Chapter 1

Review

01/21/20

The following topics from previous courses are assumed to be known. If needed, review this material on your own. You can find review material on our current textbook [3], and in the textbook for previous course [2].

1.1 Groups

The following definition, is somewhat different from, although equivalent to, the usual definition of a group.

Definition 1.1 A *group* consists of a non-empty set G with three operations:

- a *binary* operation, denoted by $\_ \cdot \_$, called the group multiplication,
- a *unary* operation, denoted by $\_^{-1}$, called the inverse operation, and
- a *nullary* operation, or constant, denoted by 1 or e, called the identity element of G.

Moreover, these operation must satisfy the following identities:

Associativity $x \cdot (y \cdot z) = (x \cdot y) \cdot z$,

Identity element $x \cdot 1 = 1 \cdot x = x$,

Inverse elements $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

When we refer to the above as *identities*, we mean they are formulas *universally quantified* on all their variables.

The purpose of this modified version, is to avoid existential statements in the definition. Universal statements tend to behave better than existential statements under some algebraic constructions. In the standard definition, the uniqueness of the identity element, and the uniqueness of the inverse of an element, are not part of the definition, and they follow from it. In our definition, the uniqueness is built-in as inverse and identity element are defined as operations.

Note that an n-ary operation, is a function that takes n arguments and produces one (unique) result for those arguments. A zero-ary operation takes no arguments and produces one result; in other words, a zero-ary or nullary operation selects one element from G.

1.1.1 Subgroup Lattice

Definition 1.2 Given a group G, the collection of subgroups of G, denoted $\mathrm{Sub}(G)$ is called the *subgroup lattice* of G.

Definition 1.3 Given a group G, the collection of normal subgroups of G, denoted $\mathrm{Nor}(G)$ is called the *normal subgroup lattice* of G.

The word *lattice* has a technical meaning, and hidden in the previous definitions, are a couple of theorems that state $\mathrm{Sub}(G)$ and $\mathrm{Nor}(G)$ are indeed lattices. More on this later.

1.1.2 Isomorphism Theorems

The naming/numbering of the isomorphism theorems varies from one author to another. Here is a table comparing our notation with that of Dummit & Foot[2] and Grillet [3].

Our	**Dummit & Foote**[2]	**Grillet**[3]	**Other**
Factorization		Factorization	
First	First	Homomorphism	Isomorphism
Second	Second	Second	Diamond
Third	Third	First	Double quotient
Fourth	Fourth	Factorization*	Lattice
Fifth	Fourth**		

* The Factorization Theorem is only part of our Fourth Isomorphism Theorem.

** Dummit & Foote combine our Fourth and Fifth Isomorphism Theorems into a single one.

Theorem 1.1 [Factorization Theorem] *Let G be a group and N a normal subgroup of G. For any group homomorphism $\varphi : G \to H$, φ factors through the quotient map $q : G \to G/N$ iff $N \leq \ker(\varphi)$. When this is the case, the factorization is unique.*

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "q"'] & H \\ G/N \arrow[ur, dashed, "\exists!\psi"'] & \end{tikzcd}$$

Exercise 1.1.1 Prove Theorem 1.1.

There is a *set theoretic* version of this theorem. it requires we define the *kernel* of any function $f : A \to B$ as:

$$\ker(f) := \{(a_1, a_2) \in A \times A | f(a_1) = f(a_2)\} \tag{1.1}$$

Exercise 1.1.2 let A, B be sets and $f : A \to B$ a function. Show that $\ker(f)$, as defined in (1.1) above, is an equivalence relation on A, and the

function f factors through the quotient map

$$\begin{array}{rccc} q: & A & \to & A/\ker(f) \\ & a & \mapsto & [a] \end{array}$$

where $[a]$ is the equivalence class of a under the equivalence relation $\ker(f)$.

The previous exercise is a special case of the following theorem.

Theorem 1.2 [Factorization Theorem (Set Version)] *Let A be a set and θ an equivalence relation on A. For any function $f : A \to B$, f factors through the quotient map $q : A \to A/\theta$ iff $\theta \leq \ker(f)$. When this is the case, the factorization is unique.*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "q"'] & B \\ A/\theta \arrow[ur, dashed, "\exists! g"'] & \end{tikzcd}$$

This set theoretic version has applications outside of algebra. For example, if A and B are topological spaces, and f is continuous, then g is continuous, when A/θ is given the quotient topology.

Exercise 1.1.3 Prove Theorem 1.2.

Theorem 1.3 [First Isomorphism Theorem] *If $\varphi : G \to H$ is a group homomorphism, then*

$$G/\ker(\varphi) \approx \mathrm{Im}(\varphi);$$

in fact, there is a unique isomorphism $\theta : G/\ker(\varphi) \to \mathrm{Im}(\varphi)$, such that $\varphi = \iota \circ \theta \circ q$.

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "q"'] & H \\ G/\ker(\varphi) \arrow[r, dashed, "\exists!\theta"'] & \mathrm{Im}(\varphi) \arrow[u, hook, "\iota"'] \end{tikzcd}$$

Exercise 1.1.4 Prove Theorem 1.3. Hint: use Theorem 1.1.

Theorem 1.4 [Second Isomorphism Theorem] *Let G be a group, N be a normal subgroup of G and H a subgroup of G. Then HN is a subgroup of G, N is normal in HN, $H \cap N$ is normal in H and*

$$HN/N \approx H/(H \cap N)$$

The following diagram is associated with this theorem, hence the name *Diamond Theorem*. Double lines indicate normality. Note that the statement is that the corresponding quotients are isomorphic. Theorem 1.4 holds with a weaker assumption. N doesn't have to be normal in G; it suffices that H normalizes N.

$$\begin{tikzcd}
 & G \arrow[d, dash] & \\
 & HN \arrow[dl, equal] \arrow[dr, dash] & \\
N \arrow[dr, dash] & & H \arrow[dl, equal] \\
 & H \cap N \arrow[d, dash] & \\
 & 1 &
\end{tikzcd}$$

Figure 1.1: Diamond Theorem

Theorem 1.5 [Third Isomorphism Theorem] *Let G be a group, N, M normal subgroups of G with $N \leq M$. Then*

$$G/M \approx \frac{(G/N)}{(M/N)}$$

The third isomorphism theorem, can be remembered as saying "*a quotient of a quotient is a quotient*". That is why it is sometimes refered to as the *double quotient theorem*.

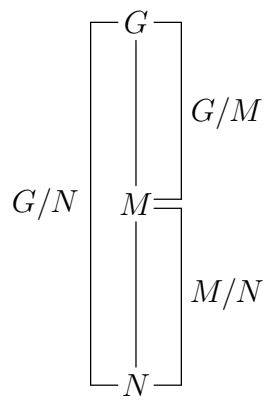


Figure 1.2: Double Quotient Theorem

For the next two theorems to make full sense, we need to know the definition of a lattice, and lattice homomorphisms. These can be found in Chapter 2 ahead. In the absence of those definitions, instead of isomorphism of lattices, the claim is of a bijective correspondence. Thus, the name *Correspondence Theorem* is sometimes used.

01/23/20 **Theorem 1.6 [Fourth Isomorphism Theorem]** *Let G be a group and N a normal subgroup of G. The lattice* $\mathrm{Sub}(G/N)$ *of subgroups of G/N is isomorphic to the interval $[N, G]$ in* $\mathrm{Sub}(G)$*. An isomorphism is given by*

$$\begin{array}{ccc} [N,G] & \to & \mathrm{Sub}(G/N), \\ M & \mapsto & M/N \end{array} \tag{1.2}$$

and this isomorphism preserves indices.

Theorem 1.7 [Fifth Isomorphism Theorem] *Let G be a group and N a normal subgroup of G. The lattice* $\mathrm{Nor}(G/N)$ *of normal subgroups of G/N is isomorphic to the interval $[N, G]$ in* $\mathrm{Nor}(G)$*. An isomorphism is given by the same map as in (1.2).*

Clearly, when it comes to groups, the fourth and fifth isomorphism theorems could be combined into a single theorem. The only reason to keep them separate, is that in other algebraic systems, quotients do not correspond to a special class of subs, as they do in groups. This can be seen in the case of rings, where quotients correspond to ideals; it is even more clear in the case of lattices, where one needs congruences to form quotients.

1.1.3 Commutators, Derived Subgroup

There are two different and non-equivalent definitions of "*commutators*". They both serve the same purpose, but they should not be combined with each other. Our choice follows Grillet's [3] notation. Dummit & Foote [2] use the other notation[1].

Definition 1.4 Let G be a group. For $x, y \in G$, the *commutator* of x and y is defined as:

$$[x, y] := xyx^{-1}y^{-1}$$

The *commutator subgroup* of G, denoted G' is the subgroup of G generated by the set of all commutators of elements of G. The commutator subgroup is also called the *derived subgroup* of G.

Remarks 1.1.1

1. Even though, the commutator of two elements is defined differently, the commutator subgroup is the same under the other definition. If we denote by ${}^{x}y$ the element xyx^{-1}, i.e. the result of the left conjugation on y by x, then the commutator

$$[x, y] = {}^{x}y \cdot y^{-1},$$

can be thought of as the "*difference*" between y and y acted on by x.

2. The inverse of a commutator is a commutator

$$[x, y]^{-1} = [y, x],$$

but the product of two commutators is not necessarily a commutator. So, the best we can say about elements of G' is that they are the product of commutators.

Lemma 1.8 *1. If $H \leq G$ then $H' \leq G'$.*

2. If $\varphi : G \to H$ is a homomorphism, then $\varphi\langle G'\rangle \leq H'$.

Theorem 1.9 *The commutator subgroup G' of a grup G is a normal subgroup of G. In fact, it is a characteristic subgroup of G, i.e. closed under all automorphisms of G. It is the smallest normal subgroup of G whose quotient is abelian. In other words, for a normal subgroup $N \trianglelefteq G$,*

$$G/N \quad \textit{is abelian iff} \quad G' \leq N.$$

[1] The other definition has $[x, y] = x^{-1}y^{-1}xy$

The derived subgroup G' of G is more than characteristic, it is a "*fully invariant*" subgroup, i.e. it is closed under all endomorphisms of G.

1.1.4 Solvable groups

Definition 1.5 The *commutator series* or *derived series* of G, denoted by $(G^{(n)}|n \geq 0)$, is defined recursevely by

$$G^{(0)} := G, \quad \text{and} \quad G^{(n+1)} := \left(G^{(n)}\right)'.$$

The group G is *solvable* if there is a k such that $G^{(k)} = 1$. The smallest such k is called the *derived length* or *solvable length* of G, and is denoted $l(G)$.

The only group of solvable length zero is the trivial group. Groups of solvable length 1 are precisely the non-trivial abelian groups. It is common practice by some authors to say "*solvable of length n*" meaning "*solvable of length $\leq n$*"; that way, one would say that abelian groups are precisely the groups of solvable length 1.

Proposition 1.10 *Let G be a group, $H \leq G$ and $N \trianglelefteq G$.*

1. *If G is solvable, then H is also solvable, and*

$$l(H) \leq l(G).$$

2. *G is solvable iff N and G/N are both solvable. In this case*

$$l(G) \leq l(N) + l(G/N).$$

Definition 1.6 A *normal series* of a group G is a series

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

Theorem 1.11 *A group is solvable iff it has a normal series with abelian factors.*

1.2 Commutative Rings

Here are some concepts and results from the course *Rings and Algebras* that we will be using. Throughout this section the term "ring" will mean *commutative ring with unity*.

1.2.1 Isomorphism Theorems

1.2.2 Polynomial Rings

The following theorem is called the "*Universal Mapping Theorem*" for polynomial rings.

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "\iota"'] & S \\ R[x] \arrow[ur, dashed, "\exists!\hat{\varphi}"] & a \arrow[ul, dashed] \\ x \arrow[u, mapsto] & \end{tikzcd}$$

Theorem 1.12 [Universal Mapping Theorem] *Let R and S be rings, $\varphi : R \to S$ a ring homomorphism, and $a \in S$ such that a commutes with $\varphi\langle R\rangle$. There is a unique homomorphism*

$$\hat{\varphi} : R[x] \to S,$$

such that

- *$\hat{\varphi}$ extends φ, i.e. for every $r \in R$, $\hat{\varphi}(r) = \varphi(r)$,*
- *$\hat{\varphi}(x) = a$.*

1.2.3 Integral Domains

Proposition 1.13 *Let D be an Integral Domain, and $M \lhd D$. M is a maximal ideal iff D/M is a field.*

Definition 1.7 Let $p \in D$ be a non-zero non-unit element (*nznu* for short).

1. We say p is *irreducible* if

$$p = ab \Rightarrow a \text{ is a unit, or } b \text{ is a unit.}$$

2. We say p is *prime* if

$$p|ab \Rightarrow p|a \text{ or } p|b, \quad \text{i.e.} \quad ab \in \langle p \rangle \Rightarrow a \in \langle p \rangle \text{ or } b \in \langle p \rangle.$$

Note 1.1 It is easy to check that *prime* implies *irreducible*.

1.2.4 Unique Factorization Domains

Lemma 1.14 *Let R be a UFD. An element of R is prime iff it is irreducible*

Lemma 1.15 *Any two elements of a UFD R have a greatest common divisor, unique up to associates.*

Definition 1.8 A polynomial $f(x) \in R[x]$ is *primitive* if the gcd of all coefficients is 1.

Proposition 1.16 [Eisenstein Criterion] *Let R be a UFD, and $f(x) \in R[x]$ a primitive polynomial. If there is $p \in R$ prime that divides all coefficients of $f(x)$, other than the leading coefficient, and p^2 does not divide the constant term, then $f(x)$ is irreducible.*

Lemma 1.17 [Gauss' Lemma] *Let R be a UFD. If $f(x), g(x) \in R[x]$ are primitive then their product $f(x)g(x)$ is also primitive.*

The following corollary is also known as Gauss's Lemma.

Corollary 1.18 *Let R be a UFD, and Q its field of fractions. For $f(x) \in R[x]$ a primitive polynommial, $f(x)$ is irreducible in $R[x]$ iff it is irreducible in $Q[x]$.*

1.2.5 Principal Ideal Domains

Proposition 1.19 *Let R be a PID, $a \in R$ and $I = \langle a \rangle$. I is a maximal ideal of R iff a is an irreducible element of R.*

1.2.6 Euclidean Domains

1.2.7 Fields

Theorem 1.20 $ID \gneq UFD \gneq PID \gneq ED \gneq Filds$

Theorem 1.21 *Let R be a ring and $R[x]$ its polynomial ring. The following table gives the best possible property for $R[x]$, given the property of R, among $\{ID, UFD, PID, ED, Field\}$.*

Coefficient Ring R	*Polynommial ring* $R[x]$
ID	*ID*
UFD	*UFD*
PID	*UFD*
ED	*UFD*
Field	*ED*

1.3 Vector Spaces

1.3.1 Bases, Dimension

Theorem 1.22 *Let V be a v.s. over a field F.*

1. *V has a basis.*

2. *Any two bases of V have the same cardinality.*

Proposition 1.23 *Let F be a field. The polynomial ring $F[x]$, as a vector space over F is infinite dimensional with basis*

$$\{x^i | i \geq 0\}.$$

1.4 Posets and Zorn's Lemma

01/28/20 **Definition 1.9**

- A partially ordered set, (*poset* for short), $(P, \leq)$ consists of a set P and a binary relation $\leq$ on P which is *reflexive*, *antisymmetric*, and *transitive*. When $\leq$ is implicitly understood from the context, we just say P is poset.
- A subset X of a poset P is itself a poset under the same order relation restricted to X.
- A *chain* is a poset (or a subset of a poset) in which every pair of elements x, y are *comparable*, i.e. either $x \leq y$ or $y \leq x$.
- An element $m \in P$ is said to be *maximal*, if for every $x \in P$,
$$m \leq x \Rightarrow m = x;$$
i.e. there is no element of P strictly larger than m.
- An element $m \in P$ is said to be *maximum* or *largest*, if $x \leq m$ for every $x \in P$.

Maximal elements don't need to exist, and when they do, they don't have to be unique.

Definition 1.10 Let P be a poset, and $X \subseteq P$. We say that $u \in P$ (resp. $l \in P$) is an upper (resp. lower) bound for X if $x \leq u$ (resp. $l \leq x$) for every $x \in X$.

Note 1.2 Note that an upper bound for X in P, does not have to belong to X. When it does, it is the largest element of X.

Theorem 1.24 [Zorn's Lemma] *Let P be a non-empty poset. If every non-empty chain in P has an upper bound, then P has a maximal element.*

Zorn's Lemma is equivalent to The Axiom of Choice, meaning that in standard set theory minus AC, either one can be proved assuming the other. ZL is in fact one of dozens of important statements throughout mathematics that are equivalent to AC.

Chapter 2

Lattices

In this chapter we have a brief discussion about lattices and complete lattices, with the material we will need in Chapter 4. We will alto touch on some basic ideas about Universal Algebras.

2.1 Equivalent Definitions

There are two alternative, and equivalent, ways to define the concept of *lattice*. The first is as a poset; the second as an algebraic system, i.e. a set with operations. Before we jump into the definition(s) of a lattice, we need a couple of poset concepts.

Definition 2.1 Let P be a poset, and $X \subseteq P$. We say that $u \in P$ is a *least upper bound* for X, if u is an upper bound for X and it is the smallest element in the set of all upper bounds for X, i.e.

- $(\forall x \in X)(x \leq u)$
- $(\forall x \in X)(x \leq v) \Rightarrow u \leq v$

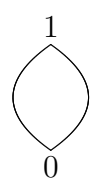
A dual definition can be given for *greatest lower bound* of a set.
The antisymmetric property guarantees that a least upper bound for a set X

is unique when it exist. In such case we denote it by l.u.b.(X) or by $\bigvee X$. However, a subset of a poset doesn't have to have a least upper bound. The greatest lower bound of X, when it exists, is denoted by g.l.b.(X) or by $\bigwedge X$.

Definition 2.2 [1st. Lattice Definition]

- A *lattice* is a non-empty partially ordered set L, in which every pair of elements have a l.u.b. and a g.l.b.. For $x, y \in L$, the l.u.b.$\{x, y\}$ is denoted $x \vee y$, and the g.l.b.$\{x.y\}$ is denoted $x \wedge y$.
- A *bounded lattice* is a lattice with largest and smallest element. The largest element is usually denoted by 1 and the smallest element by 0.

It follows easily by induction that in a lattice L, any **non-empty** finite subset has a l.u.b. and g.l.b.. As a consequence, any finite lattice is bounded. A generic picture of a bounded lattice:



For l.u.b.$(\emptyset)$ to exist, it is necessary and sufficient that L has a smallest element, and l.u.b.$(\emptyset)$ is that smallest element of L. Similarly, the existence of g.l.b.$(\emptyset)$ is equivalent to L having a largest element. Hence, in a bounded lattice every finite subset has a l.u.b. and g.l.b..

Every chain is a lattice, with the meet of two elements being the smaller and the join being the larger. In the bounded lattice

$$\left\{ \pm\frac{1}{n} \;\middle|\; n \in \mathbb{N} \right\}$$

not every subset has a l.u.b..

Notice that in a lattice L, $\vee$ and $\wedge$ can be thought of as binary operations. This gives rise to the second definition of a lattice.

Definition 2.3 [2nd. Lattice Definition] A *lattice* $(L, \vee, \wedge)$ consists of a non-empty set L and two binary operations $\vee$ and $\wedge$ that satisfy the following identities:

Associative	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	$(x \vee y) \vee z = x \vee (y \vee z)$
Commutative	$x \wedge y = y \wedge x$	$x \vee y = y \vee x$
Idempotent	$x \wedge x = x$	$x \vee x = x$
Absortion	$x \wedge (x \vee y) = x$	$x \vee (x \wedge y) = x$

A *bounded lattice* $(L, \vee, \wedge, 0, 1)$ consists of a non-empty set L, two binary operations $\vee$ and $\wedge$ and two nullary operations 0 and 1, satisfying the above identities plus the zero-element identities.

$$\textbf{Zero element} \qquad x \wedge 0 \;=\; 0 \qquad x \vee 1 \;=\; 1$$

Here is the statement about the equivalence of the two definitions of lattice.

Theorem 2.1

1. *Given a lattice $(L, \leq)$ in the poset sense, the meet and join, as binary operations, satisfy the identities in the second definition of lattice. Hence, $(L, \vee, \wedge)$ is a lattice in the algebraic sense.*

2. *Given a lattice $(L, \vee, \wedge)$ in the algebraic sense, the binary relation $\leq$ defined by*

$$x \leq y \quad \textit{iff} \quad x \wedge y = x$$

   is a partial order on L, and for $x, y \in L$, $x \wedge y$ is the g.l.b.$\{x, y\}$ *under this order, and $x \vee y$ is the* l.u.b.$\{x, y\}$. *Hence $(L, \leq)$ is a lattice in the poset sense.*

3. *Given a lattice $(L, \leq)$ in the poset sense, the partial order defined on $(L, \vee, \wedge)$ via Part 2 is the same as the original partial order on $(L, \leq)$.*

Proof. Ex. ■

The previous theorem shows not only that we can go from a lattice in one sense to a lattice in the other sense, but that going back and forth are inverse processes.

From now on, when we say lattice, we don't need to specify in what sense. We have both.

Examples 2.1.1

1. $(\mathbb{N}, \leq)$ is a lattice, bounded below, but not bounded above. It is a chain.
2. $(\mathbb{N}, |)$ is a bounded lattice, with smallest element 1 and largest element 0. In this lattice,

$$\text{l.u.b.}\{n, m\} = \text{l.c.m.}\{n, m\} \quad \text{and} \quad \text{g.l.b.}\{n, m\} = \text{g.c.d.}\{n, m\}.$$

Definition 2.4 Let $(P, \leq)$ be a poset. It is clear that the reverse order $\geq$ is also a partial order on P. The poset $(P, \geq)$ is called the *dual poset* of $(P, \leq)$. When $\leq$ is not explicitly mentioned with P, we denote the dual poset by P^o.

Lemma 2.2 *The dual of a lattice is a lattice.*

Metatheorem 2.3 [Duality Principle for Posets] *If a statement S in the language of posets holds true for all posets, then the dual statement S^o, obtained from S by reversing all inequalities, also holds true for all posets.*

Metatheorem 2.4 [Duality Principle for Lattices] *If a statement S in the language of lattices holds true for all lattices, then the dual statement S^o, obtained from S by reversing all inequalities and exchanging all meets and joins, also holds true for all lattices.*

The next two propositions illustrate the use of this duality principle. They are both related to the distributive property. Even though distributivity does not hold in every lattice, Proposition 2.5 shows that half of it does. The second part of this proposition follows from the first by the duality principle.

Proposition 2.5 *Let L be a lattice, and $x, y, z \in L$.*

1. $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$
2. $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$

Proof. Ex. ■

Most ideas related to lattices can be expressed using either the partial order, or the operations. Depending on the idea, one of them, or a combination of both, will be more appropriate. The ideas of sublattice, and lattice homomorphism, are better expressed in algebraic terms. 01/30/20

Definition 2.5 A *sublattice* of a lattice L is a non-empty subset M which is closed under meets and joins.

Examples 2.1.2

1. Not every subposet of a lattice is a lattice. Even when it is a lattice, its meet and join operations may differ from those of the bigger lattice. Consider the poset L in Figure 1.2 for the Diamond Isomorphism Theorem, which is a lattice. The subset $X = \{N, H\}$ is not a lattice. The subset $Y = \{1, N, H, G\}$, is a lattice, but it is not a sublattice of L; the meet of N and H in L is NH, whereas their join in Y is G.

2. The subset $M = \{N, H, NH, N \cap H\}$ of the lattice L in Figure 1.2 is a sublattice

Definition 2.6 Given two lattices L and M, a map $\varphi : L \to M$ is said to be a *lattice homomorphism* if it preserves the operations, meet and join. For two bounded lattices a homomorphism is required to preserve also the two constants 0 and 1.
As with other algebraic objects, lattice morphism come in six flavors: homo, mono, epi, iso, endo and auto.

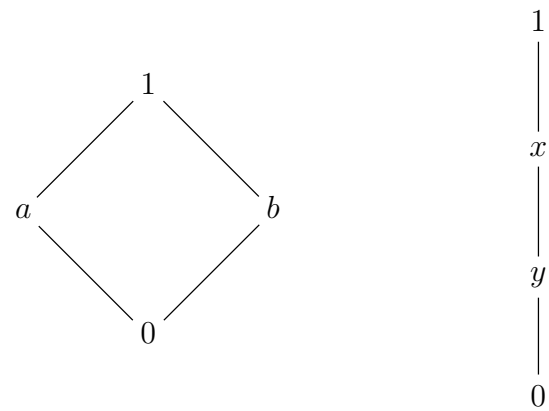
Examples 2.1.3

1. The embedding of $\{N, H, NH, N \cap H\}$ into the lattice L of Figure 1.2 is a lattice homomorphism, but not a bounded lattice homomorphism. The bottom line is that preservation of some of the operations does not imply preservation of all of them. This is unlike the case of groups, where the preservation of the binary operation implies the preservation of the unary and the nullary operations.

2. A lattice homomorphism has to be isotone, i.e., preserve the order. However, being isotone is not enough to be a homomorphism. Consider the two lattices in Figure 2.1 below, and the map

$$\varphi : 1 \mapsto 1, a \mapsto x, b \mapsto y, 0 \mapsto 0.$$

Figure 2.1: Bijective, isotone but not an isomorphism



It is an order-preserving map, but it is not a lattice homomorphism. Even though it is a bijection, it is not a lattice or poset isomorphism.

Proposition 2.6 *Consider the two distributive laws (identities)*

$$\begin{aligned} x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z) \\ x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z) \end{aligned}$$

A lattice L satisfies one of the distributive identities iff it satisfies the other one. Such lattice is called distributive.

Proof. One direction is proved directly (exercise). The other direction follows by the duality principle. ■

2.2 Complete Lattices

Definition 2.7 A *complete lattice* is a poset L in which every subset has a l.u.b. and ag.l.b..

Clearly, every complete lattice is a lattice and every finite lattice is a complete lattice. Not every lattice is complete as illustrated by $(\mathbb{N}, \leq)$.

The following proposition shows that Definition 2.7 is redundant.

Proposition 2.7 *If L is a poset in which every subset has a* l.u.b.*, then every subset of L also has a* g.l.b.*. Hence L is a complete lattice. Dually, if every subset of L has a* g.l.b.*, then every subset also has a* l.u.b.*.*

Proof. Ex. ■

Examples 2.2.1

1. $(\mathbb{N}, |)$ is a complete lattice. The join of any infinite subset is 0.
2. For a group G, $\mathrm{Sub}(G)$ is a complete lattice. The order is inclusion and the meet of any collection of subgroups of G is equal to their intersection. For $H_1, H_2 \leq G$, the join $H_1 \vee H_2$ is the smallest subgroup of G containing both H_1 and H_2, i.e. the subgroup $\langle H_1 \cup H_2 \rangle$, generated by their union. In fact, for any collection $(H_i | i \in I)$ of subgroups of G,
$$\bigvee_{i \in I} H_i = \left\langle \bigcup_{i \in I} H_i \right\rangle.$$
3. For a group G, $\mathrm{Nor}(G)$ is a complete lattice. The order is inclusion and the meet of any collection of subgroups of G is equal to their intersection. For $N_1, N_2 \leq G$, the join $N_1 \vee N_2$ is their product $N_1 N_2$.

2.3 Universal Algebras and Closure Systems

The two examples at the end of last section are a special case of a more general situation.

Definition 2.8 Let S be a set. A collection $\mathcal{F}$ of subsets of S is called a *closure system* on S if it is closed under arbitrary intersections. The elements of $\mathcal{F}$ are called *closed subsets* of S. Given $X \subseteq S$, the smallest closed subset of S that contains X is called the *closure* of X.

Since the intersection of the empty collection of subsets of S is equal to S, any closure system $\mathcal{F}$ on S is required to have S as an element, hence be non-empty. It follows immediately from Proposition 2.7 that

Corollary 2.8 *Given a closure system on S, the closed subsets of S form a complete lattice with intersection as the meet.*

Examples 2.3.1

1. The closed sets of a topological space form a closure system.
2. For any set S, $\mathcal{P}(S)$ is a closure system. All subsets are closed.
3. For any set S, $\mathcal{P}_f(S) \cup \{S\}$ is a closure system. Any finite set is closed. The closure of an infinite subset if all of S.
4. For a group G, the collections $\mathrm{Sub}(G)$ and $\mathrm{Nor}(G)$ are closure systems. Given $X \subseteq G$, the closure of X in $\mathrm{Sub}(G)$ is $\langle X \rangle$, the subgroup generated by X; the closure in $\mathrm{Nor}(G)$ is $\langle X^G \rangle$, the normal subgroup generated by X.
5. For any ring R, the collection $\mathrm{Sub}(R)$ of subrings of R and $\mathrm{Idl}(R)$ of ideals of R are closure systems.

All the above are complete lattices, and Examples 2.3.1.2,4,5 are special cases of Proposition 2.9. For that proposition we need the following definition.

Definition 2.9 We say that a non-empty poset D is a *directed set* if any two elements of D have an upper bound in D, i.e. for any $x, y \in D$ there is $z \in D$ such that $x, y \leq z$. The dual of directed is sometimes called *dual-directed*, or *directed down*.

Note that the condition for directed set is weaker than than for join *semilattice*, i.e. a poset where any two elements have a l.u.b..

Definition 2.10 Let A be a set, and $n \in \mathbb{N}$. An n-ary *operation* on A is a function $f : A^n \to A$. We call n the *arity* of the operation f. A *universal algebra* or *algebraic system*

$$\mathbf{A} = (A, (f_i)_{i \in I}))$$

consists of a non-empty set A, called the *universe* of $\mathbf{A}$, together with a family of (finitary) operations, f_i. The corresponding family of arities $(n_i)_{i \in I}$ is called the *type* of the algebra $\mathbf{A}$

02/04/20 **Proposition 2.9** *Let A be a* universal algebra*, i.e. a non-empty set with a collection of finitary operations. Let* $\mathrm{Sub}(A)$ *be the family of all subalgebras/subuniverses of A, i.e. subsets of A which are closed under all operations of A.*

1. $\mathrm{Sub}(A)$ *is a closure system, and a complete lattice. For $X \subseteq S$, the closure of X is called the* subalgebra generated *by X, and it is denoted $\langle X \rangle$.*
2. *Given a directed subfamily of* $\mathrm{Sub}(A)$*, its union is in* $\mathrm{Sub}(A)$*.*

Proof. Ex. ■

Exercise 2.3.1

1. What is the collection of operations in Example 2.3.1.2?
2. What is the collection of operations for $\mathrm{Nor}(G)$ in Example 2.3.1.4?
3. Why is Example 2.3.1.3 not necessarily an instance of Proposition 2.9?
4. Why is Example 2.3.1.1 not necessarily an instance of Proposition 2.9?

Exercise 2.3.2 Prove Proposition 2.9.2. HW

It can be shown that every complete lattice is isomorphic to a closure system.

Associated with every closure system on S, there is a *closure operator*

$$c : \mathcal{P}(S) \to \mathcal{P}(S)$$

that assigns to each subset of S the smallest closed subset that contains it. It is possible to characterize closure systems in terms of closure operators.

Definition 2.11 Let P be a poset. A function $c : P \to P$ is called a *closure map* if it is "*extensive*", "*idempotent*", and "*isotone*". That is, for all $x, y \in P$,

1. $x \leq c(x)$,
2. $c(c(x)) = c(x)$,

3. $x \leq y \Rightarrow c(x) \leq c(y)$.

When $P = \mathcal{P}(S)$ for some set S, ordered by inclusion, we refer to a closure map $c : \mathcal{P}(S) \to \mathcal{P}(S)$ as a *closure operator*.

Lemma 2.10 *Let L and M be posets and $\varphi : L \to M$ a bijection such that both φ and φ^{-1} preserve order. If L is a lattice (resp. complete lattice) then so is M, and φ is a lattice (resp. complete lattice) isomorphism.*

Proposition 2.11 *The complete lattice* $\mathrm{Idl}(\mathbb{Z})$ *of ideals of the ring of integers, is* *anti-isomorphic*[1] *to* $(\mathbb{N}, |)$.

Proof. ■

Proposition 2.12 *Let L be a lattice and $a, b \in L$ with $a \leq b$.*

1. *The* *interval* $[a, b]$ *defined by*

$$[a, b] := \{x \in L | a \leq x \leq b\}$$

   is a bounded lattice, and it is a sublattice of L.

2. *If L is a complete lattice, then $[a, b]$ is also a complete lattice with the same meets and joins, except on the empty set $\emptyset$.*

[1] Anti-isomorphic means isomorphic to the dual.

Chapter 3

Field Extensions

In this chapter we study fields and how they are related to each other. Since every homomorphism of fields is injective (see Proposition 3.1 below) it follows that fields are related by inclusion, up to isomorphism.

Throughout this chapter all rings are understood to be unitary, and so are all ring homomorphisms. Moreover, unless otherwise stated, rings are assumed to be non-trivial, i.e. $0 \neq 1$. To preserve the bijection between homomorphic images and ideals (1st Isomorphism Theorem) it is common practice to assume ideals are proper, $I \neq R$, or equivalently, $1 \notin I$.

3.1 Fields

Definition 3.1 A *field* is a non-trivial commutative ring in which every non-zero element has a multiplicative inverse. Equivalently, it is a ring in which the non-zero elements form an abelian multiplicative group.

It is easy to see that a field is an integral domain, and we will make use of this fact.

Notice that in a field F, the multiplicative inverse is a unary *partial operation*, as it is not defined for 0. This prevents us from treating fields as

universal algebras. Many results that hold for universal algebras also hold for fields, but not all of them. See Proposition 3.2 and Exercise 3.1.1 .

Exercise 3.1.1 Show that the direct product of two fields is never a field.

Definition 3.2 Given a field F, a *subfield* of F is a subring K which is closed under multiplicative inverses of all non-zero elements.

Proposition 3.1

1. *A field F is a simple ring, i.e. the only ideals are F and 0. The only quotients are 0 and F.*
2. *A homomorphism $\varphi : F \to R$ from a field to a non-trivial ring is injective. Therefore, $F \approx \mathrm{Im}(\varphi)$ is a subring of R. When R is also a field, $\mathrm{Im}(\varphi)$ is a subfield of R.*

Examples 3.1.1

1. $\mathbb{Q}$ is a subfield of $\mathbb{R}$, which is a subfield of $\mathbb{C}$.
2. $\mathbb{Z}_p$ is a field iff p is prime.

The next proposition shows that, despite fields not being universal algebras, $\mathrm{Sub}(F)$ has properties in common with the lattice of subalgebras of an algebra A. It turns out to have many properties in common with the lattice of subalgebras of an algebra A.

Proposition 3.2 *Let F be a field.*

1. *The set of subfields of F is closed under arbitrary intersections; hence $\mathrm{Sub}(F)$ is a closure system and a complete lattice.*
2. *The union of a directed family of subfield of F is a subfield of F.*

Proof. Proposition 2.9 takes care of everything other than the multiplicative inverses. It is easy to see that a non-zero element in the intersection (resp. union) of subfields, has its multiplicative inverse in the intersection (resp. union). ■

Definition 3.3 Given a field F, the smallest subfield of F, which exists by Proposition 3.2, is called the *prime subfield* of F.

The reason for this name comes from Proposition 3.3 below.

Definition 3.4 Let R be a ring, $x \in R$, and $n \in \mathbb{N}$. We denote by $n \cdot x$, the sum

$$\underbrace{x + x + \cdots + x}_{n-\text{times}}.$$

The *characteristic* of R is the smallest element n in $(\mathbb{N}, |)$, such that $n \cdot x = 0$ for all $x \in R$.
For $n < 0$, we define $n \cdot x = -((-n) \cdot x$.

Proposition 3.3 *The characteristic of a field F is either 0 or a prime p. Correspondingly, the prime subfield of F is isomorphic to $\mathbb{Q}$ or $\mathbb{Z}_p$.*

Proof. Consider the map

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & F \\ & n & \mapsto & n \cdot 1 \end{array}$$

It is easy to see that this is a ring homomorphism, whose kernel is the ideal generated by $c = \text{char}(F)$. It follows that $\mathbb{Z}/\langle c \rangle \approx \text{Im}(\varphi)$ is (isomorphic to) a subring of F, hence an integral domain. That forces c to be 0 or a prime. Since $\mathbb{Z}$ is generated by 1, then $\text{Im}(\varphi)$ is generated by $\varphi(1) = 1_F$.
If $c = 0$ then $\text{Im}(\varphi) \approx \mathbb{Z}$, and the subfield generated by this subring is isomorphic to $\mathbb{Q}$. Since every subfield of F contains 1_F, it must contain this copy of $\mathbb{Q}$, showing that this is the prime subfield of F.
If $c = p$ is a prime, then $\text{Im}(\varphi) \approx \mathbb{Z}/\langle p \rangle \approx \mathbb{Z}_p$ is a subfield of F. Again, every subfield of F contains this image, showing that this is the prime subfield of F. ■

Since $\text{Sub}(F)$ is a closure system, we can talk about the subfield generated by A for any subset A of F. We are particularly interested in the subfield generated by a subfield K and an element a, and in the subfield generated by a family of subfields, i.e. their join. We begin with the first.

Proposition 3.4 *Let K be a subfield of F, and $a \in F$.*

1. *The evaluation map*

$$\begin{array}{rccccl} \text{ev}_a: & K[x] & \to & F & & \\ & k & \mapsto & k & & \textit{for } k \in K \\ & x & \mapsto & a & & \end{array}$$

is a ring homomorphism. Its image, $\mathrm{Im}(\mathrm{ev}_a)$ *is the subring of* F *generated by* $K \cup \{a\}$*. We denote it by* $K[a]$*.*

2. *The field of fractions of* $K[a]$ *is the subfield generated by* $K \cup \{a\}$*. It is denoted by* $K(a)$*, and its elements are of the form* u/v *with* $u, v \in K[a]$*, and* $v \neq 0$*.*

The elements of $K(a)$ can be thought of as evaluations at a of rational functions in $K(x)$, but this evaluation map

$$\mathrm{ev}_a : K(x) \to F$$

is only a partial map, as many denominators may evaluate to 0. The domain is a subring of $K(x)$.

Proof. 1. That ev_a is a ring homomorphism is an immediate consequence of the UMP for polynomial rings, see Theorem 1.12. It is clear that $\mathrm{Im}(\mathrm{ev}_a)$ contains K and a, so it contains the subring generated by $K \cup \{a\}$. On the other hand, the elements of $K[a]$ are of the form $f(a)$ for some $f(x) \in K[x]$, so any ring that contains K and a must also contain $K[a]$.

2. We know that the field of fractions of a subring, is the smallest subfield containing that subring. In the closure system $\mathrm{Sub}(F)$ of subfields of F, $K(a)$ is the closure of $K[a]$, which contains the closure of $K \cup \{a\}$. By part 1, any subfield E that contains $K \cup \{a\}$ must contain $K(a)$, and therefore must contain its closure $K(a)$. ■

Definition 3.5 Let K be a subfield of F, and $a \in F$. We say that a is *transcendental* over K if the homomorphism ev_a in Proposition 3.4.1 is injective. Otherwise, we say a is *algebraic* over K. In the later case, the kernel is an ideal of $K[x]$, and since $K[x]$ is an Euclidean Domain, this ideal is principal. It is generated by a non-zero polynomial of smallest degree in the ideal. Among the individual generators of $\ker(\mathrm{ev}_a)$ there is one which is monic; we call that polynomial the *minimal* polynomial of a over K, and denote it by $\min_K(a)$. It is easy to see that this polynomial is irreducible over K; for that reason, it is also denoted $\mathrm{irr}_K(a)$. The degree of $\min_K(a)$ is called the *degree* of a over K, and it is denoted $\deg_K(a)$.

Examples 3.1.2 1. The element $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$. Its minimal polynomial is $\min_{\mathbb{Q}}(\sqrt{2}) = x^2 - 2$, and $\deg_{\mathbb{Q}}(\sqrt{2}) = 2$.

2. The elements $\pi, e \in \mathbb{R}$ are transcendental over $\mathbb{Q}$. Johann Heinrich Lambert conjectured that e and π were both transcendental numbers in his 1761 paper proving the number π is irrational. In 1873, Charles Hermite proved that e is transcendental. In 1882, Ferdinand von Lindemann published a proof that the number π is transcendental.

3. The elements of K are algebraic over K of degree 1. For $a \in K$, $\min_K(a) = x - a$. In fact, for $a \in F$, $\deg_K(a) = 1$ iff $a \in K$.

Corollary 3.5 *Let K be a subfield of F and $\alpha \in F$.*

1. *If α is trascendental over K, then $K[\alpha] \approx K[x]$, and $K(\alpha) \approx K(x)$.*

2. *If α is algebraic over K, then $K(\alpha) = K[\alpha]$.*

Proof. When α is transcendental over K, the result is obvious. Consider the case when α is algebraic over K. Since $K[x]$ is a P.I.D. and $\min_K(\alpha)$ is irreducible, it follows, from Proposition 1.19, that $\ker(\mathrm{ev}_\alpha)$ is a maximal ideal, and by Proposition 1.13, $K[\alpha] \approx K[x]/\ker(\mathrm{ev}_\alpha)$ is a field. ■

Note that when $\alpha \in F$ is transcendental, $K[\alpha] \approx K[x]$ is infinite dimensional as a vector space over K (see Proposition 1.23). We will see that the converse also holds. See Theorem 3.11 below.

The previous proposition can be extended from a single element $a \in F$, to a family A of elements of F, with essentially the same proof.

Proposition 3.6 *Let K be a subfield of F, and $A \subseteq F$. For each $a \in A$, let x_a denoted an indeterminate, and let $X = \{x_a | a \in A\}$.*

1. *The evaluation map*

$$\begin{array}{rccll} \mathrm{ev}_A : & K[X] & \to & F & \\ & k & \mapsto & k & \textit{for } k \in K \\ & x_a & \mapsto & a & \textit{for } a \in A \end{array}$$

is a ring homomorphism. Its image, $\mathrm{Im}(\mathrm{ev}_A)$ *is the subring of* F *generated by* $K \cup A$*. We denote it by* $K[A]$*. When* $A = \{a_1, \ldots, a_n\}$ *is a finite set, we also write* $K[a_1, \ldots, a_n]$*.*

2. *The field of fractions of* $K[A]$ *is the subfield generated by* $K \cup A$*. It is denoted by* $K(A)$*, and its elements are of the form* u/v *with* $u, v \in K[A]$*, and* $v \neq 0$*. When* $A = \{a_1, \ldots, a_n\}$ *is a finite set, we also write* $K(a_1, \ldots, a_n)$*.*

The elements of $K(A)$ can be thought of as evaluations at A of rational functions in $K(X)$,

$$\mathrm{ev}_A : K(X) \to F,$$

but this evaluation map is only a partial map, as many denominators may evaluate to 0. The domain is a subring of $K(X)$.

Definition 3.6 Let K be a subfield of F, and $A \subseteq F$. We say that A is *algebraically independent* over K if the map ev_A in Proposition 3.6 is injective. Othewise, we say that A is *algebraically dependent*.

Corollary 3.7 *If* A *is algebraically independent over* K*, then* $K[A] \approx K[X]$*, and* $K(A) \approx K(X)$*.*

Notice the similarity with the concept of *linear dependence*. A set of vectors is linearly dependent if they can be related by a linear equation. A set of elements is algebraically dependent if they can be related by an algebraic (polynomial) equation. The concept of algebraic independence satisfies all the conditions needed for a *matroid*.

Exercise 3.1.2 Let K be a subfield of F, and $a_1, a_2, \ldots, a_n \in F$. Show that

$$K[a_1, a_2, \ldots, a_n] = K[a_1][a_2] \cdots [a_n],$$

and

$$K(a_1, a_2, \ldots, a_n) = K(a_1)(a_2) \cdots (a_n).$$

As a consequence of Proposition 3.6 we get the first part of the next proposition. A similar argument can be used to prove the second part.

Proposition 3.8 *1. Let K, L be subfields of F. The join of K and L, also called their* composite*, and denoted by KL, is the field of fractions of the set of all sums of products kl with $k \in K$ and $l \in L$.*

2. Let $(K_i)_{i \in I}$ be a family of subfields of F. Their join is the field of fractions of the set of all sums of products of elements in $\bigcup_{i \in I} K_i$. In each product, the factors may be taken from different K_i's. When I is a totally ordered set, the factors in the products may be taken with ascending order of indices, meaning $a_{i_1} a_{i_2} \cdots a_{i_n}$ with $i_i < i_2 < \cdots < i_n$.

3.2 Field Extensions

$$\begin{array}{c} F \\ | \\ E \\ | \\ K \end{array}$$

The concept of *field extension* and subfield are the same, but from opposite points of view. We say that F is a field extension of K whenever K is a subfield of F. We write F/K is an extension. Since fields do not have interesting quotients, there is no danger in using this notation. We just have to remember that it **does not** denote a quotient. A *field tower* consists of a totally ordered set of fields, ordered as extensions. For example, we write $F/E/K$ to indicate that F is a field extension of E and E is a field extension of K. We may draw the diagram shown on the left.

Proposition 3.9 *If F is a field extension of K, then F is a vector space over K, where the scalar multiplication is just multiplication in F.*

Definition 3.7

1. Given an extension F/K, the dimension $\dim_K(F)$, of F as a vector space over K, is called the *degree* of F/K, and is denoted $[F : K]$.

2. A *finite extension* is an extension F/K of finite degree.

3. An extension F/K is said to be a *simple extension* if $F = K(a)$ for some $a \in F$. Such a is called a *primitive element* of the extension F/K.

4. An extension F/K is said to be a *finitely generated* if $F = K(a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in F$.

Note 3.1 1. Given an extension F/K, we have $[F : K] = 1$ iff $F = K$.

2. It is common practice to write the degree of an extension next to the edge in the diagram. See Example 3.2.2 below.

Examples 3.2.1 Here are some examples of extensions

$$\begin{array}{c} \mathbb{C} \\ \Big|_{2} \\ \mathbb{R} \\ \Big|_{\infty} \\ \mathbb{Q} \end{array}$$

1. $\mathbb{C}/\mathbb{R}$ is a finite extension of degree 2.
2. $\mathbb{R}/\mathbb{Q}$ is an infinite uncountable extension.
3. The field $\mathbb{Q}(\sqrt{2})$ is the set

$$\left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q} \right\}.$$

Notice that

$$\begin{aligned} (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2} \\ \tfrac{1}{(a+b\sqrt{2})} &= \tfrac{a}{a^2-2b^2} + \tfrac{-b}{a^2-2b^2}\sqrt{2} \end{aligned}$$

Now, on one hand, $\mathbb{Q} < \mathbb{Q}(\sqrt{2})$ since $\sqrt{2} \notin \mathbb{Q}$. On the other hand $\{1, \sqrt{2}\}$ is a spanning set for $\mathbb{Q}(\sqrt{2})$ as a vector space over $\mathbb{Q}$. If follows that $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = 2$, i.e. $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, and $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ as a vector space over $\mathbb{Q}$.

4. An identical argument to that in part 3, shows that $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, and $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{3})$ as a vector space over $\mathbb{Q}$. Since $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ (why?), it follows that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) > \mathbb{Q}(\sqrt{2})$, so we have $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] > 2$, and $\mathbb{Q}(\sqrt{2}, \sqrt{3}) > \mathbb{Q}(\sqrt{3})$. As before, since $\{1, \sqrt{2}\}$ is a spanning set for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a vector space over $\mathbb{Q}(\sqrt{3})$, we get that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 2$, and $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a vector space over $\mathbb{Q}(\sqrt{3})$. To obtain $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$, we will use the following theorem. See Example 3.2.2.1 below.

Exercise 3.2.1 Show that $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$. Generalize.

Theorem 3.10 [Product Rule for extensions] *Let $F/E/K$ be a field tower. For $U = \{\alpha_i | i \in I\} \subseteq F$ and $V = \{\beta_i | j \in J\} \subseteq E$, let*

$$UV = \{\alpha_i \beta_j \mid i \in I, j \in J\}.$$

1. *If U is linearly independent over E and V is linearly independent over K, then UV is linearly independent over K.*

2. *If U spans F over E and V spans E over K, then UV spans F over K.*

3. *If U is a basis for F over E and V is a basis for E over K, then UV is a basis for F over K.*

4. $$[F : K] = [F : E][E : K]. \tag{3.1}$$

Proof. 1. Suppose we have a finite support family $(a_{i,j}|i \in I, j \in J)$ of elements of K, such that

$$\sum_{(i,j)\in I\times J} a_{i,j}\alpha_i\beta_j = 0.$$

For $i \in I$, let $b_i = \sum_{j\in J} a_{i,j}\beta_j \in E$. The family $(b_i|i \in I)$ has finite support, and we get

$$\sum_{i\in I} b_i\alpha_i = 0.$$

By linear independence of U over E, we get $b_i = 0$ for all $i \in I$. By linear independence of V over K, we get $a_{i,j} = 0$ for all $i \in I, j \in J$.

2. Let $\gamma \in F$. There is a finite support family $(b_i|i \in I)$ of elements of E, such that $\gamma = \sum_{i\in I} b_i\alpha_i$. For each $i \in I$ there is a finite support family $(a_{i,j}|j \in J)$ of elements of K, such that $b_i = \sum_{j\in J} a_{i,j}\beta_j$. Combining these expressions we get

$$\gamma = \sum_{(i,j)\in I\times J} a_{i,j}\alpha_i\beta_j.$$

■

Right after Corollary 3.5 we noted that if $\alpha \in F$ is transcendental over K, then $K[\alpha]$ is infinite dimensional over K. We'll now prove the converse, completely characterizing *algebraic* v/s *transcendental* in terms of the degree of the corresponding simple extension. 02/11/2020

Theorem 3.11 *Let F/K be an extension and $\alpha \in F$.*

1. *If α is algebraic over K of degree n, then the set*
$$A = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$
is a basis for $K(\alpha)$ over K, and $[K(\alpha) : K] = n = \deg_K(\alpha)$.

2. *If α is trascendental over K, then $[K(\alpha) : K] = \infty$.*

Proof. 1. By Corollary 3.5, it suffices to prove that A is a basis for $K[\alpha]$. Let $f(x) = \min_K(\alpha) = x^n + c_1x^{n-1} + \cdots + c_{n-1}x + c_n$. The fact that α is a root of this polynomial yields that α^n is a linear combination of A, with coefficients in K. If follows by induction that any α^m, $m \in \mathbb{N}$ is in the span of A, showing that A spans $K[\alpha]$. The minimality of $\min_K(\alpha)$ yields the linear independence of A.
2. This follows from Corollary 3.5, $K(\alpha) \approx K(x)$, and the facts that $\dim_K(K[x])$ is infinite, and $K[x]$ is a K-subspace of $K(x)$. ■

Remark 3.2.1 It is not difficult to show that $\dim_K(K(x)) = \max(|K|, |\mathbb{N}|)$.

Examples 3.2.2 1. Let's revisit Example 3.2.1.4. Since $\mathbb{Q}(\sqrt{2}, \sqrt{3}) > \mathbb{Q}(\sqrt{3})$, we have $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \geq 2$. Since $\sqrt{2}$ satisfies a quadratic polynomial over $\mathbb{Q}(\sqrt{3})$, we have the other inequality $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})] \leq 2$. Using Theorem 3.10 we get $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. The following diagram summarizes the information we have gathered.

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

2. From the previous example, we can now say something about $\alpha = \sqrt{2} + \sqrt{3}$. Note first that

$$\frac{1}{\alpha} = \frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2},$$

so, $\sqrt{3} = \frac{1}{2}(\alpha + \frac{1}{\alpha})$ and $\sqrt{2} = \frac{1}{2}(\alpha - \frac{1}{\alpha})$, which yield $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \leq \mathbb{Q}(\alpha)$. The other inclusion is obvious so, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and by Theorem 3.11.1, $\deg_{\mathbb{Q}}(\alpha) = 4$. On the other hand, $\alpha^2 = 5 + 2\sqrt{6}$, so $(\alpha^2 - 5)^2 = 24$ and $\alpha^4 - 10\alpha^2 + 1 = 0$, so α is a root of $x^4 - 10x^2 + 1$, making $\min_{\mathbb{Q}}(\alpha) = x^4 - 10x^2 + 1$.

A natural question to ask here is what other fields lie between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. By the product rule of Theorem 3.10, any other intermediate fields will have degree 2 over $\mathbb{Q}$, but we don't know at this point what they may look like. We will be able to obtain a complete answer, with the help of the Fundamental Theorem of Galois Theory in Chapter 4.

Another important question to ask is whether all elements of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ are algebraic over $\mathbb{Q}$. Example 3.2.2.2 suggests a way to deal with this question, but for an arbitrary

$$\alpha = a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{4}$$

the argument gets trickier. A better approach is found below in Proposition 3.12.

Definition 3.8 Let F/K and E/K be two field extensions (over the same field K). A map $\varphi : F \to E$ is called a K-*extension homomorphism*, or simply a K-*homormorphism*, if it is a field homomorphism, and $\varphi(a) = a$ for all $a \in K$. The set of K-homomorphisms from F to E is denoted $\mathrm{Hom}_K(F, E)$. The set of K-automorphisms of F is denoted $\mathrm{Aut}_K(F)$; it is clearly a group under composition.

Note that if $\varphi : F \to E$ is a field homomorphism, F and E must have the same characteristic, hence the same prime subfield P. The homomorphism φ fixes P, hence it is a P-homomorphism.

3.3 Algebraic Extensions

Definition 3.9 An extension F/K is said to be *algebraic*, if every $\alpha \in F$ is algebraic over K. Otherwise, we say that it is *trascendental*.

Examples 3.3.1

1. $\mathbb{C}/\mathbb{R}$ is algebraic, as every complex number, $a + b\,\mathrm{i}$ satisfies a quadratic equation with real coefficients, i.e. $(x-a)^2+b^2 = 0$.
2. $\mathbb{R}/\mathbb{Q}$ is transcendental.
3. $\mathbb{Q}(\sqrt{2}))/\mathbb{Q}$ is algebraic, as each $a + b\sqrt{2}$ is a root of a quadratic polynomial with rational coefficients, i.e. $(x - a)^2 - 2b^2 = 0$.

The previous examples are a special case of the following proposition.

Proposition 3.12 *Any finite extension is algebraic.*

Proof. If F/K is a finite extension, then for any $\alpha \in F$, we have $[K(\alpha) : K] \leq [F : K] < \infty$. By Theorem 3.11, α is algebraic over K. ■

The converse of this proposition does not hold. That is, not every algebraic extension is finite. On the other hand, Theorem 3.11.1 provides a partial, i.e. elementwise converse.

Algebraic extensions share many properties with finite extensions. See for example Theorem 3.18.

Example 3.3.2 We will show below that the set $\mathbb{A}$ of algebraic numbers, i.e. complex numbers algebraic over $\mathbb{Q}$, is a subfield of $\mathbb{C}$. By Eisenstein' criterion the polynomial $x^n - 2$ is irreducible, and a root of it has degree n over $\mathbb{Q}$. Since the degrees of algebraic elements are unbounded, $\mathbb{A}/\mathbb{Q}$ cannot be finite.

The following corollary and lemma need each other, without creating a vicious circle. The corollary uses part (1) of the lemma, and part (2) of the lemma uses the corollary.

Corollary 3.13 *If $\alpha_1, \ldots, \alpha_m \in F$ are algebraic over K of degrees $n_1, \ldots, n_m$ respectively, then $K(\alpha_1, \ldots, \alpha_m)$ is a finite extension of K, of degree $\leq n_1 \cdots n_m$.*

Proof. By induction on m. The case $m = 1$ follows from Theorem 3.11.1. Assume $[K(\alpha_1, \ldots, \alpha_{m-1}) : K] \leq n_1 \cdots n_{m-1}$. By Lemma 3.14 below, we have α_m is algebraic over $K(\alpha_1, \ldots, \alpha_{m-1})$ of degree $\leq n_m$. By Proposition 3.12, and the Product Rule (3.1) for extensions, we get

$$[K(\alpha_1, \ldots, \alpha_m) : K] \leq n_1 \cdots n_m$$

as desired. ■

Lemma 3.14 *Let $K \leq E \leq F$ be an extension tower, and $\alpha \in F$.*

1. *If α is algebraic over K then it is algebraic over E.*
2. *If α is algebraic over E, and E/K is algebraic, then α is algebraic over K.*

Proof. (1) This is the easy part. Suppose α is algebraic over K, and

$$\begin{array}{c} \alpha \in F \\ \big| \\ E \\ \big|_{alg} \\ K \end{array}$$

let

$$f(x) = \min_K(\alpha) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$$

be the minimal polynomial of α over K. Since $a_1, \ldots, a_n \in K \leq E$, we have $f(x) \in E[x]$, so α is algebraic over E and $f(x)$ is a multiple of $\min_E(\alpha)$.

(2) Suppose now that α is algebraic over E, and E/K algebraic. Let

$$g(x) = \min_E(\alpha) = x^m + b_1 x^{m-1} + \cdots + b_{m-1}x + b_m$$

be the minimal polynomial of α over E. We get that α is algebraic over $K(b_1, \ldots, b_m)$. The coefficients $b_1, \ldots, b_n \in E$ are algebraic over K, so Corollary 3.13 shows that $K(b_1, \ldots, b_n)/K$ is a finite extension. By the Product Rule (3.1), we get that $[K(\alpha, b_1, \ldots, b_n) : K]$ is finite, and therefore, by Proposition 3.12, α is algebraic over K. ■

Note that the proof of Corollary 3.13 uses one part of Lemma 3.14, and the other part of Lemma 3.14 uses Corollary 3.13. The first part of Lemma 3.14 does not need E to be algebraic over K. We will find similar looking lemmas when we consider *separable* and *purely inseparable* extensions. (see Lemmas 3.57 and 3.69)

02/13/2020 **Scholium 3.15** *In the set up of Lemma 3.14, we get*

$$\min_E(\alpha) \mid \min_K(\alpha) \text{ and } \deg_E(\alpha) \leq \deg_K(\alpha).$$

The following corollary generalizes what we observed in Example 3.2.2.2.

Corollary 3.16 *If $\alpha, \beta \in F$ are algebraic over K, of degrees n and m respectively, then $K(\alpha, \beta)/K$ is a finite extension of degree $\leq nm$. Therefore, $\alpha \pm \beta$, $\alpha\beta$ and α/β, when $\beta \neq 0$, are algebraic over F and their degrees are $\leq nm$. If $(m, n) = 1$, then $[K(\alpha, \beta) : K] = mn$.*

Proof. The first statement is a special case of Corollary 3.13. The second part follows immediately. The third follows from the first and Theorem 3.10.4, the product rule for extensions. ■

Corollary 3.17 *The set of elements of F which are algebraic over K form a subfield of F.*

In particular, the set $\mathbb{A}$ of algebraic numbers forms a subfield of $\mathbb{C}$, which is an algebraic extension but not a finite extension over $\mathbb{Q}$. This fills the gap in Example 3.3.2

Even though the class of algebraic extensions is larger than that of finite extensions, both have many common properties. From Theorem 3.10, the Product Rule (3.1) for extensions, we get that a finite extension of a finite extension is finite. The next theorem gives the corresponding result for algebraic extensions. It follows at once from Lemma 3.14.

Theorem 3.18 *Let $F/E/K$ be a field tower. F/E and E/K are both algebraic extensions iff F/K is algebraic.*

The following proposition can be seen as the algebraic counterpart to Corollary 3.13.

Proposition 3.19 *Let $F/E/K$ be a field tower, with E/K algebraic, and let $S \subseteq F$ be a set of elements algebraic over E. Then $E(S)$ is algebraic over K.*

Proof. By Lemma 3.14 every element of S is algebraic over K. It follows that $E(S)$ is contained in the subfield of F consisting of all elements algebraic over K. By Theorem 3.18 $E(S)/K$ is algebraic. ■

Corollary 3.20 *Let $K \leq E_1, E_2 \leq F$ be such that E_1 and E_2 are algebraic over F. Then the join E_1E_2 is algebraic over K.*
More generally, if $K \leq E_i \leq F$ and each E_i/K is algebraic, then $\bigvee_{i \in I} E_i$ is algebraic over K.

Exercise 3.3.1 Prove Corollary 3.20.

3.3.1 Building Up

The results in this subsection show us how to "*build up*" extensions where polynomials have roots, and how to extend morphisms to those extensions.

Definition 3.10 Let E/K be a field extension, and $f(x) \in K[x]$ a polynomial. We say that $f(x)$ *splits* over E if $f(x)$ factors as a product of linear factors in $E[x]$. We also say that E has *enough roots* for $f(x)$.
We say that E is a *splitting field* for $f(x)$ over K, if $f(x)$ splits over E and E is minimal with this property.
For a set $S \subseteq K[x]$ of polynomials, we say that S *splits* over E if every $f(x) \in S$ splits over E. We say that E is a splitting field for S over K if S splits over E, and E is minimal with this property.

Note 3.2 If E is a splitting field for $f(x)$ over K, since $E[x]$ is a UFD, the roots $\alpha_1, \ldots, \alpha_n$ of $f(x)$ in E are uniquely determined by its factorization into linear factors. By minimality, we get $E = K(\alpha_1, \ldots, \alpha_n)$. Similarly, for $S \subseteq K[x]$, if A is the set of all roots of polynomials from S in E, then by minimality, $E = K(A)$.

Thus, we immediately get from Corollary 3.13 and Proposition 3.19 the following.

Corollary 3.21 *1. Let $f(x) \in K[x]$ and E/K an extension such that E is a splitting field for $f(x)$ over K. Then E/K is a finite extension.*

2. *Let $S \subseteq K[x]$ and E/K an extension such that E is a splitting field for S over K. Then E/K is an algebraic extension.*

From Note 3.2 we also get:

Corollary 3.22 *Let $f(x) \in K[x]$, and let E be an extension of K such that $f(x)$ splits over E. Then E contains a unique splitting field of $f(x)$, i.e $K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$ in E.*

We will prove a more general result on the uniqueness of splitting fields. See Corollary 3.35. Before we get there, we are going to show the existence of a splitting field for a polynomial. In Section 3.4 we will show that any family of polynomials has a splitting field. See Corollary 3.30.

Proposition 3.23 *Let K be a field, and $p(x) \in K[x]$ an irreducible polynomial. There is a finite simple extension E/K, where $p(x)$ has a root α. Moreover, $[E : K] = \deg(p(x))$, $K(\alpha) \approx K[x]/\langle p(x)\rangle$, and if $p(x)$ is monic, then $p(x) = \min_K(\alpha)$,*

Proof. Let $E = K[x]/\langle p(x)\rangle$. The irreducibility of $p(x)$ implies that $\langle p(x)\rangle$ is a prime ideal in $K[x]$, hence maximal. Therefore, E is a field. Let $\alpha = x + \langle p(x)\rangle$, be the coset of x in E. Then

$$p(\alpha) = p(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle,$$

so α is a root of $p(x)$ in E, and α is algebraic over K. By construction, $K[\alpha] = K[x]/\langle p(x)\rangle = E$, and by Corollary 3.5, $K(\alpha) = K[\alpha]$, showing E/K is a simple extension. By irreducibility of $p(x)$, it is associate to $\min_K(\alpha)$, so by Theorem 3.11, $[E : K] = \deg(\min_K(\alpha)) = \deg(p(x))$. If $p(x)$ is also monic, then it equals $\min_K(\alpha)$. ■

02/18/2020 **Theorem 3.24** *Let K be a field and $f(x) \in K[x]$ a polynomial. There is a finite extension F/K where $f(x)$ splits. Hence, $f(x)$ has a splitting field. Moreover, if $\deg(f(x)) = n$, then F can be chosen such that $[F : K] \leq n!$.*

Proof. By induction on $\deg(f(x))$. When $\deg(f(x)) = 1$, $f(x)$ splits over K. Otherwise, let $p(x)$ be an irreducible factor of $f(x)$ in $K[x]$, and let E be the

finite extension of K constructed in Proposition 3.23. We have that $p(x)$ has a root $\alpha \in E$. and $[E : K] = \deg(p(x)) \leq n$. In $E[x]$, $f(x)$ factors as

$$f(x) = (x - \alpha)g(x),$$

and $\deg(g(x)) = n - 1$. By induction, there is a finite extension F/E where $g(x)$ splits, and $[F : E] \leq (n-1)!$. By the Product Rule (3.1), F/K is finite, with $[F : K] \leq n!$, and $f(x)$ splits over F. ■

The upper bound for the degree of a splitting field of $f(x)$ over K, is the best we can get in general.

Example 3.3.3 Consider the polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. This polynommial is irreducible over $\mathbb{Q}$, so by Proposition 3.23, there is a extension $\mathbb{Q}(\alpha)$ of degree 3 over $\mathbb{Q}$, where α is a root of $f(x)$. Using synthetic division we get

$$x^3 - 2 = (x - \alpha)(x^2 + \alpha x + \alpha^2).$$

Denote by β a root of $x^2 + \alpha x + \alpha^2$. Note that $\beta \neq \alpha$, and let $\omega = \frac{\beta}{\alpha}$, so that $\beta = \alpha\omega$,

$$\omega^3 = \left(\frac{\beta}{\alpha}\right)^3 = \frac{\beta^3}{\alpha^3} = \frac{2}{2} = 1$$

and ω is a root of $x^2 + x + 1$, which is irreducible over $\mathbb{Q}$, so $\min_{\mathbb{Q}}(\omega) = x^2 + x + 1$. Synthetic division yields

$$x^2 + \alpha x + \alpha^2 = (x - \beta)(x + (\alpha + \beta)),$$

so $-(\alpha + \beta) = -\alpha(1 + \omega) = \alpha\omega^2$ is the third root of $f(x)$. A splitting field for $f(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, \omega)$.

$$\begin{tikzcd}
 & \mathbb{Q}(\omega, \alpha) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\omega) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\alpha) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

By Corollary 3.16, $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6 = 3!$.

Notice that we did not use $\mathbb{C}$, and the fact that every rational polynomial splits over $\mathbb{C}$ (Fundamental Theorem of Algebra). We could have found a splitting field of $x^3 - 2$ in $\mathbb{C}$ by taking $\alpha = \sqrt[3]{2}$ and $\omega = \mathrm{cis}(2\pi/3)$

The UMP for polynomial rings implies that given a field homomorphism $\varphi : K \to L$ there is a unique ring homomorphism $\widehat{\varphi} : K[x] \to L[x]$ which extends φ and maps $x \in K[x]$ to $x \in L[x]$. From this, we get a UMP for simple algebraic extensions.

Proposition 3.25 *Let α be algebraic over K with minimal polynomial $p(x) = \min_K(\alpha)$, and $\varphi : K \to L$ a field homomorphism. Let $p^\varphi(x)$ be the image of $p(x)$ under the induced map $\varphi : K[x] \to L[x]$. If $\beta \in L$ is a root of $p^\varphi(x)$, then there is a unique field homomorphism $\widehat{\varphi} : K(\alpha) \to L$ which extends φ and such that $\widehat{\varphi}(\alpha) = \beta$. Moreover, any homomorphism $\psi : K(\alpha) \to L$ maps α to a root of $p^\psi(x)$ in L.*

$$\begin{tikzcd} K(\alpha) \arrow[dr, dashed, "\widehat{\varphi}"] & \\ K \arrow[u, hook] \arrow[r, "\varphi"] & L \end{tikzcd}$$

Proof. By the UMP for polynomials, there is a unique ring homomorphism

$$\widetilde{\varphi} : K[x] \to L$$

that extends φ and such that $\widetilde{\varphi}(x) = \beta$. Since

$$\widetilde{\varphi}(p(x)) = p^\varphi(\widetilde{\varphi}(x)) = p^\varphi(\beta) = 0,$$

the map $\widetilde{\varphi}$ factors through $K[x]/\langle p(x)\rangle \approx K(\alpha)$, i.e.

$$\begin{tikzcd} K \arrow[r, hook] & K[x] \arrow[r, "\widetilde{\varphi}"] \arrow[d, two heads, "q"'] & L \\ & x \arrow[r, mapsto, "\widehat{\varphi}"] & \beta \\ & \alpha & \\ & K[x]/\langle p(x)\rangle \arrow[r, equal, "\widetilde{}"] & K(\alpha) \end{tikzcd}$$

Now, if $\psi : K(\alpha) \to L$ is a homomorphism, then

$$0 = \psi(0) = \psi(p(\alpha)) = p^\psi(\psi(\alpha)),$$

so $\psi(\alpha)$ is a root of $p^\psi(x)$. ■

Note that given $\varphi : K \to L$ it is possible for L not to have any root of $p^\varphi(x)$, in which case, the extension $\widehat{\varphi}$ will not exist. In the next section,

we will see that when L has the property of being algebraically closed, such roots will always exist.

Proposition 3.25 also puts an upper bound on the number of extensions that φ can have to $K(\alpha)$.

Corollary 3.26 *Let α be algebraic over K with minimal polynomial $p(x) = \min_K(\alpha)$, and $\varphi : K \to L$ a field homomorphism. The number of extensions $\widehat{\varphi} : K(\alpha) \to L$ of φ is $\leq \deg_K(\alpha)$.*

The actual number of homomorphisms $\widehat{\varphi}$ in Corollary 3.26, is going to depend on two separate issues:

- the number of linear factors, i.e. roots, $p^{\varphi}(x)$ has in $L[x]$, and
- the multiplicity of those roots.

We will deal with these two issues separately, in Sections 3.4, and 3.6 below.

3.4 Algebraic Closure

Basically, an algebraic closure of a field, is an extension where all polynomials have enough roots to split into linear factors. More precisely,

Proposition 3.27 *Let F/K be an algebraic extension. TFAE:*

(i) Every non-constant polynomial $f(x) \in K[x]$ splits in F;

(ii) every non-constant polynomial $f(x) \in F[x]$ has a root in F;

(iii) every non-constant polynomial $f(x) \in F[x]$ splits in F;

(iv) every irreducible polynomial in $F[x]$ has degree 1;

(v) F has no proper algebraic extension.

Proof. (v) $\Rightarrow$(iv) $\Rightarrow$(iii) $\Rightarrow$(i), and (iii) $\iff$ (ii) are immediate.
For (i) $\Rightarrow$(v) let L be an algebraic extension of F, and $\alpha \in L$. By Theorem 3.18, L/K is algebraic; α is algebraic over K. Then by (1), $\min_K(\alpha)$ splits in F and $\alpha \in F$, hence $L = F$. ■

Note that all but the first condition in the proposition are about F alone. The first one is about the extension F/K, and it says that F contains a splitting field for the family $K[x]$, of all polynomials over K.

Definition 3.11 A field F satisfying the conditions in Proposition 3.27 is said to be *algebraically closed*, and it is called an *algebraic closure* of K.

02/20/20 **Corollary 3.28** *F is an algebraic closure of K iff F is a splitting field of the set $K[x]$ of all polynomials over K.*

Proof. Suppose F is an algebraic closure of K. By Proposition 3.27, every polynomial in $K[x]$ splits in F, so F contains a splitting field L for $K[x]$. Again by Proposition 3.27, L is an algebraic closure of K, so it has no proper algebraic extension. Since $K \leq L \leq F$ ia an algebraic tower, we must have $L = F$. Suppose now that F is a splitting field of the set $K[x]$. By Corollary 3.21.2 F is algebraic over K, and by Proposition 3.27, F ia an algebraic closure of K. ■

To be an algebraic closure of K, F must be algebraically closed and algebraic over K.

We will show that any field K has an algebraic closure. As a consequence of that we'll get that any set of polynomials has a splitting field. We will also show that algebraic closure of a field K is unique up to isomorphism.

Theorem 3.29 *Any field K has an algebraic closure F.*

Corollary 3.30 *Any family $\{f_i(x)|i \in I\}$ of polynomials over K has a splitting field.*

Proof. Take first an algebraic closure F of K. Now take the K-extension generated by all the roots of the polynomials in the family $\{f_i(x)|i \in I\}$. ■

The main idea in the following proof, is due to Emil Artin. It mimics the proofs of Theorem 3.24 and Proposition 3.23, but instead of adding a root of a single polynomial at a time, it adds one root of every polynomial at a time. To accomplish this, instead of working with polynomials in one variable, we introduce one variable for each polynomial. Since irreducible polynomials may have arbitrarily large (finite) degrees, the process is repeated a countable number of times.

Proof of Theorem 3.29(Artin). The idea is to construct a sequence of algebraic extensions of K such that every non-constant polynomial with coefficients in one of these extensions will have a root in the next one. Let $E_0 = K$. We now describe how to obtain E_1 from E_0. Let

$$K[x]^+ := \{f(x) \in K[x] \mid \deg(f(x)) > 0\}$$

be the set of all non-constant polynomials with coefficients in K. For each $f(x) \in K[x]^+$ let x_f denote a variable, and let

$$X = \{x_f | f \in K[x]^+\}$$

be the set of all such variables. In the polynomial ring $K[X]$ let I be the ideal generated by $\{f(x_f)|f \in K[x]^+\}$. Note first that I is a proper ideal, for otherwise, we could write

$$1 = g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) \tag{3.2}$$

for some $f_1, \ldots, f_n \in K[x]^+$ and $g_1, \ldots, g_n$ in $K[X]$. Letting α_i be a root of f_i in some extension of K, which exists by repeated use of Theorem 3.24, and evaluating (3.2) at $x_{f_i} = \alpha_i$ for $i = 1, \ldots, n$ we get $1 = 0$, a contradiction.
Let M be a maximal ideal of $K[X]$ containing I, and $E_1 = K[X]/M$.
Claim: E_1 is an algebraic extension of E_0 in which every non-constant, single-variable, polynomial f over E_0 has a root. If we denote by α_f the image of x_f in E_1, then α_f is a root of $f(x)$ and E_1, which is generated as a K-extension by the set $A = \{\alpha_f | f \in K[x]^+\}$, is algebraic over K.
Repeating the previous process we get a sequence of extensions

$$E_0 \leq E_1 \leq E_2 \leq \ldots,$$

such that each E_{i+1} is algebraic over E_i, and every non-constant, single-variable polynomial over E_i has a root in E_{i+1}. Set

$$F = \bigcup_{i=0}^{\infty} E_i$$

It is clear from Theorem 3.18, that each E_i is algebraic over K, hence so is F. Any single-variable polynomial with coefficients in F has all its coefficients in some E_i and therefore has a root in E_{i+1}. By Proposition 3.27, F is an algebraic closure of K. ■

The following corollary is a consequence of Proposition 3.25 and Corollary 3.26 using the fact that when L is algebraically closed, it contains roots of all its polynomials.

Corollary 3.31 *Let $\varphi : K \to L$ be a field homomorphism, with L algebraically closed. For α algebraic over K, there is a field homomorphism $\widehat{\varphi} : K(\alpha) \to L$ which extends φ. Moreovoer, if $p(x) = \min_K(\alpha)$, the number of such extensions is equal to the number of distinct roots of $p^{\varphi}(x) \in L[x]$.*

We can take this result, and using Zorn's lemma, extend it from a simple algebraic extension to any algebraic extension.

Theorem 3.32 *Let $\varphi : K \to L$ be a field homomorphism, with L algebraically closed. For F algebraic over K, there is a field homomorphism $\widehat{\varphi} : F \to L$ which extends φ.*

$$\begin{tikzcd} F \arrow[dr, dashed, "\widehat{\varphi}"] & \\ K \arrow[u, hook] \arrow[r, "\varphi"] & L \end{tikzcd}$$

Proof. Let

$$\mathcal{S} = \{(E, \psi) | K \leq E \leq F, \psi : E \to L, \text{ and } \psi|_K = \varphi\}.$$

Order $\mathcal{S}$ by $(E_1, \psi_1) \leq (E_2, \psi_2)$ iff $E_1 \leq E_2$ and $\psi_2|_{E_1} = \psi_1$. Since $(K, \varphi) \in \mathcal{S}$, we have $\mathcal{S} \neq \emptyset$. Given a non-empty chain $\mathcal{C} = \{(E_i, \psi_i) | i \in I\} \subseteq \mathcal{S}$, let $E = \bigcup_{i \in I} E_i$. By Proposition 3.2, E is a subfield of F, and clearly $K \leq E$. Now define $\psi : E \to L$ as follows: for $a \in E$, find $i \in I$ such that $a \in E_i$; take $\psi(a) = \psi_i(a)$. That this map is well-defined follows from the conditions

on ψ_i's in $\mathcal{S}$. The fact that $\mathcal{S}$ is directed, and the ψ_i's are homomorphisms, yield that ψ is a homomorphism. Finally, $(E_i, \psi_i) \leq (E, \psi)$ by construction, so $\mathcal{C}$ has an upper bound in $\mathcal{S}$. By Zorn's lemma, there is a maximal element $(M, \mu) \in \mathcal{S}$. We claim that $M = F$. Otherwise, let $\alpha \in F - M$. Corollary 3.31 yields a homomorphism $\widehat{\mu} : M(\alpha) \to L$ such that $\widehat{\mu}|_M = \mu$, and therefore $\widehat{\mu}|_K = \varphi$ This contradicts the maximality of (M, μ). ■

It will follow from Proposition 3.56 that when F/K is a finite extension, the number of ways $\varphi : K \to L$ can be extended to $\widehat{\varphi} : F \to L$ is $\leq [F : K]$.

The next proposition shows that the following concepts/properties of field extensions:

- degree,
- algebraic,
- transcendental,
- algebraic closure,

are preserved under field homomorphisms.

Proposition 3.33 *Let F/K be a field extension, and $\varphi : F \to L$ a field homomorphism. Let $\widehat{F} = \varphi(F)$ and $\widehat{K} = \varphi(K)$.*

1. $[\widehat{F} : \widehat{K}] = [F : K]$.
2. *If F/K is algebraic, then so is $\widehat{F}/\widehat{K}$.*
3. *If F/K is transcendental, then so is $\widehat{F}/\widehat{K}$.*
4. *If F is an algebraic closure of K, then $\widehat{F}$ is an algebraic closure of $\widehat{K}$.*

Exercise 3.4.1 Prove Proposition 3.33.

Theorem 3.34 *Any two algebraic closures of K are K-isomorphic.* 02/25/20

Proof. Let F and L be two algebraic closures of K. Since L is algebraically closed and F/K is algebraic, there is a homomorphism $\varphi : F \to L$ that extends the inclusion map $\iota : K \to L$. The last condition simply says that φ is a K-homomorphism. As a field homomorphism φ is injective. By Proposition 3.33.4, $\mathrm{Im}(\varphi) \approx F$ is an algebraic closure of K. Since L is algebraic over K, by Theorem 3.18, $L/\mathrm{Im}(\varphi)$ is algebraic, and by Proposition 3.27, we must have $\mathrm{Im}(\varphi) = L$. ■

Definition 3.12 Given a field K, its unique (up to isomorphism) algebraic closure is denoted by $\overline{K}$.

Exercise 3.4.2 Show that the algebraic closure is a *closure operator*, i.e.

1. $K \leq \overline{K}$,
2. $\overline{\overline{K}} = \overline{K}$,
3. $K \leq E \Rightarrow \overline{K} \leq \overline{E}$.

Corollary 3.35 *Let K be a field, and $S \subseteq K[x]$ a set of polynomials over K.*

1. *Any splitting field for S over K is contained in an algebraic closure of K.*
2. *Any two splitting fields for S over K are K-isomorphic.*

Exercise 3.4.3 Prove Corollary 3.35.

In addition to being a closure operator, *algebraic closure* shares some properties with the concept of a *basis* for a vector space.

Proposition 3.36 *Let K be a field, and $\overline{K}$ an algebraic closure of K.*

1. *$\overline{K}$ is minimal, with the property of being an extension of K which is algebraically closed.*
2. *$\overline{K}$ is maximal, with the property of being algebraic over K.*
3. *$\overline{K}$ is smallest, up to isomorphism, with the property of being an extension of K which is algebraically closed.*
4. *$\overline{K}$ is largest, up to isomorphism, with the property of being algebraic over K.*

Exercise 3.4.4 Prove Proposition 3.36.

Corollary 3.37 *Any K-endomorphism of $\overline{K}$ is a K-automorphism.*

Proof. If $\varphi : \overline{K} \to \overline{K}$ is a K-endomorphism, then it is injective. By Proposition 3.33.4, $\mathrm{Im}(\varphi)$ is an algebraic closure of K, and by Proposition 3.36.1, we must have $\mathrm{Im}(\varphi) = \overline{K}$. ■

Lastly, let's mention that the *algebraic closure operator* ignores algebraic extensions.

Proposition 3.38 *A field extension E/K is algebraic iff $\overline{K} = \overline{E}$ (up to K-isomorphism). Hence, $\overline{K}$ contains a copy of every algebraic extension of K.*

Exercise 3.4.5 Prove Proposition 3.38.

As a consequence of Proposition 3.38, any discussion on algebraic extensions of K can be carried out inside a fixed algebraic closure $\overline{K}$.

3.5 Root Multiplicity

Given a polynomial $f(x) \in K[x]$, its splitting field over K is unique up to K-isomorphism. Hence, in the factorization of $f(x)$ into linear factors,

$$f(x) = a(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_r)^{m_r}, \text{ with } \alpha_i\text{'s distinct,} \tag{3.3}$$

a, the leading coefficient of $f(x)$, r, the number of distinct roots, and the *multiplicities* m_i of the roots α_i, do not depend on the splitting field where the factorization takes place.

Definition 3.13 A root α of a polynomial $f(x)$ has *multiplicity* m, if m is the exponent of the factor $(x-\alpha)$, in the factorization 3.3 of $f(x)$. A root of multiplicity 1 is called a *simple root*. A root of multiplicity > 1, is called a *multiple root*. To say that α is a root of multiplicity 0, is simply to say that α is not a root.

Definition 3.14 A polynomial $f(x) \in K[x]$ is said to be *separable*, it all its roots are simple roots. Otherwise, we say that $f(x)$ is *inseparable*.

A polynomial $f(x) \in K[x]$ is separable, iff all its irreducible factors are separable and distinct irreducible factors have no common roots. For this reason, our interest in separability, is focused mostly on irreducible polynomials.

Examples 3.5.1 It is possible to have all combinations on separability and irreducibility.

1. The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ is **separable** and **irreducible**.
2. The polynomial $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ is **separable** and **reducible**.
3. The polynomial $(x^2 - 2)^2 \in \mathbb{Q}[x]$ is **inseparable** and **reducible**.
4. Let t be a variable, and $K = \mathbb{Z}_2(t)$ the field of rational functions with coefficients in $\mathbb{Z}_2$. An easy degree argument shows that the polynomial $f(x) = x^2 - t \in K[x]$ is **irreducible**. If α is one root of this polynomial, then $\alpha^2 = t$, and, being of characteristic 2, we have $(x - \alpha)^2 = x^2 - t$. Hence $f(x)$ is **inseparable** over K.

The *derivative* of a polynomial is defined using the formal rules of calculus.

Definition 3.15 Let

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

be a polynomial in $K[x]$. We define the first *derivative* of $f(x)$ by

$$f'(x) = a_0nx^{n-1} + a_1(n-1)x^{n-2} + \cdots + a_{n-1}.$$

Higher order derivatives are defined recursively, and denoted by $f^{(k)}(x)$ for $k \geq 0$, as follows:

$$f^{(0)}(x) := f(x) \quad \text{and} \quad f^{(k)}(x) := \left(f^{(k-1)}(x)\right)'.$$

Note that when taking the derivative, the degree goes down by at least one. It follows that when $k > \deg(f(x))$, we get $f^{(k)}(x) = 0$. In characteristic $p \neq 0$, the degree may go down by more than one. For example, the derivative of $f(x) = x^2 - t$ in Example 3.5.1.4 above is 0. For any polynomial $f(x)$ in characteristic p, we have $f^{(p)}(x) = 0$.

Proposition 3.39 *Let K be a field.*

1. *The map $D_x : K[x] \to K[x]$ given by $D_x(f(x)) = f'(x)$, is K-linear.*
2. $(f(x)g(x))' = f(x)g'(x) + f'(x)g(x)$.
3. $(f(g(x))' = f'(g(x))g'(x)$.

Exercise 3.5.1 Prove Proposition 3.39.

Proposition 3.40 *Let $f(x) \in K[x]$, α an element of some extension of K, and $m \in \mathbb{N}$. Moreover, in characteristic $p \neq 0$, assume $m \leq p$ for the ($\Leftarrow$) direction. The multiplicity of α as a root of $f(x)$ is $\geq m$ iff α is a root of $f^{(i)}(x)$ for $0 \leq i < m$.*

Exercise 3.5.2 Prove Proposition 3.40.

Corollary 3.41 *Assume* $\mathrm{char}(K) = 0$. *Let $f(x) \in K[x]$ and let α be an element of some extension of K. The multiplicity m of α as a root of $f(x)$, is the smallest non-negative integer such that α is not a root of $f^{(m)}(x)$.*

Corollary 3.42 *$f(x) \in K[x]$ has a multiple root iff* $\mathrm{g.c.d.}(f(x), f'(x)) \neq 1$, *i.e. it is non–constant. In other words, $f(x)$ is separable iff $f(x)$ and $f'(x)$ are relatively prime.*

Examples 3.5.2

1. For $n \geq 1$, $x^{p^n} - x \in \mathbb{Z}_p[x]$ is separable since its derivative is -1. Therefore, it has p^n distinct roots, all of multiplicity 1. It is clear that this set of roots is closed under multiplication.
2. $x^n - 1 \in F[x]$ is separable iff $\mathrm{char} F \not| n$.

Corollary 3.43 *If $q(x) \in K[x]$ is irreducible of degree n, and* $\mathrm{char} K \not| n$, *then $q(x)$ is separable. In particular, if* $\mathrm{char} K = 0$ *then every irreducible polynomial over K is separable.* 02/27/20

Proof. The degree of $q'(x)$ is $n - 1$. Since $q(x)$ is irreducible, we have $\mathrm{g.c.d.}(q(x), q'(x)) = 1$, i.e. $q(x)$ and $q'(x)$ are relatively prime. ■

This corollary explains why we had to go to non-zero characteristic in Example 3.5.1.4, and why the degree of the polynomial was a multiple of the characteristic.

3.5.1 Finite Fields

We now obtain, as an easy consequence of the results in this section, a complete classification of all finite fields. Recall that a finite field has prime characteristic, and that the non-zero elements form a multiplicative finite group.

Definition 3.16 Let K be a field of prime characteristic p. The map

$$\begin{array}{rccc} \Phi: & K & \to & K \\ & a & \mapsto & a^p \end{array}$$

is called the *Frobenius map* of F.

Proposition 3.44 *The Frobenius map is a field monomorphism. If F is finite, then the Frobenius map is an autormorphism of F.*

Proof. Use the Binomial Theorem and note that the binomial coefficient $\binom{p}{k}$ is divisible by p when $0 < k < p$. ■

We'll use the following universal algebra lemma, together with the previous proposition, to obtain finite fields.

Lemma 3.45 *Let A and B be algebras of the same type (allow partial operations) and $\varphi_1, \varphi_2 : A \to B$ two homomorphisms. The equalizer of φ_1 and φ_2,*

$$[\varphi_1 = \varphi_2] := \{a \in A | \varphi_1(a) = \varphi_2(a)\}$$

is closed under all operations of A, hence it is a subuniverse, and a subalgebra of A, when non-empty.

Proof. Let f be an n-ary operation of A and $a_1, \ldots, a_n \in A$.

$$\begin{aligned} \varphi_1(f(a_1, \ldots, a_n)) &= f(\varphi_1(a_1), \ldots, \varphi_1(a_n)) \\ &= f(\varphi_2(a_1), \ldots, \varphi_2(a_n)) \\ &= \varphi_2(f(a_1, \ldots, a_n)) \end{aligned}$$ ■

Corollary 3.46 *The roots of $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$ form a subfield of the algebraic closure of $\mathbb{Z}_p$. This subfield is the splitting field of $f(x)$, and is a field with p^n elements.*

Proof. We saw in Example 3.5.2.1 that this polynomial has exactly p^n distinct roots. This set of roots is the equalizer $[\Phi^n = Id_K]$, where $K = \overline{\mathbb{Z}_p}$. ■

Theorem 3.47 *For every prime p and every $n \in \mathbb{N}$ there is a field of order p^n. Such field is unique, up to isomorphism. These are all the finite fields.*

Proof. The existence follows from Corollary 3.46. If K is a finite field of characteristic p, its prime subfield is $\mathbb{Z}_p$, and since K is a vector space over $\mathbb{Z}_p$, we have $|K| = p^n$ for some $n \geq 1$. The non-zero elements of K form a multiplicative group of order $p^n - 1$, so each of those elements satisfies $x^{p^n-1} = 1$, hence it is a root of $f(x) = x^{p^n} - x$. Clearly 0 is also a root of this polynomial, so K is a splitting field for this polynomial, and by Corollary 3.35.2, there is only one splitting field for $f(x)$, up to isomorphism. ■

Exercise 3.5.3 Show that a finite subgroup of the multiplicative group $K^\times$ of any field K is cyclic.

Definition 3.17 For a prime power $q = p^n$, we denote by $\mathbb{F}_q$, the finite field with q elements.

3.6 Separable Extensions

In this section we will consider the second issue related to the number of extensions of a homomorphism $\varphi : K \to L$, as discussed on and after Corollary 3.26. The bottom line is, that multiple roots of $p^\varphi(x)$ in L, reduce the number of extensions $\widehat{\varphi} : K(\alpha) \to L$ from the upper bound $\deg_K(\alpha)$.

Definition 3.18 Let F/K be an algebraic extension. An element $\alpha \in F$ is *separable* over K, if its minimal polynomial $\min_K(\alpha)$ is separable. We say that F/K is a *separable extension* if all elements of F are separable over K.

Proposition 3.48 *Let $q(x) \in K[x]$ be non-constant irreducible and $p = \mathrm{char} K \neq 0$.*

1. *$q(x)$ is inseparable iff $q'(x) = 0$ iff $q(x)$ is a polynomial in x^p.*

2. *There are $q_s(x) \in K[x]$ separable and $m \geq 0$ such that*

$$q(x) = q_s(x^{p^m}). \tag{3.4}$$

Moreover, q_s and m are unique with this property.

Proof. (1) If $q(x)$ is inseparable, by Corollary 3.42, g.c.d.$(q(x), q'(x))$ is non–constant. Since $q(x)$ is irreducible, this means that $q'(x)$ is a multiple of $q(x)$, but $\deg(q'(x)) < \deg(q(x))$. Hence $q'(x) = 0$.
If $q'(x) = 0$, then $q(x)$ has to have all its non-zero terms of the form $a_i x^i$ with i multiple of p. This means that $q(x) = f(x^p)$, for some $f(x) \in K[x]$.
If $q(x) = f(x^p)$, then $q'(x) = f'(x^p) \cdot (x^p)' = f'(x^p) \cdot p(x^{p-1}) = 0$.
Finally, if $q'(x) = 0$, then any root of $q(x)$ is also a root of $q'(x)$, hence a multiple root, and $q(x)$ is inseparable.
(2) If $q(x)$ is separable, take $q_s(x) = q(x)$ and $m = 0$. Otherwise, by Part 1 there is $f(x) \in K[x]$ with $q(x) = f(x^p)$. Clearly, $f(x)$ is irreducible, and $\deg(f(x)) < \deg(q(x))$, so an induction argument shows that there are $f_s(x)$ and $k \geq 0$ such that $f_s(x)$ is separable, and $f(x) = f_s(x^{p^k})$. Take $q_s(x) = f_s(x)$ and $m = k + 1$. The uniqueness of m follows since, by separability of q_s, and part 1, m it is the largest integer such that $q(x)$ is a polynomial in x^{p^m}. Once m is determined, there is only one q_s satisfying (3.4). ■

Definition 3.19 Refering to Proposition 3.48.2, the degree of q_s is called the *separable degree* of q, and it is denoted $\deg_s(q(x))$. The exponent p^m is called the *inseparable degree* of q, and it is denoted $\deg_i(q(x))$. Thus, we have

$$\deg(q(x)) = \deg_s(q(x)) \cdot \deg_i(q(x)). \tag{3.5}$$

For the sake of consistency, when char$K = 0$, we let $q_s(x) = q(x)$ and *separable degree* is just the degree. The inseparable degree is 1, so that Equation 3.5 holds for every field K, regardless of characteristc.

From decompositon (3.4) we get.

Corollary 3.49 *For $q(x) \in K[x]$ non-constant, irreducible polynomial, and $p = \text{char}K \neq 0$, the separable degree is the number of distinct roots, and the inseparable degree is the common multiplicity of all its roots, which is a power of p. Each root of $q(x)$ is a p^m-th root of a root of $q_s(x)$.*

Proof. Let $a_1, \ldots, a_r$ be the distinct roots of $q_s(x)$. By Proposition 3.48 we have

$$\begin{aligned} q_s(x) &= (x-a_1)\cdots(x-a_r), \quad \text{and} \\ q(x) &= (x^{p^m}-a_1)\cdots(x^{p^m}-a_r), \end{aligned}$$

so, the roots of $q(x)$ are the p^m-th roots of $a_1, \ldots, a_r$. If α_i is a p^m-th root of a_i, then $\alpha_i^{p^m} = a_i$ and

$$x^{p^m} - a_i = x^{p^m} - \alpha_i^{p^m} = (x-\alpha_i)^{p^m}.$$

Since $a_1, \ldots a_r$ are distinct, $\alpha_1, \ldots, \alpha_r$ are also distint, so

$$q(x) = (x-\alpha_1)^{p^m} \cdots (x-\alpha_r)^{p^m}$$

has $r = \deg_s(q(x))$ distinct roots, each with multiplicity $p^m = \deg_i(q(x))$. ■

From Proposition 3.25 and Corollary 3.49, we immediately get.

Proposition 3.50 *Let α be algebraic over K. The number of K-homomorphisms from $K(\alpha)$ to $\overline{K}$ is equal to the separable degree of* $\min_K(\alpha)$.

Due to Proposition 3.50 we make the following definition.

Definition 3.20 For an algebraic extension F/K the *separable degree* of F over K, denoted by $[F:K]_s$ is the number of K-homomorphisms from F to $\overline{K}$, i.e.

$$[F:K]_s := |\mathrm{Hom}_K(F, \overline{K})|.$$

Corollary 3.26 can now be rewritten and extended as follows.

Corollary 3.51 *Let α be algebraic over K. $[K(\alpha):K]_s \leq [K(\alpha):K]$. Moreover, in characteristic p, $[K(\alpha):K] = p^m \cdot [K(\alpha):K]_s$, where p^m is the common multiplicity of all the roots of* $\min_K(\alpha)$. *Thus, α is separable over K iff $[K(\alpha):K] = [K(\alpha):K]_s$. In characteristic 0, we always have $[K(\alpha):K] = [K(\alpha):K]_s$.*

Proposition 3.52 *Let K be a field of prime characteristic p, and $\Phi : K \to K$ the Frobenius endomorphism.*

1. *If the Frobenius endomorphism is surjective, then every irreducible polynomial $q(x)$ over K is separable.*

2. *Conversely, if the Frobenius endomorphism is not surjective, then there is an inseparable irrreducible polynomial in $K[x]$.*

Proof. (1) Let $q(x) \in K[x]$ be irreducible. For the sake of contradiction, assume $q(x)$ is inseparable. By Proposition 3.48.1, $q(x)$ is a polynomial in x^p, i.e. there is $f(x) \in K[x]$ so that $q(x) = f(x^p)$. So we have:

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \\ q(x) &= a_n x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1 x^p + a_0 \end{aligned}$$

Since Φ is surjective, there are $b_0, \ldots, b_n \in K$ such that $a_i = \Phi(b_i) = b_i^p$. Thus, we have, using Proposition 3.44,

$$\begin{aligned} q(x) &= b_n^p x^{np} + b_{n-1}^p x^{(n-1)p} + \cdots + b_1^p x^p + b_0^p \\ &= \left(b_n x^n + b_{n-1}x^{(n-1)} + \cdots + b_1 x + b_0\right)^p, \end{aligned}$$

contradicting the irreducibility of $q(x)$.

(2) Suppose now that Φ is not surjective. Let $a \in K - \Phi(K)$, and consider the polynomial $q(x) = x^p - a$. Since $q'(x) = 0$, by Corollary 3.42, $q(x)$ is inseparable. It has a multiple root, call it α, so $\alpha^p = a$, and $\min_K(\alpha)$ is a factor of $q(x)$. Since $a \notin \Phi(K)$, we have $\alpha \notin K$, and

$$1 < \deg_K(\alpha) = \deg(\min_K(\alpha)) \leq \deg(q(x)) = p.$$

Note that $(x-\alpha)^p = x^p - \alpha^p = x^p - a = q(x)$, so α is the only root of $\min_K(\alpha)$, and its multiplicity as a root of $\min_K(\alpha)$ equals $\deg_K(\alpha)$. On the other hand, by Corollary 3.51, this multiplicity is a power of p, So, $\deg_K(\alpha) = p$ and $q(x) = \min_K(\alpha)$ is irreducible over K. ■

Definition 3.21 A field K is said to be *perfect*, if every irreducible polynomial over K is separable. By Corollary 3.43 and Proposition 3.52, this condition is equivalent to either K having characteristic 0, or having prime characteristic, and the Frobenius map being surjective (many authors take this disjunction as the definition of perfect).

Corollary 3.53 1. *Every finite field $\mathbb{F}_q$ is perfect.*

2. *Over a finite field $\mathbb{F}_q$, every irreducible polynomial is separable.*

3. If K is perfect, and F/K is algebraic, then F is perfect.

Exercise 3.6.1 Prove Corollary 3.53.

Example 3.5.1 of an irreducible and inseparable polynomial, was over the field $K = \mathbb{Z}_2(t)$, an infinite field, and transcendental extension of a field of prime characteristic. The previous corollary shows why we had to go there to find it. In a sense, that example is minimal and representative of what is needed.

Proposition 3.54 *Let $K \leq E \leq F$ be an algebraic tower.* 03/12/20

$$[F : K]_s = [F : E]_s \cdot [E : K]_s.$$

Proof. WLOG, we may assume $\overline{K} = \overline{E} = \overline{F}$, so we need to show

$$|\mathrm{Hom}_K(F, \overline{K})| = |\mathrm{Hom}_E(F, \overline{K})| \cdot |\mathrm{Hom}_K(E, \overline{K})|.$$

Given $\varphi \in \mathrm{Hom}_K(E, \overline{K})$, by Theorem 3.32, there is $\widetilde{\varphi} : \overline{K} \to \overline{K}$ which extends φ. For each φ fix one such $\widetilde{\varphi}$, and consider the map

$$\begin{array}{rccc} \nu : & \mathrm{Hom}_K(E, \overline{K}) \times \mathrm{Hom}_E(F, \overline{K}) & \to & \mathrm{Hom}_K(F, \overline{K}) \\ & (\varphi, \psi) & \mapsto & \widetilde{\varphi} \circ \psi \end{array}$$

By Corollary 3.37, $\widetilde{\varphi}$ is a K-automorphism of $\overline{K}$. Given $\gamma \in \mathrm{Hom}_K(F, \overline{K})$, let

$$\varphi = \gamma|_E \in \mathrm{Hom}_K(E, \overline{K}), \text{ and } \psi = \widetilde{\varphi}^{-1} \circ \gamma.$$

For $a \in E$, $\gamma(a) = \varphi(a)$, so $\psi(a) = a$, and $\psi \in \mathrm{Hom}_E(F, \overline{K})$ and $\nu(\varphi, \psi) = \widetilde{\varphi} \circ \widetilde{\varphi}^{-1} \circ \gamma = \gamma$, so ν is surjective.
To see that ν is injective, let $\varphi_1, \varphi_2 \in \mathrm{Hom}_K(E, \overline{K})$ and $\psi_1, \psi_2 \in \mathrm{Hom}_E(F, \overline{K})$, be such that $\nu(\varphi_1, \psi_1) = \nu(\varphi_2, \psi_2)$, i.e. $\widetilde{\varphi_1} \circ \psi_1 = \widetilde{\varphi_2} \circ \psi_2$. It follows that $\psi_2 = \widetilde{\varphi_2}^{-1} \circ \widetilde{\varphi_1} \circ \psi_1$, and $\widetilde{\varphi_2}^{-1} \circ \widetilde{\varphi_1}$ fixes E, so $\widetilde{\varphi_1}|_E = \widetilde{\varphi_2}|_E$, i.e. $\varphi_1 = \varphi_2$. Since $\widetilde{\varphi}$ was uniquely selected for each φ, we get $\widetilde{\varphi_1} = \widetilde{\varphi_2}$, and it follows that $\psi_1 = \psi_2$. ■

Scholium 3.55 *Let $K \leq E \leq F$ be an algebraic tower, and $\overline{K}$ their algebraic closure. There is a bijection*

$$\mathrm{Hom}_K(F, \overline{K}) \approx \mathrm{Hom}_E(F, \overline{K}) \times \mathrm{Hom}_K(E, \overline{K}).$$

Proposition 3.56 *For every finite extension E/K, we have*

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

Moreover,

1. *If* $\mathrm{char} K = 0$, *then* $[E : K] = [E : K]_s$.
2. *If* $\mathrm{char} K = p \neq 0$, *then* $[E : K] = p^m [E : K]_s$, *for some* $m \geq 0$.

Proof. Any finite extension is an extension by finitely many algebraic elements, i.e. $E = K(\alpha_1, \ldots, \alpha_n)$. That places E at the top of a finite tower, with finite simple steps. For each step, Corollary 3.51 yields the desired result. Theorem 3.10.4 and Proposition 3.54 allow us to combine them. ■

The next lemma does for separable extensions what Lemma 3.14 did for algebraic extensions.

Lemma 3.57 *Let $K \leq E \leq F$, and $\alpha \in F$, algebraic over K.*

$$\begin{tikzcd} \alpha \in F \arrow[d, dash] \\ E \arrow[d, dash, "sep"] \\ K \end{tikzcd}$$

1. *If α is separable over K, then it is separable over E.*
2. *If α is separable over E, and E/K is separable, then α is separable over K.*

Exercise 3.6.2 Prove Lemma 3.57.

Proposition 3.58 *Let E/K be a finite extension. TFAE:*

1. *E is separable over K;*
2. *E is generated by finitely many separable element;*
3. $[E : K] = [E : K]_s$.

Proof. (1) $\Rightarrow$ (2) is immedidate.
(2) $\Rightarrow$ (3). Let $E = K(\alpha_1, \ldots, \alpha_n)$ with α_i's separable over K, so that E

$$\begin{array}{c} E = K(\alpha_1, \ldots, \alpha_n) \\ \vdots \\ K(\alpha_1, \ldots, \alpha_i) \\ | \\ K(\alpha_1, \ldots, \alpha_{i-1}) \\ \vdots \\ K(\alpha_1) \\ | \\ K \end{array}$$

is at the top of a finite tower of simple extensions. By Lemma 3.57, we have that α_i is separable over $K(\alpha_1, \ldots, \alpha_{i-1})$, so each step of the tower is separable, and by Corollary 3.51, the desired equality holds on each step. By Proposition 3.54, the equality holds for the extension E/K.

(3) $\Rightarrow$ (1). Assume $[E : K] = [E : K]_s$, and let $\alpha \in E$. Consider the tower $K \leq K(\alpha) \leq E$. Using Theorem 3.10 and Proposition 3.54, together with Proposition 3.56, we get

$$\begin{aligned} [K(\alpha) : K] &= \frac{[E : K]}{[E : K(\alpha)]} = \frac{[E : K]_s}{[E : K(\alpha)]} \\ &\leq \frac{[E : K]_s}{[E : K(\alpha)]_s} = [K(\alpha) : K]_s \\ &\leq [K(\alpha) : K] \end{aligned}$$

which yields $[K(\alpha) : K]_s = [K(\alpha) : K]$, showing α is separable over K. ■

Using the previous proposition, we can now show that every finite separable extension is simple.

Theorem 3.59 [Primitive Element Theorem] *Every finite separable extension E/K is a simple extension.*

Proof. When K is finite, E is also finite, and the multiplicative group $E^\times$ is cyclic.

Assume now that K is infinite. We proceed by induction on $[E : K]$. The result is trivial when $[E : K] = 1$. By Proposition 3.58, it suffices to consider the case $E = K(\alpha, \beta)$. Let $n = [E : K] = [E : K]_s > 1$, and

$$\mathrm{Hom}_K(E, \overline{K}) = \{\varphi_1, \ldots, \varphi_n\}.$$

Let $\alpha_i = \varphi_i(\alpha)$ and $\beta_i = \varphi_i(\beta)$. The polynomial

$$f(x) = \prod_{i<j} ((\alpha_i + \beta_i x) - (\alpha_j + \beta_j x))$$

has degree $\binom{n}{2}$, and at most that many roots in K. Let $t \in K$ be such that $f(t) \neq 0$. Since $t \in K$, we have $\varphi_i(t) = t$. Setting $\gamma = \alpha + \beta t$, and $\gamma_i = \varphi_i(\gamma)$ we get $\gamma_i = \alpha_i + \beta_i t$, and

$$f(t) = \prod_{i<j} (\gamma_i - \gamma_j) .$$

Since $f(t) \neq 0$, we must have that $\gamma_1, \ldots, \gamma_n$ are all distinct, hence $\varphi_1, \ldots, \varphi_n$ remain distinct, when restricted to $K(\gamma)$. This means that $[K(\gamma) : K]_s \geq n$, from which it follows that $K(\gamma) = K(\alpha, \beta)$. ■

Corollary 3.60 *Suppose E/K is separable and every $\alpha \in E$ has degree at most n over K. Then $[E : K] \leq n$, and E is a simple extension of K.*

Proof. Pick $\alpha \in E$ of largest degree over K. For any $\beta \in E$ there is $\gamma \in E$ such that $K(\alpha, \beta) = K(\gamma)$, so $\deg_K(\gamma) \geq \deg_K(\alpha)$. By maximality of $\deg_K(\alpha)$ we get $\deg_K(\alpha) = \deg_K(\gamma)$ and this forces the inclusion $K(\alpha) \leq K(\gamma)$ to be equality. Hence $\beta \in K(\alpha)$, and $K(\alpha) = E$. ■

Exercise 3.6.3 Let $K = \mathbb{F}_2(s, t)$ be the field of rational functions in two variables s and t, over the two element field, $\mathbb{F}_2$. Let $\alpha = \sqrt{s}$ and $\beta = \sqrt{t}$, i.e. α is a root of $x^2 - s \in K[x]$, and similarly for β. Prove or disprove that $K(\alpha, \beta)$ is a simple extension of K.

We close this section with a number of properties of separable extensions, which are identical in form, and often in proof, to properties of algebraic extensions.

Theorem 3.61 *Let $K \leq E \leq F$ be a algebraic tower. F/E and E/K are both separable extensions iff F/K is separable.*

Proof. Follows immediately using Lemma 3.57. ■

Proposition 3.62 *Let $K \leq F$ and $\alpha \in F$.*

1. *$K(\alpha)/K$ is separable iff α is separable over K.*
2. *The set of elements of F separable over K form a subfield of F.*

3. *Let $S \subseteq F$. If every $\alpha \in S$ is separable over K, then $K(S)/K$ is separable.*

4. *If $E_1, E_2 \leq F$ are separable extensions of K, then so is their composite E_1E_2.*

5. *If $E_i \leq F$ is separable over K, for every $i \in I$, then $\bigvee_{i \in I} E_i$ is also separable over K.*

Exercise 3.6.4 Prove Proposition 3.62.

Definition 3.22 The field

$$K^{sep} := \{\alpha \in \overline{K} | \alpha \text{ is separable over } K\},$$

is called the *separable closure* of K.

As it is defined in terms of the algebraic closure, the separable closure is unique, up to isomorphism. In characteristic 0, the separable closure is equal to the algebraic closure.

Proposition 3.63 1. *The map $K \mapsto K^{sep}$ is a closure operator.*

2. *K^{sep} is maximal with the property of being separable over K.*

3. *K^{sep} is minimal with the property of having no proper separable extension.*

Exercise 3.6.5 Prove Proposition 3.63.

3.7 Purely Inseparable Extensions

In terms of separability, purely inseparable elements/extensions are at the other end of the spectrum from separable elements/extensions. Since in characteristic zero, all algebraic extensions are separable, we restrict our attention in this section to fields of prime characteristic p. 03/17/20

Proposition 3.64 *Let E/K be an algebraic extension in prime characteristic p. Let $\alpha \in E$. TFAE:*

(i) $\min_K(\alpha)$ *has only one root;*

(ii) there is $k \in \mathbb{N}$ *such that* $\min_K(\alpha) = x^{p^k} - a$ *for some* $a \in K$*;*

(iii) there is $l \in \mathbb{N}$ *such that* $\alpha^{p^l} \in K$*.*

Proof. (i)⇒(iii) If $q(x) = \min_K(\alpha)$ has only one root, i.e. it has separability degree 1, then by (3.4) we have

$$q(x) = (x - \alpha)^{p^k} = x^{p^k} - \alpha^{p^k} \in K[x],$$

where $p^k = \deg_i(q(x))$ is the inseparable degree of $q(x)$, i.e. the multiplicity of α as a root of $q(x)$.
(iii)⇒(ii) If $a = \alpha^{p^l} \in K$, then α is a root of $f(x) = x^{p^l} - a$. Since $f(x)$ has only one root, namely α, then $q(x) = \min_K(\alpha)$ has only one root, and by (3.4) it has to be of the form $x^{p^k} - a$ where p^k is the multiplicity of α as a root of $q(x)$, and $a \in K$.
(ii)⇒(i) If $q(x) = \min_K(\alpha) = x^{p^k} - a$, then $\alpha^{p^k} = a$ and $q(x) = (x - \alpha)^{p^k}$ has α as its only root. ■

Definition 3.23 An element α, algebraic over K is said to be *purely inseparable* over K, if it safistifies the conditions of Proposition 3.64. An algebraic extension E/K is said to be *purely inseparable* if all elements of E are purely inseparable over K.

Remark 3.7.1 Let α be algebraic over K, and $q(x) = \min_K(\alpha)$. Using Definition 3.25, Proposition 3.64, and (3.5) we get

$$\begin{array}{rcrcl} \alpha \text{ is separable over } K & \Longleftrightarrow & \deg_s(q(x)) & = & \deg(q(x)) \\ & \Longleftrightarrow & \deg_i(q(x)) & = & 1, \\ \alpha \text{ is purely inseparable over } K & \Longleftrightarrow & \deg_s(q(x)) & = & 1 \\ & \Longleftrightarrow & \deg_i(q(x)) & = & \deg(q(x)). \end{array}$$

Examples 3.7.1 1. Note that all elements of K are purely inseparable over K. In fact, these are the only elements which are both separable and purely inseparable over K. To be separable, an element of an extension must have inseparable degree 1; to be purely inseparable, it must have separable degree 1.

2. Let $K = \mathbb{F}_2(t)$ be the field of rational functions in one variable t over $\mathbb{F}_2$. Let $f(x) = x^6 - t \in K[x]$. Since $R = \mathbb{F}_2[t]$ is a UFD, by Eisenstein Criterion, using t, we get that $f(x)$ is irreducible in $R[x]$. Since $f(x)$ is primitive in $R[x]$ and K is the field of fractions of R, by Corollary 1.18 to Gauss' lemma, $f(x)$ is irreducible in $K[x]$. Let α be a root of $f(x)$. Then $\min_K(\alpha) = f(x)$. By Remark 3.7.1 above and the fact that the inseparable degree of $f(x)$ is a power of 2, we can't have α purely inseparable over K. On the other hand, $g(x) = x^3 - t$ is separable over K, and $f(x) = g(x^2)$, so α has inseparability degree 2, and it is inseparable over K. In conclusion, the extension $K(\alpha)/K$ is neither separable, nor purely inseparable. It is just inseparable.

3. Let $K = \mathbb{F}_2(t)$, and let β be a root of $g(x) = x^3 - t$. Since $g'(x) = x^2$ has no common root with $g(x)$, β is separable over K, so $K(\beta)/K$ is separable. Since $\alpha^2 = \beta$, α is purely inseparable over $K(\beta)$. Any element $\gamma \in K(\alpha)$ has the form

$$\begin{array}{c} K(\alpha) \\ {\scriptstyle p.i.}\Big|\,{\scriptstyle 2} \\ K(\beta) \\ {\scriptstyle sep.}\Big|\,{\scriptstyle 3} \\ K \end{array}$$

$$\gamma = u + v\alpha,$$

for some $u, v \in K(\beta)$. It follows that $\gamma^2 = u^2 + v^2\alpha^2 \in K(\beta)$, so $K(\alpha)$ is purely inseparable over $K(\beta)$. Thus, we have decomposed the extension $K(\alpha)/K$ into two steps: the bottom one $K(\beta)/K$ is separable, and the top one $K(\alpha)/K(\beta)$ is purely inseparable. This is typical of any algebraic extension as we will see in Theorem 3.71 below.

Lemma 3.65 *Let K be a field of prime characteristic p, and let $\overline{K}$ be its algebraic closure.*

1. *For $n \geq 0$, the set*

$$K^{1/p^n} = \{\alpha \in \overline{K} | \alpha^{p^n} \in K\}$$

is an algebraic, purely inseparable, extension of K.

2. *The set*

$$K^{1/p^\infty} := \bigcup_{n=0}^{\infty} K^{1/p^n}.$$

is an algebraic, purely inseparable, extension of K

3. *If $K \mapsto K^{1/p^\infty}$ is a closure operator.*

4. *The field K^{1/p^∞} is a perfect field, the smallest perfect field that contains K.*

Exercise 3.7.1 Prove Lemma 3.65.

Definition 3.24 The field K^{1/p^∞} is called the *perfect closure* of K.

Lemma 3.66 *Let $\varphi : K \to L$ be a field homomorphism. There is a unique field homomorphism $\widehat{\varphi} : K^{1/p^\infty} \to \overline{L}$ which extends φ. Moreover,* $\mathrm{Im}(\widehat{\varphi}) \leq L^{1/p^\infty}$.

Proof. By Theorem 3.32 there is at least one such $\widehat{\varphi}$. Note however, that for $\alpha \in K^{1/p^\infty}$ its minimal polynomial is of the form $x^{p^k} - a$ for some $a \in K$. By Proposition 3.25, $\widehat{\varphi}(\alpha)$ has to be a root β of $x^{p^k} - \varphi(\alpha)$. It follows that $\beta^{p^k} = \varphi(\alpha) \in L$, so $\beta \in L^{1/p^\infty}$, and the polynomial factors as $x^{p^k} - \varphi(\alpha) = x^{p^k} - \beta^{p^k} = (x - \beta)^{p^k}$, so β is the only root of this polynomial. This means there is exactly one $\widehat{\varphi}$. ■

Proposition 3.67 *Let E/K be an algebraic extension, so that $E \leq \overline{K}$. TFAE:*

(i) *E/K is purely inseparable;*

(ii) *$E \leq K^{1/p^\infty}$;*

(iii) *$[E : K]_s = 1$, i.e. there is exactly one K-homomorphism $E \to \overline{K}$;*

(iv) *there is exactly one K-homomorphism $E \to K^{1/p^\infty}$;*

(v) *for every homomorphism $\varphi : K \to L$ there is a unique homomorphism $\widetilde{\varphi} : E \to \overline{L}$, that makes the following diagram commute,*

$$\begin{tikzcd} E \arrow[r, dashed, "\widetilde{\varphi}"] & \overline{L} \\ K \arrow[u, hook] \arrow[r, "\varphi"] & L \arrow[u, hook] \end{tikzcd}$$

and the image of $\widetilde{\varphi}$ is contained in L^{1/p^∞}.

This proposition tells us that K^{1/p^∞} is the largest purely inseparable extension of K. For that reason, some authors call the field K^{1/p^∞}, the *purely inseparable closure* of K. However, this name is not appropriate, as the *smallest* purely inseparable extension of K is K itself.

Proof. (i)⇒(ii) Follows from Proposition 3.64.
(ii)⇒(iii) Assume $E \leq K^{1/p^\infty}$. The inclusion map $i : E \to \overline{K}$ is a K-homomorphism. Now, let $\varphi : E \to \overline{K}$ K-homomorphims. For $\alpha \in E$, $\alpha^{p^k} \in K$ for some $k \geq 0$, and by Proposition 3.64, the minimal polynomial $\min_K(\alpha)$ has only one root, namely α. By Proposition 3.25, we must have $\varphi(\alpha) = \alpha$, so φ is just the inclusion map.
(iii)⇒(ii) Given $\alpha \in E$, from Proposition 3.54, we get $[K(\alpha) : K]_s = 1$. Proposition 3.50 yields that α is the only root of its minimal polynomial, and by Proposition 3.64, $\alpha \in K^{1/p^\infty}$.
(iii)⇒(iv) (iii) and (ii) are equivalent, and together, they clearly imply (iv).
(iv)⇒(v) Let $\psi : E \to K^{1/p^\infty}$ be the only one K-homorphism. Composing with $\widehat{\varphi}$ from Lemma 3.66 we get that $\widetilde{\varphi} = \widehat{\varphi} \circ \psi : E \to \overline{L}$ has the desired property.

$$\begin{tikzcd}
E \arrow[r, "\psi"] & K^{1/p^\infty} \arrow[r, "\widehat{\varphi}"] & \overline{L} \\
& K \arrow[ul, hook, "\iota"] \arrow[u] \arrow[r, "\varphi"] & L \arrow[u, hook]
\end{tikzcd}$$

For the uniqueness of $\widetilde{\varphi}$, note that $E \approx \psi(E) \leq K^{1/p^\infty}$, and for any K-homomorphism $\widetilde{\varphi} : E \to \overline{L}$ the homomorphism $\widetilde{\varphi} \circ \psi^{-1} : \psi(E) \to \overline{L}$ extends to $\widehat{\varphi}$ by Theorem 3.32. Uniqueness of $\widehat{\varphi}$ implies the uniqueness of $\widetilde{\varphi}$.
(v)⇒(i) Let $\alpha \in E$. The uniqueness of $\widetilde{\iota} : E \to \overline{K}$ extending $\iota : K \to \overline{K}$, implies, by Theorem 3.32, that there is only one $\overline{\iota} : K(\alpha) \to \overline{K}$ that extends ι. By Proposition 3.25 $\min_K(\alpha)$ has only one root in $\overline{K}$, and by Propostion 3.64, α is purely inseparable over K. ■

Corollary 3.68 *K^{1/p^∞} is maximal with the property of being purely inseparable over K, and it is minimal with the property of not having a proper inseparable extension.*

Lemma 3.69 *Let $K \leq E \leq F$, and $\alpha \in F$, algebraic over K.*

1. *If α is purely inseparable over K, then it is purely inseparable over E.*

2. *If α is purely inseparable over E, and E/K is purely inseparable, then α is purely inseparable over K.*

Proof. (1) is obvious and (2) follows using Proposition 3.64. ■

Theorem 3.70 *Let $K \leq E \leq F$ be a algebraic tower. F/E and E/K are both purely inseparable extensions iff F/K is purely inseparable.*

The next theorem shows that the decomposition we saw in Example 3.7.1.3 of an algebraic extension, as a two stage tower with purely inseparable on top, and separable at the bottom, holds in general.

Theorem 3.71 *Let E/K be an algebraic extension, so that $E \leq \overline{K}$, and let*

$$\begin{array}{c} E \\ {\scriptstyle p.i.}\Big| \\ E_s \\ {\scriptstyle sep.}\Big| \\ K \end{array}$$

$$E_s = E \cap K^{sep} = \{\alpha \in E | \alpha \textit{ is separable over } K\}.$$

1. *E_s/K is separable.*

2. *E/E_s is purely inseparable.*

3. *When E_s/K is a finite extension, $[E : K]_s = [E_s : K]$.*

Proof. 1. There is nothing to prove.

2. Let $\alpha \in E$, and $q(x) = \min_K(\alpha)$. By Proposition 3.48.2, there are $q_s(x) \in K[x]$ separable, and $k \geq 0$ such that $q(x) = q_s(x^{p^k})$. Since α^{p^k} is a root of $q_s(x)$, it is separable over K, i.e. $\alpha^{p^k} \in E_s$. By Proposition 3.64, α is purely inseparable over E_s.

3. Every K-homomorphism $\psi \in \mathrm{Hom}_K(E, \overline{K})$ restricts to a K-homomorphism $\psi|_{E_s} \in \mathrm{Hom}_K(E_s, \overline{K})$. Since E/E_s is purely inseparable, by Proposition 3.67, every K-homomorphism $\varphi \in \mathrm{Hom}_K(E_s, \overline{K})$ extends to a unique K-homomorphism $\widehat{\varphi} \in \mathrm{Hom}_K(E, \overline{K})$. So we have, $[E : K]_s = [E_s : K]_s$. Since E_s/K is separable, when this extension is finite, by Proposition 3.58, $[E_s : K]_s = [E_s : K]$. ■

Remark 3.7.2 When E_s/K is an infinite extension, the equality $[E_s : K]_s = [E_s : K]$ from Proposition 3.58 does not necessarily hold, and the best we can say is that $[E_s : K]_s$ is also infinite. Thus, one can say in general, that $[E : K]_s =_f [E_s : K]$, meaning they are both finite and equal, or both infinite. See Exercise 4.2.1 , and Example 4.6.1.

Definition 3.25 The *inseparable degree* of an algebraic extension E/K is defined as

$$[E : K]_i := [E : E_s].$$

When E_s/K is a finite extension, we have $[E : K] = [E : K]_s[E : K]_i$. Note that when E/K is a finite extension the inseparable equals

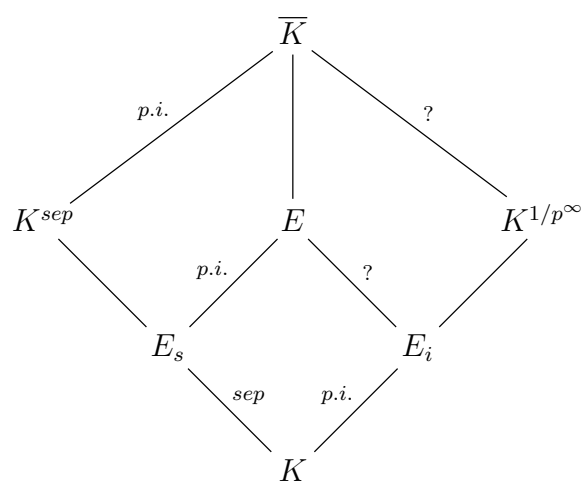
$$[E : K]_i = \frac{[E : K]}{[E : K]_s},$$

Corollary 3.72 *For an algebraic tower $K \leq E \leq F$,*

$$[F : K]_i = [F : E]_i \cdot [E : K]_i.$$

Exercise 3.7.2 Is $\overline{K}$ separable over K^{1/p^∞}?

Exercise 3.7.3 Let E/K be an algebraic extension, and let $E_i = E \cap K^{1/p^\infty}$. Prove or disprove that E/E_i is separable.



Chapter 4

Galois Theory

In Chapter 3 we have explored the set of homomorphisms from an algebraic extension E/K into their algebraic closure $\overline{K}$, $\mathrm{Hom}_K(E, \overline{K})$. We saw that the number of such homomorphisms is bounded by the degree of the extension (Proposition 3.56), and that this upper bound is achieved iff the extension is separable (Proposition 3.58). We often refer to this property by saying that a separable extension has "*enough*" homomorphisms. 03/24/20

In order to give the set $\mathrm{Hom}_K(E, \overline{K})$ an algebraic structure of its own, it would help if the image of those homomorphisms landed back inside E. This will not always be the case; but when this happens, we will get a group $\mathrm{Aut}_K(E)$. Galois Theory can be defined as the study of the connection between certain field extensions E/K and their groups of automorphisms.

4.1 Normal Extensions

Normal extensions are the extensions that have the desired property, of turning elements of $\mathrm{Hom}_K(E, \overline{K})$ into elements of $\mathrm{Aut}_K(E)$. There are a number of equivalent conditions that will ensure this.

Proposition 4.1 *Let E/K be an algebraic extension, so that $E \leq \overline{K}$. TFAE:*

(i) E is the splitting field of a set of polynomial over K;

(ii) for every K-homomorphism $\varphi : E \to \overline{K}$, $\varphi(E) = E$.

(iii) for every K-homomorphism $\varphi : E \to \overline{K}$, $\varphi(E) \subseteq E$.

(iv) For every K-homomorphism $\varphi : \overline{K} \to \overline{K}$, $\varphi(E) = E$.

(v) For every K-homomorphism $\varphi : \overline{K} \to \overline{K}$, $\varphi(E) \subseteq E$.

(vi) Every irreducible polynomial $q(x) \in K[x]$ which has a root in E splits in E.

Proof. (ii)⇒(iii) and (iv)⇒(v) are obvious.
(ii)⇒(iv) and (iii)⇒(v). Every K-automorphism of $\overline{K}$ restricts to an K-homomorphism from E to $\overline{K}$.
(iv)⇒(ii) and (v)⇒(iii). By Theorem 3.32, every K-homomorphism $E \to \overline{K}$ extends to an K-homomorphism $\overline{K} \to \overline{K}$.
(i)⇒(ii). Let $A \subseteq K[x]$, E the splitting field of A over K, and $\varphi : E \to \overline{K}$ a K-homomorphism. Let S be the set of roots of polynomials in A. So we have $E = K(S)$. By Proposition 3.25, φ has to map S to S. Since φ is injective and each polynomial in A has finitely many roots, we must have $\varphi(S) = S$. So, $\varphi(E) = \varphi(K(S)) = K(\varphi(S)) = K(S) = E$.
(iii)⇒(vi). Let $f(x) \in K[x]$ be irreducible with a root $\alpha \in E$. Let $\beta \in \overline{K}$ be another root of $f(x)$. By Proposition 3.25, the UMP of simple algebraic extensions, there is an K-homomorphism $\varphi : K(\alpha) \to \overline{K}$ such that $\varphi(\alpha) = \beta$. By Theorem 3.32 we can extend φ to a homomorphism $\varphi : E \to \overline{K}$. By (iii), we must have $\beta \in E$. So, $f(x)$ splits in E.
(vi)⇒(i), Let A be the set of irreducible polynomials over K which have a root in E. Then E is the splitting field of A over K.

■

Definition 4.1 An algebraic extension satisfying the conditions of Proposition 4.1 is said to be a *normal extension*.

Examples 4.1.1

1. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal, as it is the splitting field of $x^2 - 2 \in \mathbb{Q}(x)$.

2. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal, as it contains one of the roots of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$, but is missing the other two roots, which are not real.

3. For any K, $\overline{K}/K$ is normal.

Corollary 4.2 *Every quadratic extension is normal.*

Proof. Let $[E : K] = 2$, and $\alpha \in E - K$. The minimal polynomial $q(x) = \min_K(\alpha)$ has degree 2 and splits in E but not in K, so E is the splitting field of $q(x)$. ■

Definition 4.2 Let E/K be an algebraic extension so that $E \leq \overline{K}$, and $\alpha \in E$. For every K-automorphism φ of $\overline{K}$ the element $\varphi(\alpha)$ is called a *conjugate* or *Galois conjugate* of α over K. The extension $\varphi(E)/K$ is called a *conjugate extension* of E/K.

Note that the group $\mathrm{Aut}_K(\overline{K})$ acts by conjugation (as defined above) on the elements of $\overline{K}$. It also acts by conjugation on $\mathrm{Sub}_K(\overline{K})$, the lattice of all extensions E/K such that $E \leq \overline{K}$. We can now restate parts of Proposition 4.1 in the following corollary.

Corollary 4.3 *Let E/K be an algebraic extension so that $E \leq \overline{K}$. TFAE:*

i) *E/K is normal;*

ii) *E contains all conjugates of its elements;*

iii) *E/K has no conjugate extensions other than itself;*

iv) *E is stable under element conjugation, i.e. under the action of* $\mathrm{Aut}_K(\overline{K})$ *on* $\overline{K}$ *.*

v) *E is fixed under extension conjugation, i.e. under the action of* $\mathrm{Aut}_K(\overline{K})$ *on* $\mathrm{Sub}_k(\overline{K})$ *.*

By expanding the codomain of automorphisms of E/K to $\overline{K}$ we obtain the map

$$\begin{array}{rcl} \mathrm{Aut}_K(E) & \to & \mathrm{Hom}_K(E, \overline{K}) \\ \varphi & \mapsto & \iota \circ \varphi \end{array}$$

where $\iota : E \to \overline{K}$ is the inclusion map. Clearly this map is always injective, and we may, with a minor abuse of notation, think of it as an inclusion map, i.e. $\mathrm{Aut}_K(E) \subseteq \mathrm{Hom}_K(E, \overline{K})$. Using this notation, we get the following corollary from Proposition 4.1.

Corollary 4.4 *The algebraic extension E/K is normal iff*

$$\mathrm{Aut}_K(E) = \mathrm{Hom}_K(E, \overline{K}).$$

Proposition 4.5 *Let E/K be an algebraic extension, F/K a field extension, and EF their composite, say inside $\overline{F}$. If E/K is normal then so is EF/F.*

$$\begin{tikzcd}
 & \overline{F} \arrow[d, dash] & \\
 & EF \arrow[dl, dash] \arrow[dr, equal] & \\
E \arrow[dr, equal, "alg"'] \arrow[urr, equal] & & F \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Double lines denote normal extensions.

The converse does not hold. See Example 4.1.2.3 below.

Proof. Note that $\overline{F}$ contains an algebraic closure $\overline{K}$ of K, which in turn contains E, so the join EF makes sense in $\mathrm{Sub}_K(\overline{F})$, and it is algebraic over F. Let $\varphi : EF \to \overline{F}$ be a F-homomorphism. The restriction to E fixes K and takes values in $\overline{K}$, since every element of E, being algebraic over K has to be mapped to a root of its minimal polynomial. By normality of E/K we have $\varphi(E) \subseteq E$, and since $\varphi(F) = F$ we get $\varphi(EF) \subseteq EF$. Hence EF/F is normal. ■

Proposition 4.6 *1. Let $F/E/K$ be an algebraic tower. If F/K is normal, then so is F/E.*

2. The normal extensions of K form a complete sublattice of $\mathrm{Sub}_K(\overline{K})$.

3. Each $\varphi \in \mathrm{Aut}_K(\overline{K})$ induces a complete lattice automorphism of $\mathrm{Sub}_K(\overline{K})$. All normal extensions of K are fixed points of this automorphism.

Proof. (1) Let $\overline{F} = \overline{E} = \overline{K}$ be their algebraic closure. If $\varphi : F \to \overline{K}$ is an E-homomorphism, then it is a K-homomorphism as well, and by normality of F/K we have $\varphi(F) = F$. Hence F/E is normal.
(2) Let $(E_i/K | i \in I)$ be a family of normal extensions contained in $\overline{K}$, and $\bigvee_{i\in I} E_i$ their join in $\mathrm{Sub}_K(\overline{K})$. Let $A_i \subseteq K[x]$ be such that E_i is the splitting field of A_i, and let $A = \bigcup_{i\in I} A_i$. The splitting field of A is the smallest subfield of $\overline{K}$ that contains all E_i, i.e. $\bigvee_{i\in I} E_i$; hence $\left(\bigvee_{i\in I} E_i\right) \Big/ K$ is normal. Now, let $\varphi : \overline{K} \to \overline{K}$ be a K-homomorphism. Then for each $i \in I$, $\varphi(E_i) = E_i$, and therefore $\varphi\left(\bigcap_{i\in I} E_i\right) \subseteq \bigcap_{i\in I} \varphi(E_i) = \bigcap_{i\in I} E_i$; hence $\left(\bigcap_{i\in I} E_i\right) \Big/ K$ is normal. ■

Exercise 4.1.1 Prove Proposition 4.6.3.

Examples 4.1.2 1. Let $\alpha = \sqrt[4]{2}$ denote the positive fourth-root of 2.

$$\begin{array}{c} \mathbb{Q}(\sqrt[4]{2}) \\ | \\ \mathbb{Q}(\sqrt{2}) \\ | \\ \mathbb{Q} \end{array}$$

Since α is a root of $x^2 - \sqrt{2}$, we have $[Q(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$, making $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ a normal extension. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is also quadratic, hence normal. However, the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal, as the polynomial $x^4 - 2$ has a root in $\mathbb{Q}(\sqrt[4]{2})$ but does not split in it, as it has two non-real roots.

2. The splitting field of $x^3 - 1 \in \mathbb{Q}[x]$ is $\mathbb{Q}(\omega)$ where $\omega = \mathrm{cis}(2\pi/3)$ is a primitive cubic root of 1, i.e. a root of $x^3 - 1$ not equal to 1, hence a root of $x^2 + x + 1$. Being quadratic, $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal. Note that the two roots of this polynomial are ω and ω^2.

3. The roots of $x^3 - 2 \in \mathbb{Q}[x]$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. It follows that the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\omega, \sqrt[3]{2})$. It is easy to see that the degrees of extensions are as indicated in the following diagram:

$$\begin{tikzcd}
 & \mathbb{Q}(\omega, \sqrt[3]{2}) \arrow[dl, equal, "3"'] \arrow[dr, equal, "2"] & \\
\mathbb{Q}(\omega) \arrow[dr, equal, "2"'] & & \mathbb{Q}(\sqrt[3]{2}) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

The extension $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ is normal, but the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal. Normality on the top of the diamond does not imply normality at the bottom. This example is also a counterexample to the converse of Proposition 4.5.

Proposition 4.7 *Let E/K be an algebraic extension with algebraic closure $\overline{K}$.*

1. *The intersection of all normal extensions of K that contain E is equal to the composite (join) of all extensions conjugate to E/K. Let's denote it by E^n.*

2. *The map $E \mapsto E^n$ is a closure operator on the set of algebraic extensions of K. We call E^n the* normal closure *of E over K.*

3. *The normal closure of E/K is the spliting field of the set of polynomials*

$$A = \{\min_K(\alpha) \mid \alpha \in E^\times\}.$$

Proof. (1). Let F/K be a normal extension that contains E, and $\varphi(E)$ a conjugate of E for some $\varphi \in \mathrm{Aut}_K(\overline{K})$. From $E \leq F$ and normality of F/K, we get $\varphi(E) \leq \varphi(F) = F$. From here we get that the join L of all conjugates of E/K is contained in the intersection of normal extensions that contain E.

$$L := \bigvee_{\varphi \in \mathrm{Sub}_K(\overline{K})} \varphi(E) \leq \bigwedge_{\substack{E \leq F \\ F/K \text{ normal}}} F.$$

Now, by Proposition 4.6.3 any $\psi \in \mathrm{Aut}_K(\overline{K})$ induces a complete lattice automorphism in $\mathrm{Sub}_K(\overline{K})$ which permutes the conjugates of E, hence $\psi(L) = L$,

so L/K is normal, which yields the other inclusion.
(2). From Proposition 4.6.2, we get that the normal extensions or K form a closure system, with $E \mapsto E^n$ as the corresponding closure operator. ■

Exercise 4.1.2 Prove Proposition 4.7.3.

4.2 Galois Extensions

We will consider now extensions that are both separable and normal; that is, algebraic extensions that have enough homomorphisms into their algebraic closure, and where the image of those homomorphisms land back inside the extension. The second conditions turns the set of homomorphisms into a group, and the first guaratees this group is large enough, in particular, non-trivial. 03/26/2020

Definition 4.3 A *Galois extension* is an algebraic field extension E/K which is both separable and normal. For a Galois extension E/K, the group $\mathrm{Aut}_K(E)$ $(= \mathrm{Hom}_K(E, \overline{K}))$ is called the *Galois group* of the extension, and it is denoted $\mathrm{Gal}(E : K)$, $\mathrm{Gal}(E/K)$ or $\mathrm{Gal}_K(E)$.

From Propostions 4.5, 4.6, 3.62, and Lemma 3.57 we immediately get the following results.

Proposition 4.8 *1. Let $F/E/K$ be an algebraic tower, such that F/K is Galois. Then F/E is Galois, and if E/K is normal then it is also Galois.*

2. Let E/K be an algebraic extension, F/K a field extension, and FE their composite, say inside $\overline{F}$. If E/K is Galois then so is EF/F.

3. The Galois extensions of K form a complete sublattice of $\mathrm{Sub}_K(\overline{K})$.

Examples 4.2.1 1. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois of order 2, and its Galois group is cyclic of order 2.

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{id, \sqrt{2} \mapsto -\sqrt{2}\}.$$

2. The degree 3 extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois. Note that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})$ is a trivial group.

3. Let $\omega = \mathrm{cis}(2\pi/3)$. The extension $\mathbb{Q}(\omega)/\mathbb{Q}$ is Galois of order 2, and its Galois group is cyclic of order 2

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{id, \omega \mapsto \omega^2\}.$$

4. The extension $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ is Galois of order 6. By Proposition 3.25, any automorphism of this extension has to map ω to one of $\{\omega, \omega^2\}$, and $\sqrt[3]{2}$ to one of $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$. It then follows that

$$1: \begin{array}{ccc} \omega & \mapsto & \omega \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \end{array} \qquad \sigma: \begin{array}{ccc} \omega & \mapsto & \omega^2 \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \end{array}$$

$$\rho: \begin{array}{ccc} \omega & \mapsto & \omega \\ \sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2} \end{array} \qquad \rho\sigma: \begin{array}{ccc} \omega & \mapsto & \omega^2 \\ \sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2} \end{array}$$

$$\rho^2: \begin{array}{ccc} \omega & \mapsto & \omega \\ \sqrt[3]{2} & \mapsto & \omega^2\sqrt[3]{2} \end{array} \qquad \sigma\rho: \begin{array}{ccc} \omega & \mapsto & \omega^2 \\ \sqrt[3]{2} & \mapsto & \omega^2\sqrt[3]{2} \end{array}$$

are all the automorphisms, and they are all distinct. A little computation with the above maps, shows that

$$\mathrm{Gal}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) \approx S_3.$$

The extension $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ is the splitting field of the polynomial $x^3 - 2$, and the roots of this polynomial form an equilateral triangle on the complex plane. The group $\mathrm{Gal}(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ is the group of symmetries of this triangle.

Proposition 4.9 *If E/K is Galois then $|\mathrm{Aut}_K(E)| =_f [E : K]$, meaning that both are finite and equal, or both are infinite. When E/K is a finite extension, the converse holds.*

Proof. Assume E/K is a Galois extension. By normality, we have $\mathrm{Aut}_K(E) = \mathrm{Hom}_K(E, \overline{K})$. By separability, we have $[E : K]_s =_f [E : K]$ (See Exercise 4.2.1 below). Combining both, we get

$$|\mathrm{Aut}_K(E)| = |\mathrm{Hom}_K(E, \overline{K})| = [E : K]_s =_f [E : K]. \tag{4.1}$$

This proves one direction.
Now, assume that E/K is a finite extension. We have

$$|\mathrm{Aut}_K(E)| \leq |\mathrm{Hom}_K(E, \overline{K})| = [E : K]_s \leq [E : K]. \tag{4.2}$$

If we also have $|\mathrm{Aut}_K(E)| = [E : K]$, then must have equality across (4.2). The first equality yields E/K is normal, the last equality yields E/K is separable. ■

Exercise 4.2.1 Prove that if E/K is separable then $[E : K]_s =_f [E : K]$, meaning both are finite and equal, or both are infinite. Note that this and its converse were proved for finite extensions in Proposition 3.58. Show that the converse is not true in general.

Later, in Example 4.6.1, we will see that this weak version ($=_f$) of equality, is the best we can get, even for a Galois extension.

Examples 4.2.2 1. The extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is Galois of degree 4. Any automorphism of this extension is determined by what it does to $\sqrt{2}$ and $\sqrt{3}$. By Proposition 3.25, $\sqrt{2}$ has to be mapped to $\pm\sqrt{2}$, and $\sqrt{3}$ to $\pm\sqrt{3}$. Since we know that there are exactly four automorphism of this extension, the following maps are all automorphisms.

$$\begin{array}{lcl@{\qquad}lcl} \sqrt{2} & \mapsto & \sqrt{2} & \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & \sqrt{3} & \sqrt{3} & \mapsto & \sqrt{3} \\ & & & & & \\ \sqrt{2} & \mapsto & \sqrt{2} & \sqrt{2} & \mapsto & -\sqrt{2} \\ \sqrt{3} & \mapsto & -\sqrt{3} & \sqrt{3} & \mapsto & -\sqrt{3} \end{array}$$

2. Let $K = \mathbb{F}_p$, and $E = \mathbb{F}_{p^n}$. Since K is perfect, E/K is separable. E is the splitting field of $x^{p^n} - x$ over K, so E/K is normal. We know that $[E : K] = n$, so we get that $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a group of order n. The Frobenius endomorphism Φ of $\mathbb{F}_{p^n}$ is an element of G, and for any $x \in E^\times$, $\Phi^d(x) = x$ iff $x^{p^d} = x$ iff the multiplicative order of x divides $p^d - 1$. Since $E^\times$ is cyclic, there is $x \in E^\times$ of order $p^n - 1$. Hence the smallest d such that $\Phi^d = 1_E$ is at least n. But any element of G has order a divisor of n. We conclude that Φ has order n as an element of G, and G is cyclic generated by Φ.

4.3 Cyclotomic Extensions

03/31/20 Recall that for a prime p, the polynomial

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Q}[x] \tag{4.3}$$

is irreducible over $\mathbb{Q}$. One can, for example, use Eisenstein criteria on

$$\phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{p-1} x^{p-2} + \cdots + \binom{p}{2} x + \binom{p}{1}.$$

The roots of $\phi_p(x)$ are precisely the primitive p-th roots of unity. We want to extend this construction to arbitrary n-th roots. This will take a little more work as the polynomial

$$\frac{x^n - 1}{x - 1}$$

is not necessarily irreducible.

Definition 4.4 Given a field K, the *n-th roots of unity* are the roots of the polynomial $x^n - 1$.

Note that these roots depend only on the prime subfield of K, either $\mathbb{Q}$ or $\mathbb{F}_p$. Hence, they depend only on the characteristic of K. When n is a multiple of the characteristic, say $n = p^k \cdot m$, with $k \geq 1$ and $p \not| m$, the polynomial $x^n - 1$ is not separable, and its roots have multiplicity p^k, since $x^n - 1 = (x^m - 1)^{p^k}$. The n-th roots of unity are the p^k-th roots of the m-th roots of unity, and the latter are separable over the prime subfield. For these reasons, we will only consider n-th roots of unity for n not a multiple of the characteristic. There are exactly n of them.

The n-th roots of unity form a multiplicative subgroup of $K^\times$, which, by Exercise 3.5.3 , is cyclic, so it is the cyclic group of order n.

Definition 4.5 An n-th root of unity is called *primitive* if it is a generator of the cyclic group of n-th roots of unity. We will distinguish one of the primitive n-th roots of unity with the symbol ξ_n. In characteristic zero, we can take $\xi_n = \mathrm{cis}(2\pi/n)$.

Lemma 4.10 *Let K be a field, and $n \in \mathbb{N}$ not a multiple of* $\mathrm{char}(K)$.

1. *An n-th root of unity $\xi = \xi_n^k$ is primitive iff* $\text{g.c.d.}(n,k) = 1$.

2. *There are $\phi(n)$ primitive n-th roots of unity, where ϕ is Euler's function.*

3. *If d is a divisor of n, then every d-th root of unity is an n-th root of unity.*

4. *Each n-th root of unity is a primitive d-th root of unity for a unique d divisor of n*

Proof. 1. Recall from group theory, that for a cyclic group of order n, with generator a, an element a^k is also a generator iff $\text{g.c.d.}(n,k) = 1$.

2. Since $\phi(n)$ counts the number of $0 \leq k < n$ for which $\text{g.c.d.}(n,k) = 1$, from part (1), it follows that there are exactly $\phi(n)$ elements, each of which generates the group. Therefore, there are exactly $\phi(n)$ primitive n-th roots of unity.

3. This is obvious.

4. For ξ an n-th root of unity, let d be its multiplicative order in $K^\times$. ■

Definition 4.6 Let K be a field and n not a multiple of $\text{char}(K)$. The *n-th cyclotomic polynomial* is defined as the monic separable polynomial, whose roots are precisely the primitive n-th roots of unity, i.e.

$$\phi_n(x) := \prod_{\substack{\xi \text{ primitive} \\ n\text{-th root}}} (x - \xi) = \prod_{\text{g.c.d.}(k,n)=1} \left(x - \xi_n^k\right)$$

Note that the degree of $\phi_n(x)$ is $\phi(n)$. This explains why we use the same symbol. This definition includes the case considered in Equation 4.3.

Proposition 4.11 *Let K be a field, and n not a multiple of* $\text{char}(K)$.

1.
$$x^n - 1 = \prod_{d|n} \phi_d(x) \tag{4.4}$$

2.

$$\begin{aligned} \phi_1(x) &= (x-1) \\ \phi_n(x) &= \frac{x^n - 1}{\prod_{d|n, d<n} \phi_d(x)} \end{aligned} \tag{4.5}$$

3. For a prime p, different from $\mathrm{char}(K)$*,*

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$$

Formula (4.5), or equivalently (4.4), is a recursive formula that can be used to compute the cyclotomic polynomials.

Example 4.3.1 The cyclotomic polynomials $\phi_n(x)$ for $n \leq 12$ are given by

$$\begin{aligned} \phi_1(x) &= x - 1 \\ \phi_2(x) &= x + 1 \\ \phi_3(x) &= x^2 + x + 1 \\ \phi_4(x) &= x^2 + 1 \\ \phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\ \phi_6(x) &= x^2 - x + 1 \\ \phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ \phi_8(x) &= x^4 + 1 \\ \phi_9(x) &= x^6 + x^3 + 1 \\ \phi_{10}(x) &= x^4 - x^3 + x^2 - x + 1 \\ \phi_{11}(x) &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ \phi_{12}(x) &= x^4 - x^2 + 1 \end{aligned}$$

provided that n is not a multiple of $\mathrm{char}(K)$.

We now restrict our attention to $\mathrm{char}(K) = 0$ where the prime subfield is $\mathbb{Q}$. Let's recall Gauss lemma from Chapter 1.

Recall that, for a UFD R, a polynomial $f(x) \in R[x]$ is said to be *primitive*, if the g.c.d. of its coefficients is 1, i.e. a unit. Gauss's Lemma 1.17, and its Corollary 1.18, tell us

Lemma 4.12 [Gauss] *Let R be a UFD. If $f(x), g(x) \in R[x]$ are primitive then their product $f(x)g(x)$ is also primitive.*

Corollary 4.13 *Let R be a UFD, and Q its field of fractions. Let $f(x), h(x) \in R[x]$ be primitive and $g(x) \in Q[x]$ be such that $f(x) = g(x) \cdot h(x)$. Then $g(x) \in R[x]$, and it is also primitive.*

Proof. Write all coefficients of $g(x)$ in reduced form, and let a be the g.c.d. of the numerators of these coefficients, and b the *lcm* of the denominators. Then $\hat{g}(x) = \dfrac{b}{a} g(x)$ has coefficients in R and is primitive. From the assumption we get

$$b \cdot f(x) = a \cdot \hat{g}(x) \cdot h(x).$$

From Gauss' lemma, taking the g.c.d. of coefficients on both sides, we get that $a = b$ and $\hat{g}(x) = g(x)$. ■

As a special case we get.

Corollary 4.14 *Let $f(x), h(x) \in \mathbb{Z}[x]$ be primitive and $g(x) \in \mathbb{Q}[x]$ be such that $f(x) = g(x) \cdot h(x)$. Then $g(x) \in \mathbb{Z}[x]$, and it is also primitive.*

Theorem 4.15 [Gauss] *In characteristic zero, the cyclotomic polynomial $\phi_n(x)$ is monic, irreducible over $\mathbb{Q}$, with integral coefficients.*

Proof. The fact that it is monic is immediate from the definition. That it has rational coefficients follows by induction on n and the division algorithm, as follows. From the recursive formula (4.5) we have in $\mathbb{Q}[x]$

$$x^n - 1 = \phi_n(x) \cdot \prod_{d|n, d<n} \phi_d(x)$$

Since, by inductive hypothesis, $\prod_{d|n, d<n} \phi_d(x) \in \mathbb{Q}[x]$, the uniqueness in the division algorithm forces $\phi_n(x)$ to be in $\mathbb{Q}[x]$. Now, using again induction on n we can see that the coefficients of $\phi_n(x)$ are integers, using Corollary 4.14. To see that $\phi_n(x)$ is irreducible, write $\phi_n(x) = f(x) \cdot g(x)$ with $f(x), g(x) \in \mathbb{Z}[x]$, and $f(x)$ irreducible. Since $\phi_n(x)$ is monic, the leading coefficients of $f(x)$ and $g(x)$ are equal to ± 1, so we may take $f(x)$ to be monic.

Claim: if β is a root of $f(x)$ and p is a prime not divisor of n then β^p is also a root of $f(x)$. Since $p \not| n$, β^p is a primitive n-th root of unity, hence a root of $\phi_n(x)$. If it wasn't a root of $f(x)$ it would be a root of $g(x)$, so $g(\beta^p) = 0$, and β is a root of $g(x^p)$. Since $f(x)$ is the minimal polynomial of β over $\mathbb{Q}$, it divides $g(x^p)$, i.e. $g(x^p) = f(x) \cdot h(x)$ for some $h(x) \in \mathbb{Z}[x]$. If we reduce modulo p we get, using Fermat's little theorem,

$$\overline{g}(x)^p = \overline{g}(x^p) = \overline{f}(x) \cdot \overline{h}(x)$$

which tells us that any root of $\overline{f}(x)$ is also a root of $\overline{g}(x)$. Since $\overline{\phi_n}(x) = \overline{f}(x) \cdot \overline{g}(x)$, then $\overline{\phi_n}(x)$ has a multiple root, and so does $x^n - 1 \in \mathbb{F}_p[x]$. But this contradicts Corollary 3.42 since $p \not| n$, and $(x^n - 1)' = nx^{n-1} \neq 0$ whose only root is 0. This proves the claim.
Repeatedly using the claim we just proved, one can now see that for any k with g.c.d.$(k, n) = 1$, β^k is a root of $f(x)$, so all the roots of $\phi_n(x)$ are roots of $f(x)$. Since $\phi(x)$ has no multiple roots then we conclude that $g(x) = 1$ and $\phi(x) = f(x)$ is irreducible. ■

Corollary 4.16 *1. The cyclotomic polynomial $\phi_n(x)$ is the minimal polynomial for each primitive n-th roots of unity over $\mathbb{Q}$.*

2. $\mathbb{Q}(\xi_n)$ is the splitting field for $\phi_n(x)$ over $\mathbb{Q}$, and

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(n)$$

3. The Galois group

$$\mathrm{Gal}(\mathbb{Q}(\xi_n) : \mathbb{Q}) \approx U_n$$

the group of units of the ring $\mathbb{Z}_n$.

Proof. 1. For ξ a primitive n-root of unity, $\phi_n(\xi) = 0$, and since $\phi_n(x) \in Q[x]$ is monic and irreducible, we get $\min_{\mathbb{Q}}(\xi) = \phi_n(\xi)$.

2. By Lemma 4.10.1, all the roots of $\phi_n(x)$ are powers of ξ_n, and ξ_n is one of those roots, so $\mathbb{Q}(\xi_n)$ is the splitting field of $\phi_n(x)$ over $\mathbb{Q}$. The result on the degree follows from Proposition 3.12.

3. By Lemma 4.10.1, for each $k \in U_n$, ξ_n^k is a primitive n-th root of unity, i.e. a root of $\phi_n(x)$. By Proposition 3.25, there is a $\mathbb{Q}$-homomorphism, $\theta_k : \mathbb{Q}(\xi_n) \to \mathbb{A}$ such that $\theta_k(\xi_n) = \xi_n^k$. Since $\mathbb{Q}(\xi_n)/\mathbb{Q}$ is a Galois

extension, by Corollary 4.4, θ_k is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\xi_n)$. The map

$$\begin{array}{rccc} \theta: & U_n & \to & \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \\ & k & \mapsto & \theta_k \end{array}$$

is the desired isomorphism. In fact, $\theta_k \circ \theta_l(\xi_n) = \theta_k(\xi_n^l) = \xi_n^{kl} = \theta_{kl}(\xi_n)$, and since the image of ξ_n determines the automorphism, we get

$$\theta_k \circ \theta_l = \theta_{kl}. \qquad \blacksquare$$

Definition 4.7 The *n-th cyclotomic extension* of $\mathbb{Q}$ is the field $\mathbb{Q}(\xi_n)$.

We will revisit the cyclotomic extensions after the we establish the Fundamental Theorem of Galois Theory in Section 4.5.

Exercise 4.3.1 Show that if n is even then

$$\phi_{2n}(x) = \phi_n(x^2),$$

and if $n \geq 3$ is odd then

$$\phi_{2n}(x) = \phi_n(-x).$$

4.4 Posets - Galois Connections

In this section we take a brief detour into poset and lattice territory.

4.4.1 Artinian Induction

Definition 4.8 A poset P is said to be *Artinian* if it does not have any infinite descending chain. We also say that P satisfies the *descending chain condition*, DCC for short.

Examples 4.4.1

1. The set $(\mathbb{N}, \leq)$ is an Artinian poset. In fact, any well-ordered set is Artinian.
2. The set $(\mathbb{N}, |)$ is an Artinian poset.

3. An *Artinian Ring* is a ring in which the lattice $\mathrm{Idl}(R)$ is an Artinian poset.

Theorem 4.17 [Artinian Induction] *Let P be an Artinian poset, and let $S(x)$ be a first-order formula in the language of P. If we can show that*

$$(\forall x \in P)((\forall y < x)(S(y)) \Rightarrow S(x)),$$

then we can conclude that

$$(\forall x \in P)(S(x)).$$

Proof. Assume otherwise, and construct an infinite descending chain of elements that don't satisfy S. ■

Remarks 4.4.1

1. We will say that we are doing *induction* on P whenever we use this theorem.
2. Induction on the Artinian poset $(\mathbb{N}, \leq)$ is the so-called strong induction.
3. Induction on a well-ordered set is called *transfinite induction*.

4.4.2 Möbius Inversion Formula

Definition 4.9 A poset P is said to be *locally finite*, if for every $x, y \in P$, the interval $[x, y]$ is finite.

Examples 4.4.2

1. The poset $(\mathbb{N}, \leq)$ is locally finite.
2. The poset $(\mathbb{N}, |)$ is locally finite.

The Möbius function is usually defined with values in the ring of integers $\mathbb{Z}$, but it can be defined on any ring R.

Definition 4.10 Let P be a locally finite poset, and R a ring (e.g. $\mathbb{Z}$). Define the partial function *Mobiüs function*

$$\mu : P \times P \to R$$

for $y \leq x$ in P as follows:

$$\mu(x,x) = 1 \text{ and } \sum_{z \in [y,x]} \mu(y,z) = 0 \text{ when } y < x. \tag{4.6}$$

In other words,

$$\mu(y,x) = -\sum_{y \leq \underline{z} < x} \mu(y,z) \tag{4.7}$$

Remarks 4.4.2

1. Note that the variable of the summation is the second variable of the Möbius function. However, the definition could have been done by using the first variable, and we would have gotten the same function. Some authors do define it that way, using the formula in Exercise 4.4.1 .

2. If desired, the function could be a total function on $P \times P$ by setting $\mu(y,x) = 0$ when $y \not\leq x$, and this would be compatible with (4.6).

3. Sometimes we underline the summation variable, for the sake of clarity, as in (4.7).

Exercise 4.4.1 Let P be a locally finite poset. For $y \neq x \in P$

$$\sum_{y \leq z \leq x} \mu(z, x) = 0$$

Hint: Fix $y \in P$, and then use induction on the Artinian poset

$$\{u \in P \mid u > y\}.$$

Solution. That the poset

$$\{u \in P \mid u > y\}.$$

is Artinian, is immediate from P being locally finite. By induction on x. The bottom case is when $y \prec x$, and we have

$$\begin{aligned}
\sum_{y \leq z \leq x} \mu(z, x) &= \mu(y, x) + \mu(x, x) \\
&= \mu(y, x) + \mu(y, y) \\
&= \sum_{y \leq z \leq x} \mu(y, z) \\
&= 0
\end{aligned}$$

Now, using (4.7) and the induction hypothesis on $u < x$, we have

$$\begin{aligned}
\sum_{y \leq z \leq x} \mu(z, x) &= 1 - \sum_{y \leq z < x} \sum_{z \leq u < x} \mu(z, u) \\
&= 1 - \sum_{y \leq u < x} \sum_{y \leq z \leq u} \mu(z, u) \\
&= 1 - \mu(y, y) - \sum_{y < u < x} \sum_{y \leq z \leq u} \mu(z, u) \\
&= 1 - 1 - 0 = 0
\end{aligned}$$

■

Theorem 4.18 [Möbius Inversion Formula] *Let P be a poset with finite downsets, R a ring, and M an R-module. Let $f, g : P \to M$. If* 04/02/20

$$g(x) = \sum_{y \leq x} f(y),$$

then

$$f(x) = \sum_{y \leq x} \mu(y, x) g(y). \tag{4.8}$$

Proof. Since P has finite downsets, it is Artinian, and we proceed by induction on P. The statement is clear when x is minimal and the downset of x is $\{x\}$. Otherwise, usign a change in the order of summation

$$\begin{aligned}
f(x) &= g(x) - \sum_{\underline{y} < x} f(y) \\
&= g(x) - \sum_{\underline{y} < x} \sum_{\underline{z} \leq y} \mu(z, y) g(z) \quad \text{(by induction)} \\
&= g(x) - \sum_{\underline{z} < x} \sum_{z \leq \underline{y} < x} \mu(z, y) g(z) \quad \text{(summation order)} \\
&= g(x) - \sum_{\underline{z} < x} g(z) \sum_{z \leq \underline{y} < x} \mu(z, y) \\
&= g(x) + \sum_{\underline{z} < x} g(z) \mu(z, x) \quad (4.7) \\
&= \sum_{\underline{z} \leq x} \mu(z, x) g(z)
\end{aligned}$$

■

Remarks 4.4.3

1. The Formula (4.8) is called the **Möbius Inversion Formula**.

2. Let $x, y, u, v \in P$. Since the value $\mu(y, x)$ depends only on the interval $[y, x]$, we have that if $[y, x] \approx [v, u]$ (as posets) then $\mu(y, x) = \mu(v, u)$. In particular, in $(\mathbb{N}^+, |)$, if $b|a$ then $a = bd$ for some $d \in \mathbb{N}^+$ and $[b, a] \approx [1, d]$. Thus we have, $\mu(b, a) = \mu(1, d)$. This value is denoted $\mu(d) = \mu(a/b)$. From (4.6) we get: for $n > 1$,

$$\sum_{d|n} \mu(d) = 0.$$

Proposition 4.19 *In the poset* $(\mathbb{N}^+, |)$ *we have:*

1. $\mu(1) = 1$,
2. $\mu(n) = (-1)^k$ *if* n *is the product of* k *distinct primes,*
3. $\mu(n) = 0$ *otherwise, i.e.* n *is not square free.*

Proof. 1. The first part is obvious.

2. If n is square free, and the product of k distinct primes,

$$n = p_1 \cdots p_k$$

then for each proper subset $I \subset \{1, \ldots, k\}$ the number $n_I = \prod_{i \in I} p_i$ is the product of $|I|$ distinct primes and by induction $\mu(n_I) = (-1)^{|I|}$. For each $l < k$ there are $\binom{k}{l}$ subsets with l elements, and

$$0 = \sum_{I \subseteq \{1,\ldots,k\}} \mu(n_I) = \sum_{l=0}^{k-1} \binom{k}{l} (-1)^l + \mu(n)$$

By the binomial theorem we have

$$0 = (1-1)^k = \sum_{l=0}^{k} \binom{k}{l} (-1)^l,$$

and therefore, $\mu(n) = (-1)^k$.

3. When n is not square-free, with prime factorization

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad \text{some} \quad \alpha_i > 1,$$

Let $m = p_1 \cdots p_k$. Let D be the set of divisors of n, D_{sf} the set of square-free divisors of n, i.e the divisors of m, and $D' = D - D_{sf}$. In

particular, $n \in D'$ and by induction, for each $d \in D'$ if $d < n$, we have $\mu(d) = 0$. Now,

$$\begin{aligned} 0 &= \sum_{d \in D} \mu(d) \\ &= \sum_{d \in D_{sf}} \mu(d) + \sum_{d \in D'} \mu(d) \\ &= \sum_{d|m} \mu(d) + \sum_{d \in D', d \neq n} \mu(d) + \mu(n) \\ &= 0 + 0 + \mu(n) \end{aligned}$$

■

Corollary 4.20 *Let f, g be functions with domain $\mathbb{N}^+$. If $g(n) = \sum_{d|n} f(d)$ then $f(n) = \sum_{d|n} \mu(n/d) g(d)$.*

Examples 4.4.3

1. Since $n = \sum_{d|n} \varphi(d)$, then $\varphi(n) = \sum_{d|n} \mu(n/d) d$. For example,

   $\varphi(24) = \mu(6) \cdot 4 + \mu(3) \cdot 8 + \mu(2) \cdot 12 + \mu(1) \cdot 24 = 4 - 8 - 12 + 24 = 8$

   We say that d, a divisor of n, is *co-even*/*co-odd*, if n/d is square-free and the product of an even/odd number of distinct primes. So, we can write

   $$\varphi(n) = \sum_{\substack{d|n \\ \text{co-even}}} d - \sum_{\substack{d|n \\ \text{co-odd}}} d. \tag{4.9}$$

   Among the divisors of 24, 4 and 24 are co-even, whereas 8 and 12 are co-odd.

2. Since $x^n - 1 = \prod_{d|n} \phi_d(x)$, then

   $$\phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \frac{\prod_{\substack{d|n \\ \text{co-even}}} (x^d - 1)}{\prod_{\substack{d|n \\ \text{co-odd}}} (x^d - 1)} \tag{4.10}$$

Note that we are treating the multiplicative abelian group of non-zero rational functions, as a $\mathbb{Z}$-module. For Example,

$$\phi_{24}(x) = \frac{(x^{24}-1)(x^4-1)}{(x^{12}-1)(x^8-1)} = \frac{x^{12}+1}{x^4+1} = x^8 - x^4 + 1.$$

Exercise 4.4.2 Show that the sequence of coefficients of the cyclotomic polynomial $\phi_n(x)$, for $n \geq 2$, is palindrome, i.e. if

$$\Phi_n(x) = \sum_{i=0}^{\varphi(n)} a_i x^i,$$

then $a_{\varphi(n)-i} = a_i$.

Exercise 4.4.3 Prove or disprove: all cyclotomic polynomials have all their coefficients in $\{0, \pm 1\}$.

4.4.3 Closure Maps – Galois Connections

Definition 4.11 Let P be a poset. A map $c : P \to P$ is called a *closure map* if it satisfies: 04/14/20

(i) $x \leq c(x)$ (Extensive)

(ii) $c(c(x)) = c(x)$ (Idempotent)

(iii) $x \leq y \Rightarrow c(x) \leq c(y)$ (Isotone)

An element $y \in P$ is said to be *closed* if $y = c(x)$ for some $x \in P$, or equivalently if $y = c(y)$.

We often write $1 \leq c$ for (i), and $c^2 = c$ for (ii), in Definition 4.11.

Example 4.4.4 A closure operator on a set A is a closure map on $\mathcal{P}(A)$.

Lemma 4.21 *Let P be a poset and $c : P \to P$ a closure map. For any $x \in P$*

$$c(x) = \min\{y \in P | x \leq y \text{ and } y \textit{ is closed}\}$$

Proof. Clearly, the element $c(x)$ belongs to the set on the right. Now, if $y \in P$ is such that $x \leq y$ and y is closed, then, by isotonicity, we get $c(x) \leq c(y) = y$. ■

Proposition 4.22 *Let L be a complete lattice and $c : L \to L$ a closure map. The set M of closed elements of L under c is a complete lattice with the same meet as L, and with join of X given by $c(\bigvee X)$, the closure of the join of X is L.*

Proof. To see that the meet of closed elements is closed, let $(y_i | i \in I)$ be a family of closed elements, and let $y = \bigwedge y_i$. Since $y \leq y_i$, we get $c(y) \leq c(y_i) = y_i$ for all $i \in I$, and therefore $c(y) \leq \bigwedge y_i = y$. The other inequality holds by extension.
By Proposition 2.7, M is a complete lattice with the same meet as L. Now, if $X \subseteq M$, then for any $x \in X$, we have $x \leq \bigvee X \leq c(\bigvee X)$ and $c(\bigvee X) \in M$. If $y \in M$ is such that $x \leq y$ for all $x \in X$, then $\bigvee X \leq y$ and therefore $c(\bigvee X) \leq c(y) = y$. Thus, $c(\bigvee X)$ is the sup of X in M. ■

Example 4.4.5 Let G be a group and $L = \mathcal{P}(G)$. L is a complete lattice with meet by intersection and join by union. Let

$$\begin{array}{rccc} c: & L & \to & L \\ & X & \mapsto & \langle X \rangle \end{array}$$

Then $M = \mathrm{Sub}(G)$, which as shown earlier, is a complete lattice with meet by intersection and join, by the subgroup generated by the union.

Definition 4.12 A *Galois connection*

$$P \underset{\beta}{\overset{\alpha}{\rightleftharpoons}} Q$$

consists of two posets P and Q, and two maps $\alpha : P \to Q$ and $\beta : Q \to P$, satisfying:

1. α and β are antitone, i.e. order-reversing, meaning that for any $x_1, x_2 \in P$ and for any $y_1, y_2 \in Q$,

$$x_1 \leq x_2 \quad \Rightarrow \quad \alpha(x_1) \geq \alpha(x_2)$$

$$y_1 \leq y_2 \quad \Rightarrow \quad \beta(y_1) \geq \beta(y_2);$$

2. $\beta \circ \alpha \geq 1_P$ and $\alpha \circ \beta \geq 1_Q$, meaning that for any $x \in P$ and for any $y \in Q$,

$$\beta(\alpha(x)) \geq x \quad \text{and} \quad \alpha(\beta(y)) \geq y.$$

Lemma 4.23 [“3=1”] *If* $P \underset{\beta}{\overset{\alpha}{\rightleftharpoons}} Q$ *is a Galois connection then*

$$\alpha\beta\alpha = \alpha, \quad \textit{and} \quad \beta\alpha\beta = \beta.$$

Proof. Apply α to $1 \leq \beta\alpha$ to get $\alpha \geq \alpha\beta\alpha$. Apply $1 \leq \alpha\beta$ to α to get $\alpha \leq \alpha\beta\alpha$. ■

Oftentimes we will denote the two maps α and β of a Galois connection, by the same symbol, say $*$. In that case, the statement of the Lemma is $* * * = *$, or just “$3 = 1$”, for short. Condition 2 in Definition 4.12 can be written as $1 \leq **$.

Theorem 4.24 *Let* $P \underset{\beta}{\overset{\alpha}{\rightleftharpoons}} Q$ *be a Galois connection.*

1. $\beta\alpha$ *and* $\alpha\beta$ *are closure maps on* P *and* Q*, respectively.*
2. $x \in P$ *is closed iff* $x = \beta(y)$ *for some* $y \in Q$*.*
3. $y \in Q$ *is closed iff* $y = \alpha(x)$ *for some* $x \in P$*.*
4. *The posets* S *and* T *of closed elements of* P *and* Q *respectively are anti-isomorphic via the restrictions of* α *and* β*.*

Note that for closed elements of P and Q "$3 = 1$" improves to "$2 = 0$".

Corollary 4.25 *If* $L \underset{\beta}{\overset{\alpha}{\rightleftharpoons}} M$ *is a Galois connection between two complete lattices, then the complete lattices of closed elements are dual isomorphic.*

The following lemma gives us a tool to construct a wide variety of Galois connections, as the examples below show.

Lemma 4.26 *Let* A*,* B *be sets, and* $\rho \subseteq A \times B$ *a binary relation from* A *to* B*.*

$$\begin{array}{rcl} \mathcal{P}(A) & \underset{\beta}{\overset{\alpha}{\rightleftharpoons}} & \mathcal{P}(B) \\ X & \mapsto & \{b \in B | x \ \rho \ b \text{ for all } x \in X\} \\ \{a \in A | a \ \rho \ y \text{ for all } y \in Y\} & \leftarrow\!\shortmid & Y \end{array}$$

is a Galois connection, and the closed subsets of A *and* B *form dual isomorphic complete lattices. In both of them meet is intersection.*

Exercise 4.4.4 Prove Lemma 4.26.

Examples 4.4.6

1. Let A be a set and G a group (resp. monoid, semigroup) acting on A. Let $\rho \subseteq A \times G$ be given by

$$a \ \rho \ g \iff a^g = a$$

The closed subsets of G are subgroups (resp. submonoids, subsemigroups). The closed subsets of A are the subsets fixed by a subgroup (resp. submonoid, subsemigroup) of G. If $X \subseteq A$, then X^* is the *fixer* of X. For $Y \subseteq G$, let $H = \langle Y \rangle$. Then $Y^* = H^*$ consists is the set of elements fixed by Y.

2. When A is an algebra and G acts by automorphisms (resp. endomorphisms) on A, the closed subsets of A are subalgebras of A.

3. When F is a field and G a group of automorphisms of F, we get the classical Galois connection from Galois theory. See Section 4.5 below.

4. When G is a group acting on itself by conjugation then

$$x \rho y \iff xy = yx$$

and the closed subsets of G are precisely the centralizers in G. This is an example of a *symmetric Galois connection*, i.e. one where the two posets are the same, as well as the two maps α, β.

Corollary 4.27 *The centrilizers in a group G form a complete self-dual lattice contained, as a poset, in the interval $[Z(G), G]$.*

Exercise 4.4.5 Is the lattice of centrilizers in G a sublattice of $\mathrm{Sub}(G)$?

4.5 The Fundamental Theorem of Galois Theory

04/16/20 In this section we will look in detail at the Galois connection described in Example 4.4.6.3, arising from the binary relation $\rho \subseteq F \times G$, defined as follows: let F be a field and G a group of automorphisms of F. For $a \in F$ and $\varphi \in G$,

$$a \rho \varphi \iff \varphi(a) = a.$$

The closed subsets under this Galois connection are given by the following definition.

Definition 4.13 Let F be a field and G a group of automorphisms of F. We denote by F_G, or by $\mathrm{Fix}_F(G)$ the set

$$F_G := \{a \in F | \varphi(a) = a \text{ for all } \varphi \in G\}.$$

It is a subfield of F, called the *fixed field* of G.
For K a subfield of F, i.e. for F/K a field extension, recall from Definition 3.8 that we denote by $\mathrm{Aut}_K(F)$, or $\mathrm{Aut}(F/K)$ the set

$$\mathrm{Aut}_K(F) := \{\varphi \in \mathrm{Aut}(F) | \varphi(a) = a \text{ for all } a \in K\}.$$

It is a subgroup of $\mathrm{Aut}(F)$, called the *automorphism group* of the extension F/K. When F/K is a Galois extension, we also denote it by $\mathrm{Gal}(F/K)$, $\mathrm{Gal}_K(F)$, or $\mathrm{Gal}(F : K)$.

In particular, when we consider the group of all automorphisms of F, we get a Galois connection

$$\mathrm{Sub}(F) \underset{\beta}{\overset{\alpha}{\rightleftharpoons}} \mathrm{Sub}(\mathrm{Aut}(F)) \tag{4.11}$$

Remark 4.5.1 Note that $F_1 = F$, and for any $G \leq \mathrm{Aut}(F)$, F_G contains the prime subfield P of F, so the closed subfields of F lie in the interval $[P, F]$, between the prime subfield P and F, with F being one of them. On the group side, note that $\mathrm{Aut}(F/F) = 1$ and $\mathrm{Aut}(F/P) = \mathrm{Aut}(F)$, since any automorphism of F has to fix the multiplicative identity 1, and therefore must fix P. The closed subgroups of $\mathrm{Aut}(F)$ lie in the interval from 1 to $\mathrm{Aut}(F)$, with both of them being there.

Proposition 4.28 [Artin] *Let F be a field, and G a* **finite** *group of automorphisms of F. Let $E = F_G$ be the fixed subfield of G. The extension F/E is a finite Galois extension, and $\mathrm{Gal}(F/E) = G$. Using the * notation for the Galois connection, this last statement is $G^{**} = G$.*

Proof. Let $\alpha \in F$, and $G\alpha = \{\alpha_1, \ldots, \alpha_n\}$, the orbit of α under the action of G, with $\alpha_1, \ldots, \alpha_n$ distinct, and $\alpha = \alpha_1$. Let

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in F[x].$$

Note that any $\varphi \in G$ permutes the orbit of α. Thus it permutes the factors of $f(x)$, hence it fixes its coefficients, i.e. $f(x) \in E[x]$, and $f(x)$ is a multiple of $\min_E(\alpha)$, so

$$\deg_E(\alpha) \leq \deg(f(x)) = n \leq |G|.$$

Since $\alpha_1, \ldots, \alpha_n$ are distinct, it follows that α is separable over E. By Corollary 3.60, it follows that $[F : E] \leq |G|$. By the Primitive Element Theorem, F/E is a simple extension, so we can choose $\alpha \in F$ such that $F = E(\alpha)$, and F is the splitting field of $f(x) \in E[x]$, hence F/E is normal, and Galois. Using the * notation for the Galois connection we have,

$$G \leq G^{**} = (F_G)^* = E^* = \mathrm{Aut}(F/E).$$

On the other hand, since F/E is finite Galois, by Proposition 4.9,

$$|\mathrm{Aut}(F/E)| = [F : E] = [E(\alpha) : E] = \deg_E(\alpha) \leq n \leq |G|.$$

It follows that $\mathrm{Gal}(F/E) = G$. ■

Artin's proposition tells us that every **finite** subgroup of $\mathrm{Aut}(F)$ is closed under the Galois connection. The following proposition says that every subfield K of F, for which F/K is Galois, it closed under the Galois connection.

Proposition 4.29 *Let F/K be a Galois extension and $G = \mathrm{Gal}(F/K) = K^*$. The fixed field of G, $F_G = K$, i.e. $K^{**} = K$.*

Proof. We already have $K \leq K^{**}$. Let $\alpha \in K^{**}$. Any K-homomorphism $\varphi : K(\alpha) \to \overline{K}$, extends to a K-homomorphism $\widehat{\varphi} : F \to \overline{K}$. Since F/K is normal, we have $\mathrm{Im}(\widehat{\varphi}) = F$, i.e. $\widehat{\varphi} \in G$. Since $\alpha \in G^*$, it follows that $\alpha = \widehat{\varphi}(\alpha) = \varphi(\alpha)$, Thus $[K(\alpha) : K]_s = 1$, and since α is separable over K, we get $[K(\alpha) : K] = 1$, i.e. $K(\alpha) = K$, hence $\alpha \in K$. ■

Propositions 4.28 and 4.29 are the main ingredients of the fundamental theorem. It deals with finite Galois extensions. In Section 4.6 we will get the general case.

Theorem 4.30 [Fundamental Theorem of Galois Theory] *Let F be a field, and consider the Galois connection*

$$\begin{array}{ccc} \mathrm{Sub}(F) & \underset{\beta}{\overset{\alpha}{\rightleftharpoons}} & \mathrm{Sub}(\mathrm{Aut}(F)) \\ E & \longmapsto & \mathrm{Aut}_E(F) \\ F_H & \longleftarrow\!\shortmid & H \end{array}$$

from (4.11). Let $K \leq F$ such that F/K is a finite Galois extension, and let $G = \mathrm{Gal}(F/K) = \mathrm{Aut}_K(F)$.

1. *The maps α, β, restricted to $\mathrm{Sub}_K(F)$ and $\mathrm{Sub}(G)$,*

$$\mathrm{Sub}_K(F) \underset{\beta}{\overset{\alpha}{\rightleftharpoons}} \mathrm{Sub}(\mathrm{Aut}_K(F)). \tag{4.12}$$

   are bijections. The two lattices, $\mathrm{Sub}_K(F)$ and $\mathrm{Sub}(G)$ are anti-isomorphic, with α, β, inverse of each other, providing the dual isomorphisms.

2. *(α, β) preserves $[\ :\ ]$, meaning*

   - *for $K \leq E_1 \leq E_2 \leq F$, $[E_2 : E_1] = [E_1^* : E_2^*]$, and*
   - *for $1 \leq H_1 \leq H_2 \leq G$, $[H_2 : H_1] = [H_1^* : H_2^*]$.*

3. *(α, β) preserves normality, i.e. for $E \in \mathrm{Sub}_K(F)$, E/K is normal iff $\alpha(E)(= \mathrm{Aut}_E(F))$ is a normal subgroup of G. Moreover, in this case we have*

$$\mathrm{Gal}(E/K) \approx \frac{\mathrm{Gal}(F/K)}{\mathrm{Gal}(F/E)}.$$

Before we consider the proof of the Fundamental Theorem, let's consider a couple of examples.

Examples 4.5.1 1. In Example 4.2.1 we have seen that $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is a Galois extension, with Galois group isomorphic to the Klein 4-group,

$$V_4 = C_2 \times C_2 = \{1, a, b, c\} = \{++, +-, -+, --\}$$

where the two signs indicate where $\sqrt{2}$ and $\sqrt{3}$ are mapped, as we know that any automorphism must map $\sqrt{2} \mapsto \pm\sqrt{2}$, and $\sqrt{3} \mapsto \pm\sqrt{3}$. This group has three non-trivial, proper subgroups, namely $A = \langle a \rangle$, $B = \langle b \rangle$ and $C = \langle c \rangle$. By the FTGT, each of these subgroups fixes an intermediate subfield of this extension, i.e. a proper subfield of $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ that properly contains $\mathbb{Q}$, and these are all the intermediate subfields, $F_A = \mathbb{Q}(\sqrt{2})$, $F_B = \mathbb{Q}(\sqrt{3})$, $F_C = \mathbb{Q}(\sqrt{6})$.

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
A \arrow[dr, dash] & B \arrow[d, dash] & C \arrow[dl, dash] \\
 & V_4 &
\end{tikzcd}$$

2. In Example 4.1.2.4 we showed that $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ is Galois, with Galois group $G = \{1, \rho, \rho^2, \sigma, \rho\sigma, \sigma\rho\}$ isomorphic to S_3. In fact, G acts as the permutation group of the roots of $x^3 - 2$. Since we know all the subgroups of S_3, the FTGT gives us all the intermediate fields of this extension, it gives us the degree of the extensions, and it also tells us which of these extensions are normal and Galois. Recall that

$$\begin{array}{rrcl} \rho: & \omega & \mapsto & \omega \\ & \sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2} \end{array} \qquad \begin{array}{rrcl} \sigma: & \omega & \mapsto & \omega^2 \\ & \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \end{array}$$

In terms of the roots we have

$$\begin{array}{rrcl} \rho: & \sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2} \\ & \omega\sqrt[3]{2} & \mapsto & \omega^2\sqrt[3]{2} \\ & \omega^2\sqrt[3]{2} & \mapsto & \sqrt[3]{2} \end{array} \qquad \begin{array}{rrcl} \sigma: & \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \\ & \omega\sqrt[3]{2} & \mapsto & \omega^2\sqrt[3]{2} \\ & \omega^2\sqrt[3]{2} & \mapsto & \omega\sqrt[3]{2} \end{array}$$

The non-trivial, proper subgroups of S_3 are $A = \langle\sigma\rangle$, $B = \langle\sigma\rho\rangle$, $C = \langle\rho\sigma\rangle$, and $R = \langle\rho\rangle$. Hence the proper subfields of $F = \mathbb{Q}(\omega, \sqrt[3]{2})$, that properly contain $\mathbb{Q}$ are:

- $F_A = \mathbb{Q}(\sqrt[3]{2})$,
- $F_B = \mathbb{Q}(\omega\sqrt[3]{2})$,
- $F_C = \mathbb{Q}(\omega^2\sqrt[3]{2})$,
- $F_R = \mathbb{Q}(\omega)$.

$$\begin{tikzcd}
 & & \mathbb{Q}(\omega, \sqrt[3]{2}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash] & \mathbb{Q}(\omega\sqrt[3]{2}) \arrow[d, dash] & \mathbb{Q}(\omega^2\sqrt[3]{2}) \arrow[dl, dash] & \mathbb{Q}(\omega) \arrow[dl, equal] \\
 & \mathbb{Q} & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & & 1 \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\sigma\rangle \arrow[dr, dash] & \langle\sigma\rho\rangle \arrow[d, dash] & \langle\rho\sigma\rangle \arrow[dl, dash] & \langle\rho\rangle \arrow[dl, equal] \\
 & S_3 & &
\end{tikzcd}$$

Proof of Theorem 4.30. 04/21/20

1. We want to show that every subgroup of G, and every $E \in \mathrm{Sub}_K(F)$, are closed under the Galois connection (4.12). By Proposition 4.9, the group G is finite, and so are all its subgroups; thus Proposition 4.28 applies, and all subgroups of G are closed. By Proposition 4.8, for every $E \in \mathrm{Sub}_K F$, the extension F/E is Galois, and by Proposition 4.29, E is closed.

2. Let $K \leq E \leq F$. By Proposition 4.8, F/E is Galois. Using Proposition 4.9 for F/K and F/E, we get

$$[E : K] = \frac{[F : K]}{[F : E]} =^{(4.9)} \frac{|\mathrm{Aut}(F/K)|}{|\mathrm{Aut}(F/E)|} = \frac{|K^*|}{|E^*|} = [K^* : E^*].$$

   From here, one easily gets the general case. Note that this proof depends on F/K and F/E being finite. Below, in Lemma 4.37.1, we give a proof that does not depend on the finiteness of F/K, only the finiteness of E/K.

3. That (α, β) preserve normality, follows from Lemma 4.31 below. Suppose now that E/K is normal. Every K-automorphisms φ of F, restricts to a K-homomorphism $E \to F \to \overline{K}$, and by normality its image is equal to E, so it restricts to a K-automorphism $\varphi|_E$, of E. Clearly, the map

$$\begin{array}{ccc} \mathrm{Gal}(F/K) & \to & \mathrm{Gal}(E/K) \\ \varphi & \mapsto & \varphi|_E \end{array}$$

is a group homomorphism, with kernel equal to $\mathrm{Aut}(F/E) = \mathrm{Gal}(F/E)$. Conclude using the first isomorphism theorem for groups. ■

The preservation of normality by (α, β) does not require the Galois extension F/K to be finite.

Lemma 4.31 *Let F/K be a Galois extension, and $G = \mathrm{Gal}(F/K)$. For $E_1, E_2 \in \mathrm{Sub}_K(F)$. The subfields E_1 and E_2 are conjugate over K iff the subgroups E_1^* and E_2^* are conjugate in G.*

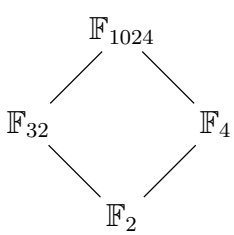
Proof. Suppose E_1, E_2 are conjugate, i.e. there is an automorphism $\varphi \in \mathrm{Aut}_K(F)$ such that $\varphi(E_1) = E_2$. For any $\psi \in E_2^* = \mathrm{Aut}_{E_2}(F)$, we have $\varphi^{-1} \circ \psi \circ \varphi$ fixes E_1, so we have a map, conjugation by φ,

$$\begin{array}{rcl} \mathrm{Aut}_{E_2}(F) & \to & \mathrm{Aut}_{E_1}(F) \\ \psi & \mapsto & \psi^{\varphi} \end{array}$$

which is easy to see is an isomorphism. Thus E_2^* and E_1^* are conjugate in G. Conversely, assume that E_2^* and E_1^* are conjugate in G, i.e. there is $\varphi \in G = \mathrm{Aut}_K(F)$ such that $(E_2^*)^{\varphi} = E_1^*$. We want to show that $\varphi(E_1) = E_2$. For $\alpha \in E_1$, and $\psi \in E_2^*$ we have $\psi^{\varphi} \in E_1^*$, so, $\varphi^{-1} \circ \psi \circ \varphi(\alpha) = \alpha$, i.e. $\psi \circ \varphi(\alpha) = \varphi(\alpha)$ and therefore, $\varphi(\alpha) \in E_2^{**} = E_2$, by Proposition 4.29. Thus, φ maps E_1 into E_2; similarly, φ^{-1} maps E_2 into E_1, and therefore $\varphi|_{E_1} : E_1 \to E_2$ is an isomorphism, i.e. E_1 and E_2 are conjugate subfields of F. ■

We now use the Fundamental Theorem of Galois Theory, the Fundamental Theorem of Finite Cyclic Groups, and what we know about finite fields, to count the number of irreducible polynomials of degree 10 over $\mathbb{F}_2$.

Example 4.5.2 In Example 4.2.2.2 we have shown that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension with cyclic Galois group of order n, generated by the Frobenius automorphism Φ. The cyclic group C_n has exactly one subgroup of order d for each d divisor of n. The lattice $\mathrm{Sub}(C_n)$ is isomorphic to the lattice of divisors of n. Therefore, $\mathbb{F}_{p^d}$ is a subfield of $\mathbb{F}_{p^n}$ iff d is a divisor of n. The lattice of subfields of $\mathbb{F}_{p^n}$ is dual-isomorphic to the lattice of subgroups of C_n. For example for $n = 1024 = 2^{10}$, there is a field with



1024 elements, namely, $\mathbb{F}_{2^{10}}$, the splitting field of the polynomial $x^{1024} - x \in \mathbb{Z}_2[x]$. This field has only three proper subfields, $\mathbb{F}_{2^1}$, $\mathbb{F}_4 = \mathbb{F}_{2^2}$, and $\mathbb{F}_{32} = \mathbb{F}_{2^5}$. This can be used to count the number of irreducible polynomials of degree 10 over $\mathbb{F}_2$. By uniqueness of finite fields, $\mathbb{F}_{1024}$ is the only extension of $\mathbb{F}_2$ of degree 10. The roots of all irreducible polynomials of degree 10 over $\mathbb{F}_2$ live in F_{1024}. All elements of $\mathbb{F}_{1024}$ have degree divisor of 10. Those of degree 5 are elements of $\mathbb{F}_{32}$, those of degree 2, are elements of F_4, and those of degree 1 are elements of $\mathbb{F}_2$. By the inclusion-exclusion principle, that leaves $1024-32-4+2 = 990$ elements of degree 10 over $\mathbb{F}_2$. Every irreducible polynomial over $\mathbb{F}_2$ is separable, so every irreducible polynomial of degree 10, has 10 of those 990 elements as its roots, and no two of those polynomials share a root. Therefore, there are 99 (monic) irreducible polynomials of degree 10 over $\mathbb{F}_2$.

Exercise 4.5.1 Show that the directed union

$$\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$$

is the algebraic closure of $\mathbb{F}_p$.

Exercise 4.5.2 What is the lattice of subgroups of U_n? What is the lattice of subfields of the cyclotomic extension $\mathbb{Q}(\xi_n)$? Write down the bijection between these two lattices.

We close this section with an improvement on Proposition 4.8.2, page 73 that will be needed in Chapter 5.

Proposition 4.32 *If E/K is a Galois extension and F/K is any field extension, then EF/F is Galois. Its Galois group embeds in* $\mathrm{Gal}(E/K)$*, and when E/K is finite,*

$$\mathrm{Gal}(EF/F) \approx \mathrm{Gal}(E/E \cap F).$$

$$\begin{tikzcd}
 & EF \arrow[dl, dash] \arrow[dr, equal] & \\
E \arrow[dr, equal] & & F \arrow[dl, dash] \\
 & E \cap F \arrow[d, dash] & \\
 & K &
\end{tikzcd}$$

Proof. From Proposition 4.8 we know that EF/F is a Galois extension. Since E/K is algebraic, each $\sigma \in \mathrm{Aut}(EF/F)$ maps E into $\overline{K}$, and since E/K is normal, we have $\sigma(E) = E$. This tells us that the map

$$\begin{array}{rccc} \varphi: & \mathrm{Gal}(EF/F) & \to & \mathrm{Gal}(E/K) \\ & \sigma & \mapsto & \sigma|_E \end{array}$$

is well-defined. It is clearly a homomorphism, and if $\sigma|_E = 1$ then σ fixes E and F, hence it fixes EF, and $\sigma = 1$. This shows φ is injective, giving us the desired embedding. Let $G = \mathrm{Gal}(EF/F)$. For every $\sigma \in G$, $\sigma|_E$ fixes $E \cap F$, so $\mathrm{Im}(\varphi) \leq \mathrm{Gal}(E/E \cap F)$. Let $H = \mathrm{Im}(\varphi)$. Then $H^* \geq E \cap F$. Note that for any $\sigma \in G = \mathrm{Gal}(EF/F)$, since $\sigma|_E \in H$, we have σ fixes $H^* = E_H$. Therefore $E_H \leq (EF)_G = F$, and $E_H = E \cap F$. We then get $H = H^{**} = (E \cap F)^* = \mathrm{Gal}(E/E \cap F)$. ■

4.6 Infinite Galois Extensions

Even though we would like to extend Theorem 4.30 to arbitrary Galois extensions, the following example, due to McCarthy [5], shows that it requires some adjustments.

Example 4.6.1 [McCarthy,1966] Let F be the splitting field over $\mathbb{Q}$ of the family of polynomials

$$\{x^2 - r | r \in \mathbb{Q}\}.$$

Remarks 4.6.1 Note that

1. F is generated, as an extension of $\mathbb{Q}$ by the set

$$R = \{\sqrt{p} | p \text{ is a prime, or } p = -1\}.$$

i.e. $F = \mathbb{Q}(R)$. Clearly, $F/\mathbb{Q}$ is a Galois extension, of infinite countable degree.

2. Any $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ is completely determined by where it maps the elements of R, and for each $\alpha \in R$, we must have $\sigma(\alpha) = \pm\alpha$. This implies that each $1 \neq \sigma$ has order 2, and $G = \mathrm{Gal}(F/\mathbb{Q})$ is elementary abelian 2-group, and can be viewed as a vector space over $\mathbb{F}_2$.

3. For each subset $S \subseteq R$ there is an automorphism $\sigma_S : F \to F$, such that $\sigma_S(\alpha) = -\alpha$ if $\alpha \in S$, and $\sigma_S(\alpha) = \alpha$ if $\alpha \in R - S$ Hence G is uncountable, and has uncountably many subgroups.

4. Let B be a basis for G as a vector space over $\mathbb{F}_2$. Then B is uncountable, and for each $\sigma \in B$, the set $B - \{\sigma\}$ generates a subgroup of index 2 in G. Therefore, G has **uncountably** many subgroups of finite index.

5. In this example we have

$$[F : \mathbb{Q}] < [F : \mathbb{Q}]_s = |\mathrm{Hom}_{\mathbb{Q}}(F, \mathbb{A})| = |\mathrm{Aut}_{\mathbb{Q}}(F)| = |\mathrm{Gal}(F/\mathbb{Q})|,$$

showing that Propositios 3.56, 4.9, and 3.58 do not hold in general for infinite extensions, not even when they are separable and Galois.

6. We have shown in Theorem 3.59, that any finite separable extension is *simple*, i.e. generated by a single element. Since $F/\mathbb{Q}$ is algebraic, F is countable, so it follows from Theorem 3.59 that there are only **countably** many $E \in \mathrm{Sub}_{\mathbb{Q}}(F)$ with $E/\mathbb{Q}$ a finite extension.

7. Since the Galois connection

$$\mathrm{Sub}_{\mathbb{Q}}(F) \underset{\alpha}{\overset{\beta}{\rightleftarrows}} \mathrm{Sub}(G)$$

maps finite extensions $E/\mathbb{Q}$ to subgroups of finite index in G, it follows from parts 4 and 6 above that that the maps α, β cannot be bijections.

Note however, that for any Galois extension F/K, Proposition 4.29 says that $\beta\alpha = 1$, and therefore α is injective and β is surjective.

Exercise 4.6.1 Prove the statement in Remark 4.6.1.4.

Exercise 4.6.2 Show that the group G in Example 4.6.1 is isomorphic to $\mathcal{P}(R)$ with symmetric difference as the binary operation.