Monotonicity Theorems

In this section we cover a lovely short paper of C. Faith [**Fa61**]. As motivation, for a finitely generated field extension K/F, let $\mathrm{ng}(K/F)$ denote the minimum size of a set of generators for K/F. Let us collect what we already know about this invariant:

• We have $\mathrm{ng}(K/F) \geq \mathrm{trdeg}(K/F)$, with equality if and only if K/F is purely transcendental. (Indeed, the transcendence degree of $K(x)/K$ is 0 or 1 according to whether K is algebraic or transcendental, which gives the equality. If K/F has transcendence degree r and can be generated by r elements, these elements must be algebraically independent over F: if not and we add generators one by one, then at least once we get an algebraic extension.)

• If K/F is algebraic (and thus of finite degree), we have $\mathrm{ng}(K/F) = 0$ if and only if the subfield lattice $\mathcal{L}(K/F)$ is finite (Primitive Element I), and this holds if K/F is separable (Primitive Element Corollary) or is generated by a finite set of elements all but one of which is separable (Primitive Element II).

• If $F \subseteq K \subseteq L$ with L/F finitely generated, and $\mathrm{ng}(L/F) \leq 1$, then also $\mathrm{ng}(K/F) \leq 1$. (Indeed, first suppose that L/F is algebraic, hence of finite degree. Since $\mathrm{ng}(L/F) \leq 1$, by Primitive Element I the subfield lattice $\mathcal{L}(L/F)$ is finite, which implies that the lattice $\mathcal{L}(K/F)$ is finite, and then $\mathrm{ng}(K/F) \geq 1$ by Primitive Element I again. Now suppose that L/F is transcendental, so $\mathrm{ng}(L/F) = 1$ and thus $L \cong F(t)$. Then by Lüroth's Theorem either $K = F$ so $\mathrm{ng}(K/F) = 0$ or $K \cong F(t)$ so $\mathrm{ng}(K/F) = 1$.)

• Suppose K/F is finitely generated and separably generated, of transcendence degree r. Then $r \leq \mathrm{ng}(K/F) \leq r+1$. (Indeed the lower bound was established above.

Let $u_1, \ldots, u_r$ be a separating transcendence basis for K/F. Then $K/F(u_1, \ldots, u_r)$ is finite degree separable, so by the Primitive Element Corollary there is $a \in K$ such that $K = F(u_1, \ldots, u_r, a)$.)

• For any prime p, if F is an algebraically closed field of characteristic p, Zariski showed [**Za58**] there is a finitely generated field extension K/F and an F-algebra homomorphism that is inseparable degree p extension $K \hookrightarrow F(t_1, t_2)$. Taking $L := F(t_1, t_2)$ we find that $\mathrm{ng}(K/F) \geq 3 > 2 = \mathrm{ng}(K(t_1, t_2)/F)$. More generally, for a field F, let us call a finitely generated field extension K/F that is not purely transcendental but admits a finite degree F-algebra homomorphism $K \hookrightarrow F(t_1, \ldots, t_{\mathrm{trdeg}(K/F)})$ a **Lüroth counterexample over F**; if $\mathrm{trdeg}(K/F) = r$, we may also call it an **r-Lüroth counterexample over F**. Any Lüroth counterexample is a failure of monotonicity of $\mathrm{ng}(\cdot)$, albeit not by much: if $F \subseteq K \subseteq F(t_1, \ldots, t_r)$, then $F(t_1, \ldots, t_r)/F$ is separably generated (which, recall, is equivalent to separable for finitely generated field extensions), so by Corollary 11.15 K/F is separably generated, so $K \cong_F F(t_1, \ldots, t_r, a)$ with a separable over $F(t_1, \ldots, t_r)$ and thus $\mathrm{ng}(K/F) \leq r + 1$. If F is algebraically closed of characteristic 0, then Castelnuovo showed there are no 2-Lüroth counterexamples, but 2-Lüroth counterexamples arise over many non-algebraically closed fields, e.g. over $\mathbb{Q}$. Every field F admits 3-Lüroth counterexamples, and one certainly expects that every field admits r-Lüroth counterexamples for all $r \geq 4$, but I'm not sure whether this is known to be true.

There are two main results in [**Fa61**]. The first is that Lüroth counterexamples are the only counterexamples to monotonicity of $\mathrm{ng}(\cdot)$ on the class of finitely generated field extensions, so for any $F \subseteq K \subseteq L$ with L/F finitely generated we have first of all that $\mathrm{ng}(K) \leq \mathrm{ng}(L) + 1$ and second of all by Lüroth's Theorem that we have $\mathrm{ng}(K) \leq \mathrm{ng}(L)$ when $\mathrm{trdeg}(L/F)$ is 0 or 1. Faith shows this by showing another monotonicity result: for any $F \subseteq K \subseteq L$ with L/F finitely generated, we have $\dim_F \mathrm{Der}_F(K) \leq \dim_F \mathrm{Der}_F(L)$. This result is also of interest, and it showcases the usefulness of derivations to establish even very basic-sounding results in field theory.

LEMMA 12.31. *Let $K = F(\alpha, \beta)$ be a finite degree field extension such that $F(\alpha, \beta)/F(\beta)$ is separable. Then there is $\gamma \in K$ that is separable over F such that $K = F(\beta, \gamma)$.*

PROOF. Let F_s be the separable closure of F in $F(\alpha)$, so by the Primitive Element Corollary there is $\gamma \in F_s$ such that $F_s = F(\gamma)$. Because $F(\alpha, \beta)/F(\beta)$ is separable, so is its lift $F(\alpha, \beta, \gamma)/F(\beta, \gamma)$. Since $F(\alpha, \gamma) = F(\alpha)$ is a purely inseparable extension of $F(\gamma)$, so is its lift $F(\alpha, \beta, \gamma)/F(\beta\gamma)$. Thus $F(\alpha, \beta, \gamma)/F(\beta, \gamma)$ is both inseparable and purely inseparable, so $F(\alpha, \beta) = F(\alpha, \beta, \gamma) = F(\beta, \gamma)$. □

THEOREM 12.32. *Let K/F be a finitely generated field extension. Then:*

a) *We have $\mathbf{d}(K/F) \leq \mathrm{ng}(K/F) \leq \mathbf{d}(K/F) + 1$.*

b) *If K/F is* not *separably generated, then $\mathrm{ng}(K/F) = \mathbf{d}(K/F)$.*

PROOF. Put $d := \mathbf{d}(K/F)$, $n := \mathrm{ng}(K/F)$ and $r := \mathrm{trdeg}(K/F)$.

a) Let S be a minimal set of generators for K/F. Then, as we have already seen, since an F-derivation on K is determines by its values on S, we get a K-linear injection $\mathrm{Der}_F(K) \hookrightarrow K^S$, which gives $d \leq n$. By Theorem 12.16 there

are $u_1, \ldots, u_d \in K$ such that $K/F(u_1, \ldots, u_d)$ is separable algebraic (and thus of finite degree). Put $U \coloneqq F(u_1, \ldots, u_d)$; by the Primitive Element Corollary, there is $a \in K$ such that $K = U(a)$ and thus $K = F(u_1, \ldots, u_d, a)$, giving $n \leq d+1$.
b) Suppose that K/F is not separably generated; by Theorem 12.16c), this is equivalent to $d > r$. Let $a \in K$ be as in part a). Then, after reordering the u_i's, we may assume that u_d is algebraic over $F(u_1, \ldots, u_{d-1})$. Applying Lemma 12.31 with F the field $T \coloneqq F(u_1, \ldots, u_{d-1})$, α the element a and β the element u_d, we $c \in K$ such that $K = T(u_d, c)$ and c is separable over T. By Primitive Element II, we have that K/T is monogenic, and thus $n \leq d$. □

THEOREM 12.33 (Faith's Monotonicity I). *Let $F \subseteq K \subseteq L$ be field extensions, with L/F finitely generated. Then $\mathbf{d}(K/F) \leq \mathbf{d}(L/F)$.*

PROOF. Step 0: Let S be a (finite, since K/F is finitely generated) differential basis for K/F, with dual differential basis $\{D_s\}_{s \in S}$. Recall that the dual differential basis is characterized by:

$$\forall s, s' \in S,\ D_s(s') = \begin{cases} 1 & \text{if } s = s' \\ 0 & \text{otherwise} \end{cases}.$$

Suppose that for all $s \in S$, D_s extends to an element $D_s \in \mathrm{Der}_F(L)$. Then these extended derivations are L-linearly independent: indeed, for $s \in S$, let $a_s \in L$ and suppose that $\sum_{s \in S} a_s D_s = 0$. For all $s \in S$, evaluating at s gives $a_s = 0$, proving the claim. Thus under this hypothesis, we have that $\mathbf{d}(K/F) \leq \mathbf{d}(L/F)$, as desired.
Step 1: Suppose that $\mathrm{trdeg}(K/F) = \mathrm{trdeg}(L/F)$ – so L/K has finite degree – and that L/K is separable. Then by Corollary 12.8, every derivation on K extends uniquely to a derivation on L, so by Step 1 we have $\mathbf{d}(K/F) \leq \mathbf{d}(L/F)$.
Step 2: Suppose that $\mathrm{trdeg}(K/F) = \mathrm{trdeg}(L/F)$ and that L/K is purely inseparable of degree p. Then we have

$$FK^p \subseteq FL^p \subseteq K \subseteq L.$$

By Theorem 12.16, we have

$$\mathbf{d}(K/F) = [K : FK^p] \text{ and } \mathbf{d}(L/F) = [L : FL^p].$$

Because the Frobenius map gives field isomorphisms $K \xrightarrow{\sim} K^p$ and $L \xrightarrow{\sim} L^p$, we have $[L^p : K^p] = [L : K] = p$ and thus $[FL^p : FK^p] \mid p$. It follows that

$$\begin{aligned} \mathbf{d}(K/F) = [K : FK^p] &= [K : FL^p][FL^p : FK^p] \mid p[K : FL^p] \\ &= [L : K][K : FL^p] = [L : FL^p] = \mathbf{d}(L/F). \end{aligned}$$

Step 3: Every finite degree field extension decomposes as a finite tower where the first step is separable and the successive steps are purely inseparable of degree p, so Steps 1 and 2 imply that if $\mathrm{trdeg}(K/F) = \mathrm{trdeg}(L/F)$, then $\mathbf{d}(K/F) \leq \mathbf{d}(L/F)$.
Step 4: Suppose that $\mathrm{trdeg}(K/F) < \mathrm{trdeg}(L/F)$. Then there is a field M with $K \subseteq M \subseteq L$, with M/K purely transcendental and L/M of finite degree. Since M/K is purely transcendental, every derivation on K can be extended to M, so by Step 0 we have $\mathbf{d}(K/F) \leq \mathbf{d}(M/F)$, and by Step 3 we have $\mathbf{d}(M/F) \leq \mathbf{d}(L/F)$. It follows that $\mathbf{d}(K/F) \leq \mathbf{d}(L/F)$, completing the proof. □

COROLLARY 12.34. *Let $F \subseteq K \subseteq L$ be field extensions, with L/F finitely generated. Suppose that at least one of L/F and K/F is* not *separably generated. Then* $\mathrm{ng}(K/F) \leq \mathrm{ng}(L/F)$.

PROOF. Suppose that at least one of L/F and K/F is not separably generated. If L/F is separably generated, then by Corollary 11.15 also K/F is separably generated, so it must be that L/F is not separably generated. If also K/F is not separably generated, then by Theorems 12.32 and 12.33 we have

$$\mathrm{ng}(K/F) = \mathbf{d}(K/F) \leq \mathbf{d}(L/F) = \mathrm{ng}(L/F).$$

If K/F is separably generated, then we have $\mathrm{ng}(K/F) \leq \mathrm{trdeg}(K/F) + 1 \leq \mathrm{trdeg}(L/F) + 1 \leq \mathrm{ng}(L/F)$, where the last inequality is because L/F, not being separably generated, is certainly not purely transcendental. □

THEOREM 12.35 (Faith's Monotonicity II). *Let $F \subseteq K \subseteq L$ be field extensions, with L/K finitely generated. The following are equivalent:*

(i) *We have* $\mathrm{ng}(K/F) = \mathrm{ng}(L/F) + 1$.
(ii) *We have* $\mathrm{ng}(K/F) > \mathrm{ng}(L/F)$.
(iii) *L/K is a Lüroth counterexample: that is,* $\mathrm{trdeg}(K/F) = \mathrm{trdeg}(L/F)$, *$L/F$ is purely transcendental and K/F is not purely transcendental.*

PROOF. I hope we can agree that (i) $\implies$ (ii).
(iii) $\implies$ (i): (We explained this above, but we are happy to repeat it.) Suppose $\mathrm{trdeg}(K/F) = \mathrm{trdeg}(L/F) = r$, that L/F is purely transcendental and that K/F is not. Then $\mathrm{ng}(K/F) \geq r + 1$; and on the other hand since L/F is separably generated, Corollary 11.15 implies that K/F is separably generated, so $\mathrm{ng}(K/F) \leq r+1$. Thus $\mathrm{ng}(K/F) = r + 1 = \mathrm{ng}(L/F) + 1$.
(ii) $\implies$ (iii): We go by contraposition: suppose that L/K is not a Lüroth counterexample. We will show $\mathrm{ng}(K/F) \leq \mathrm{ng}(L/F)$. By Corollary 12.34 we may assume that K/F and L/F are both separably generated.
Case 1: Suppose that L/F is not purely transcendental. Since K/F is separably generated, we have

$$\mathrm{ng}(K/F) \leq \mathrm{trdeg}(K/F) + 1 \leq \mathrm{trdeg}(L/F) + 1 = \mathrm{ng}(L/F).$$

Case 2: If L/F is purely transcendental and $\mathrm{trdeg}(K/F) < \mathrm{trdeg}(L/F)$, then:

$$\mathrm{ng}(K/F) \leq \mathrm{trdeg}(K/F) + 1 \leq \mathrm{trdeg}(L/F) = \mathrm{ng}(L/F).$$

Case 3: Suppose that L/F is purely transcendental and $\mathrm{trdeg}(K/F) = \mathrm{trdeg}(L/F)$. Then – since we are assuming that L/K is not a Lüroth counterexample – we have that K/F is purely transcendental, so $K \cong_F L$ and $\mathrm{ng}(K) = \mathrm{ng}(L)$. □

Part IV

Formally Real Fields and Ordered Fields

CHAPTER 13

Basics on Ordered Algebraic Structures

1. Ordered Commutative Groups

An **ordered commutative group** $(G, \leq)$ is a commutative group $(G, +)$ equipped with a total ordering $<$ that is compatible with the group law in the sense that

(OCG) For all $x, y, z \in G,\ x \leq y \implies x + z \leq y + z$.

A homomorphism of ordered commutative groups $f : (G, \leq) \to (H, \leq)$ is a group homomorphism that is **isotone**: for all $x_1 \leq x_2$, $f(x_1) \leq f(x_2)$.

LEMMA 13.1. *For x, y, z in an ordered commutative group G, if $x < y$ then $x + z < y + z$.*

PROOF. Since $x < y$, certainly $x \leq y$, so by (OCG) we have $x + z \leq y + z$. If $x + z = y + z$, then adding $-z$ to both sides gives $x = y$, a contradiction. □

LEMMA 13.2. *Let x_1, x_2, y_1, y_2 be elements of an ordered commutative group G with $x_1 \leq x_2$ and $y_1 \leq y_2$. Then $x_1 + y_1 \leq x_2 + y_2$.*

PROOF. Applying (OCG) with x_1, x_2, y_1 gives $x_1 + y_1 \leq x_2 + y_1$. Applying (OCG) with y_1, y_2, x_2 gives $x_2 + y_1 = y_1 + x_2 \leq y_2 + x_2$. By transitivity we have $x_1 + y_1 \leq x_2 + y_2$. □

EXERCISE 13.1. *Let $(G, +)$ be an ordered commutative group. Let $x_1, \ldots, x_n \in G$. Show: if $x_i \geq 0$ for all i and $x_1 + \ldots + x_n = 0$, then $x_i = 0$ for all i.*

To an ordering on a commutative group we associate its **positive cone**:

$$G^+ = \{x \in G \mid x > 0\}.$$

Elements of G^+ are called **positive**. We also define

$$G^- = \{x \in G \mid x < 0\}.$$

Elements of G^- are called **negative**.

LEMMA 13.3. *Let x be a nonzero element of the ordered commutative group G. Then exactly one of x, $-x$ is positive. Thus $G = \{0\} \coprod G^+ \coprod G^-$.*

PROOF. If $x > 0$ and $-x > 0$, then adding them gives $0 > 0$, a contradiction. If x is not positive then $x < 0$. By Lemma 13.1 we may add $-x$ to both sides, getting $0 = x + (-x) < 0 + x = -x$. □

LEMMA 13.4. *Let x_1, x_2 be elements of an ordered commutative group.*

a) *If $x_1, x_2 \in G^+$, then $x_1 + x_2 \in G^+$.*
b) *If $x_1, x_2 \in G^-$, then $x_1 + x_2 \in G^-$.*

PROOF. a) Since $x_1 > 0$ and $x_2 > 0$, then by Lemma 13.1 we have

$$0 < x_1 < x_1 + x_2.$$

b) If $x_1 < 0$ and $x_2 < 0$, then by Lemma 13.3 we have $-x_1, -x_2 > 0$. Now part a) gives $-x_1 - x_2 = -(x_1 + x_2) > 0$, so by Lemma 13.1 again we have $x_1 + x_2 < 0$. □

In an ordered commutative group we define $|x|$ to be x if $x \geq 0$ and $-x$ otherwise.

EXERCISE 13.2. *Let x, y be elements of an ordered commutative group G.*

a) *Suppose $x \leq y$ and $n \in \mathbb{N}$. Show: $nx \leq ny$.*
b) *Suppose $x \leq y$ and $n \in \mathbb{Z}^{<0}$. Show: $nx \geq ny$.*

EXAMPLE 13.5. *Let H be a subgroup of an ordred commutative group $(G, \leq)$. Restricting $<$ to H makes H an ordered commutative group.*

EXAMPLE 13.6 (Lexicographic Ordering). *Let $\{G_i\}_{i \in I}$ be a nonempty indexed family of ordered commutative groups. Suppose that we are given a well-ordering on the index set I. We may then endow the direct product $G = \prod_{i \in I} G_i$ with the structure of an ordered commutative group, as follows: for $(g_i), (h_i) \in G$, we decree $(g_i) < (h_i)$ if for the least index i such that $g_i \neq h_i$, $g_i < h_i$.*

For a commutative group G, we put $G_{\mathbb{Q}} \coloneqq G \otimes_{\mathbb{Z}} \mathbb{Q}$. There is a group homomorphism

$$\iota : G \to G_{\mathbb{Q}},\ x \mapsto x \otimes 1$$

for which the kernel is $G[\text{tors}]$ [**Cl-CA**, Exc. 7.10b)]. Thus ι is an injection if and only if G is torsionfree.

THEOREM 13.7 (Levi [**Lev43**]). *For an commutative group G, the following are equivalent:*

(i) *G admits at least one ordering.*
(ii) *G is torsionfree.*

PROOF. (i) $\implies$ (ii) Let $<$ be an ordering on G, and let $x \in G^\bullet$. By Lemma 13.4 we have $nx \neq 0$ for all $n \in \mathbb{Z}^+$.
(ii) $\implies$ (i): Let G be a torsionfree commutative group. As above, we have an injective group homomorphism $\iota : G \hookrightarrow G_{\mathbb{Q}}$. Since $\mathbb{Q}$ is a field, the $\mathbb{Q}$-module $G_{\mathbb{Q}}$ is free, i.e., it is isomorphic to $\bigoplus_{i \in I} \mathbb{Q}$. Choose a total ordering on I. Give each copy of $\mathbb{Q}$ its standard ordering as a subfield of $\mathbb{R}$ and put the lexicographic ordering on $\bigoplus_{i \in \mathbb{Q}} \mathbb{Q} \cong G_{\mathbb{Q}}$. Via the injection ι this induces an ordering on G. □

EXERCISE 13.3. *Let $(G, \leq)$ be an ordered commutative group. Show that there is a unique extension of $\leq$ to $G_{\mathbb{Q}}$ that makes $G_{\mathbb{Q}}$ into an ordered commutative group.*

An **anti-isomorphism** of commutative groups is an order-reversing group isomophism. For every ordered commutative group $(G, \leq)$, the inversion map $x \in G \mapsto -x$ is an anti-isomorphism of G.

EXERCISE 13.4.

a) *Show that the commutative group $\mathbb{Z}$ admits exactly two orderings $\leq_1$ and $\leq_2$. Also show that inversion gives an isomorphism $(\mathbb{Z}, \leq_1) \xrightarrow{\sim} (\mathbb{Z}, \leq_2)$.*
b) *Give an example of an commutative group G admitting orderings $\leq_1$ and $\leq_2$ such that $(G, \leq_1)$ is not isomorphic or anti-isomorphic to $(G, \leq_2)$.*

1.1. Archimedean equivalence classes. For $x, y \in G$, we write $x \prec y$ if there exists $n \in \mathbb{Z}^+$ such that $|x| \leq n|y|$. We claim that $\prec$ is a **quasi-ordering** on G, i.e., a reflexive, transitive but not necessarily anti-symmetric binary relation. The reflexivity is immediate. For the transitvity: if $x \prec y$ and $y \prec z$ then there exist $n_1, n_2 \in \mathbb{Z}^+$ such that $|x| \leq n_1|y|$ and $|y| \leq n_2|z|$, and thus $|x| \leq n_1 n_2 |z|$.

As is the case for any quasi-ordering, the relation $x \prec y$ and $y \prec x$ is an equivalence relation, and the quasi-ordering descends to a partial ordering on equivalence classes. Write $x \approx y$ for the resulting equivalence relation on the ordered group G: explicitly, there exist $n_1, n_2 \in \mathbb{Z}^+$ such that $|x| \leq n_1|y|$ and $|y| \leq n_2|x|$.

In any ordered commutative group G, $\{0\}$ is its own $\approx$-equivalence class, hence any nontrivial ordered commutative group has at least two $\approx$-equivalence classes. We refer to nonzero $\approx$-equivalence classes as **Archimedean equivalence classes**. We denote the set of Archimedean equivalence classes of G as $\widetilde{\Omega}(G)$ and the set of Archimedean equivalence classes of $G \setminus \{0\}$ as $\Omega(G)$.

EXERCISE 13.5. *Let $(G, \leq)$ be an ordered commutative group.*

a) *Show the quasi-ordering $\prec$ on G descends to a well-defined total ordering on $\widetilde{\Omega}(G)$ in which $[0]$ is the least element.*

b) *Deduce that the quasi-ordering $\prec$ on $G^\bullet$ descends to a well-defined total ordering on $\Omega(G)$. Show by example that $\Omega(G)$ need not have either a least element or a greatest element.*

A subset S of a totally ordered set X is **convex** if for all $x, y, z \in X$ with $x < z < y$, if $x, y \in S$, then also $z \in S$. The intersection of any family of convex subsets is a convex subset, so for any subset S, there is a unique minimal convex subset $\mathrm{Conv}(S)$ containing S, called its **convex hull**.

EXERCISE 13.6. *Let $(G, \leq)$ be an ordered commutative group.*

a) *Show: if H is a subgroup of G, then its convex hull $\mathrm{Conv}(H)$ is a convex subgroup of G.*

b) *Show: if S is a convex subset of G, then $\langle S \rangle$ is a convex subgroup of G.*

c) *Show: if S is a subset of G, then $\mathrm{Conv}(\langle S \rangle) = \langle \mathrm{Conv}(S) \rangle$. We call this common convex subgroup the convex subgroup generated by S.*

d) *Let $C(G)$ be the set of convex subgroups of G. Show: $C(G)$ is linearly ordered under inclusion.*

e) *Let $x, y \in G$. Show: $x \approx y$ if and only if x and y generate the same convex subgroup of G. Deduce: there is an isotone embedding $\iota : \Omega(G) \hookrightarrow C(G)$. A convex subgroup generated by a single element in this way is called **principal**.*

f) *Exhibit a totally ordered group G with a nonprincipal convex subgroup.*

An ordered commutative group with $\#\Omega(G) \leq 1$ is called **Archimedean**. Equivalently, for all $x, y \in G^\bullet$, there are $n_1, n_2 \in \mathbb{Z}^+$ such that $|x| \leq n_1|y|$ and $|y| \leq |x|$.

EXAMPLE 13.8. *The group $(\mathbb{R}, +)$ is Archimedean: for any $x \in \mathbb{R}^{>0}$ there are positive integers n_1 and n_2 such that $\frac{1}{n_1} \leq x \leq n_2$. Indeed the second inequality follows from the least upper bound axiom: if this were not the case then the set $\mathbb{Z}^+$ of positive integers would be bounded above in $\mathbb{R}$, and this set cannot have a least upper bound. The first inequality follows from the second upon taking reciprocals.*

EXAMPLE 13.9. *A subgroup of an Archimedean ordered commutative group is Archimedean. In particular, any subgroup of $(\mathbb{R}, +)$ is Archimedean in the induced ordering.*

Remarkably, the converse is also true.

THEOREM 13.10. *(Hölder [**Hö01**]) Let $(G, \leq)$ be an ordered commutative group. If G is Archimedean, there is an embedding of ordered commutative groups $G \hookrightarrow \mathbb{R}$.*

PROOF. We may assume G is nontrivial. Let $x \in G^+$. We will construct an order embedding of G into $\mathbb{R}$ mapping x to 1.

Namely, let $y \in G$. Then the set of integers n such that $nx \leq y$ has a maximal element n_0. Put $y_1 = y - n_0 x$. Now let n_1 be the largest integer n such that $nx \leq 10y_1$: observe that $0 \leq n_1 < 10$. Continuing in this way we get a set of integers $n_1, n_2, \ldots \in \{0, \ldots, 9\}$. We define $\varphi(y)$ to be the real number $n_0 + \sum_{k=1}^{\infty} \frac{n_k}{10^k}$. It is not hard to show that φ is isotone – $y \leq y' \implies \varphi(y) \leq \varphi(y')$ – and also that φ is injective: we leave these tasks to the reader.

But let us check that φ is a homomorphism of groups. For $y \in G$, and $r \in \mathbb{Z}^+$, let $\frac{n}{10^r}$ be the rational number obtained by truncating $\varphi(y)$ at r decimal places. The numerator n is characterized by $nx \leq 10^r y < (n+1)x$. For $y' \in G$, if $n'x \leq 10^r y' \leq (n'+1)x$, then

$$(n + n')x \leq 10^r(y + y') < (n + n' + 2)x,$$

so

$$\varphi(y + y') - (n + n')10^{-r} < \frac{2}{10^r}$$

and thus

$$|\varphi(y + y') - \varphi(y) - \varphi(y')| < \frac{4}{10^r}.$$

Since r is arbitrary, we conclude $\varphi(y + y') = \varphi(y) + \varphi(y')$. □

PROPOSITION 13.11. *Let G be a nontrivial Archimidean ordered commutative group. Then exactly one of the following holds:*

(i) *G is order-isomorphic to $\mathbb{Z}$.*
(ii) *The ordering on G is dense.*

PROOF. Step 1: Suppose G^+ has a least element x. Let $y \in G^+$. Since the ordering is Archimedean there is a largest $n \in \mathbb{Z}^+$ such that $nx \leq y$. Then $y - nx \geq 0$; if $y > 0$ then $y - nx \geq x$ so $y \geq (n+1)x$, contradicting the maximality of n. Thus $y = nx$, i.e., every positive element of G^+ is a multiple of x. It follows that there is a unique order isomorphism from G to $(\mathbb{Z}, <)$ carrying x to 1.
Step 2: Suppose G is not isomorphic to $(\mathbb{Z}, <)$, so there is no least positive element. In other words, given any positive element x there exists 0 with $0 < y < x$. Now let $a, b \in G$ with $a < b$. If $0 < y < b - a$ then $a < y < b$. So the ordering is dense. □

EXERCISE 13.7.

a) *Let $\iota : \mathbb{R} \hookrightarrow \mathbb{R}$ be an embedding of ordered commutative groups. Show that there is $\alpha \in \mathbb{R}^{>0}$ such that $\iota(x) = \alpha x$ for all $x \in \mathbb{R}$. Deduce that ι is an isomorphism of ordered commutative groups.*
b) *Let $f : \mathbb{R} \hookrightarrow G$ be an embedding of ordered commutative groups. Show: if G is Archimedean, then f is an isomorphism.*

2. The Hahn Embedding Theorem

Hölder's Theorem already shows the relevance of the set $\Omega(G)$ of nonzero Archimedean equivalence classes in the structure theory of ordered commutative groups, so it is natural to ask for a generalization / analogue in the case where $\Omega(G)$ has more than one element. One place to start is by asking: what are the possible isomorphism types of totally ordered sets that can arise as $\Omega(G)$ for some ordered commutative group G? The perhaps surprising answer is: all of them!

To warm up to this, let $G_1, \ldots, G_n$ be nontrivial Archimedean ordered commutative groups, and consider $G := \prod_{i=1}^n G_i$ endowed with the lexicographic ordering. If for each $1 \leq i \leq n$ we fix an element $x_i \in G^\bullet$, then it is not hard to see that

$$(x_1, 0, \ldots, 0) \succ (0, x_2, 0, \ldots, 0) \succ \ldots \succ (0, \ldots, 0, x_n)$$

are a complete set of representatives for the nonzero Archimedean equivalence classes, so $\#\Omega(G) = n$. We note that there is an order-reversal here: if we put $S := \{1, \ldots, n\}$ with its usual ordering, then the nonzero Archimedean equivalence classes in $\prod_{i \in S} G_i$ come out in the opposite order: the smallest is $(0, \ldots, 0, x_n)$. More generally, if $(S, \leq)$ is a well-ordered set and for all $i \in S$ we have a nontrivial Archimedean ordered group G_i, then we can lexicographically order $G = \prod_{i \in S^\vee} G_i$, and then we have a canonical isomorphism of the ordered set $\Omega(G)$ with the order-dual $S^\vee$ of X (in which $x \leq^\vee y$ if and only if $y \leq x$), so this argument shows that any ordered set that is dual-well-ordered – i.e., every nonempty subset has a maximum – arises up to isomorphism as the set of nonzero Archimedean equivalence classes of an ordered commutative group.

However, if we are given any totally ordered set S and any family $\{G_i\}_{i \in S}$ of ordered commutative groups, there is a way to define a lexicographic ordering not on the entire Cartesian product $\prod_{i \in S} G_i$ but on a certain subgroup of it. Namely, for any $f \in \prod_{i \in S} G_i$, we define the **support** $\mathrm{supp}(f)$ to be the set of $i \in S$ such that $f(i) \neq 0$, and we define $\mathcal{F}(S, \{G_i\}_{i \in S})$ to be the set of $f \in \prod_{i \in S} G_i$ such that $\mathrm{supp}(f)$ is a well-ordered subset of S. Then $\mathcal{F}(S, \{G_i\}_{i \in S}$ is a subgroup of $\prod_{i \in S} G_i$ – this comes down to the fact that the union of two well-ordered subsets of a totally ordered set is well-ordered – and the lexicographic ordering is well-defined on this subgroup and makes it into an ordered commutative group.

EXERCISE 13.8. *Let S be a totally ordered set, and for each $i \in S$, let G_i be a nontrivial Archimedean ordered commutative group.*

a) *Show: $\Omega(\mathcal{F}(S, \{G_i\}_{i \in S})$ is order-isomorphic to $S^\vee$.*
b) *Let $\mathcal{F}_0(S, \{G_i\}_{i \in S}$ be the subgroup of $\mathcal{F}(S, \{G_i\}_{i \in S})$ given by the direct sum $\prod_{i \in S} G_i$: equivalently, it is the set of elements of $\mathcal{F}(S, \{G_i\}_{i \in S})$ with finite support. Show: $\mathcal{F}_0(S, \{G_i\}_{i \in S})$ is also order-isomorphic to $S^\vee$.*

Thus for any totally ordered set S, we have $\Omega(\mathcal{F}(S^\vee, \{G_i\}_{i \in S})) = (S^\vee)^\vee = S$.

For a totally ordered set S, we define the **Hahn group of S**

$$\mathcal{F}(S, \mathbb{R}) := \mathcal{F}(S, \{\mathbb{R}\}_{i \in S}).$$

In other words, in the above construction we take each $G_i = \mathbb{R}$. Now we have a remarkable generalization of Hölder's Theorem due to H. Hahn [**Ha07**].

THEOREM 13.12 (Hahn Embedding Theorem). *Let G be an ordered commutative group. Then there is a canonical embedding of ordered commutative groups*

$$\mathfrak{h} : G \hookrightarrow \mathcal{F}(\Omega(G)^\vee, \mathbb{R}).$$

The dual in the statement of Theorem 13.12 makes us wonder whether we should go back and flip the ordering in our definition of the $\prec$ relation, which would mean that an element of an ordered commutative group G gets larger as it gets closer to 0 and the element 0 is the largest of all. This may ring bells for those familiar with valuation theory: if for $x, y \in G^\bullet$ we write $v(x)$ for the Archimedean equivalence class of x and put $v(x) \leq v(y)$ if and only if $y \prec x$, then the map $v : G^\bullet \to \Omega(G)$ satisfies the property

$$\forall x, y \in G^\bullet \text{ such that } x + y \neq 0,\ v(x+y) \geq \min(v(x), v(y)).$$

Those whose bells were just rung will now believe the map v *is* some kind of valuation, which is one of the threads to pull in order to prove Theorem 13.12.

Hahn's paper [**Ha07**] is a *tour de force* of transfinite algebra; it is intricate and seems quite technical, but the objects and ideas introduced there have found their place in the algebraic pantheon. Simplifications and generalizations of Hahn's work emerged in the 1950's in papers of Conrad [**Co53**], Clifford [**Cl54**] and Gravett [**Gr55**], [**Gr56**]; these works show that after developing about five pages of valuation theory on groups as hinted at above, one can prove Theorem 13.12 in about five pages. I am not aware of any essential simplifications since then, though attractive expositions exist: e.g. much of [**DW**, Ch. 1] is devoted to the proof of a stronger version of Theorem 13.12. We will not give a proof here.

3. Introducing Ordered Fields and Formally Real Fields

3.1. Definitions and First Examples. An **ordered ring** is a ring R together with a total ordering $\leq$ on R compatible with the commutative group $(R, +)$ and satisfying the additional property

(OR) $\forall x, y \geq 0$, $xy \geq 0$.

A homomorphism $f : (R, \leq) \to (R', \leq')$ of ordered rings is a ring homomorphism that is also an isotone (a.k.a. increasing, a.k.a. order-preserving) map: for all $x, y \in R$, $x \leq y$ implies $f(x) \leq f(y)$.

A total ordering $\leq$ on a ring R is called **compatible** if $(R, \leq)$ is an ordered ring.

An **ordered field** is an ordered ring whose underlying ring is a field. From this point on, when we speak of an ordering on a ring we will always mean a compatible total ordering.

EXERCISE 13.9. *Let R be a domain with fraction field F. Show: every ordering on R extends uniquely to an ordering on F.*

EXERCISE 13.10. *Let $(F, \leq)$ be an ordered field. Show: for $x, y \in F$, if $x > 0$ and $y > 0$, then $xy > 0$.*

LEMMA 13.13. *Let $(F, \leq)$ be an ordered field, and let $x, y, x_1, \ldots, x_n \in F$.*

a) *If $x > 0$ and $y < 0$, then $xy < 0$.*

b) *If $x, y < 0$, then $xy > 0$.*
c) *If $a_1, \ldots, a_n \in F^{>0}$, then $x_1^2 + \ldots + x_n^2 \geq 0$, with equality if and only if $x_1 = \ldots = x_n = 0$.*

PROOF. a) Suppose $x > 0$ and $y < 0$. Adding $-y$ gives $-y > 0$, and then using Exercise 13.10 we get $-(xy) = x(-y) > 0$, and adding xy gives $xy < 0$.
b) Suppose $x, y < 0$. As above we get $-x, -y > 0$, and then Exercise 13.10 gives $xy = (-x)(-y) > 0$.
c) For $1 \leq i \leq n$, if $x_i > 0$, then by Exercise 13.10 also $x_i^2 > 0$, while if $x_i < 0$ then by part b), $x_i^2 > 0$, and of course if $x_i = 0$ then $x_i^2 = 0$. It follows that $a_i x_i^2 \geq 0$ for all i, so $a_1 x_1^2 + \ldots + a_n x_n^2 \geq 0$. By Exercise 13.1, if $a_1 x_1^2 + \ldots + a_n x_n^2 = 0$, then for all i we have $a_i x_i^2 = 0$, hence $x_i = 0$. □

For a field F, we denote by $X(F)$ the set of all orderings[1] on F.

EXERCISE 13.11. *Let $(K, \leq)$ be an ordered field and let F be a subfield of K. Denote by $\leq_F$ the restriction to F of $\leq$. Show: $(F, \leq_F)$ is an ordered field and the inclusion of F into K is an homomorphism of ordered fields.*

EXAMPLE 13.14. *The usual ordering $\leq$ on $\mathbb{R}$ makes it into an ordered field. Thus for a field F, an embedding $\iota : F \hookrightarrow \mathbb{R}$ induces an ordering on F.*

Let us consider a number field F: that is, a field extension of $\mathbb{Q}$ of finite degree n. Let α be a primitive element of $F/\mathbb{Q}$, with minimal polynomial $f \in \mathbb{Q}[t]$. Then field embeddings $\iota : F \hookrightarrow \mathbb{R}$ are in bijection with real roots of f. It is standard in number theory to denote the number of real roots of f by r and the number of complex conjugate pairs of nonreal roots by s, so $n = r + 2s$; we call (r, s) the **signature** of the number field F. We say that F is **real** if $r \geq 1$ and **totally real** if $r = n$. It follows that if n is odd then $r \geq 1$, so every odd degree number field is real and thus admits an ordering. One can show that for every $n \in \mathbb{Z}^{\geq 2}$ and every $r, s \in \mathbb{N}$ with $r + 2s = n$ there are infinitely many nonisomorphism number fields with signature (r, s).

What if $r = 0$, i.e., the number field F has no real embedding? The simplest case of this is $(r, s) = (0, 1)$, i.e., of imaginary quadratic fields $F = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Q}^{<0}$. In this case, since

$$(\sqrt{D})^2 = D < 0,$$

hence by Lemma 13.13d), F cannot be ordered. Already if $(r, s) = (0, 2)$ – i.e., if F is a quartic number field with no real embeddings – it does not seem obvious how to proceed. If we are given a *particular* such field, we could try to find $x_1, \ldots, x_n \in F$ such that $x_1^2 + \ldots + x_n^2$ is a negative rational number, but in general? We need more theory for this.

EXERCISE 13.12. *Let $D \in \mathbb{Q}^\times \setminus \mathbb{Q}^{\times 2}$ be such that $D > 0$, so $F \coloneqq \mathbb{Q}(\sqrt{D})$ is a real quadratic field. We define orderings $\leq_1$ and $\leq_2$ on F using the two field embeddings $F \hookrightarrow \mathbb{R}$.*

a) *Show: $\leq_1 \neq \leq_2$: i.e., we have two distinct orderings on F.*
b) *Show: $X(F) = \{\leq_1, \leq_2\}$.*

EXERCISE 13.13. *Let F be a number field of signature (r, s) with $r \geq 2$. Let $f \in \mathbb{Q}[t]$ be the minimal polynomial of a primitive elements α for $F/\mathbb{Q}$, and let*

[1]Again, this means total orderings that make F into an ordered field.

$\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_r$ be the real roots of f. For $1 \leq i \leq r$, let $\leq_i$ be the ordering on F obtained from embedding $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{R}$ by $\alpha \mapsto \alpha_i$. Let $1 \leq i < j \leq r$, and let $\{x_n\}_{n=1}^{\infty}$ be a strictly increasing sequence in $\mathbb{Q}$ converging in $\mathbb{R}$ to α_j.

a) *Show: for all $n \in \mathbb{Z}^+$, $\alpha - x_n >_j 0$.*
b) *Show: for all sufficiently large $n \in \mathbb{Z}^+$, $\alpha - x_n <_i 0$.*
c) *Deduce: the r orderings $\leq_1, \ldots, \leq_r$ on F are distinct.*

Later, we will show that for any number field F, the set $X(F)$ of orderings on F is in bijection with the set of field embeddings $\iota : F \hookrightarrow \mathbb{R}$.

EXERCISE 13.14. *Let F be a field.*

a) *Show: there is a natural left action of $\mathrm{Aut}(F)$ on $X(F)$.*
b) *Give an example where the orbit space $\mathrm{Aut}(K)\backslash X(K)$ consists of more than one element.*

EXAMPLE 13.15. *If $f \in \mathbb{R}[t] \setminus \{0\}$, then f has finitely many roots and is continuous, so it is either the case that $f(x) > 0$ for all sufficiently large $x \in \mathbb{R}$ or $f(x) < 0$ for all sufficiently large $x \in \mathbb{R}$. For $f, g \in \mathbb{R}$, put $f \leq g$ if $f = g$ or $g - f$ is positive for sufficiently large x. This is an ordering on the polynomial ring $\mathbb{R}[t]$, which by Exercise 13.9 extends uniquely to an ordering on the rational function field $\mathbb{R}(t)$: again, $f \leq g$ if $f = g$ or $g - f$ is positive for sufficiently large x. In this ordering $t > c$ for all real numbers c, which shows that the underlying order on the additive group is not Archimidean. Indeed, in the set of $\Omega(\mathbb{R}(t), +))$ of Archimedean equivalence classes we have $1 < t < t^2 < \ldots < t^n < \ldots$.*

EXERCISE 13.15. *Let $(F, \leq)$ be an ordered field, and let $K := F(t)$. Every nonzero element of K can be written uniquely as $\frac{p(t)}{q(t)}$ where $p(t) = a_n t^n + \ldots + a_1 t + a_0$ is a nonzero polynomial, $q(t)$ is a monic polynomial and p and q have no common factor. For $x, y \in K$, define $x \leq y$ if $x = y$ or if writing $y - x = \frac{p(t)}{q(t)}$ as above, then the leading coefficient a_n of $p(t)$ is positive for the given ordering on F.*

a) *Show: this gives an ordering on $F(t)$. When $F = \mathbb{R}$, show that this is the same ordering as in Example 13.15 above.*
b) *Show: this is the unique ordering on $F(t)$ extending the given ordering on F and for which $t > c$ for all $c \in F$.*
c) *Show: there is a unique ordering on $F(t)$ extending the given ordering on F and for which $t < c$ for all $c \in F$.*
d) *Show: there is a unique ordering on $F(t)$ extending the given ordering on F and for which $0 < t < c$ for all $c \in F^{>0}$.*
e) *Show: there is a unique ordering on $F(t)$ extending the given ordering on F and for which $c < t < 0$ for all $c \in F^{<0}$.*

EXERCISE 13.16. *Let $(F, \leq)$ be an ordered field. Show: there is a unique ordering on the formal Laurent series field $F((t))$ (i.e., the fraction field of the formal power series ring $F[[t]]$) extending the given ordering on F and for which $0 < t < c$ for all $c \in F^{>0}$.*

PROPOSITION 13.16. *Every ordered field has characteristic 0.*

PROOF. The additive group of an ordered field is an ordered commutative group, hence is torisonfree by Theorem 13.7. But in the additive group of a field of characteristic $p > 0$, every nonzero element has order p. □

3.2. Orderings as cones. For a subset $S \subseteq F$, put $S^\bullet = S \setminus \{0\}$.

We consider the following conditions on a subset P of a field F:

(PO1) $P + P \subseteq P$, and $PP \subseteq P$.
(PO2) $\Sigma_\square(F) := \{x_1^2 + \ldots + x_n^2 \mid x_i \in K\} \subseteq P$.
(PO3) $-1 \notin P$.
(PO3′) $P \cap (-P) = \{0\}$.
(PO3″) $P^\bullet + P^\bullet \subseteq P^\bullet$.
(PO3‴) $P \neq F$.
(PO4) $P \cup (-P) = F$.

EXERCISE 13.17. *Let $P \subset F$ satisfy (PO1) and (PO2).*

a) *Show: (PO3), (PO3′), and (PO3″) are equivalent conditions on P.*
b) *Suppose* $\operatorname{char} F \neq 2$. *Show: (PO3‴) and (PO3) are equivalent conditions on P. (Hint: $x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2$.)*
c) *Deduce: if* $\operatorname{char} F \neq 2$, *then* $-1 \in \Sigma_\square(F) \iff \Sigma_\square(F) = F$.
d) *Suppose* $\operatorname{char} F = 2$. *Show: P satisfies (PO1) and (PO2) if and only if P is a subfield of F containing F^2.*

EXERCISE 13.18. *Let $P \subseteq F$ satisfy (PO1) and (PO4). Show: P satisfies (PO2).*

LEMMA 13.17. *Let F be a field.*

a) *If $\leq$ is a field ordering on F, put $P = F^{\geq 0}$. Then F satisfies (PO1), (PO2), (PO3) and (PO4) above, and also $1 \in P$.*
b) *Let $P \subseteq F$ satisfy (PO1) through (PO4). Define a relation $\leq$ on F by $x \leq y \iff y - x \in P$. Then $\leq$ is a field ordering on F with $F^{\geq 0} = P$.*

PROOF. a) Property (PO1) is part of the definition of an ordered field. It follows easily from Lemma 13.13 that for all $x \in F$, $x^2 \geq 0$, and (PO2) follows from this. Again by Lemma 13.13 we get that $1 = 1^2 > 0$; adding -1 gives $-1 < 0$; so 1 is in P and -1 is not (PO3). Property (PO4) follows from Lemma 13.3.
b) Using (PO3) and (PO4), we get that $\leq$ is a total ordering. Given $x, y, z \in F$ with $x \leq y$, then $(y + z) - (x + z) = y - x \in P$, so $x + z \leq y + z$: $(F, \leq)$ is an ordered commutative group. Property (PO1) implies property (OR), so $(F, \leq)$ is an ordered field, and clearly $x \geq 0$ if and only if $x \in P$. □

Thus Lemma 13.17 shows that an ordering $\leq$ on a field F is determined by the induced subset $P := F^{\geq 0}$ of non-negative elements and shows that for a subset P of F, conditions (P01), (PO2), (P03), (P04) are sufficient to be the set of non-negative elements of an ordering on F. It is standard to call P the **positive cone** of the ordering; because 0 is not positive, I prefer to use this name for $P^\bullet$ rather than P. More to the point though, P, being a subset of F, is a slightly simpler structure than $\leq$, being a subset of $F \times F$. Henceforth we will allow ourselves to speak of either $\leq$ or P as the **ordering** on F, and we will often speak of the "ordered field (F, P)."

EXERCISE 13.19. *Let P_1, P_2 be two orderings on a field K. Show:*

$$P_1 \subseteq P_2 \implies P_1 = P_2.$$

CHAPTER 14

Formally Real Fields

1. Preorderings and Formally Real Fields

For a field F, we are interested in the set $X(F)$ of orderings on F. The most basic question to ask is whether $X(F)$ is nonempty: that is, does F admit any ordering? We will give an important necessary and sufficient condition for this.

Recall that for a field F,

$$\Sigma_{\square}(F) \coloneqq \{x_1^2 + \ldots + x_n^2 \mid n \in \mathbb{Z}^+,\ x_i \in F\}$$

denotes the set of all sums of squares in F. Every nonzero element of $\Sigma_{\square}(F)$ must be positive in any ordering P of F, and since 1 is certainly a sum of squares, -1 cannot be positive in any ordering of F. This motivates the following definition: a field F is **formally real** if $-1 \notin \Sigma_{\square}(F)$.

LEMMA 14.1. *A field F is formally real if and only if: for all $n \in \mathbb{Z}^+$ and $x_1, \ldots, x_n \in F$, if $x_1^2 + \ldots + x_n^2 = 0$, then $x_i = 0$ for all $1 \leq i \leq n$.*

PROOF. If F is not formally real, then there are $x_1, \ldots, x_n \in F$ such that $-1 = x_1^2 + \ldots + x_n^2$, so

$$1^2 + x_1^2 + \ldots + x_n^2 = 0$$

gives a vanishing sum of squares in which not all terms vanish. Conversely, given $x_1, \ldots, x_n \in F$ with $x_i \neq 0$ for some i such that $x_1^2 + \ldots + x_n^2 = 0$, then

$$-1 = \sum_{j \neq i} \left(\frac{x_j}{x_i}\right)^2,$$

so F is not formally real. □

EXERCISE 14.1. *Let $\{F_i\}_{i \in I}$ be a directed system of fields, with direct limit F. Show: F is formally real if and only if F_i is formally real for all $i \in I$.*

Comparing Lemma 13.13d) with Lemma 14.1, we deduce: an ordered field is formally real (though this was probably clear anyway...). Remarkably, the converse of this result is true: we will show that every formally real field admits an ordering. To do so, we will give a generalization of (the cone version of) an ordering on a field.

Let F be a field. A subset $P \subseteq F$ satisying (PO1), (PO2) and (PO3) is called a **preordering** of K. A preordering P contains $\Sigma_{\square}(F)$ and does not contain -1, so if F admits a preordering then it is formally real. Conversely, if F is formally real, then $\Sigma_{\square}(F)$ is a preordering on F.

If F has characteristic $p > 0$, then $-1 = 1^2 + \ldots + 1^2$ ($p - 1$ times) is a sum

of squares, so formally real fields have characteristic 0. More precisely, in characteristic different from 2, Exercise 13.17 shows that -1 not being a sum of squares is equivalent to $\Sigma_\square(F) \subsetneq F$, so in a nonformally real field of characteristic different from 2, every element is a sum of squares. However, if F has characteristic 2 then $\Sigma_\square(F) = F^2$, so $\sigma_\square(F) \subsetneq F$ if and only if F is *not* perfect. But in characteristic 2 we have $-1 = 1 \in \Sigma_\square(F)$, so once again F cannot be formally real.

To sum up: in studying formally real fields and preorderings, we must restrict to characteristic 0. Then F is formally real if and only if it has a preordering, in which case $\Sigma_\square(F)$ is the unique minimal preordering. Our strategy is to show that in a formally real field we can extend the preordering $\Sigma_\square(F)$ to an ordering.

EXERCISE 14.2. *Let T be a preordering on F and $x, y \in T$. Show that $x, y \in T,\ x + y = 0 \implies x = y = 0$.*

LEMMA 14.2. *Let F be a field such that*

$$\Sigma_\square(F) \cap (-\Sigma_\square(F)) = \{0\}$$

and

$$\Sigma_\square(F) \cup (-\Sigma_\square(F)) = F^\times.$$

Then $P = \Sigma_\square(F)$ is the unique ordering on F.

EXERCISE 14.3. *Prove Lemma 14.2.*

EXERCISE 14.4. *Use Lemma 14.2 to show that each of the following fields admits a* unique *ordering: $\mathbb{R}$, $\mathbb{Q}$, the field of constructible numbers.*

LEMMA 14.3. *Let F be a field, $T \subseteq F$ a preordering on F, and $a \in F^\times$. The following are equivalent:*

(i) *The set $T[a] := \{x + ya \mid x, y \in T\}$ is a preordering.*
(ii) *The element $-a$ does* not *lie in T.*

PROOF. $\neg$ (ii) $\implies$ $\neg$ (i): If $-a \in T$, then both a and $-a$ lie in $T[a]$, so $T[a]$ does not satisfy (PO3′), which is equivalent to (PO3), so $T[a]$ is not a preordering. (ii) $\implies$ (i): In all cases it is clear that $T[a]$ satisfies (PO1) and (PO2), so it suffices to show that $-a \notin T$ implies that $-1 \notin T[a]$. Indeed, if $-1 \in T[a]$, then $-1 = x + ya$ for $x, y \in T$, then since T is a preordering we have $y \neq 0$, and thus

$$-a = \frac{1+x}{y} = (y^{-1})^2(y)(1+x) \in T,$$

a contradiction. □

For the next result, we use the convention that the intersection of an empty family of subsets of F is F itself.

THEOREM 14.4. *Let T be a preordering on a field F. Then:*

a) *The set T is the intersection of all orderings $P \supseteq T$. In particular, there is an ordering on F extending T.*
b) *(Artin–Schreier) If F is formally real, then it admits an ordering.*

PROOF. a) Step 1: Let $\mathcal{S}$ be the set of all preorderings on F containing T. The union of a chain of preorderings is again a preordering. Applying Zorn's Lemma, we get a maximal element $\mathcal{T} \supseteq T$. By Lemma 14.3 we have that for all $a \in F$, if

$-a \notin \mathcal{T}$, then $a \in \mathcal{T}$, so $\mathcal{T}$ satisfies (PO4) and is therefore an order.
Step 2: Let $b \in F \setminus T$. We must construct an ordering $P \supseteq T$ with $b \notin P$. But by Lemma 14.3, $T[-b]$ is a preordering, which by Step 1 extends to an ordering P, and since $-b \in P$, we have $b \notin P$.
b) If F is formally real, then $\Sigma_\square(F)$ is a preordering on F. In particular, $\Sigma_\square(F)$ is a proper subset of K, whereas by part a) if there were no orderings on F then the intersection over all orderings containing $\Sigma_\square(F)$ would be the empty intersection, and thus would equal F. □

COROLLARY 14.5 (Artin). *Let F be a field of characteristic different from 2. For $x \in F$, the following are equivalent:*

(i) *For every ordering P on F, we have $x \in P$.*
(ii) *The element x is a sum of squares.*

PROOF. If F is not formally real, then it has no orderings, hence $\Sigma_\square(F)$ is not a preordering, so because $\operatorname{char} F \neq 2$ we have $\Sigma_\square(F) = F$. Thus in this case every element of F satisfies both (i) and (ii). If K is formally real, we apply Theorem 14.4a) to the preordering $\Sigma_\square(F)$. □

Corollary 14.5 is an important step towards the solution of Hilbert's 17th problem: show that any positive semidefinite polynomial $f \in \mathbb{R}[t_1, \ldots, t_n]$ is a sum of squares of rational functions.

2. Interlude on Quadratic Forms

Let F be a field of characteristic different from 2 and let $\langle \cdot, \cdot \rangle$ be a bilinear form over F, say with underlying vector space F^n. We associate the **quadratic form**

$$q : F^n \to F,\ q(x) \coloneqq \langle x, x \rangle.$$

Then q is the function obtained from evaluating a homogeneous quadratic polynomial $q(t_1, \ldots, t_n \in F[t_1, \ldots, t_n]$. Indeed, if the bilinear form has Gram matrix $M(i,j) = \langle e_i, e_j \rangle$, then

$$q(t_1, \ldots, t_n) = \sum_{1 \leq i \leq n} M(i,i) t_i^2 + \sum_{1 \leq i < j \leq n} \frac{M(i,j)}{2} t_i t_j.$$

The bilinear form can be recovered from q as

$$\langle x, y \rangle = \frac{1}{2} q(x+y) - q(x) - q(y),$$

so in this setting bilinear forms and quadratic forms are equivalent objects. Again, since $\operatorname{char} F \neq 2$, all bilinear forms can be diagonalized: for some basis $f_1, \ldots, f_n$ of F^n, we have $\langle f_, f_j \rangle = 0$ when $i \neq j$. There is a unique $P \in \mathrm{GL}_n(F)$ such that $f_i = Pe_i$ for all $1 \leq i \leq n$, and then $P^T G P$ is a diagonal matrix with (i,i) entry $a_i \coloneqq \langle f_i, f_i \rangle$. The corresponding diagonalized quadratic form is

$$q = a_1 t_1^2 + \ldots a_n t_n^2.$$

Clearly the bilinear form is nondegenerate if and only if $a_i \neq 0$ for all i, and in this case we also say that q is nondegenerate. Henceforth we will only consider nondegenerate quadratic forms.

A nondegenerate quadratic form q is **isotropic** if there is $0 \neq x = (x_1, \ldots, x_n) \in F^n$ such that $q(x) = 0$; otherwise q is **anisotropic**. If $n = 1$, then a nondegenerate

quadratic form is of the form ax^2 for $a \in F^\times$: this form is anisotropic.

These concepts turn out to be highly relevant to the theory of ordered fields. First of all, Lemma 14.1 implies that a field of characteristic not 2 is formally real if and only if, for all $n \in \mathbb{Z}^+$, the sum of n squares form

$$S_n(t_1, \ldots, t_n) \coloneqq t_1^2 + \ldots + t_n^2$$

is anisotropic, so by Artin–Schreier this is the necessary and sufficient condition for such a field F to admit an ordering (once more: we know that fields of positive characteristic admit no orderings). The main object in the algebraic theory of quadratic forms is the Witt ring $W(F)$ of F: this is a ring whose elements are isomorphism classes of anisotropic quadratic forms over F. There is a rich theory, especially over fields of classical interest.

Let us mention the Hasse–Minkowski Theorem, which concerns quadratic forms over a number field F. Suppose that F has signature (r, s): r real embeddings and s complex conjugate pairs of nonreal embeddings. A number field F comes endowed with a set σ_F of **places**, which are equivalence classes of absolute values on F. First there are finitely many **infinite places**. There are r real places: these come from applying the real embeddings of F into $\mathbb{R}$ and taking the usual real absolute value. Then there are s complex places: these come from applying one out of each complex conjugate pair of nonreal embeddeings of F into $\mathbb{C}$ and taking the usual complex absolute value. The other places are called **finite** and correspond to nonzero prime ideals $\mathfrak{p}$ in the ring of intgers $\mathbb{Z}_F$ of F: each such ideal induces a discrete valuation $v_\mathfrak{p} : F^\times \to \mathbb{Z}$, and (up to a choice of normalization that amounts to varying the absolute value within its equivalence class) we take $|x| \coloneqq 2^{-v_\mathfrak{p}}$ for nonzero x and $|0| \coloneqq 0$. Each of these absolute values induces a metric d_v on F by $(x, y) \mapsto |x - y|_v$ and we define F_v to be the completion of F with respect to this metric. If v is real, then $F_v \cong \mathbb{R}$; if v is complex, then $F_v \cong \mathbb{C}$; while if v is finite, then F_v is a p-adic field.

THEOREM 14.6 (Hasse–Minkowski). *Let F be a number field, and let $q = q(t_1, \ldots, t_n) \in F[t_1, \ldots, t_n]$ be a nondegenerate quadratic form. The following are equivalent:*

(i) *The quadratic form q is isotropic.*
(ii) *For all places $v \in \Sigma_F$, the quadratic form $q \in F_v[t_1, \ldots, t_n]$ is isotropic.*

This result is supplemented by a complete classification of quadratic forms q_v over F_v for all places v. We may assume that q_v is nondegenerate, diagonal and that $n \geq 2$. Let us mention some relevant points:

• When v is a complex place, every q_v is isotropic: we may prescribe the first $n - 1$ values arbitrarily and then solve $q(x_1, \ldots, xn - 1, t_n) = 0$ for t_n by taking a square root.
• When v is a real place, $q_v = a_1 t_1^2 + \ldots + a_n t_n^2$ is anisotropic if and only if the coefficients a_i are either all positive or all negative. (This follows e.g. from the fact that $q_v(\mathbb{R}^n)$ is a connected subset of $\mathbb{R}$.) When this occurs, we say that q_v is **definite**; otherwise we say that q_v is **indefinite**.
• When v is a finite place and $v \geq 5$, then q_v is isotropic.

COROLLARY 14.7. *Let F be a number field, let $n \geq 5$, and let $q(t_1, \ldots, t_n) \in F[t_1, \ldots, t_n]$ be a nondegenerate quadratic form. Then q is isotropic if and only if it is indefinite at every real place of F.*

From this result we deduce:

THEOREM 14.8. *A number field F is formally real if and only if it can be embedded in $\mathbb{R}$.*

PROOF. The field F is formally real if and only if for all $n \in \mathbb{Z}^+$ the sum of squares form $S_n = t_1^2 + \ldots + t_n^2 = 0$ is anisotropic. If S_k is isotropic, then clearly so is S_n for all $n \geq k$, so F is formally real if and only if S_n is anisotropic for all $n \geq 5$. For all $n \in \mathbb{Z}^+$, the real quadratic form S_n is definite, so by Corollary 14.7, for $n \geq 5$, the quadratic form S_n is anisotropic over F if and only if F is real. □

Here is a crisper repackaging of the new content of Theorem 14.8.

EXERCISE 14.5. *Show: if F is a nonreal number field, then there are $x_1, x_2, x_3, x_4 \in F$ such that*

$$-1 = x_1^2 + x_2^2 + x_3^3 + x_4^2.$$

If F is a field of characteristic different from 2 that is not formally real, its **level** $\mathbf{s}(F)$ is the least $n \in \mathbb{Z}^+$ such that -1 is a sum of n squares. A remarkable theorem of Pfister asserts that the level is always 2^k for some $k \in \mathbb{N}$. The case we need of this is ridiculously elementary:

EXERCISE 14.6. *Let F be a field, and suppose there are $x, y, z \in F$ such that $-1 = x^2 + y^2 + z^2$.*

a) *Show:*

$$-1 = \frac{(x^2 + y^2)(1 + z^2)}{(1 + z^2)^2}.$$

b) *Show: for A, B, C, D in any commutative ring,*

$$(A^2 + B^2)(C^2 + D^2) = (AC - BD)^2 + (AD + BC)^2.$$

c) *Deduce: -1 is a sum of two squares in F.*

Thus the level of a nonreal number field is 1, 2 or 4. The first case is no mystery: clearly the level is 1 if and only if F contains a fourth root of unity. Thus for any imaginary quadratic field other than $\mathbb{Q}(\sqrt{-1})$, the level is at least 2.

EXAMPLE 14.9. *Let $D \in \mathbb{Z}^+$, and let $F = \mathbb{Q}(\sqrt{-D})$. Then*

$$-1 = \left(\frac{1}{\sqrt{-D}}\right)^2 + \ldots + \left(\frac{1}{\sqrt{-D}}\right)^2 (D \text{ times}),$$

so $\mathbf{s}(F) \leq D$. It follows that

$$\mathbf{s}(\mathbb{Q}(\sqrt{-1})) = 1, \mathbf{s}(\mathbb{Q}(\sqrt{-2})) = 2,$$

and, using Pfister's Theorem,

$$\mathbf{s}(\mathbb{Q}(\sqrt{-3})) = 2.$$

However, this does not tell us anything helpful for $D \geq 4$.

A field F has level 2 if and only if there are $x, y, z \in F$, not all 0, such that $x^2 + y^2 + z^2 = 0$. This holds if and only if the Hamilton quaternion algebra $B := \left(\frac{-1,-1}{F}\right)$ is not a division algebra. The Hasse Principle holds for division algebras as well, so a number field F has level 2 if and only if, for all places v of F, $B_v := \left(\frac{-1,-1}{F_v}\right)$ is not a division algbera. Over $F = \mathbb{Q}$, the Hamilton quaternion algebra *is* a division algebra, and the places over which it is locally a division algebra are the infinite place ∞ and the finite place 2. So F has level 2 if and only if it is not real and for all places $v \mid 2$ of F, we have that B_v is not a division algebra. For any finite degree extension L/K of p-adic fields, if $B_{/K}$ is a division quaternion algebra, then $B \otimes_K L$ is not a division algebra if and only if $[L : K]$ is even. So we get the following result, originally due to Fein–Gordon–Smith [**FGS71**, Thm. 1].

COROLLARY 14.10. *A number field F has level 2 if and only if it is nonreal and for prime $\mathfrak{p}$ of $\mathbb{Z}_F$ lying over 2, we have $2 \mid e_{\mathfrak{p}} f_{\mathfrak{p}}$.*

EXERCISE 14.7.

a) *Let D be a negative squarefree integer, and let $F := \mathbb{Q}(\sqrt{D})$. Show: $\mathbf{s}(F) = 2$ if and only if D is even or $D \equiv 3, 5 \pmod 8$.*

b) *Let $p > 2$ be a prime, and let $F := \mathbb{Q}(\zeta_p)$ be the pth cyclotomic field. Show: $\mathbf{s}(F) = 2$ if and only if the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$ is even.*

3. Extensions of Formally Real Fields

Let K/F be a field extension. If K is formally real, then by Artin–Schreier it admits an ordering P, which restricts to an ordering $\mathfrak{p}$ on F. The converse scenario is much more interesting: suppose $\mathfrak{p}$ is an ordering on a field F and that K/F is a field extension. Can $\mathfrak{p}$ be extended to K?

Clearly it is necessary that K be formally real. But this is not sufficient. Let $F = \mathbb{R}(t)$. By Example 13.15, there is a unique ordering $\mathfrak{p}$ on F extending the usual (in fact unique, by Exercise 14.4) ordering on $\mathbb{R}$ and in which $t > c$ for all $c \in \mathbb{R}$. Let $K := F(\sqrt{-t}) = \mathbb{R}(\sqrt{-t})$. Clearly $\mathfrak{p}$ does not extend to K because we have made the negative element t a square. However, $\sqrt{-t}$ is transcendental over $\mathbb{R}$, so as abstract fields we have $K \cong F$ and therefore K is formally real.

In general the extension problem for orderings is a rich one with a large literature. But we will give one fundamental and useful result, an extension of the Artin–Schreier Theorem. First:

LEMMA 14.11. *For an ordered field $(F, \mathfrak{p})$, an extension K/F, and $c \in K$, the following are equivalent:*

(i) *There are $a_1, \ldots, a_n \in \mathfrak{p}^\bullet$ and $x_1, \ldots, x_n \in K$ such that*
$$c = a_1 x_1^2 + \ldots + a_n x_n^2.$$

(ii) *We have $c \in \bigcap_{P \supset \mathfrak{p}} \mathbb{P}$, the intersection being over all orderings of K extending $\mathfrak{p}$.*

PROOF. Let
$$T := \{a_1 x_1^2 + \ldots + a_n x_n^2 \mid a_i \in \mathfrak{p},\ x_i \in K\},$$
so the desired equivalence can be rephrased as $T = \bigcap_{P \supset \mathfrak{p}} P$. Moreover T satisfies (PO1) and (PO2), and an ordering P of K contains T if and only if it contains $\mathfrak{p}$.

Case 1: Suppose $-1 \notin T$. Then T is a preordering on K, and by Theorem 14.4a), we have $T = \bigcap_{P \supset \mathfrak{p}} P$.
Case 2: If $-1 \in T$, then $T = K$ and there is no ordering on K extending $\mathfrak{p}$, so $T = K = \bigcap_{P \supset \mathfrak{p}} P$. □

We are now ready for one of our main results.

THEOREM 14.12. *For an ordered field $(F, \mathfrak{p})$ and a field extension K/F, the following are equivalent:*

(i) *There is an ordering on K extending $\mathfrak{p}$.*
(ii) *For all $a = (a_1, \ldots, a_n) \in (\mathfrak{p}^\bullet)^n$, the quadratic form*

$$q_a = a_1 t_1^2 + \ldots + a_n t_n^2$$

is anisotropic over K.

PROOF. (i) $\implies$ (ii) is immediate from Lemma 13.13c).
(ii) $\implies$ (i): If for some $a \in (\mathfrak{p}^\bullet)^n$ the quadratic form $q_a(x)$ represents -1, then the form $q_{a,1} = a_1 t_1^2 + \ldots + a_n t_n^2 + t_{n+1}^2$ would be isotropic, contrary to our hypothesis. It follows that

$$-1 \notin T := \{a_1 x_1^2 + \ldots + a_n x_n^2 \mid a_i \in \mathfrak{p},\ x_i \in K\},$$

so T is a preordering of K extending $\mathfrak{p}$. By Theorem 14.4a), the preordering T extends to at least one ordering of K. □

Theorem 14.12 can be viewed as a "relative" version of the Artin–Schreier Theorem. To see what this means, suppose a field K is formally real, and consider Theorem 14.12 applied with $F = \mathbb{Q}$ endowed with its unique ordering $\mathfrak{p}$. Suppose there were $a_1, \ldots, a_n \in \mathbb{Q}^{>0}$ such that the quadratic form $a_1 t_1^2 + \ldots + a_n t_n^2$ were isotropic over K. Scaling a quadratic form by any nonzero element of the field does not change its an/isotropy, so we may clear denominators to get $A_1, \ldots, A_n \in \mathbb{Z}^+$ such that $A_1 t_1^2 + \ldots + A_n t_n^2$ is isotropic over K: there are $x_1, \ldots, x_n \in K$, not all 0, such that $A_1 x_1^2 + \ldots + A_n x_n^2 = 0$. But writing out $A_i x_i^2$ as $x_i^2 + \ldots + x_i^2$ (A_i times) shows that the sum of $A_1 + \ldots + A_n$ squares form is isotropic over K, contradicting the formal reality of K. Therefore by Theorem 14.12, there is an ordering on K extending $\mathfrak{p}$: this is the Artin–Schreier Theorem.

We will now deduce several sufficient conditions for extending orderings.

THEOREM 14.13. *Let $(F, \mathfrak{p})$ be an ordered field, and let $K = F(\{\sqrt{x}\}_{x \in \mathfrak{p}})$ be the extension obtained by adjoining all square roots of positive elements. Then the ordering $\mathfrak{p}$ extends to K.*

PROOF. By Theorem 14.12, it suffices to show that for all $n, r \in \mathbb{Z}^+$ and all $b_1, \ldots, b_r, c_1, \ldots, c_n \in \mathfrak{p}$, if $x_1, \ldots, x_n \in K_r := F(\sqrt{b_1}, \ldots, \sqrt{b_r})$ are such that

$$c_1 x_1^2 + \ldots + c_n x_n^2 = 0, \tag{45}$$

then $x_1 = \ldots = x_n = 0$. For any fixed n, we prove this by induction on r. Suppose by induction that the equation $c_1 x_1^2 + \ldots + c_n x_n^2 = 0$ has no nontrivial solutions over K_{r-1}, and let $(z_1, \ldots, z_n) \in K_r^n$ be a solution to (45). Write $z_i = x_i + \sqrt{b_r} y_i$, with $x_i, y_i \in K_{r-1}$. Then equating "rational parts" in the equation

$$0 = \sum c_i z_i^2 = \sum c_i x_i^2 + \sum b_r c_i y_i^2 + 2 \sum c_i x_i y_i \sqrt{b_r}$$

shows that $(x_1, \ldots, x_n, y_1, \ldots, y_n) \in K_{r-1}^{2n}$ is a solution of

$$c_1 t_1^2 + \ldots + c_n t_n^2 + b_r c_1 t_{n+1}^2 + \ldots + b_r c_n t_{2n}^2 = 0.$$

By induction, $x_1 = \ldots = x_n = y_1 = \ldots = y_n = 0$, i.e., $z_1 = \ldots = z_n = 0$. □

To obtain further results we take a perspective arising from quadratic form theory. Let us say a field extension K/F is **anisotropic** if every anisotropic quadratic form $q(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ remains aniostropic when extended to K. (In the algebraic theory of quadratic forms one studies the **Witt kernel** of a field extension: the kernel of the natural ring homomorphism $W(F) \to W(K)$. An anisotropic extension is precisely one in which the Witt kernel is trivial.) From Theorem 14.12 we immediately deduce the following result.

COROLLARY 14.14. *If $(F, \mathfrak{p})$ is an ordered field and K/F is an anisotropic extension, then the ordering $\mathfrak{p}$ extends to K.*

EXERCISE 14.8. *Let F be a field and let $\{K_i\}_{i \in I}$ be a directed system of anisotropic extensions of K. Show: $\varinjlim K_i/F$ is an anisotropic extension.*

The next results give the two basic examples of anisotropic extensions.

THEOREM 14.15. *A purely transcendental extension K/F is anisotropic.*

PROOF. Step 0: It suffices to prove that $F(t)/F$ is anisotropic. Indeed, if so then an immediate induction gives that $F(t_1, \ldots, t_n)/K$ is anisotropic, and we finish by applying Exercise 14.8.
Step 1: Let F be any field, and let $(f_1, \ldots, f_n) \in F(t)^n$ be an n-tuple of rational functions, not all zero. Then there is a nonzero rational function f such that $(ff_1, \ldots, ff_n)$ is a **primitive vector** in $F[t]$, i.e., each $ff_i \in F[t]$ and $\gcd(ff_1, \ldots, ff_n) = 1$. Indeed this holds with $F[t]$ and $F(t)$ replaced by any UFD and its fraction field.
Step 2: Let $q = a_1 x_1^2 + \ldots + a_n x_n^2$ be a nonsingular quadratic form over F such that $q_{F(t)}$ is isotropic: there are rational functions $f_1, \ldots, f_n$, not all zero, such that

$$a_1 f_1^2 + \ldots + a_n f_n^2 = 0.$$

Let $f \in F(t)^\times$ be the rational function as in Step 1; then multiplying through by f^2 we get a primitive polynomial solution, i.e., there exist polynomials $p_1(t), \ldots, p_n(t) \in F[t]$ with $\gcd(p_1(t), \ldots, p_n(t)) = 1$ and

$$a_1 p_1(t)^2 + \ldots + a_n p_n(t)^2 = 0.$$

Now we substitute $t = 0$ (or any value of F): we cannot have $p_1(0) = \ldots = p_n(0) = 0$, because then all of the p_i's would be divisible by t, contradicting primitivity. Therefore $q(p_1(0), \ldots, p_n(0)) = 0$ shows that q is isotropic over F. □

The proof of Theorem 14.15 used only that q was a form – i.e., a homogeneous polynomial – not that it was a *quadratic* form. Indeed any system of homogeneous polynomials would work as well, so the argument really shows: if $V_{/F}$ is a projective variety which has a $F(t)$-rational point, then it has a F-rational point.[1]

To be honest, we took this route because the remark in the last paragraph seemed

[1]The same conclusion holds for arbitrary varieties over any infinite field, or for complete varieties over a finite field. But taking the projective line over $\mathbb{F}_q$ and removing its $\mathbb{F}_q$-rational points shows that *some* hypothesis is necessary!.

interesting. In fact we can *directly* extend orderings to purely transcendental field extensions, as we already saw in the case of one indeterminate in Example 13.15.

EXERCISE 14.9. *Let (F, P) be an ordered field, and let $\{t_i\}_{i \in I}$ be an indexed set of indeterminates, and endow it with a total ordering. Show: there is a unique extension of P to an ordering on $F(\{t_i \mid i \imath I\})$ that restricts to the given ordering on the set of indeterminates and such that for all $i \in I$ and all $c \in F$ we have $t_i > c$.*

The following was conjectured by Witt in 1937 and proven by Springer in 1952.[2]

THEOREM 14.16. *(Springer* [**Sp52**]*) A field extension K/F of finite* odd *degree is anisotropic.*

PROOF. We go by induction on the degree, the case $d = 1$ being trivial. Suppose the result holds for all field extensions of odd degree less than d, and K/F be an extension of odd degree d. If K/F had any proper subextension, then we would be done by a dévissage argument. So we may assume in particular that K is monogenic over F: $K = F[x]$. Let $p(t) \in F[t]$ be the minimal polynomial of x. Let q be an anisotropic quadratic form over F that becomes isotropic over K: i.e., there exists an equation

$$q(g_1(t), \ldots, g_n(t)) = h(t)p(t) \tag{46}$$

with polynomials $g_i, h \in F[t]$, not all $g_i = 0$, and $M := \max \deg g_i \leq d - 1$. As in the proof of Proposition 14.15, we may also assume that $(g_1, \ldots, g_n)$ is a primitive vector in $F[t]$. Since q is anisotropic, the left hand side of (46) has degree $2M \leq 2d - 2$, so $\deg h$ is *odd* and at most $d - 2$. In particular, h has an irreducible factor $\tilde{h}$ of odd degree at most $d-2$; let y be a root of $\tilde{h}$ in $\overline{F}$. Taking $t = y$ in (46), we see that $q(g_1(y), \ldots, g_n(y)) = 0$. Note that since $F[t]$ is a PID, the condition $\gcd(g_1, \ldots, g_n) = 1$ is equivalent to the fact that $1 \in \langle g_1, \ldots, g_n \rangle$, which implies that the polynomials $g_1, \ldots, g_n$ remain setwise coprime as elements of $F[y][t]$. In particular, not all $g_i(y)$ are equal to 0, so that $q_{F[y]}$ is isotropic. By induction, this implies that q was isotropic, contradiction! □

COROLLARY 14.17. *If F is formally real, and K/F is an extension of finite* odd *degree, then K is also formally real.*

PROOF. If F is formally real, then for all $n \in \mathbb{Z}^+$, the sum of n squares form S_n is anisotopic over F. By Theorem 14.16, the form S_n is anisotropic over K, so K is formally real. □

EXERCISE 14.10. *In the algebraic theory of quadratic forms it is shown that the Witt kernel of a quadratic extension $K = F(\sqrt{p})/F$ is the principal ideal generated by $\alpha = \langle 1, -p \rangle$: [**Cl-QF**, Thm. II.20]. In other words, it consists of quadratic forms $a_1x_1^2 + \ldots + a_nx_n^2 - pa_1x_1^2 - \ldots - pa_nx_n^2$ for $a_1, \ldots, a_n \in F^\times$. Use this (and induction) to give another proof of Theorem 14.13.*

4. The Grand Artin–Schreier Theorem

A field F is **real-closed** if it is formally real and admits no proper formally real algebraic extensions. For instance, $\mathbb{R}$ is evidently real-closed since its unique non-trivial algebraic extension is $\mathbb{C} = \mathbb{R}(\sqrt{-1})$, which is not formally real.

[2]According to D. Hoffmann, Artin orally conveyed a proof of Witt's conjecture to Witt in 1939: he calls the result the Artin–Springer Theorem.

EXERCISE 14.11. *For a field k, we define the field of* ***Puiseux series with coefficients in k***

$$P_k := \bigcup_{n \in \mathbb{Z}^+} k((t^{\frac{1}{n}})).$$

a) *Use Example 8.31 to show that the real $P_{\mathbb{R}}$ of real Puiseux series is real-closed.*
b) *Show: in the unique ordering on $P_{\mathbb{R}}$, for all $n \in \mathbb{Z}^+$ and $a \in \mathbb{Q}^{>0}$, we have $0 < t^{1/n} < a$.*

The previous examples of real-closed fields F were obtained by showing that F is formally real and $F(\sqrt{-1})$ is algebraically closed. In fact this is a characterization of real-closed fields. In particular the absolute Galois group of a real-closed field is finite and nontrivial. Remarkably, this too is a characterization of real-closed fields! These assertions are part of the following result, one of the most striking and celebrated theorems in all of field theory.

THEOREM 14.18. *(Grand Artin–Schreier Theorem)*
Let F be a field with algebraic closure $\overline{F}$ and separable closure F^{sep}. The following are equivalent:

(i) *F is real-closed: it is formally real and admits no proper formally real algebraic extension.*
(ii) *F is formally real, every odd degree polynomial over F has a root, and for each $x \in F$, one of x, $-x$ is a square.*
(iii) *F is formally real and $F(\sqrt{-1})$ is algebraically closed.*
(iv) *The extension $\overline{F}/F$ is nontrivial and of finite degree.*
(v) *The absolute Galois group $\mathfrak{g}_F := \mathrm{Aut}(F^{\mathrm{sep}}/F)$ is finite and nontrivial.*

REMARK 14.1. *Recall that $F^{\mathrm{sep}} = \overline{F}$ if and only if F is perfect. Conditions (i) through (iii) clearly imply that F has characteristic 0, hence is perfect. Condition (iv) easily implies that F is perfect: contrapositively, if F is not perfect, then F has characteristic p and there is $x \in F \setminus F^p$, and then for all $n \in \mathbb{Z}^+$, we have that $[F(x^{p^{-n}}) : F] = p^n$, showing that $\overline{F}/F$ has infinite degree. For a perfect field F, conditions (iv) and (v) are manifestly the same, but it is (true but) not at all clear why condition (v) implies that F is perfect, hence the point of stating the two conditions separately. And indeed the implication (v) $\implies$ (i) is by far the lion's share of the proof. Our treatment of it closely follows lecture notes of K. Conrad.*

PROOF. (i) $\implies$ (ii): Suppose F is formally real. Let $f \in F[t]$ be an odd degree polynomial. If f has no root in F, then it has an an irreducible factor of odd degree $d > 1$, and thus there is a proper odd degree extension K/F. By Corollary 14.17, the field K is formally real, contradicting the real closure of F. Suppose that neither x nor $-x$ is a square. One of them is positive; WLOG say it is x. By Theorem 14.13 $F(\sqrt{x})/F$ is a proper formally real extension, contradiction. (ii) $\implies$ (iii) By Theorem 14.4, F admits an ordering P. With respect to P, the hypothesis that for all $x \in F$ one of x and $-x$ is a square becomes that every $x \in P$ is a square. Also, since F is ordered, we certainly have $[F(\sqrt{-1}) : F] = 2$. Let $\overline{F}$ be an algebraic closure of $F(\sqrt{-1})$: we wish to show that $\overline{F} = F(\sqrt{-1})$. By hypothesis on odd degree polynomials having a root, the absolute Galois group of F is a pro-2-group, and thus so is the absolute Galois group of $F(\sqrt{-1})$. If $F(\sqrt{-1}) \neq \overline{F}$ then, we are entitled to a proper finite degree extension M of $F(\sqrt{-1})$, which is Galois

over $F(\sqrt{-1})$ and has degree a power of 2. By the basic theory of 2-groups together with the Galois correspondence, there must exist a subextension G of $M/F(\sqrt{-1})$ with $[G : F(\sqrt{-1})] = 2$. But we claim that the hypotheses on F imply that $F(\sqrt{-1})$ is quadratically closed. Indeed, let a, b be arbitrary elements of F. We claim that there are $c, d \in F$ such that

$$a + b\sqrt{-1} = (c + d\sqrt{-1})^2.$$

This amounts to the system $a = c^2 - d^2$, $b = 2cd$. Substituting $d = \frac{b}{2c}$, we get the equation $c^2 = a + \frac{b^2}{4c^2}$, or $c^4 - ac^2 - \frac{b^2}{4} = 0$. The quadratic formula gives

$$c^2 = \frac{a \pm \sqrt{a^2 + b^2}}{2}.$$

Since inside the radical we have a sum of squares, the squareroot does exist in F. If we choose the plus sign in the square root, it is easy to see that the expression is again non-negative, so we can solve for c in our field F.
(iii) $\implies$ (iv) is immediate.
(iv) $\implies$ (v): Suppose $\overline{F}/F$ is nontrivial and of finite degree. As mentioned above, the finiteness of $[\overline{F} : F]$ implies that $\overline{F} = F^{\text{sep}}$, and thus $\#\mathfrak{g}_F = \#\operatorname{Aut}(F^{\text{sep}}/F) = [F^{\text{sep}} : F] = [\overline{F} : F]$, so $\mathfrak{g}_F$ is finite and nontrivial.
(v) $\implies$ (i): This proof will be given below. □

Now we begin the proof of (v) $\implies$ (i), so suppose that $\mathfrak{g}_F$ is finite and nontrivial.

Step 1: We wish to show that $\#\mathfrak{g}_F = 2$. If not, then by Sylow theory there is a subgroup H of order either 4 or an odd prime ℓ. We will rule these out. Because H is the absolute Galois group of $(F^{\text{sep}})^H$, ruling this out is logically the same as showing that $\mathfrak{g}_F$ cannot have order 4 or $\ell > 2$, so we will use $\mathfrak{g}_F$ rather than changing the notation.

First we suppose $\#\mathfrak{g}_F = \ell$ and let σ be a generator of $\mathfrak{g}_F$.

Step 3: We claim that the characteristic of F is not equal to ℓ. If it were, then Artin–Schreier theory would apply, so that $\overline{F} = F(\alpha)$, where α is a root of an Artin–Schreier polynomial $t^p - t - a \in F[t]$. We may write any element $b \in \overline{F}$ as

$$b = b_0 + b_1\alpha + \ldots + b_{\ell-1}\alpha^{\ell-1}$$

for unique $b_0, \ldots, b_{\ell-1} \in F$. Thus

$$b^\ell - b = \sum_{i=0}^{\ell-1} b_i^\ell \alpha^{\ell i} - b_i\alpha^i = \sum_{i=0}^{\ell-1} b_i^\ell(\alpha + a)^i - b_i\alpha^i = \left(b_{p-1}^p - b_{p-1}\right)\alpha^{p-1} + O(\alpha^{p-2}),$$

where by $O(\alpha^{p-2})$ we mean a polynomial in α of degree at most $p - 2$. Choose $b \in F^{\text{sep}}$ such that $b^p - b = a\alpha^{p-1}$, and then equating coefficients of α^{p-1} gives $b_{p-1}^p - b_{p-1} - a = 0$. Since $b_{p-1} \in F$, this contradicts the irreducibility of $t^p - t - a$.

Step 4: Suppose ℓ is a prime such that $\#\mathfrak{g}_F = \ell$. Since the characteristic of F is not ℓ, F^{sep} contains a primitive ℓth root of unity ζ. Moreover, since $[F(\zeta) : F] \leq \ell - 1$ and thus coprime to ℓ, we must have $\zeta \in F$. So Kummer Theory applies to give $\overline{F} = F(\gamma)$, where $\gamma^\ell = c \in F$. Choose $\beta \in F^{\text{sep}}$ such that $\beta^\ell = \gamma$, so $\beta^{\ell^2} = c$. Thus $\beta^{\ell^2} = \sigma(\beta^{\ell^2}) = (\sigma\beta)^{\ell^2}$, so $\sigma(\beta) = \omega\beta$ with $\omega^{\ell^2} = 1$. Then ω^ℓ, being an ℓth root of

unity, lies in F. If $\omega^\ell = 1$, then $(\sigma(\beta))^\ell = \beta^\ell$, so $\sigma(\beta^\ell) = \beta^\ell$ and then $\beta^\ell = \gamma \in F$, contradiction. So ω is a primitive (ℓ^2)th root of unity. It follows easily that there is $k \in \mathbb{Z}$ such that

$$\sigma\omega = \omega^{1+\ell k}.$$

From $\sigma\beta = \omega\beta$, we get

$$\beta = \sigma^p\beta = \sigma^{\ell-1}\omega\beta = \omega\sigma(\omega)\cdots\sigma^{\ell-1}(\omega)\beta = \omega^{1+(1+\ell k)+\ldots+(1+\ell k)^{\ell-1}}\beta.$$

From this we deduce

$$\sum_{i=0}^{\ell-1} 1 + (1+\ell k) + \ldots + (1+\ell k)^{\ell-1} \equiv 0 \pmod{\ell^2}.$$

Expanding out the binomial and reducing modulo ℓ^2, we get

$$0 \equiv \sum_{i=0}^{\ell-1}(1+i\ell k) \equiv \ell + \frac{(\ell-1)(\ell)}{2}(\ell k) \pmod{\ell^2}.$$

If ℓ is odd, this gives $0 \equiv \ell \pmod{\ell^2}$, a contradiction. When $\ell = 2$, we get

$$2 + 2k \equiv 0 \pmod 4,$$

so that k is odd. In this case ω has order 4 and $\sigma\omega = \omega^{1+2k} = \omega^3$, so $\sigma\omega \neq \omega$ and $\omega \notin F$. Let us write ω as i. In summary: if $\#\mathfrak{g}_F$ is prime, then it equals 2, $\sqrt{-1} \notin F$ and F does not have characteristic 2.

Step 5: Now suppose that $\#\mathfrak{g}_F = 4$. Then $\mathfrak{g}_F$ has a subgroup H of order 2. In the proof of Step 3 we did not use that $\ell > 2$, so applying this argument with H in place of $\mathfrak{g}_F$ shows that F cannot have characteristic 2. Then there is at least one subextension K of F^{sep}/F with $[F^{\mathrm{sep}} : K] = 2$. Then the above reasoning shows that $\sqrt{-1} \notin K$, hence not in F, but then $F(\sqrt{-1})$ is a subfield of F^{sep} with $[F^{\mathrm{sep}} : F(\sqrt{-1})] = 2$ and containing a 4th root of unity, contradicting the above analysis.

In summary, we have shown so far that if $\mathfrak{g}_F$ is finite and nontrivial, then $\#\mathfrak{g}_F = 2$, F does not have characteristic 2 and $F^{\mathrm{sep}} = F(\sqrt{-1})$. It now suffices to show that F is formally real: then it has characteristic 0 so $[\overline{F} : F] = 2$, so clearly F admits no proper formally real algebraic extension, so it is real-closed. This is handed by the following result:

LEMMA 14.19. *Let F be a field in which $-1 \notin F^2$ and such that every element of $F(\sqrt{-1})$ is a square in $F(\sqrt{-1})$. Then:*

a) $\Sigma_\square(F) = F^2$, *and*
b) *F is formally real.*

PROOF. Put $i = \sqrt{-1}$. To show part a), it is enough to see that the sum of two squares in $F(i)$ is again a square in $F(i)$. Let $a, b \in F$. By hypothesis, there are $c, d \in F$ such that $(a+bi) = (c+di)^2$, so $a = c^2 - d^2$ and $b = 2cd$ and thus $a^2 + b^2 = (c^2+d^2)^2$.
a) If F had positive characteristic p, then -1 is a sum of $p-1$ squares but not itself a square, contradicting part a).
b) Since $-1 \notin F^2$, by part a) -1 is not a sum of squres, so F is formally real. $\square$

EXERCISE 14.12. *Let F be a formally real field, and let $n \in \mathbb{Z}^+$. Let $f_n : F \to F$ by $f_n(x) = x^n$.*

a) *Show: f_n is injective if and only if n is odd.*
b) *Suppose that F is real-closed. Show: f_n is bijective if and only if n is odd.*

We now give some variations on Theorem 14.18.

EXERCISE 14.13. *(E. Fried): Let F be a field. Suppose that there is $d \in \mathbb{Z}^+$ such that for every irreducible polynomial $P \in K[t]$, $\deg(P) \leq d$. Show that F is real-closed or algebraically closed.*

EXERCISE 14.14. *(Knopfmacher–Sinclair) Let F be a field. Suppose that the set of isomorphism classes of finite-dimensional field extensions of F is finite. Show that F is real-closed or algebraically closed.*

EXERCISE 14.15. *(E. Fried): Let C be an algebraically closed field and K a subfield of C with $K \neq C$. Suppose that C is finitely generated over K. Show: K is real-closed and $C = K(\sqrt{-1})$.*

By Leptin–Waterhouse, every profinite group is the automorphism group of some algebraic Galois extension. However, if we restrict to **absolute Galois groups** – that is, $\mathfrak{g}_F := \mathrm{Aut}(F^{\mathrm{sep}}/F)$ for a field F, then Theorem 14.18 shows that this is no longer the case. First of all, it shows that if $\#\mathfrak{g}_F > 2$, then $\mathfrak{g}_F$ is infinite. But since a closed subgroup of an absolute Galois group is also an absolute Galois group, applying the Profinite Sylow Theorem, we get more: let p be a prime number such that $p \mid |\mathfrak{g}_F|$. If $p \neq 2$, then $p^\infty \mid |\mathfrak{g}_F|$, while if $p = 2$ and $2^2 \mid |\mathfrak{g}_F|$, then $2^\infty \mid |\mathfrak{g}_F|$. Conversely, Exercise 8.28 shows that these are the only restrictions on the profinite order of the absolute Galois group of a field.

There are however many other restrictions on the absolute Galois group of a field. Let us just select what may be the easiest one to state: by a result of Koenigsmann [**Ko05**], the direct product $\mathfrak{g}_{F_1} \times \mathfrak{g}_{F_2}$ of two absolute Galois groups can only be an absolute Galois group if it has no nontrivial elements of finite order and if at least one of $\mathfrak{g}_{F_1}$ and $\mathfrak{g}_{F_2}$ is pro-solvable (an inverse limit of finite solvable groups). Thus for instance $\mathfrak{g}_{\mathbb{F}_q} \times \mathfrak{g}_{\mathbb{R}} \cong \hat{\mathbb{Z}} \times \mathbb{Z}/2\mathbb{Z}$ is not an absolute Galois group, which is interesting because $\mathfrak{g}_{\mathbb{R}((t))} \cong \hat{\mathbb{Z}} \rtimes \mathbb{Z}/2\mathbb{Z}$, a nontrivial *semi*-direct product. Also, since the simple group A_5 is a quotient of $\mathfrak{g}_{\mathbb{Q}}$, the group $\mathfrak{g}_{\mathbb{Q}}$ is not prosolvable, so $\mathfrak{g}_{\mathbb{Q}} \times \mathfrak{g}_{\mathbb{Q}}$ is not an absolute Galois group.

We now come to a key concept in the study of ordered fields. Let F be a formally real field. A **real closure** of F is a real-closed algebraic extension of F.

PROPOSITION 14.20. *Every formally real field admits at least one real closure.*

PROOF. Let F be formally real, and let $\overline{F}$ be an algebraic closure of F. Consider the set of formally real subextensions of $\overline{F}/F$, partially ordered by inclusion. By Exercise 14.1, the union of a chain of formally real fields is formally real, so by Zorn's Lemma there is a maximal formally real subextension of $\overline{F}/F$, which is by definition real-closed. □

COROLLARY 14.21. *Let R be a real-closed field, let F be a subfield of R. Then R contains a unique real-closure of F, namely the algebraic closure of F in R.*

PROOF. Existence: Let F' be the algebraic closure of F in R. Like every subfield of R, the field F' is formally real. If $P \in F'[t]$ is an irreducible polynomial of odd degree, then $F'[t]/(P)$ is a formally real extension of F', so P has a root in R and therefore also in F'. Moreover, if $\alpha \in (F')^\times$, then exactly one of $\alpha, -\alpha$ is a square in R, so that $t^2 \pm \alpha$ has a root in R and thus in F'. By Theorem 14.18, F' is real-closed, so is a real-closure of F. Uniqueness: if $F_1, F_2 \subseteq R$ are real-closed subfields, each algebraic over F, then F_1F_2 is formally real and algebraic over the real-closed F_1, so $F_1F_2 = F_1$ and thus $F_1 = F_2$. □

By Corollary 14.21, there is a unique real-closed subfield of $\mathbb{R}$ that is algebraic over $\mathbb{Q}$. We denote this field by $\mathcal{R}$ and call it the **field of real algebraic numbers**. If c denotes complex conjugation on $\mathbb{C}$, then of course $c(\mathbb{Q}) = \mathbb{Q}$, so $c(\overline{\mathbb{Q}}) = \overline{\mathbb{Q}}$. Since c does not fix $\sqrt{-1}$, it has order 2 as an automorphism of $\overline{\mathbb{Q}}$, so $\overline{\mathbb{Q}}^{\{1,c\}}$ is an index 2 subfield of $\overline{\mathbb{Q}}$ such that $\overline{\mathbb{Q}}^{\{1,c\}}(\sqrt{-1}) = \overline{\mathbb{Q}}$. Corollary 14.21 gives that

$$\overline{\mathbb{Q}}^{\{1,c\}} = \mathcal{R}$$

is the field of real algebraic numbers.

This may suggest that real closures behave very similarly to algebraic closures, but this is not the case! Any two algebraic closures of a field F are isomorphic as F-algebras, but this need *not* be the case for real-closures.

EXAMPLE 14.22. *Let $F = \mathbb{Q}(t)$.*

Because π is transcendental over $\mathbb{Q}$, there is a unique homomorphism $\iota_1 : F \hookrightarrow \mathbb{R}$ that maps t to π. The algebraic closure F_1 of $\iota_1(F)$ in $\mathbb{R}$ is a real-closed subfield of $\mathbb{R}$, so F_1 is Archimedean.

Let $\iota_2 : F \hookrightarrow P_{\mathbb{R}}$, the real Puiseux series field. Let F_2 be the algebraic closure of $\iota_2(F)$ in $P_{\mathbb{R}}$. The unique ordering on F_2 is inherited from the ordering on $P_{\mathbb{R}}$. By Exercise 14.11 we have $t < a$ for all $a \in \mathbb{Q}^{>0}$, so F_2 is non-Archimedean.

Again, two real-closed fields are isomorphic as fields if and only if they are isomorphic as ordered fields, so F_1 and F_2 are nonisomorphic real closures of F.

The way forward is to define real-closures not just for fields but for *ordered fields*. This is the main topic of the final chapter.

CHAPTER 15

Ordered Fields

1. Sign Changing in Ordered Fields

Let $(F, \mathfrak{p})$ be an ordered field, and let $f \in F[t]$ be a polynomial. If for $a, b \in F$ we have $f(a)f(b) < 0$, then we say f **changes sign between a and b**. If such a, b exist we say f **changes sign**.

LEMMA 15.1. *Let $(F, \mathfrak{p})$ be an ordered field. Then:*

a) *Every odd degree $f \in F[t]$ changes sign.*
b) *For all $a > 0$, the polynomial $t^2 - a$ changes sign.*

EXERCISE 15.1. *Prove Lemma 15.1.*

PROPOSITION 15.2. *For an ordered field $(F, \mathfrak{p})$, the following are equivalent:*

(i) ***(Polynomial Intermediate Value Theorem)** Let $f \in F[t]$ and let $a < b \in F$ be such that $f(a)f(b) < 0$. Then there is $c \in F$ such that $a < c < b$ and $f(c) = 0$.*
(ii) *The field F is real-closed.*

PROOF. (i) $\implies$ (ii): Suppose the Polynomial Intermediate Value Theorem holds in F. By Lemma 15.1, every odd degree polynomial $f \in K[t]$ change sign hence has a root. Similarly, if $a \in F^\times$, then either a or $-a$ is positive; without loss of generality $a > 0$, and by Lemma 15.1, $t^2 - a$ changes sign so has a root. Thus there is $b \in F$ with $b^2 = a$. By Theorem 14.18 F is real-closed.
(ii) $\implies$ (i): Without loss of generality we may assume that $f(a) < 0$,, $f(b) > 0$ and that f is monic irreducible. By Theorem 14.18 f has degree 1 or 2. At this point the proof is an amusing callback to high school algebra. If f has degree 1 then it is $f(a) + \left(\frac{f(b)-f(a)}{b-a}\right)x$, so it has a unique root and is moreover increasing, so its unique root must occur in (a, b). Otherwise $f(t) = t^2 + ct + d$, so by the quadratic formula if it does not have a root then $c^2 - 4d < 0$, but then for all $x \in K$, $f(x) = \left(x + \frac{c}{2}\right)^2 + \left(d - \frac{c^2}{4}\right) > 0$, contradiction! □

We can now show that a few more results from calculus hold for polynomial functions over any real-closed field.

COROLLARY 15.3 (Polynomial Rolle's Theorem).
Let F be a real-closed field field, and let $\mathfrak{p} = F^{\times 2} \cup \{0\}$ be its unique ordering. Let $a < b \in F$, and let $f \in F[t]$ be such that $f(a) = f(b) = 0$. Then there is $c \in F$ such that $a < c < b$ and $f'(c) = 0$.

PROOF. We may assume that $f \neq 0$ and thus that f has only finitely many roots in F. Because of this, we may assume that $f(x) \neq 0$ for all $a < x < b$ and therefore write

$$f(t) = (t-a)^p(t-b)^q g(t)$$

where $g \in F[t]$ is nonzero on the entire closed interval $[a,b]$. The Polynomial Intermediate Value Theorem implies that g has constant sign on $[a,b]$. If we put

$$h(t) := p(t-b)g(t) + q(t-a)g(t) + (t-a)(t-b)g'(t),$$

then we have

$$f'(t) = (t-a)^{p-1}(t-b)^{q-1}h(t).$$

Since

$$h(a) = p(a-b)g(a) \text{ and } h(b) = q(b-a)g(b),$$

we have $h(a)h(b) < 0$, so by the Polynomial Intermediate Value Theorem there is $c \in (a,b)$ such that $h(c) = 0$, which implies that $f'(c) = 0$. □

Remark 15.1.

a) *In **Advanced Problem 5861b)** of the 1972 issue of the* American Mathematical Monthly*, Michael Slater asked if the Polynomial Rolle's Theorem can hold for any ordered field that is not real-closed.*[1] *In* [**Pe81**]*, Pelling answered this question positively, which is surprising in view of Proposition 15.2. Later, Brown–Craven–Pelling characterized ordered fields for which Rolle's Theorem holds in* [**BCP86**, Thm. 2.1]*. Their characterization is rather technical for a general field-theoretic audience: these are the ordered fields admitting a valuation that is Henselian, has real-closed residue field and whose valuation group $(\Gamma, +)$ is p-divisible for all $p > 2$. Strangely, this is a condition on a field, not an ordered field, but the existence of such a valuation on a field F implies that the real spectrum of F is homeomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\Gamma/2\Gamma}$, which is certainly nonempty, and then the result implies that Rolle's Theorem holds for all of these orderings on F. We all such fields **Rolle fields**.*

b) *If the Polynomial Rolle's Theorem holds in an ordered field F, it has the following consequence: if $f \in F[t]$ is split, then also $f' \in F[t]$ is split. This condition makes sense in any field: we call such a field **split-Rolle**, so Rolle fields are split Rolle, while any algebraically closed field is (almost trivially) split Rolle but not Rolle. Also $\mathbb{F}_2$ is split-Rolle but not Rolle: $\mathbb{F}_2$ is not formally real, and the split polynomials over $\mathbb{F}_2$ are those of the form $f = t^a(t-1)^b$ for $a, b \in \mathbb{N}$, with derivative*

$$f' = at^{a-1}(t-1)^b + bt^a(t-1)^{b-1}.$$

Then f' is clearly split over $\mathbb{F}_2$ unless a and b are both odd, in which case

$$f' = t^{a-1}(t-1)^{b-1}(t-1+t) = t^{a-1}(t-1)^{b-1}$$

is split. In [**Kap95**, p. 30]*, Kaplansky mentions that he had tried without success to characterize split-Rolle fields. In* [**CC77**, §4] *Craven–Csordas show (as a byproduct of a more general problem concerning "multiplier sequences" for $f \in \mathbb{F}_q[t]$) that among finite fields the split-Rolle fields are precisely $\mathbb{F}_2$ and $\mathbb{F}_4$. The paper* [**Cr97**] *is exclusively devoted to split-Rolle fields. In particular Craven shows: in characteristic $p > 0$, a split-Rolle is perfect and is either isomorphic to $\mathbb{F}_2$ or $\mathbb{F}_4$ or contains $\overline{F_p}$. He also shows that the Puiseux series field over $\mathbb{F}_2$ is split-Rolle (and clearly not algebraically closed; indeed $\mathbb{F}_2$ is algebraically closed in it), that the real*

[1] An asterisk appears, indicating that Slater did not submit a solution to this problem.

Laurent series field $\mathbb{R}((t))$ is split-Rolle but the complex Laurent series field $\mathbb{C}((t))$ is not.

EXERCISE 15.2. *Let F be a real-closed field, and let $\mathfrak{p}$ be its unique ordering. Let $a < b$ be elements of F.*

a) *Prove the Polynomial Mean Value Theorem: if $f \in F[t]$, then there is $c \in (a, b)$ such that*

$$\frac{f(b) - f(a)}{b - a} = f'(c).$$

b) *Show: if $f'(c) > 0$ for all $c \in (a, b)$, then f is strictly increasing on $[a, b]$.*
c) *Show: if f has positive degree and $f'(c) \geq 0$ for all $c \in (a, b)$, then f is strictly increasing on $[a, b]$.*

PROPOSITION 15.4. *Let $(F, \mathfrak{p})$ be an ordered field, and let $f \in F[t]$ be an irreducible polynomial that changes sign. Then the field $L := F[t]/(f)$ admits an ordering extending $\mathfrak{p}$.*

PROOF. We go by induction on $n = \deg f$, the base case $n = 1$ being trivial. So suppose $n \geq 2$, that the result holds for all smaller degrees and – seeking a contradiction – that it fails for some irreducible f of degree n. By Theorem 14.12 then there are $a_i \geq 0$ and $f_i \in F[t]$, each of degree at most $n - 1$, such that

$$1 + \sum_i a_i f_i(t)^2 \equiv 0 \pmod{f}$$

and thus there is $0 \neq h \in K[t]$ with $\deg h \leq n - 2$ such that

$$1 + \sum_i a_i f_i(t)^2 = f(t)h(t).$$

Plugging in $t = a$ and $t = b$ we find $f(a)h(a) > 0$ and $f(b)h(b) > 0$ and thus $h(a)h(b) < 0$. There must then be at least one irreducible factor $g(t)$ of $h(t)$ such that $g(a)g(b) < 0$. Since

$$\deg g \leq \deg h \leq n - 2 < n = \deg f$$

and

$$1 + \sum_i a_i f_i(t)^2 \equiv 0 \pmod{g},$$

this contradicts our induction hypothesis. □

EXERCISE 15.3. *Use Proposition 15.4 to deduce new proofs of many (as many as possible!) of the results of § 16.3.*

THEOREM 15.5. *(Sylvester) Let $(F, \mathfrak{p})$ be an ordered field, and let $(R, \mathcal{P})$ be a real-closed extension. Let $f \in F[t]$ be a nonzero monic separable polynomial, and put $A := F[t]/(f)$. Let B_f be the **trace form** on the F-algebra A, i.e., the bilinear form $\langle x, y \rangle = \mathrm{Tr}_{A/K}(x, y)$. Let $C = R(\sqrt{-1})$. Then:*

a) *The number of roots of f in R is equal to the signature of B_f.*
b) *Half the number of roots of f in $C \setminus R$ is equal to the number of hyperbolic planes appearing in the Witt decomposition of B_f.*

PROOF. Let $f(t) = f_1(t) \cdots f_r(t)$ be the factorization of f over $R[t]$. Since f is separable, the polynomials f_i are distinct, and since $R(\sqrt{-1})$ is algebraically closed, each f_i has degree 1 or 2. Since $A \otimes_F R \cong R[t]/(f)$, the trace form of $A \otimes_F R$ is simply the scalar extension to R of the trace form B_f. Further, by the Chinese Remainder Theorem we have

$$R[t]/(f) \cong \prod_{i=1}^{r} R[t]/(f_i),$$

so

$$(B_f)_{/R} \cong \bigoplus_{i=1}^{r} B_{f_i}.$$

It is easy to see that if $\deg f_i = 1$ then the trace form is just $\langle 1 \rangle$, whereas if $\deg f_i = 2$ – so $R[t]/(f_i) \cong C$ – then Example 6.10 shows that the trace form is congruent to $\langle 2, -2 \rangle \cong \langle 1, -1 \rangle = \mathbb{H}$, the hyperbolic plane. Both parts of the theorem follow immediately. □

2. Real Closures

A **real closure** of the *ordered* field $(F, \mathfrak{p})$ is a field extension R/F that is algebraic, real-closed, and such that the unique ordering $\mathcal{P}$ on R extends the ordering $\mathfrak{p}$ on F: equialently, we have $\mathcal{P} \cap F = \mathfrak{p}$. In particular, R/F is a real-closure of the underlying formally real field F as previously defined.

It is not much more difficult to show that an ordered field has *at least one* real closure than was the case for formally real fields:

THEOREM 15.6. *Every ordered field $(F, \mathfrak{p})$ admits a real closure.*

PROOF. Let $K = F(\{\sqrt{x}\}_{x \in \mathfrak{p}})$. By Theorem 14.13, K is formally real, and by Proposition 14.20, there is a real-closed algebraic extension R of K. Let $\mathcal{P} = \{x^2 \mid x \in R\}$ be the positive cone of the unique ordering on R. Every $x \in \mathfrak{p}$ is a square in K and hence also in R: that is, $\mathfrak{p} \subseteq \mathcal{P} \cap F$. Conversely, if $x \in F \setminus \mathfrak{p}$, then $-x \in \mathfrak{p} \subseteq \mathcal{P}$, so $x \notin \mathcal{P}$, hence $x \notin \mathcal{P} \cap F$. Thus $\mathcal{P} \cap F = \mathfrak{p}$. □

Now we are ready for a key result:

THEOREM 15.7. *Let $(E, \mathcal{P})/(F, \mathfrak{p})$ be an algebraic extension of ordered fields. Let R be a real-closed field, and let $\sigma : F \to R$ be an ordered field embedding. Then there is a* unique *ordered field embedding $\rho : E \hookrightarrow R$ extending σ.*

PROOF. Step 1: Suppose first that $[E : F]$ is finite; as we are in characteristic 0, we may write $E = F(\alpha)$ for some $\alpha \in E$. Let $f \in F[t]$ be the minimal polynomial for α. By Theorem 15.6, the ordered field $(E, \mathcal{P})$ admits a real closure $\tilde{E}$. Since α is a root of f in $\tilde{E}$, by Theorem 15.5, also f has a root in S, which shows that there is an F-algebra embedding $E \hookrightarrow S$. We are not done: we need an embedding of *ordered* fields. So seeking a contradiction, let $\sigma_1, \ldots, \sigma_n$ be all the F-embeddings of E into S and suppose that none of them are order-preserving: thus, for all $1 \leq i \leq n$, there is $x_i \in \mathcal{P}$ such that $\sigma(x_i)$ is not a square in R. Now let

$$K \coloneqq E(\sqrt{x_1}, \ldots, \sqrt{x_n}).$$

Then K is a subfield of $\tilde{E}$, from which it inherits an ordering. By the same argument that we applied above to E, there is an F-algebra embedding $\sigma : K \hookrightarrow R$. The

restriction of σ to E must be σ_i for some i, but then on the one hand we have $\sigma(x_i) = \sigma(\sqrt{x_i})^2 > 0$, while on the other we have $\sigma(x_i) = \sigma_i(x_i) < 0$: contradiction.
Step 2: Returning to the case of E/F algebraic, consider the set of pairs (K, σ_K) with K a subextension of E/F and $\sigma_K : K \hookrightarrow R$ an ordered field embedding extending σ, with the evident partial ordering: $(K_1, \sigma_{K_1}) \leq (K_2, \sigma_{K_2})$ if $K_1 \subseteq K_2$ and $\sigma_{K_2}|_{K_1} = \sigma_{K_1}$. The union of a chain of such pairs is again such a pair, so by Zorn's Lemma we get a maximal such pair (K, σ_K). If $K \supsetneq E$, then applying Step 1 with K in place of F gives a larger such pair, so we must have $K = E$, showing the existence of the desired ordered field embedding $\rho : E \hookrightarrow R$.
Step 3: Let $\rho_1, \rho_2 : (E, \mathcal{P}) \to R$ be two order embeddings. After Step 2, we may extend each ρ_i to an order embedding on a real-closure $\tilde{E}$ of $(E, \mathcal{P})$. Let $\alpha \in E$, let $f \in F[t]$ be the minimal polynomial of α, and let $\alpha_1 < \ldots < \alpha_r$ be the roots of f in $\tilde{E}$. Since a homomorphism of real-closed fields is automatically order-preserving, for either $i = 1, 2$ we have that $\rho_i(\alpha_1) < \ldots < \rho_i(\alpha_r)$ are roots of f in R, but moreover, by Theorem 15.5, these are *all* the roots of f in R. Thus for all $1 \leq j \leq r$, both $\rho_1(\alpha_j)$ and $\rho_2(\alpha_j)$ are the jth smallest root of f in R, so $\rho_1(\alpha_j) = \rho_2(\alpha_j)$. Since $\alpha = \alpha_j$ for some j, we conclude $\rho_1(\alpha) = \rho_2(\alpha)$, so $\rho_1 = \rho_2$. □

COROLLARY 15.8. *Let $(F, \mathfrak{p})$ be an ordered field.*

a) *For $i = 1, 2$, let R_i be a real-closed field, and let $\sigma_i : F \hookrightarrow R_i$ be an ordered field embedding. There is a* unique *F-algebra embedding $\rho : R_1 \hookrightarrow R_2$ extending σ_2: i.e., such that $\sigma_2 = \rho \circ \sigma_1$.*
b) *(Uniqueness of Real Closures) Any two real-closures of the ordered field $(F, \mathfrak{p})$ are uniquely isomorphic as F-algebras.*

PROOF. a) If $\rho : R_1 \hookrightarrow R_2$ is an F-algebra embedding, then because R_1 and R_2 are real-closed, necessarily ρ is order-preserving, and thus ρ is an ordered field embedding extending σ_2. Now apply Theorem 15.7 with $E \coloneqq R_1$, $R \coloneqq R_2$ and $\sigma \coloneqq \sigma_2$: there is a unique ordered field embedding $\rho : R_1 \to R_2$ extending σ_2.
b) Suppose now that for $i = 1, 2$ the extension R_i/F is algebraic, hence a real closure of the ordered field $(F, \mathfrak{p})$. Then $R_2/\rho(R_1)$ is an algebraic extension of real-closed fields, so $R_2 = \rho(R_1)$. □

In light of this result, for any ordered field (F, ρ), we denote by F^{rc} the real closure of $(F, \mathfrak{p})$, which is unique up to *unique* F-algebra isomorphism. It follows immediately that $\mathrm{Aut}(F^{\mathrm{rc}}/F) = \{1\}$, so the real closure of any non-(real-closed) ordered field is not a Galois extension.

A field F is **rigid** if its automorphism group is trivial. Of course $\mathbb{Q}$ is rigid: any automorphism of $\mathbb{Q}$ fixes 1, hence fixes every postive integer, hence fixes every negative integer, hence fixes every fraction. Here is another very well-known example:

PROPOSITION 15.9. *The field $\mathbb{R}$ is rigid.*

PROOF. Because $\mathbb{R}$ is real-closed - or, more simply, because every positive element of $\mathbb{R}$ is a square, every field automorphism $f : \mathbb{R} \to \mathbb{R}$ must be a strictly increasing function. For an increasing function $f : \mathbb{R} \to \mathbb{R}$ and all $c \in \mathbb{R}$, the one-sided limits

$$L_{c,-} \coloneqq \lim_{x \to c^-} f(x) \text{ and } L_{c,+} \coloneqq \lim_{x \to c^+} f(x)$$

both exist: the former is the supremum of f on $(-\infty, c)$ and the latter is the infimum of f on (c, ∞). Then f is continuous at c if and only if $L_{c,-} = L_{c,+}$; otherwise we have $L_{c,-} < L_{c,+}$ and no value of $(L_{c,-}, L_{c,+})$ is attained by f. But for our field automorphism f, we have $f(\mathbb{R}) \subseteq f(\mathbb{Q}) = \mathbb{Q}$, which, being dense in $\mathbb{R}$, rules out the possibility of a discontinuity at c. Therefore f is continuous, and since $f(x) = x$ for all x in the dense subset $\mathbb{Q}$, we must have $f(x) = x$ for all $x \in \mathbb{R}$. □

Since $\mathbb{Q}$ has a unique ordering, the concepts of real closure of $\mathbb{Q}$ as formally real field and real closure of $\mathbb{Q}$ as an ordered field coincide, and thus the field $\mathcal{R}$ is the real-closure of $\mathbb{Q}$ as an ordered field. Because every automorphism of $\mathcal{R}$ pointwise fixes $\mathbb{Q}$, we conclude:

PROPOSITION 15.10. *The field $\mathcal{R}$ of real algebraic numbers is rigid.*

This may suggest that every real-closed field is rigid...but this is not the case. Suppose $(F, \mathfrak{p})$ is an ordered field and σ is an order-preserving automorphism of F. Let F^{rc} be the real closure of $(F, \mathfrak{p})$. Then $F \xrightarrow{\sigma} F \hookrightarrow F^{\mathrm{rc}}$ is an ordered field embedding; applying Theorem 15.7 to this embeddding and $E = F^{\mathrm{rc}}$, we find that there is a unique ordered field embedding $\rho : F^{\mathrm{rc}} \to F^{\mathrm{rc}}$ extending σ, and again because $F^{\mathrm{rc}}/\rho(F^{\mathrm{rc}})$ is an algebraic extension of real-closed fields, we find that ρ must be surjective. Conversely, if $\rho \in \operatorname{Aut} F^{\mathrm{rc}}$ has the property that $\rho(F) = F$, then the induced automorphism of F is order-preserving, because every automorphism of F^{rc} is order-preserving, and the order on F is inherited from that of F^{rc}. Thus we have proved:

PROPOSITION 15.11. *Let $(F, \mathfrak{p})$ be an ordered field, with real-closure F^{rc}. The subgroup of $\operatorname{Aut} F^{\mathrm{rc}}$ consisting of automorphisms that restrict to automorphisms of F is isomorphic under this restriction map to the group $\operatorname{Aut}(F, \mathfrak{p})$ of order-preserving automorphisms of F.*

There is the small matter that we haven't yet seen a nontrivial order-preserving automorphism of an ordered field yet. But the next exercise remedies this.

EXERCISE 15.4. *Let $F = \mathbb{R}(t)$ endowed with the unique ordering $\mathfrak{p}$ in which $t > \alpha$ for all $\alpha \in \mathbb{R}$. Recall from Theorem 10.3 that $\operatorname{Aut}(\mathbb{R}(t)/\mathbb{R}) = \mathrm{PGL}_2(\mathbb{R})$ acting as linear fraction transformations $t \mapsto \frac{at+b}{ct+d}$. Taking $a = d = 1$ and $c = 0$, we find that for all $b \in \mathbb{R}$ there is a unique automorphism σ_b of F that fixes $\mathbb{R}$ pointwise and carries t to $t+b$. Show: each σ_b is an order-preserving automorphism of $(F, \mathfrak{p})$.*

But moreover, if F^{rc} is a real-closure of an ordered field F, then an automorphism of F^{rc} need not restrict to an automorphism of F.

EXERCISE 15.5.

a) *Let $\mathfrak{p}$ be the unique ordering on the Laurent series field $\mathbb{R}((t))$ for which $0 < t < \alpha$ for all $\alpha \in \mathbb{R}$. Show: the real closure of $(\mathbb{R}((t)), \mathfrak{p})$ is the real Puiseux series field $P_{\mathbb{R}}$.*

b) *Show: there is a unique automorphism σ of $P_{\mathbb{R}}$ that maps each formal Laurent series in $t^{\frac{1}{n}}$ to the corresponding formal Laurent series in $t^{\frac{1}{2n}}$. Deduce: $\operatorname{Aut} P_{\mathbb{R}}$ is infinite.*

c) *Observe: $\sigma(\mathbb{R}((t)))$ is* not *contained in $\mathbb{R}((t))$.*
Also observe: $\sigma^{-1}(\mathbb{R}((t)) \subsetneq \mathbb{R}((t))$.

Coming back to our main story, we derive the following result:

COROLLARY 15.12. *Let F be a formally real field. Then there is a natural bijection between the set of F-isomorphism classes of real-closures of F and the set of orderings on F.*

PROOF. To a real-closed algebraic extension $\iota : F \hookrightarrow R$, we associate the ordering $\mathfrak{p}_\iota$ that F inherits from the (unique) ordering on R. Conversely, if $\mathfrak{p}$ is an ordering on F, we associate the (unique, up to unique F-algebra isomorphism) real-closure $F^{\mathrm{rc},\mathfrak{p}}$ of $(F,\mathfrak{p})$. It is now essentially immediate that these two mappings are mutually inverse, as we ask the reader to confirm. □

Let us return to the case of a formally real number field F. Then every ordering on F comes from an embedding of F into a real-closure. But every real-closure of F is also a real closure of $\mathbb{Q}$, which is unique up to (unique!) isomorphism: one version is the field $\mathcal{R} := \mathbb{R} \cap \overline{\mathbb{Q}}$. If $F = \mathbb{Q}(\alpha)$ and $f \in \mathbb{Q}[t]$ is a minimal polynomial of α, then the embeddings of F into $\mathcal{R}$ are in bijection with the roots of f in $\mathcal{R}$, which – because $\mathcal{R}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{R}$ – are precisely the roots of f in $\mathbb{R}$. Thus finally we get a result that was promised towards the beginning of this chapter:

THEOREM 15.13. *The set of orderings on a number field F is naturally in bijection with the set of field embeddings from F into $\mathbb{R}$.*

EXERCISE 15.6. *Let $F/\mathbb{Q}$ be a finite Galois extension. Show: if F is formally real, then it is totally real: every embedding $\sigma : F \hookrightarrow \mathbb{C}$ satisfies $\sigma(F) \subseteq \mathbb{R}$.*

EXERCISE 15.7. *Let F be a formally real field. Show that the group of roots of unity in F is $\{\pm 1\}$.*

EXERCISE 15.8. *Let $F/\mathbb{Q}$ be an algebraic field extension.*

a) *Show: the set of orderings of F is in bijection with the set of embeddings $\sigma : F \hookrightarrow \mathbb{R}$.*
b) *Let $\mathfrak{p}$ be an ordering on F. Show: there is no nontrivial automorphism of $(F,\mathfrak{p})$.*

We end this section by examining the following issue: as we saw, the real closure of $\mathbb{Q}$ is unique up to unique $\mathbb{Q}$-algebra isomorphism...but nevertheless there is a sense in which it is not unique. Namely, we took a particular copy $\mathcal{R}$ of this field, namely the intersection inside $\mathbb{C}$ of $\overline{\mathbb{Q}}$ and $\mathbb{R}$. Since real-closed fields are characterized algebraically as not being algebraically closed but becoming algebraically closed upon adjoinint $\sqrt{-1}$), then as mentioned earlier we of course have $\mathcal{R}(\sqrt{-1}) = \overline{\mathbb{Q}}$. But now we ask: if $\mathcal{R}$ the only subfield of $\overline{\mathbb{Q}}$ with this property?

After a little thought, the answer is *no*. Let $\alpha \in \mathcal{R}$ be an algebraic number that is real but not totally real: that is, its minimal polynomial $f \in \mathbb{Q}[t]$ has degree d, and the number r of roots in $\mathcal{R}$ (or any real-closed field) satisfies $1 \leq r < d$. Then α has a conjugate α' that does not lie in $\mathcal{R}$. As a particular example of this, we may take $\alpha = 2^{1/n}$ for any odd $n \in \mathbb{Z}^{\geq 3}$: then we have $d = n$ and $r = 1$, and we may take $\alpha' := \zeta_n 2^{1/n}$ for any nth root of unity $\zeta_n \neq 1$. Then $\mathbb{Q}(\alpha')$, being isomorphic to $\mathbb{Q}(\alpha)$, is formally real, so by the very definition of real-closed field, there must exist a real-closed subfield R of $\overline{\mathbb{Q}}$ containing α'. Then, although R must be uniquely isomorphic to $\mathcal{R}$, it cannot be equal to it. In fact, in our example with $\alpha = 2^{1/n}$ for odd $n \in \mathbb{Z}^{\geq 3}$, if we write the conjugates of α as $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ and for all $2 \leq i \leq n$ let R_i be a real-closed subfield of $\overline{\mathbb{Q}}$ containing α_i, then the

fields $\mathcal{R}, R_2, \ldots, R_n$ must all be distinct, because if any two coincided, then some real-closed field would contain two conjugates of $2^{1/n}$ and thus an odd nth root of unity other than 1, contradicting Exercise 15.7.

We can say more: let C be an algebraically closed field of characteristic 0. We say that a real-closed subfield R of C is **associated to C** if C/R is algebraic – then we must have $C = \mathbb{R}(\sqrt{-1})$, so there is a unique involution $\iota \in \operatorname{Aut} C$ – i.e., an order 2 element – such that $\mathbb{R} = \mathbb{C}^\iota := \mathbb{C}^{\{1,\iota\}}$. Conversely, by Theorem 14.18, if $\iota \in \operatorname{Aut} C$ has order 2, then C^ι is a real-closed field associated to C. Thus real-closed fields associated to C are in bijection with involutions in $\operatorname{Aut} C$.

We say a real-closed field R is **abstractly associated to C** if it is isomorphic to a subfield that is associated to C. Thus for instance we know that $\mathcal{R}$ is up to isomorphism the only real field that is abstractly associated to $\overline{\mathbb{Q}}$, but we just saw that there are infinitely many real-closed subfields of R that are associated to $\overline{\mathbb{Q}}$.

EXERCISE 15.9. *Let C be an algebraically closed field of characteristic 0, and let R be a real-closed field.*

a) *Show: R is abstractly associated to C if and only if* $\operatorname{trdeg}(C/\mathbb{Q}) = \operatorname{trdeg}(R/\mathbb{Q})$.
b) *Suppose that C is uncountably infinite. Show: R is abstractly associated to C if and only if $\#R = \#C$.*

Let C be an algebraically closed field of characteristic 0, and let $\kappa := \operatorname{trdeg}(C/\mathbb{Q})$. Let F be a rational function field over $\mathbb{Q}$ in a set of κ indeterminates. By Theorem 14.15, the field F is formally real, so admits a real-closure R. Since R/F is algebraic, we have $\operatorname{trdeg}(R/\mathbb{Q}) = \kappa = \operatorname{trdeg}(C/\mathbb{Q})$, so by Exercise 15.9 the field R is abstractly associated to C. By our above discussion, this means that $\operatorname{Aut} C$ has at least one involution.

EXERCISE 15.10. *Let C be an algebraically closed field of characteristic 0, and let R_1 and R_2 be two real-closed subfields associated to C, with corresponding involutions ι_1 and ι_2 in* $\operatorname{Aut}\mathbb{C}$. *Show: the following are equivalent:*

(i) *The fields R_1 and R_2 are conjugate under the action of* $\operatorname{Aut}\mathbb{C}$*: there is $\sigma \in \operatorname{Aut} C$ such that $\sigma(R_1) = R_2$.*
(ii) *The involutions ι_1 and ι_2 are conjugate in* $\operatorname{Aut}\mathbb{C}$.
(iii) *The fields R_1 and R_2 are isomorphic.*

We deduce: the set of conjugacy classes of involutions in $\operatorname{Aut} C$ is naturally in bijection with the set of isomorphism classes of real-closed fields R with $\operatorname{trdeg}(R/\mathbb{Q}) = \operatorname{trdeg}(C/\mathbb{Q})$. In particular, the involutions in $\operatorname{Aut}\overline{\mathbb{Q}}$ form a single conjugacy class.

EXERCISE 15.11. *Let R be a real-closed field, put $C := \mathbb{R}(\sqrt{-1})$, and let $\iota \in \operatorname{Aut}\mathbb{C}$ be the involution such that $R = C^\iota$. Show: the following are equivalent:*

(i) *The field R is rigid:* $\operatorname{Aut} R = \{1\}$.
(ii) *The normalizer of* $\{1, \iota\}$ *in* $\operatorname{Aut} C$ *is* $\{1, \iota\}$.

THEOREM 15.14. *Let $\mathcal{I}$ be the set of involutions in* $\operatorname{Aut}\overline{\mathbb{Q}}$.

a) *The set $\mathcal{I}$ is a conjugacy class in* $\operatorname{Aut}\overline{\mathbb{Q}}$.
b) *We have $\#\mathcal{I} = \mathfrak{c} = 2^{\aleph_0}$.*

PROOF. a) From Exercise 15.10, we know that conjugacy classes of involutions of $\operatorname{Aut}\overline{\mathbb{Q}}$ are in bijective correspondence with isomorphism classes of real-closed

fields R with $\mathrm{trdeg}(R/\mathbb{Q}) = \mathrm{trdeg}(\overline{Q}/Q) = 0$. But any real-closed field of absolute transcendence degree 0 is a real-closure of $\mathbb{Q}$, which as above is unique because $\mathbb{Q}$ has a unique ordering. Thus every real-closed subfield associated to $\overline{\mathbb{Q}}$ is isomorphic to the field $\mathcal{R}$ of real algebraic numbers, so any two involutions in $\mathrm{Aut}\,\overline{\mathbb{Q}}$ are conjugate. b) Let ι be the involution of $\overline{\mathbb{Q}}$ whose fixed field is the field $\mathcal{R}$ of real algebraic numbers. We know that $\mathcal{R}$ is rigid, so by Exercise 15.11 we have that the normalizer of $\{1, \iota\}$ in $\mathrm{Aut}\,\overline{\mathbb{Q}}$ is $\{1, \iota\}$. Since by part a), the conjugation action of $\mathrm{Aut}\,\overline{\mathbb{Q}}$ on $\mathcal{I}$ is transitive, the Orbit-Stabilizer Theorem gives a bijection from the coset space $(\mathrm{Aut}\,\overline{\mathbb{Q}})/\{1, \iota\}$ to $\mathcal{I}$. It follows from Theorem 10.13 that $\#(\mathrm{Aut}\,\overline{\mathbb{Q}})/\{1, \iota\} = \mathfrak{c}$. □

If C is an algebraically closed field that is transcendental over $\mathbb{Q}$, let $\mathcal{I}_C$ be the set of involutions in $\mathrm{Aut}\,C$. The structure of the set $\mathcal{I}_C$ is a bit different than in the algebraic case considered in Theorem 15.14.

Exercise 15.12.

a) *Let C_2/C_1 be an extension of algebraically closed fields of characteristic 0. Let $\iota_1 \in \mathrm{Aut}\,C_1$ be an involution. Show: ι_1 extends to at least one involution $\iota_2 \in \mathrm{Aut}\,C_2$.*

b) *Let C be an algebraically closed field of characteristic 0 and let $\mathcal{I}_C$ be the set of involutions in $\mathrm{Aut}\,C$. Show:*

$$\#\mathcal{I}_C \geq \mathfrak{c}.$$

However, the result of Exercise 15.12b) is just a first salvo. For instance, consider the complex field $\mathbb{C}$. Because the real field $\mathbb{R}$ is a rigid real-closed field associated to $\mathbb{C}$, the proof of Theorem 15.14b) works to show that the set of index 2 subfields of $\mathbb{C}$ isomorphic to $\mathbb{R}$ is naturally in bijection with $(\mathrm{Aut}\,\mathbb{C})/\{1, c\}$ (here c denotes complex conjugation), hence by Theorem 10.13 has cardinality $2^{\#\mathbb{C}} = 2^{\mathfrak{c}} = 2^{2^{\aleph_0}}$. This makes us suspect that in general we should have $\#\mathcal{I}_C = 2^{\#C}$. But also this example shows that it is no longer the case that every involution of $\mathrm{Aut}\,\mathbb{C}$ is conjugate to c: equivalently, not every real-closed field of continuum cardinality is isomorphic to $\mathbb{R}$. Indeed:

Exercise 15.13. *Let $\kappa \geq 1$ be a cardinal.*

a) *Show: there is a non-Archimedean real-closed field R with $\mathrm{trdeg}(R/\mathbb{Q}) = \kappa$.*

b) *(Baer [**Ba70**]) Let $C/\mathbb{Q}$ be an algebraically closed field with $\mathrm{trdeg}(C/\mathbb{Q}) = \kappa$. Show: the set $\mathcal{I}_C$ of involutions in $\mathrm{Aut}\,C$ is nonempty.*

So among real-closed fields of continuum cardinality, there is at least one Archimedean one and at least one non-Archimedean one, so $\mathrm{Aut}\,\mathbb{C}$ has at least two conjugacy classes of involutions.

Let $C/\mathbb{Q}$ be an algebraically closed field. Again we denote by $\mathcal{I}_C$ the set of involutions in $\mathrm{Aut}\,C$; moreover, let us put $\mathcal{C}(\mathcal{I}_C)$ be the set of conjugacy classes of these involutions. The study of $\mathcal{C}(\mathcal{I}_C)$ is a surprisingly recent piece of field theory. It seems to be initiated by a work of Baer [**Ba70**], who as above showed that $\mathcal{I}_C$ is always nonempty. Dieudonné [**Di74**] showed

$$\#\mathcal{C}(\mathcal{I}_C) \geq \min(\mathrm{trdeg}(C/\mathbb{Q}) + 1, \aleph_0),$$

and Schnor [**Sc92**] showed that whenever $\mathrm{trdeg}(C/\mathbb{Q}) \geq 1$ we have

$$\#\mathcal{C}(\mathcal{I}_C) \geq \aleph_0.$$

This is still not the sharp result, which we will state and prove later on.

3. Artin–Lang and Hilbert

LEMMA 15.15. *Let K be real-closed, and let $h_1, \ldots, h_n \in K[t]^\bullet$. Let P be an ordering on $K(t)$. Then there are infinitely many $a \in K$ such that*

$$\forall 1 \leq i \leq n,\ \operatorname{sgn}(h_i) = \operatorname{sgn}(h_i(a)).$$

PROOF. Let $h \in K[t]^\bullet$. Then we may write

$$h = u(t - c_1) \cdots (t - c_r) q_1(t) \cdots q_s(t)$$

with $u, c_1, \ldots, c_r \in K^\times$ and $q_j(t)$ a monic irreducible quadratic for all $1 \leq j \leq s$. For any j,

$$q_j(t) = q(t) = t^2 + bt + c = (t + \frac{b}{2})^2 + (c - \frac{b^2}{4}),$$

and since q_j is irreducible over the real-closed field K, $c - \frac{b^2}{4} > 0$. It follows that $q > 0$ and that for all $a \in K$, $q(a) > 0$. Thus

$$\operatorname{sgn} h = \operatorname{sgn} u \prod_{i=1}^{r} \operatorname{sgn}(t - c_i),$$

$$\forall a \in K,\ \operatorname{sgn} h(a) = \operatorname{sgn} u \prod_{i=1}^{r} \operatorname{sgn}(a - c_i).$$

We may thus assume that each h_i is monic and $\prod_{i=1}^n h_i$ has distinct roots in K. Let c be the smallest root which is strictly greater than t, or ∞ if there is no such root. Then for all $a \in (t, c)$, $\operatorname{sgn} h_i(a) = \operatorname{sgn} h_i(t)$ for all i: this is an infinite set. □

THEOREM 15.16 (Artin–Lang Homomorphism Theorem). *Let R be a real-closed field, and let $E = R(x_1, \ldots, x_m)$ be a finitely generated field extension. If E is formally real, then there is an R-algebra map $R[x_1, \ldots, x_m] \to R$.*

PROOF. Let d be the transcendence degree of E/R. The case $d = 0$ is trivial: then $E = R[x_1, \ldots, x_m] = R$.
Step 1: We reduce to the $d = 1$ case. Indeed, let E' be a subextension of E/R of transcendence degree 1. Let $\mathcal{R}$ be a real-closure of E, and let $\mathcal{R}'$ be the algebraic closure of E' in $\mathcal{R}$, so by Corollary 14.21, the field $\mathcal{R}'$ is real-closed. Assuming the result in transcendence degree 1, there is a homomorphism of $\mathcal{R}'$-algebras

$$\varphi : \mathcal{R}'[x_1, \ldots, x_m] \to \mathcal{R}'.$$

Then

$$\operatorname{trdeg}(K(\varphi(x_1), \ldots, \varphi(x_m))/K) \leq \operatorname{trdeg}(\mathcal{R}'/K) = \operatorname{trdeg}(E'/K) = \operatorname{trdeg}(E/K) - 1,$$

so by induction on d we may assume there is a K-algebra map $K[\varphi(x_1), \ldots, \varphi(x_m)] \to K$. Composing with the restriction of φ to $K[x_1, \ldots, x_m]$ we get a K-map to K.
Step 2: Suppose $E = K(x, y_1, \ldots, y_r)$, with x transcendental over K and $y_1, \ldots, y_r$ algebraic over K. We want a K-algebra map $K[x, y_1, \ldots, y_r] \to K$. By the Primitive Element Corollary, there is $y \in E$ such that $E = K(x)[y]$; further, we may take y to be integral over $K[x]$. Then:

$$\exists g_1, \ldots, g_r \in K[x, y],\ h \in K[x]^\bullet \text{ such that } \forall 1 \leq i \leq r,\ y_i = \frac{g_i(x, y)}{h(x)}.$$

If $\varphi : K[x,y] \to K$ is such that $\varphi(h) \neq 0$, then φ induces a K-algebra map $K[x, y_1, \ldots, y_r] \to K$. Thus it is enough to show: there are infinitely many K-algebra maps $\varphi : K[x,y] \to K$. Indeed, if $0 = \varphi(h) = h(\varphi(x))$, then φ maps x to one of the finitely many roots of h in K; since y is algebraic over $K(x)$, having fixed $\varphi(x)$ there are only finitely many choices for $\varphi(y)$.
Step 3: Let

$$f = (x, Y) = Y^n + c_{n-1}(x)Y^{n-1} + \ldots + c_0(x)$$

be the minimal polynomial for y over $K(x)$. Since y is integral over $K[x]$, we have $c_i(x) \in K[x]$ for all i. For $a \in K$, put $f_a(Y) = f(a, Y) \in K[Y]$. We look for roots of f_a in K. For if $b \in K$ is such that $f_a(b) = f(a,b) = 0$, there is a unique K-algebra map $\varphi : K[x,y] \to K$ with $\varphi(x) = a$, $\varphi(y) = b$. So it is enough to show: there are infinitely many $a \in K$ such that there is $b \in K$ with $f_a(b) = 0$.
Step 4: Finally we use that E is formally real! Let P be an ordering on E and let R be a real-closure of (E, P). Then $f(x, Y) \in K[x][Y]$ has a root in R, namely $y \in E \subset R$. By Sylvester's Theorem, $\operatorname{sgn}(B_f)/K(x) > 0$. If we can show that there are infinitely many $a \in K$ such that $\operatorname{sgn}((B_f)_a)/K) > 0$, then applying Sylvester's Theorem again we will get infinitely many a such that $f_a(Y)$ has a root in K and be done. We may diagonalize the quadratic form corresponding to B_f as $\langle h_1(x), \ldots, h_n(x)\rangle$, say. Staying away from the finitely many a such that $h_i(a)$ is zero or undefined for some i, we have that $B_{f_a} \cong \langle h_1(a), \ldots, h_n(a)\rangle$. By Lemma 15.15 there are infinitely many a such that $\operatorname{sgn} B_{f_a} = \operatorname{sgn} B_f > 0$, and we're done. □

Actually Lang proved a stronger result, giving in particular a necessary and sufficient condition for E to be formally real. His result uses the language of arithmetic geometry, so far as I can see in an essential way, so this result will unfortunately not be accessible to all readers, but here it is:

THEOREM 15.17 (Lang [**La53**]). *Let $V_{/R}$ be a geometrically integral algebraic variety over a real-closed field R, with function field $E = R(V)$. Then E is formally real if and only if V has a* nonsingular *R-point.*

The Artin–Lang homomorphism theorem is powerful enough to yield a quick proof of the following result, which when one takes $K = R = \mathbb{R}$, was the 17th of Hilbert's Problems proposed to the worldwide mathematical community in 1900.

THEOREM 15.18 (Artin). *Let K be a formally real field admitting a unique ordering, and let R be a real closure of K. If $f \in K[t_1, \ldots, t_m]$ is such that*

$$f(a_1, \ldots, a_n) \geq 0 \ \forall (a_1, \ldots, a_n) \in R^n,$$

then f is a sum of squares in $K(t_1, \ldots, t_m)$.

PROOF. We argue by contraposition: suppose $f \in K[t_1, \ldots, t_m]$ is not a sum of squares in $K(t_1, \ldots, t_m)$. By Corollary 14.5, there is an ordering P on $E = K(t_1, \ldots, t_m)$ such that $f <_P 0$. Let $\mathcal{R}$ be a real closure of (E, P). Then $f < 0$ in $\mathcal{R}$, so there is $w \in \mathcal{R}$ with $w^2 = -f$. By Corollary 14.21, the algebraic closure R_0 of K in $\mathcal{R}$ is real-closed, hence is a real-closure of the *ordered* field K since K admits exactly one ordering. By uniqueness of real closures $R_0 = R$. The field $R(t_1, \ldots, t_m, w)$ is a subfield of the real-closed field $\mathcal{R}$, hence by Artin–Lang there is an R-algebra map

$$\varphi : R[t_1, \ldots, t_n, w, \frac{1}{w}] \to R.$$

Note that the effect of including $\frac{1}{w}$ is that $\varphi(w)\varphi(\frac{1}{w}) = 1$, hence $\varphi(w) \neq 0$. For $1 \leq i \leq n$, put $a_i = \varphi(t_i)$; then $(a_1, \ldots, a_n) \in R^n$ and

$$f(a_1, \ldots, a_n) = \varphi(f) = -\varphi(w)^2 < 0.$$

□

EXERCISE 15.14. *Let (K, P) be an ordered field with real-closure R. Suppose $f \in K[t_1, \ldots, t_n]$ has the property that $f(a) \geq 0$ for all $a \in R^n$. Show that there is a positive definite quadratic form $q_{/K}$ such that q represents f over $K(t_1, \ldots, t_n)$: there are $x_1, \ldots, x_n \in K(t_1, \ldots, t_n)$ such that $q(x_1, \ldots, x_n) = f$.*

4. Archimedean and Complete Fields

As usual, a subset S of an ordered field F is called **bounded above** if there exists a single element $x \in F$ such that $s \leq x$ for all $s \in S$; **bounded below** is defined similarly.

Recall that for an ordered commutative group G we define the relation $\prec$ by $x \prec y$ if there is $n \in \mathbb{Z}^+$ such that $|x| \leq n|y|$, and we say that $x \approx y$ if $x \prec y$ and $y \prec x$. This is an equivalence relation; the equivalence classes are called the **Archimedean equivalence classes**; the identity element 0 is the only element in its Archimedean equivalence class; we let $\Omega(G)$ be the set of nonzero Archimedean equivalence classes; and we say that G is Archimedean if $\#\Omega(G) \leq 1$.

We call an ordered field **non-Archimedean** if it is not Archimedean.

EXERCISE 15.15. *Let F be an ordered field, and let $a, b, c, d \in F^\times$.*

a) *Show: if $a \prec b$ and $c \prec d$, then $ac \prec bd$.*
b) *Show: if $a \approx b$ and $c \approx d$, then $ac \approx bd$.*
c) *Show that the following are equivalent:*
   (i) *We have $x \prec y$.*
   (ii) *We have $\frac{x}{y} \prec 1$.*
   (iii) *We have $\frac{1}{y} \prec \frac{1}{x}$.*
d) *Show: $x \approx y$ if and only if $\frac{1}{x} \approx \frac{1}{y}$.*

PROPOSITION 15.19. *An ordered field F is Archimedean if and only if its subset $\mathbb{Q}$ is unbounded above.*

PROOF. An ordered field is Archimedean if and only if for every $x \in F^\times$ we have $x \approx 1$, which means that there is $n \in \mathbb{Z}^+$ such that $|x| \leq n$. So:
Suppose that F is *not* Archimedean. Then there is $x \in F^\times$ such that $|x| > n$ for all $n \in \mathbb{Z}^+$. Then $|x|$ is an upper bound for $\mathbb{Q}$.
Now suppose that there is $x \in F$ that is an upper bound for $\mathbb{Q}$, so for all $n \in \mathbb{Z}^+$ we have $x \geq n$. Thus for all $n \in \mathbb{Z}^+$ we have $x \geq n + 1 > n > 0$, so we have $x \not\prec 1$ and F is non-Archimedean. □

EXAMPLE 15.20. *If x is any rational number, then $x + 1$ is a larger rational number. Thus the field $\mathbb{Q}$ is Archimedean.*

EXERCISE 15.16. *Show that any subfield of an Archimedean ordered field is Archimedean, but a subfield of a non-Archimedean ordered field may be Archimedean.*

An element x of an ordered field is **infinitely large** if $x > n$ for all $n \in \mathbb{Z}^+$ and **infinitesimal** if $0 \leq |x| < \frac{1}{n}$ for all $n \in \mathbb{Z}^+$. Thus a nonzero element x is infinitely large if and only if $\frac{1}{x}$ is infinitesimal. It follows from Exercise 15.15 that an ordered field is non-Archimedean if and only infinitely large elements exist if and only if nonzero infinitesimal elements exist.

EXERCISE 15.17. *Suppose x is an infinitely large element of an ordered field. Show that for all $y \in \mathbb{Q}$, $x - y$ is infinitely large.*

EXERCISE 15.18. *Let K be an ordered field; consider the field $K(t)$.*

a) *Proposition 14.15 shows that $K(t)$ admits at least one non-Archimedean ordering. Show that in fact $K(t)$ admits at least four non-Archimedean orderings. Can you improve upon 4?*

b) *Show: for every infinite cardinal κ, there exists a non-Archimedean ordered field of cardinality κ.*

A partially ordered *set* $(S, \leq)$ is **Dedekind complete** if every nonempty subset which is bounded above has a least upper bound.

EXERCISE 15.19. *Show that a partially ordered set is Dedekind complete if and only if every subset that is bounded below has a greatest lower bound.*

PROPOSITION 15.21. *Let F be a Dedekind complete ordered field. Then the ordering is Archimedean.*

PROOF. We go by contraposition: if F is non-Archimedean, then the subset $\mathbb{Z}^+$ is bounded above, and the set of upper bounds is precisely the set of infinitely large elements. However, Exercise 15.17 shows in particular that the set of infinitely large elements has no least element: if x is infinitely large, so is $x - 1$. □

Famously, $\mathbb{R}$ satisfies the least upper bound axiom, i.e., its ordering is Dedekind complete. So by Proposition 15.21 the ordering on $\mathbb{R}$ is Archimedean. This is not news to us: in §14.1 we used that $(\mathbb{R}, +)$ is an Archimedean ordered commutative group. But from a foundational perspective, we now see that this is a consequence of Dedekind completeness. It follows of course that every subfield of $\mathbb{R}$ is Archimedean.

The order topology: let $(S, \leq)$ be any linearly ordered space. Recall that we can use the ordering to endow S with a topology, the **order topology**, in which a base of open sets consists of all open intervals.[2] Order topologies have several pleasant properties: for instance, any order topology is a hereditarily normal space (i.e., every subspace is normal: for us, this includes Hausdorff).

PROPOSITION 15.22. *Let K be an ordered field. Then the order topology endows K with the structure of a topological field. That is, the addition and multiplication operations are continuous as functions from $K \times K$ to K.*

EXERCISE 15.20. *Prove Proposition 15.22. (Suggestion: use the characterization of continuous functions as those which preserve limits of nets.)*

PROPOSITION 15.23. *For any Archimedean ordered field F, $\mathbb{Q}$ is dense in the order topology on F.*

[2]If there is a bottom element $\mathfrak{b}$ of S, then the intervals $[\mathfrak{b}, b)$ are deemed open. If there is a top element $\mathfrak{t}$ of S, then the intervals $(a, \mathfrak{t}]$ are deemed open. Of course, no ordering on a field has either top or bottom elements, so this is not a relevant concern at present.

PROOF. It is sufficient to show that for $a, b \in F$ with $0 < a < b$, there exists $x \in \mathbb{Q}$ with $a < x < b$. Because of the nonexistence of infinitesimals, there exist $x_1, x_2 \in \mathbb{Q}$ with $0 < x_1 < a$ and $0 < x_2 < b - a$. Thus $0 < x_1 + x_2 < b$. Therefore the set $S = \{n \in \mathbb{Z}^+ \mid x_1 + nx_2 < b\}$ is nonempty. By the Archimedean property S is finite, so let N be the largest element of S. Thus $x_1 + Nx_2 < b$. Moreover we must have $a < x_1 + Nx_2$, for if $x_1 + Nx_2 \leq a$, then $x_1 + (N+1)x_2 = (x_1 + Nx_2) + x_2 < a + (b - a) = b$, contradicting the definition of N. □

EXERCISE 15.21. *Deduce from Proposition 15.23 that the order topology on any Archimedean ordered field is second countable. (Hint: show in particular that open intervals with rational endpoints form a base for the topology.) From the normality of all order topologies cited above and Urysohn's Metrization Theorem, it follows that the order topology on an Archimedean ordered field is metrizable.*[3]

The order topology on K endows $(K, +)$ with the structure of a commutative topological group. In such a situation we can define Cauchy nets, as follows: a net $x_\bullet : I \to G$ in a commutative topological group G is **Cauchy** if for each neighborhood U of the identity $0 \in G$ there exists $i \in I$ such that for all $j, k \geq i$, $x_j - x_k \in U$. A topological group is **complete** if every Cauchy net converges.

Let F be an ordered field. We define the absolute value function from F to $F^{\geq 0}$, of course taking $|x|$ to be x if $x \geq 0$ and $-x$ otherwise.

EXERCISE 15.22. *Let F be an ordered field. Show that the triangle inequality holds: for all $x, y \in F$, $|x + y| \leq |x| + |y|$.*

Thus for any ordered field F, one can define the function $\rho : F \times F \to F^{\geq 0}$ by $\rho(x, y) = |x - y|$ and this has all the formal properties of a metric except that it is F-valued. In particular, for any net $x_\bullet$ in F we have $x_\bullet \to x$ if and only if $|x_\bullet - x| \to 0$. In general it can be of some use to consider "F-valued metrics" where F is a non-Archimedean ordered field. But here is the key point: if the ordering on F is Archimedean, then the convergence can be expressed by inequalities involving rational numbers (rather than the infinitesimal elements that would be required in the non-Archimedean case): namely, for an Archimedean ordered field F, a net $x_\bullet : I \to F$ converges to $x \in F$ if and only if for all $n \in \mathbb{Z}^+$, there exists $i_n \in I$ such that $j \geq i \implies |x_j - x| < \frac{1}{n}$. Topologically speaking, we are exploiting the fact that the topology of an Archimedean ordered field has a countable neighborhood base at each point. Thus it is sufficient to replace nets by sequences. In particular we have the following simple but important result.

LEMMA 15.24. *Let K be an Archimedean ordered field. Then the following are equivalent:*

(i) *Every Cauchy net in K is convergent.*
(ii) *Every Cauchy sequence in K is convegent.*

PROOF. Of course (i) $\implies$ (ii). Now suppose that every Cauchy sequence in K converges, and let $x_\bullet : I \to K$ be a Cauchy net. We may assume that I has no maximal element, for otherwise the net is certainly convergent. Choose $i_1 \in I$ such that $j, k \geq i_1$ implies $|x_j - x_k| < 1$. Now pick $i_2 \in I$ such that $i_2 > I_1$ and $j, k \geq i_2$

[3]However, we are not going to use this fact in our discussion. Rather, as will become clear, an ordered field K comes with a canonical "K-valued metric", which will be just as useful to us as an "$\mathbb{R}$-valued metric" – a special case!

implies $|x_j - x_k| < \frac{1}{2}$. Continuing in this manner we get an increasing sequence $\{i_n\}$ in I such that for all n, if $j, j \geq i_n$, $|x_j - x_k| < \frac{1}{n}$. Thus from the net we have extracted a Cauchy subsequence, which by hypothesis converges, say to x. From this it follows immediately that the net $x_\bullet$ converges to x. □

Remark: The proof here is based on [**Wi**, Thm. 39.4], which asserts that the uniform structure associated to a complete metric is a complete uniform structure if and only if the metric is a complete metric.

THEOREM 15.25.
For an Archimedean ordered field K, the following are equivalent:

(i) *K is Dedekind complete ordered set: every nonempty subset that is bounded above has a supremum.*

(ii) *$(K, +)$ is a Cauchy-complete topological group: every Cauchy net converges.*

PROOF. (i) $\implies$ (ii): Dedekind complete implies Archimedean implies second countable implies first countable implies it is enough to look at Cauchy sequences. The argument is then the usual one from elementary real analysis: suppose K is Dedekind complete, and let x_n be a Cauchy sequence in K. Then the sequence is bounded, so there exists a least upper bound x. We can construct a subsequence converging to x in the usual way: for all $k \in \mathbb{Z}^+$, let x_{n_k} be such that $|x_{n_k} - x| < \frac{1}{n}$. (That this implies that the subsequence converges is using the the Archimedean property that for all $x > 0$, there exists $n \in \mathbb{Z}^+$ with $\frac{1}{n} < x$.) Then, as usual, a Cauchy sequence with a convergent subsequence must itself be convergent.
(ii) $\implies$ (i): let $S \subset K$ be nonempty and bounded below. Let $\mathcal{B}$ be the set of all lower bounds of S, with the ordering induced from K. What we want to show is that $\mathcal{B}$ has a greatest element: we will prove this by Zorn's Lemma. Let $\mathcal{C}$ be a nonempty chain in $\mathcal{B}$. We may view this as a net $x : \mathcal{C} \to K$. We claim that it is Cauchy: i.e., for every open neighborhood U of 0, there exists an index i such that for all $j, k \geq i$, $x_i - x_j \in U$. Because the ordering is Archimedean, this is equivalent to $|x_i - x_j| < \epsilon$ for some positive rational number ϵ. But since $\mathcal{C}$ is a set of lower bounds for the nonempty set S, it is certainly bounded above, and if the desired conclusion were false there would exist infinitely many pairs of indices (i, j) with $j > i$ and $x_j - x_i \geq \epsilon$, and by the Archimedean nature of the ordering this would imply that $\mathcal{C}$ is unbounded above, contradiction! Therefore the net $x_\bullet$ is Cauchy and converges by assumption to $x \in K$. This element x is an upper bound for $\mathcal{C}$ and a lower bound for S. Thus by Zorn's Lemma $\mathcal{B}$ has a maximal element, i.e., S has a greatest lower bound. □

An Archimedean ordered field satisfying the equivalent conditions of Theorem 15.25 will simply be said to be **complete**.

PROPOSITION 15.26 (Strong Rigidity for Archimedean Ordered Fields). *Let $(F, \mathfrak{p})$ be an Archimedean ordered field, and let $f : F \to F$ be an order-preserving field homomorphism. Then $f = 1_F$ is the identity map.*

PROOF. Suppose not, and let $x \in F$ be such that $f(x) \neq x$.
Case 1: Suppose $x < f(x)$. By Proposition 15.23 there is $q \in \mathbb{Q}$ with $x < q < f(x)$. Applying f, we get $f(x) < f(q) = q$, a contradiction.
Case 2: Similarly, if $f(x) < x$, then there is $q \in \mathbb{Q}$ with $f(x) < q < x$, and applying f gives $q = f(q) < f(x)$, a contradiction. □

LEMMA 15.27. *Let R and S be topological rings and D a dense subring of R. Suppose that $f : R \to S$ is a continuous* set map *from R to S which upon restriction to D is a homomorphism of rings. Then f is itself a homomorphism of rings.*

EXERCISE 15.23. *Prove Lemma 15.27. (Hint: use the net-theoretic characterization of dense subspaces: for any $x \in R$, there exists a net $x_\bullet : I \to D$ which converges to x.)*

THEOREM 15.28 (Main Theorem on Archimedean Ordered Fields).
A complete Archimedean field R is a final object in the category of Archimedean ordered fields. That is:

(i) *For any Archimedean field K and Dedekind complete field R, there is a unique embedding of ordered fields $K \hookrightarrow R$.*
(ii) *Any two Dedekind complete fields are (uniquely!) isomorphic.*

PROOF. (i) The idea here is that we have copies of $\mathbb{Q}$ inside both K and L and that in an Archimedean ordered field an element is uniquely specified by all of its order relations with elements of $\mathbb{Q}$. Formally, we define a map $\varphi : K \to L$ as follows: we map x to $\sup\{q \in \mathbb{Q} \mid q < x\}$. As above, it is clear that φ is order-preserving. When restricted to the dense subring $\mathbb{Q}$ it is certainly a homomorphism, so in order to apply Lemma 15.27 we need only check that φ is continuous. But again, a base for the topology of any Archimedean field is given by open intervals (a, b) with $a, b \in \mathbb{Q}$. Evidently φ maps the interval (a, b) of K to the interval (a, b) of L, so it is therefore continuous: done.
(ii) Let R_1 and R_2 be complete Archimedean fields. By (i), there exist embeddings of ordered fields $\varphi : R_1 \to R_2$ and $\varpi : R_2 \to R_1$. Applying Proposition 15.26 to the endomorphisms $\varpi \circ \varphi$ and $\varpi \circ \varphi$, we get $\varpi \circ \varphi = 1_{R_1}$ and $\varphi \circ \varpi = 1_{R_2}$, thus ϖ and φ are mutually inverse isomorphisms: so $R_1 \cong R_2$ as ordered fields. Moreover the same argument applies to show that any two isomorphisms φ_1, φ_2 from R_1 to R_2 are inverses of the isomorphism ϖ, so $\varphi_1 = \varphi_2$: there is only one isomorphism from R_1 to R_2. □

We have already identified the real numbers $\mathbb{R}$ as a complete Archimedean field, so we know that the final object referred to in Theorem 15.28 indeed exists. Let us restate things in a more concrete fashion using $\mathbb{R}$.

COROLLARY 15.29. *For any Archimedean ordered field K, there is a unique embedding of ordered fields $K \hookrightarrow \mathbb{R}$. Thus we may identify the Archimedean ordered fields – up to unique isomorphism – as subfields of $\mathbb{R}$ with the inherited ordering.*

Thus distinct real-closed subfields of $\mathbb{R}$ are not isomorphic. Following J.D. Hamkins and B. Poonen, we use this to establish the claim made at the end of Section 7:

EXERCISE 15.24. *Let S be a transcendence basis for $\mathbb{R}/\mathbb{Q}$. For each $T \subseteq S$, let R_T be the algebraic closure of $\mathbb{Q}(T)$ in $\mathbb{R}$, so R_T is real-closed by Corollary 14.21.*

a) *Show: $\#S = \mathfrak{c} = \#\mathbb{R}$.*
b) *Show: for distinct subsets T_1 and T_2 of S, we have $R_{T_1} \neq R_{T_2}$.*
c) *Let $1 \leq \kappa \leq \aleph_0$ be a cardinal number. Show: the number of subsets $T \subseteq S$ of cardinality κ is $\mathfrak{c}$.*
d) *For κ as in part c), let C be an algebraically closed field of characteristic 0 with $\operatorname{trdeg}(C/\mathbb{Q}) = \kappa$, and thus $\#C = \aleph_0$. Show: the number of conjugacy classes of order 2 elements in $\operatorname{Aut} C$ is $\mathfrak{c}$.*

e) *Let $\aleph_0 < \kappa \leq \mathfrak{c}$ be a cardinal number. Show: the number of subsets $T \subseteq S$ of cardinality κ is at least 2^κ.*[4] *(Hint: $\kappa + \kappa = \kappa$.)*

f) *For κ as in part e), let C be an algebraically closed field of characteristic 0 with $\mathrm{trdeg}(C/\mathbb{Q}) = \kappa$, and thus also $\#C = \kappa$. Show: the number of conjugacy classes of order 2 elements in $\mathrm{Aut}\, C$ is 2^κ. In particular: the number of conjugacy classes of order 2 elements in $\mathrm{Aut}\, \mathbb{C}$ is $2^{\mathfrak{c}}$.*

Since every Archimedean ordered field can be embedded in $\mathbb{R}$, if C is an algebraically closed field of characteristic 0 of cardinality $\kappa > \mathfrak{c}$ (let me know if you ever meet one in real life), then every real-closed subfield associated to C is non-Archimedean. Although we will not show it here, still the number of isomorphism classes of such fields is 2^κ and thus the number of conjugacy classes of involutions in $\mathrm{Aut}\, C$ is 2^κ: see `https://mathoverflow.net/questions/12949`.

Ultimately, producing rigid Archimedean real-closed fields turned out to be easy – every Archimedean real-closed fields (and even every uniquely ordered Archimedean field) is rigid. What about rigid non-Archimedean real-closed fields? We have seen exactly one example – the field $P_{\mathbb{R}}$ of real Puiseux series – and $\mathrm{Aut}\, P_{\mathbb{R}}$ is finite by Exercise 15.5. It turns out that the existence of a rigid non-Archimedean real-closed field remained open until quite recently: in 2024, Marker–Steinhorn constructed a rigid non-Archimedean real-closed field R with $\mathrm{trdeg}(R/\mathbb{Q}) = 2$ and showed that no non-Archimedean real-closed field R with $\mathrm{trdeg}(R/\mathbb{Q}) = 1$ is rigid [**MS25**]. They remark that they expect that their method extends to construct examples of any asbsolute transcendence degree $2 \leq d < \aleph_0$, but they do not know whether there are rigid non-Archimedean real-closed fields of infinite transcendence degree.

By the way, how do we know that this field "of real numbers" we've heard so much about actually exists? We've proven some fairly remarkable facts about it: maybe rumors of its existence are greatly exaggerated!

Of course we are being facetious. A rigorous construction of $\mathbb{R}$ was first given by R. Dedekind in the late 19th century. Accounts of his method (using what are now called) "Dedekind cuts" may be found in many texts. However, our Cauchy-theoretic perspective also gives an easy answer to this question. Namely, one has the notion of **Cauchy completion** of any commutative topological group G: namely, given G there exists a complete topological group $\hat{G}$ and a homomorphism of topological groups $G \to \hat{G}$ which is *universal* for homomorphisms from G into a complete topological group (If G is Hausdorff the map to the completion is an embedding.) The construction can be given in terms of an equivalence relation on the class of Cauchy nets on G, for instance. Moreover, when G is the additive group of an ordered field F, it is not hard to show that $\hat{F}$ is also an ordered field. Note well that we can therefore construct many **Cauchy complete** non-Archimedean ordered fields. However what we want is a Dedekind complete ordered field, and for this, according to Theorem 15.25 it is sufficient – and clearly also necessary – to complete an *Archimedean* ordered field, like $\mathbb{Q}$.

If one just wants to construct $\mathbb{R}$, all this is overkill: by Lemma 15.24, we can get away with Cauchy sequences rather than Cauchy nets. Thus we may construct

[4]Actually the number of such subsets is exactly 2^κ, as can be deduced from part f) of the exercise or of course shown more directly: see e.g. `https://math.stackexchange.com/questions/191006`. But this inequality is all we need.

$\mathbb{R}$ from $\mathbb{Q}$ in the following appealingly algebraic way: as the quotient $\mathcal{R}$ of the ring $\mathcal{C}(\mathbb{Q})$ of all Cauchy sequences in $\mathbb{Q}$ by the maximal ideal $\mathfrak{c}_0$ of sequences converging to 0. Therefore the quotient is a Cauchy complete field, say $\mathcal{R}$. The ordering on $\mathcal{Q}$ extends to $\mathcal{R}$ and that $\mathcal{Q}$ is dense in $\mathcal{R}$ in the order topology, which implies that the ordering on $\mathcal{R}$ is Archimedean. Thus $\mathcal{R}$ is a Cauchy complete, Archimedean ordered field, so it is Dedekind complete.

5. The Real Spectrum

For a field F, the **real spectrum of F** is the set $X(F)$ of orderings on F endowed with the topology given by the **Harrison subbase**

$$\{H(a) \coloneqq \{P \in X(F) \mid a \in P\}\}_{a \in F^\times}.$$

In more words, for $a \in F$, $H(a)$ is the set of orderings on F with respect to which a is positive. Thus the open sets for $X(F)$ are unions of the Harrison base $\bigcap_{i=1}^n H(a_i)$ for $a_1, \ldots, a_n \in F$. Because

$$H(-a) = X(F) \setminus H(a),$$

the elements of the Harrison base are all clopen.

PROPOSITION 15.30. *The real spectrum $X(F)$ of a field F is a **Boolean topological space**: it is compact, Hausdorff and totally disconnected.*

PROOF. If P_1, P_2 are distinct elements of $X(F)$, then there is $a \in F^\times$ such that $a \in P_1$ and $-a \in P_2$, and thus $P_1 \in H(a)$, $P_2 \in H(-a) = X(F) \setminus H(a)$, so $X(F)$ is Hausdorff and totally disconnected.

There is a natural injection $\iota : X(F) \hookrightarrow \{\pm 1\}^{F^\times}$: namely, to an ordering P of F, we assign the function $x \in F^\times \mapsto \mathrm{sgn}_P(x)$, i.e., $+1$ if $x \in P$ and -1 if $x \notin P$. The group $\{\pm 1\}^{F^\times}$ has a natural profinite structure and thus is itself a Boolean topological space. A base for the topology on $\{\pm 1\}^{F^\times}$ is obtained as follows: for each finite subset $S = \{x_1, \ldots, x_n\}$ of $F^\times$, choose for all $1 \le i \le n$ an element $\epsilon_i \in \{\pm 1\}$ and taking U_S to be the subset of $\{\pm 1\}^{F^\times}$ such that for all $1 \le i \le n$ the x_i-coordinate is ϵ_i. Then $\iota^{-1}(U_S) = \bigcap_{i=1}^n H(\epsilon_i x_i)$, so this base for the topology on $\{\pm 1\}^{F^\times}$ induces the Harrison base on $X(F)$, viewed as a subset of $\{\pm 1\}^{F^\times}$ via ι. Thus ι is a topological embedding.

Now let $\epsilon = (\epsilon_x)_{x \in F^\times}$ be an element of $\{\pm 1\}^{F^\times} \setminus \iota(X(F))$, meaning there is no ordering on F such that $x \in P$ if and only if $\epsilon_x = 1$, and let

$$P(\epsilon) \coloneqq \{x \in F^\times \mid \epsilon_x = 1\}.$$

For $x \in F^\times$, let $\pi_x : \{\pm 1\}^{F^\times} \to \{\pm 1\}$ be projection onto the x-coordinate. If $-1 \in P(\epsilon)$, then $\pi_1^{-1}(-1)$ is an open neighborhood of ϵ disjoint from $\iota(X(F))$. If for some $x \in F^\times$ we have $\epsilon_x = \epsilon_{-x}$, then $\{\epsilon_x\} \times \{\epsilon_{-x}\} \times \{\pm 1\}^{F^\times \setminus \{\pm x\}}$ is an open neighborhood of ϵ disjoint from $\iota(X(F))$. Otherwise, since $P(\epsilon)$ is not the cone of an ordering on F, there are $x, y \in P(\epsilon)$ such that one of $x + y$ and xy is not in $P(\epsilon)$; let z be $x + y$ if $x + y \notin P(\epsilon)$ or xy if $x + y \in P(\epsilon)$ and $xy \notin P(\epsilon)$. Then $\{\epsilon_x\} \times \{\epsilon_y\} \times \{\epsilon_z\} \times \{\pm 1\}^{F^\times \setminus \{x,y,z\}}$ is an open neighborhood of ϵ disjoint from $\iota(X(F))$. Thus $\iota(X)$ is closed in $\{\pm 1\}^{F^\times}$, so it is compact and hence so is the homeomorphic space X. □

EXERCISE 15.25. *Let K/F be a field embedding. Show: the natural restriction map $X(K) \to X(F)$ is continuous.*

In Chapter 7, we saw that a topological group is compact, Hausdorff and totally disconnected if and only if it is profinite: isomorphic to an inverse limit of finite discrete groups. A very similar result holds for topological spaces:

PROPOSITION 15.31. *For a topological space X, the following are equivalent:*

(i) *X is a **profinite space**: there is an inverse system $\{X_i\}_{i \in I}$ of finite discrete spaces with surjective transition maps such that X is homeomorphic to $\varprojlim X_i$.*

(ii) *X is a Boolean space: compact Hausdorff and totally disconnected.*

PROOF. (i) $\implies$ (ii): This is almost identical to the earlier result for topological groups: the inverse limit $\varprojlim X_i$ embeds as a closed subspace of $\prod_{i \in I} X_i$, which is compact (by Tychonoff's Theorem) Hausdorff and totally disconnected, hence also $\varprojlim X_i$ is compact, Hausdorff and totally disconnected.

(ii) $\implies$ (i): Let X be a totally disconnected compact Hausdorff space, which we may certainly assume is nonempty. A partition $\mathcal{P}$ of X determines and is determined by an equivalence relation on X, so via the natural map $q_{\mathcal{P}} : X \to \mathcal{P}$ we endow $\mathcal{P}$ with the quotient topology, in which a subset V is open if and only if $q_{\mathcal{P}}^{-1}(V)$ is open in X. This topology on $\mathcal{P}$ is discrete if and only if each element of $\mathcal{P}$ is an open subset of X. Let I be the set of **clopen partitions of X**, i.e., partitions of X in which each element is a clopen subset. As above, the quotient map $q_{\mathcal{P}} : X \to \mathcal{P}$ endows each clopen partition $\mathcal{P}$ with the discrete topology. Because a clopen partition is an open cover without any proper subcover and X is compact, each clopen partition on X is finite. For $\mathcal{P}_1, \mathcal{P}_2 \in I$, we put $\mathcal{P}_1 \preceq \mathcal{P}_2$ if $\mathcal{P}_2$ refines $\mathcal{P}_1$: that is, every element of $\mathcal{P}_2$ is contained in a (necessarily unique) element of $\mathcal{P}_1$, or equivalently the elements of $\mathcal{P}_1$ are unions of elements of $\mathcal{P}_2$. This is a partial ordering on I that makes it into a directed set: a common refinement of two clopen partitions $\mathcal{P}_1$ and $\mathcal{P}_2$ is obtained by taking all nonempty intersections of an element of $\mathcal{P}_1$ with an element of $\mathcal{P}_2$. Moreover, if $\mathcal{P}_1 \preceq \mathcal{P}_2$, we have a surjective transition map $r_{\mathcal{P}_2, \mathcal{P}_1}$ by mapping each element of $\mathcal{P}_2$ to the unique element of $\mathcal{P}_1$ that contains it as a subset. For $\mathcal{P}_1 \leq \mathcal{P}_2$ we have $q_{\mathcal{P}_1} = r_{\mathcal{P}_2, \mathcal{P}_1} \circ q_{\mathcal{P}_2}$, so by the universal property of the inverse limit we get a continuous map

$$\hat{q} : X \to \varprojlim_I \mathcal{P}_i.$$

By [**Cl-GT**, Thm. 6.53], a compact Hausdorff totally disconnected space admits a base of clopen sets, so if x_1 and x_2 are distinct points of X there is a clopen set U_1 containing x_1 but not x_2, and thus for the clopen partition $\mathcal{P} \coloneqq \{U_1, X \setminus U_1\}$ we have $q_{\mathcal{P}}(x_1) \neq q_{\mathcal{P}}(x_2)$. Thus $\hat{q}$ is injective. An element y of $\varprojlim_I \mathcal{P}_i$ is a choice of one element U_i from each clopen partition $\mathcal{P}_i$ with the compability condition that in the common refinement of a finite set $\mathcal{P}_1, \ldots, \mathcal{P}_n$ of clopen partitions, we must take $\bigcap_{i=1}^n U_i$, which must therefore be nonempty. Thus $\{U_i\}_{i \in I}$ is a family of closed sets in the compact space X satisfying the finite intersection condition, so there is $x \in \bigcap_{i \in I} U_i$ and then $\hat{q}(x) = y$, so $\hat{q}$ is surjective. Being a continuous bijection from a compact space to a Hausdorff space, $\hat{q}$ is a homeomorphism. □

REMARK 15.2. *Compact Hausdorff totally disconnected spaces are called Boolean spaces and also* Stone spaces *because of **Stone Duality*** [**Cl-CA**, Thm. 9.18]*, an anti-equivalence of categories from the category of Boolean rings (or, if you prefer Boolean algebras; those two categories are more plainly equivalent) to the category*

of Boolean spaces: to a Boolean ring R one associates $\operatorname{Spec} R$ *with the Zariski topology, and to a Boolean space X one associates the characteristic ring $\mathcal{C}(X)$ consisting of clopen subsets of X, made into a ring under symmetric difference for addition and intersection for multiplication. If R is finite, then* $\operatorname{Spec} R$ *is finite, and if X is finite, then $\mathcal{C}(X)$ is finite. Since every finitely generated Boolean ring is finite, every Boolean ring is the direct limit of its finite subrings: $B = \varinjlim B_i$. Applying Stone Duality gives: every Boolean space is an inverse limit of finite Boolean spaces. The proof that we gave above is a more explicit form of this argument.*

EXERCISE 15.26. *In Chapter 7, we saw that an infinite profinite group has at least continuum cardinality. Exhibit a countably infinite Boolean space.*

In Chapter 7 we introduced profinite groups, showed that automorphism groups of algebraic Galois extensions equipped with the Krull topology are profinite, and then saw that every profinite group arises as such a Galois group. Now we've introduced profinite spaces and showed that sets of orderings on a field equipped with the Harrison topology are Boolean. The following result completes this analogy:

THEOREM 15.32. *(Craven* [**Cr75**]*) Let X be a Boolean space.*

a) *There is a field F such that X is homeomorphic to the real spectrum $X(F)$.*
b) *If X is moreover second countable (equivalently, metrizable), then we may take the field F in part a) to be algebraic over $\mathbb{Q}$.*

Unfortunately we will not prove Theorem 15.32a) here, but the last of the following exercises gives a loose sketch of a proof of Theorem 15.32b).

EXERCISE 15.27. *Let $F = \varinjlim_\alpha F_\alpha$ be a direct limit (i.e., directed union) of fields. Show $X(F) = \varprojlim_\alpha X(F_\alpha)$ as topological spaces.*

EXERCISE 15.28. *Let $F/\mathbb{Q}$ be a formally real Galois extension.*

a) *Show $\operatorname{Aut}(F/\mathbb{Q})$ acts continuously and simply transitively on $X(F)$.*
b) *Deduce: the space $X(F)$ is homeomorphic to the Krull topology on $\operatorname{Aut}(F/\mathbb{Q})$.*
c) *Suppose $F/\mathbb{Q}$ has infinite degree. Deduce: $X(F)$ is homeomorphic to the Cantor set.*

EXERCISE 15.29. *Use the Artin–Whaples ("Weak") Approximation Theorem to show that any inverse system of finite sets with surjective transition maps*

$$\ldots \to S_{n+1} \to S_n \to \ldots \to S_1$$

can be realized as the system of $X(F_n)$'s where

$$F_1 \ldots \hookrightarrow F_n \hookrightarrow F_{n+1} \hookrightarrow \ldots$$

is a tower of number fields. Conclude that any Boolean space with a countable basis arises as the space of orderings of an algebraic field extension of $\mathbb{Q}$.

CHAPTER 16

Orderings and Valuations

In this final chapter, we explore connections between ordered fields and valuation theory. The *raison d'être* is the payoff that for any infinite cardinal κ, there are 2^κ isomorphism classes of non-Archimedean real-closed fields of cardinality κ, which is a natural complement to the results on Archimdean real-closed fields derived in the previous chapter.

In the first section of this chapter, we review the basic definitions for valuations on a field, but we warn that our treatment of valuation theory is *not* fully self-contained: at several key points we use results on extensions of valuations and the structure theory of Henselian valued fields. Overall this chapter is suitable for an audience with some prior familiarity with valuation theory. Valuation theory is substantially treated in two other expositions of mine: [**Cl-CA**, Ch. 17] covers the commutative algebra of valuation rings, while [**Cl-NTII**, Ch. 1-2] covers rank 1 valuations – or equivalently, non-Archimedean norms – thoroughly and has a little bit to say about the higher rank case that is discussed here. A reasonable working knowledge of valuation theory in rank 1 would put the reader in a good place to appreciate the material of this final chapter. The main difference between the rank 1 case and the general case is the primary role played by completeness in the rank 1 case, which must be replaced by a combination of Henselianity and spherical completeness (not discussed here) in the general case.

We use the recent text [**EP**] of Engler–Prestel as a reference for unproved results on valuation theory.

1. Krull Valuations and Valuation Rings

Let K be a field, and let $(\Gamma, +, <)$ be an ordered commutative group. A **Γ-valued valuation** on K is a surjective map

$$v : K^\times \to \Gamma$$

such that
(VF1) For all $x, y \in K^\times$, we have $v(xy) = v(x) + v(y)$, and
(VF2) For all $x, y \in K^\times$ such that $x + y \neq 0$, we have $v(x + y) \geq \min(v(x), v(y))$.

It can be convenient to adjoin to Γ an element ∞; we extend the ordering to $\Gamma \cup \{\infty\}$ by putting $\infty > \gamma$ for all $\gamma \in \Gamma$. Then we may define $v(0) := \infty$, and (VF1) and (VF2) hold even if some of x, y and $x + y$ are 0.

Exercise 16.1. *Let R be a commutative ring, let $(\Gamma, +, <$ be an ordered commutative group, and let $v : R \setminus \{0\} \to \Gamma$ be a map satisfying:*

(VR1) For all $x, y \in R \setminus \{0\}$, we have $v(xy) = v(x) + v(y)$, and
(VR2) For all $x, y \in R \setminus \{0\}$ such that $x+y \neq 0$, we have $v(x+y) \geq \min(v(x), v(y))$.

a) *Show: R is a domain, and let F be the fraction field of R.*
b) *Let Γ' be the subgroup of Γ generated by $v(R \setminus \{0\})$. Show: there is a unique valuation $v : K^\times \to \Gamma'$ extending the map v on $R \setminus \{0\}$.*

We call a field K equipped with a valuation $v : K^\times \to \Gamma$ a **valued field**. Let (K_1, Γ_1, v_1) and (K_2, Γ_2, v_2) be valued fields. An **embedding of valued fields**

$$\Phi : (K_1, \Gamma_1, v_1) \to (K_2, \Gamma_2, v_2)$$

is a pair (f, ι) where $f : K_1 \to K_2$ is a field embedding, $\iota : \Gamma_1 \to \Gamma_2$ is an embedding of ordered commutative groups and we have

$$v_2 \circ f = \iota \circ v_1$$

as functions from $K_1^\times$ to Γ_2. If we have embeddings

$$\Phi = (f_1, \iota_1) : (K_1, \Gamma_1, v_1) \to (K_2, \Gamma_2, v_2) \text{ and } \Psi = (f_2, \iota_2) : (K_2, \Gamma_2, v_2) \to (K_3, \Gamma_3, v_3)$$

then

$$\Psi \circ \Phi \coloneqq (f_2 \circ f_1, \iota_2 \circ \iota_1) : (K_1, \Gamma_1, v_1) \to (K_3, \Gamma_3, v_3)$$

is an embedding of valued fields. We can then define an **isomorphism** of valued fields as an embedding that admits a two-sided inverse embedding. Then an embedding $\Phi = (f, \iota)$ is an isomorphism if and only if f is a field isomorphism and ι is an isomorphism of ordered commutative groups if and only if f and ι are surjective.

We say that a valuation v is **trivial** if Γ is the trivial group (i.e., $\#\Gamma = 1$) and **nontrivial** otherwise. We say a valuation v is **discrete** if $\Gamma \cong \mathbb{Z}$ as an ordered group. If $v : K^\times \to \Gamma$ is a discrete valuation, a **uniformizing element** (or **uniformizer**) is an element $\pi \in K^\times$ such that $v(\pi)$ is the unique positive generator of Γ.

We say that v has **rank 1** if Γ is nontrivial and Archimedean; equivalently by Theorem 13.10, the valued field is isomorphic to one in which the value group Γ is a subgroup of $(\mathbb{R}, +)$.

REMARK 16.1. *In some contexts one is only dealing with rank 1 valuations. In this case it is convenient to drop the requirement that the map $v : K^\times \to \Gamma$ be surjective, and then we can take all rank 1 valuations as having codomain $\mathbb{R}$. In this case we just need to define the value group as $v(K^\times)$.*

EXAMPLE 16.1. *On $\mathbb{Q}$ we have the p-adic valuation $v_p : \mathbb{Q}^\times \to \mathbb{Z}$. Here we take a nonzero rational number x and write it in the form $p^c \frac{a}{b}$ with $a, b, c \in \mathbb{Z}$ and $p \nmid ab$, and then we put $v_p(x) = c$. This is a discrete valuation on $\mathbb{Q}$, in which p is a uniformizing element.*

EXERCISE 16.2. *Let R be a unique factorization domain (UFD) with fraction field K, and let p be a nonzero prime element of R. Show that there is a discrete valuation $v_p : K^\times \to \mathbb{Z}$ that is characterized by:*
- *For all $u \in R^\times$, we have $v(u) = 0$,*
- *For every prime element q such that $(q) \neq (p)$, we have $v(q) = 0$.*

EXERCISE 16.3. *Let (K, v) be a valued field. Let $x, y \in K^\times$ be such that $v(x) < v(y)$. Show: $v(x + y) = v(x - y) = v(x)$.*

We now give an equivalent, but more algebraic, formalism for valued fields that is roughly analogous to passing from an ordering on a field to its positive cone.

A subring R of a field K is a **valuation ring** if for all $x \in K^\times$, at least one of x and x^{-1} lies in R. It is clear that then K is the fraction field of R. We claim that a valuation ring is a local ring: it has a unique maximal ideal, or equivalently the nonunits of R form a maximal ideal. To see this, let x and y be nonzero nonunits of R. Then one of $\frac{x}{y}$ and $\frac{y}{x}$ lies in R; interchanging x and y if necessary, we may assume that $\frac{x}{y} \in R$. Then $1 + \frac{x}{y} = \frac{x+y}{y} \in R$, so if $x + y \in R^\times$ then $\frac{1}{y} \in R$, contradicting the assumption that y is not a unit. Clearly if $x \in R$ is a nonunit, so is $-x$. If $x, y \in R$ with x a nonunit, then yx must be a nonunit (since an element that divides a unit is a unit). Thus the set $\mathfrak{m}$ of nonunits of R is the unique maximal ideal of R. The **residue field** of a valuation ring R is $k \coloneqq R/\mathfrak{m}$, and we have a natural map $q : R \to k$.

Exercise 16.4.

a) *Let L/K be a field extension, and let T be a valuation ring of L. Show: $T \cap K$ is a valuation ring of K.*

b) *Let K be a field, and let R_1, R_2 be two valuation rings of K, with maximal ideals $\mathfrak{m}_1$ and $\mathfrak{m}_2$. Show: if $\mathfrak{m}_1 = \mathfrak{m}_2$, then $R_1 = R_2$.*

For a valued field $v : K^\times \to \Gamma$, we put

$$R_v \coloneqq \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}.$$

Then R_v is a valuation ring: indeed, for all $x \in K^\times$, we have $v(x^{-1}) = -v(x)$, so at least one of $v(x)$ and $v(x^{-1})$ lies in $\Gamma^{\geq 0}$.

Exercise 16.5. *Let v be a trivial valuation on a field K. Show: $R = K$, $\mathfrak{m} = (0)$ and $k = K$.*

Now let R be a valuation ring with fraction field K, and put $\Gamma \coloneqq K^\times/R^\times$, a commutative group. For elements $\underline{x} = xR^\times$ and $\underline{y} = yR^\times$, we define $\underline{x} \leq \underline{y}$ if $\frac{y}{x} \in R$: since multiplication or division by an element of $R^\times$ does not disturb whether an element of $K^\times$ lies in R, this is indeed a condition on the classes of x and y modulo $R^\times$.

Exercise 16.6. *Let R be a valuation ring with fraction field K, and define $\leq$ on $K^\times/R^\times$ as above.*

a) *Show: $(K^\times/R^\times, \leq)$ is an ordered commutative group.*

b) *Show: the quotient map $q : K^\times \to K^\times/R^\times$ is a $(K^\times/R^\times)$-valued valuation on K.*

Exercise 16.7. *Let (K_1, Γ_1, v_1) and (K_2, Γ_2, v_2) be two valued fields, with valuation rings $R_i \subseteq K_i$.*

a) *Let $(f, \iota) : (K_1, \Gamma_1, v_1) \to (K_2, \Gamma_2, v_2)$ be an embedding of valued fields. Show: $R_2 \cap f(K_1) = f(R_1)$.*

b) *Let $f : K_1 \hookrightarrow K_2$ be a field embedding such that $R_2 \cap f(K_1) = f(R_1)$. Show: there is an embedding $\iota : \Gamma_1 \to \Gamma_2$ such that $(f, \iota) : (K_1, \Gamma_1, v_1) \to (K_2, \Gamma_2, v_2)$ is an embedding of valued fields.*

c) *Deduce: if for $i \in \{1, 2\}$ we have a valuation $v_i : K \to \Gamma_i$ on K, then the valued fields (K, Γ_1, v_1) and (K, Γ, v_2) are isomorphic if and only if their valuation rings are equal.*

In particular, given a valuation $v : K \to \Gamma_v$ and an extension field L/K, we want to speak of valuations $w : L \to \Gamma_L$ on L **extending** the valuation v. For this, if we use the initial formalism of valuation groups, we need to supply an embedding of ordered commutative groups $\iota : \Gamma_v \hookrightarrow \Gamma_w$, and thus whenever there is any extension at all there is a proper class of such extensions obtained by replacing Γ_w with an isomorphic ordered commutative group. We are really interested in the set of isomorphism classes of extensions of v to L, and the formalism of valuation rings handles this much more easily: if R is the valuation ring of v, then isomorphism classes of extensions of v to L correspond to valuation rings S of L such that $S \cap K = R$. Indeed, using valuation rings we can show:

PROPOSITION 16.2. *Let v be a valuation on a field K, and let L/K be a field extension. Then v extends to a valuation on L.*

PROOF. Let $(R, \mathfrak{m}_R)$ be the valuation ring of v. By [**Cl-CA**, Lemma 17.25] there is a valuation ring $(T, \mathfrak{m}_T)$ of L such that $R \subseteq T$ and $\mathfrak{m}_T \cap R = \mathfrak{m}_R$. Exercise 16.4 gives $T \cap K = R$. □

EXERCISE 16.8. *Let $v : K^\times \to \Gamma$ be a valuation on a field K. For $x \in K$ and $\gamma \in \Gamma$, put*

$$U_x(\gamma) \coloneqq \{y \in K \mid v(x - y) > \gamma\}.$$

a) *Show: the sets $U_x(\gamma)$ for $x \in K$ and $\gamma \in \Gamma$ form the base for a unique topology on K, the **v-topology**.*
b) *Show: the v-topology makes K into a Hausdorff topological field.*
c) *Each subset $U_x(\gamma)$ is clopen in the v-topology, which is therefore totally disconnected.*
d) *Show: the v-topology is discrete if and only if v is trivial.*
e) *Show: if v has rank 1, then the v-topology is metrizable.*

2. Hahn Series

We now define a class of valued fields that are, in an important special case, also ordered fields. As motivation, we give another take on the monoid ring construction from Exercise 2.4. Let R be a commutative ring, and let $(M, +)$ be a commutative monoid. For a function $f : M \to R$, we define its **support**

$$\operatorname{supp}(f) \coloneqq \{x \in M \mid f(x) \neq 0.\}$$

Then the underlying R-module of the monoid ring $R[M]$ may be viewed as the R-submodule of R^M consisting of functions with finite support, since indeed this is a free R-module with basis the "delta functions"

$$\delta_m : x \mapsto \begin{cases} 1 & \text{if } x = m \\ 0 \text{ otherwise} & \end{cases}$$

as m ranges over elements of R, and then the multiplication operation on $R[M]$ is given by the **convolution product**

$$(f * g) : x \mapsto \sum_{y+z=x} f(y)g(z).$$

From Exercise 2.4, the ring $R[M]$ is a domain if and only if R is a domain and M is cancellative and torsionfree.

EXERCISE 16.9. *Let $(M,+)$ be a commutative monoid. A **group completion** $G(M)$ of M is a commutative group $(G(M)+)$ and a monoid map $\iota : M \to G(M)$ that is universal for monoid map into a commutative group: if H is a commutative group and $f : M \to H$ is a monoid map, then there is a unique group homomorphism $F : G(M) \to H$ such that $f = F \circ \iota$.*

a) *Show: any two group completions of M are canonically isomorphic.*

b) *Construct a group completion of M as follows: we introduce a relation $\sim$ on the commutative monoid $M \times M$ as follows: $(x_1, y_1) \sim (x_2, y_2)$ if and only if there is $z \in M$ such that $z + x_1 + y_2 = z + x_2 + y_1$.*
   (i) *Show: $\sim$ is an equivalence relation on $M \times M$, and let $G(M)$ be the set of $\sim$-equivalence classes.*
   (ii) *For $a, a', b, b' \in M \times M$, show: if $a \sim a'$ and $b \sim b'$, then $a+b \sim a'+b'$. Deduce: $[a]+[b] := [a+b]$ is a well-defined binary operation on $G(M)$.*
   (iii) *Show: $(G(M),+)$ is a commutative group.*
   (iv) *Show: the map*
$$\iota : M \to G(M),\ x \mapsto [(x,0)]$$
   is a group completion of M.

c) *Show: the following are equivalent:*
   (i) *There is a group G and an injective monoid map $\iota : M \hookrightarrow G$.*
   (ii) *The map $\iota : M \to G(M)$ from M to its group completion is injective.*
   (iii) *The monoid M is cancellative: for all $x, y, z \in M$, if $z + x = z + y$, then $x = y$.*

As an important example, let F be a field, and let $M := (\mathbb{N}, +)$. Then the monoid ring $F[M]$ is nothing else than the polynomial ring $F[t]$, once we identify a polynomial $\sum_{n \geq 0} a_n t^n$ (with $a_n = 0$ for all but finitely many n, of course) with the function $n \mapsto a_n$. The group completion of $\mathbb{N}$ is $\mathbb{Z}$, and the monoid ring (a.k.a. the **group ring**) $F[\mathbb{Z}]$ is the ring $F[t, t^{-1}]$ of Laurent polynomials $\sum_{n \in \mathbb{Z}} a_n t^n$: again $a_n = 0$ for all but finitely many n. The fraction field of both $F[\mathbb{N}]$ and $F[\mathbb{Z}]$ is the rational function field $F(t)$. It is now natural to seek to view elements of $F(t)$ as F-valued functions on $\mathbb{Z}$, and this is done via the field embedding $F(t) \hookrightarrow F((t))$, which associates to each rational function $f \in F(t)$ its formal Laurent series expansion $\sum_n a_n t^n$. Note that the latter sum is *not* necessarily finite; rather the condition is that there exist $N \in \mathbb{Z}$ such that $a_n = 0$ unless $n \geq N$. (For instance, the Laurent series expansion of $\frac{1}{1-t}$ is $\sum_{n=0}^{\infty} t^n$.)

EXERCISE 16.10. *Let $(X, \leq)$ be an infinite linearly ordered set.*

a) *Show: X contains either an infinite ascending chain*
$$x_1 < x_2 < \ldots < x_n < \ldots$$
   or an infinite descending chain
$$x_1 > x_2 > \ldots > x_n > \ldots.$$
   *(Hint: X contains an infinite sequence $\{y_n\}$ with distinct terms. Define $N \in \mathbb{Z}^+$ to be a **peak** of the sequence if $y_n < y_N$ for all $n > N$. Treat separately the case in which the sequence $\{y_n\}$ has infinitely many peaks and finitely many peaks.)*

b) *Let $\{x_n\}_{n=1}^{\infty}$ be a sequence in X. Show: there is a subsequence $\{x_{n_k}\}_{k=1}^{\infty}$ that is either strictly increasing, strictly decreasing or constant.*

c) *Show that the following are equivalent:*
   (i) *X is well-ordered.*
   (ii) *Every weakly decreasing infinite sequence in X is eventually constant.*
   (iii) *Every infinite sequence in X has a weakly increasing subsequence.*

Now suppose more generally that F is a field and $(G, +)$ is a torsionfree commutative group, so that by Exercise 2.4 the group ring $F[G]$ has a fraction field $F(G)$. It is now natural to ask whether $F(G)$ can be embedded into a larger field whose elements can be viewed as F-valued functions on G. This can be done by choosing an ordering $\leq$ on G, which is possible by Levi's Theorem (Theorem 13.7). Using this ordering, we define the **Hahn series field** $F((G))$. The elements of $F((G))$ are functions $f : G \to F$ such that $\mathrm{supp}(f)$ is a well-ordered subset of G. (When $G = \mathbb{Z}$, a nonempty subset is well-ordered if and only if it has a least element, so $F((\mathbb{Z}))$ is indeed the formal Laurent series field $F((t))$.) For $g \in G$, we write t^g for the δ function at g and write elements of $F((G))$ as $\sum_{g \in G} a_g t^g$: thus for all $g \in G$ we have $a_g \in F$, and the set of $g \in G$ such that $a_g \neq 0$ is well-ordered. This suggests that the addition and multiplication operators on $F((G))$ should be: if

$$f = \sum_g a_g t^g \text{ and } g = \sum_g b_g t^g \in F((G)),$$

then

$$f + g \coloneqq \sum_g (a_g + b_g) t^g$$

and

$$f \cdot g \coloneqq \sum_{h+k=g} a_h b_k t^g;$$

but we must check that these give well-defined elements of $F((G))$. For $f + g$: we have $\mathrm{supp}(f + g) \subseteq \mathrm{supp}(f) \cup \mathrm{supp}(g)$, and the union of two well-ordered sets (and hence also any subset thereof) is well-ordered: an infinite descending chain in $X \cup Y$ would yield an infinite descending chain in either X or Y. The case of $f \cdot g$ is a bit more involved, and we use the following result:

LEMMA 16.3. *Let $(G, \leq)$ be an ordered commutative group, let $n \in \mathbb{Z}^+$, and let $A_1, \ldots, A_n$ be well-ordered subsets of G.*

a) *For all $g \in G$, the set $\{(a_1, \ldots, a_n) \in \prod_{i=1}^n A_i \mid a_1 + \ldots + a_n = g\}$ is finite.*
b) *The set*

$$A_1 + \ldots + A_n \coloneqq \{a_1 + \ldots + a_n \mid a_i \in A_i \text{ for all } 1 \leq i \leq n\} \subseteq G$$

is well-ordered.

PROOF. In both parts, an immediate induction argument reduces us to the $n = 2$ case. We will write A and B in place of A_1 and A_2.
a) Seeking a contradiction, suppose there is $g \in G$ such that the set of ordered pairs $(a, b) \in A \times B$ such that $a + b = g$ is infinite. By Exercise 16.10a), there is then an infinite strictly monotone sequence $\{a_n\}_{n=1}^\infty$ in A such that for all $n \in \mathbb{Z}^+$ we have $b_n = g - a_n \in B$. If the sequence $\{a_n\}$ is strictly decreasing, this contradicts the well-orderedness of A, while if the sequence $\{a_n\}$ is strictly increasing, then the sequenec $\{b_n\}$ is strictly decreasing, contradicting the well-orderedness of B.
b) Seeking a contradiction: suppose that $A + B$ is *not* well-ordered: then there are

infinite sequences $\{a_n\}_{n=1}^\infty$ in A and $\{b_n\}_{n=1}^\infty$ in B such that $\{a_n + b_n\}$ is strictly decreasing. By Exercise 16.10b), there is an infinite subsequence $\{a_{n_k}\}_{k=1}^\infty$ that is either strictly decreasing or weakly increasing. The former contradicts the well-orderedness of A, while in the latter case, the sequence $b_{n_k} = (a_{n_k} + b_{n_k}) - a_{n_k}$ is strictly decreasing, contradicting the well-orderedness of B. □

Let $f, g \in F((G))$. Applying Lemma 16.3 with $A := \text{supp}(f)$ and $B := \text{supp}(g)$ shows first that for all $g \in G$, the inner sum $\sum_{h+k=g} a_h b_k$ in the definition of $f \cdot g$ is finite – so $f \cdot g$ is well-defined – and second that $\text{supp}(f \cdot g)$ is well-ordered, so $f \cdot g \in F((G))$.

EXERCISE 16.11. *Let F be a field, and let $(G, \leq)$ be an ordered commutative group. Define $v : F((G)) \setminus \{0\} \to G$ by mapping $f \in F((G)) \setminus \{0\}$ to the least element of* $\text{supp}(f)$.

a) *Show: v satisfies properties (VF1) and (VF2) for valuations.*
b) *Deduce: $F((G))$ is a domain.*

To show that $F((G))$ is a field, we need a stronger form of Lemma 16.3:

LEMMA 16.4 (Neumann). *Let $(G, \leq)$ be an ordered commmutative group, and let $A \subseteq G^+$ be well-ordered.*

a) *The set*
$$\Sigma(A) := \bigcup_{n=1}^\infty \{a_1 + \ldots + a_n \mid a_i \in A\}$$
is well-ordered.
b) *For all $g \in G$, the set of tuples $(n, a_1, \ldots, a_n)$ such that $n \in \mathbb{Z}^+$, $a_1, \ldots, a_n \in A$ and $a_1 + \ldots + a_n = g$ is finite.*

PROOF. We follow Alling [**Al**, §7.21].
a) Seeking a contradiction, we suppose that $\Sigma(A)$ is *not* well-ordered, and thus there is an infinite decreasing sequence $\{u_n\}_{n=1}^\infty$ in $\Sigma(A)$, with
$$u_n = a_{n,1} + \ldots + a_{n,m(n)}$$
and each $a_{i,j} \in A$. For $g \in G$, let $[g]$ be the convex subgroup generated by g. By Exercise 13.6, the set of convex subgroups of G is totally ordered under inclusion, so for all $n \in \mathbb{Z}^+$ we have
$$[u_n] = \max_{1 \leq j \leq m(n)} [a_{n,m(j)}].$$
The map $G^{\geq 0} \to C(G)$ by $g \mapsto [g]$ is order-preserving, so $\{[a] \mid a \in A\}$ is a well-ordered subset of the set $C(G)$ of convex subgroups of G. It follows that $\{[u_n] \mid n \in \mathbb{Z}^+\}$ is a well-ordered subset of $C(G)$. Thus, among all strictly decreasing sequences $\{u_n\}$ in $\Sigma(A)$, we may choose one that minimizes $[u_1]$, and then we have $[u_n] = [u_1]$ for all $n \in \mathbb{Z}^+$. There is also a minimal $a \in A$ such that $[a] = [u_n]$ for all $n \in \mathbb{Z}^+$. Thus for all $n \in \mathbb{Z}^+$ there is $b_n \in A$ such that $b_n = a_{n,j}$ for some j and $[b_n] = [a] = [u_n]$. So:

• For all $n \in \mathbb{Z}^+$, $a \leq b_n \leq u_n$ and $[a] = [b_n] = [u_n]$, so for some $r \in \mathbb{Z}^+$ and all $n \in \mathbb{Z}^+$ we have $u_n \leq u_1 \leq ra$.

Among all such sequences $\{u_n\}_{n=1}^\infty$, choose one that minimizes r. Since $\{u_n\}$ is

strictly decreasing and $\{b_n\}$ lies in the well- ordered set A, we can only have $b_n = u_n$ for finitely many n. Thus for all sufficiently large n we can write

$$u_n = v_n + b_n \tag{47}$$

with v_n a sum of all but one $a_{n,j}$. After passing to a subsequence, we may assume that (47) holds for all $n \in \mathbb{Z}^+$. Since A is well-ordered, there is a subsequence $\{b_{n_k}\}_{k=1}^{\infty}$ of $\{b_n\}$ that is weakly increasing, and then (47) shows that $\{v_{n_k}\}$ is strictly decreasing. It follows that for all $k \in \mathbb{Z}^+$,

$$v_{n_k} < u_{n_k}$$

and

$$[v_{n_k}] = [a]$$

because $\{u_n\}$ minimizes $[u_1]$ among strictly decreasing sequences. For all $k \in \mathbb{Z}^+$,

$$v_{n_k} + a \leq v_{n_k} + b_{n_k} = u_{n_k} \leq u_1 \leq ra,$$

so

$$v_{n_k} \leq (r-1)a.$$

This contradicts the minimality of r.

b) For $n \in \mathbb{Z}^+$, let $\Sigma_n(A) \coloneqq \{a_1 + \ldots + a_n \mid a_i \in A\}$; this subset is well-ordered by Lemma 16.3. Thus to prove part a) it suffices to show that for each $g \in G$, the set of $n \in \mathbb{Z}^+$ such that $g \in \Sigma_n(A)$ is finite. Seeking a contradiction, we suppose not: then the set $\mathcal{C}$ of $g \in G$ that lie in $\Sigma_n(A)$ for infinitely many $n \in \mathbb{Z}^+$ is a nonempty subset of the well-ordered set $\Sigma(A)$, so there is a least such g. There is a strictly increasing function $m : \mathbb{Z}^+ \to \mathbb{Z}^{\geq 2}$ and for all $n \in \mathbb{Z}^+$ elements $a_{n,1}, a_{n,m(n)} \in A$ such that $\sum_{k=1}^{m(n)} a_{n,k} = g$. Now consider the following infinite sequence:

$$a_{1,1}, \ldots, a_{1,m(1)}, a_{2,2}, \ldots, a_{2,m(2)}, \ldots, a_{n,n}, \ldots, a_{n,m(n)}, \ldots$$

Since A is well-ordered, by Exercise 16.10c) it admits a weakly increasing subsequence, which after removing some terms and reordering the $a_{n,k}$'s for fixed n, we may assume is $\{s_{n_k,1}\}_{k=1}^{\infty}$. Now consider the sequence

$$b_n \coloneqq a_{n,2} + \ldots + a_{n,m(n)} = g - a_{n,1}.$$

Its subsequence $\{b_{n_k}\}_{k=1}^{\infty}$ is weakly decreasing, with terms lying in $\Sigma(A)$, which is well-ordered by part a), so by Exercise 16.10c) the sequence is eventually constant: let $K \in \mathbb{Z}^+$ be such that $b_{n_k} = b_{n_{k+1}}$ for all $k \geq K$. Thus $b_{n_K} \in \mathcal{C}$ and $b_{n_K} = g - a_{n_K,1} < g$: contradiction. □

Let $\epsilon \in F((G))$ hae $v(\epsilon) > 0$: that is, $\operatorname{supp}(f) \subseteq G^+$. For a sequence $\{x_n\}_{n=0}^{\infty}$ in F, we claim that the formal series $\sum_{n=0}^{\infty} x_n \epsilon^n$ defines an element of $F((G))$. To see this, put $A \coloneqq \operatorname{supp}(\epsilon)$. If A is empty, then ϵ is 0, and we put $\sum_{n=0}^{\infty} x_n \epsilon_n \coloneqq x_0$, so suppose A is nonempty. Let $g \in G$. By Lemma 16.4, there is $N(g) \in \mathbb{Z}^+$ such that for all $n > N(g)$, there are no elements $a_1, \ldots, a_n \in A$ with $a_1 + \ldots + a_n = g$. It follows that for $n \geq N(g)$, the element g does not lie in $\operatorname{supp}(\epsilon^n) \supseteq \operatorname{supp}(x_n \epsilon^n)$. Thus we can define the coefficient of g in $\sum_{n=0}^{\infty} x_n \epsilon^n$ to be the coefficient of g in $\sum_{n=0}^{N(g)} x_n \epsilon^n$. The resulting element of F^G has support lying in $\{0\} \cup \bigcup_{n=1}^{\infty} \operatorname{supp}(\epsilon^n) \subseteq \{0\} \cup \Sigma(A)$, which is well-ordered by Lemma 16.4.

In particular, consider the series

$$S(\epsilon) \coloneqq \sum_{n=0}^{\infty} \epsilon^n.$$

We claim that

$$S(\epsilon)(1-\epsilon) = 1.$$

To see this, we'll compare coefficients of t^g for $g \in G$: note that both sides are supported on $G^{\geq 0}$. The t^0-coefficient of both sides is 1. Let $g > 0$, and choose $N(g) \in \mathbb{Z}^+$ such that for $n > N(g)$, g does not lie in the support of ϵ^n. Then the coefficient of t^g in $S(\epsilon)(1-\epsilon)$ is the coefficient of t^g in $(1+\epsilon+\ldots+\epsilon^{N(g)})(1-\epsilon) = 1-\epsilon^{N(g)+1}$ is 0, as of course is the coefficient of t^g in $1 = t^0$.

Finally, we can show that $F((G))$ is a field: let $f \in F((G)) \setminus \{0\}$. We may write $f = a_g t^g + \sum_{h>g} a_h t^h$ with $a_g \in F^\times$, and then

$$a_g^{-1} t^{-g} f = 1 - \sum_{h>0} \frac{-a_h}{a_g} t^h = 1 - \epsilon,$$

where $\epsilon \coloneqq \sum_{h>0} \frac{-a_h}{a_g} t^h$ and $v(\epsilon) > 0$. Thus

$$f^{-1} = a_g^{-1} t^{-g} S(\epsilon).$$

Now that we know that $F((G))$ is a field, Exercise 16.11 shows that the map $v : F((G))^\times \to G$ that maps f to the least element of its support is indeed a valuation on $F((G))$. The following exercise reiterates this and draws some quick consequences:

Exercise 16.12. *Let F be a field, let G be an ordered commutative group. We define a map*

$$v : F((G))^\times \to G$$

as follows: for $f \in F(((G))^\times$, we may write $f = a_g t^g + \sum_{h>h} a_h t^h$ with $a_g \neq 0$, and then we put

$$v(f) \coloneqq g.$$

a) *Show: v is a valuation on $F((G))$.*
b) *Show: the valuation ring is $F[[G]] \coloneqq \sum_{g \geq 0} a_g t^g$, the set of Hahn series with support contained in $G^{\geq 0}$. Also show: the maximal ideal $\mathfrak{m}$ of $F[[G]]$ is $\sum_{g>0} a_g t^g$, the set of Hahn series with support contained in G^+.*
c) *Show: the map $\sum_{g \geq 0} a_g t^g \mapsto a_g$ induces an isomorphism $F[[G]]/\mathfrak{m} \xrightarrow{\sim} F$.*

We have

$$F[G^{\geq 0}] \subseteq F[[G]] \text{ and } F(G) \subseteq F((G)).$$

Moreover, since for all $g \in G$ we have $t^g \in F(G)$, the restriction of v to $F(G)$ still has value group Γ, and because for all $x \in F$ we have $x \cdot t^0 \in F[G^{\geq 0}]$, the residue field of $F[[G]] \cap F(G)$ is still F. Thus each of $(F(G), v)$ and $(F((G)), v)$ show that there are valued fields with any prescribed totally ordered commutative group as value group and every possible field as residue field. Except in the trivial case $G = \{e\}$ – in which case we have $F(G) = F((G)) = F$ – we have $F(G) \subsetneq F((G))$, and the latter field seems *much* larger: for instance, if F and G are countably infinite then so is $F(G)$, while for any $g \in G^{>0}$ the field $F((G))$ contains all elements of F^G with

support contained in $\{ng \mid n \in \mathbb{N}\}$, hence contains a copy of $F^{\aleph_0}$, so has at least continuum cardinality.

PROPOSITION 16.5. *Let $(G, \leq)$ be an ordered commutative group, and let $(F, \mathfrak{p})$ be an ordered field. Let $P^\bullet$ be the set of elements $f \in F((G))$ such that when we write $f = a_g t^g + \sum_{h>g} a_h t^h$ with $a_g \neq 0$, then we have $a_g > 0$. Then $P := P^\bullet \cup \{0\}$ is an ordering on $F((G))$ such that $P \cap F = \mathfrak{p}$.*

EXERCISE 16.13. *Prove Proposition 16.5.*

EXERCISE 16.14. *Let k be a field. Let $\Gamma := (\mathbb{Q}, +)$, endowed with the ordering it inherits from $\mathbb{R}$. Show: the* ***Puiseux series field***

$$P_k := \bigcup_{n \in \mathbb{Z}^+} k((t^{1/n}))$$

is a proper subfield of the Hahn series field $k((\Gamma))$.

3. Compatibility Between Orderings and Valuations

3.1. Compatibility.

PROPOSITION 16.6. *Let K be a field. Let $v : K^\times \to \Gamma$ be a valuation on K with valuation ring $(R, \mathfrak{m})$. Let $q : R \to R/\mathfrak{m} =: k$ be the homomorphism to the residue field. Let P be an ordering on K. The following are equivalent:*

(i) *$(R, +)$ is a P-convex subgroup.*
(ii) *$(\mathfrak{m}, +)$ is a P-convex subgroup of $(R, +)$: if $0 < x < y$ with $x \in R$ and $y \in \mathfrak{m}$, then $x \in \mathfrak{m}$.*
(iii) *$P_k := q(P \cap R)$ is an ordering on k.*
(iv) *We have $1 + \mathfrak{m} \subseteq P$.*

When these equivalent conditions hold, we say that the valuation v and the ordering P are ***compatible****.*

PROOF. (i) $\implies$ (ii): Suppose that $(R, +)$ is a P-convex subgroup, and let $0 < x < y$ with $x \in R$ and $y \in \mathfrak{m}$, so $v(y) > 0$. Then $0 < y^{-1} < x^{-1}$. If $x \notin \mathfrak{m}$, then $x^{-1} \in \mathfrak{m}$, so by convexity also $y^{-1} \in \mathfrak{m}$, so $v(y) < 0$: contradiction.
(ii) $\implies$ (iii): Suppose (ii). It is immediate that $P_k = q(P \cap R)$ is closed under addition and multiplication. For $x \in k^\times$, choose $X \in R$ with $q(X) = R$. Then one of X and $-X$ lies in $P \cap R$, so one of x and $-x$ lies in P_k. Seeking a contradiction, suppose that $-1 \in P_k$, so there is $x \in P$ with $x + 1 \in \mathfrak{m}$. Since $0 < 1 \leq x + 1$, condition (ii) implies $1 \in \mathfrak{m}$: contradiction.
(iii) $\implies$ (iv): Going by contrapositive, if there is $x \in \mathfrak{m}$ such that $1 + x \notin P$, then $-1 - x \in P \cap R$, so $q(-1 - x) = -1 \in P_k$, so P_k is not an ordering on k.
(iv) $\implies$ (i): Again we go by contrapositive: suppose that we have $x, y \in K$ with $0 < x < y$, $y \in R$ but $x \notin R$. Then $0 < y^{-1} < x^{-1}$ and $x^{-1} \in \mathfrak{m}$, so also $-x^{-1}y \in \mathfrak{m}$. If (iv) holds, then $1 - x^{-1}y \in P$, and since $x \in P$, also $x - y \in P$: contradiction. □

When the equivalent conditions of Proposition 16.6 hold, the quotient map $q : R \to k$ is isotone: if for $x, y \in R$ we have $x \leq y$, then $y - x \in P \cap R$, so $q(y) - q(x) = q(y - x) \in P_k$, so $q(x) \leq q(y)$.

EXAMPLE 16.7. *Let Γ be an ordered commutative group, let $(F, \mathfrak{p})$ be an ordered field, let $v : F((\Gamma)) \to \Gamma$ be the valuation constructed above on the the Hahn series field $F((\Gamma))$, and let P be the induced ordering on the Hahn series field $F((\Gamma)$ from Proposition 16.5. Then v and P are compatible: on one hand, if $R = F[[\Gamma]]$ is the valuation ring of $F((\Gamma))$ and $q : R \to F$ is the quotient map, then $q(P \cap R) = \mathfrak{p}$ is an ordering on F, so condition (iii) of Proposition 16.6 holds. On the other hand, if $\mathfrak{m}$ is the maximal ideal of R, then $1 + \mathfrak{m}$ consists of Hahn series with lowest degree term t^0, all of which lie in P, so condition (iv) of Proposition 16.6 holds.*

As a special case of this, if $(F, \mathfrak{p})$ is an ordered field, then the unique ordering on the formal Laurent series field $F((t))$ containing $\mathfrak{p}$ and t is compatible with the valuation on $F((t))$ that maps $\sum_{n \neq N} a_n t^n$ with $a_N \neq 0$ to N.

3.2. The canonical valuation on an ordered field.

Now let (K, P) be an ordered field. We say $x \in K$ is **finitely large** if $x \preceq 1$ – that is, $|x| \leq n$ for some $n \in \mathbb{Z}^+$ – and otherwise we say that x is **infinitely large**. For $x \in K$, we say that x is **infinitesimal** if $x = 0$ or $x \neq 0$ and $\frac{1}{x}$ is infinitely large – equivalently, x is infinitesimal if and only if $|x| < \frac{1}{n}$ for all $n \in \mathbb{Z}^+$.

If $x_1, x_2 \in K$ are finitely large, then also $-x_1, -x_2$ are finitely large. For $i = 1, 2$, choose $n_i \in \mathbb{Z}^+$ such that $|x_i| \leq n_i$. Then $|x_1 + x_2| \leq n_1 + n_2$ and $|x_1 x_2| \leq n_1 b_2$. If $x \in K$ is infinitely large, then $|x| > 1$, so $|\frac{1}{x}| < 1$ and thus $\frac{1}{x}$ is finitely large. Finally, if $x, y \in K$ with $|x| \leq |y|$ and y is finitely large, then also x is finitely large. It follows that the set R of finitely large elements of K is a valuation ring and a P-convex subgroup, so by Proposition 16.6 there is an induced ordering on the residue field $k \coloneqq R/\mathfrak{m}$. The maximal ideal $\mathfrak{m}$ of R consists precisely of the infinitesimal elements of K. For $x \in P_k$, let $X \in P \cap R$ be such that $q(X) = x$, and let $n \in \mathbb{Z}^+$ be such that $x \leq n$. Then $q(x) \leq q(n) = n$, so the ordered field (k, P_k) is Archimedean.

Let (K, P) be an ordered field, and recall that for $x, y \in K$, putting $x \approx y$ if $x \prec y$ and $y \prec x$ gives an equivalence relation on K, and we denote by $\Omega(K)$ the set of $\approx$ equivalence classes of nonzero elements of K. For $x \in K^\times$ we denote by $[x]$ the $\approx$-equivalence class of x. Then $[1] = R^\times$, and for $x, y \in K^\times$ we have $[x] = [y]$ if and only if $[\frac{x}{y}] = [1]$ if and only if $x \pmod{R^\times} = y \pmod{R^\times}$. Thus $\Omega(K)$ is canonically isomorphic to $K^\times/R^\times$, which gives $\Omega(K)$ the structure of a commutative group.

By Exercise 13.5, for any ordered commutative group G, the Archimedean equivalence classes of elements of $G \setminus \{0\}$ form a totally ordered set, where we define $[x] \leq [y]$ if and only if $x \prec y$ (and check that this is well-defined independent of the choice of representatives). In particular this gives us an ordering on $\Omega(K)$ for an ordered field K. Viewing $\Omega(K)$ as $K^\times/R^\times$ also gives $\Omega(K)$ an ordering, compatible with the group structure, in which $[x] \leq [y]$ if and only if $\frac{y}{x} \in R$ if and only if $y \prec x$. Thus these two orderings on $\Omega(K)$ are not equal but *dual to each other*. (An element of an ordered field that is very close to zero is very *small* in the ordering on the field, whereas an element of a valued field that is very close to zero has very *large* valuation.) In order for the natural map $v : K^\times \to \Omega(K)$ to be a valuation, we need to take the latter ordering on $\Omega(K)$, in which $[x] \leq [y] \iff y \prec x$.

Let us sum up the above discussion:

THEOREM 16.8. *Let (K, P) be an ordered field.*

a) *If we order the set $\Omega(K)$ of Archimedean equivalence classes of elements of $K^\times$ via $x \leq y \iff |\frac{y}{x}| \leq n$ for some $n \in \mathbb{Z}^+$, then the natural map $v : K^\times \to \Omega(K)$ is a valuation on K, called the* ***canonical valuation****.*

b) *The valuation ring $(R, \mathfrak{m})$ of v is the subring of finitely large elements, which is a convex subring.*

c) *Let $k \coloneqq R/\mathfrak{m}$ be the residue field, and let $P_k \coloneqq (P \cap R) \pmod{\mathfrak{m}}$. Then (k, P_k) is an Archimedean ordered field.*

EXERCISE 16.15. *Let Γ be an ordered commmutative group and F an Archimedean ordered field, which gives an ordering on $F((\Gamma))$ by Proposition 16.5.*

a) *Show: $\Omega(F(\Gamma)) = \Gamma$.*

b) *Show: the canonical valuation v on the ordered field $F((G))$ is the valuation v on $F((G))$ defined in Exercise 16.12.*

The following consequence makes a remarkable connection between valuation theory and the study of non-Archimedean fields.

COROLLARY 16.9. *An ordered field (K, P) admits a nontrivial valuation with P-convex valuation ring if and only if it is non-Archimedean.*

PROOF. The valuation v of Theorem 16.8 has Archimedean residue field k, so if K is non-Archimedean then $K \neq k$ and thus $\mathfrak{m} \neq 0$: the valuation is nontrivial. If K is Archimedean, then the only convex subgroups of K are $\{0\}$ and K, so the only convex subring of K is K itself. □

EXAMPLE 16.10. *Let $K = \mathbb{R}(t)$, endowed with the unique ordering in which $0 < t < \frac{1}{n}$ for all $n \in \mathbb{Z}^+$. Writing $f \in K^\times$ as $\sum_{n \geq N} a_n t^n$ with $a_N \neq 0$, then $f > 0$ if and only if $a_N > 0$. Let $v : K^\times \to \Omega(K)$ be the canonical valuation.*

Every nonzero element f of K can be written as $\frac{p}{q}$ with $p, q \in R[t]$ and $q \neq 0$, and we put $\deg(f) \coloneqq \deg(p) - \deg(q) \in \mathbb{Z}$. Then we have $f/t^{\deg(f)}$ is finitely large and not infinitesimal, so $f \approx t^{\deg(f)}$, while for all $n \in \mathbb{Z}$ we have $t^{n+1} \precneqq t^n$, so $\{t^n \mid n \in \mathbb{Z}\}$ is a set of representatives for $\Omega(K)$ in $K^\times$. It follows that $\Omega(K) \cong \mathbb{Z}$ and t is a uniformizing element, so the canonical valuation v is discrete.

The valuation ring R is the set of rational functions $\frac{f}{g}$ which, when written in lowest terms, have $g(0) \neq 0$, or in other words, the rational functions that are regular at 0*. The maximal ideal is the principal ideal generated by t. The residue field is $\mathbb{R}$, and the map $R \to R/\mathfrak{m}$ can be thought of as evaluation at* 0*.*

PROPOSITION 16.11. *We revisit the setup of Proposition 16.6. The equvialent conditions given there are also equivalent to each of the following:*

(v) *For all $x, y \in K$, if $0 < x \leq y$, then $v(x) \geq v(y)$.*

(vi) *The valuation ring R contains the valuation ring R_c of the canonical valuation v_c from Theorem 16.8.*

PROOF. (v) $\implies$ (i): Assume (v), and let $x, y \in K$ with $0 < x \leq y$ with $y \in R$. By (i) we have $v(x) \geq v(y) \geq 0$, so $x \in R$.
(i) $\implies$ (vi): Let R_c be the valuation ring of the canonical valuation, i.e., the set of all finitely large elements of K with respect to P. Since R_c is the set of elements $x \in K$ with $|x| \leq n$ for some $n \in \mathbb{Z}^+$, it is the unique smallest P-convex subring of K, and thus (i) implies $R_c \subseteq R$.

(vi) $\implies$ (v): Suppose $R_c \subseteq R$. Then we have a natural surjective homomorphism of ordered groups $q : K^\times/R_c^\times \to K^\times/R^\times$, with respect to which we may view the valuation v as $q \circ v_c$. Thus it is enough to show that for all $0 < x \leq y$ in K we have $v_c(x) \geq v_c(y)$. We know that v_c satisfies the equivalent conditions of Proposition 16.6: in particular, for all $x \in \mathfrak{m}_c$, we have $1 + x \in P$. Seeking a contradiction, we suppose that $v_c(x) < v_c(y)$, so $\frac{-y}{x} \in \mathfrak{m}_c$, so $1 + \frac{-y}{x} = \frac{x-y}{y} \in P$, and since $y \in P$ we conclude $x - y \in P$, i.e., $x > y$: contradiction. □

The valuation rings R containing a given valuation ring R_c are in isotone bijection with prime ideals of R_c, which in turn are in antitone bijection with convex subgroups of the value group Γ_c of R_c [**Cl-CA**, Thm. 17.22]. Thus for a given ordering P on K, there is more than one nontrivial compatible valuation if and only if $\Omega(K)$ is non-Archimedean.

EXERCISE 16.16. *Let (k, P_k) be an ordered field, and let $K \coloneqq k((t))$.*

a) *Show: We have $\Omega(K) \cong \mathbb{Z} \times \Omega(k)$, where the right hand side gets the lexicographic ordering.*

b) *Deduce: the canonical valuation v_c on K is discrete if and only if k is Archimedean.*

3.3. The Baer-Krull Representation Theorem.

For a valuation $v : K \to \Gamma$ on a field K with valuation ring R, maximal ideal $\mathfrak{m}$ and residue field k, we let $X^v(K)$ denote the set of orderings on F that are compatible with v in the sense of Proposition 16.6 above.

LEMMA 16.12. *The subset $X^v(K)$ is closed in $X(K)$, hence compact.*

PROOF. Let $P \in X(K) \setminus X^v(K)$. By Proposition 16.6, there is $x \in \mathfrak{m}$ such that $\operatorname{sgn}_P(1 + x) < 0$. Then $H(-1 - x)$ is an open neighborhood of P in the complement of $X^v(K)$, so $X^v(K)$ is closed in the compact space $X(K)$, hence is itself compact. □

THEOREM 16.13 (Baer–Krull Representation Theorem). *Let $v : K \to \Gamma$ be a valuation with valuation ring R, maximal ideal $\mathfrak{m}$ and residue field k. We denote by $\overline{v}$ the composite map*

$$K^\times \xrightarrow{v} \Gamma \to \Gamma/2\Gamma.$$

Let $\{x_i\}_{i\in I}$ be elements of $K^\times$ such that $\{\overline{x_i}\}_{i\in I}$ is an $\mathbb{F}_2$-basis for $\Gamma/2\Gamma$. We define

$$\Phi : X^v(K) \to \{\pm 1\}^I \times X(k)$$

as follows: let $P \in X^v(K)$ be a compatible ordering, and let $P_k \coloneqq (P \cap R) \pmod{\mathfrak{m}}$ be the induced ordering on k. Then we put

$$\Phi(P) \coloneqq (\{\operatorname{sgn}_P(x_i)\}_{i\in I}, P_k).$$

a) *The map Φ is a bijection.*

b) *If we give $\{\pm 1\}$ the discrete topology and $\{\pm 1\}^I \times X(k)$ the product topology, then Φ is a homeomorphism.*

PROOF. Let $q : R \to k$ be the quotient map.

a) For $a \in K^\times$, there are unique $x_{i_1}, \ldots, x_{i_r} \in I$ such that $\overline{v}(a) = \sum_{j=1}^r \overline{v(x_{i_j})}$, so there is $b \in K^\times$ and $u \in R^\times$ such that $a = ub^2 x_{i_1} \cdots x_{i_r}$. Here b is determined by $a, x_{i_1}, \ldots, x_{i_r}$ up to a unit in R, so u is determined up to the square of a unit in R.

Given a mapping $\eta : I \to \{\pm 1\}$ and an ordering Q on k, we define a subset $P(\eta, Q)$ of K as follows: $0 \in P(\eta, Q)$, and for $a \in K^\times$ we have $a \in P(\eta, Q)$ if and only if $\eta(x_{i_1}) \cdots \eta(x_{i_r}) q(u) \in Q$. Because u is determined up to the square of a unit, this is well-defined. We claim that $P(\eta, Q)$ is an ordering on K that is compatible with v and such that $q(P(\eta, Q) \cap R) = Q$, which will show the surjectivity of Φ.

Let a, a' be nonzero elements of $P(\eta, Q)$, and write

$$a = ub^2 x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}$$

$$a' = u'(b')^2 x_{i_1}^{\epsilon_1'} \cdots x_{i_n}^{\epsilon_n'}$$

with $\epsilon_1, \ldots, \epsilon_n, \epsilon_1', \ldots, \epsilon_n' \in \{0, 1\}$.

Case 1: Suppose that $v(a) \neq v(a')$; without loss of generality, we may assume $v(a) < v(a')$, so $v(a + a') = v(a)$ and thus $a + a' = ca$ for some $c \in R^\times$. Dividing by a, we find $q(c) = q(1) = 1$, so

$$a + a' = cub^2 \pi_{i_1}^{\epsilon_1} \cdots \pi_{i_n}^{\epsilon_n}.$$

Since $a \in P(\eta, Q)$, we have $\eta(\pi_{i_1}) \cdots \eta(\pi_{i_n}) q(u) \in Q$, and thus $\eta(\pi_{i_1}) \cdots \eta(\pi_{i_n}) q(uc) = \eta(\pi_{i_1}) \cdots \eta(\pi_{i_n}) q(u) \in Q$, so $a + a' \in P(\eta, Q)$.

Case 2: Suppose that $v(a) = v(a')$. Then $v(a) \pmod{2\Gamma} = v(a') \pmod{2\Gamma}$, which since $\overline{x_{i_1}}, \ldots, \overline{x_{i_n}}$ are $\mathbb{F}_2$-linearly independent, implies $\epsilon_i = \epsilon_i'$ for all $1 \leq i \leq n$. Thus $(\frac{b}{b'})^2 = \frac{au'}{au} \in R^\times$, so $0 = v(\frac{b}{b'})^2) = 2v(\frac{b}{b'}$, and thus there is $u'' \in R^\times$ with $b' = bu''$, so

$$a + a' = (u + u'(u'')^2) b^2 x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}.$$

Since $\eta(x_{i_1}) \cdots \eta(x_{i_r}) q(u),\ \eta(x_{i_1}) \cdots \eta(x_{i_r}) q(u') \in Q$, it follows that

$$\eta(x_{i_1}) \cdots \eta(x_{i_r}) q(u + u'(u'')^2) \in Q,$$

so $a + a' \in P(\eta, Q)$.

There is a unique extension of η to an $\mathbb{F}_2$-linear map $\eta : \Gamma/2\Gamma \to \{\pm 1\}$. The pullback to η to $K^\times$ is a group homomorphism from $K^\times$ to $\{\pm 1\}$ that we will also denote by η. Then for $a \in K^\times$ we have $a \in P(\eta, Q)$ if and only if $\eta(a) q(u) \in Q$. Now we have

$$aa' = uu'(bb')^2 x_{i_1}^{\epsilon_1 + \epsilon_1'} \cdots x_{i_n}^{\epsilon_n + \epsilon_n'},$$

so $aa' \in P(\eta, Q)$ if and only if $\eta(aa') q(uu') \in Q$, but

$$\eta(aa') q(uu') = (\eta(a) q(u))(\eta(a') q(u')) \in QQ \subseteq Q,$$

so indeed $aa' \in P(\eta, Q)$.

From the definition of $P(\eta, Q)$ we see that it does not contain -1 and that for all $x \in K^\times$ it contains exactly one of x and $-x$. Thus $P(\eta, Q)$ is an ordering on K.

We have $1 + \mathfrak{m} \subseteq\subseteq P(\eta, Q)$, so by Proposition 16.6 the ordering $P(\eta, Q)$ is compatible with v. Finally, the nonzero elements of $q(P(\eta, Q) \cap R)$ are the images under q of the elements of $P(\eta, Q) \cap R^\times$, but by definition of $P(\eta, Q)$ we have that $P(\eta, Q) \cap R^\times = q^{-1}(Q^\bullet)$; since q is surjective, we have $q(P(\eta, Q) \cap R^\times) = q(q^{-1}(Q^\bullet)) = Q^\bullet$, and thus $q(P(\eta, Q) \cap R) = Q$. This shows the surjectivity of Φ.

Finally, let $P \in X^v(K)$, and let η_P be the mapping $I \to \{\pm 1\}$ given by $x_i \mapsto \operatorname{sgn}_P(x_i)$, and let $P_k \coloneqq q(P \cap R)$. Then the construction of $P(\eta_P, P_k)$ shows that $P(\eta_P, P_k) \subseteq P$. But there are no proper containments of orderings on a field, so $P = P(\eta_P, P_k)$.

b) By the universal property of the product topology, to show that Φ is continuous, it is enough to show that for all $i \in I$ the map $P \mapsto \operatorname{sgn}_P(x_i)$ is continuous and

the map $P \mapsto P_k$ is continuous. The former is immediate from the fact that the topology on $X(F)$ is obtained from its embedding into $\{\pm 1\}^{F^\times}$: otherwise put, the topology on $X(F)$ is the coarsest one making the maps $P \mapsto \mathrm{sgn}_P(x)$ continuous for all $x \in F^\times$. Let $P \in X^v(K)$; then every open neighborhood of P_k contains a neighborhood of the form $H(\overline{x})$ for some $\overline{x} \in k$. Let $x \in R$ be such that $x \pmod{\mathfrak{m}} = \overline{x}$. If $\mathrm{sgn}_P(x) = 1$ then $\mathrm{sgn}_{P_k}(\overline{x}) = 1$, while if $\mathrm{sgn}_P(x) = -1$, then $\mathrm{sgn}_P(-x) = 1$, so $\mathrm{sgn}_{P_k}(-\overline{x}) = 1$ and $\mathrm{sgn}_{P_k}(\overline{x}) = -1$. It follows that the map $P \mapsto P_k$ carries $H(x)$ into $H(\overline{x})$, so the map $P \mapsto P_k$ is continuous. Thus by Lemma 16.12, the map Φ is a continuous bijection between compact Hausdorff spaces, so it is a homeomorphism. □

Two extreme cases of Theorem 16.13 are already interesting:
• If the residue field k admits a unique ordering – e.g. if $k = \mathbb{Q}$ or if k is real-closed – then $X^v(K)$ is homeomorphic to $\{\pm 1\}^{\dim_{\mathbb{F}_2} \Gamma/2\Gamma}$. If $\Gamma(S)$ is a direct sum of copies of $\mathbb{Z}$ indexed by an ordered set S and given the lexicographic ordering, then $\Gamma(S)/2\Gamma(S)$ is an $\mathbb{F}_2$-vector space of dimension $\#S$. Taking the Hahn series field $K \coloneqq \mathbb{R}((\Gamma(S)))$ we get that $X^v(K)$ can be homeomorphic to $\{\pm 1\}^\kappa$ for any cardinal κ. As we will see later, in this case we have $X^v(K) = X(K)$.
• If the value group Γ is 2-divisible – that is, $2\Gamma = \Gamma$ – then $X^v(K) = X(k)$: every ordering on the residue field comes from a unique v-compatible ordering on K.

Corollary 16.14. *Let $v : K^\times \to \Gamma$ be a valued field, with valuation ring R and residue field k, and let P be compatible with v in the sense of Proposition 16.6. Let L/K be a field extension, and let w be an **immediate** extension of v to L: that is, the value group of w is also Γ an the residue field of w is also k. Then there is a unique extension of P to an ordering P_L on L that is compatible with w.*

Proof. Let T be the valuation ring of w, and let $q : R \to k$ and $q_L : T \to k$ be the quotient maps. Let $P_k \coloneqq q(P \cap R)$, which by compatbility is an ordering on k. As in Theorem 16.13, let $\{x_i\}_{i \in I}$ be elements of K whose images in $\Gamma/2\Gamma$ form an $\mathbb{F}_2$-basis. Let $\eta : I \to \{\pm 1\}$ be the function that maps x_i to $\mathrm{sgn}_P(x_i)$. Because the extension $(L, w)/(K, v)$ is immediate, by Theorem 16.13 there is a unique w-compatible ordering P_L on L such that $q_L(P_L \cap T) = P_k$ and for all $i \in I$ we have $\mathrm{sgn}_{P_L}(x_i) = \mathrm{sgn}_P(x_i)$. It remains to show that $P_L \cap K = P$.

Let $\mathfrak{m}$ be the maximal ideal of R and $\mathfrak{m}_L$ the maximal ideal of T, so $\mathfrak{m}_L \cap R = \mathfrak{m}$. Using Proposition 16.6: since P_L is compatible with w, we have $1 + \mathfrak{m}_L \subseteq P_L$, and intersecting with K gives $1 + \mathfrak{m} \subseteq (P_L \cap K)$, so $P_L \cap K$ is compatible with v. Thus $q((P_L \cap K) \cap R)$ is an ordering on k such that $q((P_L \cap K) \cap R) \subseteq q_L(P_L \cap T) = P_k$, and since there are no proper containments between orderings on a field, we get $q((P_L \cap K) \cap R) = P_k$. By construction, for all $i \in I$ we have $\mathrm{sgn}_{P_L \cap K}(x_i) = \mathrm{sgn}_{P_L}(x_i) = \mathrm{sgn}_P(x_i)$. Applying Theorem 16.13, we conclude that $P_L \cap K = P$. □

4. Henselian Fields

A valued field (K, v) is **Henselian** if for every algebraic extension L/K, there is a unique extension of v to L. (This holds if and only if there is a unique extension to every finite degree exetnsion L/K.) As mentioned above, this is most gracefully phrased in terms of valuation rings: if R is the valuation ring of v, then we mean that for all algebraic L/K, there is a unique valuation ring T of L such that $T \cap K = R$.

When the valuation v has rank 1, we may take $v : K^\times \to \mathbb{R}$ and then define an associated metric on K: $d(x,y) := 2^{-v(x-y)}$. Let K_v be the completion of K with respect to v; then if d_v is the metric on the completion, we have that $-\log_2(d_v)$ is a real-valued valuation on K_v extending v. An essential point of rank 1 valuation theory is that the complete rank 1 valued field (K_v, v) is Henselian [**Cl-NTII**, Thm. 1.43]. In the higher rank case, one still has a notion of completeness – every Cauchy net should converge – and completions: to every valued field (K,v), there is a unique up to isomorphism complete extension (K_v, v). However, in the higher rank case, complete valued fields need not be Henselian, and this divergence causes Henselian valued fields rather than complete valued fields to play the primary role.

THEOREM 16.15. *Let (K,v) be a valued field with residue field of characteristic 0. Then (K,v) is Henselian if and only if it admits no nontrivial algebraic immediate extension: i.e., an extension of v to a valuation w on an algebraic field extension L/K such that the valuation group of w is equal to the valuation group of v and the residue field of w is the residue field of v.*

PROOF. See [**EP**, Thm. 4.1.10]. □

Let (K,v) be a valued field, with valuation ring R. Let K^{sep} be a separable closure of K. Let $\mathfrak{g}_K := \mathrm{Aut}(K^{\mathrm{sep}}/K)$ be the absolute Galois group of K. By Proposition 16.2, the set $S(w|v)$ of valuations on K^{sep} extending v is nonempty. The group $\mathfrak{g}_K$ naturally acts on $S(w|v)$ by $(\sigma, w) \mapsto w \circ \sigma^{-1}$ (the inverse is there to give a left action), and because K^{sep}/K is normal, this action is transitive [**EP**, Thm. 3.2.15].

Now fix $w \in S(w|v)$, with corresponding valuation ring $T(w)$, and let

$$H^s(w) := \{\sigma \in \mathfrak{g}_K := \mathrm{Aut}(K^{\mathrm{sep}}/K) \mid \sigma(T(w)) = T(w)\}$$

be the subgroup of the absolute Galois group $\mathfrak{g}_K$ of K consisting of automorphisms that leave T invariant: equivalently, these are the automorphisms of the valued field (K^{sep}, w). Then $H^s(w)$ is a closed subgroup of $\mathfrak{g}_K$: indeed, let $\sigma \in \mathfrak{g}_K \setminus K^h$, so there is $x \in T(w) \setminus \sigma(T(w))$. Let L/K be a finite Galois extension with $x \in L$; then $T(w) \cap L \neq \sigma(T(w)) \cap N$. For $\tau \in \mathrm{Aut}(K^{\mathrm{sep}}/L)$ we have $\tau(T(w)) \cap L = T(w) \cap L$, so $(\sigma \circ \tau(T(w)) \neq T(w)$ and thus $\sigma\,\mathrm{Aut}(K^{\mathrm{sep}}/L)$ is an open subset of $\mathfrak{g}_K$ disjoint from $H^s(w)$. As w ranges over elements of $S(w|v)$, the subgroups $H^s(w)$ fill out a full conjugacy class in $\mathfrak{g}_K$, so $H^s(w)$ is normal in $\mathfrak{g}_K$ if and only if there is a unique extension of v to K^{sep} if and only if (K,v) is Henselian. Henceforth we fix one $w \in S(w|v)$ and put $H^s := H^s(w)$ and

$$K^h := (K^{\mathrm{sep}})^{H^s}.$$

Let v^h be the valuation with valuation ring $T(w) \cap K^h$. Thus K^h/K is a separable algebraic extension that is well-defined up to K-algebra isomorphism but is Galois over K if and only if (K,v) is Henselian.

THEOREM 16.16. *The extension $(K^h, v^h)/(K,v)$ be as above. Then:*

a) *The valued field (K^h, v^h) is Henselian.*
b) *If (L, v_L) is a Henselian extension of (K,v), then there is a unique embedding of valued K-algebras $(L, v_L) \hookrightarrow (K^h, v^h)$.*
c) *The extension $(K^h, v^k)/(K,v)$ is an immediate extension.*

*In view of these properties, we call (K^h, v^h) the **Henselization** of (K,v).*

PROOF. See [**EP**, Thm. 5.2.2 and Thm. 5.2.5]. □

THEOREM 16.17. *Let k be a field, and let Γ be an ordered commutative group. Then the Hahn series field $k((\Gamma))$ is Henselian.*

PROOF. See [**EP**, Exc. 3.5.5 and Exc. 3.5.6]. □

PROPOSITION 16.18. *Let (K, v) be a Henselian valued field. Then $X^v(K) = X(K)$: i.e., every ordering on K is compatible with v.*

PROOF. Let $(R, \mathfrak{m})$ be the valuation ring of v, and let P be an ordering on K. Seeking a contradiction, we suppose there are $c, d \in R$ with $0 < c < d$, $d \in \mathfrak{m}$ and $c \notin \mathfrak{m}$. Then $0 < \frac{d}{c} \in \mathfrak{m}$, so under the quotient map $q : R \to k$, the polynomial $t^2 + t + \frac{d}{c}$ maps to $t^2 + t$, which is separable and split in $k[t]$. By Hensel's Lemma there are $a, b \in K$ such that $(t+a)(t+b) = t^2 + t + \frac{d}{c}$, so $a + b = 1$ and $ab = \frac{d}{c} > 0$. Thus $0 \leq a, b \leq 1$, so $\frac{d}{c} = ab \leq 1$, i.e., $d \leq c$: contradiction. Thus $\mathfrak{m}$ is a P-convex subgroup of R, so Proposition 16.6 gives that v and P are compatible. □

THEOREM 16.19. *Let $v : K^\times \to \Gamma$ be a valuation on a field, with valuation ring R and formally real residue field k. Then K is real-closed if and only if all of the following hold:*

(i) *The residue field k is real-closed.*
(ii) *The value group Γ is divisible.*
(iii) *The valuation v is Henselian.*

PROOF. First suppose that K is real-closed. Then for all primes $p > 2$ we have $K^\times = K^{\times p}$, i.e., $K^\times$ is p-divisible, hence so is the quotient group $\Gamma = K^\times / R^\times$. Let $\gamma \in \Gamma$. Then there is $x \in K^\times$ such that $v(x) = v(-x) = \gamma$; since K is real-closed, one of x and $-x$ is a square. Replacing x with $-x$ if necessary, we may assume that $x = y^2$ for some $y \in K^\times$ and thus $\gamma = v(x) = v(y^2) = 2v(y)$, so Γ is 2-divisible: (ii) holds. Seeking a contradiction, suppose that k is not real-closed. Then there is a nontrivial finite degree extension l/k such that l is formally real. Formally real fields have characteristic 0, so $l \cong k[t]/(f)$ for a monic irreducible polynomial $f \in k[t]$. We may lift f to a monic polynomial $\tilde{f} \in R[t]$, which is again irreducible. By [**Cl-CA**, Cor. 15.25 and Cor. 16.19], the polynomial $\tilde{f}$ remains irreducible in $K[t]$, so it defines a nontrivial finite degree field extension L/K. For any extension of v to L, the residue field contains l, so by the Fundamental Inequality there is a unique extension of v to L. Since l is formally real we have $X(l) \neq \varnothing$, and thus by Theorem 16.13 also L is formally real. Since L/K is a nontrivial algebraic extension, this contradicts the fact that K is real-closed: (i) holds. If v were not Henselian, there would exist a nontrivial finite degree immediate extension $(L, w)/(K, v)$. Since L has residue field k, which is formally real, again Theorem 16.13 implies that L is formally real, contradicting the real-closedness of K.

Now suppose that (i), (ii) and (iii) hold. Since v is Henselian, by Proposition 16.18 and Theorem 16.13 we have that $X(K)$ is homeomorphic to $X := \{\pm 1\}^{\dim_{\mathbb{F}_2} \Gamma/2\Gamma} \times X(k)$, and since k is real-closed and Γ is 2-divisible, we have $\#X = 1$, that is K admits a unique ordering P. Seeking a contradiction, suppose that there is a nontrivial finite degree extension L/K that is formally real: then it admits an ordering P_L that must extend P (since P is the unique ordering on K). Since (K, v) is Henselian, the valuation v extends uniquely to a valuation w on L. Since L is also Henselian, we have that P_L and w are compatible, and thus the residue field l of L is formally real. But l/k is a finite degree extension and

k is real-closed, so $l = k$. Let Γ_v and Γ_w be the value groups of v and w, so $e(w|v) = [\Gamma_w : \Gamma_v] \leq [L : K] < \aleph_0$. Let $g \in \Gamma_w$. Then $e(w|v)g \in \Gamma_v$, and since Γ_v is divisible, there is $h \in \Gamma_v$ such that $e(w|v)g = e(w|v)h$. Since Γ_w is torsion-free, this implies $g = h \in \Gamma_v$, i.e., $\Gamma_v = \Gamma_w$. Thus $(L, w)/(K, v)$ is a nontrivial algebraic immediate extension, contradicting the Henselianity of (K, v). Thus K is real-closed. □

EXAMPLE 16.20. *Let K be any field of characteristic 0, and let p be a prime. By Proposition 16.2, the p-adic valuation on $\mathbb{Q}$ extends to a valuation v on K. (By* [**Cl-NTII**, Thm. 1.41]*, there is even a rank 1 extension.) Since $v(p) = 1 > 0$, the residue field of (K, v) has characteristic $p > 0$. In particular, every real-closed field admits a valuation whose residue field is not formally real, so this hypothesis in Theorem 16.19 is necessary in order for the residue field to be real-closed.*

The hypothesis about the formal reality of k applies when K is equipped with an ordering P that is compatible with v, by Proposition 16.6.

EXERCISE 16.17. *Let $v : K^\times \to \Gamma$ be a value field, with residue field k.*

a) *Suppose that K is algebraically closed. Show: K is Henselian, Γ is divisible and k is algebraically closed.*

b) *Suppose that K is Henselian, Γ is divisible and k is algebraically closed* of characteristic 0. *Use the structure theory of Henselian fields to show that K is algebraically closed.*[1]

c) *Let p be a prime, let k be an algebraically closed field of characteristic p, and let $P_k = \bigcup_{n=1}^{\infty} k((t^{1/n}))$ be the field of Puiseux series over k, which as an extension of $k((t))$ has a natural valuation $v : P_k^\times \to (\mathbb{Q}, +)$. Show: despite being Henselian, having divisible value group and algebraically closed residue field, the field P_k is* not *algebraically closed.*

It follows from Exercise 16.17b) that if k is an algebraically closed field of characteristic 0 and Γ is a divisible ordered commutative group, then the Hahn series field $k((\Gamma))$ is algebraically closed. In fact, it is a theorem of Mac Lane [**Mac39b**] that if Γ is divisible and k is *any* algebraically closed field, then the Hahn series field $k((\Gamma))$ is algebraically closed. Thus not only is the Hahn series field $k(((\mathbb{Q}, +)))$ larger than the Puiseux series field P_k, they are qualitatively different.

COROLLARY 16.21. *Let (K, P) be an ordered field, and let $v : K^\times \to \Omega(K)$ be its canonical valuation, with valuation ring R and ordered residue field (k, P_k). Let (K^h, v^h) be the Henselization of (K, v).*

a) *The following are equivalent:*
   (i) *The field K^h is real-closed.*
   (ii) *The residue field k is real-closed and the value group $\Omega(K)$ is divisible.*

b) *Suppose that the equivalent conditions of part a) hold. Then P extends uniquely to an ordering P^h of K^h that is compatible with v^h.*

PROOF. a) Suppose K^h is real-closed. By Theorem 16.19, then its residue field is real-closed and its group is divisible, but by Theorem 16.16 the extension $(K^h, v^h)/(K, v)$ is immediate, so k is real-closed and $\Omega(K)$ is divisible. Conversely – and similarly – if k is real-closed and $\Omega(K)$ is divisible, then this means that the

[1] We saw a special case of this above when we asserted that valuation theory implies that the field of complex Puiseux series is algebraically closed.

Henselian valued field (K^h, v^h) has real-closed residue field and divisible valuation group, so K^h is real-closed by Theorem 16.19.
b) This follows immediately(!) from Corollary 16.14. □

EXERCISE 16.18. *Explain why Corollary 16.21 holds trivially when (K, P) is Archimedean.*

5. Counting non-Archimedean Real-Closed Fields

Corollary 16.21 gives us a means for building a large supply of non-Archimedean real-closed fields. Let us dispose of two preliminaries first.

EXERCISE 16.19. *Let F be a countably infinite field, and let V be an infinite-dimensional F-vector space. Show: $\#V = \dim_F V$.*

EXERCISE 16.20. *Let κ be an infinite cardinal, and let $L(\kappa)$ be the number of mututually non-isomorphic linear orderings on κ (or, if you prefer, on a set of size κ). In this exercise, we will compute $L(\kappa)$.*

a) *Suppose $\kappa < \aleph_0$. Show: $L(\kappa) = 1$.*
b) *Show: $L(\kappa) \leq 2^\kappa$.*
c) *Suppose $\kappa \geq \aleph_0$. We will show $L(\kappa) \geq 2^\kappa$ and thus deduce: $L(\kappa) = 2^\kappa$. For a subset $T \subseteq \kappa$ and $x \in \kappa$, let S_x be the ordered set $\mathbb{Z}$ if $x \in T$ and the ordered set $\{0\}$ otherwise, and let $(S_T, \leq)$ be the disjoint union $\coprod_{x \in \kappa} S_x$, with each S_x given its order as above and such that for all $x_1 < x_2$, every element of S_{x_1} is less than every element of S_{x_2}.*
   (i) *Show: S_T is a linearly ordered set of cardinality κ.*
   (ii) *Show: For subsets T_1 and T_2 of κ, the sets S_{T_1} and S_{T_2} are order-isomorphic if and only if $T_1 = T_2$.*

Let S be an infinite linearly ordered set, and let $\Gamma(S) := \bigoplus_S (\mathbb{Q}, +)$ be the direct sum of S copies of $(\mathbb{Q}, +)$, lexicographically ordered. By Exercise 13.8 we have $\Omega(\Gamma(S))$ is order-isomorphic to the order dual $S^\vee$ of S, so if S_1 and S_2 are non-isomorphic linearly ordered sets, then $\Gamma(S_1)$ and $\Gamma(S_2)$ are not isomorphic as ordered commutative groups. Let $\mathcal{R}$ be the field of real-algebraic numbers, which is real-closed, Archimedean and of cardinality $\aleph_0$. The Hahn series field

$$H(S) := \mathcal{R}((\Gamma(S)))$$

is a non-Archimedean ordered field; equipped with its canonical valuation $v : H(S) \to \Gamma(S)$ it is Henselian by Theorem 16.17 and thus real-closed by Theorem 16.19. If the fields $H(S_1)$ and $H(S_2)$ are isomorphic, then the value groups of their canonical valuations are isomorphic, and thus the sets of Archimedean equivalence classes of these value groups are isomorphic (here we have passed to Archimedean equivalence classes twice!), so $S_1^\vee$ and $S_2^\vee$ are order-isomorphic, hence also S_1 and S_2 are order-isomorphic. Thus we have produced *many* non-isomorphic non-Archimedean real-closed fields.

However, we want to make one modification to this construction to better control the cardinality of the fields we produce. Namely, inside the Hahn series field $H(S)$ we have the group ring $\mathcal{R}[\Gamma(S)]$, whose elements are formal emphfinite $\mathcal{R}$-linear combinations of elements of $\Gamma(S)$. Let $\mathcal{R}(\Gamma(S))$ be the fraction field of $\mathcal{R}[\Gamma(S)]$, which is a subfield of $H(S)$. Since $\Gamma(S)$ is a $\mathcal{R}$-basis for $\mathcal{R}[\Gamma(S)]$, by

Exercise 16.19 we have

$$\#\mathcal{R}(\Gamma(S)) = \#\mathcal{R}[\Gamma(S)] = \#\Gamma(S) = \#S.$$

Since for all $\gamma \in \Gamma(S)$ we have $t^\gamma \in \mathcal{R}(\Gamma(S))$ and $v(t^\gamma) = \gamma$, the restriction of v to $\mathcal{R}(\Gamma(S))$ still has value group $\Gamma(S)$. Let us denote this restricted valuation by v_0. Similarly, for each $x \in \mathcal{R}$, we have $x = x \cdot t^0 \in \mathcal{R}(\Gamma(S))$ and if T is the valuation ring of $H(S)$ and $q : R \to \mathcal{R}$ is the quotient modulo the maximal ideal, then $q(x) = x$, so the residue field of $(\mathcal{R}(\Gamma(S)), v_0)$ is still $\mathcal{R}$. Finally, let $F(S)$ be the Henselization of $(\mathcal{R}(\Gamma(S)), v_0)$, and denote its valuation by v_h. As an algebraic extension of an infinite field, we have

$$\#F(S) = \#\mathcal{R}(\Gamma(S)) = \#S.$$

By Corollary 16.21, the field $F(S)$ is real-closed and by Theorem 16.16 its value group is still $\Gamma(S)$, so as above, if the non-Archimedean real-closed fields $F(S_1)$ and $F(S_2)$ are isomorphic, then S_1 and S_2 are order-isomorphic. Applying Exercise 16.20 and observing that of course there are no more than 2^κ isomorphism classes of fields of cardinality κ, we have proved the final result of this text:

THEOREM 16.22. *Let κ be an infinite cardinal. Then the number of isomorphism classes of non-Archimedean real-closed fields of cardinality κ is 2^κ.*

A little reflection on the construction shows that the Hahn series fields $\mathcal{R}(\Gamma((S)))$ were not really used at all. So if the purpose of this chapter was to prove Theorem 16.22, then our entire discussion of Hahn series fields was a red herring. However, this is a text on field theory that does not shy away from transfinite constructions, and Hahn series fields are a highly interesting and important class of transfinitely cosntructed fields, so we were happy to introduce them.

Bibliography

[Al] N.L. Alling, *Foundations of analysis over surreal number fields.* North-Holland Mathematics Studies, 141. Notas de Matemática [Mathematical Notes], 117. North-Holland Publishing Co., Amsterdam, 1987.

[Al18] M. Aliabadi, *A note on the fundamental theorem of algebra.* Bull. Aust. Math. Soc. 97 (2018), 382—385.

[Ap70] T.M. Apostol, *Resultants of cyclotomic polynomials.* Proc. Amer. Math. Soc. 24 (1970), 457–462.

[Ar] E. Artin, *Galois Theory.* Second edition. Notre Dame Mathematical Lectures, no. 2. University of Notre Dame, Notre Dame, Ind., 1944.

[BAI] N. Jacobson, *Basic algebra. I.* Second edition. W. H. Freeman and Company, New York, 1985.

[BAII] N. Jacobson, *Basic algebra. II.* Second edition. W. H. Freeman and Company, New York, 1989.

[Bar51] D. Barbilian, *Solution exhaustive du problème de Steinitz.* Acad. Repub. Pop. Romîne. Stud. Cerc. Mat. 2, (1951). 195–259 (misprinted 189–253).

[Ba70] R. Baer, *Die Automorphismengruppe eines algebraisch abgeschlossenen Körpers der Charakterkistik 0.* Math. Z. 117 (1970), 7–17.

[vBCEKSV25] R. van Bommel, E. Costa, N.D. Elkies, T. Keller, S. Schiavone and J. Voight, *17T7 is a Galois group over the rationals.* `https://arxiv.org/pdf/2411.07857`

[BCP86] R. Brown, T.C. Craven and M.J. Pelling, *Ordered fields satisfying Rolle's theorem.* Illinois J. Math. 30 (1986), 66–78.

[Be78] E.R. Berlekamp, *An analog to the discriminant over fields of characteristic two.* J. Algebra 38 (1976), 315—317.

[BJ01] F. Borceux and G. Janelidze, *Galois theories.* Cambridge Studies in Advanced Mathematics, 72. Cambridge University Press, Cambridge, 2001.

[BM83] G. Butler and J. McKay, *The transitive groups of degree up to eleven.* Comm. Algebra 11 (1983), 863–911.

[Br10] D. Brink, *Hölder continuity of roots of complex and p-adic polynomials.* Comm. Algebra 38 (2010), 1658—1662.

[BSCM25] A. Barquero-Sanchez and J. Calvo-Monge, *On the embedding of Galois groups into wreath products.* Comm. Algebra 53 (2025), 730–760.

[Ca53] L. Carlitz, *A theorem of Stickelberger.* Math. Scand. 1 (1953), 82–84.

[Ca14] D. Carmon, *The autocorrelation of the Möbius function and and Chowla's conjecture for the rational function field in characteristic* 2. `https://arxiv.org/pdf/1409.3694`

[CC77] T. Craven and G. Csordas, *Multiplier sequences for fields.* Illinois J. Math. 21 (1977), 801–817.

[CG72] C.H. Clemens and P.A. Griffiths, *The intermediate Jacobian of the cubic threefold.* Ann. of Math. (2) 95 (1972), 281–356.

[Ch] P.M. Cohn, *Basic algebra. Groups, rings and fields.* Springer-Verlag London, Ltd., London, 2003.

[Ch70] A. Charnow, *The automorphisms of an algebraically closed field.* Canad. Math. Bull. 13 (1970), 95–97.

[Cl-CA] P.L. Clark, *Commutative Algebra.* `http://math.uga.edu/~pete/integral2015.pdf`

[Cl-GT] P.L. Clark, *General Topology.* `https://plclark.github.io/PeteLClark/Expositions/pointset.pdf`

[Cl-NT] P.L. Clark, *Number Theory: A Contemporary Introduction*. http://math.uga.edu/~pete/4400FULL.pdf

[CL-NTI] P.L. Clark, *Algebraic Number Theory I*. https://plclark.github.io/PeteLClark/Expositions/ANT24.pdf

[Cl-NTII] P.L. Clark, *Algebraic Number Theory II: Valuations, Local Fields and Adeles*. http://math.uga.edu/~pete/8410FULL.pdf

[Cl-QF] P.L. Clark, *Lecture notes on quadratic forms*. http://alpha.math.uga.edu/~pete/quadraticforms0.pdf

[Cl12] P.L. Clark, *Covering numbers in linear algbera*.Amer. Math. Monthly 119 (2012), 65—67.

[Cl54] A.H. Clifford, *Note on Hahn's theorem on ordered commutative groups.* Proc. Amer. Math. Soc. 5 (1954), 860–863.

[Co53] P.F. Conrad, *Embedding theorems for commutative groups with valuations.* Amer. J. Math. 75 (1953), 1–29.

[Co-CQ] K. Conrad, *Galois groups of cubics and quartics in all characteristics*. https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquarticallchar.pdf

[Co-SA] K. Conrad, *Recognizing Galois groups S_n and A_n*. https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisSnAn.pdf

[Cr75] T.C. Craven, *The Boolean space of orderings of a field.* Trans. Amer. Math. Soc. 209 (1975), 225–235.

[Cr97] T.C. Craven, *A weak version of Rolle's theorem* Proc. Amer. Math. Soc. 125 (1997), 3147—3153.

[CW50] J.W.S. Cassels and G.E. Wall, *The normal basis theorem.* J. London Math. Soc. 25 (1950), 259–264.

[Cx] D.A. Cox, *Galois theory.* Second edition. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2012.

[DF] D.S. Dummit and R.M. Foote, *Abstract algebra.* Third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[DG94] M. Dugas and R. Göbel, *Automorphism groups of fields.* Manuscripta Math. 85 (1994), no. 3-4, 227–242.

[Di74] J. Dieudonné, *Sur les automorphismes des corps algébriquement clos.* Bol. Soc. Brasil. Mat. 5 (1974), 123–126.

[DM] J.D. Dixon and B. Mortimer, *Permutation groups.* Graduate Texts in Mathematics, 163. Springer-Verlag, New York, 1996.

[Du91] D.S. Dummit, *Solving solvable quintics.* Math. Comp. 57 (1991), 387–401.

[DW] H.G. Dales and W. H. Woodin, *Super-real fields. Totally ordered fields with additional structure.* London Mathematical Society Monographs. New Series, 14. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1996.

[EP] A.J. Engler and A. Prestel, *Valued fields.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[Fa61] C. Faith, *Derivations and generations of finite extensions.* Bull. Amer. Math. Soc. 67 (1961), 550—553.

[FGS71] B. Fine, B. Gordon and J.H. Smith, *On the representation of -1 as a sum of two squares in an algebraic number field.* J. Number Theory 3 (1971), 310-–315.

[FJ] M.D. Fried and M. Jarden, *Field arithmetic.* Fourth edition. Revised by Moshe Jarden. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 11. Springer, Cham, 2023.

[Gi68] R. Gilmer, *Classroom Notes: A Note on the Algebraic Closure of a Field.* Amer. Math. Monthly 75 (1968), 1101—1102.

[Gr55] K.A.H. Gravett, *Valued linear spaces.* Quart. J. Math. Oxford Ser. (2) 6 (1955), 309–315.

[Gr56] K.A.H. Gravett, *Ordered commutative groups.* Quart. J. Math. Oxford Ser. (2) 7 (1956), 57–63.

[Ha07] H. Hahn, *Über die nichtarchimedischen Größensysteme.* Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Wien, Mathematisch - Naturwissenschaftliche Klasse (Wien. Ber.) 116 (1907), 601–655.

[Hi92] D. Hilbert, *Ueber die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten* J. CreHe 110 (1892), 104–129.

[Hö01] O. Hölder, *Die Axiome der Quantitat und die Lehre vom Mass*. Ber. Verh. Sachs. Ges. Wiss. Leipzig, Math.-Phys. Cl. 53 (1901), 1–64.

[Ho20] X.-D. Hou, $\mathrm{PGL}_2(\mathbb{F}_q)$ *acting on* $\mathbb{F}_q(x)$. Comm. Algebra 48 (2020), 1640–1649.

[HR] E. Hewitt and K.A. Ross, *Abstract harmonic analysis. Vol. I: Structure of topological groups. Integration theory, group representations*. Die Grundlehren der mathematischen Wissenschaften, Band 115. Springer-Verlag, Berlin-Göttingen-Heidelberg; Academic Press, Inc., Publishers, New York, 1963.

[HSTT] Handbook of set-theoretic topology. Edited by Kenneth Kunen and Jerry E. Vaughan. North-Holland Publishing Co., Amsterdam, 1984.

[IM98] I.M. Isaacs and D.P. Moulton, *Real fields and repeated radical extensions.* J. Algebra 201 (1998), 429–455.

[In56] A. W. Ingleton, *The rank of circulant matrices.* J. London Math. Soc. 31 (1956), 632—635.

[Is80] I.M. Isaacs, *Roots of polynomials in algebraic extensions of fields*. Amer. Math. Monthly 87 (1980), 543–544.

[Is85] I.M. Isaacs, *Solution of polynomials by real radicals.* Amer. Math. Monthly 92 (1985), 571-–575.

[Ja1] N. Jacobson, *Basic algebra. I.* Second edition. W. H. Freeman and Company, New York, 1985.

[Ja2] N. Jacobson, *Basic algebra. II.* Second edition. W. H. Freeman and Company, New York, 1989.

[Ja37] N. Jacobson, *Abstract derivation and Lie algebras.* Trans. Amer. Math. Soc. 42 (1937), 206—224.

[Ja44] N. Jacobson, *Galois theory of purely inseparable fields of exponent one.* Amer. J. Math. 66 (1944), 645—648.

[Je] T.J. Jech, *The axiom of choice.* Studies in Logic and the Foundations of Mathematics, Vol. 75. North-Holland Publishing Co., New York, 1973.

[JV90] E.T. Jacobson and W.Y. Vélez, *The Galois group of a radical extension of the rationals.* Manuscripta Math. 67 (1990), 271—284.

[JY82] C.U. Jensen and N. Yui, *Polynomials with* D_p *as Galois group.* J. Number Theory 15 (1982), 347—375.

[Ka00] M.-c. Kang, *Cubic fields and radical extensions.* Amer. Math. Monthly 107 (2000), 254–256.

[Kap95] I. Kaplansky, *Fields and rings.* Reprint of the second (1972) edition. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1995.

[Kh09] A. Khare, *Vector spaces as unions of proper subspaces.* Linear Algebra Appl. 431 (2009), 1681—1686.

[Ki13] J.A. Kiehlmann, *Classifications of countably-based abelian profinite groups.* J. Group Theory 16 (2013), 141—157.

[Ko05] J. Koenigsmann, *Products of absolute Galois groups.* Int. Math. Res. Not. 2005, no. 24, 1465–1486.

[Kr] G. Karpilovsky, *Topics in field theory*. North-Holland Mathematics Studies, 155. Notas de Matematica [Mathematical Notes], 124. North-Holland Publishing Co., Amsterdam, 1989.

[Kr53] W. Krull, *Über eine Verallgemeinerung des Normalkörperbegriffs*. J. Reine Angew. Math. 191 (1953), 54–63.

[KW89] L.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial.* Amer. Math. Monthly 96 (1989), 133—137.

[La] S. Lang, *Algebra*. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[La53] S. Lang, *The theory of real places.* Ann. of Math. (2) 57 (1953), 378–391.

[Le55] H. Leptin, *Ein Darstellungssatz für kompakte, total unzusammenhngende Gruppen*. Arch. Math. (Basel) 6 (1955), 371–373.

[Lev43] F.W. Levi, *Contributions to the theory of ordered groups*. Proc. Indian Acad. Sci., Sect. A. 17 (1943), 199–201.

[Li66] J. Lipman, *Balanced field extensions.* Amer. Math. Monthly 73 (1966), 373–374.

[LoI] F. Lorenz, *Algebra. Vol. I. Fields and Galois theory.* Translated from the 1987 German edition by Silvio Levy. With the collaboration of Levy. Universitext. Springer, New York, 2006.

[LoII] F. Lorenz, *Algebra. Vol. II. Fields with structure, algebras and advanced topics.* Translated from the German by Silvio Levy. With the collaboration of Levy. Universitext. Springer, New York, 2008.

[Ma64] H.B. Mann, *On the casus irreducibilis.* Amer. Math. Monthly 71 (1964), 289–290.

[Mac39a] S. Mac Lane, *Steinitz field towers for modular fields.* Trans. Amer. Math. Soc. 46, (1939). 23–45.

[Mac39b] S. Mac Lane, *The universality of formal power series fields.* Bull. Amer. Math. Soc. 45 (1939), 888–890.

[Mi] J.S, Milne, *Fields and Galois theory.* `https://www.jmilne.org/math/CourseNotes/FT.pdf`

[Mo] P. Morandi, *Field and Galois theory.* Graduate Texts in Mathematics, 167. Springer-Verlag, New York, 1996.

[MS25] D. Marker and C. Steinhorn, *Rigid real closed fields.* `https://arxiv.org/pdf/2407.00542v2`

[Ne49] B.H. Neumann, *On ordered division rings.* Trans. Amer. Math. Soc. 66 (1949), 202–252.

[Ni39] I. Niven, *The transcendence of* π. Amer. Math. Monthly 46 (1939), 469–471.

[NS07] N. Nikolov and D. Segal, *On finitely generated profinite groups. I. Strong completeness and uniform bounds.* Ann. of Math. (2) 165 (2007), 171—238.

[Pa74] T. Parker, *Some applications of Galois theory to normal polynomials.* Amer. Math. Monthly 81 (1974), 1009–1011.

[Pe81] M.J. Pelling, *Solution of advanced problem No. 5861*, Amer. Math. Monthly, vol. 88 (1981). pp. 150-152.

[Pi09] D. Pierce, `https://dialinf.wordpress.com/2009/08/28/completions-and-the-archimedean-property/`

[Po74] B. Poizat, *Groupes profinis et théorie de Galois.* C. R. Acad. Sci. Paris Sér. A 278 (1974), 121—124.

[Rm] S. Roman, *Field theory.* Second edition. Graduate Texts in Mathematics, 158. Springer, New York, 2006.

[Rt] J. Rotman, *Galois theory.* Second edition. Universitext. Springer-Verlag, New York, 1998.

[RS] L. Ribes and P. Zalesskii, *Profinite groups.* Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 40. Springer-Verlag, Berlin, 2010.

[Sc92] B. Schnor, *Involutions in the group of automorphisms of an algebraically closed field.* J. Algebra 152 (1992), 520–524.

[Se] J.-P. Serre, *Topics in Galois theory.* Second edition. With notes by Henri Darmon. Research Notes in Mathematics, 1. A K Peters, Ltd., Wellesley, MA, 2008.

[Sh54] I.R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group.* Izv. Akad. Nauk SSSR Ser. Mat. 18 (1954), 525—578.

[Sh07] J. Shipman, *Improving the fundamental theorem of algebra.* Math. Intelligencer 29 (2007), 9—14.

[SM85] L. Soicher and J. McKay, *Computing Galois groups over the rationals.* J. Number Theory 20 (1985), 273—281.

[Si] J.H. Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[Sp52] T.A. Springer, *Sur les formes quadratiques d'indice zéro.* C. R. Acad. Sci. Paris 234 (1952), 1517–1519.

[St10] E. Steinitz, *Algebrasiche Theorie der Körper.* Journal für die reine und angewandte Mathematik, 1910.

[Su99] B. Sury, *On an example of Jacobson.* Amer. Math. Monthly 106 (1999), 675-–676.

[SW98] A. Schmidt and K. Wingberg, *Safarevic's theorem on solvable groups as Galois groups.* `https://arxiv.org/abs/math/9809211`

[Su15] N. Sutherland, *Computing Galois groups of polynomials (especially over function fields of prime characteristic).* J. Symbolic Comput. 71 (2015), 73—97.

[Sw62] R.G. Swan, *Factorization of polynomials over finite fields.* Pacific J. Math. 12 (1962), 1099–1106.

[Sw68] M.E. Sweedler, *Structure of inseparable extensions.* Ann. of Math. (2) 87 (1968), 401—410.

[SZ67] J. Sonn and H. Zassenhaus, *On the theorem on the primitive element.* Amer. Math. Monthly 74 (1967), 407—410.

[Th84] J.G. Thompson, *Some finite groups which appear as* $\mathrm{Gal}(L/K)$*, where* $K \subseteq \mathbb{Q}(\mu_n)$. J. Algebra 89 (1984), no. 2, 437–499.

[vdW] B.L. van der Waerden, *Algebra. Vol. I.* Based in part on lectures by E. Artin and E. Noether. Translated from the seventh German edition by Fred Blum and John R. Schulenberger. Springer-Verlag, New York, 1991.

[Wa74] W.C. Waterhouse, *Profinite groups are Galois groups.* Proc. Amer. Math. Soc. 42 (1974), 639–640.

[Wa94] W.C. Waterhouse, *The normal closures of certain Kummer extensions.* Canad. Math. Bull. 37 (1994), 133–139.

[Wa04] W.C. Waterhouse, *Intersections of two cofinite subfields.* Arch. Math. (Basel) 82 (2004), 298–300.

[We] S.H. Weintraub, *Galois theory.* Second edition. Universitext. Springer, New York, 2009.

[We21] S.H. Weintraub, *The theorem of the primitive element.* Amer. Math. Monthly 128 (2021), 753–754.

[Wi] S. Willard, *General topology.* Reprint of the 1970 original. Dover Publications, Inc., Mineola, NY, 2004.

[Ya66] P.B. Yale, *Automorphisms of the Complex Numbers.* Math. Magazine 39 (1966), 135–141.

[Za58] O. Zariski, *On Castelnuovo's criterion of rationality* $p_a = P_2 = 0$ *of an algebraic surface.* Illinois J. Math. 2 (1958), 303–315.

[ZSI] O. Zariski and P. Samuel, *Commutative algebra. Vol. 1. With the cooperation of I. S. Cohen.* Corrected reprinting of the 1958 edition. Graduate Texts in Mathematics, No. 28. Springer-Verlag, New York-Heidelberg-Berlin, 1975.

[Zy15] D. Zywina, *The inverse Galois problem for* $\mathrm{PSL}_2(\mathbb{F}_p)$. Duke Math. J. 164 (2015), 2253—2292.